Crimeware: el crimen del Siglo XXI

Autor: Lic. Cristian Borghello, Technical & Educational Manager de ESET Latinoamérica

10 de septiembre de 2009

ESET Latinoamérica
Av. Del Libertador 6250 6to piso
C1428ARS Buenos Aires, Argentina
info@eset-la.com www.eset-la.com

Introducción

Durante milenios el ser humano ha encontrado distintas formas de realizar actos vandálicos, fraudes o engaños en contra de sus semejantes. El siglo XXI, con toda su parafernalia tecnológica, tampoco es ajeno a esta situación y, si bien los nombres que reciben estos ataques pueden haber cambiado, siempre se trata de concebir una metodología para obtener una ventaja económica sobre el otro.

Actualmente, la industria del malware se muda irreversiblemente desde el cliente hacia los servidores en Internet dando forma a una nueva economía virtual y paralela que mueve sumas millonarias de dinero. El crimeware es cualquier tipo de malware que ha sido diseñado y desarrollado para perpetrar un crimen del tipo financiero o económico.

"Es inmoral pero el dinero lo hace correcto"

Jeanson James Ancheta, primer condenado en EE.UU. por controlar una Botnet en 2005

http://en.wikipedia.org/wiki/Jeanson_James_Ancheta

Historia

La creación de sistemas informáticos automáticos capaces de realizar múltiples tareas, data de la década del '40, período en que John Louis Von Neumann establece la idea de "programa almacenado" (Arquitectura Von Neumann) **[1]** y "regala" al ser humano una nueva herramienta para llevar a cabo labores impensables hasta ese momento.

A partir de allí, la aparición de nuevas formas de crear programas susceptibles de replicarse no se ha detenido. Como consecuencia, nace en 1983 lo que se considera el primer virus informático, desatando una "carrera armamentística" que continúa hasta nuestros días. El objetivo primigenio de esta competencia era la búsqueda de fama y reconocimiento por parte de sus creadores, pero actualmente ha mutado a fines económicos para obtener dinero de los usuarios.

Posteriormente, y si bien es difícil establecer fechas exactas por las características dinámicas de la tecnología, el entorno de amenazas creció hasta el punto en que hoy miles de archivos dañinos aparecen a cada minuto y muchos de ellos han generado pérdidas multimillonarias a los usuarios y a las organizaciones, con costos asociados a pérdidas o daños directos ocasionados por el programa, pérdida de información sensible vital para el negocio, inversión de tiempo y dinero para eliminar la amenaza, daño a la imagen y muchas otras.

Así, con el nacimiento del nuevo milenio y la evolución de las amenazas en concomitancia con los adelantos técnicos y tecnológicos, el malware se convirtió en una herramienta más para llevar adelante los delitos que la humanidad practica desde siempre.

Definiciones necesarias

Un **delito** es definido como "una conducta, acción u omisión típica (tipificada por la ley), antijurídica (contraria al Derecho), culpable y punible. Supone una conducta infraccional e intencional del derecho penal, es decir, una acción u omisión tipificada y penada por la ley" **[2]**.

Un **crimen por computadora (computer crime)**, más ampliamente conocido como “delito informático”, es una violación de la ley que se realiza en forma deliberada utilizando un equipo informático o contra un equipo informático o una aplicación que se ejecute en él **[3]**. Se refiere a una actividad donde cualquier infraestructura tecnológica actual que emplee equipos informáticos es el origen, la herramienta o el objetivo de un ataque.

Es importante destacar que, en forma general, se llama “crimen” o “delito” a este tipo de acciones que transgreden la ley, pero de acuerdo a las distintas legislaciones (o la no existencia de ellas) en cada país, las mismas podrían no ser castigadas. En muchos casos, la ausencia de leyes que especifiquen claramente cuándo se habla de una acción relacionada con equipos informáticos, tipificada y susceptible de ser considerada objeto de pena por parte de la ley, produce un hueco legal que libra de condena a los culpables de estas actividades.

Si bien el cibercrimen no cambia las reglas actuales al definir la comisión de un delito, el hecho de que el mismo se lleve a cabo en un lugar no físico como el ciberespacio es utilizado como nuevo pretexto para evadir las leyes y, por ende, la correspondiente pena.

Los delitos se llevan a cabo cuando existe una Motivación, Oportunidad e Intención (*Motivation*, *Opportunity*, *Means*, según sus siglas en inglés). Por lo tanto, cualquier situación que propicie alguna de estas tres variables será de potencial éxito para el atacante. También se dice que un crimen comprende un objetivo perseguido, los instrumentos para cometerlo y el material necesario (*targets*, *tools*, *material*, las tres T, según sus siglas en inglés).

Las herramientas tecnológicas actuales potencian estas variables y brindan al cibercriminal factores aptos para ser aprovechados favorablemente, tales como:

- Dependencia de la tecnología: la relación estrecha con la tecnología hace que los usuarios se conviertan en dependientes de ella.
- Anonimato y suplantación de identidad: la relativa facilidad para “desaparecer” en el mundo virtual dificulta el rastreo de los responsables de acciones maliciosas u ilegales. Además, es sencillo para el atacante hacerse pasar por quien no es o encubrir su identidad.
- Facilidad de adaptación: las herramientas pueden ser modificadas fácilmente para adaptarse al medio y a las dificultades encontradas durante su empleo.
- Escalabilidad: un solo programa dañino (o ataque o transacción) puede generar grandes ingresos (más por menos).
- Universalidad de acceso: cualquiera puede convertirse en un delincuente porque las herramientas “están al alcance de todos”, al igual que las víctimas.
- Proliferación de herramientas y códigos: este ítem se encuentra relacionado directamente con el punto anterior, ya que Internet provee las herramientas necesarias para que cualquier persona con escasos conocimientos pueda llevar adelante un delito informático.

- Dificultad para perseguir a los culpables: las jurisdicciones internacionales son un escollo difícil para establecer caminos legales y llegar a un atacante.
- Intangibilidad de las pruebas: teniendo en cuenta que este tipo de delitos se llevan a cabo en el mundo virtual, obtener pruebas válidas y lograr que la corte las comprenda y considere reviste una cierta dificultad.
- Grupos de delincuentes profesionales: miles de grupos integrados por distintos personajes con diversos niveles de conocimiento técnico, legal y financiero (trabajo interdisciplinario) logran una profesionalización del cibercrimen difícil de imaginar.
- Escasa conciencia por parte del usuario: el mismo suele utilizar cualquier tipo de tecnología sin recibir capacitación al respecto.

Para mencionar sólo algunos ejemplos, un tipo de crimen que envuelve a la tecnología informática como medio y como objetivo es el ataque de denegación de servicio, donde un dispositivo o infraestructura ve saturados sus servicios por una sobrecarga intencional del mismo.

Por otro lado, delitos que involucran a la tecnología informática pero persiguen otros fines más profundos son el robo de información, robo de identidad, ciberterrorismo **[4]** o Information Warfare **[5]**, en los que se intenta obtener una ventaja sobre el adversario indiferentemente de los medios utilizados. El alcance del presente trabajo no contempla este tipo de ataques.

Una vez definidos los delitos informáticos, es necesario conocer las herramientas por medio de las cuales se los lleva a cabo actualmente.

Se define como **malware** a cualquier programa informático que pueda representar algún riesgo de daño hacia un equipo o sus sistemas y aplicaciones. Definido de modo amplio, este perjuicio puede ser del tipo físico (muy poco común), relacionado con los tiempos de procesamiento, económico, de fuga o pérdida de información, de interferencia, interrupción o saturación de servicios, daño explícito a la información, a la reputación, etc.

En forma general, se denomina malware a todos los tipos de programas dañinos actuales: virus informático, troyano, gusano, spyware, ransomware, etc.

Si bien la creación de malware es realizada por personas con pocos escrúpulos y en busca de dinero fácil, su primer objetivo es la propagación de estos archivos dañinos y la instalación de los mismos en el sistema del usuario, lo que se logra a través de técnicas de persuasión y engaño conocidas como **Ingeniería Social [6]** y del aprovechamiento de diversas vulnerabilidades en las aplicaciones utilizadas por los usuarios.

Esta necesidad de propagar el malware creado ha dado nacimiento a otras infraestructuras como la diseminación de correos basura (spam) y la utilización de canales como las redes P2P y la

mensajería instantánea para seguir con la cadena de usuarios infectados. La creación y diseminación de malware para afectar sistemas y aprovechar sus ventajas son los primeros pasos para llevar adelante cualquier tipo de ataque o crimen actual.

Por extensión, **crimeware** es cualquier tipo de malware que ha sido diseñado y desarrollado para perpetrar un **crimen del tipo financiero o económico**. El término fue acuñado por el Secretario General del *Anti-Phishing Working Group*, Peter Cassidy, **[7]** para diferenciar este tipo de amenaza de otras clases de software malicioso.

Originalmente, el crimeware abarcaba dos acciones principales:

- Robo de credenciales en línea: cualquier dato que pueda ser utilizado para identificar a un usuario.
- Realización de transacciones comerciales o financieras no autorizadas: llevar a cabo acciones con los datos obtenidos para robar, estafar, defraudar o timar financieramente a la víctima.

Actualmente, el crimeware envuelve además a todos los procedimientos que sirven de objetivo y plataforma para soportar esas acciones delictivas. Como es fácil apreciar, el **fin es puramente económico**. Hoy más que nunca cobra sentido la frase “la información es poder”, y ese poder se logra con dinero (y viceversa).

Millones de sistemas infectados son utilizados para enviar malware actualizado, continuando así su ciclo de propagación. En la actualidad, este mecanismo ha permitido reclutar millones de PC que son controladas por un usuario con fines maliciosos, formando lo que se conoce como **botnet**.

Evolución constante

Si se puede hablar de un “secreto” en la industria millonaria del crimeware, éste es la evolución constante de las nuevas creaciones de archivos dañinos, incorporando renovadas funciones técnicas y de engaño contra el usuario.

En los ‘80 y ‘90, la creación de virus informáticos (programas capaces de realizar una infección, definida como la acción de modificar un archivo existente del sistema) tenía como objetivo, en general, encauzar el desafío personal e intelectual del autor y su búsqueda de conocimiento técnico y de funciones poco conocidas o explotadas del sistema operativo.

Cuando este conocimiento pasó la barrera de lo puramente técnico y de las motivaciones personales, comenzaron a aflorar nuevos objetivos como el económico. Hoy en día, algunos de los

móviles pueden ser psicológicos, de revancha o venganza, políticos, de espionaje y, por supuesto, financieros.

La forma propicia de llevar adelante estos delitos es la suplantación de identidad. Muchas veces, el robo de identidad incluye cualquier actividad relacionada con la obtención de los datos privados de la víctima (nombre de usuario, contraseñas, PIN, números de tarjeta de créditos, etc.), aunque suele ser llevada a cabo a través de un equipo informático. Los delitos referidos a esta forma de robo de identidad son uno de los tipos de crímenes que más han crecido en el último tiempo.

Por supuesto, la evolución de nuevos medios de comunicación en concomitancia con las ventajas de la tecnología no pasó desapercibida para los creadores de malware, que se valieron de su utilización masiva para propagar sus creaciones.

En el siglo XX era común que el malware atacara funcionalidades y programas relacionados o íntimamente ligados al sistema operativo, por lo que los canales de ingreso eran relativamente fáciles de controlar o, al menos, existían en cantidad limitada y se conocían. Actualmente, cualquier aplicación puede ser utilizada como medio para infectar al usuario a partir del aprovechamiento de sus vulnerabilidades como plataforma de ataque. Todas las aplicaciones tienen algún punto sensible o susceptible de ser explotado y, por lo tanto, cualquiera de ellas es un medio potencial que podrá ser utilizado por los creadores de malware.

El crimeware se propaga haciendo uso de dos canales: la Ingeniería Social y la explotación de vulnerabilidades **[11]**. Presenta, además, las siguientes características:

- Actualización constante desde Internet: cuando un malware es modificado (muchas veces con motores automáticos), la versión anterior, ya instalada en el cliente, descarga las nuevas variantes. Como puede verse, este método es el mismo utilizado por cualquier otra aplicación normal instalada por el usuario.
- Explotación de diferentes medios para la instalación: se utilizan *exploits* para cualquier aplicación comúnmente utilizada por el usuario (archivos PDF, MP3, ANI, WMF, etc.)
- Empaquetamiento: esta función comprende la compresión de los archivos ejecutables dañinos para facilitar la propagación (un archivo más pequeño es más fácil de replicar por distintos medios) y evitar la detección por parte de las herramientas antivirus (un archivo más pequeño es más fácil de modificar constantemente).
- Cifrado y ofuscamiento: se cifran u ofuscan las funciones del malware y la información extraída de los sistemas infectados, para evitar el análisis por parte de los especialistas.
- Motores polimórficos: se intenta que cada infección sea distinta a la anterior modificando automáticamente el código del programa dañino. Con esta función se evita que los programas antivirus con capacidades proactivas y de heurística limitada puedan detectarlo.

- Técnicas de defensa: cada programa dañino es capaz de detectar el análisis del sistema o de las aplicaciones involucradas, evitar el debug, el uso de sistemas virtualizados, la eliminación de las aplicaciones infecciosas, etc.
- Instalación silenciosa y ocultamiento: cada programa es diseñado, ya no para mostrarse abiertamente al usuario, sino con el objetivo de permanecer oculto el mayor tiempo posible en el sistema afectado. El tiempo de permanencia del malware en el equipo es directamente proporcional a la cantidad de información (y dinero) obtenida. Para ello, algunas de las herramientas utilizadas son los rootkits, capaces de ocultar funciones al sistema operativo y, consecuentemente, al usuario o a las herramientas de análisis y detección.
- Movimiento del código desde el cliente hacia los servidores: esta característica ha cobrado relevancia a principios de este siglo ya que así como las aplicaciones han comenzado su migración hacia la web, el malware también lo hace progresivamente.

Con respecto al último punto cabe destacar que, del mismo modo que hoy en día es habitual crear y compartir con otras personas un documento de ofimática en Internet, es normal el desarrollo de aplicaciones compartidas por parte de los delincuentes, oportunidad en la cual cada integrante desarrolla alguna función en particular del crimeware. Así como es usual que las actualizaciones de cualquier aplicación se descarguen desde el servidor del fabricante, es normal lo mismo en lo que respecta al malware.

En este nuevo modelo, la plataforma de ataque se encuentra o se está moviendo definitivamente hacia Internet y ya no se centra en el cliente, más que como un objetivo. Como resultado de esta migración, nace el ***Crimeware as a Service*** **(CaaS)**, referido al ofrecimiento a través de la web de servicios de creación, actualización, cifrado y polimorfismo del malware instalado en el cliente. Este sistema brinda todas las características anteriores y con la velocidad necesaria para satisfacer la demanda de cualquier atacante.

El nombre de este tipo de servicio guarda relación directa con **Software como Servicio (SaaS por sus siglas en inglés, *Software as a Service*) [19]**, modelo de distribución de software en el cual la compañía de IT provee el servicio de mantenimiento, operación diaria y soporte del mismo.

El grado de variabilidad y volatilidad de estas nuevas creaciones tiene la ventaja (para sus autores) de que son muy difíciles de obtener para analizarlas, lo que evita su estudio y detección. Muchas de estas amenazas nunca llegan a los analistas o llegan demasiado tarde (*flying under the radar*).

En este contexto, aparece también un nuevo modelo de negocios denominado ***Criminal to Criminal*** **(C2C).** Éste se define como el negocio realizado entre criminales a través de diferentes

canales. De este modo, además, se conforma el mercado negro virtual, en donde se trafican códigos maliciosos e información obtenida de forma fraudulenta a cambio de dinero **[18]**.

Los números y el dinero

Cualquier medio de comunicación informático puede ser utilizado para propagar crimeware y, actualmente, todos ellos confluyen en Internet, donde alcanzan niveles de uso masivos. En consecuencia, la industria del malware se muda irreversiblemente desde el cliente hacia los servidores en Internet, con objetivos económicos, mientras que el crimeware ha dado forma a una nueva economía virtual y paralela que mueve sumas millonarias de dinero no registrado o muy difícil de rastrear.

Por eso, el Convenio sobre cibercriminalidad del Consejo de Europa (en inglés, *Council of Europe Convention on Cybercrime*) **[3]** reconoció en 2001 la urgencia de luchar contra el cibercrimen e instó a todos los países a colaborar adoptando medidas y legislaciones tendientes a combatir en forma adecuada este tipo de crímenes.

Si bien es complicado realizar cálculos que brinden números reales, es necesario dar, de algún modo, una idea acabada de esas sumas de dinero. Estimaciones de Valerie McNiven, consejera en asuntos de cibercrimen del gobierno norteamericano, indican que el crimeware registra más transacciones y dinero que el narcotráfico **[9]**.

Según datos recogidos por el Laboratorio de ESET **[8]**, el 66% del malware actual creado en Latinoamérica corresponde a distintas variantes de troyanos, gran parte de los cuales tiene el objetivo de recolectar información privada del usuario, de una corporación o relacionada con la finanzas de cualquiera de ellos.

El siguiente gráfico muestra estos porcentajes:

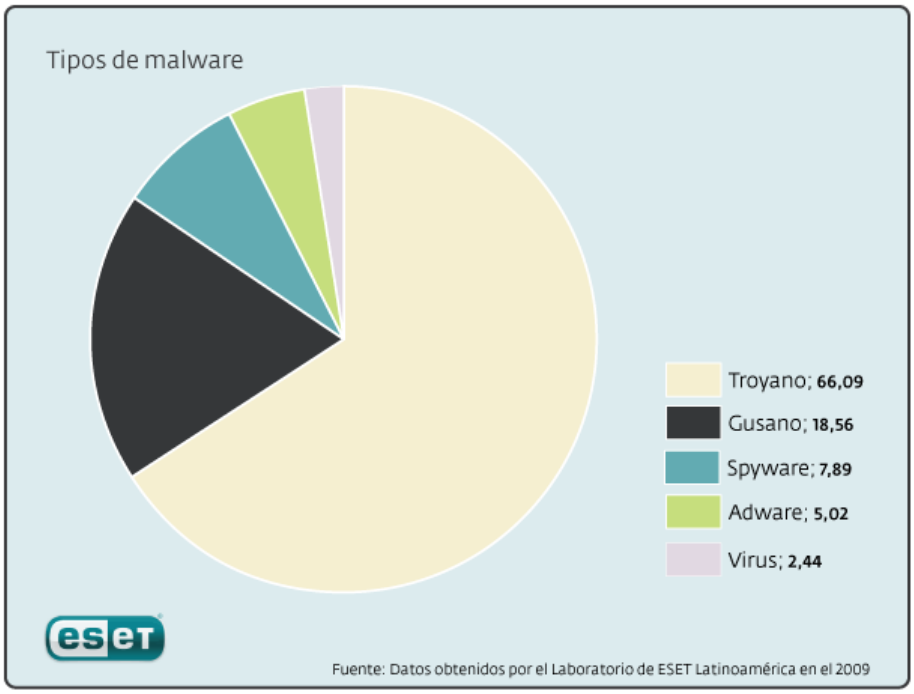

Imagen 1 – Tipos de malware en Latinoamérica

Si bien muchos de estos programas diseñados en países como Brasil (en un alto porcentaje), Argentina, México, Colombia y Perú no alcanzan la evolución de otras versiones desarrolladas en Asia (principalmente China) y Europa del Este (países de la ex Unión Soviética en su mayoría), todos ellos muestran el mismo patrón: son creados para obtener información financiera del usuario o para manipular al mismo para que entregue esa información.

Con respecto a las pérdidas anuales ocasionadas por el crimeware, es difícil establecer un parámetro que sirva de comparación y medición ya que la mayoría de las organizaciones mantienen como confidencial la información sobre si han sufrido este tipo de ataques, debido a que la trascendencia de la misma podría dañar su imagen.

Por ejemplo: **mi2g**, empresa pionera en la gestión de riesgos, estimó este costo en U$S 290 mil millones durante el 2004 **[14]** (incluyendo amenazas como MyDoom, NetSky y SoBig) y otro estudio de *Computer Economics* mencionó que en el mismo año se habían perdido U$S 17,5 mil millones **[15]** (16 veces menos). Sin entrar en detalles, se estima que sólo el gusano detectado por

ESET NOD32 como Conficker, creado en octubre de 2008 y que explota una vulnerabilidad ya parcheada en el servicio RPC de Microsoft Windows, ha causado pérdidas por U$S 9 mil millones en 3,5 millones de equipos infectados **[16]**.

Rentabilidad

Si se habla de un modelo económico que rinde ganancias millonarias a diferentes actores del mercado negro, es fundamental comprender su monto y los motivos por los que resulta tan atractivo realizar negocios a través de estos canales.

Con este objetivo, se analizan dos modelos ampliamente explotados: el del spam y el del phishing. En este estudio se consideran resultados limitados en cuanto al éxito del atacante, lo que implica que, en la realidad, tanto la cantidad de infecciones como las ganancias y la rentabilidad del negocio son mayores a las que se esbozan a continuación con carácter expositivo.

Rentabilidad obtenida por un spammer

Un spammer es la persona responsable de realizar un envío masivo de correos. La rentabilidad del spam se puede calcular en forma sencilla de la siguiente manera:

Gastos

- Compra del troyano escrito a medida: U$S 2.000
- Alquiler de la botnet: U$S 5.000
- Costos totales: U$S 7.000 (cabe destacar que se puede alquilar la botnet sin comprar el troyano, y viceversa)

Ganancias

- Un troyano diseñado para enviar spam, infecta 1.000 sistemas
- Cada sistema infectado envía 100.000 correos
- Un anunciante (advertiser), persona que contrata el servicio, paga U$S 0,002 por cada correo
- Ganancia: 1.000 * 100.000 * 0,002 = U$S 200.000

Rentabilidad

- Ganancia Neta (Ganancia - Costos): U$S 200.000 - U$S 7.000 = U$S 193.000
- Índice de rentabilidad (Ganancia / Costos): U$S 193.000 / U$S 7.000 = 25 veces

Un caso particular de análisis de un malware de este tipo, es el troyano detectado por ESET NOD32 como Waledac **[13]**. Esta amenaza cobró relevancia a fines de 2008 con mensajes navideños y, a partir de ese momento, ha cambiado sus técnicas de Ingeniería Social constantemente para seguir infectado sistemas y esparciendo correo basura. Se considera a Waledac como la evolución de Nuwar (también conocido como Gusano de la Tormenta) que, desde enero de 2007, había creado diferentes formas de engañar a los usuarios.

Actualmente, una botnet alquilada asegura el envío de un millón de mensajes por un costo que varía entre U$S 100 y U$S 150. Según un análisis del Laboratorio de ESET Latinoamérica **[8]**, un único sistema infectado con Waledac[1] puede enviar 150.000 correos diarios. En consecuencia, podríamos aseverar que con sólo infectar 7 equipos el dueño de la botnet puede proporcionar este servicio sin inconvenientes.

Las evaluaciones se dividieron en 4 etapas de una hora cada una, realizadas en diferentes horarios:

- Etapa 1: entre las 18:00 y las 19:00 hs. Se enviaron 6.968 correos
- Etapa 2: entre las 20:30 y las 21:30 hs. Se enviaron 7.148 correos
- Etapa 3: entre las 10:00 y las 11:00 hs. Se enviaron 5.610 correos con utilización del sistema
- Etapa 4: entre las 13:00 y las 14:00 hs. Se enviaron 6.568 correos con utilización del sistema
- Promedio de envío por hora: 6.548 correos
- Promedio por minuto: 109 (casi dos correos por segundo)
- **Promedio diario: 156.000 correos enviados**

Con este promedio diario, si se tiene en cuenta la infección de sólo 500 equipos (un promedio aceptable según SudoSecure **[17]**, que se encarga de seguir esta amenaza día a día desde su aparición) sólo Waledac estaría generando 78 millones de correos basura diarios; en su caso, acerca de productos farmacéuticos.

[1] La versión utilizada de Waledac corresponde al archivo con MD5: 8036ce700043ce6dbe38561ff12d7f4c. Detección: http://www.virustotal.com/es/analisis/4d2cfd73cbceac4b191d8b5f3749c0b6

Rentabilidad obtenida por un phisher

Un phisher es la persona responsable de realizar ataques del tipo phishing. La rentabilidad del phishing puede calcularse de la siguiente manera:

Gastos

- Un kit de phishing puede adquirirse por U$S 10, asumiendo que el delincuente desee comprarlo y no desarrollarlo por sí mismo
- Costo de una base de datos de correo actualizada: U$S 8
- Alquiler de servidor para enviar correo, por día: U$S 120 (incluso se puede anular este costo)
- Se envían 100.000 correos cada 6 hs. (400.000 en el día). Se asume que no se alquila una botnet y que no se utiliza un troyano como Waledac.
- Sitio vulnerado para alojar la página falsa: U$S 10
- Tarjeta de Crédito válida adquirida a personas que las comercializan ilegalmente: U$S 8
- Registro del dominio (con la Tarjeta de Crédito): U$S 10
- Costos totales: U$S 10 + U$S 8 + U$S 120 + U$S 10 + U$S 8 + U$S 10 = U$S 166

Ganancia

- La tasa de éxito de un correo de phishing es de 0,0001. Una persona es engañada cada 10.000 correos enviados (con 400.000 correos diarios son engañados 40 usuarios)
- Promedio de ganancia (dinero u objetos) obtenido por cuenta robada: U$S 1.000
- Ganancia: 40 * U$S 1.000 = U$S 40.000

Rentabilidad

- **Ganancia Neta (Ganancia - Costos):** U$S 40.000 - U$S 166 = U$S 39.834
- **Índice de rentabilidad (Ganancia / Costos):** 39.834 / 166 = 240 veces

Como puede verse en estos cálculos orientativos, con poco esfuerzo el delincuente obtiene una rentabilidad muy grande, casi sin correr riesgos de ningún tipo. A continuación, se muestran las acciones fraudulentas con mayor índice de rentabilidad:

Acción	Rentabilidad
Phishing	400 (en el ejemplo del presente trabajo, 240)
Remates falsos desde cuentas robadas	317
Spam	187 (en el ejemplo del presente trabajo, 25)
Simulación de tareas con Bots	166
Instalación de Adware/Spyware	102
Extorsión online	32
Tráfico de credenciales	31
Inyecciones de código	27
Compra/venta de números de tarjetas de crédito robadas (carding)	9

Tabla 1 - Rentabilidad por tipo de acción fraudulenta. Fuente: Virus Bulletin 2007 [12]

Paradójicamente, el modelo del crimeware es tan eficiente que pasa desapercibido para los delincuentes, dado que el volumen de información robada es tan elevado que resulta imposible de ser procesado. Por ejemplo, en enero de 2007, un estudio publicado por RSA mencionaba que los datos recopilados por un troyano correspondían a información del navegador, direcciones IP, contraseñas y nombres de usuario de alrededor de 70.000 equipos infectados en 160 países durante un mes **[10]**.

Por supuesto que si algunos delincuentes no se percatan de ello, mucho menos lo hace el público.

A medida que los datos obtenidos continúan siendo procesados, los servicios se segmentan y dan lugar a una mayor profesionalización del crimeware: aparecen nuevos actores con funciones más granulares cobrando sus servicios en un mercado cada vez más rentable.

Kit de infección y ataque

Si bien luego de lo expuesto puede parecer complicado armar toda la infraestructura que da soporte a esta red de criminales, la verdad es que el mercado negro actual provee estas herramientas (generalmente conocidas como kit) y las sitúa al alcance de cualquiera que cuente con las motivaciones delictivas necesarias para buscarlas.

A mediados de 2007 se hizo conocido en Rusia uno de los primeros kits que permitía instalar scripts dañinos en sistemas previamente vulnerados. MPack (Webattacker II) costaba entre U$S 700 y U$S 1.000 y se ofrecía con un año de soporte por parte de sus autores. Además, si el comprador deseaba incorporar "nuevas funcionalidades", podía adquirir *exploits* desde U$S 50 a U$S 150 dependiendo de la criticidad del mismo. En cambio, el precio de un *exploit 0-day* varía entre U$S 5.000 y U$S 50.000.

A partir de ese momento no han dejado de aparecer nuevas opciones y a medida que los códigos van cobrando estado público son perfeccionados. Algunos de ellos se muestran a continuación:

Kit o Pack	Costo
76Service	De U$S 1.000 a U$S 2.000
Adrenalin	U$S 3.500
YES Exploit System	U$S 700
Barracuda Full versión	U$S 1.600
Barracuda Lite versión	U$S 1.000
CRUM Cryptor Polymorphic	U$S 100
CRUM Joiner Polymorphic	U$S 50 + U$S 20 por las actualizaciones
Phishing Framework Pack	U$S 400 + U$S 10 por cada sitio que se le solicite

	duplicar
Unique Pack	U$S 600 + U$S 50 por actualización

Tabla 2 - Costo de los diferentes kits existentes

A continuación se muestran dos sitios web donde se anuncia la venta de este tipo de crimeware. El primero de ellos, Unique Pack, es ruso y se vende con un costo de U$S 600[2] mientras que el segundo, un troyano argentino, es comercializado a través de PayPal y con manual de uso en su sitio web:

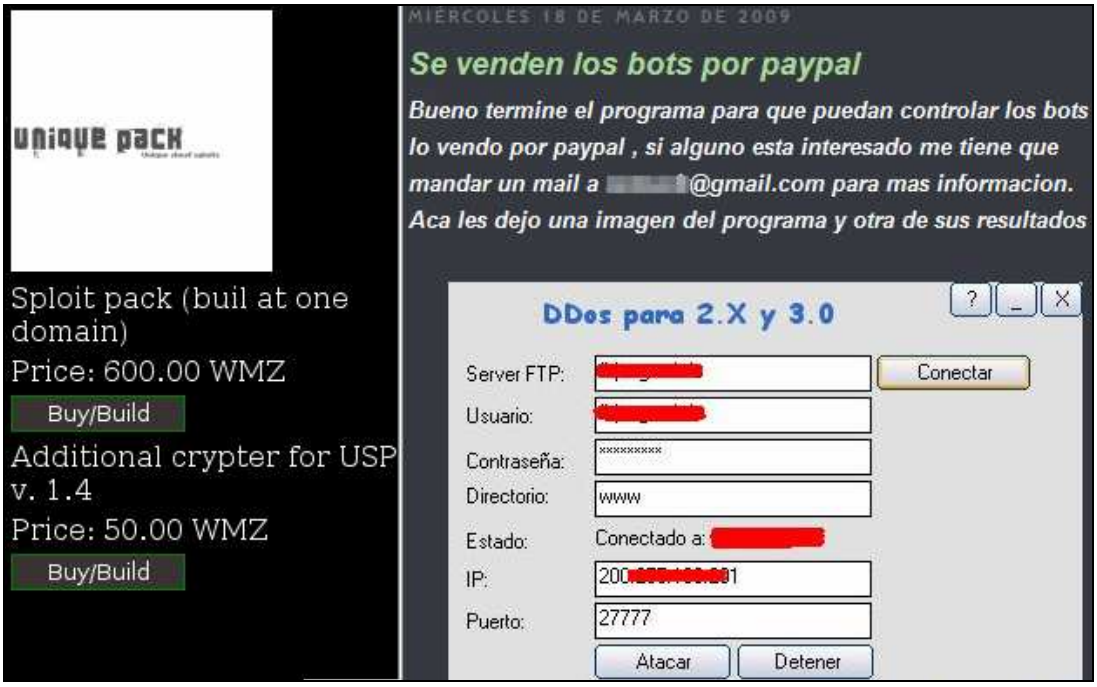

Imagen 2 – Kits a la venta en Internet

[2] WMZ es la moneda virtual de WebMoney equivalente a dólares norteamericanos
http://en.wikipedia.org/wiki/WebMoney

Además, cada uno de estos kits es capaz de explotar distintas vulnerabilidades para posibilitar la infección de una mayor cantidad de sistemas. Algunas de estas vulnerabilidades son:

- MS06-014 (MDAC_RDS). Crítica, solucionada en abril de 2006.
- MS06-055 (VML). Crítica, solucionada en septiembre de 2006.
- MS06-057 (WebViewFolderIcon). Crítica, solucionada en octubre de 2006.
- MS06-067 (DirectAnimation_KeyFrame). Crítica, solucionada en noviembre de 2006.
- MS06-071 (MSXML_setRequestHeader). Crítica, solucionada en noviembre de 2006.
- SuperBuddy LinkSBIcons (CVE-2006-5820)
- OurGame various errors (SA30469). Junio de 2008
- QuickTime RTSP (CVE-2007-0015)
- NCTAudioFile2 SetFormatLikeSample (CVE-2007-0018)
- Buffer overflow en Adobe Flash Player (CVE-2007-0071)
- Yahoo! Webcam Uploader (CVE-2007-3147)
- Yahoo! Webcam Viewer (CVE-2007-3148)
- Adobe Collab overflow (CVE-2007-5659)
- GomPlayer OpenURL (CVE-2007-5779)
- Aurigma Photo Uploader (CVE-2008-0660)
- Creative CacheFolder (CVE-2008-0955)
- WksPictureInterface (CVE-2008-1898)
- Office Snapshot Viewer (CVE-2008-2463)
- Adobe util.printf overflow (CVE-2008-2992)
- Windows Media Encoder (CVE-2008-3008)

Como puede verse, existen herramientas de infección y ataque para casi cualquier software por lo que si el usuario no actualiza todas sus aplicaciones, se constituye en una potencial víctima. Además, como muchos de estos kits son modulares, se pueden incorporar o solicitar nuevos módulos con un costo extra.

Metodología

Internet brinda las herramientas necesarias para almacenar la información obtenida, ya que la misma es enviada utilizando canales como FTP, motores SMTP propios para el envío de correos, scripts dinámicos diseñados para escuchar comandos y almacenar la información en base de datos y canales, redes y protocolos IRC y P2P. En el malware actual más evolucionado, estos canales se encuentran cifrados para evitar el análisis de la información robada.

Al ser un software, el crimeware tiene las mismas características y ventajas de cualquier otro tipo de aplicación, por lo que puede ser distribuido por diferentes mecanismos:

- Ingeniería Social: para convencer y persuadir al usuario de sus ventajas y que éste lo instale. Este mecanismo es utilizado y perfeccionado cada día por los delincuentes.
- Inyección de la aplicación o el script en sitios web: cuanto más conocido y popular sea el sitio, mayor será el éxito de la distribución del malware. Se suelen utilizar mecanismos de Black SEO[3] para hacer crecer artificialmente la popularidad de un sitio o bien inyectar los scripts en sitios populares. ¿Qué pasaría si alguien inyecta un script dañino en Google?
- Aprovechamiento de vulnerabilidades en sitios web: se buscan automáticamente vulnerabilidades de Cross-Site Scripting (XSS) y de Inyección SQL **[20]** (y de cualquier otro tipo) en los sitios para insertar los scripts mencionados anteriormente.
- Aprovechamiento de vulnerabilidades en las aplicaciones y en cualquier sistema operativo: cuanto más popular sea la aplicación, mayor será su utilización y aprovechamiento.
- Inserción de aplicaciones dañinas en software conocido o creación de aplicaciones falsas (*rogue* o *scareware*).

Una vez propagadas e instaladas las aplicaciones, pueden aprovecharse sus beneficios económicos y financieros de la siguiente forma:

- Robo de información personal para venta en “mercados secundarios”(por ejemplo, ataques de phishing)
- Robo de secretos comerciales y propiedad intelectual para ataques dirigidos, fraudes, extorsión, etc.
- Ataques de denegación de servicios distribuidos (DDoS) lanzados desde los usuarios infectados.
- Envío de spam
- Fraudes de clic, simulando tráfico hacia publicidad online.
- Ransomware, aplicaciones orientadas a “secuestrar” el sistema operativo o documentos del usuario para luego cobrar una “recompensa” por su recuperación.
- Cientos de otros fines.

[3] **SEO: Search Engine Optimizer:** Métodos para posicionar adecuadamente un sitio web en los buscadores. Si se utiliza con fines fraudulentos, se habla de Black SEO http://es.wikipedia.org/wiki/Posicionamiento_en_buscadores

A modo de ejemplo, uno de los caminos podría ser el siguiente:

1. El usuario ingresa a un sitio web.
2. El sitio ha sido previamente vulnerado y se ha dejado un script en el mismo (generalmente desarrollado en VisualScript o JavaScript).
3. Valiéndose de una vulnerabilidad en el sistema del usuario, el script descarga un archivo ejecutable (malware) y lo ejecuta en forma transparente sin que el usuario se percate de ello.
4. El malware puede ser un troyano del tipo bot que escucha comandos brindados por un delincuente radicado en cualquier lugar del mundo. Sin depender de las distancias físicas, en ese momento el atacante tiene el control del sistema como si estuviera sentado delante de él.
5. El delincuente puede entonces realizar lo que desee con ese equipo (robo de información, envío de spam, distribución de otros malware, alojamiento web de pornografía o pedofilia, ataques distribuidos, etc.).

Este método no es el único, ya que las técnicas del crimeware se perfeccionan y actualizan cada día haciendo uso de todo medio tecnológico disponible. En la siguiente imagen, se puede apreciar el robo de información a través del envío de la misma utilizando los protocolos HTTP (un script PHP) y SMTP (el envío de un correo):

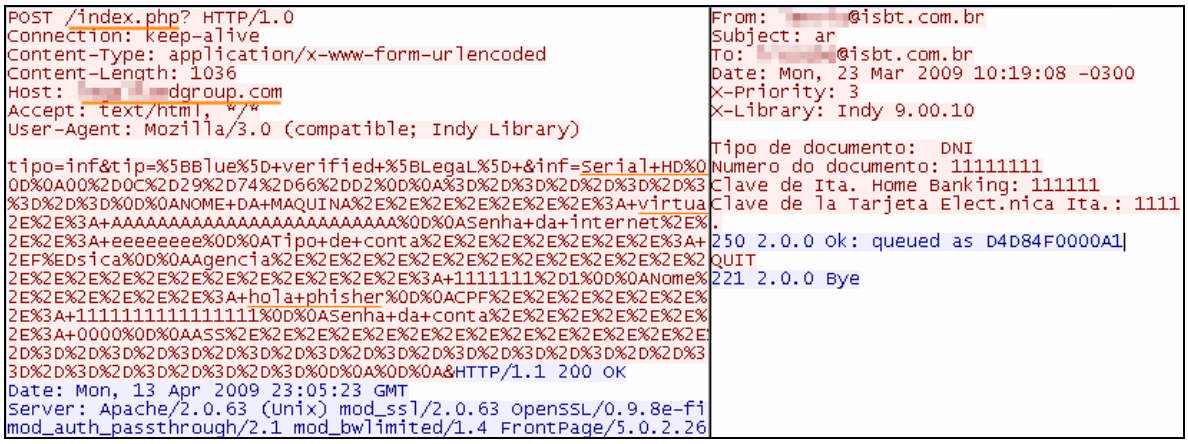

Imagen 3 – Envío de información robada al usuario

Actores

La profesionalización del crimeware requiere que cada servicio sea ofrecido por distintas personas o grupos delictivos, cada uno de los cuales obtiene sus ganancias en base a las tareas realizadas y al volumen de las mismas. De este modo, se originan los roles de los distintos actores que intervienen en este escenario virtual.

En el siguiente gráfico, se pueden ver algunos de ellos y las relaciones que los vinculan:

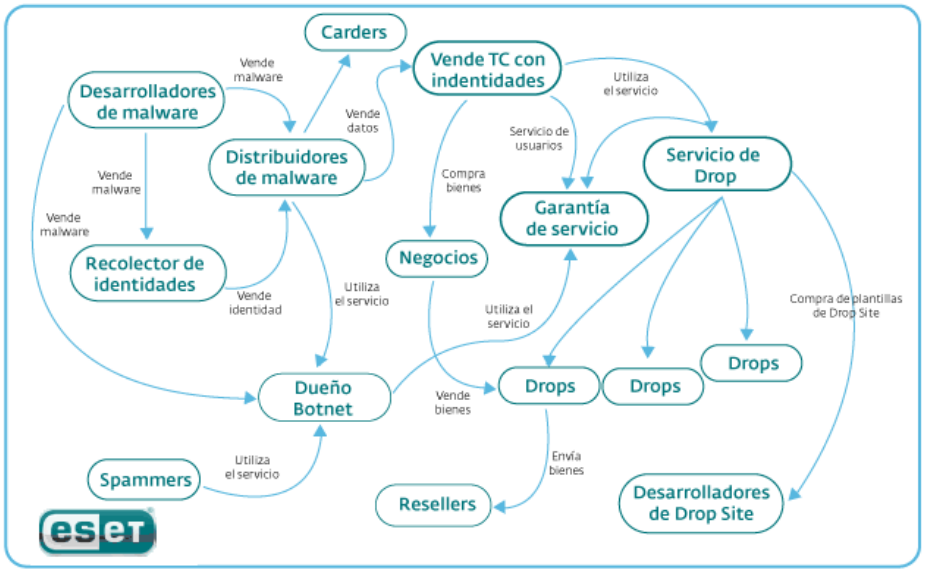

Imagen 4 – Diferentes actores del crimeware y su relación. Fuente: Virus Bulletin 2007 [12]

Si bien el gráfico sólo muestra algunos de ellos, el esquema sirve para comprender el ciclo de vida en el que se encuentran insertos.

Por ejemplo, el desarrollador de malware escribe piezas de código a pedido de sus distribuidores, de un spammer o de alguien que se dedica a recolectar información personal. El distribuidor lo puede vender a un botner o bot herder **[23]** (dueño de la botnet) quien, a su vez, alquila los sistemas que haya infectado. Por otro lado, un carder **[24]** (persona que se dedica a defraudar utilizando números de tarjetas de crédito robadas) puede vender sus servicios a sitios fraudulentos responsables de comercializar productos y servicios a las víctimas.

Este diagrama sirve, además, para demostrar cuán difícil puede ser la desarticulación del funcionamiento de estas redes de delincuentes, ya que para lograrlo es necesario detener el accionar de varios grupos. Por otro lado, su reorganización no suele tomar demasiado tiempo dado que, en caso de ser aprehendida alguna de las partes, no es difícil encontrar un sustituto que haga su trabajo.

Por ejemplo, en septiembre de 2008 se dio de baja a Atrivo/Intercage (AS 27595), uno de los ISP más importantes en el mundo vinculado a botnets como Srizbi, Cutwail, Mega-D y Storm. Dos meses después se desbarató el ISP McColo (AS 2678) en cuyos servidores se alojaban los paneles de control (C&C) de botnet como Rustock, Srizbi, Pushdoy y Mega-D, responsables de generar gran cantidad de spam **[21]**.

En ese momento, la cantidad de correo basura descendió un 50% o más y la noticia cobró relevancia por el éxito alcanzado. Sin embargo, los números del spam no tardaron en recuperar sus índices normales, tal como evidencia el siguiente gráfico:

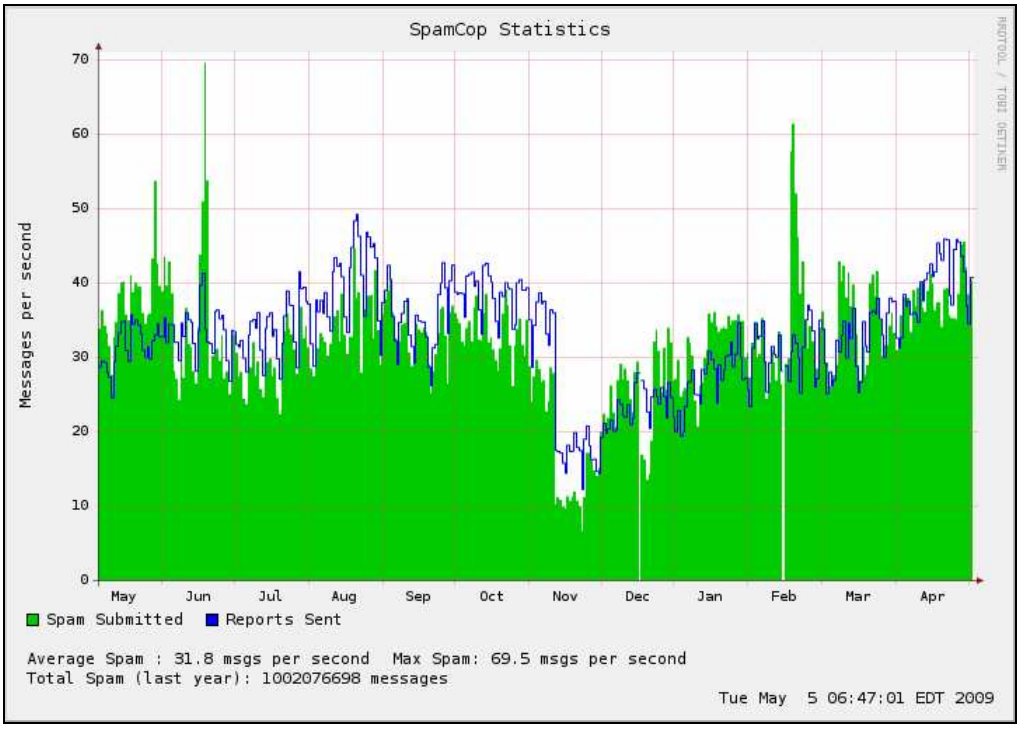

Imagen 5 –Índice de spam mundial en el último año. Fuente SpamCop [22]

Crecimiento de las botnet

La existencia de las botnet se remonta al año 2002/2003 con la aparición del troyano SDBot, uno de los malware de este tipo más populares y antiguos (junto a Agobot, Spybot y GTBot) **[25]**. En ese entonces, las botnet de mayor tamaño no superaban los 100.000 equipos infectados, aunque se debe considerar que puede haber decenas o centenas de redes.

Ya en 2006 se consideraba que podía alcanzarse la suma de 5 millones de botnet, con un tamaño de miles en vez de decenas de miles de equipos **[26]**, pero con un poder de cómputo y conectividad mayor. Esto demuestra el gran interés de los delincuentes por construir su propio imperio de sistemas controlados.

Botnet	Host controlados	Spam diario (miles de millones)
Srizbi	500.000 (antes de su baja en 2008)	60
Bobax	185.000	9
Rustock	150.000 (antes de su baja en 2008)	30
Cutwail	125.000 (antes de su baja en 2008)	16
Storm	85.000 (antes de su baja en 2008)	3
Grum	50.000	2
OneWordSub	40.000	Desconocido
Osdox/Mega-D	35.000 (antes de su baja en 2008)	10

Tabla 3 - Tamaño de botnet [27]

La mayoría de las botnet mencionadas hacen uso de canales de IRC, muchos de ellos sin cifrar, por lo que es sencillo obtener datos de la estructura interna de la red. Sin embargo, redes más evolucionadas como Phatbot, Peacomm, Zhelatin (o Strom) y los recientes Waledac y Conficker utilizan redes estructuradas de control sobre protocolos P2P cifrados, por lo que obtener información de las mismas se ha vuelto complicado.

Legislación internacional

Ha quedado claro que cometer delitos a través del uso de las tecnologías no es demasiado complicado cuando se tiene la motivación necesaria para delinquir. Por lo tanto, es hora de que cada país comience a considerar seriamente las advertencias y consejos vertidos en 2001 en *Council of Europe Convention on Cybercrime* **[3]**.

En el Capítulo III de este convenio se insiste sobre la necesidad de que se realice un trabajo interdisciplinario y acordado entre los miembros de la comunidad internacional, para elaborar acuerdos que permitan un avance en las legislaciones que detenga el aumento del ciberdelito.

En lo que respecta a Latinoamérica, existe legislación vigente que se refiere a la creación de malware y otros tipos de ataques relacionados con el crimeware, como (por ejemplo) el siguiente artículo de la Ley Argentina 26.388 promulgada en 2008, que modifica el Código Penal, estableciendo:

> *Art. 10.- Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:*
>
> *En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.*

O el siguiente artículo de la Ley 19.223/1993 de la República de Chile:

> *Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.*

Pero, indistintamente del país que se tome en consideración, se observan los siguientes inconvenientes:

- Dificultad para obtener evidencia: la misma no es tangible y su inmediatez la hace difícil de seguir y registrar.
- Dificultad para los abogados y jueces: la tecnología actual no goza de buen entendimiento en estas áreas y los “expertos” en la materia suelen tener dificultades para transmitirla.
- Interpretación de la letra de la ley: al no pertenecer a una ciencia exacta, para cada abogado, juez, perito o persona en el mundo, la ley puede tener una interpretación distinta. Si bien es responsabilidad de los legisladores que este impacto se minimice, a veces este objetivo no se logra y da lugar a brechas que son aprovechadas por los delincuentes.

- Volumen de información registrada: es difícil guardar cada hecho histórico a través de logs y registros en cada lugar por el cual circula la información. Países como Argentina ya han tenido problemas similares con leyes que intentan establecer este límite **[28]**.
- Jurisdicción internacional: cada país decide qué guardar, qué entregar en caso de exhortos, qué condenar, etc.
- Secretos de estado o corporativos: en determinadas circunstancias una empresa o un estado podrían decidir que no se entregue información a una autoridad judicial o policial, escudándose en razones comerciales o estratégicas.

Debido a estos y otros argumentos, hasta ahora la legislación internacional y la jurisprudencia no avanzan a un ritmo acelerado, como sí lo hacen la tecnología y los criminales. Incluso, a veces parece insalvable el abismo que separa ambos mundos y tan solo se observan tímidos esfuerzos de algunos estados para impulsar la promulgación de este tipo de leyes. Lamentablemente, y al tratarse de jurisdicciones internacionales, se torna difícil avanzar en algún sentido cuando quede al menos un país desde el cual este tipo de criminales pueda seguir delinquiendo.

Estrategias de prevención y conclusiones

Ante la mirada inquisitiva de distintos profesionales, el paisaje se presenta desolador e incluso los más pesimistas podrían decir que es inútil cualquier esfuerzo por mejorarlo. Sin embargo, así como parece relativamente fácil delinquir, es bastante sencillo prevenir este tipo de hechos.

1. Existen herramientas de protección que el usuario debería considerar, y emplear con responsabilidad: un antivirus con capacidades proactivas que sea capaz de detectar programas dañinos conocidos y desconocidos, un firewall que le permita filtrar conexiones entrantes y salientes, un filtro antispam, un detector de intrusiones (IDS); todas ellas herramientas provistas en ESET Smart Security.
2. La falta de concientización en el uso de las tecnologías es la siguiente barrera importante a levantar, educando sobre temas relacionados y sobre las medidas básicas que cualquier usuario debería contemplar para hacer uso de la tecnología. Debe recordarse que esta última sólo es una herramienta para realizar cualquier tipo de tarea; no casualmente la misma tarea que realizan los delincuentes en contra del usuario.
3. Una vez comprendido eso (no es una tarea sencilla), debe contemplarse la seguridad por capas en donde cada estrato sirve como protección a los demás y, si se vulnera uno de ellos, será tarea de los siguientes proteger el recurso; el dinero en un banco es protegido por guardias de seguridad, alarmas, cámaras, cerraduras, detectores de movimientos,

puertas blindadas, cajas fuertes, etc. Cada elemento mencionado es una barrera que un ladrón deberá sortear en caso de querer hacerse con el botín.

Estas tres estrategias son relevantes a la hora de proteger un sistema. El secreto es comprenderlas y practicarlas.

Cada nuevo avance de la humanidad representa nuevos desafíos. Una vez que se entienda que la tecnología es una herramienta y el escenario actual en el cual se desarrollan las actividades delictivas, será responsabilidad de todos aportar lo necesario para que este siglo no siga siendo reconocido por el volumen de crimeware actual y que, al contrario, éste comience a ser revertido.

Bibliografía y Weblografía

[1] Cronología de los virus informáticos. Lic. Cristian Borghello, CISSP. ESET Latinoamérica. 2006-2008
http://www.eset-la.com/threat-center/1600-cronologia-virus-informaticos

[2] Delito. Wikipedia en español
http://es.wikipedia.org/wiki/Delito

http://buscon.rae.es/draeI/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=delito

[3] Council of Europe Convention on Cybercrime. Año 2001
http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm

[4] Ciberterrorismo. Wikipedia en español
http://es.wikipedia.org/wiki/Ciberterrorismo
http://en.wikipedia.org/wiki/Cyber-terrorism

[5] Information Warfare. Wikipedia en Inglés
http://en.wikipedia.org/wiki/Information_warfare

[6] Ingeniería Social. Lic. Cristian Borghello, CISSP. ESET. 2006-2008
http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social

[7] Anti-Phishing Working Group
http://www.antiphishing.org/

[8] Laboratorio de ESET Latinoamérica
http://blogs.eset-la.com/laboratorio/

[9] “El cibercrimen es más lucrativo que el narcotráfico”. Valerie McNiven, consejera por temas de cibercrimen del gobierno norteamericano. Noviembre de 2005

“El cibecrimen es como el narcotráfico”. Bruce Schneier. Diario El País. Enero 2008

http://labs.news.yahoo.com/s/nm/20051128/wr_nm/cybercrime_dc

http://www.elpais.com/articulo/red/Schneier/cibecrimen/narcotrafico/elpeputeccib/20080117elpcibenr_4/Tes

http://www.schneier.com/blog/archives/2005/11/fraud_and_organ.html

http://www.cybersource.com/news_and_events/view.php?page_id=1425

[10] Defensa contra el enemigo, la lógica detrás de la creciente amenaza del crimeware. Whitepaper RSA. 2007

http://9901_CRIME_WP_0607-lowres_LE

[11] Crimeware: Understanding New Attacks and Defenses. Markus Jakobsson, Zulfikar Ramzan, Addison Wesley Professional. April 2008. ISBN-13: 978-0-321-50195-0

[12] Menace 2 the wires: Advances in the business models of cybercriminals. Guillaume Lovet. Virus Bulletin. September 2007

[13] Waledac: el troyano enamorado

http://www.eset-la.com/threat-center/2042-waledac-troyano-enamorado

[14] Informe de mi2g: $290 of malware damage per Windows PC worldwide in 2004

http://www.mi2g.com/cgi/mi2g/press/240804.php

[15] Informe de Computer Economics: Annual Worldwide Economic Damages from Malware Exceed $13 Billion

http://www.computereconomics.com/article.cfm?id=1225

[16] Conficker's Infection Tracking. Mayo 2009

http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking

[17] Waledac Tracker

http://www.sudosecure.net/waledac/

[18] The new battleground in cybercrime. Yuval Ben-Itzhak. Noviembre 2007

http://news.zdnet.com/2100-1009_22-178194.html

'BOT ROAST II'. Cracking Down on Cyber Crime

http://www.fbi.gov/page2/nov07/botnet112907.html

[19] SaaS Software como servicio. Wikipedia en español

http://es.wikipedia.org/wiki/Software_como_servicio

[20] Cross-Site Scripting (XSS). Wikipedia en español

http://es.wikipedia.org/wiki/Cross_site_scripting

Inyección SQL. Wikipedia en español

http://es.wikipedia.org/wiki/SQL_injection

[21] Baja de Attrivo/Intercage y McColo

http://www.messagelabs.com/download.get?filename=MLIReport_2008.09_Sep_Final.pdf

http://www.icann.org/correspondence/burnette-to-tsastsin-28oct08-en.pdf

http://cidr-report.org/cgi-bin/as-report?as=AS27595&v=4&view=2.0

[22] SpamCop Year Statistics

http://www.spamcop.net/spamgraph.shtml?spamyear

[23] Botner o bot herder. Wikipedia en inglés

http://en.wikipedia.org/wiki/Bot_herder

[24] Credit card fraud. Wikipedia en inglés

http://en.wikipedia.org/wiki/Credit_card_fraud

[25] Botnets, redes organizadas para el crimen. Lic. Cristian Borghello, CISSP. ESET Latinoamérica. 2008

http://www.eset-la.com/threat-center/1573-botnets-redes-organizadas-crimen

[26] Malware: Worms and Botnets. Vitaly Shmatikov. Stanford. April 2009

http://www.cs.utexas.edu/~shmat/courses/cs378_spring09/13botnets.ppt

[27] Spambot data updated

http://www.marshal8e6.com/TRACE/traceitem.asp?article=615

[28] La suspensión de la reglamentación de la Ley sobre Datos de Tráfico en Materia de Telecomunicaciones

http://www.habeasdata.org/comentario-suspension-ley-datos-de-trafico