

Informe de Criminología Virtual de McAfee:

Estudio Norteamericano Sobre Crimen
Organizado e Internet

Introducción

Las tecnologías de la información cambian la forma en que se desenvuelven las sociedades, por lo cual no debería sorprender que además hayan modificado las características de los actos delictuales.

"Se puede afirmar que el correo electrónico y la Web son los medios de comunicación e intercambio de información más utilizados en la actualidad. Millones de personas usan a diario la Internet. Pero también la usan diversos tipos de criminales.

Hemos ingresado a una nueva fase de actividad maliciosa. El crimen cibernético ahora está motivado por la obtención de dinero, lo que ha llevado a la creciente participación de criminales organizados. Ellos aprovecharán todas las oportunidades para explotar las nuevas tecnologías y tomar ventaja de la carencia general de conciencia sobre la seguridad. Además, sus métodos son cada vez más sutiles y sofisticados. De esta forma, la protección proactiva se está convirtiendo en un imperativo, pues es la única manera de ofrecer confianza absoluta a los usuarios.

Como líder en soluciones antivirus y de prevención de intrusos, McAfee® es uno de los principales actores en ayudar a los clientes y a las empresas a comprender mejor las amenazas que enfrentan en línea y en mostrarles las mejores formas de protección contra ellas.

Aunque el incremento del crimen cibernético parece una tendencia preocupante, todos pueden protegerse a sí mismos y a su información personal de manera simple y con una pequeña cuota de sentido común".

Lee Fisher, Estratega de seguridad de McAfee

Los computadores, las redes computacionales y la Internet se han convertido en un elemento integral de la actividad empresarial y social. El valor de la información que está disponible en los computadores y redes atrae a los criminales y esta atracción será cada vez mayor en la medida en que las tecnologías de la información redefinan las actividades económicas. A principios de la era computacional, el *crimen computacional* significaba el robo de un PC o el acceso ilegal a un mainframe para obtener información o tiempo adicional de procesamiento. Actualmente, el crimen computacional contempla una amplia gama de delitos que afectan a las empresas y al valor almacenado en las redes computacionales.

Cada vez con mayor frecuencia, el *dinero* se transa en los computadores o en Internet. Según estimaciones del FBI, en el año 2004 el costo del crimen cibernético ascendió a aproximadamente US\$400 mil millones.

El Informe de Criminología Virtual de McAfee revela cómo una nueva clase de criminales está usando la Internet de maneras nuevas, sistemáticas y profesionales para cometer actos ilegales.

El informe analiza las nuevas áreas de preocupación, que incluyen el uso de nuevas tecnologías como las *botnets* o redes de computadores que se pueden controlar en forma remota.

"Porque es ahí donde está el dinero..."

—Frase atribuida al ladrón de bancos Willie Sutton, cuando le preguntaron sus razones para robar bancos, 1952

El informe sugiere formas en que las empresas y las personas pueden protegerse contra las actividades criminales. En él también se analiza la forma en que se están desarrollando el crimen organizado y el crimen cibernético y considera las futuras amenazas que esta actividad puede plantear a los computadores domésticos, las redes computacionales de los gobiernos y los sistemas computacionales del sector empresarial.

Hace dos años, los investigadores de McAfee observaban el surgimiento de aproximadamente 300 amenazas potencialmente maliciosas al mes, en tanto que ahora, la cifra se elevó astronómicamente a 2.000, lo que se debe en gran medida al creciente número de bots. El crimen cibernético además constituye un fiel reflejo de la actividad criminal fuera de línea, con aproximadamente un 85 por ciento del malware desarrollado exclusivamente para obtener ganancias financieras.

El Informe de Criminología Virtual de McAfee, que fue solicitado por McAfee y elaborado por el Dr. James A. Lewis, Directivo del Center for Strategic and International Studies, revela cómo se están desarrollando el crimen organizado y el crimen cibernético y analiza las futuras amenazas que esta actividad puede plantear a los computadores domésticos, al igual que a la infraestructura gubernamental y a los sistemas computacionales de los sectores financiero y de salud.



Sección uno

Crimen cibernético, versión nueva y mejorada

La Internet comenzó siendo una especie de parque de ciencias en línea, utilizada principalmente para el intercambio de información sobre investigaciones entre una comunidad de usuarios que generalmente se conocían entre sí. Debido a su comercialización y crecimiento masivo, la Internet se transformó en una nueva y dinámica instancia para la actividad económica en la que participan decenas de millones de usuarios anónimos. El anonimato y el alcance de nivel internacional que ofrece la Internet la convierte en un entorno ideal para el crimen, pues implica poco riesgo y representa un alto potencial para obtener dinero.

"La información en sí misma constituye un objetivo. La información es la nueva divisa mundial".

—Ralph Basham, Director del Servicio Secreto de Estados Unidos

El valor de las actividades en Internet y la riqueza en activos almacenados en los computadores son las principales fuentes de atracción. Si bien el comercio electrónico representa sólo una fracción del comercio total, a fines de 2004 éste ascendió a casi US\$70 mil

millones en Estados Unidos, lo que representa un incremento del 24 por ciento con respecto al año 2003. Un tercio de la fuerza laboral de Estados Unidos trabaja en línea (aproximadamente 50 millones de personas); esto reviste gran importancia, dado que más de la mitad de las transacciones de comercio electrónico (e-commerce) se realizan desde el lugar de trabajo y que quienes realizan sus actividades en línea con frecuencia participan en tareas de mayor valor que los colegas que están fuera de línea. Sesenta millones de residentes en Norteamérica (casi la mitad de la población de usuarios de Internet en Canadá y Estados Unidos) poseen cuentas bancarias en línea. La combinación de la banca y el comercio atrae a los criminales más que ninguna otra actividad.

Y dado el alcance internacional de la Internet, la tentación resulta irresistible para estos "empresarios del crimen". El valor de la información y de las transacciones que se realizan en redes computacionales ha aumentado a tal punto que el crimen cibernético se ha convertido en una actividad organizada y profesional. Los criminales cibernéticos aprovechan las vulnerabilidades de las redes y de los computadores para obtener acceso a información valiosa, como información de identificación personal, datos financieros o propiedad intelectual.

ESTUDIO DE CASO: Operación Firewall

En una investigación conocida como *Operation Firewall* (Operación Firewall), en octubre de 2004, las autoridades estadounidenses y canadienses anunciaron el arresto de veintiocho personas de seis países, involucradas en una red de crimen cibernético organizado. Los grupos criminales clandestinos tenían nombres como Shadowcrew, Carderplanet y Darkprofits. Administraban sitios Web donde compraban y vendían información de tarjetas de crédito e identidades falsas, compartían información sobre cómo cometer fraudes y vendían las herramientas necesarias para efectuar dichos delitos. Compraron y vendieron casi 1,7 millones de números de tarjetas de crédito robadas. Según estimaciones de las instituciones financieras afectadas, sus pérdidas ascienden a US\$4,3 millones.

Los criminales ahora utilizan la Internet para realizar extorsión, fraude, lavado de dinero y robo. Las tecnologías de la información les permiten cometer estos delitos de manera más eficiente y con menos riesgo. Las víctimas se pueden encontrar en forma automática. El uso de seudónimos o identidades en línea proporciona un anonimato que resulta atractivo para los criminales. Según estimaciones, quizás sólo el 5 por ciento de los criminales cibernéticos son capturados y procesados. La Internet ofrece a los criminales una forma expedita de mover dinero entre cuentas bancarias y países. La naturaleza de la Internet dificulta que la policía dé seguimiento a las transacciones con el objetivo de reunir evidencia y las leyes nacionales difieren bastante, lo que obstaculiza los procesos judiciales.

Categorías del crimen cibernético

Extorsión: en la variante de Internet de fraude por "protección", las pandillas criminales amenazan a las empresas con la interrupción de sus redes, ataques de denegación de servicio o robo de información valiosa, a menos que depositen un "tributo" u honorarios de *consultoría en seguridad* en una cuenta bancaria en el extranjero.

Daño a la reputación: un hacker o un competidor pueden dañar el sitio Web de una empresa, causando no sólo humillación sino que también pérdidas en ventas. Las amenazas a la reputación a menudo forman parte de un plan de extorsión: la información afectada será divulgada al público a menos que

la víctima pague. En otros casos, el rencor o el deseo de causar daño da lugar a que el ataque se efectúe sin advertencia previa.



Fraude: el anonimato y las oportunidades de falsificación que ofrece la Internet facilitan el fraude. El fraude se presenta en diversas formas. Los fraudes “con honorarios por adelantado” aprovechan la codicia y la ambición al ofrecer, con frecuencia mediante un correo electrónico que afirma provenir de un pariente de un príncipe o dictador, la oportunidad de obtener una buena cantidad de millones.

"Ésta es una industria que mueve miles de millones de dólares, con hackers bien informados que buscan por todas partes las vulnerabilidades y las aprovechan para robar identidades"

—Alan Paller, Director de
SANS Institute

El correo electrónico solicita al destinatario el número de su cuenta bancaria o un pago como parte de un plan de lavado de dinero que producirá un botín millonario. En otra variante, el criminal cibernético ofrece y publicita un tipo determinado de acciones en una sala de chat en línea. Cuando el precio de las acciones sube debido a la información falsa, el criminal cibernético cobra las ganancias. También es posible que el criminal cibernético cree un sitio Web falso que se asemeje al de un vendedor en línea. En ocasiones, un simple error de escritura al ingresar el nombre legítimo lleva al consumidor al sitio del criminal. Cuando el consumidor efectúa un pedido, el criminal no sólo obtiene el dinero de la transacción sino que también la información de la cuenta del consumidor. En algunos casos, los criminales cibernéticos acceden de manera ilícita a las bases de datos y manipulan los registros para obtener ventajas. El fraude en subastas constituye otra variante común: el mejor postor paga al vendedor falso por un artículo de alto valor y a cambio recibe cualquier cosa o simplemente nada.

Fraude electrónico (phishing): actualmente, es la forma más común de fraude y comienza como un correo electrónico que supuestamente proviene de un banco, una empresa de tarjetas de crédito o un vendedor que insta al usuario a visitar un sitio Web y proporcionar información de su cuenta. El fraude electrónico se vuelve más sofisticado, con sitios Web falsos que son imposibles de diferenciar de los que pertenecen a empresas legítimas. El estafador a menudo utiliza técnicas psicológicas, como el anuncio de que *su cuenta ha sido suspendida*, lo que obliga al usuario desprevenido a proporcionar información. Algunos sitios de criminales cibernéticos ofrecen kits de fraude electrónico “hágalo usted mismo” por menos de US\$300.

Interrupción del servicio: un criminal cibernético puede usar un ataque en Internet para interrumpir un servicio esencial. Los ataques de denegación de servicio constituyen un método, pero los gusanos y virus que contienen códigos maliciosos son otro. Un importante fabricante de automóviles fue una de las numerosas empresas que tuvo que desactivar su red de correo electrónico durante unos días debido al virus Love Letter. Algunos virus pueden borrar totalmente la memoria de un computador, incluidos los registros de nómina o las facturas. La amenaza de interrupción de servicio puede ser parte de un plan de extorsión o un área de riesgo potencial para determinadas infraestructuras críticas.

Robo de información: el robo de información, la categoría más dañina del crimen en Internet, puede efectuarse en diversas formas. Los criminales cibernéticos pueden extraer información de identificación personal o información de crédito de la base de datos de una empresa y perjudicar a miles de consumidores. También pueden extraer la información financiera de la empresa. Finalmente, los criminales cibernéticos pueden robar propiedad intelectual valiosa (diseños, proyectos y planes de marketing) de una empresa. Si bien el costo informado del robo de información va en descenso, continúa siendo uno de los riesgos más importantes que puede enfrentar una empresa debido a la Internet.

Lavado de dinero: el crecimiento de los servicios financieros de nivel internacional facilita la ejecución de operaciones bancarias en todo el mundo a través de Internet. Financial Action Task Force, un grupo de agencias encargadas de hacer cumplir las leyes, destaca que “Dentro del sector de banca minorista, los servicios como banca telefónica y banca en Internet permiten a los clientes efectuar transacciones de manera indirecta desde cualquier ubicación con sólo tener acceso telefónico o a Internet”. Aunque el uso de Internet permite a estas agencias dar un mayor seguimiento a las transacciones mediante registros electrónicos, el volumen de transacciones, el anonimato y la carencia de un sistema consistente de mantenimiento de registros resultan características atractivas para criminales y terroristas.

El éxito de los criminales cibernéticos plantea desafíos nuevos y complejos para la aplicación de las leyes. El anonimato y la conectividad global de la Internet permiten a los criminales cibernéticos cometer en línea crímenes tradicionales, como extorsión, narcotráfico o pornografía a una escala mucho mayor. Estos delitos pueden trascender las fronteras nacionales o continentales. No es necesaria la presencia física de los criminales para cometer el delito. Esto reduce el riesgo de captura y de procesamiento judicial y dificulta mucho más la aplicación de las leyes.

Comparaciones entre el crimen de la vida real y el crimen cibernético

Todas las versiones en línea de estos delitos ofrecen a los criminales diversas ventajas:

- 1 Los criminales no necesitan encontrarse físicamente en la escena del crimen para cometer el delito.
- 2 Estos delitos se pueden cometer desde diferentes ubicaciones geográficas; por ejemplo, alguien en Rusia puede cometer un delito en Estados Unidos, Canadá, Francia, Reino Unido, Alemania, Italia, etc.
- 3 A través de los computadores, los delitos se llevan a cabo en forma automática, a alta velocidad y atacan a un gran número de víctimas a la vez, lo que dificulta el seguimiento y el procesamiento judicial.



Asalto a un banco
Asalto bancario en el pasado: las pandillas asaltan bancos importantes/vehículos de seguridad.

Fraude por "protección"
Antiguamente, los dueños de tiendas debían pagar un tributo a las pandillas de crimen organizado para evitar que robaran o incendiaran sus tiendas.

Extorsión en línea
Actualmente, los criminales organizados tratan de obligar a las empresas a pagar un tributo para *proteger* las tiendas en línea contra ataques en línea

Hacking (Intervención de sistemas):
Intervenir los sistemas computacionales de un banco y transferir dinero mediante sistemas de pago electrónico.

Robo de tarjetas de crédito
Los criminales roban estados de tarjetas de crédito y facturas de servicios públicos de los botes de basura para utilizar la identidad de sus víctimas en forma fraudulenta.

Estafas con acciones "en alza"
Los criminales fingen ser corredores y venden acciones por teléfono a un precio inflado artificialmente o acciones de empresas que ni siquiera se cotizan en la bolsa.

Robo de tarjetas de crédito en línea:
Los criminales cibernéticos roban miles de números de tarjeta de crédito en forma simultánea al intervenir las bases de datos de las empresas

Estafa con acciones
Comprar acciones de empresas y utilizar sitios de corretaje de acciones donde se emiten declaraciones falsas que elevan el precio de las mismas con el fin de venderlas en alza.

Llamadas fraudulentas
Criminales que llaman por teléfono a sus víctimas para solicitarles su número de tarjeta de crédito, detalles de seguridad o contraseñas, fingiendo ser empleados del departamento de seguridad de un banco.



Fraude electrónico (Phishing)
Los correos electrónicos de fraude electrónico guían a la víctima al sitio Web de un criminal, el cual se asemeja al sitio Web de un banco, donde el criminal le solicita un número de tarjeta de crédito, números PIN y detalles de seguridad y los almacenan para sus propios fines criminales.

Ladrones
Quienes efectúan llamadas fraudulentas se presentan en el domicilio de la víctima haciéndose pasar por empleados de una empresa legítima. Mientras tanto, su cómplice ingresa por la puerta trasera para robar posesiones valiosas.

Virus
El mismo mecanismo funciona en línea. La *puerta trasera* (back door) de un PC se abre mediante intervención ilegal de un hacker, lo que permite a los virus propagarse fácilmente e infectar una máquina.

El crimen cibernético trasciende las fronteras de los países, lo que se basa en avances tecnológicos que plantean nuevos y complejos desafíos para la identificación de quienes cometen estos delitos y para la recopilación de las evidencias. La evidencia digital es frágil y transitoria y las tecnologías que datan de antes de la era digital y se utilizan para recopilar evidencia con frecuencia son inútiles. La creciente sofisticación de los criminales cibernéticos constituye un serio desafío para la aplicación de las leyes. Muchas fuerzas policíacas aún no poseen la capacidad de actuar en forma efectiva en el ciberespacio. Esto se debe en parte a que no existen leyes adecuadas que penalicen el crimen cibernético. Muchos países aún carecen de una estructura legal adecuada para la disuasión y penalización de delitos cibernéticos o dependen de una legislación poco consistente para ello. Las discrepancias en cuanto a qué constituye un delito, la irregularidad, poca preparación o ausencia de autoridades que permitan a los gobiernos investigar y procesar los casos de crimen cibernético, sumadas a procedimientos de tramitación basados en papeles, en ocasiones han dificultado la cooperación internacional en lo que se refiere al crimen cibernético.

Las sofisticadas herramientas shareware (de uso compartido) para el crimen cibernético que están disponibles en sitios de hackers o “warez” otorgan incluso a los criminales cibernéticos principiantes las armas necesarias para cometer delitos en Internet. Éstas abarcan desde manuales en línea para hackers hasta kits de virus “hágalo usted mismo” y herramientas sofisticadas que requieren cierto nivel de conocimiento para su uso. La creciente conexión entre hackers y criminales profesionales ofrece una alianza de destrezas criminales con conocimientos computacionales

ESTUDIO DE CASO: Operación Cyber Chase

En abril de 2005, una investigación llamada *Operation Cyber Chase* (Operación Cyber Chase) guió a autoridades estadounidenses de la Drug Enforcement Agency (DEA, Agencia Antidrogas), FBI y otros organismos a una farmacia que comercializaba mediante Internet y que vendió fármacos controlados por un valor de US\$20 millones a miles de personas en todo el mundo. La farmacia en línea no exigía recetas, sólo el número de una tarjeta de crédito y la dirección. La red de Internet, cuya sede estaba en la India, suministraba fármacos a 200 sitios Web. El distribuidor extranjero enviaba los fármacos a granel a Filadelfia y a otros sitios en Estados Unidos, donde se volvían a empaquetar y eran enviados a los clientes. Las autoridades confiscaron US\$7 millones depositados en bancos y 7 millones de dosis de fármacos y arrestaron a veintitrés personas en once ciudades de Estados Unidos, la India y Canadá. Los compradores en línea pagaron precios superiores al valor de mercado, lo que llevó a la policía a sospechar que muchos de ellos consumían dichos fármacos en exceso. Las autoridades federales obtuvieron la mayoría de los nombres de los compradores y sus números de tarjetas de crédito y es posible que envíen esta información a los estados en que residen.

que crea un nuevo nivel de riesgo para las empresas. Finalmente, cabe destacar que los criminales cibernéticos han demostrado una gran rapidez para aprovechar la integración económica permitida por la conectividad de nivel internacional y el crecimiento de los servicios financieros internacionales para cometer delitos en otros países o continentes mientras permanecen escondidos cómodamente en otro lugar.

Antes del año 2000, los criminales cibernéticos actuaban solos y eran los responsables de la mayoría de los delitos computacionales. Para estos hackers individuales, la motivación principal era la publicidad y la notoriedad, no la obtención de dinero. Los hackers persiguen la admiración en su mundo virtual. El perfil psicológico de los hackers demuestra la atracción que ejerce el ciberespacio en ellos. Tienden a ser hombres jóvenes y con carencias afectivas, pese a que un número cada vez mayor de mujeres se están uniendo a sus filas. Sus actividades como hackers constituyen una parte importante de su identidad. John Suler, psicólogo especialista en ciberespacio de Rider University, destaca: “¿Qué motiva al hacker? Algunos se sienten cautivados por el desafío y la emoción de aventurarse en territorios prohibidos, en tanto que la motivación de otros es simplemente su carácter rebelde. En casos extremos, un hacker (y, especialmente, el aspirante a hacker) siente la urgencia de demostrar que es mejor y más inteligente que los demás. La bravuconería y la necesidad desesperada de probarse a sí mismo puede ser una de característica más común en el aspirante a hacker que en el hacker experimentado”. Los hackers motivados por estos objetivos sociales o personales seguirán siendo una característica de la Internet. Sin embargo, durante los últimos años, el crimen cibernético ha dejado de ser territorio exclusivo de principiantes y hackers para atraer a criminales profesionales. Los criminales han tomado conciencia de las enormes ganancias financieras que pueden obtener mediante la Internet y con un riesgo relativamente pequeño. Ellos aportan las habilidades, el conocimiento y las conexiones necesarias para una empresa criminal de gran escala y alta rentabilidad que, en combinación con las destrezas computacionales, amplía el espectro y el riesgo que impone el crimen cibernético.

“No hemos observado ninguna jugada importante con respecto a la Internet por parte de los grupos de la mafia tradicional... al menos no del calibre de las acciones de los grupos de hackers de Europa Oriental. No obstante, a medida que aumente la cantidad de dinero transada y que haya más publicidad, probablemente lo harán”.

—David Thomas, Director de la Sección de Intrusión Computacional del FBI

Algunos aspectos del crimen cibernético, como el spyware y el fraude electrónico, han captado la atención pública; sin embargo, las conexiones entre los diversos ataques y la creciente sofisticación del crimen cibernético suscita bastante menos interés. El crimen cibernético ofrece varias ventajas a los criminales. También les permite incursionar en nuevos ámbitos para perpetrar sus delitos. La Internet está teniendo el mismo efecto en el crimen que el que ejerce en otras organizaciones, haciéndolo avanzar hacia estructuras más uniformes y menos jerárquicas y generando una mayor confianza en las confederaciones informales. Las redes criminales en línea a menudo son alianzas informales que trascienden los límites nacionales.

Jerarquía de los criminales cibernéticos

Script Kiddie (hacker recién iniciado): un atacante sin mayor sofisticación tecnológica, normalmente menor de 20 años, que utiliza un archivo macro u otras listas de comandos desarrollados por otra persona para aprovechar las **vulnerabilidades** de los computadores. Con frecuencia, los *script kiddies* no saben cómo funciona el programa que ejecutan.

Cyberpunk: un delincuente en línea que utiliza sus habilidades computacionales para irrumpir en sistemas y redes computacionales. El término proviene de novelas de ciencia ficción como **Neuromante** y **El Jinete en la Onda del Shock**. Por lo general, las ganancias financieras no constituyen su objetivo primordial. Muchos ataques de *cyberpunks* se remiten al **graffiti cibernético**, es decir la modificación bochornosa del sitio Web atacado.

Hackers y crackers: el término hacker, originalmente describía a la persona que disfruta aprendiendo lenguajes de programación y jugando con sistemas computacionales. Muchos de estos hábiles programadores se sienten motivados por un afán liberador. El término se está utilizando en forma cada vez más peyorativa, pues la prensa lo usa para describir a alguien que obtiene acceso no autorizado a un computador o a una red.

La comunidad de hackers denomina a estos individuos **crackers**. Los hackers con frecuencia trabajan solos y están motivados por objetivos sociales (deseo de prestigio en la comunidad de hackers), más que por la obtención de ganancias financieras. Los hackers a menudo utilizan una jerga especializada para identificar sus sitios Web y herramientas. La convención más común es usar una “z” en lugar de una “s” para indicar el plural, como en **warez** (software), **hackz** (técnicas para intervenir sistemas) y **crackz** (software que puede eliminar las restricciones de licencia de productos de software).

Pandillas cibernéticas: grupos de criminales profesionales y hackers que cuentan con las habilidades computacionales suficientes para realizar sus actividades en el ciberespacio. Con bastante frecuencia, los grupos están establecidos en países que tienen leyes benevolentes contra el crimen cibernético, pero también pueden constituir redes flexibles e informales de criminales ubicados en varios países que acuerdan cooperar entre ellos en una operación criminal determinada.

El progreso más interesante es la capacidad de estos grupos criminales más avanzados de planificar y ejecutar estrategias de ataques a largo plazo que son de interés mínimo para los hackers motivados por razones sociales o los script kiddies. Por ejemplo, las diversas versiones del virus Sobig observadas durante el año 2003, parecen haber sido un esfuerzo de sus autores por probar y perfeccionar el virus. El Sobig fue encriptado para demorar los esfuerzos de defensa y, una vez que estaba instalado, descargaba automáticamente spyware desde otro sitio Web, sin que los usuarios se dieran cuenta. Muchos virus o troyanos están orientados a acciones o comunidades específicas. Un troyano activaba un programa capturador de teclado (keylogger) cada vez que determinadas palabras como *mi cuenta* o *número de cuenta* aparecían en un navegador. Además, instalaba un programa de control remoto en el computador infectado. Otro virus tenía como objetivo personas cuyo correo electrónico de la empresa en que trabajaban delataba su pertenencia a una de más de miles de instituciones financieras. Estos virus y troyanos demuestran un nuevo nivel de sofisticación y experiencia en el crimen cibernético.

“Las redes computacionales, las transferencias electrónicas de grandes sumas de dinero, los negocios virtuales tienen lugar en un mundo cibernético que brinda incalculables oportunidades, pero que también ofrece anonimato virtual y posibilidades de robo de tal alcance y magnitud que habrían sido imposibles incluso hace sólo una década”.

—Giuliano Zaccardelli, Delegado de la Real Policía Montada de Canadá (RCMP), 27 de enero de 2005



Sección dos

El ataque de los zombies

Existen dos corrientes básicas en el crimen cibernético: el aprovechamiento de vulnerabilidades en los sistemas operativos y otros programas de software o la *ingeniería social*, donde el criminal engaña a una víctima para que le brinde acceso a su computador o red. Una vez que se identifica la vulnerabilidad en un programa de software, los criminales cibernéticos pueden buscar automáticamente computadores equipados con estos programas vulnerables (a menudo de quienes no han actualizado sus programas), utilizando herramientas especializadas que rastrean la Internet. Según estimaciones, se encontrará y se infectará un computador desprotegido sólo minutos después de que se conecte a Internet.

El caso del hacker contratado

Un empresario contrató a un hacker de dieciséis años de Nueva Jersey para desactivar los sitios Web de sus competidores. El hacker ejecutó un programa que colocaba bots en 2.000 computadores desprotegidos y, luego los utilizaba para un ataque de denegación de servicio distribuida. Los ataques se repitieron durante cinco meses y perjudicaron no solamente a las empresas a las que iban dirigidos, sino que también a sus proveedores de servicio de Internet (ISP) y, siguiendo el efecto dominó, a cientos de otras empresas no relacionadas que utilizaban el mismo ISP. El FBI estimó que los ataques costaron a todas las empresas más de US\$2 millones y se arrestó tanto al hacker como al ejecutivo en marzo de 2005.

“Éste es un ejemplo de una tendencia en crecimiento: los ataques de denegación de servicio se están utilizando para fines de extorsión o para eliminar o perjudicar a la competencia. Es un problema en aumento que tomamos muy en serio, considerando su impacto y potencial destructivo”.

—Frank Harrill, Agente Especial de Supervisión del FBI

Este enfoque hacia el crimen cibernético requiere al principio un alto nivel de habilidades computacionales, pero una vez que éste se desarrolla, las vulnerabilidades y herramientas para aprovecharlas se comparten y comercializan entre todos los miembros de la comunidad criminal cibernética.

La ingeniería social no exige el mismo nivel de destreza computacional. Ella se focaliza más en las defensas, al engañar a los usuarios de computadores para que proporcionen información o permitan sin darse cuenta la instalación del programa criminal para que resida en su computador. Algunos ataques exitosos combinan el aprovechamiento de vulnerabilidades con la ingeniería social; un correo electrónico puede usar una frase de Asunto atractiva que inste al destinatario a abrirlo, acción que ejecutará un programa oculto para aprovechar las vulnerabilidades de software en el computador.

Los criminales cibernéticos son cada vez más sofisticados en cuanto a sus técnicas y tecnologías de ataque y han llegado a usar las herramientas y redes automatizadas de los computadores intervenidos. Los criminales aprovechan la potencia computacional distribuida presente en las redes modernas para lanzar ataques en forma automática, a alta velocidad y contra un gran número de víctimas en forma simultánea. Los criminales pueden instalar programas que se ejecutan sin que los propietarios se den cuenta, con el fin de dañar o robar información desde dicho computador o para obtener una base desde la que lanzarán sus ataques a otro objetivo. Un solo criminal puede enviar un millón de correos electrónicos en minutos, por sólo unos cuantos centavos, y encontrar cientos de computadores protegidos inadecuadamente para controlar o capturar. Los sitios Web de criminales pueden insertar spyware o virus junto con descargas legítimas. Ciertos correos electrónicos spam o fraude electrónico permiten a los criminales acceder a las listas de correo de una empresa o persona que contienen más direcciones.

Los usuarios pueden encontrar sus computadores infectados con malware de diversas maneras, que incluyen abrir archivos adjuntos de correos electrónicos maliciosos, descargar programas o simplemente visitar un sitio Web fraudulento. Los criminales cibernéticos también han comenzado a utilizar los servicios de mensajería instantánea y de noticias mediante correos electrónicos falsos. Las redes Peer-to-peer (P2P, de uso compartido) para compartir archivos han constituido una verdadera ventaja para los criminales cibernéticos. El software P2P concede a otros participantes de la red un acceso ampliado a los computadores e implica la descarga de archivos grandes. Resulta fácil insertar códigos maliciosos en una descarga legítima. Una estrategia que usan estos criminales es suscribirse a la red, identificar los archivos que se descargan con mayor frecuencia y luego colocar una versión corrupta del archivo popular en un computador, sabiendo que los programas P2P en los computadores de otros miembros de la red encontrarán y descargarán automáticamente tanto los programas maliciosos como los legítimos. Por ejemplo, el virus MyDoom tuvo su origen en una red entre pares y luego se propagó al correo electrónico.

Este enfoque hacia el crimen cibernético requiere al principio un alto nivel de habilidades computacionales, pero una vez que éste se desarrolla, las vulnerabilidades y herramientas para aprovecharlas se comparten y comercializan entre todos los miembros de la comunidad criminal cibernética.

La ingeniería social no exige el mismo nivel de destreza computacional. Ella se focaliza más en las defensas, al engañar a los usuarios de computadores para que proporcionen información o permitan sin darse cuenta la instalación del programa criminal para que resida en su computador.

Algunos ataques exitosos combinan el aprovechamiento de vulnerabilidades con la ingeniería social; un correo electrónico puede usar una frase de Asunto atractiva que inste al destinatario a abrirlo, acción que ejecutará un programa oculto para aprovechar las vulnerabilidades de software en el computador.

Los criminales cibernéticos son cada vez más sofisticados en cuanto a sus técnicas y tecnologías de ataque y han llegado a usar las herramientas y redes automatizadas de los computadores intervenidos. Los criminales aprovechan la potencia computacional distribuida presente en las redes modernas para lanzar ataques en forma automática, a alta velocidad y contra un gran número de víctimas en forma simultánea. Los criminales pueden instalar programas que se ejecutan sin que los propietarios se den cuenta, con el fin de dañar o robar información desde dicho computador o para obtener una base desde la que lanzarán sus ataques a otro objetivo. Un solo criminal puede enviar un millón de correos electrónicos en minutos, por sólo unos cuantos centavos, y encontrar cientos de computadores protegidos inadecuadamente para controlar o capturar. Los sitios Web de criminales pueden insertar spyware o virus junto con descargas legítimas. Ciertos correos electrónicos spam o fraude electrónico permiten a los criminales acceder a las listas de correo de una empresa o persona que contienen más direcciones.

Los usuarios pueden encontrar sus computadores infectados con malware de diversas maneras, que incluyen abrir archivos adjuntos de correos electrónicos maliciosos, descargar programas o simplemente visitar un sitio Web fraudulento. Los criminales cibernéticos también han comenzado a utilizar los servicios de mensajería instantánea y de noticias mediante correos electrónicos falsos. Las redes Peer-to-peer (P2P, de uso compartido) para compartir archivos han constituido una verdadera ventaja para los criminales cibernéticos. El software P2P concede a otros participantes de la red un acceso ampliado a los computadores e implica la descarga de archivos grandes. Resulta fácil insertar códigos maliciosos en una descarga legítima. Una estrategia que usan estos criminales es suscribirse a la red, identificar los archivos que se descargan con mayor frecuencia y luego colocar una versión corrupta del archivo popular en un computador, sabiendo que los programas P2P en los computadores de otros miembros de la red encontrarán y descargarán automáticamente tanto los programas maliciosos como los legítimos. Por ejemplo, el virus MyDoom tuvo su origen en una red entre pares y luego se propagó al correo electrónico.

Herramientas de los criminales cibernéticos

Bots: un bot (abreviación de robot) es un computador en el cual un gusano o un virus han instalado programas de ejecución automática que permiten a los criminales cibernéticos obtener acceso y control. Los criminales cibernéticos utilizan virus o bots para buscar computadores vulnerables donde puedan cargar sus propios programas o almacenar datos. Una red de bots es un conjunto de estos computadores infectados que los atacantes a menudo intervienen con semanas o meses de antelación usando gusanos o virus para insertar componentes de backdoor (puerta trasera) que se puedan controlar en forma central y utilizar para lanzar ataques simultáneos. Los emisores de spam, los hackers y otros criminales cibernéticos adquieren o arriendan redes de bots, lo que dificulta a las autoridades el seguimiento de los verdaderos culpables.

Captura de teclado: un programa que registra de manera encubierta las teclas pulsadas por un usuario de computador y almacena los datos para acceder posteriormente o envía en forma secreta la información al autor. La ventaja de un programa capturador de teclado es que el criminal cibernético no necesita engañar al usuario del computador para que suministre información delicada. El capturador de teclado registra lo que un usuario hace durante una transacción legítima y pone esa información a disposición del criminal cibernético.

Inserción: adjuntar de manera encubierta virus o spyware a una descarga benigna o legítima, como un protector de pantalla, un juego, programas gratuitos o una imagen. Cuando un usuario de computador descarga e instala un archivo legítimo, inconscientemente está otorgando permiso para la instalación del programa del criminal.

Denegación de servicio: un ataque diseñado específicamente para evitar el funcionamiento normal de una red o sistema computacional y para evitar que los usuarios autorizados accedan a ellos. Un ataque de ***denegación de servicio distribuida*** utiliza miles de computadores capturados por un gusano o troyano para lanzar decenas de miles de mensajes de correo electrónico a su objetivo en un período muy breve. Los atacantes pueden ejecutar ataques de denegación de servicio al destruir o alterar datos o al usar computadores zombies para bombardear el sistema con correos electrónicos hasta que sus servidores estén tan sobrecargados, que los demás usuarios ya no pueda acceder.

Packet Sniffer: programa de software que monitorea el tráfico de la red. Los atacantes usan packet sniffers para capturar y analizar los datos transmitidos mediante una red. Los sniffers especializados capturan contraseñas que se transmiten mediante un computador en red sin el consentimiento de los usuarios. Normalmente, causan algún suceso inesperado y adverso cuando un computador los ejecuta. Los virus contaminan los programas computacionales legítimos y a menudo son introducidos a través de archivos adjuntos de correo electrónico que por lo general presentan títulos ingeniosos para atraer la curiosidad de los usuarios.

Rootkit: un conjunto de herramientas que usa un intruso después de intervenir un computador. Las herramientas permiten al criminal cibernético mantener el acceso, evitar la detección, incorporar backdoors (puertas traseras) ocultas y recopilar información tanto del computador intervenido como de otros sistemas computacionales de la red. Los rootkits están disponibles para la mayoría de los principales sistemas operativos.

Spyware: software que recopila información sin que los usuarios se den cuenta. El spyware normalmente se incorpora de manera encubierta con otro programa. El usuario no sabe que al instalar uno, está instalando también el otro. Una vez instalado, el spyware monitorea la actividad del usuario en Internet y transmite dicha información secretamente a otra persona. El spyware además puede recopilar y retransmitir información relativa a direcciones de correo electrónico, contraseñas y números de tarjeta de crédito.

Líneas de comandos: programas o listas de comandos breves, normalmente disponibles como programas compartidos en sitios de hackers, que se pueden copiar, insertar remotamente en un computador y usar para atacar e interrumpir las operaciones computacionales.

Ingeniería social: la ingeniería social no se limita al crimen cibernético, sino que además es un elemento importante en el fraude cibernético. La ingeniería social engaña a su receptor para que realice una acción o proporcione información. Las razones ofrecidas parecen legítimas, pero albergan una intención criminal. El fraude electrónico es un ejemplo obvio: un porcentaje determinado de usuarios responderá sin pensarlo dos veces a una solicitud que parece provenir de una institución legítima.

Troyano: un programa malicioso que los usuarios de computadores descargan e instalan sin darse cuenta. Algunos troyanos dan la impresión de ser una aplicación benigna. Muchos de ellos se ocultan en la memoria del computador en forma de archivos con un nombre no descriptivo. Los troyanos contienen comandos que el computador ejecuta automáticamente sin que el usuario se dé cuenta. En ocasiones, pueden actuar como un zombie y enviar spam o participar en un ataque de denegación de servicio distribuida, o bien pueden funcionar como un capturador de teclado u otro programa de monitoreo que recopile datos y los envíe en forma encubierta al atacante. Actualmente, muchos troyanos también intentan desactivar los programas antivirus. Con bastante frecuencia, el término se usa para describir programas maliciosos que no se replican, con lo cual se establece la diferencia entre troyanos y virus.

Gusano: los gusanos son virus en todo el sentido de la palabra, que viajan por las redes, se duplican automáticamente y se envían a sí mismos por correo a otros computadores cuyas direcciones se encuentran en el computador anfitrión. Se propagan al enviar copias de sí mismos a otros computadores mediante correo electrónico o IRC (Internet Relay Chat).

Virus: un programa o parte de un código que se propaga de computador en computador sin el consentimiento de los usuarios. Normalmente, causan algún suceso inesperado y adverso cuando un computador los ejecuta. Los virus contaminan los programas de computador legítimos y a menudo son introducidos a través de archivos adjuntos de correo electrónico que con frecuencia presentan títulos ingeniosos para atraer la curiosidad de los usuarios.

Zombie: programas que se ejecutan en los computadores para otorgar el control a una persona que no es el usuario. Los zombies ejecutan automáticamente comandos enviados por alguien que no es el usuario, sin que este último se dé cuenta. Los zombies se crean al colocar un código ejecutable en la máquina de un usuario (a menudo usando un troyano). Un criminal cibernético puede obtener control sobre el computador y hacer que ejecute automáticamente (y con frecuencia, en forma encubierta) un comando para iniciar un ataque de denegación de servicio, enviar spam o realizar otras actividades.

El objetivo de muchos criminales cibernéticos es infectar miles de computadores y transformarlos en una red de dispositivos que ataquen al unísono luego de recibir una orden, o sea una botnet o red de robots. Una botnet es una red de computadores que ya han sido infectados por gusanos o virus. Ciertos paquetes de malware incluso incorporan su propio software de servidor para facilitar la conexión oculta del bot a la Internet.

Quienes lograron crear botnets también han creado una poderosa herramienta para cometer delitos. Los emisores de spam, los hackers y otros criminales cibernéticos adquieren o arriendan botnets; algunos propietarios arriendan sus redes a otros por montos tan reducidos como US\$200 o US\$300 por hora. Los criminales cibernéticos han reconocido el valor de las botnets, que se están transformando en la principal arma para cometer fraude y extorsión.

Las botnets son fundamentales para los ataques de denegación de servicio distribuida, emisión de spam y fraude electrónico, o sea el robo de información personal financiera. Los emisores de spam y los estafadores usan las redes de bots para comunicarse con miles de víctimas potenciales. CERT de Carnegie Mellon dejó de publicar el número de incidentes de crimen computacional en el año 2004 con la siguiente declaración: “Dado el amplio uso de herramientas de ataque automatizadas, los ataques dirigidos a los sistemas conectados a Internet se han convertido en una constante, por lo cual proporcionar la cifra de incidentes informados no resulta de gran utilidad para evaluar el alcance y la magnitud de los ataques”. Las botnets hacen posible una forma de extorsión en línea. El criminal cibernético utiliza los computadores bajo su control para bombardear los sitios Web de una empresa con miles de correos electrónicos: un ataque de denegación de servicio distribuida. Los criminales cibernéticos entonces envían un correo electrónico amenazando con un nuevo bombardeo si la empresa no les paga.

El fraude en línea es un área de crecimiento del crimen cibernético. La Internet crea ambigüedades en cuanto al proceso de identificación (un bit se asemeja mucho a otro), lo que facilita el fraude. Una declaración de identificación es eliminada de cualquier contexto en el que podamos ponderar su validez. No existen señales externas ni oportunidad de detección como con las credenciales físicas. Las identidades ambiguas son una importante fuente de incertidumbre y riesgo en las redes digitales que abarcan todo el planeta y también constituyen una instancia de oportunidad para el crimen cibernético.

Las estafas en Internet, que engañan a las personas mediante sitios Web falsos y cuentan desgracias para luego solicitar información bancaria y de tarjetas de crédito, amenazan con abrumar al centro de investigación del crimen en Internet del FBI debido al volumen de los ataques. Además, si bien estas estafas eran realizadas principalmente por hackers estadounidenses, los funcionarios del FBI y los expertos computacionales observan cada vez con mayor frecuencia que los culpables ahora son miembros del crimen organizado y grupos terroristas que operan desde el extranjero.

Un importante consorcio contra el fraude electrónico estima que 75 millones de los 150 millones de correos electrónicos de fraude electrónico se envían a diario a través de Internet. Otro informe concluyó que 57 millones de estadounidenses recibieron correos electrónicos de fraude electrónico durante el año 2004. El tres por ciento de estos 57 millones sufrieron pérdidas por un total de US\$1,2 millones. Aun cuando la tasa de respuesta es sólo una décima parte del uno por ciento, la cifra de víctimas continúa siendo 60.000. Los correos electrónicos de fraude electrónico representan más de la mitad de los 15.000 reclamos mensuales que presentan los ciudadanos al centro de investigación del crimen en Internet del FBI. Actualmente, las empresas informan 100.000 incidentes al mes. El FBI ha debido actualizar sus bases de datos para adaptarse a esta afluencia.

El FBI sospecha que la creciente habilidad de los estafadores evidencia la introducción de criminales experimentados en los esquemas de fraude. Creen que los sindicatos del crimen, especialmente en Rusia y en la ex Unión Soviética, han comenzado a tomar conciencia de la cantidad de dinero que pueden obtener con poco o nada de gastos. Según estimaciones, un tercio de todos los delitos de crimen cibernético se atribuye a grupos de dichas regiones. El FBI además cree que los simpatizantes de los terroristas que operan fuera de Norteamérica también han comenzado a aplicar esquemas de fraude electrónico para robar identidades y obtener dinero, luego de que las medidas antiterroristas los privaron de sus fuentes tradicionales de financiamiento.

Es difícil lograr el procesamiento judicial de los extorsionadores en línea. Los expertos consideran que existe un gran número de casos desconocidos que jamás se informaron a la policía. Las empresas de juegos de azar en línea han sido el objetivo de las estafas de extorsión, pero se muestran reticentes a hablar en forma abierta sobre sus experiencias por temor a atraer más atención no deseada. Además, prefieren bajar el perfil del problema por miedo a menoscabar la confianza en la industria.

Un importante vendedor por Internet, preocupado por su reputación, eliminó de su sitio un enlace a una línea telefónica de asistencia contra fraudes.

ESTUDIO DE CASO: Extorsión en línea
La industria de juegos de azar en línea, que genera ingresos por US\$8 mil millones, ha sufrido cientos de ataques durante el último año. Un gerente explicó que en enero de 2004 una invasión de correos electrónicos en blanco sobrecargaron los servidores y entorpecieron el tráfico de los clientes a un nivel insostenible. Poco después, la empresa recibió un correo electrónico escrito en un inglés rudimentario. Éste advertía a la empresa que debía depositar electrónicamente US\$40.000 en diez cuentas diferentes en Europa Oriental si deseaba que sus computadores permanecieran en línea para recibir las apuestas de los clientes.

Sección tres

La perspectiva futura



El avance hacia un mundo en red y una economía de la información sólo aumenta los incentivos para los criminales cibernéticos y el alcance de sus actividades. A medida que las personas y las empresas dependen cada vez más de la Internet para hacer negocios y como herramienta fundamental de comunicación, los criminales cibernéticos cuentan con más oportunidades para obtener dinero de manera ilícita y mayor es el riesgo de ataques maliciosos contra los usuarios.

El surgimiento de amenazas a los dispositivos móviles

Los dispositivos móviles inalámbricos, como teléfonos celulares o asistentes personales digitales (PDA), constituyen un objetivo atractivo para el crimen cibernético. Hasta ahora, la mayoría de los casos se han tratado de bromas: el PDA de una persona famosa es intervenido y su lista de teléfonos y fotos se publican en la Web o los destinatarios reciben un mensaje instantáneo que borra la memoria de sus teléfonos. A medida que se incrementa el número de

dispositivos inalámbricos y de aplicaciones que se ejecutan en ellos, aumentará la tentación de transformar estas bromas en delitos más graves como malversación de fondos, extorsión y robo de identidad.

En un futuro cercano, los teléfonos celulares se asemejarán más a los computadores, pues ofrecerán navegación en la Web y funcionarán como tarjetas de crédito, lo que permitirá a un usuario realizar automáticamente sus pagos mediante el teléfono. Cuando información más valiosa se almacene en el teléfono o el PDA, los criminales cibernéticos se sentirán atraídos hacia este nicho. El spam jugará un papel importante como vehículo que transporta troyanos y virus a los dispositivos móviles, de la misma forma en que opera ahora con los computadores.

Voz sobre IP (VoIP, Voice over Internet Protocol)

VoIP aún no constituye un objetivo importante para el crimen cibernético. No obstante, en la medida en que se expanda, puede ofrecer nuevas oportunidades a los criminales para aprovechar las vulnerabilidades computacionales que presenta la prestación de servicios telefónicos.

Desde el correo electrónico al software malicioso

La cantidad de virus que utilizan el correo electrónico como portador está en descenso. El envío de correos electrónicos continuará siendo un atractivo para los criminales cibernéticos, pero ellos utilizarán con mayor frecuencia otros métodos para insertar códigos maliciosos en un computador.

Aprovechamiento de las redes Wi-Fi

Las redes Wi-Fi están creciendo rápidamente en número y cobertura. La tecnología Wi-Fi resulta naturalmente atractiva para los criminales cibernéticos debido a la dificultad para asegurar las redes inalámbricas contra los intrusos. La *Guerra móvil (War driving)*, donde los hackers o criminales conducen por la ciudad buscando puntos de acceso abiertos, constituye un nuevo tipo de delito que ofrece a los criminales cibernéticos un acceso fácil a redes y a datos valiosos. Kevin Mitnick, un hacker rehabilitado, afirma: “Las nuevas vulnerabilidades inalámbricas son aún peores que los métodos antiguos”.

Spam y spyware

El spam a menudo se percibe como una molesta táctica de marketing que satura las casillas de correo y las conexiones a Internet. Los criminales cibernéticos han utilizado el spam como un portador confiable de bots, troyanos y otros tipos de spyware. En septiembre de 2004, el gobierno de Estados Unidos estimó que cada emisor de spam envió hasta 200 millones de mensajes al día. El spyware, al igual que el spam, es una herramienta cuestionable de Internet que originalmente se utilizó para fines de marketing. Ahora los criminales cibernéticos sofisticados la están adoptando con más frecuencia. Según diversas estimaciones, el porcentaje de computadores infectados supera el 50%.

ESTUDIO DE CASO: Guerra móvil
En diciembre de 2004, dos hombres en un automóvil ubicado en un estacionamiento de una tienda de artículos de ferretería intervinieron continuamente la red computacional nacional de la empresa, alterando sus programas computacionales y accediendo a números de tarjetas de crédito y otra información. Los intrusos obtuvieron acceso a la red nacional de la empresa al ingresar a la cuenta de un usuario mediante la red inalámbrica de una única tienda. Cuando estuvieron dentro del sistema, los intrusos obtuvieron acceso a tiendas de seis estados y al sistema computacional de la oficina central. Los hackers alteraron el software que usaba la empresa para procesar las transacciones con tarjeta de crédito en todo el país e instalaron un programa malicioso que inhabilitó varios computadores de la empresa.

Fraude electrónico y robo de identidad

Las debilidades de la administración de identidades digitales y la capacidad de usar identidades falsas para intervenir redes mundiales financieras y de tarjetas de crédito seguirán siendo atractivas para los criminales cibernéticos. Aunque las mejoras en software y tecnología de autenticación reducirán algunas áreas de riesgo de robo de identidad, la ingeniería social continuará ofreciendo oportunidades para cometer delitos y es muy probable que se descubran nuevas vulnerabilidades tecnológicas como la capacidad de duplicar ilegalmente algunos datos biométricos de identificación.

“Los hackers buscan regularmente vulnerabilidades en nuestra infraestructura de información muchas veces todos los días. Los gusanos y los virus que pueden apoderarse de sistemas vitales se propagan a una velocidad impresionante. Estos incidentes cibernéticos pueden causar perjuicios por millones de dólares y pueden plantear un riesgo físico real cuando intervienen infraestructura de vital importancia”.

—Margaret Bloodworth, Viceministra
de Seguridad Pública y
Respuesta a Emergencias de Canadá,
25 de mayo de 2005

Conclusión

El crimen cibernético llegó para quedarse. A medida que la seguridad computacional mejora, los costos de los daños que éste produce pueden disminuir, pero también evolucionar hacia diferentes formas de ataque. Sin embargo, mientras los computadores participen cada vez más en las actividades cotidianas, los criminales seguirán utilizándolos. Las personas se pueden defender del crimen cibernético al aplicar una dosis razonable de “higiene computacional”, instalar programas antivirus y anti-spyware, mantener los sistemas actualizados y tomar medidas de precaución razonables. El uso ampliado de tecnologías de encriptación y autenticación dificultará las actividades de los criminales.

“Con la Convención del Consejo de Europa, observamos que al aplicar la legislación correcta, es posible procesar efectivamente a los culpables”.

—Paul Kurtz, Director Ejecutivo,
Alianza Industrial para la
Seguridad Cibernética y ex
funcionario de seguridad
cibernética de la Casa Blanca

La industria de tecnologías de la información ha iniciado el largo y difícil proceso de crear computadores y redes más seguros.

El mayor financiamiento para la aplicación de las leyes, que incluye el desarrollo profesional de forenses cibernéticos, mejores medios para la cooperación internacional (como los esfuerzos planteados en la cumbre G-8 para crear puntos nacionales de contacto para combatir el crimen cibernético) y legislaciones nacionales realmente efectivas (definidas en el Tratado sobre Crimen Cibernético del Consejo de Europa) también ayudarán a limitar las oportunidades de los criminales cibernéticos.

El Informe Anual 2004 del Centro de Coordinación CERT de Carnegie Mellon sostiene: “Los próximos veinte años nos traerán mucho más de todo: Más amenazas, más ataques, más recursos en riesgo, más interconexión, más comunicación, más emergencias”.

Es difícil determinar si nos encontramos en un momento de auge del crimen cibernético y si podemos esperar que esta tendencia decrezca en el futuro o todo lo contrario. Lo único que podemos dar por sentado es que mientras las personas usen computadores, serán blanco de los criminales.

GLOSARIO

Bot: código computacional invasor utilizado para ejecutar un ataque de denegación de servicio.

Crimen cibernético: término utilizado para describir todos los delitos que se cometen usando computadores, especialmente mediante la Internet.

Espionaje cibernético corporativo: empresas legítimas que se sirven del crimen cibernético para atacar a sus competidores o robar información comercial delicada.

Denegación de servicio distribuida (DDoS): hackers que vinculan miles de computadores y los activan para bombardear el sitio Web de una empresa con consultas falsas, con lo cual paralizan las operaciones normales antes de emitir una exigencia de soborno.

Extorsión: obtener dinero de un tercero mediante amenaza.

Hacking (Intervención de sistemas): acceso no autorizado a un computador, red o sitio Web de un tercero.

Fraude electrónico: uso de correos electrónicos falsos o sitios Web ficticios para engañar a las personas a fin de que divulguen detalles financieros personales para que los criminales puedan acceder a sus cuentas.

Pump (impulso) y dump (inundación): criminales organizados que compran acciones de bajo valor de una empresa, divulgan información comercial falsa mediante Internet para incrementar el precio de las acciones (impulso) y luego las venden al precio alto (inundación).

Script Kiddies: hackers, normalmente adolescentes fanáticos de la computación, que intervienen un sistema por diversión en lugar de estar motivados por la obtención de ganancias financieras.

Caballo de Troya: un programa malicioso que da la impresión de ser inofensivo, aunque su verdadera intención está oculta.

Zombie: un computador infectado que está bajo el control de otra persona.