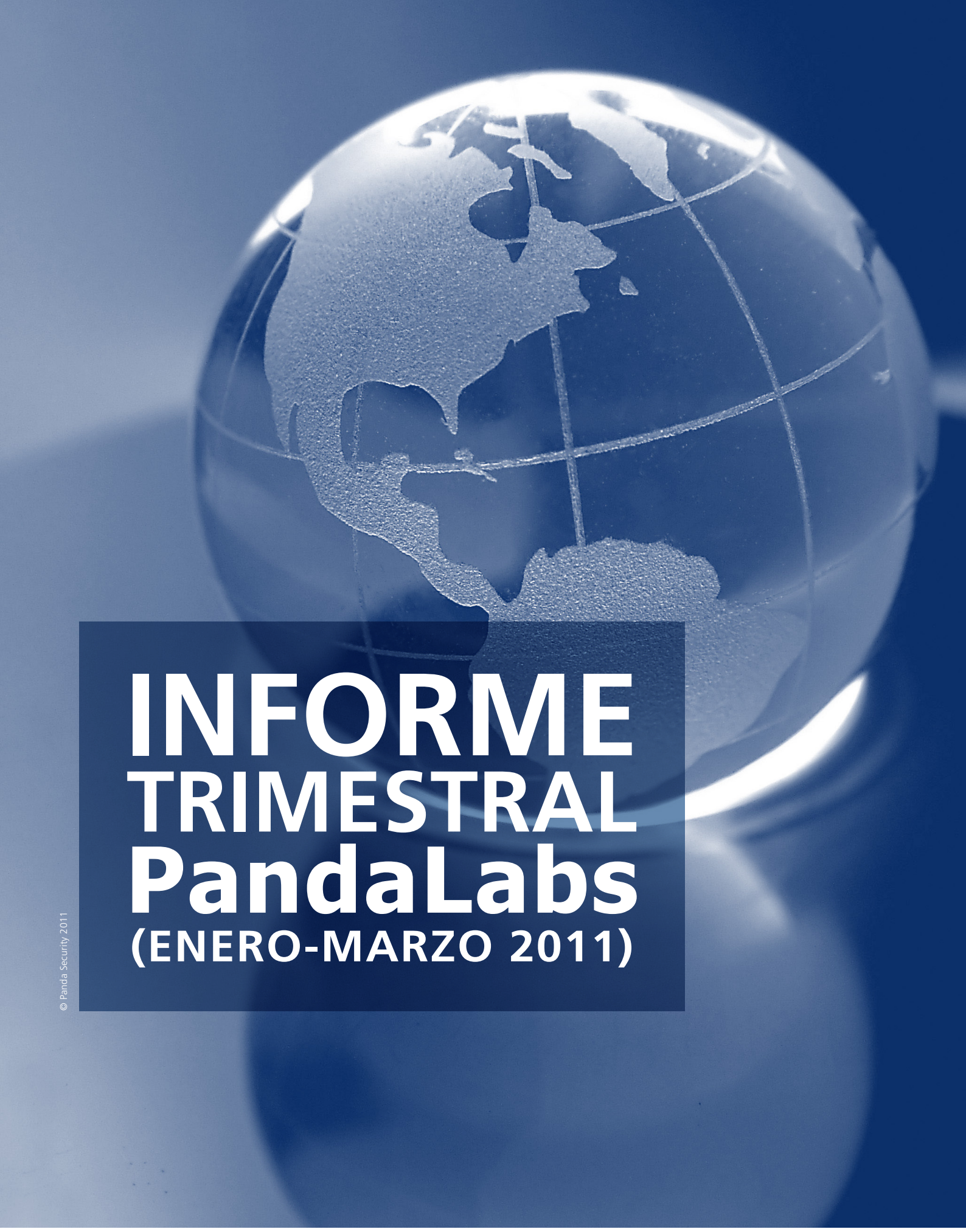


INFORME TRIMESTRAL PandaLabs

(ENERO-MARZO 2011)

PANDA SECURITY

Índice

Introducción

Ya ha concluido el primer trimestre de este 2011, y las novedades en materia de seguridad han seguido su tendencia prevista. Comienzan a aparecer ataques a terminales móviles, y Facebook sigue siendo el rey en todos los terrenos, por lo que los ciberdelincuentes tratan de utilizarlo para engañar a los usuarios.
Por otro lado, sucesos del mundo real -lejos en principio de Internet- como las revueltas en países del norte de África, han tenido grandes repercusiones en el mundo del ciberactivismo y la seguridad. También la ciberguerra / ciberespionaje han tenido gran protagonismo, teniendo casi siempre a China como la gran sospechosa detrás de muchos de los ataques descubiertos.

Malware en Móviles

Este primer trimestre de 2011 los titulares hablando de malware para dispositivos móviles han sido unos de los protagonistas. Esto se debe a varios motivos: por un lado, en el último trimestre de 2010 el nº de smartphones vendidos superó al número de PCs. Además, Android se está convirtiendo en la plataforma de referencia en telefonía móvil, y es posible que muy pronto lo sea en el terreno de las tablets. Por otro lado, la preocupación en el sector de la seguridad está creciendo, por lo que las investigaciones y pruebas de concepto denunciando problemas de seguridad se han multiplicado en los últimos meses.

Los ciberdelincuentes, por su parte, están empezando a percatarse de que hay un incipiente mercado del que se pueden beneficiar, y están comenzando a realizar pruebas sobre el mismo, al mismo tiempo que siguen con técnicas que ya habían probado con éxito en el pasado, utilizando malware para enviar SMS a números premium.

Aprovechando el Día de San Valentín, unos criminales rusos distribuyeron una aplicación que supuestamente permitía mandar un MMS con fotos románticas a nuestra media naranja. La aplicación contenía diferentes dibujos que los usuarios podían usar para felicitar a sus parejas, mientras que en segundo plano, la aplicación comenzaba a enviar SMS a un número premium.

FIG.01
IMÁGENES PARA SAN VALENTÍN UTILIZADAS POR TROYANO PARA TELÉFONOS MÓVILES.

FIG.02
IMÁGENES PARA SAN VALENTÍN UTILIZADAS POR TROYANO PARA TELÉFONOS MÓVILES.

Al mismo tiempo, un nuevo malware para Android aparecía en escena, se trataba de un troyano –detectado como Trj/ADRD.A- que robaba información personal y la enviaba al delincuente. Una de las recomendaciones que más se repetían al hacerse eco de esta noticia, era la de no descargarse aplicaciones de tiendas alternativas o de lugares cuya procedencia no sea fiable. En esta ocasión, el troyano había sido distribuido en tiendas de Android en China (no en la oficial) junto a juegos y fondos de pantalla.

A diferencia que con el iOS en el iPhone, en Android puedes instalar cualquier aplicación desde cualquier lugar, algo que los delincuentes están empezando a explotar. Pero esta no es la única diferencia, ya que las aplicaciones que se suben a la tienda oficial de Android (Android Market) tampoco son examinadas con la misma minuciosidad que las de Apple, lo que ha dado lugar a algún que otro "*susto*".

Unos días más tarde tuvo lugar la distribución de otro troyano para Android, también en China, que venía oculto dentro de una aplicación legal que los ciberdelincuentes habían reempaquetado con el troyano de regalo. Este troyano tenía diferentes funcionalidades, desde el envío de SMS a visita de páginas web. También permitía bloquear SMS entrantes.

A principios de marzo tuvo lugar el mayor ataque de malware en Android conocido hasta la fecha, esta vez las aplicaciones maliciosas se encontraban en el Android Market, la tienda oficial para comprar aplicaciones. En sólo 4 días las aplicaciones que instalaban el troyano habían tenido más de 50.000 descargas. El troyano en esta ocasión era mucho más avanzado, ya que no sólo robaba información personal del dispositivo, sino que podía descargar e instalar otras aplicaciones sin el conocimiento del usuario. Google eliminó todas las aplicaciones maliciosas de su tienda, y días más tarde eliminó las aplicaciones maliciosas de los móviles de los usuarios.

En sólo 4 días las aplicaciones que instalaban el troyano habían tenido más de 50.000 descargas.

Otro gran ataque a dispositivos móviles ha tenido lugar en este trimestre, esta vez de manos de los creadores del famoso troyano bancario conocido como ZeuS. Como muchos bancos están comenzando a utilizar un doble factor de autenticación utilizando dispositivos móviles, cuando nuestro PC está infectado y vamos a hacer alguna transacción nos aparece en la página del banco (modificada por el troyano Zeus) una pantalla donde nos solicitan el nº de móvil y el modelo, de tal forma que nos enviarán un mensaje para instalar un "***certificado de seguridad***" en el móvil, que es realmente un troyano preparado para interceptar todos los mensajes que recibamos. Esta es la 2ª variante de este tipo descubierta, la primera apareció el año pasado y ya hablamos de ella en el informe anterior.

Malware en Facebook

Facebook sigue siendo la red social por excelencia, y los ciberdelincuentes no tienen dudas en utilizarlo de todas las maneras posibles. Hemos visto cómo se ha popularizado la creación de aplicaciones para Facebook que postean en el muro de los usuarios con asuntos sugerentes, y al pinchar sobre ellos nos piden instalar la aplicación y luego nos piden rellenar una encuesta para poder acceder a algún tipo de premio. Los delincuentes obtienen así su beneficio económico, aunque en ocasiones además nos solicitan el número de teléfono móvil, de tal forma que al darlo nos suscriben a un servicio de pago.

No todos los ataques utilizados en Facebook se realizan con malware. Como muchas veces hemos comentado, la gente publica demasiada información personal en sus perfiles, lo que facilita el "***hackeo***" de cuentas de correo electrónico y de Facebook. George S. Bronk ha sido **detenido en California** precisamente por llevar a cabo este tipo de actividades. Utilizaba la información disponible en Facebook para hacerse con la cuenta de correo electrónico de la víctima. Una vez "***secuestrada***" la cuenta, buscaba información personal con la que hacer chantaje y obtener así dinero.

Y parece que cualquiera puede ser víctima de estos ataques, ya que el propio **Mark Zuckerberg** –creador de Facebook- ha sido víctima de un ataque de este tipo, y su página de fans de Facebook fue hackeada, mostrando un mensaje que comenzaba con "***Let the hacking begin***".

FIG.03

IMÁGEN DE LA PAGINA REAL DE MARK ZUCKERBERG, CREADOR DE FACEBOOK, TRAS SER HACKEADA.

Malware bancario

Cuando hablamos de malware bancario normalmente pensamos en la multitud de troyanos que aparecen para infectar a los clientes de los bancos y poder robarles la información para acceder a sus cuentas bancarias, pero en ocasiones vemos otro tipo de ataques. En enero, The Pentagon Federal Credit Union denunció que a través de un PC infectado se accedió a una de sus bases de datos con información confidencial de sus clientes. Entre la información robada se encontraban nombres, direcciones, números de seguridad social e información sobre cuentas y tarjetas de crédito.

Otra práctica habitual que no está relacionada con malware, es el uso de dispositivos de copia de tarjetas de crédito utilizados en cajeros. En enero **se condenó** a dos hombres de 32 y 31 años de edad por este hecho, a 7 y 5 años de cárcel respectivamente. Se sospecha que pertenecen a una banda de criminales rusos y americanos que están operando en todo el país.

Pero no sólo es el sector bancario el que se enfrenta al peligro. Tras un robo en la República Checa y un intento de pirateo en Austria, la Comisión Europea se vio obligada a **suspender el sistema de comercio de derechos de emisión de CO2**. Por supuesto, los ciberdelincuentes buscaban un beneficio económico. Ya se dio un **ataque similar hace unos meses**, cuando un pirata informático robó 1,6 millones de derechos de emisión a la cementera Holcim en Rumanía. A 15 euros cada uno, suponía unas pérdidas de 24 millones de euros. En este tipo de ataques, además de las pérdidas económicas, es el propio sistema el que se ve atacado y muestra su vulnerabilidad.

Esta diversificación se puede ver en otros ámbitos. En este trimestre hemos visto cómo aparecían variantes del conocido troyano bancario ZeuS cuyo objetivo no eran entidades bancarias, sino sistemas de pago online como Webmoney o MoneyBookers.

Otro ataque que ha tenido lugar tuvo como víctima de ZeuS al **gobierno británico**, que reconoció haber sido infectado tras recibir un ataque dirigido que contenía una versión de este troyano que, además de estar preparado para robar credenciales bancarias, puede robar todo tipo de información de la víctima.

A vueltas con Stuxnet

Si pensabais que ya no sabíamos todo del ataque protagonizado por Stuxnet, el gusano dirigido a sabotear el programa nuclear iraní, estáis equivocados. Aún queda mucha información por conocer, y poco a poco se descubren nuevas pistas que nos revelan nueva información. Han aparecido noticias que indicaban a EEUU e Israel como los autores del ataque, aunque sin pruebas consistentes. Sin embargo, una noticia nos sorprendió a todos cuando el General israelí Gabi Ashkenazi, en una fiesta celebrando su último día de trabajo, se atribuyó el ataque de Stuxnet como uno de sus triunfos.

El General israelí Gabi Ashkenazi, en una fiesta celebrando su último día de trabajo, se atribuyó el ataque de Stuxnet como uno de sus triunfos.

Por otro lado, se ha sabido que Stuxnet ha conseguido su objetivo. Científicos rusos que trabajan en la planta nuclear de Bushehr han mostrado su preocupación al Kremlin sobre la falta de medidas de seguridad y han tratado de convencer al gobierno iraní para que retrase sus planes de puesta en marcha del reactor hasta finales de año, para que se pueda realizar una evaluación adecuada de los daños que Stuxnet ha causado. Finalmente, la puesta en marcha del reactor -prevista a finales de enero-, ha sido pospuesta.

Ciberactivismo

Cuando en las predicciones de 2011 augurábamos que el ciberactivismo iba a ser un protagonista indiscutible a lo largo del año entrante, no podíamos imaginar que iba a tardar tan poco en serlo. Cierto es que ha sido debido a las revueltas políticas en las dictaduras del norte de África –que no una causa de las mismas- pero el protagonismo de Internet y de las redes sociales en concreto, ha sido clave en el desarrollo de los acontecimientos.

En Egipto Internet se convirtió en una especie de campo de batalla entre el gobierno egipcio y los protestantes, principalmente en lugares como Facebook o en páginas de grupos como Anonymous.

FIG.04
CARTEL DEL GRUPO ANONYMOUS ANUNCIANDO SU CAMPAÑA A FAVOR DE LOS PROTESTANTES EGIPCIOS

El gobierno egipcio llegó a sentirse tan acorralado, que en una acción sin precedentes cortó completamente el acceso a Internet y las redes de telefonía móvil de todo el país.

Por otro lado, en diferentes países occidentales desde donde usuarios participaron en los ataques del pasado año en defensa de Wikileaks dentro de la conocida como "***Operation: Payback***", se han realizado detenciones de usuarios que participaron en los mismos. Principalmente se trata de adolescentes que utilizaron la herramienta LOIC para participar en los ataques sin utilizan ningún tipo de proxy anónimo o red privada virtual que les hubiera permitido ser indetectables. Todo apunta a que se trata de una acción ejemplarizante por parte de los gobiernos (Holanda, Reino Unido y EEUU) para amedrentar a los protestantes.

Otra "***batalla***" digna de mención ha sido la protagonizada por la firma de seguridad norteamericana HBGary Federal y el grupo Anonymous. Todo comenzó cuando el CEO de la compañía americana, Aaron Barr, dijo tener datos de los cabecillas de Anonymous y que pensaba hacerlos públicos. Simpatizantes de Anonymous se sintieron aludidos, por lo que ni cortos ni perezosos trataron de colarse en la compañía… y lo consiguieron en apenas unas horas. No sólo hackearon su página web y su cuenta de Twitter, sino que consiguieron robar decenas de miles de correos electrónicos que acto seguido fueron distribuidos desde The Pirate Bay.

Por si esto no fuera suficiente, el contenido de algunos de estos correos ha resultado ser realmente comprometedor para la compañía norteamericana, ya que han sacado a la luz prácticas claramente inmorales (como la propuesta de desarrollo de un rootkit) que han colocado a la empresa en una situación tan delicada que su CEO, Aaron Barr, no ha tenido más remedio que dimitir.

Ciberguerra

Además del caso Stuxnet, cada vez tenemos más noticias sobre casos de ciberguerra (englobando dentro de ellos casos de ciberespionaje).

En enero se supo que un ataque dirigido había alcanzado de lleno al Ministerio de Economía canadiense. Las primeras investigaciones apuntaban a China, si bien es cierto que es muy difícil demostrar quién estaba realmente detrás del ataque. No se ha hecho pública qué información ha sido robada.

En febrero la compañía americana McAfee hizo público un informe en el que se hablaba de la operación "Night Dragon", donde una serie de compañías energéticas habían sido víctimas de espionaje en una operación que había estado activa al menos durante dos años. Posteriormente se ha podido conocer que entre las compañías víctimas del ataque se encontraban Exxon Mobil, Royal Dutch Shell, BP, Marathon Oil, ConocoPhillips, y Baker Hughes. Los ataques, de nuevo, venían desde China, aunque no se puede demostrar que el gobierno Chino esté directamente implicado.

En marzo se hizo público que el Ministerio de Economía francés fue víctima de otro ataque –cuyo origen apunta de nuevo a China- cuyo objetivo era el robo de documentos sobre la reunión del G-20 en febrero, que tenía lugar en París. Más de 150 ordenadores estaban afectados, y otros ministerios franceses habían sufrido intentos de intrusiones sin éxito.

El Ministerio de Economía francés fue víctima de otro ataque –cuyo origen apunta de nuevo a China- cuyo objetivo era el robo de documentos sobre la reunión del G-20

También en marzo, 40 páginas web pertenecientes principalmente al gobierno de Corea del Sur, fueron víctimas de un ataque de denegación de servicio. Este ataque ha sido muy similar a otro que tuvo lugar en 2009, del que se culpó a Corea del Norte, pero tras la investigación todo apuntaba a… China.

FIG.05
LA CIBERGUERRA ESTÁ AQUÍ

Comenzamos el año 2011 con un balance trimestral que sigue confirmando la gran avalancha de nuevo malware que se está creando. No es que nos repitamos constantemente: es que es la realidad.

En PandaLabs ha aumentado el número de nuevas muestras que recibimos cada día: de 55.000 hace apenas unos meses, a 63.000 a finales del pasado año y a una media de 73.190 en lo que llevamos de año. Es decir, un 16% más si lo comparamos con el último trimestre del año 2010.

Este recuento es malware confirmado, es decir, son muestras ya analizadas por Inteligencia Colectiva, nuestro sistema automático de detección, clasificación y análisis de malware, o por nuestro equipo técnico. O lo que es lo mismo, en el primer trimestre de año, recibimos de media al día 195.463 ficheros para analizar, de los cuales, el 37,4% son nuevas amenazas.

En cuanto al reparto por tipo de amenazas, son los troyanos los que, sin duda, están creciendo, copando el ranking de nuevo malware en casi un 70%.

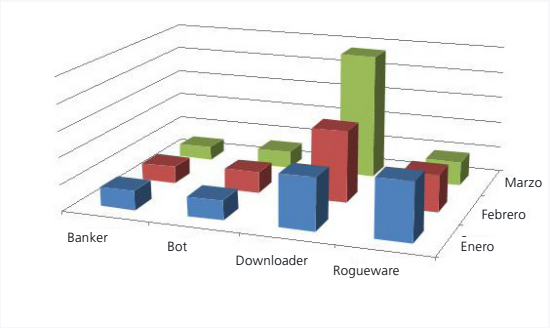


FIG.06

LOS DOWNLOADER HAN AUMENTADO CONSIDERABLEMENTE ES ESTE PRIMER TRIMESTRE

Si analizamos el subtipo de amenazas que más han crecido, viendo su evolución en los últimos tres meses, sin duda concluimos que la creación de nuevos troyanos bancarios está estabilizada; los bots parece que decrecen, al igual que los rogueware o falsos antivirus.
Pero echemos un vistazo a la evolución de la categoría de Downloaders, dentro de la familia de los troyanos: aquí encontramos parte de la explicación a la subida de nuevas amenazas.

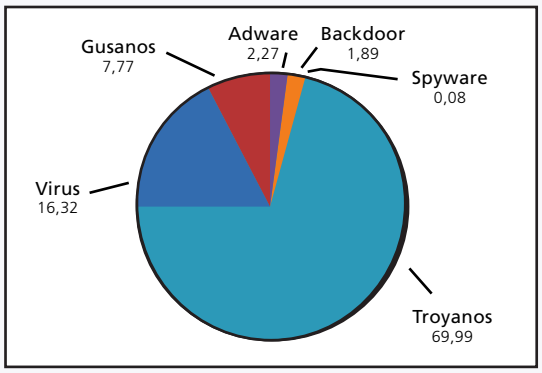


FIG.07

TIPOS DE MALWARE

Los Downloaders son un tipo de Troyano que está preparado para, una vez ha infectado el ordenador del usuario, conectarse a través de Internet y descargar otro tipo de malware. Los ciberdelincuentes lo utilizan frecuentemente, porque el downloader –a diferencia de otros troyanos- pesa realmente poco y pasa totalmente inadvertido, ya que contiene sólo unas pocas líneas de código que le permite conectarse a Internet.

Respecto a las categorías de malware que cuentan con menor representación dentro del ranking final, llama la atención la cantidad de dialers que los ciberdelincuentes siguen produciendo, mayoritariamente enfocados a países poco desarrollados todavía (tecnológicamente hablando) que siguen conectándose a Internet a través de los tradicionales módems.

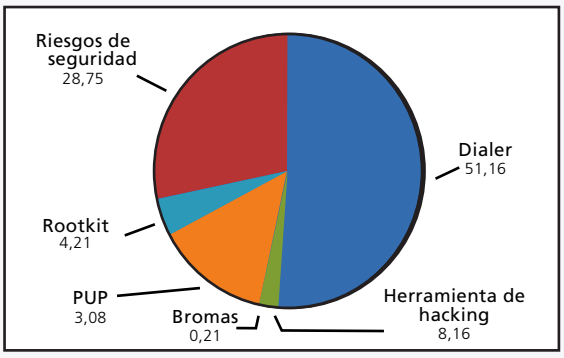


FIG.08

DESGLOSE DEL TIPO "OTROS"

Los países más infectados por malware del Q1

Pocas sorpresas nos hemos llevado a la hora de elaborar el ranking de países más infectados, a nivel mundial, por cualquier tipo de malware. Lo realmente reseñable es el hecho de que más o menos la mitad del ranking de la tabla sigan con niveles de infección del 50% o superior, llegando incluso a rozar el 70% en el caso de China, Tailandia o Japón.

Estas cifras se obtienen de los usuarios que utilizan, de forma gratuita, nuestro antivirus online Panda ActiveScan 2.0. De todos los ordenadores infectados, la herramienta guarda información estadística de cuántos PCs por país están infectados por algún tipo de amenaza informática.

Este trimestre vemos cómo Estados Unidos ha desaparecido del Top 20 de países más infectados, aunque países como Francia o España, que andan rozando los límites de clasificación, han aparecido en escena de nuevo en este primer trimestre. Lo mismo sucede con Irlanda, que hasta ahora no aparecía en el ranking, y ahora se ha colocado en la penúltima posición.

Perú y Ecuador cierran el ranking, con niveles que se sitúan entre el 30 y el 40%, datos que mejoran con respecto a las mediciones de otras ediciones de este informe trimestral.

Finalmente, en cuanto a qué tipo de malware está mayoritariamente infectando a determinados países, vemos que, evidentemente, la categoría de troyanos son los que se llevan todo el protagonismo, seguidos por los tradicionales virus y gusanos.

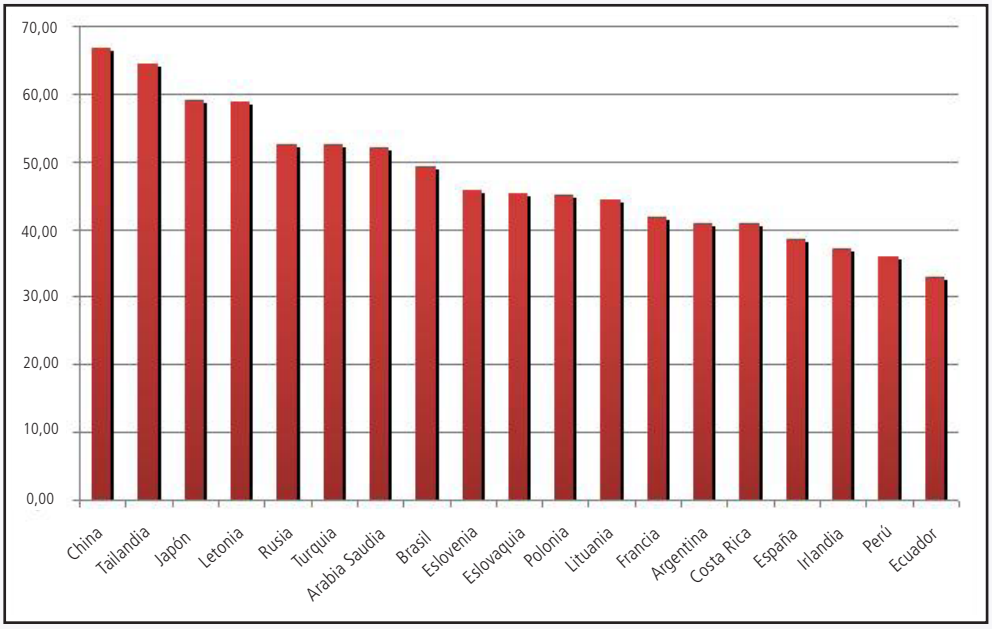
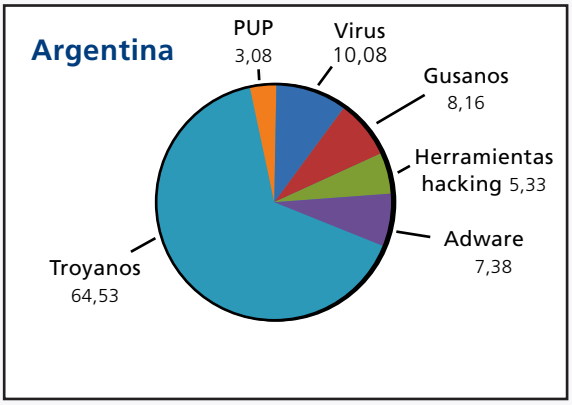
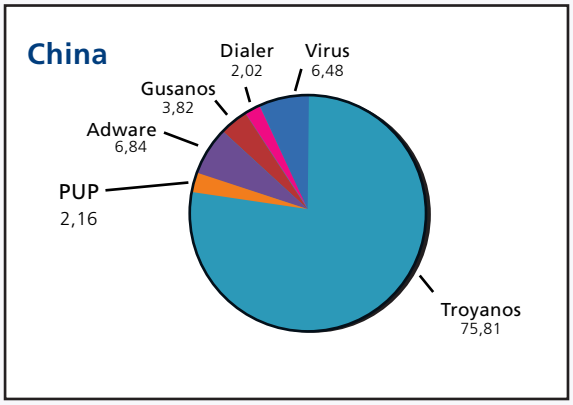
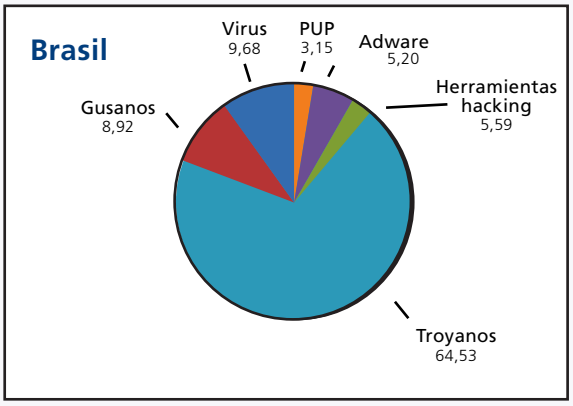


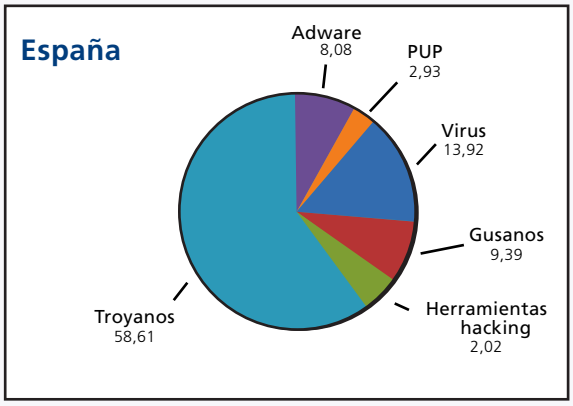
FIG.09

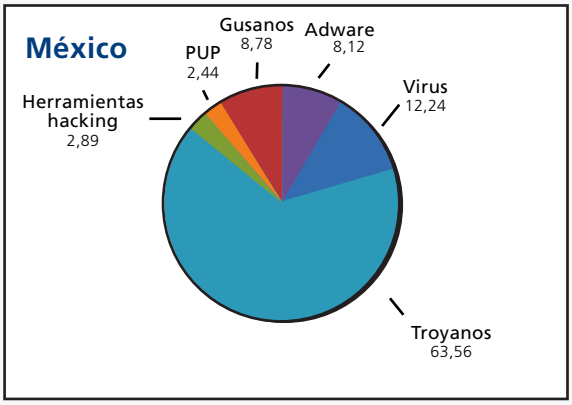
PORCENTAJE DE INFECCIÓN POR PAÍSES











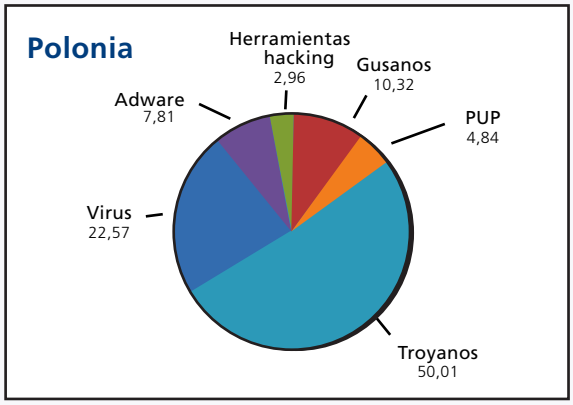


FIG.10

TIPOS DE MALWARE POR PAÍS

Para el resumen de vulnerabilidades de este primer trimestre vamos a cambiar un poco la temática sin desviarnos del tema central, que son las vulnerabilidades. En este artículo vamos hablar sobre el concurso PWN2OWN organizado por el equipo de ZeroDay [1] Inciative de la compañía TippingPoint.

PWN2OWN es la combinación de 3 palabras: "***PWN***", "***2***" y "***OWN***". PWN (abreviatura de powned) que más o menos viene a significar: el sistema ha sido comprometido por el atacante, el número 2 es la codificación de la palabra TO (por su similitud en fonética con TWO) y OWN, abreviatura de "***owned***" o propiedad. Es pocas palabras, si consigues comprometerlo, normalmente ejecutando el código arbitrario que ha introducido el atacante, te lo puedes llevar a casa además de 15.000 $ como premio, reconocimiento, y posiblemente una interesante oferta de trabajo.

En el concurso, todos los sistemas operativos y versiones de aplicaciones que se intentan vulnerar están totalmente parcheados.

Este año el concurso se ha celebrado entre los días 9 y 11 de marzo en Vancouver y, como viene siendo habitual, dentro de la conferencia de seguridad CanSecWest [2].

Este concurso se lleva celebrando desde el año 2007 y en él, se dan cita los mejores investigadores en localizar nuevas vulnerabilidades para romper las últimas protecciones de seguridad de los sistemas operativos y dispositivos móviles más importantes. De hecho, en el concurso, todos los sistemas operativos y versiones de aplicaciones que se intentan vulnerar están totalmente parcheados. Es común que días antes del concurso las compañías lancen sus últimas correcciones y parches de seguridad para evitar que sus productos sean vencidos.

El primer día del concurso le toco a Apple sufrir la primera derrota. Investigadores de la empresa VUPEN se aprovecharon de una vulnerabilidad en la última versión del motor WebKit [3] de Safari para saltarse las protecciones de ASLR [4] y DEP [5] en la versión de 64bit de un MacOSX Snow Leopard totalmente parcheado. De esta forma, los ganadores del concurso recibieron la cantidad de 15.000$ y un MacBooc Air como recompensa a las 2 semanas de trabajo que invirtieron para dar con la vulnerabilidad, para la que necesitaron crear herramientas a medida con el objetivo de poder crear un exploit funcional que les diera la victoria. Tras la exitosa explotación, varios usuarios del sistema operativo de la manzana se pronunciaron en varios foros exigiendo a Apple más compromiso en la securización de su sistema operativo y aplicaciones, ya que en anteriores ediciones también había sido el sistema más fácil de explotar. Así que los usuarios de Apple estarán impacientes por ver que pasa el próximo año con la nueva versión de su sistema operativo que tiene como nombre Lion, y ver si realmente saca sus garras para hacer frente a los investigadores y salir ileso por primera vez.

El segundo en caer fue Internet Explorer 8 (32 bit) que se estaba ejecutando en un Windows 7 Service Pack 1. Stephen Fewer investigador de la empresa Harmony Security, tardó cerca de mes y medio en preparar un elaborado exploit que se aprovecha nada más y nada menos de tres vulnerabilidades para conseguir la ansiada ejecución de código. Stephen utilizó 2 vulnerabilidades para poder ejecutar código en el navegador y utilizó una última vulnerabilidad para saltarse el modo protegido de Internet Explorer.

Pasando ya al segundo día de la competición, llego el turno de probar la seguridad en los dispositivos móviles. Nuevamente Apple se llevó un varapalo y el iPhone 4 fue derrotado por el famoso experto en seguridad y ex-trabajador de la NSA Charlie Miller, quien también disponía de un exploit funcional para MacOS X, pero este año los investigadores de la empresa VUPEN se le adelantaron. Charlie Miller ya ha demostrado otros años en esta misma competición que es capaz de romper todas las barreras de seguridad que Apple dispone en su sistema operativo y dispositivo móvil. No obstante, el investigador también ha reconocido que la creación de un exploit funcional para la versión 4.3 de IOS, la nueva versión que está lista para el iPhone 4 y el iPad, sería mucho más difícil debido a la implementación del sistema ASLR en esta última versión. Esta mitigación está diseñada junto con DEP como máxima protección para evitar la explotación satisfactoria o ejecución de código a través de una vulnerabilidad, como ya hemos comentando recientemente en nuestros informes trimestrales. Mencionar que Charlie Miller lanzó su exploit nuevamente a través de una vulnerabilidad encontrada en la versión móvil del navegador Safari, el exploit consiguió acceder a la información confidencial del teléfono.

También fue vencido el terminal de la empresa RIM con su sistema operativo Blackberry OS 6. Nuevamente, se explotó una vulnerabilidad en el motor WebKit (este motor es utilizado por Google para su navegador Android y Apple para IOS y MacOSX). A diferencia del iPhone, Blackberry si disponíade las protecciones de seguridad ASLR y DEP en sus sistema operativo, pero como ya hemos mencionado, estas protecciones no han podido con los investigadores de seguridad y estos han conseguido comprometer el dispositivo accediendo a su información confidencial.

En Panda Security disponemos de los productos y tecnologías necesarios que harán de tus sistemas los más seguros.

Este año los elogios van para Google ya que ni su dispositivo Android, ni su navegador Google Chrome, ni su sistema Google Chrome OS han sido comprometidos en este evento. Mencionar que días antes a la competición Google arregló, al igual que Apple, ciertos fallos encontrados en su navegador Google Chrome, y es posible que esto hizo que los investigadores no participasen en el intento al ver que sus exploits ya no funcionaban. Mencionar que el nuevo sistema operativo para móviles de Microsoft, Windows Phone 7, tampoco fue vulnerado. Es posible que esto haya sido debido a que el principal investigador que apuntaba a superar el reto, GeoHot, no pudo asistir al evento al estar ocupado en la demanda que Sony le ha puesto por hackear la PlayStation 3. Mencionar que este Hacker también ha sido capaz de hackear el iPhone de Apple y hace unos meses había comentado que estaba interesado en realizar lo mismo con Windows Phone 7.

Como conclusión podemos decir que las compañías de seguridad y software están haciendo grandes esfuerzos por mejorar la seguridad en sus sistemas operativos y aplicaciones con el objetivo de proteger cada vez mejor a sus clientes ya que son conscientes del peligro que pueden correr.

La implementación de DEP y ASLR ha sido un gran avance para impedir que la explotación de una vulnerabilidad consiga la ejecución del código inyectado por el atacante. No obstante, aún queda camino por recorrer y prueba de ello es el concurso PWN2OWN, que desde el punto de vista de la seguridad es muy positivo y necesario para que los fabricantes puedan conocer las nuevas debilidades que disponen sus productos, y vean la necesidad de invertir más tiempo en la mejora de éstos, así como aprender de los mejores.

No obstante hay que tener siempre presente que el eslabón más débil de la cadena es el ser humano, como ejemplo podemos decir que hace tan sólo unos meses, muchos usuarios de Android han sido infectados por software malicioso al descargar ciertas aplicaciones a su móvil, para esta acción no hace falta explotar ninguna vulnerabilidad, basta con descargar una aplicación de una fuente desconocida o ser víctima de algún engaño. Por lo tanto, no sólo las compañías tienen que mejorar en seguridad, si no que los usuarios debemos de ser conscientes de lo que descargamos y por dónde navegamos.

Como hemos visto en algunas ocasiones, un sistema operativo totalmente actualizado no es suficiente, por lo tanto tenemos que hacer uso de otras tecnologías y aplicaciones que eviten una posible intrusión o infección en nuestros sistemas. Seas usuario de Microsoft Windows o Apple MacOSX, en Panda Security disponemos de los productos y tecnologías necesarios que harán de tus sistemas los más seguros.

1 http://zdi.tippingpoint.com/
2 http://cansecwest.com/
3 http://www.webkit.org/
4 http://en.wikipedia.org/wiki/Address_space_layout_randomization
5 http://en.wikipedia.org/wiki/Data_Execution_Prevention

Ciberactivismo y ciberguerra a escena

El III Security Blogger Summit, celebrado el pasado febrero en Madrid, abordó las nuevas tendencias de Ciberactivismo y Ciberguerra, así como los peligros a los que hoy están sometidos los usuarios y las instituciones en la Red. Asimismo, se estableció un foro de debate en torno a los casos más recientes, la cooperación entre países y los límites de estas actividades en Internet. También se discutió acerca de las tendencias que se verán en 2011 y el marco legal para este tipo de actividades cibernéticas.

Los ponentes del III Security Blogger Summit que han participado en el evento han sido varios reconocidos bloggers y periodistas, como Enrique Dans, Chema Alonso, Rubén Santamarta, además de Elinor Mills y Bob McMillan, prestigiosos periodistas estadounidenses especializados en seguridad informática. Todos ellos coincidieron en resaltar la importancia de los ataques coordinados a escala mundial contra cualquier institución.

Ciberactivismo, una manifestación en Internet

El III Security Blogger Summit dio comienzo con un keynote de Enrique Dans, Profesor del IE y reconocido blogger, en el que abordó la dimensión social del ciberactivismo en revueltas recientes como la de Irán, Túnez o Egipto. Asimismo, insistió en la idea de que la web social disminuye las barreras del activismo, ya que "*podemos hacer un RT y creer que ya formamos parte de un fenómeno de ciberactivismo*".

Acerca de los últimos acontecimientos en torno a WikiLeaks y a la defensa de Julian Assange, Enrique Dans afirmó que "*Fenómenos como el de WikiLeaks serán imparables y cada persona podrá dar a conocer información relevante desde un sitio web, aunque lo hará de forma intoxicada, porque no ejercerá como un medio de comunicación*".

Sin embargo, Bob McMillan, periodista especializado en seguridad informática en San Francisco, no tardó en afirmar que para él "*la importancia de WikiLeaks es la misma que la de el New York Times*" y añadió que "*WikiLeaks ha ayudado a quienes deseaban filtrar información y pensar en cambiar la ley cuando se producen ataques de denegación de servicio como en la "Operación Vengar a Assange" es muy difícil, aunque creamos que estos casos de ciberactivismo puedan ser legítimos*".

Asimismo, en la mesa redonda moderada por Josu Franco, Director de Estrategia Corporativa de **Panda Security**, Elinor Mills, redactora senior de CNET News para temas de seguridad con más de 20 años de experiencia afirmó que en las manifestaciones sociales, "las personas hemos sustituido las juntas de vecinos por las herramientas que nos facilita Internet".

> ***WikiLeaks ha ayudado a quienes deseaban filtrar información y pensar en cambiar la ley.***

Por su parte, Chema Alonso, Ingeniero Informático por la URJC con postgraduado en Sistemas de Información y autor de "*Un Informático en el Lado del Mal*", añadió que "la evolución técnica está cambiando la forma de manifestarse y ya no es necesario ser 3 millones de personas para hacerse notar", mientras que Rubén Santamarta, investigador de seguridad, con cerca de una década de experiencia en el mundo de la ingeniería inversa y la seguridad IT, afirmó que "*el ciberactivismo ha surgido de la situación global que vivimos*".

Además, preguntados por el público, se abordó la legalidad del ciberactivismo frente a la legitimidad de estas actividades. "*Los usuarios necesitan sinceridad y esa es la clave de WikiLeaks*", afirmó Rubén Santamarta. "*Para mí, lo preocupante es que no ha habido ninguna reacción por parte de los gobiernos ante todas las revelaciones de WikiLeaks*", concluyó Enrique Dans.

Ciberguerra, ¿realidad o sensacionalismo?

Los invitados al III Security Blogger Summit abordaron algunos de los casos más relevantes en términos de ciberguerra, como los supuestos ataques a centrales nucleares iranís con el troyano Stuxnet, así como la denominada Operación Aurora, sobre los ataques procedentes de China y dirigidos a Google para conseguir secretos empresariales.

Elinor Mills y Bob McMillan coincidieron en señalar que el término Ciberguerra era "*demasiado exagerado*" para lo que en realidad está sucediendo. "*Todavía no sabemos muy bien cuáles son las dimensiones de la ciberguerra, y puede confundirse con el espionaje o incluso el cibercrimen*" afirmó Elinor Mills. Bob McMillan añadió que "*Stuxnet ha sido un arma cibernética, pero eso no quiere decir que estemos inmersos en una ciberguerra. Si realmente se estuviera preparando una ciberguerra, ésta sería a escala mundial, como las dos grandes guerras del siglo XX*".

Sin embargo, Rubén Santamarta insistió en la idea de que la ciberguerra está dando sus primeros pasos y estallará dentro de 10 años. "*Tenemos que pensar que no se trata de una guerra con ejércitos. Es una guerra de cuarta generación, donde es posible dañar a un país sin invadirlo con un ejército. Lo que sucede es que antes de que un país le declare la guerra a otro, éste tiene que tener controlado el país previamente a través de Internet; y eso ya está sucediendo*".

Asimismo, Santamarta añadió que "*la esperanza que tenemos es que no todo el mundo está dispuesto a cometer un ataque de esas dimensiones*". Chema Alonso incluso afirmó "*que hoy en día las personas capaces de hacerlo son muy pocas y con mucho talento*".

Podéis encontrar más información sobre el 3er Security Blogger Summit en **www.securitybloggersummit.com.**

FIG11

PARTICIPANTES EN LA MESA DEL SECURITY BLOGGER SUMMIT

El mercado negro de cibercrimen

En este primer trimestre, PandaLabs, nuestro laboratorio antimalware, ha descubierto una vasta red de venta de datos bancarios robados así como otro tipo de productos, operada por cibercriminales, que cuenta con hasta 50 tiendas online a las que sólo se puede acceder mediante el contacto previo personal con los hackers encargados de su promoción en foros y chats.

El llamado mercado negro del cibercrimen, que tradicionalmente se centraba en la distribución de números de tarjetas bancarias robadas a usuarios de todo el mundo y credenciales de acceso a banca online, han diversificado su negocio en 2010 ofreciendo todo un abanico de productos y servicios.

Ahora, los datos bancarios van acompañados de una larga ristra de datos personales del titular de la tarjeta o cuenta, con los que, lógicamente, se puede operar de forma más veraz. Todo ello, eso sí, desde un módico precio de 2$ por tarjeta de crédito sin información adicional y sin garantía de saldo. Si el comprador quiere garantía de dinero existente en línea de crédito o en la cuenta online del banco, tendrá que pagar un poco más: desde 80$ para saldos bajos y hasta 700$ por credenciales de acceso a una cuenta con un saldo garantizado de 82.000$.

Estos precios varían si lo que queremos comprar son datos de acceso a cuentas creadas y con historial de tiendas online o a sitios de pasarelas de pago, como PayPal. En este caso, para una cuenta simple sin saldo verificado, tendremos que pagar 10$, cantidad que subirá hasta los 1.500$ dependiendo de la plataforma y la garantía de dinero disponible.

Igualmente, estos ciberdelincuentes ofrecen la venta máquinas duplicadoras de tarjetas físicas (de 200 a 1.000$) y de falsos cajeros automáticos (hasta 3.500$ por unidad y según modelo), o tarjetas bancarias ya duplicadas físicamente listas para ser utilizadas (a partir de 180$).

Además, también ofrecen servicios de blanqueo de dinero (realización de transferencias bancarias o cobro de cheques) a cambio de comisiones que pueden ir desde el 10 hasta el 40% del total de la operación. Y más: si el usuario quiere datos bancarios para comprar cualquier producto online, pero teme ser pillado por la dirección de entrega, estos ciberdelincuentes hacen la compra por él y lo envían a cualquier sitio cobrando entre 30 y 300$ (según el producto elegido).

Y si lo que el usuario quiere es tener su propia tienda online falsa para obtener de esta manera y de forma directa tanto datos de los usuarios que piquen como el dinero de compras de productos, que nunca recibirán (como es el caso de los falsos antivirus), el equipo de "***diseño***" de los vendedores ofrecen proyectos llave en mano que incluyen el diseño y desarrollo de la tienda completa, su publicación y posicionamiento en buscadores para garantizar tráfico. En este caso, el precio "***depende del proyecto***".

El alquiler de redes para el envío de spam (a través de ordenadores comprometidos por un bot, por ejemplo) en función del número de ordenadores elegido y la frecuencia de envío, o el tiempo de alquiler, está disponible desde 15%. El precio sube a 20$ si además se quiere alquilar un servidor SMTP o una VPN que garantice el anonimato del emisor.

PRODUCTOS	PRECIO
Tarjetas de crédito	Desde 2$ hasta 90$
Tarjetas de crédito físicas	Desde 180$ + coste de los datos
Máquinas duplicadoras de tarjetas	Desde 200 hasta 1.000 $
Cajeros automáticos falsos	Hasta 3.500$
Credenciales bancarias	Desde 80 y hasta 700$ (con garantía de saldo)
Transferencias bancarias y cobro de cheques	Entre el 10 y el 40% del total a transferir o cobrar
Cuentas de tiendas online y pasarelas de pago	Entre 80 y 1.500$ con saldo verificado
Diseño e implementación de falsas tiendas online	Según proyecto (sin especificar)
Compra y envío de productos	Entre 30 y 300$ (dependiendo producto)
Alquiler envío de spam	A partir de 15$
Alquiler SMTP	A partir de 20$. 40$ para uso durante 3 meses
Alquiler VPN	20$ para utilización para 3 meses

FIG.12

ESTE ES UN RESUMEN DE LOS PRODUCTOS OFERTADOS Y SU RANGO DE PRECIOS

Como la vida misma

Como si de cualquier otro tipo de negocio se tratara, el mercado negro cuenta con todos los ingredientes que un comprador necesita para confiar en el vendedor. Por ejemplo, existe mucha competencia en el mercado negro, y la ley de la oferta y la demanda les obliga a ajustar los precios y a ofrecer descuentos por volumen.

Suelen utilizar foros escondidos underground que les garantiza el no tener curiosos ajenos al negocio.

Muchos de ellos ofrecen datos de acceso a cuentas bancarias o de tarjetas de crédito robadas a modo de prueba, y garantizan su material: si el cliente no queda satisfecho, le devuelven el dinero; o si cualquiera de los datos vendidos no funciona, el vendedor le cambia el artículo por otro que goce de buena salud.

Eso sí, siendo el mercado negro tiene sus peculiaridades: llegar a estos vendedores no es sencillo, suelen utilizar foros escondidos underground que les garantiza el no tener curiosos ajenos al negocio. Así, su oficina es Internet, y en sus reclamos publicitarios hasta publican las horas de atención al público. Los hay más lanzados que tienen cuentas activas en Facebook y Twitter, utilizándolo de escaparate de sus productos.

Además, y lógicamente, el contacto se realiza siempre vía aplicaciones de mensajería instantánea, para garantizar el anonimato, o mediante direcciones de correo electrónico gratuitas genéricas.

Una vez contactados, la transacción puede hacerse directamente o bien el vendedor proporcionará una dirección web con login y password de acceso a una tienda online donde el comprador puede componer a su gusto su "*cesta de la compra*".

Eso sí, el pago siempre se hace por adelantado y utilizando siempre compañías de envío de dinero, como Western Union, Lyberty Reserve, WebMoney o similares. El estudio completo está disponible en **http://prensa.pandasecurity.com/centro-de-prensa/white-papers/#monograficos**

FIG13

FUNCIONAMIENTO DEL CIBERCRIMEN

Conclusión

El mundo de la seguridad sigue siendo tan apasionante como siempre, sino más. Según aparecen nuevas técnicas de protección, los criminales tratan de idear nuevos formas para saltárselas. Los gobiernos de muchos países occidentales están aprendiendo que hay ciberataques de la forma más dura, siendo víctimas de los mismos, por lo que tendrán que ponerse muy serios a la hora de implantar medidas de protección. La situación en Libia se ha recrudecido con una cuasi guerra civil, lo que deja el ciberactivismo en un segundo plano. Aún así, hay tensión en otras dictaduras de la zona y veremos cómo evoluciona la situación en la zona.

El próximo trimestre veremos cómo se comportan las ventas de tablets basados en Android, como el Motorola XOOM o el Samsung Galaxy Tab II, algo que puede tener mucha incidencia en el futuro del desarrollo de malware para Android. Si los tablets logran sustituir en muchas de las tareas a los PCs, Android se convertirá en el nuevo Windows. También desde el punto de vista del malware.

Sobre PandaLabs

PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- Desde **PandaLabs** se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.

- **PandaLabs** se encarga asimismo de llevar a cabo el análisis detallado de todos los tipos de malware, con la finalidad de mejorar la protección ofrecida a los clientes de Panda Security, así como para informar al público en general.

- Del mismo modo, **PandaLabs** mantiene un continuo estado de vigilancia, siguiendo muy de cerca las diferentes tendencias y evoluciones acontecidas en el campo del malware y la seguridad. Su objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.

- Se puede obtener información sobre las últimas amenazas descubiertas por en el blog de **PandaLabs** en: **http://pandalabs.pandasecurity.com/**