Costos del negocio delictivo encabezado por el crimeware

Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica
Fecha: lunes 5 de abril de 2010

ESET Latinoamérica, Av. Del Libertador 6250, 6to piso
Buenos Aires, C1428ARS, Argentina
Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629
info@eset-la.com, www.eset-la.com

Índice

Introducción

A lo largo del tiempo los códigos maliciosos han ido ganando terreno en ciertos aspectos ilícitos, a través de un conjunto de programas dañinos cuyos objetivos no solo centran sus esfuerzos en generar problemas en el sistema operativo, sino que también buscan obtener un beneficio económico.

En la actualidad hablar acerca de códigos maliciosos y negocios es habitual, y la relativa trivialidad que antiguamente presentaban estos programas, junto a las motivaciones de sus creadores, han cambiado de manera radical, presentando un panorama completamente diferente, dando lugar a una nueva generación de amenazas más complejas, más agresivas y con intenciones más claras y concretas: **obtener dinero de forma fraudulenta**.

El presente informe se sumerge en la investigación del negocio generado por estas amenazas, dejando en evidencia el impacto que representa esta problemática, las motivaciones que se esconden detrás de su desarrollo y la manera en que estos operan, para alimentar una economía clandestina que crece exponencialmente día a día, modelando un ciclo delictivo que en la actualidad es ampliamente explotado a través de Internet.

Panorama actual

En la actualidad las aplicaciones dañinas están diseñadas para desarrollar un modelo de negocio con intenciones fraudulentas que, desde el punto de vista conceptual, se conocen con el nombre de crimeware **[1]**, y se encuentran orientadas a generar un rédito económico aprovechando la Internet como infraestructura de ataque.

El modelo de negocio que se crea en torno al crimeware tiene su origen en países de Europa del Este, particularmente en la zona europea de Rusia, y es llevado a cabo por personas malintencionadas que utilizan estas aplicaciones en beneficio del desarrollo de una economía clandestina.

Estas actividades fraudulentas y dañinas están siendo imitadas por países de América Latina como Brasil, México, Perú y Argentina, que además, según ThreatSense.Net, el Sistema de Alerta Temprana de ESET, representan los países latinoamericanos con mayores registros de infección por malware.

La demanda en cuanto al desarrollo de crimeware es muy alta y la oferta aún mayor, transformándose en un problema potencial que puede impactar peligrosa y directamente contra los activos de cualquier organización **[2]** o persona de cualquier parte del mundo e incluso de forma masiva, en conflictos entre países como el caso de Rusia contra Estonia.

Evolución y motivaciones

En sus comienzos el desarrollo de programas dañinos se inició con la creación de virus informáticos **[3]** y la motivación que se escondía detrás era esencialmente obtener reconocimiento en el mundo *underground* y entre quienes se dedicaban a ese campo de la informática o, en su minoría, con fines de investigación.

Sin embargo esta situación fue tomando otro rumbo hasta constituir en la actualidad un negocio que se gesta en base a un conjunto de aplicaciones dañinas, denominadas malware, que obedecen a las apetencias económicas de delincuentes informáticos.

En la actualidad la creación y propagación de malware no se enfoca puntualmente en generar problemas en el sistema operativo o incorporar módulos de ataques relativamente sencillos de solucionar, sino que centran sus esfuerzos en aspectos financieros y económicos, completamente diferentes de los perseguidos en aquellos comienzos.

Esta motivación económica provocó un cambio radical en la forma de propagación de las aplicaciones maliciosas, y también en su detección; a tal punto que actualmente el volumen que aparece cada día aumenta rápidamente, siendo necesarias más y mejores técnicas proactivas para su detección.

Como consecuencia las compañías antivirus comenzaron a colaborar entre sí a través del intercambio de muestras para su análisis y estudio de comportamiento. En este sentido y como se muestra en la siguiente imagen, durante los últimos años la cantidad de archivos intercambiados se ha duplicado cada año.

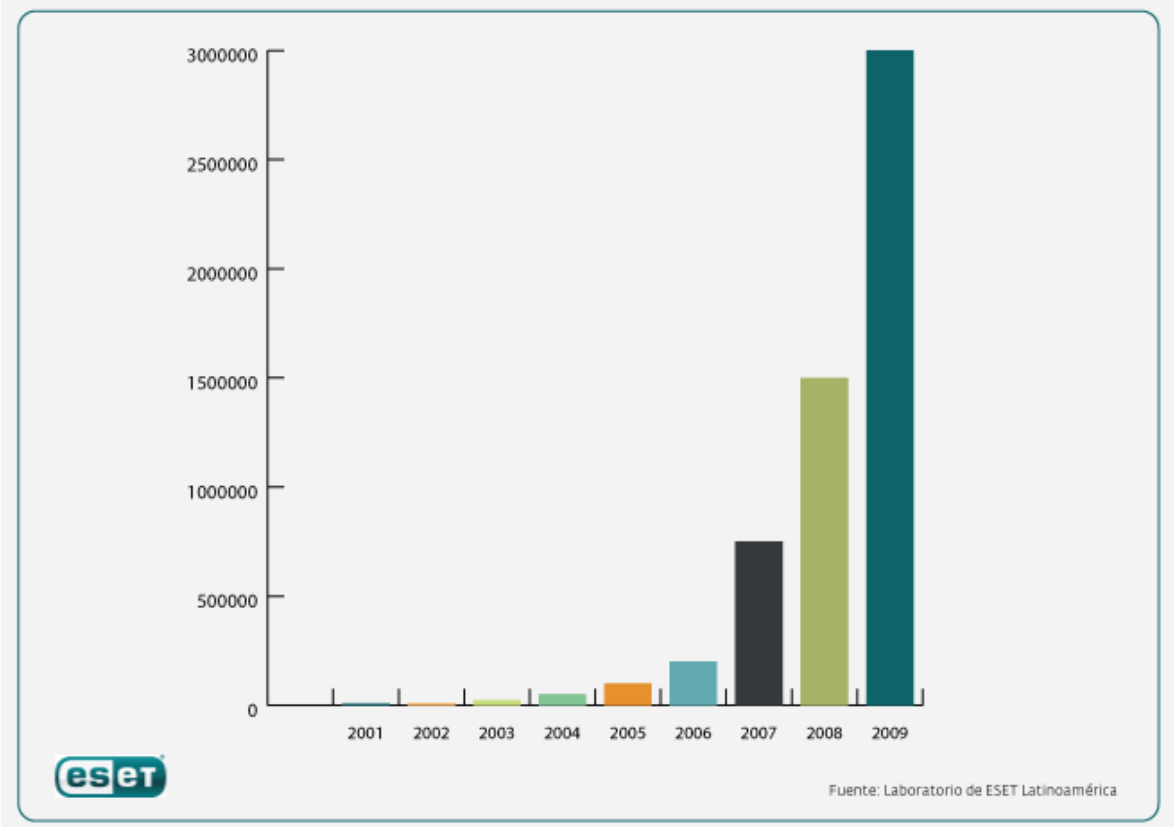

Imagen 1 - Cantidad de muestras compartidas entre compañías antivirus

Para lograr los objetivos económicos antes mencionados ha nacido un mercado y un modelo de negocio, orientado en forma exclusiva a comercializar malware y todo tipo de programas diseñados para engañar e infectar a los usuarios.

Ciclo de comercialización

El modelo de negocio clandestino que utilizan los delincuentes informáticos está compuesto por varias etapas en las cuales se emplean diferentes estrategias, en función del negocio que ofrecen. La siguiente imagen muestra las diferentes etapas del proceso de comercialización de crimeware.

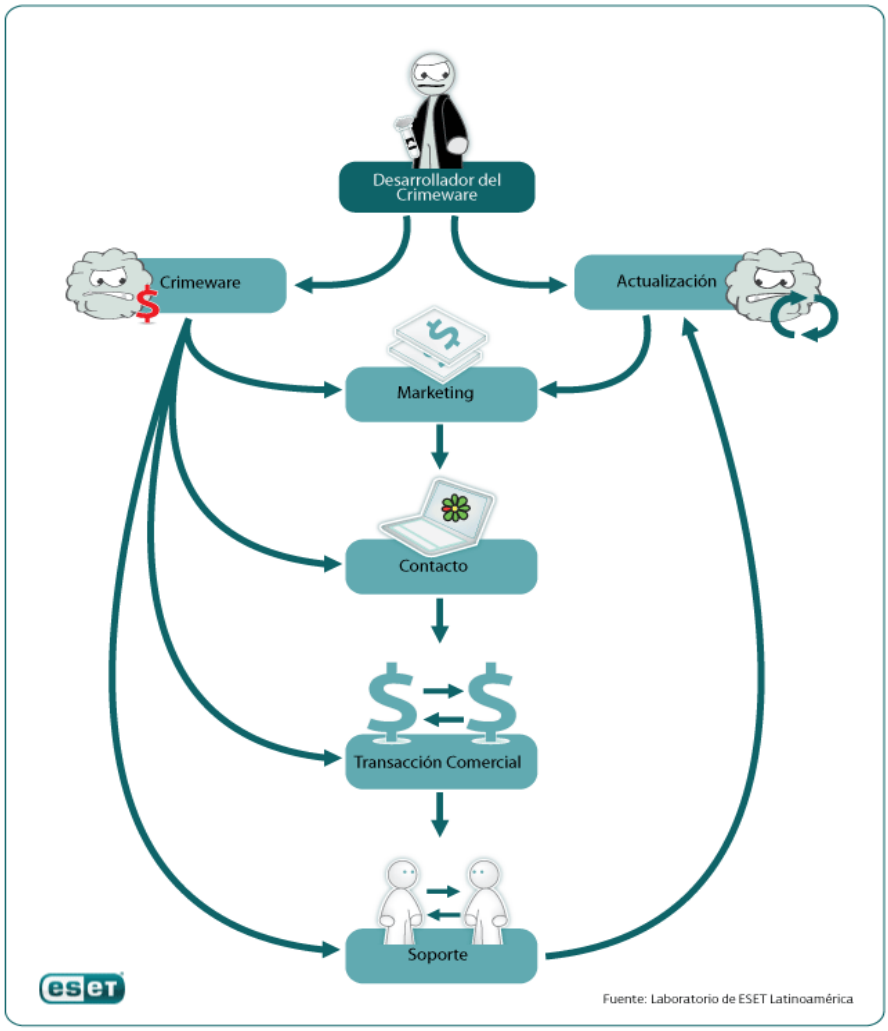

Imagen 2 – Ciclo de comercialización del crimeware

El proceso inicial de publicidad y marketing se realiza a través de foros clandestinos, donde se oferta el crimeware; sin embargo, durante 2009 se han visto casos donde la campaña de marketing se realizaba a través de redes sociales y páginas web.

La segunda etapa corresponde a la del contacto que entabla un potencial comprador con el desarrollador del crimeware quien además ofrece asesoramiento a sus clientes. Esta acción se lleva a cabo generalmente a través de clientes de mensajería instantánea, siendo ICQ[1] uno de los canales más utilizados. Sin embargo, se han observado casos donde el asesoramiento se lleva a cabo por correo electrónico, e incluso en tiempo real vía chat a través de la página web de venta.

El tercer paso del ciclo de comercialización es la realización de la compra. En esta fase el cliente debe realizar el pago por el crimeware a través de servicios que permiten realizar transacciones comerciales y son difíciles de rastrear. Generalmente, el mecanismo se lleva a cabo a través de servicios de transacciones en línea como los ofrecidos por *WebMoney*, *e-Gold* o *Z-PAYMENT*.

Este tipo de servicio es similar al ofrecido por *PayPal*, con la diferencia de que *WebMoney* en principio nació para suplir las necesidades del público ruso y porque no requiere de una cuenta bancaria ni información de tarjetas de crédito (PayPal sí la requiere) para realizar movimientos monetarios, transformándolo en uno de los servicios adoptados para facilitar las actividades generadas por el crimeware.

Una vez ejecutado el proceso de compra, el desarrollador del crimeware ofrece soporte técnico como un servicio que forma parte del acuerdo, siendo el mecanismo mediante el cual se realizan las consultas, las mismas vías empleadas para el contacto inicial.

Finalmente, en caso de lanzarse una nueva versión o actualizaciones del software, el desarrollador del crimeware comienza nuevamente con el ciclo.

[1] ICQ es un cliente de mensajería instantánea y el primero de su tipo en ser ampliamente utilizado en Internet

Programas de afiliados

Otra alternativa dentro del ciclo de comercialización es la adhesión, por parte de los delincuentes informáticos, a un "programa de afiliados". Se trata de un sistema que se encarga de administrar, controlar y proveer el código dañino que es objeto de propagación.

Quienes se adhieren a los programas de afiliados reciben un porcentaje de dinero en concepto de comisión, por la venta y/o instalación exitosa de cada amenaza, que suele rondar entre el 30% y el 40%[2].

El sistema ofrece también la posibilidad de controlar y verificar el estado de cada afiliado vía web a través de un panel de control, en el cual se pueden observar datos estadísticos, la cantidad de ventas exitosas y el porcentaje de dinero acumulado por el afiliado.

Los programas de afiliados proveen una alternativa de gestión a los procesos delictivos y constituyen un modelo aplicable a cualquiera de los recursos que actualmente comercializan.

Un ejemplo concreto donde se aplica esta estrategia de negocio es con la venta de programas del tipo rogue y para envío de spam.

Históricamente, uno de los programas de afiliados con mayor relevancia fue **TrafficConverter** (ya dado de baja), donde los afiliados con mayor nivel de actividad lograron obtener **U$S 330.000** en comisiones **[3]**.

Modularización del crimeware

Si bien el modelo de comercialización se aplica a cualquier tipo de software, generalmente el crimeware se compone de diferentes módulos, donde cada uno de ellos se encuentra diseñado para realizar una tarea específica, y los mismos se venden por separado, permitiendo a su creador obtener mayores ganancias

Esto significa que el delincuente informático puede comprar un crimeware con determinada cantidad de funcionalidades por un costo específico, pero además puede agregar módulos

[2]Estos porcentajes son obtenidos en base a un promedio estimativo, que resulta de las investigaciones realizadas por el Laboratorio de Análisis e Investigación de ESET Latinoamérica en torno a distintos tipos de crimeware analizados.

alternativos, cuyos valores serán establecidos en función de sus objetivos, lo que incrementa el costo final de la aplicación.

Recursos de explotación y sus costos

Luego de varios años de evolución, el desarrollo de malware se profesionalizó y entró en escena una nueva generación de amenazas íntimamente ligadas al ámbito fraudulento.

Los atacantes buscan constantemente idear nuevas estrategias que posibiliten la automatización de los procesos de desarrollo, propagación e infección, a través de recursos y aplicaciones que al mismo tiempo permitan asegurar, controlar y administrar las computadoras infectadas de forma centralizada y remota.

Estos servicios también se ofrecen y comercializan a través de Internet, y se constituyen mediante componentes que reciben el nombre de *Crimeware-as-a-Service* **[4]**, es decir, comercialización de servicios creados a medida. Algunos ejemplos de estos servicios son el cifrado de archivos maliciosos, procesos de polimorfismo, alojamiento de sitios web, almacenamiento de bases de datos, dominios con datos robados, entre otros.

A continuación se exponen algunos de estos recursos y alternativas empleados por los delincuentes informáticos para gestionar sus negocios fraudulentos.

Servidores Bulletproof

Quienes realizan negocios clandestinos en Internet necesitan contratar una serie de servicios de infraestructura que garanticen un nivel de seguridad para sus actividades, a efectos de entorpecer en cierta forma los procesos de investigación realizados por los profesionales de seguridad. Por eso, uno de los servicios más contratados son los servidores conocidos como *Bulletproof*, o a "prueba de balas" según su traducción al español.

Los *Bulletproof* son servidores dedicados y extremadamente robustos y con alta tolerancia a fallas (rotura, mal funcionamiento, etc.), cuyos proveedores aseguran que no podrán ser vulnerados o dados de baja (lo cual no necesariamente debe ser cierto); características por las cuales son utilizados por los delincuentes informáticos para alojar todo tipo de material malicioso.

Costos

Respecto al costo, este depende directamente de las características del hardware, pero también pueden ser contratados según el tipo de contenido que se alojará allí. Algunos costos de servidores son los siguientes:

- Un servidor "a prueba de balas" destinado al alojamiento de malware, código *exploit*, envío de spam, botnets **[5]** o material destinado a cometer fraudes, posee un valor cuyo rango ronda entre los **U$S 80 y U$S 200 mensuales.**
- Cuando la contratación del servidor *bulletproof* depende de las características físicas, su costo mensual puede ser entre **U$S 100 y U$S 400 mensuales.**

La siguiente imagen muestra un ejemplo de cómo se ofrecen los servidores *bulletproof* y su valor según el hardware utilizado.

Imagen 3 – Venta de servidores *bulletproof*

Alquiler de botnets

Las botnets se forman por medio de códigos maliciosos diseñados para atacar los sistemas y convertirlos en computadoras infectadas, a lasque se conoce bajo el término de zombi.

Actualmente las botnets constituyen un componente esencial para los procesos delictivos y fraudulentos, porque permiten a los delincuentes realizar ataques en forma masiva y en gran escala, manteniendo el control de las computadoras infectadas.

Esto permite generar un modelo de negocio centrado en el alquiler de botnets, donde el rédito económico del botmaster[3] puede calcularse en función de las actividades que los atacantes realizan a través de las computadoras infectadas, como por ejemplo propagación de phishing y códigos maliciosos, envío de spam, realizar ataques del tipo DDoS (*Distributed Denial of Services*; en español, Denegación de Servicio Distribuida), obtención de información confidencial, entre muchos otros.

Costos

En la siguiente imagen se aprecia la oferta de venta y alquiler, a través de un foro ruso, del conocido crimeware llamado *Eleonore Exploit Pack v1.3* diseñado para el control de botnets. En este caso, el valor para la compra es de **U$S 1.000**, mientras que el alquiler por día de una red zombi administrada a través de esta aplicación es de **U$S 40**.

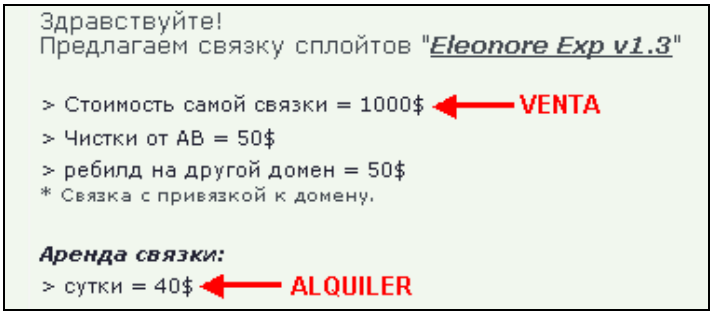

Imagen 4 – Venta de crimeware y alquiler de botnets

Esta aplicación podría permitir generar y controlar una botnet de aproximadamente 10.000 a 20.000 zombis, para luego alquilarla de forma segmentada (es común ver botnets de mucho mayor tamaño).

[3] Persona que administra y controla una botnet.

Cabe destacar que el costo suele ser por el alquiler de un segmento de la botnet, que generalmente se compone de aproximadamente el 10% de la cantidad total de zombis que componen la red.

Si se toma como ejemplo el valor expuesto en la figura anterior respecto al alquiler de la botnet por un segmento del 10% de equipos infectados, y sin considerar la contratación de servidores *bulletproof* ni los objetivos para la cual es alquilada, se desprende que la ganancia teórica que podría obtener un botmaster por ese segmento es de:

- **U$S 40 por día**
- **U$S 1.200 por mes** (U$S 40 durante 30 días)
- **U$S 14.600 por año** (U$S 40 durante 365 días)

Quizás pueda parecer que estos valores representan un número importante; sin embargo, es una cifra mínima que un botmaster recupera en tan solo un mes, considerando que su inversión fue de **U$S 1.000** (costo por la compra de la aplicación *Eleonore Exploit Pack v1.3).*

También puede considerarse un ambiente, hipotético pero más cercano a la realidad, en el cual el botmaster ocupa el 100% de la botnet y contrata un servidor *bulletproof* (el más costoso según la figura 3 es de **U$S 385** por mes). En este caso, el margen de ganancia teórico del botmaster será de:

- **U$S 14.215 por mes** (14.600 - 385)
- **U$S 170.580 al año** (14.215 en 12 meses)

Como se puede apreciar, a través de una mínima inversión, un botmaster (que no necesita tener conocimientos informáticos), genera un negocio mediante el cual posee la probabilidad de ganar más de U$S 10.000 mensuales, sin moverse de su casa y con un riesgo prácticamente nulo.

Ransomware

Otro tipo de amenaza, con menos protagonismo que las botnets, pero con una importante tasa de actividad, e incluso en muchos casos propagados a través de botnets, son los códigos maliciosos del tipo ransomware.

Este tipo de crimeware se encuentra diseñado para “secuestrar” recursos a nivel lógico en un sistema utilizando algún algoritmo de cifrado, para luego solicitar un “rescate” de índole económico. Los recursos secuestrados pueden estar constituidos por el cifrado de archivos o carpetas, o el bloqueo del acceso al sistema operativo.

En las primeras generaciones de ransomware, la estrategia de infección consistía en cifrar los archivos[4], generalmente ofimática del tipo PDF, ODT, DOC, XLS, etc., empleados por el usuario de la computadora atacada, y de esta manera los delincuentes accedían a un beneficio económico a través de acciones extorsivas, solicitando a la víctima determinado monto de dinero a cambio de la clave que permita recuperar los recursos comprometidos.

Sin embargo, y si bien en la actualidad el objetivo y esencia es el mismo, los delincuentes suelen recurrir a una modalidad distinta donde el recurso tecnológico empleado es la mensajería SMS a través de dispositivos celulares. Por este motivo, el ransomware que emplea esta metodología de infección es denominado SMS Ransomware **[6]**.

La siguiente captura es un ejemplo de ransomware diseñado para bloquear el acceso al sistema operativo y solicitar el envío de mensajes SMS a un determinado número para poder obtener la clave de desbloqueo.

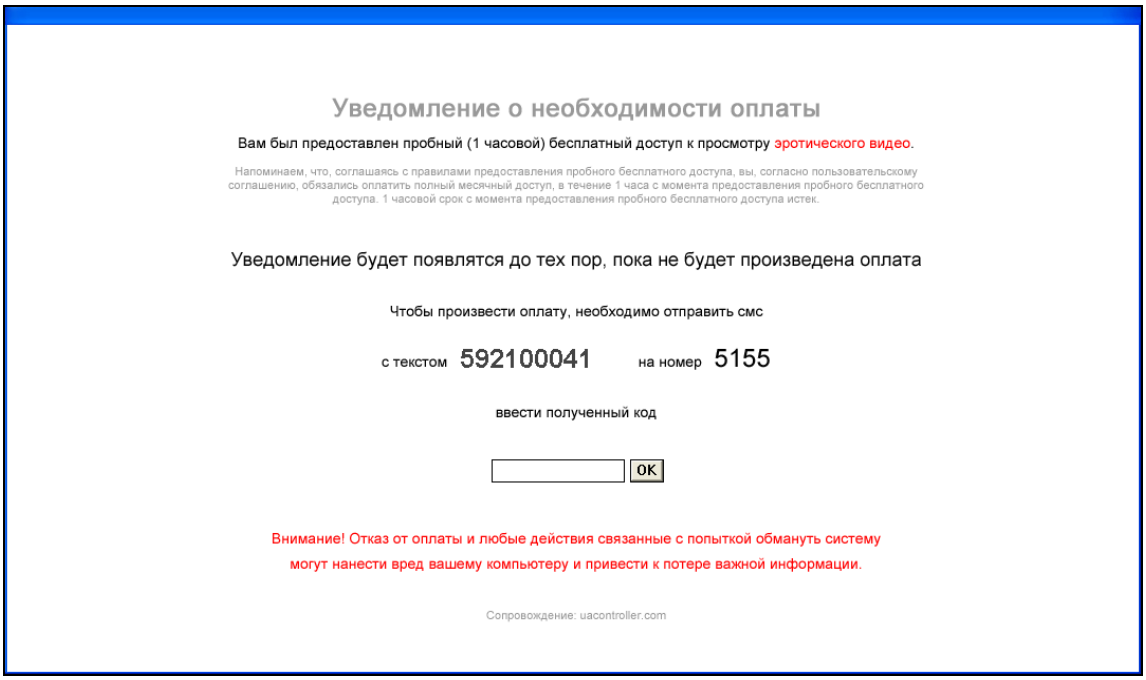

Imagen 5 – SMS Ransomware en Windows

[4] Desde le punto de vista técnico, las primeras variantes de ransomware empleaban algún mecanismo de cifrado; esto mantiene a este tipo de malware dentro de la rama que estudia la criptografía aplicada a códigos maliciosos, denominada criptovirología.

Parte del texto se refiere al envío de un mensaje SMS con el texto *592100041* al número *5155*. El siguiente paso que realizará el atacante cuando reciba el mensaje SMS, es enviar a la víctima la clave de desbloqueo, o descifrado[5]. Cabe destacar que en algunos casos el atacante puede hacer caso omiso y no enviar la información de desbloqueo.

Costos

El negocio que representa el crimeware del tipo ransomware posee dos vectores; por un lado, el desarrollo y comercialización del malware "a medida" que luego será utilizado por un atacante; y por el otro, el beneficio económico que obtiene el atacante por cada mensaje enviado por las victimas.

En el primero de los casos, la venta de ransomware a medida suele rondar entre los **U$S 40** y **U$S 100** sin incluir el código fuente, variante en la cual el importe asciende a aproximadamente **U$S 1.000**.

La siguiente imagen muestra un ejemplo de comercialización de ransomware a través de un foro ruso. En el mismo se establece el valor del malware en **U$S 100**.

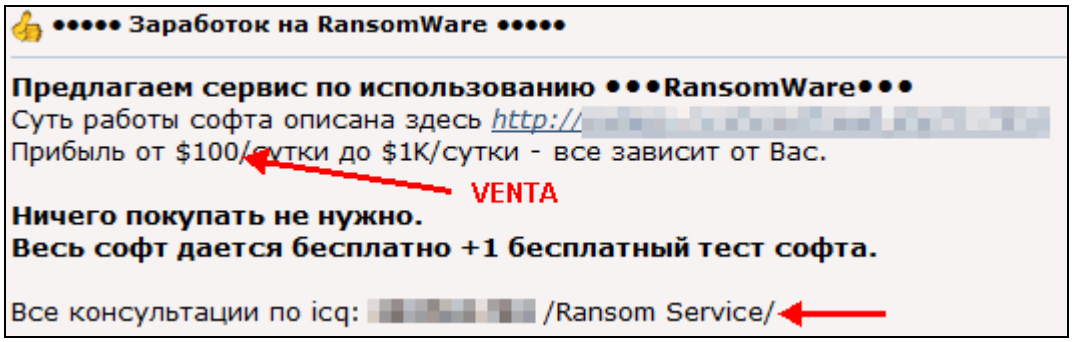

Imagen 6 – Venta de ransomware

Por otro lado, el atacante obtiene el rédito económico a través de cada mensaje SMS enviado por una víctima, donde por cada uno de ellos el costo es de aproximadamente **U$S 1** a **U$S 8**, dependiendo del país afectado

[5] Cuando el usuario procede al desbloqueo del sistema a través de la clave enviada por el atacante, automáticamente se eliminan los rastros del ransomware.

La propagación de ransomware suele ser por correos electrónicos o páginas web falsas (aunque podría emplearse cualquier medio de comunicación), y a través de campañas masivas de propagación, con lo cual el margen de ganancia que obtienen los atacantes se incrementa considerablemente si se considera la probabilidad de que un porcentaje de usuarios caiga en la trampa.

SMS Ransomware en Mac OS ¿Solo una prueba de concepto?

El gran caudal de crimeware que se encuentra actualmente activo, es desarrollado para plataformas Microsoft Windows. Sin embargo, los atacantes buscan constantemente idear nuevas formas de obtener beneficios económicos a través de aquellas plataformas que cuentan con un incremento en cuanto a su utilización; como por ejemplo, las plataformas Mac OS.

Teniendo en cuenta esta situación, recientemente se conoció un ransomware desarrollado para plataformas Mac OS. Se trata en realidad de una prueba de concepto (PoC), pero que a pesar de ello deja en evidencia que los delincuentes se encuentran en pleno proceso de desarrollo de alternativas fraudulentas orientadas a otras plataformas **[7]**.

Rogue

Otro de los negocios fraudulentamente lucrativos lo constituye el rogue **[8]**. Este tipo de código malicioso se caracteriza fundamentalmente por emitir alertas sobre supuestas infecciones, buscando que la víctima adquiera un programa de seguridad falso y que en realidad es un malware.

Imagen 7 – Falsa alerta de infección generada por un rogue

En los últimos años la propagación de programas rogue ha aumentado y actualmente se propagan empleando diferentes recursos y técnicas. Entre ellas se destacan:

- **Troyano downloader**. En esta metodología, el rogue es descargado en la computadora víctima a través de un troyano del tipo downloader. Este troyano opera a modo de instalador y es generalmente mediante éste, que se lleva a cabo la primera etapa de infección.

- **Bloqueo del sistema operativo**. Algunas variantes de la familia de malware detectada por ESET NOD32 con el nombre de *Win32/LockScreen*, emplean el concepto de ransomware para presionar a la víctima a fin de que compre un supuesto programa de seguridad, que en realidad es un rogue.

  En este caso, la estrategia consiste en bloquear el acceso al sistema operativo invocando falsas razones de seguridad y solicitando, a través de una alerta, la compra de un supuesto antispyware para recibir la clave que permitirá desbloquear el sistema. La siguiente imagen constituye un ejemplo de esta técnica:

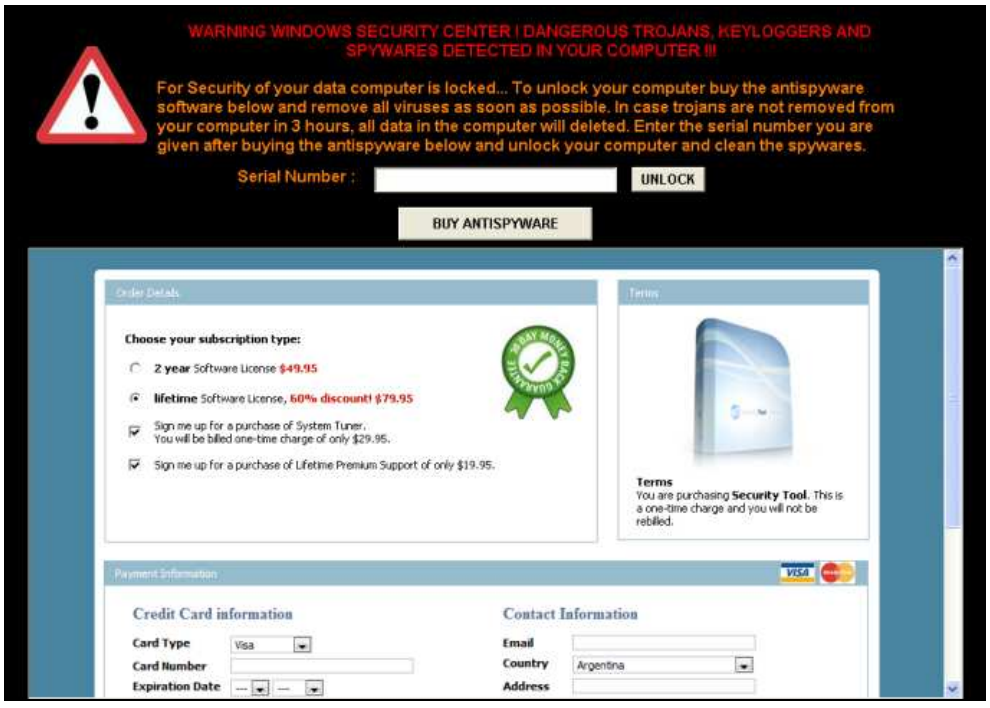

Imagen 8 – Ransomware solicitando la compra de rogue

- **Drive-by-Download**. En este caso, el rogue es transferido a la computadora víctima cuando el usuario accede a una página web que ha sido maliciosamente manipulada con antelación, en la cual se inyectó código que redirige a la descarga automática del rogue.

- **BlackHat SEO**. Esta técnica **[9]** consiste en obtener un nivel de posicionamiento web óptimo en los buscadores, utilizando métodos abusivos. De esta manera, los atacantes logran ubicar en los primeros puestos de las posiciones las páginas web que propagan el rogue.

  Esta técnica y la Ingeniería Social **[10]**, constituyen piezas fundamentales dentro del ciclo de propagación de rogue, y cuando sucede algún hecho de importancia a nivel mundial, los atacantes lanzan una campaña de BlackHat SEO para atraer víctimas **[11]**.

  La siguiente imagen muestra la búsqueda de información sobre el terremoto sucedido en febrero de 2010 en Chile, donde a través BlackHat SEO se posicionó una página web maliciosa que hace referencia al tema buscado, pero que propaga rogue.

Imagen 9 – BlackHat SEO orientado al terremoto producido en Chile

Costos

A continuación se expone una tabla con algunos de los programas rogue que se encuentran incluidos en los programas de afiliados y que actualmente poseen mayor tasa de actividad en la escena del crimeware, junto a los valores de comercialización y las ganancias aproximadas del afiliado, correspondientes al 40% de comisión.

Nombre del Rogue según ESET NOD32	Costo por licencia (U$S)	Ganancia afiliado (U$S)
Antivirus Plus	101,45	40,58
GreenAV	99,99	39,99
No Malware	79,50	31,80
XP Police Antivirus	69,99 / 99,99*	27,99 / 39,99
Personal Antivirus	59,95	23,98
Windows Defender 2010	59,95	23,98
Internet Security 2010	49,95	19,98
Contraviro	49,95 / 79,95*	19,98 / 31,98
Anti-Virus Elite 2010	27,00	10,80
Adware Remover	19,95	7,98

Tabla 1 - Tabla de valores

En el modelo de negocio que ofrecen los programas de afiliados, los códigos maliciosos del tipo rogue son, junto al spam, las alternativas más difundidas. Sin embargo esta situación, (que se presenta en la actualidad) por la misma naturaleza del negocio, podría ser utilizada para difundir otros tipos de malware.

Crimeware Kit

Otra de las vetas de negocio que posee un protagonismo importante es el desarrollo de aplicaciones web destinadas al control y administración de botnets y/o explotación de vulnerabilidades.

Este tipo de crimeware se compone de paquetes que en algunos casos disponen de constructores internos denominados *builders,* que permite generar un malware a medida junto a un archivo de

configuración. Son ejemplo de este tipo de aplicación ZeuS **[12]** y SpyEye, detectados por ESET NOD32 como la familia de malware *Win32/Zbot* y *Win32/SpyEye* respectivamente.

También se comercializan alternativas donde no solo permiten propagar malware (la mayoría no posee constructor de malware interno) sino que también se componen de un conjunto de *exploits*[6] preinstalados, llamado *exploits pack*.

En consecuencia, los atacantes pueden explotar vulnerabilidades de manera masiva, propagar malware para formar botnets a través de ataques Drive-by-Download, visualizar estadísticas sobre el estado de las infecciones, y administrar los zombis de forma remota y centralizada a través de un panel de control, denominado de C&C (Comando y Control) **[13]**.

En este sentido muchas campañas masivas de infección son generadas a través de este tipo de aplicaciones, mediante las cuales se propagan exploits embebidos en, por ejemplo, archivos del tipo PDF o SWF. Ejemplos de *exploits pack* son *Unique Exploit Pack*, YES Exploit System y *Fragus*.

Generalmente estos paquetes de administración se encuentran escritos en lenguaje de programación PHP y permiten controlar las botnets a través del protocolo HTTP; es decir, vía web.

Costos

La comercialización de estos crimeware también se lleva a cabo a través de foros clandestinos, donde el desarrollador deja la información de contacto, generalmente un número ICQ, como en los casos anteriores.

Durante el último año, sin embargo, algunos crimeware utilizan como estrategia de promoción, páginas web que habitualmente se encuentran a cargo de un afiliado, quien es el que publicita el crimeware, se expone y corre el riesgo (mínimo) de ser rastreado.

En la imagen se observa un caso de comercialización vía web de un conocido paquete crimeware llamado *YES Exploit System*, donde se observa la leyenda *"Official Business-Partner's Site"*.

[6] Código que permite aprovechar vulnerabilidades en sistemas operativos y aplicaciones

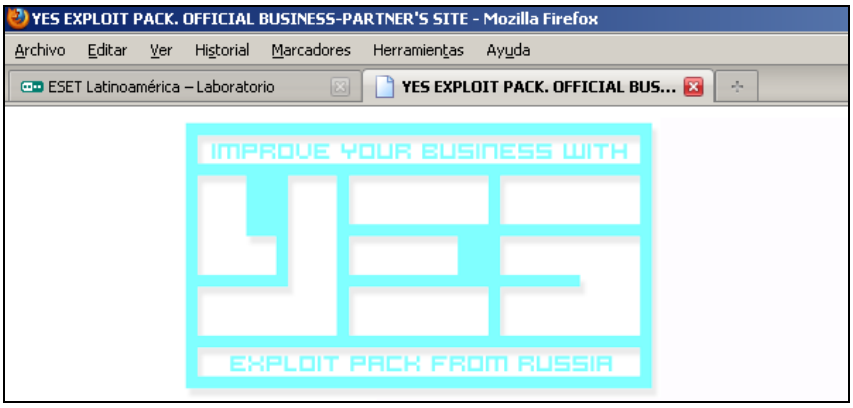

Imagen 10 – Venta de crimeware YES Exploit System vía web

A continuación se exponen los costos de algunas de las aplicaciones de este estilo más relevantes en la escena del crimeware:

Paquete crimeware	Costo (U$S)
ZeuS Kit v1.3	3.000 / 4.000
YES Exploit System v3.0	1.150
Eleonore Exploit Pack v1.3	1.000
Fragus v1.0	980
myLoader	700

Tabla 2 - Costos de algunos crimeware kit

Es importante destacar que el costo de cada crimeware estará dado en función de los componentes o módulos que posea, y entonces los precios varían desde **U$S 500** hasta **U$S 4.000** aunque durante los procesos de investigación llevados a cabo en el Laboratorio de Análisis de ESET Latinoamérica se ha encontrado crimeware con valores máximos de **U$S 13.000**.

También existe otro comercio clandestino relacionado con la posibilidad de desarrollar o de adquirir módulos específicos para determinada aplicación y que no necesariamente son creados por los desarrolladores de la aplicación original.

A modo de ejemplo, a continuación se exponen los valores que poseen en el mercado clandestino los módulos para el crimeware ZeuS:

- **Backconnect**: módulo que permite realizar una conexión remota con la computadora víctima. Su valor actualmente es de **U$S 1.500.**
- **Firefox form grabber:** módulo diseñado para robar datos desde formularios web cuando se utiliza el navegador Firefox. Su costo es de **U$S 2.000.**
- **Jabber (IM) chat notifier**: permite que el atacante obtenga información sobre la cuenta bancaria de la víctima, en tiempo real. Su valor es de **U$S 500.**

La evolución de los negocios presentados deja en evidencia que las ganancias obtenidas por los delincuentes informáticos alcanzan valores muy altos, lo que justifica también en gran parte el porqué de la profesionalización en cuanto a su desarrollo, y la cantidad de alternativas que se ofrecen en el mercado clandestino.

Conclusión

Los mecanismos empleados por los delincuentes informáticos han evolucionado hasta convertirse en negocios sumamente rentables, que crecen día a día y que constantemente buscan obtener ventajas a través de diferentes actividades ilegales, cuya víctima final es el usuario infectado.

Debe considerarse, además, que este despliegue de recursos, acciones y estrategias ideadas por los delincuentes informáticos tiene en su mira a la información de los usuarios y la economía e imagen de las compañías sin importar su envergadura o prestigio.

Esta situación hace necesario que se fortalezcan los mecanismos de seguridad de los usuarios y de todas las organizaciones, ya que los delincuentes informáticos siempre están pensando cómo violar las barreras de seguridad, y para ello cuentan con infinidad de recursos a fin de ejecutar sus acciones fraudulentas y alimentar la economía clandestina.

Más información

[1] Crimeware, el crimen del Siglo XXI
http://www.eset-la.com/centro-amenazas/2219-crimeware-crimen-siglo-xxi

[2] Malware en entornos empresariales
http://blogs.eset-la.com/laboratorio/2010/01/05/malware-entornos-empresariales/

[3] Massive Profits Fueling Rogue Antivirus Market
http://voices.washingtonpost.com/securityfix/2009/03/obscene_profits_fuel_rogue_ant.html

[4] Crimeware-as-a-Service en la industria delictiva
http://www.eset-la.com/centro-amenazas/2263-crimeware-as-a-service-industria-delictiva

[5] Botnets, redes organizadas para el crimen
http://www.eset-la.com/centro-amenazas/1573-botnets-redes-organizadas-crimen

[6] Ransomware
http://blogs.eset-la.com/laboratorio/2009/11/20/nuevo-ransomware-in-the-wild/

[7] Malware para sistemas operativos GNU/Linux y Mac OS
http://www.eset-la.com/centro-amenazas/2248-malware-sistemas-operativos-linux-mac-os

[8] Listado de programas de seguridad falsos
http://blogs.eset-la.com/laboratorio/2009/11/13/listado-programas-seguridad-falsos-viii/

[9] BlackHat SEO y propagación de malware
http://blogs.eset-la.com/laboratorio/2009/05/22/estrategias-blackhat-seo-propagacion-malware/

[10] Ingeniería Social
http://www.eset-la.com/centro-amenazas/1515-arma-infalible-ingenieria-social

[11] Terremoto de Haití, motivo para más rogue
http://blogs.eset-la.com/laboratorio/2010/01/14/terremoto-haiti-motivo-rogue/

[12] Botnets. Una breve mirada al interior de ZeuS (III)
http://blogs.eset-la.com/laboratorio/2009/06/02/botnets-breve-mirada-interior-zeus-iii/

[13] Control centralizado y propagación de malware
http://www.eset-la.com/centro-amenazas/2181-control-centralizado-propagacion-malware