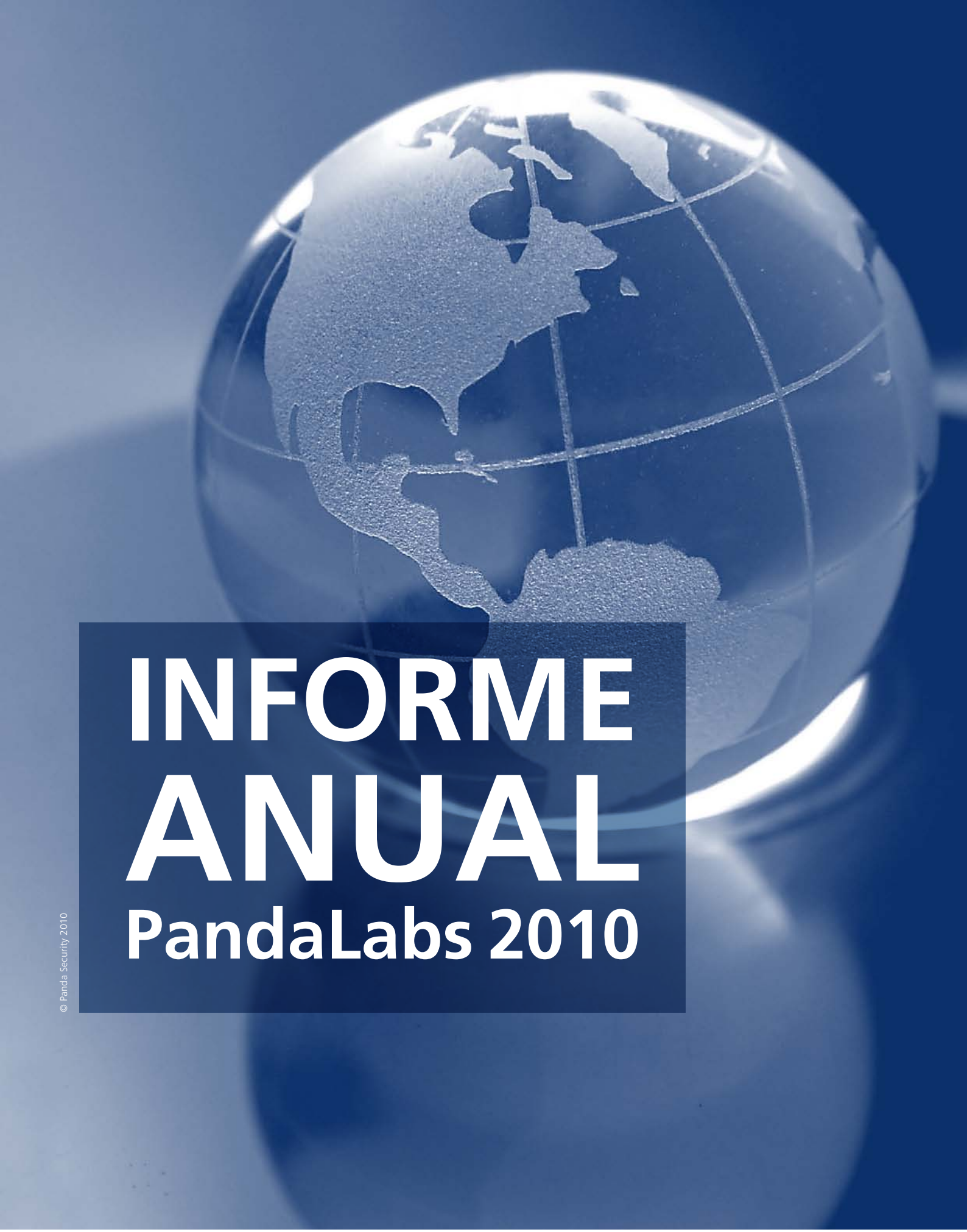


INFORME ANUAL
PandaLabs 2010

PANDA SECURITY

Índice

Introducción 03

Amenazas del 2010 04

Stuxnet, Irán y Centrales Nucleares 04

Ciberguerra 05

Aurora 06

Ciberdelincuencia 06

Ciberprotestas 07

Mariposa 09

Redes sociales 11

Rogueware 16

Cifras del 2010 19

Más BlackHat SEO 22

Windows 7 vs Mac OS X Snow Leopard 23

Seguridad en Móviles 25

El spam en 2010 26

Vulnerabilidades en 2010 28

Tendencias 2011 30

Conclusión 32

Sobre PandaLabs 33

Introducción

Tenemos que confesar que para los que llevamos muchos años en el mundo de la seguridad, 2010 ha sido un año más que interesante. Hemos tenido prácticamente de todo: distribuciones masivas de virus más clásicos y tradicionales, muchos más ataques BlackHat SEO, redes sociales utilizadas para distribución de malware, secuestros de funcionalidades de los sitios más populares, etc…

Pero sin lugar a dudas, creemos que 2010 ha sido un año clave para la seguridad y la privacidad: ahora, más que nunca, sentimos que realmente se está trabajando en pro de la mejora de la seguridad de empresas y particulares. ¿Por qué? Sencillo: ha habido varias detenciones durante el año (destacando, por supuesto, Operación Mariposa), fruto del trabajo de investigación de equipos policiales de muchos países. Aún a pesar de que todavía queda mucho para llegar a un punto donde todos nos sintamos seguros de verdad, al menos, estamos en el camino correcto.

Pero además, el que haya noticias relativas a seguridad que hayan visto la luz y la opinión pública conozca el trasfondo del cibercrimen es algo beneficioso en términos de concienciación y educación. Hace algunos años, cuando hablábamos de ciberguerra o ciberterrorismo, muchos periodistas –por no decir la gente ajena al mundillo de la seguridad- nos miraban como si estuviésemos contando el último estreno de Spielberg.

Ahora, al menos, es una realidad (aunque haya pasado a este status sólo porque lo hayan publicado los medios, no porque no existiera).

Además, este año hemos inaugurado la era del ciberactivismo. Sin duda, la coordinación internacional propulsada por Anonymous para lanzar ataques DDoS contra sociedades protectoras de derechos de autor, primero, y contra todo tipo de entidades en apoyo a Julian Assange, de Wikileaks, últimamente, parece haber hecho despertar la conciencia de comunidad virtual que defiende sus derechos y libertades.

También Mac parece haber despegado como objetivo de los ciberdelincuentes. Que, por cierto, siguen haciendo su agosto cosechando beneficios a costa de víctimas inocentes… Porque este año se han creado más de 20 millones de ejemplares de nuevo malware, y hemos llegado a registrar 60 millones de malware clasificados en Inteligencia Colectiva. Un panorama nada alentador… por lo menos, para no bajar la guardia.

Microsoft ha publicado 104 actualizaciones este año con relación con la seguridad, y Mac llevaba ya 175 en octubre. A esto tendremos que sumar el hecho de que parece que Android comienza también –al menos tímidamente- a ser el punto de mira de delincuentes. Así que… más malware; hecho de forma más ingeniosa; con más posibilidades de vectores de distribución y, por lo tanto, de infección; aprovechándome de multitud de vulnerabilidades; afectando a más plataformas… y… Mejor que te leas el informe completo que, este año, va muy cargadito. ¡Que lo disfrutes!

Este año ha sido especialmente intenso en lo que a amenazas se refiere, y muchos acontecimientos han agitado el mundo de la seguridad. El desmantelamiento de la Red Mariposa, el gusano "Here you Have" –ataque reivindicado por la resistencia iraquí-, el aprovechamiento de vulnerabilidades 0-Day, Stuxnet y el ataque a centrales nucleares (sistemas SCADA), el gusano Rainbow o OnMouseOver de Twitter, el secuestro del botón "Me Gusta" de Facebook, las amenazas de Android (como FakePlayer), el nacimiento del ciberactivismo como tal liderado por Anonymous, la filtración de Wikileaks… Un año en el que ha habido sucesos relacionados con la ciberseguridad de todos los colores, gustos y sabores… Sin duda, un presagio para un 2011 de lo más interesante…

Stuxnet, Irán y centrales nucleares

Éste es uno de los nombres propios de este año, sin duda alguna. En julio de este año se hizo público el descubrimiento de Stuxnet, un nuevo gusano. Uno de los miles que cada día aparecen, así que ¿por qué este es tan especial? A primera vista era un gusano que se propagaba a través de dispositivos USB, como muchos otros. Pero tenía algo que lo hacía especial: con sólo ver el contenido del USB, por ejemplo, usando el Explorador de Windows, el ordenador se infectaba. Esto lo conseguía a través de un exploit 0-Day implementado en el gusano que explotaba una vulnerabilidad hasta entonces desconocida en Windows. Por si no fuera suficiente, tenía más 0-Day incorporados, además de explotar alguna vulerabilidad ya conocida..

Para asegurarse el pasar desapercibido, instalaba en el sistema un driver que aseguraba su ocultación mediante técnicas rootkit, driver que habían conseguido firmar digitalmente mediante una firma legítima 'robada'. Pero no hacía nada en los ordenadores infectados, salvo seguir con su propagación. A no ser que tuvieras instalado un PLC (Programmable Logic Controller) fabricado por la empresa alemana Siemens. En caso afirmativo, utiliza otra vulnerabilidad desconocida, en este caso en el software controlador del PLC, para leer y escribir información en él.

Hasta aquí lo que es información, pero las especulaciones que han surgido a raíz de este incidente no han dejado de aparecer a lo largo de estos meses. La complejidad de Stuxnet implica que haya sido necesario un grupo de trabajo de varias personas altamente especialistas, además de una cantidad de fondos nada despreciables (hablamos de millones de dólares) en equipamiento para el equipo y la adquisición de los diferentes 0-Day en el mercado negro. Esto ha llevado a concluir que sólo puede estar participado por un estado. ¿China? ¿USA? Nadie lo sabe. Pero aún así, faltaba un ingrediente fundamental en toda intriga de espías: un objetivo. Y cuando un investigador alemán apuntó que el ratio de infección en Irán era inusualmente alto, y que ese tipo de controladores de Siemens se utilizan en centrales nucleares como la de Bushehr en Irán, se alimentó el rumor de que Israel estaba detrás de el ataque, ya que se encontraron referencias en Stuxnet que podían interpretarse como una firma del único país democrático de Oriente Medio.

FIG.01

PLANTA DE ENRIQUECIMIENTO DE URANIO DE NATANZ

Por otro lado, se ha publicado otro posible objetivo de Stuxnet, que es la planta de enriquecimiento de uranio de Natanz, ya que las centrifugadoras utilizan los controladores de Siemens, por lo que Stuxnet podría llegar a modificar, por ejemplo, la velocidad de centrifugado de la maquinaria.

Lo que sí sabemos es que efectivamente han conseguido infectar la planta nuclear de Bushehr, o al menos es lo que las autoridades iranís han **reconocido**. De hecho, en diciembre el mismo presidente de Irán, **Mahmoud Ahmadinejad**, reconoció cómo Stuxnet había afectado a sus instalaciones nucleares.

Y ésta, por méritos propios, podemos decir que se ha convertido en la noticia del año, y en el caso más espectacular de la historia de ciberguerra o ciberespionaje

Ciberguerra

Aparte del caso Stuxnet, otros hechos acercan más la realidad de ciberguerra. En enero, Corea del Sur **hacía público** que estaba montando un centro de comando destinado a luchar contra posibles ataques de Corea del Norte y China. En Estados Unidos **se hacía oficial** la creación del Ciber Comando en la Marina, como una de las ramas pertenecientes al Ciber Comando del ejército estadounidense anunciado meses antes.

Junto a estos elementos serios de lo que se podría llamar ciberguerra, o incluso mejor ciberdefensa, hay otros un poco más pintorescos, aunque se pueden englobar también aquí. Tal es el caso del gusano conocido como "Here you have", segunda variante de un gusano aparecido en agosto, y una de las características que tenía es que en el mensaje de correo que se enviaba aparecía como remitente "iraq_resistance" y parecía estar ligado al grupo terrorista "Brigadas de Tariq ibn Ziyad."

Tres días después de la aparición de esta variante, una persona que se identifica como el creador del gusano publicó un vídeo en Youtube, firmado por "IRAQ Resistance – Leader of Tarek Bin Ziad Group", y publicado por un usuario con el alias "iqziad", de 26 años y desde España, según los datos rellenados por el mismo ciberdelincuente en su perfil de YouTube.

Tāriq ibn Ziyād al-Layti (en árabe, طارق بن زياد, Tarik en la transcripción tradicional española, muerto en 720) fue un general bereber que lideró la invasión musulmana de la Península Ibérica en el siglo VIII, conquistando la Hispania visigoda, según la historiografía tradicionalmente admitida, basada en crónicas árabes de los siglos X y XI.

Según lo que cuenta el video, este gusano ha sido creado y distribuido para afectar principalmente a Estados Unidos por dos razones: para conmemorar los atentados del 11-S y reivindicar el respeto al Islam, haciendo referencia al intento de quema del Corán del pastor Terry Jones.

El vídeo muestra una imagen estática de Andalucía junto a una foto y un escudo, presumiblemente identificativo del propio grupo. Esta es la traducción al español de la locución del vídeo:

"Hola. Mi Nick es Iraq Resistance. Escuchar las razones que hay detrás del virus del 9 de septiembre que ha afectado a la NASA, Coca-Cola, Google y a muchos jugadores americanos. Lo que quiero decir que es los Estados Unidos no tienen derecho a invadir a nuestra gente y robar el petróleo bajo el nombre de armas nucleares. ¿Lo habéis visto? No hay evidencias de ningún proyecto. Es muy fácil matar y destruir. Segundo, sobre el Cristiano, Terry Jones. Lo que ha intentado hacer el mismo día en que este gusano se distribuyó tampoco es justo. Sé que no todos los Cristianos son iguales, y muchos periódicos han escrito que yo soy un hacker terrorista porque he hecho un virus informático, pero no que Mr. Terry Jones lo es. ¿Y no es él terrorista por haberse metido contra el comportamiento musulmán? Creo, América, venga ya! Sé justo. ¿Dónde está vuestra libertad, que debería acabar contigo??? Como dice tu gente educada y moderna. No sé si realmente hay otro y realmente no quiero "machacar" ordenadores y realmente no hay ninguno afectado como sabéis del informe. Podría "machacar" a todos los infectados, pero no lo haré y no uséis la palabra terrorista, por favor. Espero que la gente entienda que no soy una persona negativa. Gracias por publicarlo".

Pero volviendo a la parte más seria, hemos visto cómo el interés por este tipo de situaciones se convierte en algo real, donde gobiernos de diferentes países ven que es una necesidad estar preparado ante ataques de este tipo. Por ejemplo, el primer ministro británico, David Cameron, **anunció** *un fondo de 650 millones de libras para ciberseguridad. La preocupación es tal que en Europa se lanzaron* **una serie de pruebas**, *basadas en lanzar ataques falsos a ciertas instituciones europeas.*

Aurora

Apenas comenzábamos 2010 cuando nos sorprendía la noticia, dada a conocer por Google, de que un sofisticado y coordinado ataque bautizado "Operación Aurora" tenía como objetivo diferentes y grandes compañías multinacionales. Los hackers aprovechaban una vulnerabilidad de Internet explorer para instalar un troyano de manera silenciosa en los ordenadores de los usuarios y conseguir, de esta manera, tener acceso remoto a toda su información personal.

Dicha vulnerabilidad Zero Day afectaba a las tres versiones del navegador Internet Explorer (6, 7 y 8) en sistemas operativos Windows 2000 SP4, WXP, 2003, Vista y Windows 7. Este ataque fue bautizado Aurora después de que los investigadores detectaran esta cadena de texto en el código fuente de uno de los troyanos involucrados en el ataque. Existen dos hipótesis sobre el objetivo final que querían lograr los hackers: una versa sobre la intencionalidad de robar información de propiedad intelectual a grandes compañías y la otra, más simplista, apunta al robo de información de cuentas de Gmail de supuestos y conocidos activistas de derechos humanos en China.

Varios empleados de Google de diferentes países recibieron correos electrónicos extraños que les invitaban a acceder a una página de Internet a través de un link. Lo que pasó después se ha denominado como uno de los ciberataques más sofisticados hasta ahora registrados. Dicho ataque afectó a más de 30 compañías multinacionales. Quizá lo más curioso del caso, según apuntan algunas fuentes de información, es que las personas que recibieron el e-mail –es decir, las "víctimas"–, no eran aleatorias, sino que se trataba de directivos y altos cargos que supuestamente tenían permisos de acceso a diferentes aplicaciones con privilegios. Es lo que llamamos "ataques dirigidos", frente a los ataques masivos o indiscriminados, donde no se selecciona el receptor o potencial víctima.

El troyano realizaba conexiones cifradas contra servidores alojados en Texas y en Taiwán. La utilización de DNS dinámicas era una de las principales características del ataque, lo que ha dificultado su rastreo. Sin embargo, se identificaron algunos servidores que alojaban dominios registrados por el servicio Peng Yong 3322.org en China, según diferentes análisis técnicos publicados al respecto.

Google apuntó a China como responsable del ataque, dado que uno de los servidores origen estaba en ese país. Las autoridades del Gobierno chino negaron tener algo que ver con el incidente internacional. Pasará algún tiempo hasta que realmente se descubra todo lo relacionado con Operación Aurora. Y mientras sigan existiendo vulnerabilidades 0-day y los usuarios continúen siendo víctimas de técnicas de ingeniería social, seguiremos estando expuestos a este tipo de ataques.

Ciberdelincuencia

Por mucho que hablemos de ciberguerra y ciberespionaje, no podemos perder de vista la ciberdelincuencia, que va en busca del dinero de los usuarios de Internet, sean empresas o personas. En enero, el FBI comenzó a investigar el **robo de más de 3 millones de dólares** en un colegio de Nueva York. En febrero, se descubrió que se habían robado más de 3 millones de euros a través de un **ataque de phishing**. Casos como estos **suceden todos los días**, no es algo excepcional. A lo largo de este año hemos visto como pequeñas empresas se **iban a pique** debido a robos de este tipo, o cómo grupos aún sin identificar han estado operando durante años, robando pequeñas cantidades de cientos de miles de usuarios, llevándose en total **10 millones de dólares**.

Los delincuentes también roban información con la que obtener dinero. Una forma de lucha es tratar de evitar que se trafique con esta información, algo realmente complejo, más aún cuando descubrimos que hay gobiernos que son los primeros en comprar información robada, **como el caso del gobierno alemán**.

Aunque la forma de atajar el problema de raíz es acabar con cualquiera que infrinja la ley, algo fácil de decir. Siempre que pensamos en estos delincuentes involuntariamente le aplicamos el típico estereotipo de jovencito que está pegado al ordenador todo el día, pero es algo que deberíamos borrar de nuetra mente. Internet es simplemente una herramienta de la que cualquiera con malas intenciones puede abusar. Como ejemplo tenemos al ciclista estadounidense Floyd Landis, que fue acusado por un juzgado francés, e incluso se lanzó una orden de arresto por haber entrado ilegalmente en uno de los ordenadores del laboratorio de la **agencia antidopaje francesa**.

Algo bueno a destacar este año es que parece que la policía rusa está empezando a tomarse en serio este tipo de crímenes y ha comenzado a realizar arrestos de ciudadanos rusos envueltos en este tipo de actividades. Como ejemplo tenemos la investigación abierta a **Igor Gusev** o el arresto de 10 miembros de una banda dedicada al **chantaje**.

Ciberprotestas

Sin duda, en 2010 hemos visto un movimiento que marcará un antes y un después en la relación entre Internet y la sociedad: las ciberprotestas. Este fenómeno, protagonizado por Anonymous, no era algo completamente desconocido pero ha sido en 2010 cuando se ha "universalizado".

Anonymous es un conjunto de usuarios, sin una jerarquía como las de cualquier grupo tradicional, formado por miles de usuarios de todo el mundo y unidos en la defensa de una causa. Si bien el grupo de Anonymous tiene ya unos años, comenzaron a hacerse conocidos con su participación, junto con The Pirate Bay, en el apoyo a las protestas en Irán por las fraudulentas elecciones que tuvieron lugar en 2009 y que supuestamente ganó Mahmoud Ahmadinejad.

FIG.02

PÁGINA CREADA POR ANONYMOUS Y THE PIRATE BAY EN APOYO A LA POBLACIÓN IRANÍ.

Pero ha sido en la 2ª mitad de 2010 cuando el grupo ha llegado a su máxima fama. Todo empezó cuando fue revelado que una serie de empresas de la industria cinematográfica habían contratado los servicios de una empresa india que se dedicaba a lanzar ataques de denegación de servicio (Dos) contra páginas web de compartición de archivos que no hacían caso a sus requerimientos de quitar ciertos enlaces de sus sites.

Anonymous no tardó en organizarse para lanzar un ataque contra la web de la empresa india, si bien alguien se les adelantó, por lo que decidieron ir a por la industria cinematográfica y discográfica, así como contra asociaciones anti-piratería ligadas a éstas. El funcionamiento fue similar al de cualquier protesta en el mundo real, pero aprovechando las ventajas de Internet. En primer lugar comenzaron a repartir panfletos como los siguientes para reclutar voluntarios y coordinar la protesta:

FIG.03

PROTESTA ONLINE CONTRA LA RIAA.

La acción fue todo un éxito, por lo que fueron actualizando objetivos, el mismo tipo de entidades pero en distintos países, como Reino Unido o España. Tras estos ataques, realizamos una entrevista a sus miembros para tratar de entender sus motivaciones:

P: ¿Qué es Anonymous?

R: *Simplemente es una descripción de lo que somos. Anonymous no es una organización con una jerarquía y líderes. Nos consideramos anarquistas. Estamos formados por gente de todo tipo. En resumen, somos un grupo de gente tremendamente motivada para hacer todo lo que esté en nuestra mano para responder ante aquello que consideramos moralmente cuestionable.*

Luchamos contra el lobby anti-piratería. La piratería supone el siguiente paso en la revolución cultural de la información compartida

P: ¿Cual es vuestra misión actual?

R: *Luchar contra el lobby anti-piratería. Recientemente ha habido un aumento enorme de los ataques a la libertad personal en Internet promovidos por este grupo. Fíjate en la Ley de Economía Digital del Reino Unido y la normativa europea de los "tres avisos". Ambas iniciativas amenazan con cerrar las conexiones a Internet de los usuarios basándose en acusaciones de la industria musical y cinematográfica. En Estados Unidos se acaba de presentar un proyecto de ley que podría permitirle al gobierno norteamericano obligar a registradores de dominio de nivel superior como ICANN y Nominet a cerrar sitios Web sin NINGÚN tipo de juicio justo. ¡Se te declara culpable antes de demostrar si lo eres o no! Nuestras tácticas se inspiran en las de la gente que nos ha provocado: AiPlex Software. Hace unas cuantas semanas admitieron haber atacado sitios de intercambio de ficheros mediante ataques de denegación de servicio.*

Recomendamos leer nuestra declaración oficial ***aquí****.*

P: ¿Estáis a favor de la piratería?

R: *Sí. Se trata del siguiente paso en la revolución cultural de la información compartida. Imagínatelo como el comienzo de una nueva era de la información; el inicio de una auténtica "igualdad de oportunidades", en la que no importa la riqueza o capacidad de cada uno. Yo mismo nunca hubiera llegado a dónde estoy ahora mismo sin los libros que he pirateado. ¡No me los podía permitir!*

P: ¿Qué sitios habéis atacado?

R: *Las Asociaciones Americanas de la Industria Musical y Cinematográfica [MPAA y RIAA], la Industria Fonográfica Británica [BPI], la Federación Australiana contra el Robo del Derecho de Autor [AFACT] , la Asociación Holandesa para la Protección de los Derechos de la Industria del Entretenimiento [BREIN], ACS:Law, Aiplex, Websheriff, y Dglegal.*

P: Vuestro póster original decía que se utilizarían "redes de bots" en el ataque. ¿Alguno de vosotros se beneficia económicamente de ciber-delitos?

R: *Eso depende de si empleas la definición de 'criminal informático' que utiliza el lobby anti-piratería. Para serte claro no aprobamos la obtención de beneficios económicos a partir de redes de bots o de malware; pero la gran mayoría de lo que constituye un ciber-delito es algo tan sencillo como descargarte tu canción favorita en lugar de pagar un precio ridículo por la misma (un precio del que el artista sólo se queda con un porcentaje mínimo).*

P: ¿Qué relación tenéis con 4chan? ¿Sois todos miembros activos?

R: *Algunos de nosotros frecuentamos 4chan, pero no tenemos ningún tipo de afiliación con ningún foro o sitio Web. Sólo lo utilizamos para comunicarnos.*

P: ¿Cuánto tiempo va a durar el ataque?

R: *No hay un plazo fijado. Seguiremos con él hasta que se nos pase el enfado.*

P: ¿Estáis dispuestos a ir a la cárcel por esta causa?

R: *Sí, pero hemos tomado todas las medidas necesarias para asegurarnos de que nuestro anonimato permanece intacto. Es más, ¿por qué no se le hace esa pregunta a la gente que contrató a Aiplex para atacarnos?*

P: Si pudierais resolver esta situación, ¿qué os gustaría que hicieran los organismos audiovisuales mundiales?

R: *Personalmente, me gustaría que desaparecieran de una puta vez. Que eliminasen todas esas leyes brutales que han promovido. Que tratasen a las personas como PERSONAS en vez de como criminales. Tienen que cambiar esa concepción tan anticuada y tradicional que tienen de la que las leyes sobre los derechos de propiedad intelectual sólo pueden ser aplicadas por empresas ricas y poderosas. Eso ya no resulta válido en la era de Internet, la Era de la Información.*

Los artistas controlados por la industria audiovisual tienen muy poca voz sobre los contenidos que producen y sólo obtienen un porcentaje mínimo de los beneficios. Esto es evidente, como lo demuestra el hecho de que muchos artistas se han apartado del control de la industria. Ahí están los ejemplos de Nine Inch Nails y Radiohead. Los dos grupos han aceptado la piratería y aún así siguen obteniendo importantes beneficios.

P: ¿Sois conscientes de que estos ataques son ilegales en muchos países y de que vuestro grupo podría acarrear problemas legales a gente inocente que apoya vuestra causa?
R: *Creo que la mayor parte de gente/participantes es consciente de ese riesgo. En un mundo en el que se ignora nuestra voz, creemos que no nos queda otra opción que la acción directa.*

P: Algunas personas ven esto como el futuro de las protestas. ¿Prevés que pueda haber protestas como ésta en el fututo por otras causas?
R: *Seguramente. En cuanto a las protestas, espero que el futuro de las protestas sea la ACCIÓN. No el andar en círculos con pancartas inútiles que todo el mundo ignora.*

Las acciones de Anonymous siguieron, pero en diciembre hubo un cambio que hizo que aumentara la popularidad del grupo. Cuando Wikileaks comenzó a recibir ataques debido a la presión del gobierno estadounidense sobre diferentes empresas (suspensión de las cuentas de Wikileaks mediante las que recibían donativos en Paypal, Visa, Mastercard, expulsión del servicio de Amazon donde tenían alojada la web, etc. Anonymous hizo público que se alineaba con Wikileaks y que respondería con ataques DDoS a todo aquel que fuera contra Julian Assange, autor de Wikileaks.

Así comenzaron toda una serie de ataques contra las páginas web de PayPal, Mastercard, Visa, Postfinance, etc. Al mismo tiempo hubo contraataques (sin conocerse a sus autores) contra Anonymous. Se arrestó a un adolescente de 16 años en Holanda, tras lo cual se lanzaron varios ataques contra webs relacionadas con el arresto (fiscalía, policía, etc.). Días después se arrestó a un segundo joven, de 19 años, por estos ataques.

FIG.04

MENSAJE EN TWITTER ANUNCIANDO EL ATAQUE A MASTERCARD.COM

En algunos países existe un vacío legal en cuanto a participar en ataques DDoS (Distributed Denial of Service), pero algunos como Holanda o Reino Unido lo incluyen en su legislación incluso con penas de cárcel de hasta 6 años en Holanda y de 2 años en el Reino Unido.

Muchos medios han definido todos estos acontecimientos como **ciberguerra**, algo inapropiado y lejos de la realidad. Estos acontecimientos pueden ser catalogados como **ciberprotesta**s o **ciberactivismo**, y dado el éxito han tenido a lo largo de la segunda mitad de 2010, es algo que tendrá mucho protagonismo el próximo año.

Mariposa

Un 3 de marzo de 2010, a las 10:00 de la mañana, anunciábamos… "***Panda Security y Defence Intelligence coordinan el cierre de una importante red de bots con autoridades policiales internacionales".***

Según las empresas de seguridad informática Defence Intelligence y Panda Security, la red de bots Mariposa, diseñada para robar información confidencial, ha sido cerrada por las autoridades y ha dejado de estar en poder de tres presuntos delincuentes informáticos acusados de controlar la red. Los datos robados incluyen información de cuentas bancarias, tarjetas de crédito, nombres de usuario y contraseñas de una red global de unos 12 millones 700.000 equipos comprometidos pertenecientes a usuarios domésticos, empresas, agencias gubernamentales, y universidades de más de 190 países. La red de botnets fue desactivada el 23 de diciembre de 2009 gracias al esfuerzo conjunto de diversos expertos de seguridad y agencias y cuerpos de seguridad, incluyendo Defence Intelligence, Panda Security, el FBI y la Guardia Civil española.

Con casi 13 millones de ordenadores comprometidos, se estima que Mariposa es una de las mayores redes de bots de la historia. Christopher Davis, CEO de Defence Intelligence, la primera empresa en descubrir esta red de bots, explica: "Sería más sencillo para mí dar una lista de las empresas del índice Fortune 1000 que no se han visto afectadas por esta amenaza, que dar el enorme listado de las que sí lo han sido".

Pero, hasta llegar a este anuncio, hubo mucho trabajo los meses previos… Así fue…

El making off

En Mayo de 2009, Defence Intelligence hizo público el descubrimiento de una nueva red de bots, bautizada como "Mariposa". Además de la información facilitada en su momento, se empezó un trabajo que ha durado meses, cuyo objetivo era acabar con una red criminal que estaba detrás de lo que iba a convertirse en una de las mayores redes de bots de la historia.

Lo primero que se hizo fue crear el Mariposa Working Group (MWG), del que forman parte Defence Intelligence, el Georgia Institute of Technology y Panda Security; junto a expertos de seguridad y agencias y cuerpos de seguridad de diferentes países, la idea era aunar fuerzas para tratar de eliminar la botnet y llevar a los criminales ante la justicia.

Una vez recogida toda la información, lo más importante era planificar cómo quitar el control de la red a los criminales que estaban detrás, así como poder identificarlos. Así que localizados los diferentes paneles de control desde los que mandaban instrucciones a la red, pudimos ver qué tipo de actividades llevaban a cabo. Principalmente se dedicaban a alquilar partes de la red de bots a otros criminales, robo de credenciales de los equipos infectados, cambio de resultados a los usuarios cuando utilizaban motores de búsqueda (Google, etc.), y mostrar popups de publicidad.

La finalidad, como podéis ver, era puramente económica. El grupo de delincuentes detrás de Mariposa se hacía llamar DDP Team (Días de Pesadilla Team), información que logramos más tarde cuando debido a un error fatal pudimos descubrir a uno de los cabecillas de la banda.

Localizar a los criminales se volvió realmente complicado, ya que siempre se conectaban a los servidores de control de Mariposa a través de servicios anónimos de VPN (Virtual Private Network, Red Privada Virtual), lo que imposibilitaba localizar la dirección IP real que tenían, la mejor pista que nos podría llevar hasta ellos.

El día 23 de Diciembre de 2009, en una operación coordinada a nivel mundial, el Mariposa Working Group consiguió cortar el control de Mariposa al grupo de delincuentes. El líder de la banda, alias Netkairo, se puso nervioso e intentó entonces a toda costa recuperar el control de la red de bots. Como he comentado anteriormente, para conectarse a los servidores de control de Mariposa usaba servicios anónimos de VPN que impedían localizar su ubicación real, pero en una de las ocasiones en las que trataba de recuperar el control de la red de bots cometió un error fatal: se conectó directamente desde el ordenador de su casa y olvidó utilizar la VPN.

Netkairo finalmente consiguió recuperar el control de Mariposa, y a continuación lanzó un ataque de denegación de servicio contra Defence Intelligence utilizando todos los bots que tenía a su disposición. Este ataque afectó seriamente a un gran Proveedor de Acceso a Internet (ISP) y dejó sin conectividad durante varias horas a multitud de clientes, entre los que se encontraban centros universitarios y administrativos de Canadá.

Finalmente el Mariposa Working Group consiguió que el DDP Team perdiera de nuevo el acceso a Mariposa. Cambiamos la configuración DNS de los servidores a los que se conectaban los bots, de tal forma que pudimos en ese momento ver la cantidad de bots que estaban reportando. El resultado nos dejó helados, cuando vimos que más de 12 millones de direcciones IP se estaban conectando y enviando información a los servidores de control, convirtiendo a Mariposa en una de las redes de bots más grandes de la historia.

El 3 de Febrero de 2010, la Guardia Civil procedió a la detención de Netkairo. Se trataba de F.C.R., español, de 31 años de edad. Tras su detención, las fuerzas de seguridad incautaron material informático, cuyo análisis forense llevó a la policía a localizar a otros 2 componentes de la banda, también españoles: J.P.R., de 30 años, alias "jonyloleante", y J.B.R., de 25 años, alias "ostiator". Ambos fueron arrestados el 24 de Febrero de 2010.

Las víctimas de Mariposa están repartidas por todo el mundo, hay equipos comprometidos pertenecientes a usuarios domésticos, empresas, agencias gubernamentales y universidades de más de 190 países.

¿Quién Estaba Detrás de Mariposa?
El pasado 3 de Febrero de 2010, la Guardia Civil procedió a la detención de Netkairo. Se trataba de F.C.R., español, de 31 años de edad. Tras su detención, las fuerzas de seguridad incautaron material informático, cuyo análisis forense llevó a la policía a localizar a otros 2 componentes de la banda, también españoles: J.P.R., de 30 años, alias "jonyloleante", y J.B.R., de 25 años, alias "ostiator". Ambos fueron arrestados el 24 de Febrero de 2010.

Dada la trascendencia internacional de la operación, así como la repercusión mediática de la noticia, nos podría parecer que nos encontramos ante grandes genios informáticos.

Analizando sus perfiles profesionales, llegamos a la conclusión de que, al igual que muchos jóvenes actuales, la informática se plantea como un hobby y, por lo tanto, son autodidactas. Probablemente, en su camino de investigación, darían inocentemente con la forma de conseguir dinero rápido de manera fácil.

Y ahora…
Cuando casi nos habíamos olvidado del caso Mariposa, este verano se anunciaron varios arrestos en Eslovenia. La gente se preguntaba si esto estaba realmente relacionado con el caso Mariposa, ya que los tipos detrás de Mariposa eran españoles y los arrestados son eslovenos.

El pasado marzo, cuando se hizo pública la historia, hablamos sobre los españoles arrestados, y que ellos habían comprado el bot. Probablemente os disteis cuenta de que no mencionamos nada sobre el vendedor del bot. Esto fue no porque no supiéramos quién estaba detrás, sino porque el FBI nos pidió amablemente que no hiciéramos pública la información, ya que estaban persiguiendo a Iserdo.

¿Quién es Iserdo? Es el apodo de un esloveno que ha sido el desarrollador principal del Butterfly Bot, y el que estaba en contacto con Netkairo. Asimismo, fue el que le vendió a Netkairo el bot con el que montó la red Mariposa.

Según Netkairo, él y Ostiator le dieron a Iserdo un "99%" de la idea para desarrollar el bot. Esto es muy poco probable que sea cierto, recordad además que estábamos teniendo esa conversación porque Netkairo quería que lo contratáramos para trabajar en el laboratorio (sic).

Tras los arrestos en Eslovenia, la policía dio una rueda de prensa donde revelaron información sobre el caso. Habían realizado registros en siete viviendas, donde se incautaron 75 dispositivos (ordenadores, discos duros, memorias, etc.). Confirmaron que habían detenido a 2 sospechosos, de 23 y 24 años. Después de 48 horas fueron puestos en libertad, pero la investigación continúa en curso.

La policía confirmó que uno de los arrestados es sospechoso de ser el autor del malware (conocido como ButterflyBot) con el que se creó la red de bots Mariposa. Además, también confirmaron que están investigando 2 delitos: la creación de herramientas que posibilitan crímenes informáticos y el lavado de dinero.

Ojalá en el próximo informe anual podamos seguir hablando de Mariposa, pero podamos confirmar penas y condenas acordes con el crimen que estos cibercriminales han cometido.

2010: el año de las redes sociales

No es nuevo, no nos sorprende y esta tendencia de usar las más famosas redes sociales para diferentes fines cibercriminales seguirá llenando las páginas de estos informes durante 2011 y en adelante… Pero éste es un resumen de qué ha pasado en 2010, y la verdad es que ha habido bastante noticias relacionadas con redes sociales y problemas de seguridad… y casi más relacionadas con problemas de privacidad.

Básicamente, las redes sociales cuentan con millones de usuarios que a diario, y muchas horas al día, se conectan, interactúan, intercambian, comentan y, en ocasiones, también las usan como trabajo. Y aquí es donde viene el peligro: este excelente caldo de cultivo ha hecho que las miradas de los cibercriminales se centren en comunidades donde encuentran un buen número de potenciales víctimas. Para empezar, echemos primero un vistazo a algunos datos…

Primer Informe Anual sobre el Indice de Riesgo en Redes Sociales

Según datos extraídos del primer informe anual sobre el **Indice de Riesgo** de las redes sociales para PYMEs, el uso de redes sociales durante horario de trabajo es una práctica habitual (el 77% de los empleados lo hacen), y consecuentemente, el 33% dice que se ha infectado el parque corporativo por malware que se ha distribuido por estas comunidades.

Según el estudio, las mayores preocupaciones de las PYMEs respecto a las redes sociales incluyen la privacidad y las pérdidas económicas (74%), infecciones de malware (69%), pérdida de productividad de los empleados (60%) y las relacionadas con la reputación de la empresa (50%), seguida de los problemas del rendimiento y uso de la red (29%).

Sin embargo, esta preocupación no impide a las PYMEs la utilización de los beneficios de las redes sociales ya que un 78% de los encuestados reportan que utilizan estas herramientas para apoyar la investigación y la inteligencia competitiva, mejorar su servicio de soporte al cliente, implementar las relaciones públicas y las iniciativas de marketing y generar beneficios directos. Facebook es la herramienta social más popular utilizada por las PYMEs: 69% de las empresas tienen cuentas activas en este sitio, seguido por Twitter (44%), YouTube (32%) y LinkedIn (23%).

FIG.05

GRÁFICA DE RESULTADOS DEL USO DE LAS HERRAMIENTAS SOCIALES

Facebook es mencionado como el principal culpable para las compañías que han experimentado infecciones de malware (71,6%) y violaciones de privacidad (73,2%). YouTube ocupa el segundo lugar en cuanto a infecciones (41,2%), mientras que Twitter contribuyó a una cantidad significativa de violaciones de privacidad (51%). Para las compañías que han reportado pérdidas económicas debido a violaciones de privacidad por parte de los empleados, Facebook, fue una vez más el sitio más mencionado como el sitio social en el que se originaron las pérdidas (62%), seguido de Twitter (38%), YouTube (24%) y LinkedIn (11%).

Millones de usuarios= millones de oportunidades para conseguir víctimas

Creemos que este año hemos visto prácticamente de todo –en cuanto a seguridad se refiere- a través de redes sociales… Uno de los principales objetivos de los ciberdelincuentes ha sido el robo de identidad: haciéndose pasar por usuarios conocidos es más fácil la distribución de contenidos con ganchos que consigan víctimas. La técnica más comúnmente utilizada para robar la identidad ha sido, este año, la siguiente:

Paso 1: el gancho

El gancho viene, normalmente, desde el perfil de un amigo que ya ha sido hackeado. El usuario recibe un mensaje (que parece lícito y auténtico) indicando que es necesario pinchar en un enlace para algo. En la mayoría de los casos, este mensaje es del tipo "vídeo impactante" o "apareces en este video", y normalmente va personalizado con el nombre del usuario.
Un ejemplo:

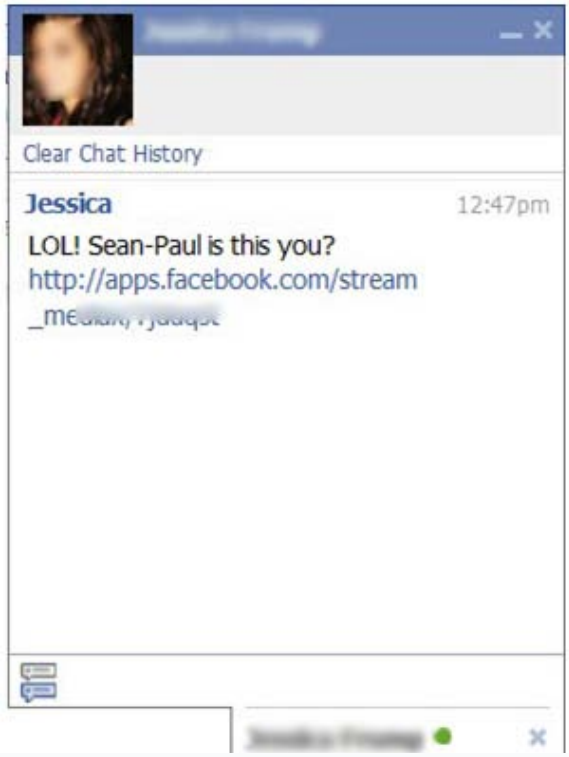


FIG.06

MENSAJE ES DEL TIPO "VÍDEO IMPACTANTE" O "APARECES EN ESTE VIDEO

Paso 2: Intento de Phishing

Ahora que los cibercriminales han atraído la atención del usuario, necesitan su nombre de usuario y contraseña para iniciar la siguiente fase del ataque. El enlace de la aplicación en la que han hecho click parece exactamente igual que la página de entrada de Facebook, pero en realidad es una copia alojada en otra dirección web:

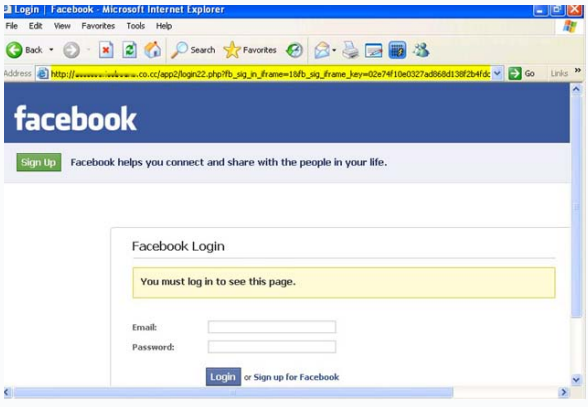


FIG.07

INTENTO DE PHISHING

Paso 3: Obtener acceso total

Ahora que el usuario ha pinchado en el enlace y ha suministrado sus datos de acceso, le será requerido el conceder a la aplicación maliciosa pleno acceso a su información personal, así como derechos para publicar información a través de su perfil. Esto les asegura que podrán difundir este ataque entre todos los amigos y familiares del usuario.

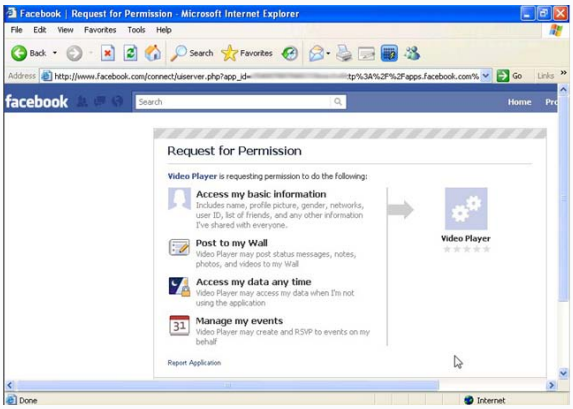


FIG.08

SOLICITUD DE ACCESO TOTAL A LA INFORMACIÓN PERSONAL

Después de obtener el permiso, el ataque se dirigirá a los contactos de la víctima y comenzará de nuevo el proceso con nuevos usuarios, como en el siguiente ejemplo:

FIG.09

CAPTACIÓN DE NUEVOS USUARIOS

Me gusta!

Y hablando de Facebook. Otra técnica ampliamente utilizada este año la del secuestro de la opción "Me gusta" de la popular red social Facebook. Simplemente navegando a través de páginas web que contienen el botón de "Me gusta" de Facebook, o a través de los muros o del sistema de mensajería interna de la red social –y siempre y cuando se esté logueado en el sistema-, se intenta atraer la atención de los usuarios con asuntos llamativos relacionados con juegos, películas, asuntos sexuales, etc.

Cuando el usuario hace click sobre el enlace, automáticamente es derivado a una página que contiene imágenes y vídeos sobre la temática ofrecida y al visitarla aparece en el perfil del usuario la opción "Me gusta" haciendo referencia a dicha página, con un texto no controlado por el usuario.

Esta técnica, conocida como clickjacking, se genera con una sencilla aplicación que lanza una acción javascript. Para el usuario no tiene mayor consecuencia que el hecho de no haber elegido voluntariamente la página como parte de su historial de gustos de Facebook. El verdadero negocio lo encontramos tras el sistema de pago por click, que suma y contabiliza con cada visita generando beneficios para los afiliados, y en que en cada una de estas páginas, el usuario se encuentra todo tipo de test por los que tiene que pagar si quiere realizarlos.

Y hablando de secuestros, y muy intrínsecamente relacionado con los problemas de seguridad y privacidad en redes sociales, en mayo descubríamos una red de venta de bots especializados en redes sociales y sistemas de correo gratuitos. La página, publicada abiertamente en Internet, contenía un extenso catálogo de venta de programas focalizados en redes sociales y servicios de correo gratuitos, entre ellas Twitter, Facebook, Hi5, MySpace, MyYearBook, YouTube, Tuenti, Gmail, Yahoo, etc.

FIG.10

RED DE VENTA DE BOTS ESPECIALIZADOS

En cada uno explica la finalidad para la que ha sido desarrollado el bot: para crear cuentas masivamente en las redes sociales; robo de identidades y apropiación de amigos, followers o contactos; envío de mensajes automáticos, etc. Según dicen en la página: "el bot recoge información de las identidades y nombres de los amigos y envía, de forma automática, solicitudes de amistad, mensajes con el contenido que se quiera o comentarios".

El precio de cada ejemplar de bot varía desde los 95$ para el más barato y 225$, el más caro. Ofrecen la compra de todo el catálogo por 4.500$, y garantizan que nunca serán detectados por ningún tipo de solución de seguridad, que están desarrollados para cambiar aleatoriamente los referentes, agentes o cabeceras cuantas veces sean necesarias para evitar su bloqueo. Además, eluden los mecanismos de seguridad CAPTCHA que incorporan muchos sitios web, por lo que el comprador sólo tiene que parametrizar el bot y dejar que éste actúe sólo. Finalmente, garantizan las actualizaciones del bot de por vida.

También los falsos antivirus campan a sus anchas…
A principio de año, alertábamos también de la distribución masiva entre usuarios de Facebook de una falsa alerta de virus. En realidad, se trata de un engaño más para conseguir infectarles con falsos antivirus.

La alerta llegaba por correo electrónico, y los usuarios estaban reenviándola o publicándola en sus muros, distribuyendo aún más el hoax. El texto que muestra es el siguiente:

> ALERT — Has your facebook been running slow lately? Go to "Settings" and select "application settings", change the dropdown box to "added to profile". If you see one in there called "un named app" delete it… Its an internal spybot. Pass it on. about a minute ago….i checked and it was on mine.

No lleva asociado ningún link, pero si un usuario hace una búsqueda en Internet para ampliar la información, encontramos numerosos sitios web que son falsos y que realmente, al hacer click y visitar la web, descargan en el servidores.

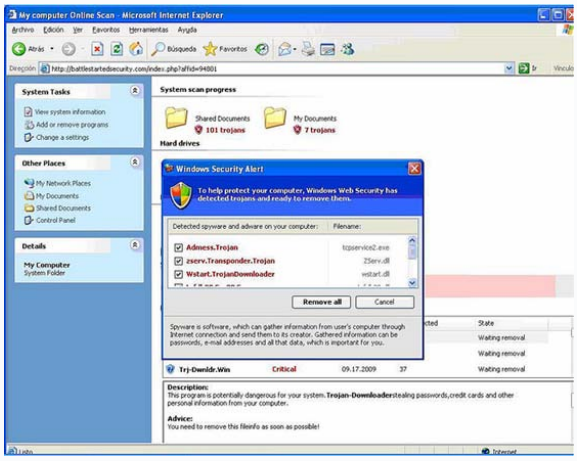


FIG.11
DESCARGA DE FALSO ANTIVIRUS

Sí, también para Mac
También hemos visto este año cómo uno de los troyanos más famosos, Koobface, se volvía a distribuir por las más conocidas redes sociales. Pero este año, intentaba alcanzar, específicamente, a los usuarios de Mac. Con el gancho de ver un vídeo, intentaba descargar al usuario unos códecs de Java, maliciosos, por supuesto. Si el usuario permitía su descarga, se instalaba en el ordenador y, además, intentaba bajarse diferentes ficheros de varios

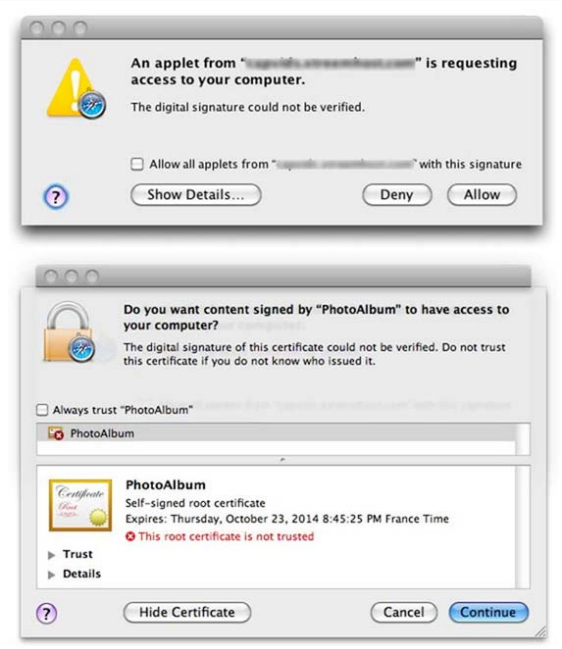


FIG.12
TROYANOS TAMBIÉN PARA MAC

Y hablando sobre Koobface… también este año el equipo de seguridad de Facebook parecía que estaba cerrando el cerco sobre los autores de esta familia de troyanos que, según estimaciones del propio personal de la red social, podrían estar ingresando la nada desdeñable cifra de 35.000$ semanales (engañando a los usuarios, por supuesto) o, lo que es lo mismo, 1,8 millones de dólares por año… Viendo éstos, y otros datos que manejamos, me imagino a más de un cibercriminal repitiendo el título de uno de mis discos favoritos de Supertramp: "Crisis? What Crisis?".

Rogueware

2010 ha sido, sin duda, el año de los falsos antivirus. Y no nos extraña: por detrás hay un negocio tan sencillo y prolífico en cuanto a beneficios, que resulta extremadamente rentable perder un rato diseñando un falso antivirus y una falsa tienda web, porque con el tiempo, las víctimas van haciendo el resto sumando euros al saldo de estos ciberdelincuentes.

En 2010 ha aparecido el 40% del total de ejemplares de falsos antivirus. O lo que es lo mismo, desde que apareció este nuevo tipo de amenazas, hace cuatro años, en PandaLabs hemos clasificado 5.651.786 ejemplares únicos y diferentes de falsos antivirus: de este total, 2.285.629 han aparecido desde enero a noviembre de 2010.

Si analizamos el total de ejemplares clasificados de este tipo de amenaza informática con respecto al total de nuestra base de datos de Inteligencia Colectiva (el sistema automático que detecta, analiza y clasifica el 99,4% de las 63.000 nuevas amenazas que aparecen diariamente), el 11,6% son falsos antivirus. Y todo ello, teniendo en consideración que la base de datos del total de malware contiene los ejemplares detectados a lo largo de los 21 años de historia de la compañía, y que los roguewares aparecieron hace sólo cuatro.

La sofisticación de sus diseños, el realismo de los mensajes utilizados y el poderoso gancho social que supone el pensar que la salud del PC está seriamente amenazada sigue funcionando, ya que son, cada vez más, los usuarios que siguen cayendo en este fraude. En lo que va de año, el 46,8% de los ordenadores mundiales están infectados con todo tipo de malware: el 5,40% lo están con este tipo de programas.

Existen miles de familias y ejemplares diferentes, pero el top de falsos antivirus que están causando más infecciones (o que engañan a más gente) son los siguientes:

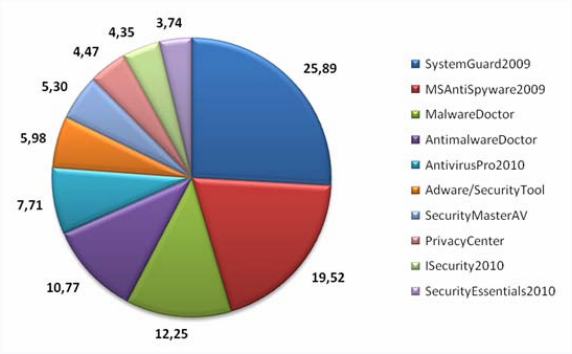


FIG.13

TOP 10 DE FALSOS ANTIVIRUS POR RATIO DE INFECCIÓN

El conseguir una víctima más de un falso antivirus significa para un hacker varias ventajas: no sólo le permite embolsarse el importe de la compra de la supuesta licencia del programa de seguridad que va a arreglar todos sus problemas –y que nunca recibe-, sino que se queda con los datos de su tarjeta de crédito que posteriormente puede vender en el mercado negro o utilizar para extraer dinero, hacer compras online, etc.

FIG.14

EL FALSO ANTIVIRUS QUE MÁS INFECCIONES HA CAUSADO EN 2010 ES SYSTEMGUARD2009

Según los cálculos que PandaLabs hizo en su monográfico **"El negocio de los Falsos Antivirus"**, sus autores están ingresando más de 34 millones de dólares al mes o 415 millones de dólares al año.

Una novedad a destacar este año ha sido la aparición de falsos antivirus que utilizan el SMS como vía para obtener ingresos de forma fraudulenta. No deja de ser un ejemplo más de cómo convergen las tecnologías y cómo las combinan los hackers para utilizar todos los medios a su alcance y obtener beneficio económico.

Como probablemente sabéis, la mayoría de estas amenazas (si no todas) provienen de países de Europa del Este como Ucrania y Rusia. Sin embargo, esto no quiere decir que los ciberdelincuentes intenten de forma deliberada infectar a usuarios de dichos países. De hecho, algunos ejemplares antiguos de rogueware estaban programados para dejar de ejecutarse al detectar un teclado ruso. Bueno, hasta ahora…

Recientemente nos hemos encontrado con un sitio de rogueware completamente en ruso. Este sitio dice proteger los ordenadores y los perfiles de las redes sociales del spam, phishing, los virus, y los intentos de hackeo.

Este es el aspecto del sitio:

FIG.15

SITIO DE ROGUEWARE COMPLETAMENTE EN RUSO

Esta es la versión traducida al inglés por Google de la página:

FIG.16

VERSIÓN TRADUCIDA AL INGLÉS

Tras hacer clic en el botón de descarga, aparecen varias opciones a las que suscribirse (todas marcadas por defecto). A continuación se muestra un análisis falso, tras lo cual debes indicar tu situación geográfica (por defecto Rusia). Una vez se selecciona 1 de los 4 proveedores de telefonía móvil que se indican, aparece un número de tarificación especial para el envío de un SMS junto con instrucciones para recibir el código de activación del producto. El coste del SMS de activación es de 300 rublos, unos 10 dólares USA.

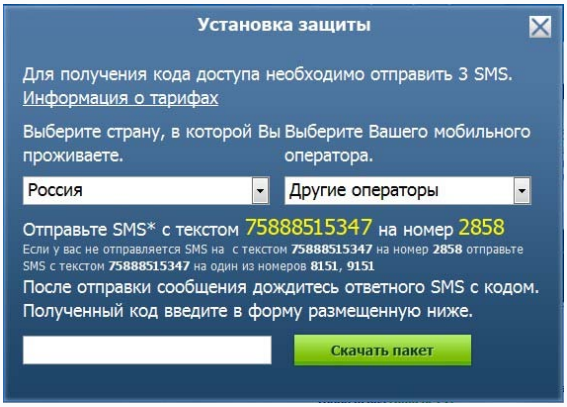


FIG.17

SMS en ruso

Esta es la versión traducida al inglés por Google del SMS:

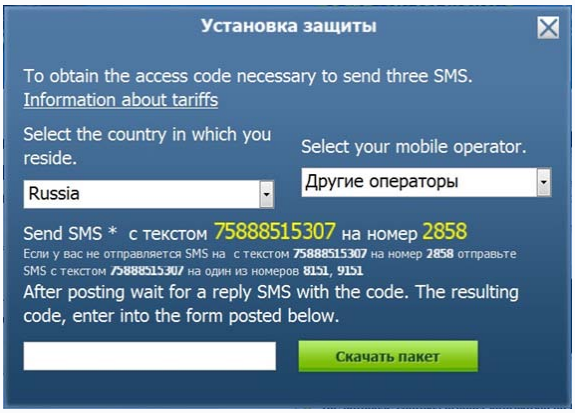


FIG.18

SMS en inglés

FIG.19

FALSO ANTIVIRUS UTILIZANDO EL NOMBRE DE UN PRODUCTO REAL DE MICROSOFT

Un poco de historia…

El negocio fraudulento de los llamados falsos antivirus, o más técnicamente, rogueware, apareció en 2006, pero fue a mediados de 2008 cuando realmente comenzaron a proliferar nuevos ejemplares de estas amenazas. El usuario se suele infectar navegando por webs, aceptando descargas disfrazadas de reproductores de códecs, pinchando en links recibidos por correo, etc.

Una vez infectado, estas aplicaciones se hacen pasar por soluciones antivirus que detectan cientos de amenazas en los ordenadores de sus víctimas. Sin embargo, cuando los usuarios tratan de eliminar dichas amenazas utilizando la aplicación, se les pide que compren la correspondiente licencia. A menudo, los usuarios, preocupados por la supuesta infección, acaban adquiriendo la licencia. Una vez pagan la licencia, no vuelven a saber nada más del supuesto vendedor y siguen teniendo el falso antivirus en su ordenador.

Los diseños de los falsos antivirus, que utilizan nombres muy reconocibles, facilitan que las víctimas piquen comprando la supuesta solución a sus problemas

Resulta curioso echar un vistazo a anteriores informes anuales y ver cómo arrancamos en cada uno de ellos esta sección. Cada año, hemos recogido y clasificado más malware que en los anteriores, y es que ésta sigue siendo la realidad desde que ya en 2005 anunciáramos: que la motivación de los cibercriminales había cambiado y que ahora buscaban el beneficio económico, por lo que esperábamos un boom del número de malware en circulación.

Pues bien, nos hubiera encantado comenzar el capítulo de este año confirmando que el nuevo malware se ha reducido, pero nada más lejos de la realidad. En 2010, los cibercriminales han creado y distribuido **un tercio del total de todos los virus que existen**. O lo que es lo mismo, en 12 meses ha aparecido el **34% de todo el malware** que ha aparecido en la historia y que ha sido clasificado por la compañía. Además, la base de datos de Inteligencia Colectiva, que detecta, analiza y clasifica automáticamente el 99,4% de las nuevas amenazas recibidas, ha alcanzado los **134 millones de ficheros diferentes, 60 de los cuales son malware (virus, gusanos, troyanos y otras amenazas informáticas)**.

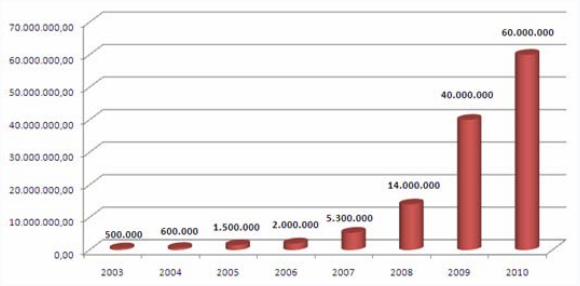


FIG.20

EVOLUCION HISTORICA DEL NUMERO DE NUEVO MALWARE CLASIFICADO POR PANDALABS

Así, y redondeando las cifras, en 2010 se han creado **20 millones de nuevos ejemplares** (tanto nuevos como variantes de familias ya conocidas) de malware, la misma cifra que se registró en todo el año 2009. Y la media de nuevas amenazas que se crean y distribuyen cada día **ha aumentado** desde 55.000 a **63.000 nuevos ejemplares diarios..**

Si lo resumimos en datos puros y duros, pertenecientes a la información contenida en nuestra base de datos de Inteligencia Colectiva, éste es el panorama:

- Se reciben 113.000 nuevos ficheros diarios en Inteligencia Colectiva, de los que 63.000 son nuevo malware. El 99,4% se procesan automáticamente por Inteligencia Colectiva prácticamente en tiempo real.

- El 52% del nuevo malware procesado por Inteligencia Colectiva sólo vive durante 24 horas, desapareciendo después.

- Durante 2010, Inteligencia Colectiva procesó más de 134.000.000 ficheros, de los cuales, más de 20.000.000 era malware desconocido o nuevo.

- Para hacerlo de forma manual, hubieran sido necesarios 1.898 técnicos y 3.705.388 horas de trabajo.

- La base de datos de Inteligencia Colectiva ocupa más de 20.000 GB o 209 billones de bits.

- Transformando esta cantidad de información en texto, podríamos escribir 808.192 enciclopedias británicas gracias a los 32 billones de palabras que ocuparía la misma extensión que la base de datos de Inteligencia Colectiva.

- Con esta magnitud, podríamos rellenar casi 36 mil millones de páginas de texto, que si pusiéramos una detrás de la otra impresas físicamente, se podría cubrir una distancia de más de 9 millones de kilómetros o ir y volver a la luna 12 veces.

- Y si tuviéramos que enviar toda esta información mediante una línea estándar de ADSL, tardaríamos 1.165 días.

Todo ello nos hace confirmar que el mercado del cibercrimen goza de buena salud, en buena medida posiblemente también condicionado a que cada vez hay más ciberdelincuentes que sin conocimientos técnicos exhaustivos se dedican a estas actividades ilícitas.

Esto, además, provoca que cada vez se creen más ejemplares de software malicioso, pero éste vive un período de tiempo muy corto: el 54% sólo está activo 24 horas en vez de meses como hace unos años; consiguen infectar sólo a unos pocos y desaparece. A medida que los antivirus son capaces de detectar el nuevo malware, los hackers lo transforman e incluso hacen ejemplares totalmente diferentes para pasar desapercibidos.

A pesar de la espectacularidad de los números, y aquí sí tenemos una buena noticia, el factor de crecimiento del nuevo malware de este año respecto a 2009 se reduce: desde el año 2003, las nuevas amenazas crecían a un ritmo del 100% o más. Pero en 2010, hasta el momento, se está creciendo alrededor de un 50%.

En cuanto a **qué tipo de malware** es el que se ha creado este año, no hay muchas sorpresas: los troyanos siguen dominando el panorama, aunque baja su peso específico (de 66% el pasado año a 55,9 en éste) a favor de la categoría de los tradicionales virus, que se coloca en segunda posición en el ranking viniendo de la tercera el pasado ejercicio (6,6% en 2009 contra 22% en 2010).

El adware, que ocupaba la segunda posición (con el 17%), se sitúa en el cuarto puesto este año (bajando a 9,6%). Y los gusanos también crecen: crecen: del 3 al 10%, así como el spyware, que también baja significativamente: del 5,7% a un 0,34.

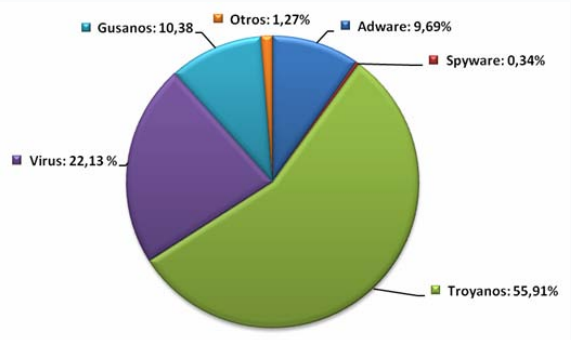


FIG.21

TIPO DE MALWARE

El que los troyanos se mantengan en los niveles habituales, no es sorprendente, dado que la mayoría están enfocados al robo de identidad o de datos bancarios para su posterior venta en el mercado negro. Y el resto, sigue la estela de la tendencia observada en los últimos dos años.

El 1,26% que corresponde a la categoría de otros está repartido entre el resto de "sospechosos habituales", cuyo ranking queda de la siguiente manera:

Otros	%
Dialer	29,11
Herramientas de hacking	26,91
PUP	24,28
Riesgos de Seguridad	19,17
Bromas	0,48
Tracking Cookie	0,05

En cuanto a infecciones, calculamos que el **53% de promedio de usuarios de PC** han estado infectados en algún momento con algún tipo de malware, incluso teniendo protección activa y actualizada. Estos son datos recogidos de todos los usuarios que diariamente, y de forma gratuita, utilizan **Panda ActiveScan 2.0**.

Respecto al **top de países con mayores infecciones**, éste es el ranking de 2010:

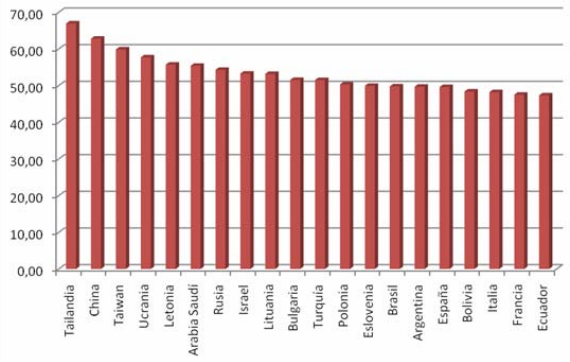


FIG.22

TOP DE PAÍSES CON MAYORES INFECCIONES

Si lo comparamos con el Top de 2009, vemos algunos cambios significativos. Por ejemplo, Taiwán venía liderando la lista, pero este año le ha ganado por la mano Tailandia y China. Países como Polonia, Colombia, España o Argentina han quedado relegadas a los últimos puestos de la lista, o incluso han desaparecido. Y otras naciones como Italia o Francia, han mejorado en cuanto a ratios de infección (es decir, tienen menos) y se van a la cabeza de lista. Suecia desaparece, así como Portugal o UK, entre otros.

Respecto a **métodos de infección**, 2010 ha sido el año rey del uso, por parte de los hackers, de redes sociales, posicionamiento de falsas webs (llamado BlackHatSEO) y el aprovechamiento de vulnerabilidades 0-day.

Más BlackHat SEO

El término Blackhat SEO hace referencia a una técnica de optimización de los motores de búsqueda con fines maliciosos que se aprovecha de las funcionalidades de dicho motores para situar páginas maliciosas en los primeros lugares de los resultados de las búsquedas. Los delincuentes que utilizan técnicas de Blackhat SEO suelen subir scripts PHP a las páginas atacadas. Estos scripts lanzan consultas al servicio de temas más populares de Google y a continuación generan archivos HTML correspondientes a los términos de búsqueda más utilizados.

El motor de búsqueda es engañado para que 'vea' el material correspondiente, mientras que el usuario es redireccionado a un sitio de distribución de malware en cuanto hace clic sobre el enlace del resultado que aparece en primer lugar. Los delincuentes que se aprovechan de las técnicas de Blackhat SEO para distribuir malware han explotado tanto los motores de búsqueda que los usuarios ya no saben si confiar o no en los resultados de sus búsquedas – Lo que no son buenas noticias ni para los usuarios ni para las empresas de los motores de búsqueda. Este año hemos sido testigos de múltiples campañas de Blackhat SEO que explotaban los temas más populares del día, viendo como muchas de ellas conseguían colar páginas maliciosas entre los primeros lugares de los resultados de las búsquedas.

El primer ataque importante producido en el 2010 se centraba en los usuarios que buscaban información sobre el teléfono Nexus One de Google y sobre el terremoto de Haití[1]. En ambos casos, los dos primeros resultados de búsqueda apuntaban a sitios empleados en campañas de rogueware, y 5 de los 6 primeros resultados eran maliciosos.

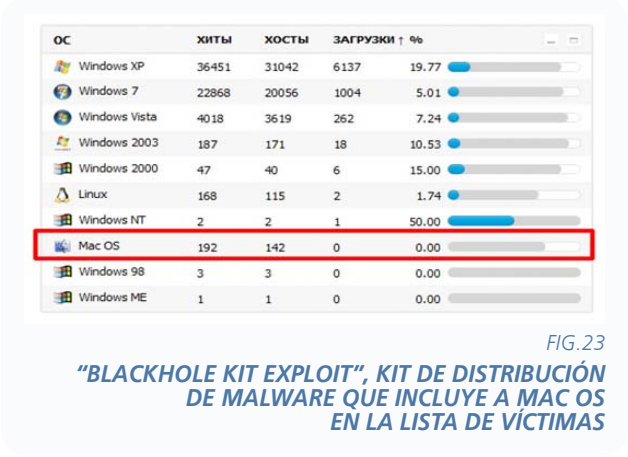
El siguiente ataque de Blackhat SEO que nos llamó la atención tenía como objetivo a los usuarios de Facebook[2]. Este ataque era distinto en el sentido de que no recurría al método típico de utilizar los términos más populares de Google. Por el contrario, los ciber-delincuentes responsables del ataque optaron por combinar las campañas tradicionales de Blackhat SEO con el oportuno anuncio de la existencia de un error en Facebook que hacía que los usuarios vieran una "aplicación sin nombre" en la configuración de su cuenta de Facebook. Esta fue la primera vez que vimos que una campaña de Blackhat SEO atacaba a los usuarios de redes sociales.

Y las campañas han seguido continuando. Ha habido tantas que sería demasiado largo entrar en detalles específicos sobre cada una de ellas, pero algunos de los ataques más importantes se han centrado en temas relacionados con las vacaciones[3], eventos comerciales[4], desastres naturales[5], anuncios de productos largamente esperados[6], eventos deportivos[7][8], cotilleos sobre famosos[9][10], programas de televisión[11], y juguetes populares[12]. Todo parece indicar que los ataques que emplean técnicas de Blackhat SEO seguirán existiendo mientras que el servicio de los temas más populares de Google siga siendo tan fácilmente accesible para los ciber-delincuentes. Según nuestras investigaciones, los resultados de las búsquedas de Google son los más vulnerables a los ataques de Blackhat SEO, mientras que los resultados del motor de búsqueda Bing de Microsoft se han mantenido relativamente a salvo -por el momento- de esta plaga.

1 http://pandalabs.pandasecurity.com/blackhat-seo-attack-targeting-google-nexus-one/
2 http://pandalabs.pandasecurity.com/unnamed-app/
3 http://pandalabs.pandasecurity.com/malware-spreading-via-halloween-related-keywords/
4 http://pandalabs.pandasecurity.com/blackhat-friday-and-cybercrime-monday/
5 http://pandalabs.pandasecurity.com/out-of-the-frying-pan-into-the-fire/
6 http://pandalabs.pandasecurity.com/this-time-it%e2%80%99s-apple-ipad%e2%80%99s-turn/
7 http://pandalabs.pandasecurity.com/extreme-sports-2010-fifa-world-cup-bhseo-attack/
8 http://pandalabs.pandasecurity.com/barcelona-vs-real-madrid-black-hat-seo-attack/
9 http://pandalabs.pandasecurity.com/fernanda-romero-arrest-leads-to-distribution-of-rogueware/
10 http://pandalabs.pandasecurity.com/chelsea-clinton-blackhat-seo-attack/
11 http://pandalabs.pandasecurity.com/lost-ronnie-james-dio-and-so-on-and-so-forth-to-distribute-rogueware/
12 http://pandalabs.pandasecurity.com/out-of-the-frying-pan-into-the-fire/

En internet podemos ver muchos documentos sobre comparativas entre Windows 7 y Mac OS X, sobre cuál es rápido, cuál tiene mejores efectos y prestaciones, incluso entre el precio de ambos ya que el sistema operativo de Apple sólo cuesta 29.90$. No obstante en este artículo queremos hablar de las principales protecciones de seguridad que disponen cada uno para hacer frente a las vulnerabilidades y técnicas de explotación que se utilizan hoy en día para comprometer el sistema atacado.

El crecimiento de la venta de equipos Apple es innegable, y por este motivo el sistema operativo de los de Cupertino está siendo otro de los puntos de mira para los desarrolladores de malware. De hecho ya es común en Internet la venta de kits de exploit que incluyen a este sistema, como es el caso de "BackHole Kit Exploit", software ruso para la creación de redes de bots. En la siguiente imagen se muestra una captura de este kit y se puede observar como cuenta con los últimos exploits que afectan al sistema operativo de Apple, Mac OS X.



ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ ↑	%
Windows XP	36451	31042	6137	19.77
Windows 7	22868	20056	1004	5.01
Windows Vista	4018	3619	262	7.24
Windows 2003	187	171	18	10.53
Windows 2000	47	40	6	15.00
Linux	168	115	2	1.74
Windows NT	2	2	1	50.00
Mac OS	192	142	0	0.00
Windows 98	3	3	0	0.00
Windows ME	1	1	0	0.00

FIG.23

"BLACKHOLE KIT EXPLOIT", KIT DE DISTRIBUCIÓN DE MALWARE QUE INCLUYE A MAC OS EN LA LISTA DE VÍCTIMAS

No es de extrañar que empresas como Panda Security ya hayan lanzado al mercado soluciones[13] de seguridad para combatir estas amenazas que empieza a potenciarse en la plataforma de la manzana.

Medidas de protección

En los siguientes párrafos, sin entrar en mucho detalle técnico, vamos a hablar de las 2 principales protecciones de seguridad que tienen implementados ambos sistemas operativos y cómo de difícil se lo ponen a los hackers y a los ciber-delicuentes desde el punto de vista de la explotación de las vulnerabilidades para ejecutar código en un sistema vulnerable de forma satisfactoria.

DEP (Data Execution Prevention)[14]

Esta técnica previene la ejecución de datos que están alojados en una zona de memoria que no tiene permisos de ejecución. El usuario malicioso utiliza estas zonas para alojar su código malicioso antes de que sea ejecutado y si DEP está activado, evita su ejecución, por lo tanto la máquina no queda comprometida. DEP está disponible en los sistemas de Microsoft desde Windows XP Service Pack 2, sin embargo los de Cupertino no incluyen la protección de DEP hasta la llegada de Snow Leopard, que es la última versión disponible de Apple y la que hemos tomado para esta comparativa.

En cuanto a DEP, mencionar que hay dos tipos de protecciones: una a nivel de Software (Software-Enforced DEP o también llamado SafeSEH), que evita la ejecución de código si al producirse una excepción durante la ejecución de un programa (lo que podría ser una explotación de una vulnerabilidad) este intenta llamar a una dirección fuera de los controladores de excepciones registrados. Este sistema, aunque dificulta la explotación de ciertas vulnerabilidades, no se puede considerar una protección completa.

Hardware-Enforced DEP que activa el bit NX /XD en las CPU compatibles, por lo tanto depende del hardware en el que estemos ejecutando el sistema operativo. Esta protección cubre las diferentes posibilidades de ejecución de código desde zonas de memoria de datos. Esta protección puede producir ciertas incompatibilidades con software legítimo, cada programa debe "indicarle" al sistema operativo si es o no compatible para que éste pueda activar dicha protección cuando sea lanzado su proceso. Es decir, aunque el sistema operativo disponga de dicha protección, si el software que estamos ejecutando no es compatible con DEP, no estaríamos protegidos. Tanto Windows 7 como Snow Leopard tienen activada esta protección, por ejemplo, en Internet Explorer 8 y Safari.

Aunque DEP a nivel de hardware mejora la seguridad del sistema considerablemente sigue sin ser suficiente. Hay ciertas técnicas de ataques donde el usuario malicioso se las ingenia (dependiendo de la versión y configuración del sistema operativo Windows) para deshabilitar en tiempo de ejecución la protección de DEP para ese programa o simplemente, dando permisos de ejecución a la zona de memoria de datos donde está alojado el código malicioso antes de ejecutarlo. De una u otra forma el usuario conseguiría saltarse la protección DEP.

[13] http://prensa.pandasecurity.com/2010/10/panda-security-lanza-panda-antivirus-para-mac/
[14] http://en.wikipedia.org/wiki/Data_Execution_Prevention
[15] http://en.wikipedia.org/wiki/NX_bit
[16] http://en.wikipedia.org/wiki/Address_space_layout_randomization

Para realizar cualquiera de estas 2 técnicas, el usuario malicioso tiene que realizar ciertas llamadas en su código a diferentes funciones especiales del sistema operativo, para lo cual el usuario debe conocer la dirección en memoria de estas funciones. Con el objetivo de evitar este tipo de acciones y así impedir la ejecución del código malicioso, ambos sistemas operativos implementan la tecnología de mitigación ASLR (Address Space Layout Randomization) disponible en Windows 7 y en MacOS X desde la versión Leopard. No obstante, tanto en Leopard con en Snow Leopard, es menos efectiva que la implementada por Microsoft en Windows 7. Al igual que hemos mencionado anteriormente la aplicación debe ser 100% compatible con ASLR para que esta tecnología de mitigación sea efectiva.

ASLR modifica la dirección de memoria de las funciones que el usuario malicioso necesita en cada inicio del sistema operativo para que el usuario malicioso no conozca su ubicación y su código malicioso no sea funcional.

ASLR es efectiva siempre que DEP esté activado y viceversa. En caso contrario un usuario malicioso sería capaz de saltarse tanto DEP o ASLR para ejecutar su código malicioso si ambas no están activadas al mismo tiempo. Sin embargo, si ambas están activadas y la aplicación es compatible con DEP y ASLR, la explotación de una vulnerabilidad y su ejecución de código a día de hoy se reduce casi a 0.

Después de este pequeño análisis podemos decir que a día de hoy, y para hacer frente a las vulnerabilidades, aunque ambos sistemas disponen de la tecnología adecuada, Microsoft Windows 7 está mejor preparado que Snow Leopard, porque su implementación de ASLR está superior a la implementada por Apple. Por lo tanto los usuarios de Mac OS X tendrán que esperar a ver cómo responde Apple con su nuevo sistema operativo, Mac OS X Lion.

En los diferentes informes que hemos ido publicando durante el año, hemos ido comentando y viendo como han sido dos plataformas (iPhone y Android) las que se han ido imponiendo en el mercado de los SmartPhones, en detrimento de las plataformas Symbian y Windows Mobile que no han reaccionado lo suficientemente rápido a este nuevo escenario y que, a pesar de que han sacado nuevas versiones de sus sistemas operativos en los últimos meses de este año, parece que no van a ser las mayoritarias.

Esta nueva coyuntura ha afectado, como es lógico al "mercado del malware", reduciéndose considerablemente la aparición de malware para plataformas Symbian y Windows Mobile, debido a que la nueva coyuntura no las hace atractivas para invertir dinero y tecnología para los hackers. A pesar de ello, aunque en un número mucho menor, ha seguido surgiendo malware para plataforma Symbian, muy enfocado a mercados donde sigue teniendo presencia importante, como en países asiáticos o emergentes.

En cuanto a las plataformas que están dominando el marcado, han surgido sobre todo intentos de Phishing mediante aplicaciones bancarias falsas, pruebas de concepto y alguna que otra aplicación comercial de espionaje.

El futuro es incierto, y aunque para muchos Android es la plataforma mas vulnerable por su política de publicación de aplicaciones, ya comentamos en anteriores artículos que precisamente es esta decisión la que podría causar el efecto contrario, ya que al no ser necesario liberar o rootear el terminal, los usuarios mayoritariamente usan Android Market para descargar aplicaciones.

Como hemos dicho, ya está en la calle el nuevo Windows Mobile 7, y aunque vaya un poco rezagado, no hay que menospreciar la fuerza de ventas de Microsoft y sobre todo la campaña de navidad 2010-2011, donde puede que acorte distancias y pueda sumarse al grupo de cabeza.

2011 será largo y habrá que ver la penetración de la plataforma Android en el mercado, ya que el número de terminales con este sistema operativo no deja de crecer. También puede ser el año de la generalización de las conexiones a Internet a través de terminales móviles, por lo que las oportunidades para el malware pueden hacer que estas plataformas sean aun más atractivas para los cibercriminales.

Solo queda esperar a que las mafias del malware empiecen a dar sus primeros pasos: no dudéis que estamos vigilantes y "One Step Ahead".

El spam sigue manteniéndose en niveles sumamente altos en 2010, aunque bien es cierto que el desmantelamiento de algunas redes de bots (como Mariposa o Bredolad) ha propiciado que se haya dejado de utilizar estos ordenadores zombies para enviar spam, circunstancia que sin duda ha mejorado el tráfico mundial. Así, el pasado ejercicio, alrededor del 95% de todo el tráfico mundial era spam, cifra que se sitúa en el 85% de promedio en 2010.

De todo el spam mundial, el 50% es enviado por tan sólo 20 países, que son los siguientes:

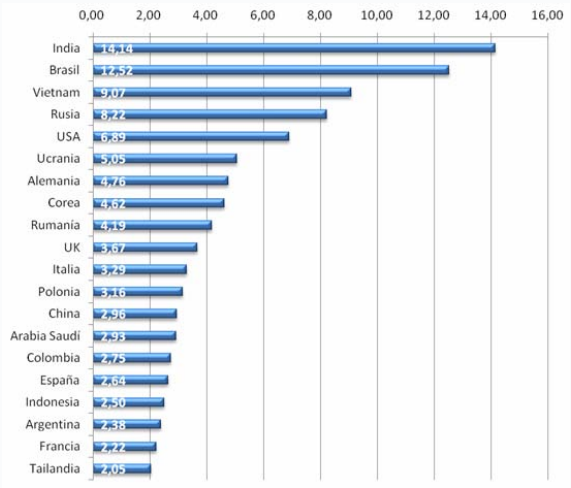


FIG.24

TOP 20 DE PAÍSES EMISORES DE SPAM EN 2010.

El farmacéutico sigue siendo el tema estrella, seguido por e-mails que intentan vender falsificaciones de productos famosos. Aquellos cuyo objetivo es conseguir la identidad de acceso a banca online o tiendas, phishing, y los enfocados al fraude ve crecer su porcentaje.

Pero en este ejercicio hemos visto importantes novedades acerca del spam, que ya no sólo vende Viagra con unos textos y estética horribles, que sólo haría caer a los muy, muy inocentes. Sino que hemos sido testigos de campañas de envío de spam intentando infectar a usuarios usando ganchos que hasta ahora no se habían utilizado.

Tal es el caso de un correo electrónico que parecía proceder de iTunes Store y era una copia exacta de los comunicados oficiales que manda por e-mail.

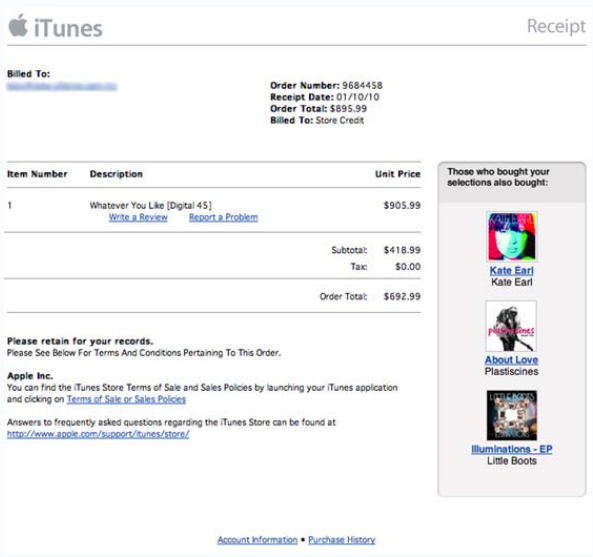


FIG.25

FALSO MENSAJE DE ITUNES.

El verdadero propósito del mensaje no es mostrar las posibilidades de compra de iTunes Store, sino que pretende que el usuario haga click en "Informar de un problema" para redirigirle a un falso instalador de Flash.

Otro caso similar ha sido detectado, pero esta vez utilizando la red profesional LinkedIn. El correo parece llegar de la dirección messages-noreply@bounce.linkedin.com en nombre del departamento de comunicación de LinkedIn [communication@linkedin.com], tratándose de una copia exacta de los recordatorios oficiales de LinkedIn vía e-mail.

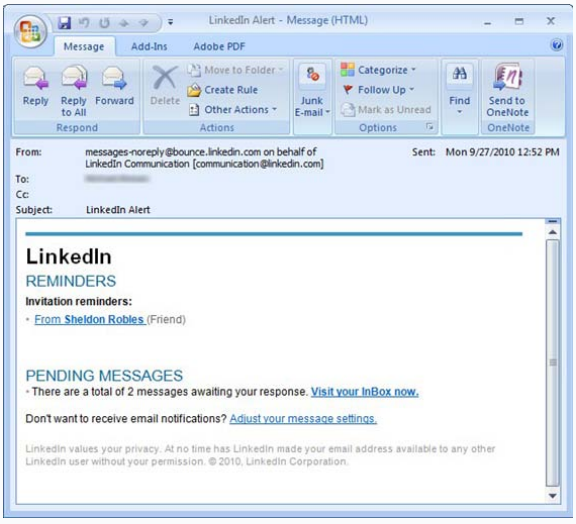


FIG.26

MENSAJE DE CORREO TRATANDO DE HACERSE PASAR POR LINKEDIN.

Cuando el usuario se dirigía a conocer la invitación, mediante un sistema de redirecciones era finalmente conducido a una tienda de productos farmacéuticos.

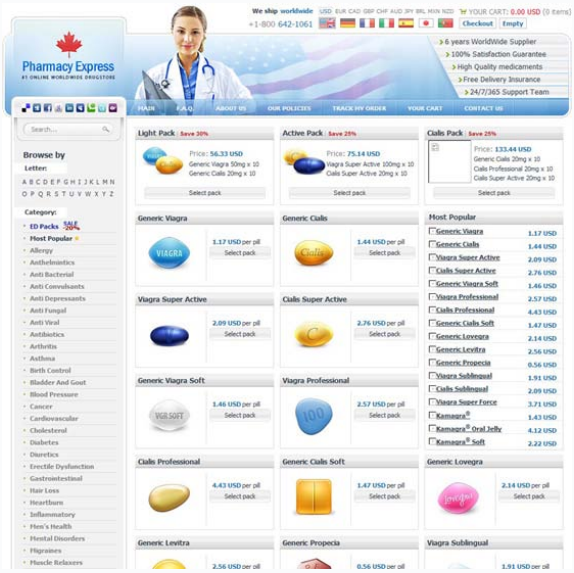


FIG.27

TIENDA DE PRODUCTOS FARMACÉUTICOS.

Y se siguen utilizando las técnicas de ingeniería social para engañar a usuarios, como la campaña de spam protagonizada por el Ministerio de Transporte, donde en un inglés un tanto "rudimentario" nos informan que el "ministro de transporte" va a realizar unos cambios en el impuesto de vehículos y nos aconsejan que leamos atentamente la documentación adjunta.

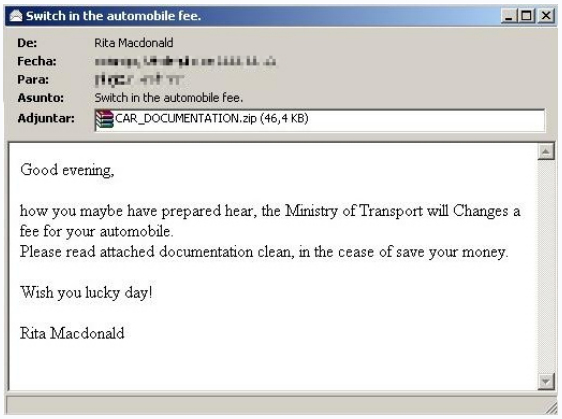


FIG.28

EJEMPLAR DEL CONOCIDO SINOWAL.

Por supuesto, la documentación adjunta no era tal sino un ejemplar del conocido Sinowal.

En cuanto a ordenadores zombies, PandaLabs ha visto una media de unos 340.000 ordenadores secuestrados diarios. Estos ordenadores, que pertenecen a redes de bots operadas por cibermafias, son los que posteriormente se suelen utilizar para el envío de spam.

Y para ello, lo que hacen es ofrecer los servicios a través del mercado negro, a unos precios que, aunque han bajado a resultas de la crisis, pueden resultar sumamente atractivos para aquellos que quieren vender sus productos sin correr ningún riesgo.

Este servicio no es nuevo, y se oferta prácticamente de todo para que los usuarios puedan enviar spam de una forma segura: bases de datos con direcciones a las que enviar el spam; alquiler de uso de las máquinas desde las que enviar el spam (redes de bots); conexiones vpn para facilitar la conexión a los paneles de control de forma anónima, etc.

Estos son sólo algunos ejemplos reales y actuales de venta de estos servicios en el mercado negro:

FIG.29

EJEMPLOS REALES DE VENTA DE SERVICIOS.

Durante el año 2010, Microsoft ha publicado un total de 101 actualizaciones, que afectan a gran parte de sus productos (Windows XP, Vista, 7, 2003 y 2008, Internet Explorer, MS IIS, MS Office, MS Exchange, MS SQLServer, Windows Media Player). No hay duda de que Microsoft sigue siendo el blanco de numerosos ataques por parte del malware.

Entre todas estas vulnerabilidades hay que destacar dos errores de diseño importantes en el sistema operativo de Microsoft Windows. A mitad de junio apareció un 0-Day, CVE-2010-2568, que afectaba a todas las versiones de Windows a partir de Windows XP e incluso a las versiones beta de Windows 7 Service Pack 1 y Windows Server 2008 R2 Service Pack 1, que fue clasificada por Microsoft como crítica.

La vulnerabilidad se produce porque Windows analiza incorrectamente los ficheros de acceso directo (ficheros con extensión .lnk y .pif) permitiendo a un usuario malicioso la ejecución remota de código si un usuario visualiza el icono del acceso directo que ha sido modificado para ese fin. Esta vulnerabilidad se empezó a explotar "In-The-Wild" utilizando el malware Rootkit/ TmpHider. Debido a las características de su explotación, al igual que para el malware de la familia autorun, los dispositivos USB son las principales vías para la distribución de malware utilizando esta vulnerabilidad.

Al tratarse de una vulnerabilidad crítica, Microsoft publicó inmediatamente un solución temporal, pero esta solución era un poco "agresiva", ya que eliminaba por completo los iconos de acceso directo de Windows. La comunidad de Internet empezó a moverse y aparecieron otras soluciones, ajenas a Microsoft, para mitigar la explotación de la vulnerabilidad. Entre estas soluciones hay que destacar la del investigador Didier Stevens, con su herramienta Ariad (aunque actualmente ya existe un parche para esta vulnerabilidad [MS10-046], este parche no es aplicable en Windows XP SP2, por lo que herramientas como Ariad siguen útiles para proteger estas versiones de Windows que ya han quedado fuera del ciclo de actualizaciones de Microsoft). Casi 2 meses después, el 2 de agosto, Microsoft puso fin a esta brecha de seguridad publicando la actualización (MS10-046) que corrige finalmente la vulnerabilidad.

Adobe también ha "sufrido" mucho durante este año, sobre todo en lo referente a Adobe Acrobat y Adobe Reader. Los atacantes se han centrado en explotar estos dos productos como una vía fácil y sencilla de infectar los equipos de los usuarios de sus productos. Es normal desconfiar cuando recibimos un correo con ejecutable, pero no tanto cuando recibimos un PDF; e incluso más terrorífico es pensar que podemos infectarnos solo por navegar y visualizar un PDF con nuestro navegador.

Ante esta situación, muchos usuarios han optado por utilizar Foxit Reader como lector de PDFs, pero no es oro todo lo que reluce, ya que también han aparecido 0-Days para este programa. Esto nos demuestra que no hay un programa 100% seguro, sólo que hay programas que no han recibido todavía la suficiente atención por parte de los creadores de malware.

Una buena noticia es que Adobe ha movido ficha y ha publicado una nueva versión de su lector de PDFs, Adobe Reader X, que incorpora una sandbox que añade una capa de seguridad extra, de forma que aunque se consiga explotar una vulnerabilidad, el ámbito de actuación del malware estará muy reducido, ya que quedará confinado a la sandbox, la cual restringe el acceso al sistema evitando la escritura de ficheros o ejecución e instalación de malware. Se trata de un movimiento interesante por parte de Adobe. Vigilaremos activamente la evolución del malware en este sentido, porque seguramente los creadores de malware intentarán buscar una forma de sobrepasar la sandbox.

No podemos dejar de mencionar el asunto estrella de este año: Stuxnet. Este malware ha sido uno de los más complejos que se han podido ver en los ultimos años. A parte de tener la capacidad de reprogramar PLC industriales (concretamente sistemas WinCC SCADA de Siemens), lo que permitiría modificar el comportamiento de plantas energéticas, nucleares, etc., se caracteriza porque explota 5 vulnerabilidades diferentes, 4 de ellas 0-days.

Las vulnerabilidades explotadas son:

- Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (MS08-067)
- Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (MS10-046)
- Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability (MS10-061)
- Microsoft Windows Kernel-Mode Drivers Privilege Escalation (MS10-073)
- Windows Task Scheduler Privilege Escalation

La primera es una vulnerabilidad antigua, del 2008, pero que todavía es utilizada activamente por el malware. La MS10-046 fue parcheada por Microsoft en Agosto, con la publicación del boletín MS10-046, como ya comentamos en el informe pasado; y la tercera, la MS10-061, fue solucionada en Septiembre. Con respecto a las dos últimas, que permiten escalada de privilegios, sólo la primera ha sido solucionada con la publicación en noviembre del boletín MS10-073. Microsoft ha confirmado que la última de ellas será parcheada en un futuro próximo, quizás a principios del año 2011, pero la fecha no ha sido todavía concretada.

Desde Pandalabs recomendamos que se actualicen los sistemas utilizando los parches de Microsoft, ya que las MS10-046 y la MS10-061 permiten la ejecución remota de código, lo que permitiría a cualquier atacante hacerse con el control del sistema.

Durante este último trimestre, y siguiendo con vulnerabilidades que afectan a los productos de Microsoft, hay que destacar una nueva vulnerabilidad (CVE-2010-3962) que afecta a Internet Explorer 6, 7 y 8, permitiendo la ejecución remota de código a través de CSS. A pesar de que a principios de noviembre la utilización de esta vulnerabilidad por parte del malware era escasa, a mitad de mes se ha detectado que ha comenzado a ser utilizada activamente por el malware, debido a que se han publicado exploits que permiten utilizarla, por lo que seguramente Microsoft publicará un parche en breve.

Mozilla Firefox se ha visto afectado por un 0-Day que apareció a principios de Octubre, estando afectadas las versiones 3.5 y 3.6 de este popular navegador. Hay que destacar que la página de los Premios Nobel fue comprometida y se insertó el código necesario para explotar esta vulnerabilidad. A finales de octubre, Firefox publicó sendas actualizaciones, para Firefox y Thunderbird, que solucionaban el problema.

Y volviendo a los productos de Adobe, en este cuarto trimestre hemos vuelto a ver 0-Days para sus productos. A finales de Octubre, apareció un nuevo 0-Day que afectaba a diferentes versiones de Adobe Flash Player, concretamente a las versiones 10.1.85.3 en Windows, Macintosh, Linux and Solaris, 10.1.95.2 en Android, en el componente authplay.dll de Adobe Reader 9.4 para Windows, Macintosh y UNIX y Adobe Acrobat 9.4 para Windows y Macintosh. La vulnerabilidad, identificada con el CVE-2010-3654, permitiría la ejecución remota de código. Se trataba de un 0day que estaba siendo activamente utilizado por el malware, por lo que Adobe publicó los correspondientes parches para solucionar el problema.

2011 traerá pocas innovaciones radicales en cuanto al ámbito del cibercrimen se refiere. **Ciberactivismo** y **ciberguerra**; **más malware** enfocado siempre a la consecución del beneficio económico, **redes sociales**, **ingeniería social** y códigos maliciosos con **alta capacidad de cambio** para evitar ser detectados son las principales claves para 2011, acompañado del aumento de **amenazas para Mac,** nuevos diseños para atacar **sistemas 64 bits** y nuevos ejemplares que se aprovecharán de **vulnerabilidades zero-day**.

Una vez más, y una vez analizado el ejercicio 2010, hemos sacado nuestra bolita de cristal, y éste es, en resumen, nuestro vaticinio de las 10 principales tendencias en seguridad para 2011:

1. Creación de malware. El año 2010 se va a cerrar con un aumento significativo del número de malware, del que ya venimos hablando hace algunos años. En este ejercicio, han sido más de 20 millones lo que se han creado, cifra superior al que se creó en 2009. Así, la base de datos de Inteligencia Colectiva de Panda tiene clasificados y almacenados más de 60 millones de amenazas. El ratio de crecimiento interanual, sin embargo, parece que está alcanzando su punto álgido: hace unos años, era de más del 100%. En 2010, ha sido del 50%. Esperamos que lo mismo suceda en 2011.

2. Ciberguerra. Stuxnet y la filtración de Wikileaks apuntando al Gobierno chino como responsable de los ciberataques a Google y a otros objetivos ha marcado un antes y un después en la historia de los conflictos. En las ciberguerras, al igual que sucede en las guerras del mundo real hoy en día, no hay bandos con uniforme en el que se puede distinguir a los diferentes combatientes. Hablamos de lucha de guerrillas, donde no se sabe quién es el que ataca, ni desde dónde lo hace, lo único que puede tratar de deducirse es el fin que persigue.

Con Stuxnet, ha quedado claro que se quería interferir en determinados procesos de centrales nucleares, específicamente en el centrifugado del Uranio. Ataques como éste, más o menos sofisticados, están teniendo lugar ahora mismo, y durante 2011 se incrementarán, aunque muchos pasarán desapercibidos para el gran público, porque tardarán algún tiempo en conocerse.

3. Ciberprotestas. Sin duda, la gran novedad de 2010. La ciberprotesta o ciberactivismo, nuevo movimiento inaugurado por el grupo Anonymous y su Operación Payback, apuntando a objetivos que pretenden acabar con la piratería en Internet primero, y apoyando a Julian Assange, autor de Wikileaks, después, se ha puesto de moda. Incluso usuarios con pocos conocimientos técnicos pueden formar parte de estos ataques de Denegación de Servicio Distribuido (ataques DDoS) o campañas de spam.

Aún a pesar de que muchos países están intentado regular legislativamente este tipo de actuaciones rápidamente, para poder ser considerada esta actividad un delito y, por lo tanto, perseguida y condenable, creemos que en 2011 veremos proliferar este tipo de cibermanifestaciones, tanto de este grupo como de otros que irán surgiendo. Internet tiene cada vez mayor importancia en nuestras vidas y es un medio de expresión que ofrece anonimato y libertad, por lo menos de momento, por lo que veremos cómo la sociedad civil se hace escuchar por estos métodos, y con éxito, por cierto.

4. Ingeniería social. "El hombre es el único animal que tropieza dos veces con la misma piedra". Este dicho popular es cierto como la vida misma, y por eso uno de los mayores vectores de ataque seguirá siendo el uso de la denominada ingeniería social para lograr infectar a internautas confiados. Además, los ciberdelincuentes han encontrado un caldo de cultivo ideal en las redes sociales, donde los usuarios son aún más confiados que cuando utilizan otro tipo de herramientas, como el correo electrónico.

Durante 2010 hemos visto varios ataques cuyo cuartel general de distribución han sido las dos redes más utilizadas a nivel mundial: Facebook y Twitter. En 2011 veremos no sólo cómo se consolidan como herramienta para los hackers, sino que seguirán creciendo en cuanto a ataques distribuidos.

Por otro lado, los ya conocidos ataques BlackHatSEO (indexación y posicionamiento de falsas webs en motores de búsqueda para engañar a los usuarios) serán también ampliamente utilizados en 2011, como siempre, aprovechando las noticias más relevantes del momento para llegar al mayor número posible de usuarios.

Y dada la proliferación, cada vez más notable, de contenido multimedia (fotos, vídeos, etc.), mucho malware seguirá siendo distribuido disfrazándose de plugins, reproductores y aplicaciones similares. No es que hayan desaparecido otros métodos, como el uso de las

populares presentaciones de PowerPoint distribuyéndose a través de cadenas de amigos, pero la educación y concienciación en seguridad hace pensar que los usuarios ya han escarmentado con este tipo de aplicaciones.

Y como la crisis suele agudizar el ingenio, y lamentablemente cada vez son necesarios menos conocimientos para convertirse en un hacker y dedicarse al robo de dinero, veremos proliferar nuevas y convincentes formas de intentar enganchar a los inocentes: a través de "ligues" falsos, con ofertas de trabajo irrechazables, con timos cada vez más sofisticados, a través de ataques de phishing a las principales entidades ya no bancarias, sino de plataformas de pago, de tiendas online, etc…

Es decir, ahora más que nunca, es importantísimo utilizar el sentido común cuando desarrollamos nuestra vida online, que muchas veces, como solemos decir, es el menos común de los sentidos.

5. Windows 7 afectará al desarrollo de malware. Como ya comentamos el pasado año, necesitaremos al menos dos años para comenzar a ver proliferar amenazas específicamente diseñadas para Windows 7. En 2010 hemos visto algunos movimientos en esta dirección, pero creemos que en 2011 seguiremos conociendo nuevos casos de malware que busca atacar a los cada vez más usuarios del nuevo sistema operativo.

6. Móviles. Esta sigue siendo la eterna pregunta: ¿cuándo despegará el malware para móviles? Pues bien, parece que en 2011 podrían verse nuevos ataques, pero tampoco de forma masiva. La mayoría de ataques actuales se dirigen a móviles con Symbian, sistema operativo que tiende a desaparecer. De los diferentes sistemas en auge, la bola de cristal de PandaLabs ve claramente cómo el número de amenazas para Android va a aumentar de forma considerable a lo largo del próximo año, convirtiéndose en la plataforma preferida por los ciberdelincuentes.

7. Tablets? El dominio del iPad es total en este campo, pero en breve habrá competidores que ofrezcan alternativas interesantes. En cualquier caso, salvo alguna prueba de concepto o algún ataque anecdótico, no creemos que en 2011 los tablets sean el principal objetivo de los ciberdelincuentes.

8. Mac. Malware para Mac hay, y seguirá habiendo. Crecerá el número a medida que siga aumentando su cuota de mercado. Lo más preocupante es la cantidad de agujeros de seguridad que tiene Apple en su Sistema Operativo: más vale que se rápidamente le pongan remedio, ya que los ciberdelincuentes son conscientes de ello y de la facilidad que conlleva estos agujeros de seguridad para distribuir malware.

9. HTML5. El que podría llegar a ser el sustituto de Flash, HTML5, es un candidato perfecto para todo tipo de delincuentes. El hecho de que pueda ser ejecutado por los navegadores sin necesidad de ningún plugin hace aún más apetitoso el poder encontrar un agujero que podría llegar a los ordenadores de los usuarios independientemente del navegador utilizado. Veremos los primeros ataques en los próximos meses.

10. Amenazas cifradas y rápidamente cambiantes. Este movimiento ya lo hemos visto en los dos últimos años, y asistiremos a un aumento todavía mayor en 2011. Que el malware está diseñado para el beneficio económico, no es ninguna novedad. Que para conseguirlo utiliza la ingeniería social para engañar a los usuarios y tiende a ser lo más silencioso posible para que no se enteren las víctimas de que están infectados, tampoco lo es. Pero el mismo mecanismo de hacerlo cada vez más silente hace que en el laboratorio se reciban más y más ejemplares ofuscados y con mecanismos de cifrado, preparados para conectarse a un servidor y ser actualizados rápidamente en el momento en que las compañías de seguridad somos capaces de detectarlos, y cada vez más dirigidos a usuarios específicos (últimamente, proliferan las empresas como objetivo, ya que la venta de datos en el mercado negro se cotizan al alza).

El panorama no tiende a mejorar. Cierto es que en 2010 hemos sido testigos de detenciones importantes que han golpeado al mundo del cibercrimen. Pero, lamentablemente, todavía insuficientes si vemos todo lo que se está moviendo. El mercado negro mueve miles de millones en beneficios, opera con total libertad amparándose en el anonimato de Internet y aprovechando los vacíos legales. La recesión económica no hace más que acentuar todavía más la situación: con millones de parados en varios países, algunos ven esta forma de salir adelante como la de menos riesgo, aunque, eso no justifica el hecho de que sea un delito.

Conclusión

Cuando le contamos a la gente todo lo que está pasando, y vemos las caras que van poniendo, siempre les preguntamos qué les parece el panorama… No pondremos la frase más corriente que nos suelen decir (porque sonaría altamente coloquial), pero les asusta.

Cierto es que desde un punto de vista global, la situación parece grave. Y no sólo lo parece, lo es. Pero esto no debe ser óbice para retirarse de Internet, para no utilizar la banca online o las tiendas, para no participar en redes sociales... para no disfrutar de todo lo bueno que tiene la Red.

Sólo significa que hemos de ser cautos y precavidos y estar preparados y alerta ante cualquier cosa que pueda suceder. Siempre decimos que también en el mundo físico hay mucha delincuencia (quizá cada vez más por la recesión económica), y no por ello dejamos de salir a la calle y hacer nuestra vida normal. Pero, eso sí, andamos más alerta y no corremos riesgos.

2011 seguro que será mucho más interesante, y quizá más peligroso. Pero seguir trabajando en pro de la seguridad desde todos los ámbitos, tanto públicos como privados, nos hará seguir avanzando en algo que creemos que es difícil de erradicar, pero no imposible.

Esperamos que hayan entrado con el pie derecho en el nuevo año y que éste les traiga muchas cosas buenas… también en el ámbito de la seguridad. Feliz 2011!

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/**