INFORME ANUAL PANDALABS

RESUMEN 2013

PANDA SECURITY

01| Introducción

Vamos a analizar los acontecimientos más destacables sucedidos durante 2013 en el mundo de la seguridad informática. También analizaremos las cifras respecto a malware recogidas por PandaLabs, el laboratorio de Panda Security, en las que podremos ver las principales tendencias tanto en la creación de malware como en el estado de salud del mundo en cuanto a infecciones.

Las noticias más destacables producidas durante 2013 tienen como protagonistas a diferentes gobiernos por sus acciones de ciberespionaje a nivel mundial. Al contrario de lo que hasta ahora venía siendo habitual -China protagonizando este apartado-, durante 2013 las revelaciones realizadas por el antiguo trabajador de la Agencia de Seguridad Nacional (ASN) norteamericana, Edward Snowden, han puesto a la NSA y al gobierno norteamericano en el ojo del huracán, ya que la polémica por los diferentes casos de espionaje que han llevado a cabo no han dejado a nadie indiferente.

En otro orden de cosas, vamos a ver cuál es la evolución en el mundo móvil y diferentes ataques producidos a todo tipo de plataformas. Android será el principal protagonista de esta área, al ser la favorita de los ciberdelincuentes para robar información y dinero a los usuarios, y veremos cómo estamos hablando de amenazas que ya no son anecdóticas.

Hablaremos de las redes sociales, y veremos cómo los casos de secuestro de cuentas de empresas y personajes famosos se han multiplicado a lo largo de este año, donde hasta el mismísimo presidente de Estados Unidos, Barack Obama, fue testigo de cómo su cuenta de Twitter era hackeada. Finalmente trataremos de vaticinar lo que nos podemos encontrar durante los próximos 12 meses en el apasionante mundo de la seguridad informática.

02| 2013 en cifras

A lo largo de 2013 han aparecido 30 millones de nuevas muestras de malware, 82.000 al día. En total tenemos registradas 145 millones de muestras de malware en PandaLabs. Los números -en cierto modo esperados vista la tendencia de los últimos 12 meses- no dejan de sorprender, y es que estamos hablando de que el 20% de todo el malware que ha existido en la historia fue creado el año pasado. En un año protagonizado por todo tipo de ataques, como el famoso virus de la policía, y con el resurgimiento del ransomware, con Cryptolocker como máximo exponente , la categoría de malware más popular continúan siendo los troyanos. Veamos los datos en detalle sobre la creación de malware a lo largo de 2013.

Nuevo malware creado en 2013, por tipo

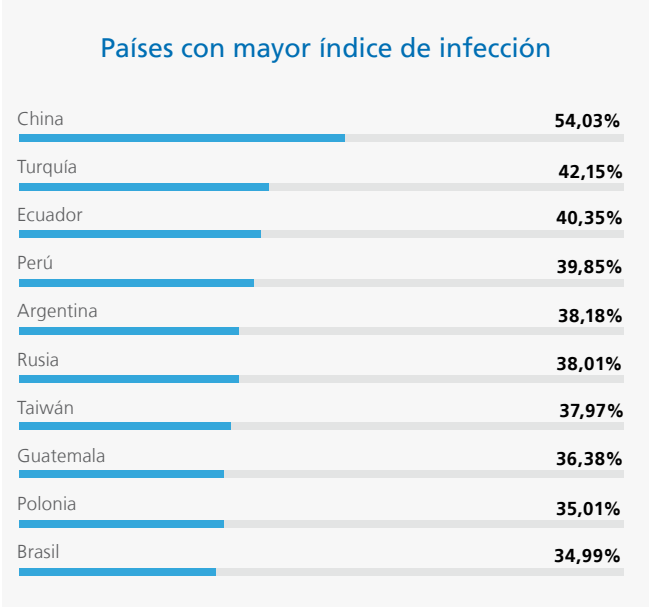
Troyanos	**71,11%**
Virus	**13,30%**
Gusanos	**8,49%**
Adware /Spyware	**6,93%**
Otros	**0,17%**

Si comparamos las cifras con las del año anterior, lo que más destaca es el aumento de los virus, pasando del 9,67% al 13,30% en 2013. La explicación viene principalmente de dos familias de virus, Sality y Xpiro. La primera existe desde hace varios años, mientras que la segunda es algo más reciente, siendo capaz de infectar ficheros ejecutables tanto de 32 como de 64 bits. Lo que explica que estos virus sean tan populares es que una de sus funcionalidades incluye el robo de información, lo que implica que hay ciberdelincuentes propagándolos activamente para obtener un beneficio económico.

Si analizamos las infecciones causadas por el malware en el mundo, gracias a los datos aportados por la Inteligencia Colectiva, vemos que las infecciones también están protagonizadas por los troyanos con un 78,97%. Parece que los ciberdelincuentes han conseguido infectar con troyanos más ordenadores que en años anteriores. En 2011 el porcentaje de ordenadores infectados con troyanos era del 66% y en 2012 llegó al 76%, con lo que se consolida la tendencia de uso de este tipo de malware por parte de los ciberdelincuentes. Veamos cómo se reparten las infecciones en todas las categorías.

Si miramos al porcentaje global de ordenadores infectados, este es del 31,53%, muy similar al del año anterior. **A nivel geográfico los países más infectados del mundo están liderados por China**, con un 54,03% de infecciones, seguida de Turquía –con un índice de infección sensiblemente más bajo, 42,15%- y Ecuador con un 40,35%.

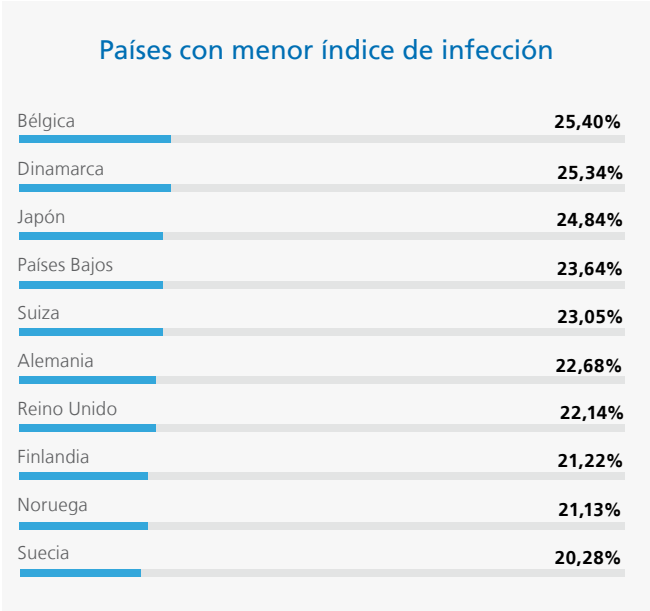
A continuación podemos ver los 10 países con mayor índice de infección.



Asia y Latinoamérica son las regiones con mayores infecciones. El resto de países con un porcentaje mayor a la media mundial son Uruguay (33,64%), Chile (33,51%), España (32,72%) y Colombia (32,22%).

Si analizamos los datos de los países mejor posicionados, aquellos cuyo índice de infección es más bajo, podemos observar que nueve de ellos son europeos, siendo Japón el único país no perteneciente al Viejo Continente. Los países escandinavos copan las primeras posiciones: Suecia se sitúa a la cabeza, con un 20,28% de infecciones, seguido de cerca por Noruega, con un 21,13% y en tercer lugar está Finlandia, con un 21,22% de infecciones.

A continuación podemos ver los 10 países con menor índice de infección.



El resto de países con un porcentaje de infección menor a la media mundial son Portugal (25,28%), Francia (25,68%), Australia (26,84%), Austria (27,69%), Canadá (27,82%), Estados Unidos (28,96%), Venezuela (29,83%), Hungría (30,96%), México (31,00%), Italia (31,47%) y Costa Rica (31,50%).

03| 2013 de un vistazo

A lo largo de este año, hemos visto cómo multitud de importantes empresas han sido objeto de ataques de todo tipo.

CIBERCRIMEN

El 1 de Febrero, **Twitter** publicó un artículo en su blog (en inglés, "*Keeping our users secure*"), explicando cómo la propia compañía había sido víctima de un ataque que ha permitido el acceso fraudulento a información de 250.000 usuarios de la red social.

Un par de semanas más tarde, **Facebook** publicaba un artículo en su blog, titulado "*Protecting People On Facebook*" (en inglés), anunciando que había sufrido el mismo ataque que Twitter, aunque, aparentemente, en esta ocasión no fueron comprometidos datos de clientes.

La siguiente víctima fue **Apple**. Sólo unos pocos días después del anuncio de Facebook, representantes de Apple comunicaron a *Reuters* que también habían sido vulnerados.

Y finalmente, aunque no menos importante, **Microsoft** reconoció haber sufrido también esta misma agresión.

No es una mala lista de empresas, ¿verdad? En principio ninguna otra gran compañía ha declarado públicamente ser víctima de este ataque, del que podemos sacar dos puntos positivos:

- Las empresas no tienen miedo de reconocer ser objetivo de este tipo de agresiones.
- Todas las compañías atacadas cuentan con buenos equipos de seguridad que han sido capaces de identificar los ataques mientras estaban en curso.

Como denominador común, todos estos ataques utilizaron un agujero de seguridad en Java desconocido hasta el momento y para el que no existía parche, lo que se conoce como una vulnerabilidad zero day ó 0-day.

Twitter, **Facebook**, **Apple** y **Microsoft** fueron víctimas de un sofisticado ataque que consiguió infectar a empleados de las cuatro empresas a través de un agujero de seguridad en Java

Las personas involucradas en seguridad informática saben que no existe un lugar 100% seguro. Es posible tomar un gran número de medidas preventivas, y funcionarán bien la mayoría de las veces. Pero siempre existirá algún punto débil, una nueva vulnerabilidad, algún error humano, y de los miles de ataques que compañías tan grandes reciben constantemente, uno podría tener éxito.

Y en este punto, ser capaz de identificar un ataque que está ocurriendo en este mismo momento es crítico. Y Twitter, Facebook, Apple y Microsoft fueron capaces de ello. Todas estas empresas están recogiendo información sobre la agresión en cuestión. Todas están trabajando con la policía para averiguar quién está detrás del proceso.

Si eres responsable de una pequeña o mediana empresa, puedes pensar que no tienes que preocuparte tanto por la seguridad como estos gigantes, ya que no eres un objetivo tan aparentemente "sexy". Y es parcialmente cierto, probablemente recibirás un número muy pequeño de ataques dirigidos (o incluso ninguno), sin embargo, serás bombardeado con los ataques de ciberdelincuentes que infectan millones de ordenadores. Y a los ciberdelincuentes les encantan los objetivos fáciles. Si tienes ordenadores sin protección, con software desactualizado, sin una estrategia seria de seguridad, serás el próximo blanco.

La mayoría de infecciones hoy en día se producen a través de los conocidos como "exploit kits", que infectan los ordenadores de los usuarios sin su conocimiento a través de alguna vulnerabilidad. Más del 90% de estos casos son vulnerabilidades de Java a través del navegador. Los ataques que recibieron Microsoft, Apple, Facebook y Twitter este mismo trimestre utilizaron Java. La mayoría de infecciones del "Virus de la Policía" consiguen llegar a los ordenadores de sus víctimas gracias a que estas tienen versiones desactualizadas de Java.

Java continúa siendo uno de los principales vectores de infección mediante el que los ciberdelincuentes logran comprometer a sus víctimas

¿Cuál es el mejor método para evitar estas infecciones? Muy sencillo: basta con eliminar Java de tu navegador. Si por algún motivo necesitas Java en el navegador para utilizar alguna aplicación, utilízala en un navegador secundario que sólo utilices para dicha tarea.

Evernote fue víctima de una intrusión que hizo a la empresa lanzar un comunicado pidiendo a más de 50 millones de usuarios que cambiaran su contraseña. La página web de la **Reserva Federal estadounidense** fue atacada, según un comunicado que publicó la propia entidad, aunque no aclaraba si hubo algún tipo de robo de información. Sin embargo, coincidió con la publicación, por parte de Anonymous, de datos personales de 4.000 ejecutivos de la banca estadounidense, lo que hace pensar que el ataque sufrido por la FED fue llevado a cabo por este grupo. La NASA fue víctima también de una intrusión. A través de la popular web Pastebin se publicó información interna que incluía direcciones de correo, nombre reales, contraseñas…

En muchas ocasiones los ciberdelincuentes tratan de aprovecharse de diferentes eventos, fechas señaladas, o noticias de gran impacto para tratar de propagar malware y conseguir nuevas víctimas. Pudimos ver que durante el segundo trimestre de 2013, utilizaron el atentado sucedido durante la maratón de Boston (EE.UU) para enviar spam con dicha temática. Los mismos ciberdelincuentes aprovecharon también el accidente ocurrido en una planta de fertilizantes en Tejas (EE.UU) para lanzar el mismo tipo de ataque.

El atentado sucedido en la maratón de Boston fue utilizado por ciberdelincuentes para propagar **malware** a través de mensajes de spam hablando del suceso

Otro tipo de ataque utilizando fechas señaladas fue el que tuvo lugar el 1 de Mayo, Día Internacional de los Trabajadores. La página web del Ministerio de Trabajo estadounidense (US Department of Labor) fue comprometida ese mismo día y comenzó a propagar malware.

Cuando hablamos de ciberdelincuentes infectando los ordenadores de usuarios para robar sus datos y enriquecerse, lo primero que nos viene a la mente es el robo de credenciales de banca online para hacerse pasar por nosotros y vaciar nuestras cuentas bancarias. Sin embargo hay otros tipos de robo, más imaginativos, que aunque parecidos tienen lugar en mundos virtuales. En este caso, World of Warcraft, el

MMORPG más jugado del mundo, vio cómo ciberdelincuentes comenzaron a robar oro de las cuentas de diferentes jugadores. Desaparecieron millones de piezas de oro. Al investigar el caso, se vio que alguien había utilizado ese oro para comprar diferentes ítems a través de la casa de subastas del juego. Finalmente se descubrió que los atacantes habían utilizado un error en la aplicación web y de móvil que permite acceder a la casa de subastas.

Un error en la aplicación para móviles World of Warcraft Armory fue utilizado por ciberdelincuentes para robar millones de piezas de oro

La federación de pequeñas empresas (FSB, Federation of Small Businesses) británica emitió un informe donde revelaba que el 41% de las pequeñas cuentas habían sufrido ataques por parte de ciberdelincuentes a lo largo del año 2012, con un coste de 785 millones de libras.

La empresa **LivingSocial** fue víctima de un ciberataque que podía afectar a más de 50 millones de clientes. Entre la información comprometida, se encontraban nombres, direcciones de correo, fechas de nacimiento y contraseñas cifradas.

El grupo **Syrian Electronic Army** ha continuado protagonizando diferentes ataques durante todo el año. En julio, a través de un ataque de phishing, consiguió comprometer las cuentas de Gmail de tres trabajadores encargados de labores de social media en la Casa Blanca. Una vez comprometidas estas cuentas, fueron utilizadas para enviar e-mails fraudulentos a otros objetivos de la Casa Blanca.

En agosto, el mismo Washington Post publicó una nota confirmando que habían sido víctimas de hacking,y que algunos de sus lectores habían sido redirigidos a páginas de la propia Syrian Electronic Army.

El Grupo **Syrian Electronic Army** se ha mostrado especialmente activo este trimestre. Entre sus víctimas se cuentan el New York Times, Twitter e incluso trabajadores de la Casa Blanca

Semanas más tarde, el New York Times y la red social Twitter fueron también víctimas de este grupo. En este caso, ninguna de las dos empresas fueron hackeadas, sino que se utilizó una técnica denominada DNS poisoning, mediante la cual los usuarios eran redirigidos a otra página cuando tecleaban la dirección web de cualquiera de los dos sitios web. Si se accedía a las páginas web utilizando la dirección IP, podía accederse a ambos sin problemas.

Este tipo de ataque, denominado DNS poisoning, no es algo nuevo, aunque es cierto que en los últimos meses se ha venido popularizando. En Malasia, un número muy importante de páginas web del país fueron víctimas de este tipo de agresión, afectando a la versión local de páginas web de empresas como Google, Microsoft o Kaspersky, entre otras.

A lo largo de 2013 hemos constatado un aumento de ataques utilizando la técnica DNS poisoning

El "**Virus de la Policía**" ha seguido causando estragos a través de numerosas variantes que han tratado de infectar a los usuarios, y es que a pesar de la desarticulación de una de las bandas responsables de estos ataques que hemos referido anteriormente, aún hay muchos ciberdelincuentes lanzando este tipo de ofensivas. Nos llamó especialmente la atención uno de ellos, debido al alto coste de la "multa", ya que aunque el precio habitual suele rondar los 100 $/€, en este caso la suma solicitada ascendía a 300 $/€.

Pero si una amenaza se ha ganado un nombre propio durante este año esta es sin duda CryptoLocker. Se trata de un troyano que utiliza tácticas de ransomware, cifrando todos los ficheros de datos importantes del usuario y pidiendo un rescate para volver a recuperarlos.

CryptoLocker es una nueva familia de malware que secuestra documentos y pide un rescate por ellos

Si bien este tipo de ataques no es nuevo, existen ciertas características que han conseguido que tengan más éxito a la hora de cobrar el rescate solicitado a las víctimas:

- En vez de cifrar todo tipo de ficheros, se centra solamente en aquellos que los usuarios más pueden valorar: fotos, vídeos, documentos de texto, etc.
- No sólo cifra ficheros en el disco, sino que también puede hacerlo en unidades que estén en la misma red local.
- El cifrado es asimétrico, por lo que se necesita obligatoriamente la clave que los ciberdelincuentes tienen para recuperar los datos, siendo inviable la utilización de herramientas específicas para poder recuperar los ficheros.
- En el mensaje que aparece para poder pagar el rescate aparece una cuenta atrás, lo que fuerza a la víctima a tener que tomar una decisión: pagar o perder todos sus datos.

Si tuviéramos que destacar un ataque de entre todos los sucedidos a lo largo del año, este sería el que sufrió Adobe.

En un primer momento, la compañía hizo público que había sido víctima de un ataque en el que le habían robado código fuente de sus productos e información personal –incluyendo contraseñas- de casi tres millones de clientes.

Poco tiempo después de conocerse la noticia se publicó en Internet un fichero que contenía 150 millones de nombres de usuario y hashes de sus respectivas contraseñas. La compañía reconocía entonces que el número de usuarios afectados no era el anunciado en un principio, y subía esa cifra al menos hasta los 38 millones.

Casi dos millones de usuarios de Adobe utilizaban como contraseña "123456"

La publicación de estos datos posibilitó que se pudiera ver qué contraseñas se repetían más, y aplicando el mismo tipo de hash usado por Adobe a los passwords más comunes se descubrió cuáles eran los más utilizadas por los usuarios, dando lugar a un resultado desolador, donde podemos ver cómo la seguridad a la hora de seleccionar una contraseña brilla por su ausencia. Las tres más populares eran las siguientes (entre paréntesis, el número de usuarios de Adobe que las utilizaban):

"123456" (1.911.938 usuarios)
"123456789" (446.162 usuarios)
"password" (345.834 usuarios)

CIBERDELINCUENCIA

El año comenzaba con buenas noticias, cuando el pasado 11 de Enero la Comisión Europea inauguró el European Cybercrime Center (EC3) con el objetivo de ayudar a los estados miembros de la Unión Europea a luchar contra los ciberataques. Los ciberdelincuentes siempre se aprovechan de lo complicada que puede ser la coordinación policial entre diferentes países para llevar a cabo sus fechorías, por lo que este tipo de iniciativas siempre son bienvenidas.

La Comisión Europea estrenó en 2013 el European Cybercrime Center (EC3) con el objetivo de ayudar a los estados miembros de la Unión Europea a luchar contra los ciberataques

También en Enero, el FBI hizo pública una investigación que comenzó en 2010 y que ha conseguido detener a una banda de ciberdelincuentes que había conseguido infectar a más de un millón de ordenadores desde 2005. Esta operación es de destacar, entre otros motivos, por lo que significa respecto a la coordinación entre diferentes países: el FBI contó con la colaboración de las fuerzas de seguridad de Letonia, Moldavia, Rumanía, Holanda, Alemania, Finlandia, Suiza y Reino Unido.

Uno de los grandes protagonistas de los últimos tiempos en lo que a infecciones se refiere es el conocido como "**Virus de la Policía**". En Febrero volvió a saltar a las portadas, pero esta vez por un motivo muy diferente, ya que la noticia era que nuestros amigos de la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional en colaboración con Europol y con Interpol habían desmantelado la banda de ciberdelincuentes responsable del "Virus de la Policía". Según el comunicado *publicado por el Ministerio del Interior* español, en total fueron detenidas 10 personas pertenecientes a una de las células financieras del grupo, que manejaba un millón de euros al año, dinero obtenido de las víctimas del malware. Seis de ellos son ciudadanos rusos, dos ucranianos y dos georgianos, todos ellos residentes en España.

La Brigada de Investigación Tecnológica (BIT) de la Policía Nacional en colaboración con Europol y con Interpol desmanteló una banda de ciberdelincuentes responsable del "Virus de la Policía"

Además fue detenido el cabecilla de toda la operación, se trata también de un ciudadano ruso. Curiosamente, a pesar de ser residente ruso, fue detenido en Dubai (Emiratos Árabes Unidos) mientras se encontraba de vacaciones.

En una operación conjunta, las policías rusa y ucraniana detuvieron al líder de la banda de ciberdelincuentes responsable de la red de bots Caberp, junto con otras 20 personas que formaban parte del equipo de desarrollo del malware. El líder de la banda tiene 28 años y se trata de un ciudadano ruso que reside en Ucrania.

EL gobierno norteamericano protagonizó durante el segundo trimestre de 2013 uno de los grandes golpes al aparato financiero de las bandas de ciberdelincuentes de todo el mundo cuando cerró Liberty Reserve, conocido como el "banco preferido de los ciberdelincuentes". Esta empresa permitía hacer transacciones monetarias de forma anónima, y, tras una investigación de varios años, se arrestó a sus propietarios. No está claro qué es lo que sucederá con todo el dinero de clientes legítimos, que no realizaban ningún tipo de actividad ilegal.

Tras una investigación de varios años, Liberty Reserve fue cerrada por el gobierno norteamericano y sus propietarios fueron arrestados

El Parlamento Europeo ha aprobado que se apliquen penas más severas a delitos relacionados con ciberataques. Por ejemplo, el simple hecho de crear o utilizar una botnet (red de bots) podrá acarrear penas de al menos tres años, sin contar otros crímenes que hayan podido cometerse mediante el uso de dichas botnets.

Una de las mejores noticias del año en la lucha contra la ciberdelincuencia la tuvimos en el último trimestre, cuando se supo que "Paunch" el autor del exploit kit más famoso y más utilizado por ciberdelincuentes de todo el mundo para infectar a usuarios, BlackHole, había sido arrestado en Rusia.

REDES SOCIALES

Las redes sociales son un punto de reunión de primer orden en el mundo digital actual. Millones de usuarios las utilizan no sólo para contactar con amigos y conocidos, sino también para mantenerse informados sobre lo que sucede en el mundo. Cualquier empresa que se precie tiene cuenta en Twitter y su página de Facebook, y en el caso de las grandes marcas cuentan con muchísimos seguidores. Es esto lo que las hace especialmente atractivas para los ciberdelincuentes. Un caso llamativo fue por ejemplo el de **Burger King**, donde los atacantes al parecer lograron adivinar la contraseña de la cuenta y se hicieron con ella. Acto seguido cambiaron la imagen de fondo por la de McDonalds y comunicaron que acababan de ser adquiridos por su principal competidor.

La cuenta de Twitter de **Burger King** fue comprometida y los atacantes cambiaron la foto de perfil por una de McDonalds

La cuenta de Twitter del fabricante automovilístico **Jeep** sufrió un ataque muy similar. En este caso, se anunció que habían sido adquiridos por Cadillac. Otro tipo de hackeos en cuentas de Twitter que hemos visto tienen un tinte más político. Un grupo de ciberdelincuentes autodenominado "Syrian Electronic Army" consiguió hackear diferentes cuentas pertenecientes a diferentes organizaciones. Por lo que se ha podido saber, primero lanzaron ataques de phishing para poder obtener las credenciales de acceso a Twitter y, posteriormente, secuestrar las cuentas. Entre sus víctimas figuran Human Rights Watch, el servicio de noticias francés France 24, o el servicio meteorológico de la BBC.

Muchas veces no somos conscientes de las consecuencias que puede acarrear un ataque de este tipo, por lo que es importante ilustrarlo con ejemplos reales: el grupo "Syrian Liberation Army" hackeó la cuenta de Twitter de **Associated Press**. Una vez conseguido el control de la cuenta, publicó una falsa noticia "Breaking: Two Explosions in the White House and Barack Obama is injured", donde decía que se habían registrado dos explosiones en la Casa Blanca, y que Barack Obama había sido herido. Acto seguido, multitud de seguidores de la cuenta comenzaron a hacerse eco de la falsa noticia, lo que provocó que el Dow Jones cayera 145 puntos.

Un falso tweet desde la cuenta hackeada de **Associated Press** provocó que el Dow Jones cayera 145 puntos

Por lo que pudo saberse, los atacantes mandaron un e-mail malicioso a numerosos empleados de AP haciéndose pasar por una noticia proveniente de un importante diario norteamericano, y, para ampliar información, incluía un enlace. Si el usuario pinchaba sobre éste, era llevado a una página similar a la de Twitter, que solicitaba el nombre de usuario y password. Así fue como el grupo "Syrian Liberation Army" consiguió secuestrar la cuenta de Twitter de AP.

El mismo grupo ha continuado con los ataques, siendo una de sus víctimas la cadena norteamericana **CBS**, que vio comprometidas tres de sus cuentas de Twitter, entre ellas, la del popular programa "60 Minutes". Otra de las víctimas de este grupo fue la cuenta de Twitter del sitio de noticias de humor The Onion.

El pasado Octubre, el mismo grupo volvió a delinquir de nuevo, consiguiendo hackear la cuenta de **Twitter del mismísimo Presidente de los Estado Unidos, Barack Obama**, publicando a través de la misma dos enlaces que redirigían a vídeos con propaganda política a favor del gobierno sirio.

En Octubre, la cuenta de **Twitter de Barack Obama** fue hackeada por el grupo "Syrian Liberation Army"

No todas las noticias de redes sociales tienen que ver con ataques: **Facebook** anunció que un error expuso el número de teléfono y dirección de correo electrónico de seis millones de sus usuarios. Además, Facebook ha completado la migración de todos sus clientes a navegación segura, y ahora todos los usuarios de la red social más grande del mundo se conectan a la misma mediante HTTPS, de tal forma que todas las comunicaciones entre los dispositivos de los internautas y Facebook están cifradas, pudiendo así evitar el robo de los datos mediante la captura de la información que viaja por la Red.

Todos los usuarios de Facebook se conectan ya mediante HTTPS

MÓVILES

La práctica totalidad de noticias sobre seguridad y ataques de malware en plataformas móviles están protagonizadas por Android, que tiene la mayor cuota de mercado en este segmento. Además de los ataques habituales, hemos descubierto alguna nueva técnica curiosa digna de mención. Un malware para Android que se encontraba escondido dentro de Google Play no sólo infectaba el móvil ¡sino que está preparado para infectar el ordenador desde un smartphone o tableta! La técnica utilizada era muy sencilla: una vez que se ejecuta en el teléfono, se conecta a Internet para descargarse unos ficheros que guarda en la raíz de la tarjeta de almacenamiento del dispositivo, de tal forma que cuando se conecte al ordenador, a través del cable USB, se ejecute automáticamente uno de los ficheros, que se trata de un troyano de Windows.

En abril se descubrió un nuevo tipo de ataque a usuarios del sistema operativo Android. En este caso, se había distribuido malware a través de aplicaciones no maliciosas. Muchas aplicaciones gratuitas incluyen algún tipo de publicidad como forma de financiación, en lugar de cobrar por la aplicación. En este caso, parece que los ciberdelincuentes publicaron aplicaciones que no eran maliciosas en sí mismas, pero ellos controlaban la publicidad que mostraban. En cuanto consiguieron suficientes usuarios de estas aplicaciones, comenzaban a mostrar anuncios con falsas notificaciones de actualización de aplicaciones, que si eran instaladas en el dispositivo lo comprometían con un troyano que enviaba SMS a números de tarificación especial. Las aplicaciones publicadas eran 32, y el total de descargas de usuarios que consiguieron a través de Google Play llegaba a los nueve millones.

A lo largo de 2013 se han descubierto numerosos ataques de malware en Android a través de publicidad mostrada en aplicaciones legítimas

Si bien la cantidad de malware para Android sigue siendo baja en comparación con la de Windows, el crecimiento que está teniendo es digno de mención. Y es que, ya no estamos hablando de ataques anecdóticos, o unas pocas decenas de muestras de malware: sólo durante 2013 se han registrado más de dos millones de nuevas muestras de malware para **Android**.

Andrian Ludwig, responsable de seguridad de Android, mostró datos que aseguran que menos del 0,001% de las instalaciones de aplicaciones de Android son capaces de saltarse las defensas multi-capa que tiene el sistema. Las estadísticas pueden mostrar diferentes realidades, pero lo que es innegable es que Android es la plataforma móvil más atacada.

Los ataques en Android son llevados a cabo principalmente mediante técnicas de ingeniería social, lo que no implica que no haya vulnerabilidades y se utilicen. De hecho, hemos sido testigos en 2013 de un nuevo tipo de ataque en el que modificando un fichero APK legítimo (instalador de aplicaciones de Android) se consigue que éste instale cualquier tipo de código malicioso sin que el sistema se percate de lo que está sucediendo.

Sin embargo, no todos los ataques suceden en esta plataforma. Plataformas como iOS, el sistema operativo de Apple para teléfonos (iPhone) y tabletas (iPad) también pueden ser víctimas de agresiones. En julio, un grupo universitario de investigadores de la Georgia Tech Information Security Center (GTISC) mostró un ataque mediante el que era posible infectar un iPhone simplemente enchufándolo a un cargador.

Se ha demostrado cómo se puede infectar un iPhone simplemente conectándolo a un cargador

Apple lanzó la nueva versión de iOS, la 7, que, además de cambios estéticos y de funcionalidad, corregía 80 vulnerabilidades diferentes, entre las que se encontraba la aquí descrita. Sin embargo, en unas pocas horas aparecieron nuevos problemas de seguridad en iOS 7: uno de ellos, por ejemplo, permitía saltarse el código de desbloqueo.

En Noviembre, tuvo lugar el "Mobile Pwn2Own 2013", evento en el que se tratan de descubrir nuevas vulnerabilidades en dispositivos móviles. Allí se vieron ataques de todo tipo, desde un robo de credenciales de Facebook en un iPhone 5 con la versión más reciente de iOS, a vulnerabilidades que permiten el robo de datos a través de aplicaciones instaladas por defecto en un Samsung Galaxy S4, sin olvidar un ataque a través de Chrome en un Nexus 4, u otro en una tablet con Windows 8.1 a través de Internet Explorer 11… Nadie quedó libre.

CIBERESPIONAJE

China suele ser uno de los países protagonistas de esta sección, y de hecho comenzó el año acaparando numerosas portadas, hasta que las revelaciones hechas por el antiguo trabajador de la NSA Edward Snowden eclipsaron el resto de noticias de esta temática. Veamos las noticias que protagonizó el gigante asiático antes de analizar el escándalo provocado por las acciones de ciberespionaje de la **NSA**.

El 30 de Enero, el diario norteamericano **The New York Times** publicaba en portada una noticia en la que explicaba cómo había sufrido un ataque en el que habían entrado en sus ordenadores y les habían estado espiando durante cuatro meses. Casualmente, el ataque se produjo justo después de un artículo de investigación publicado en el diario donde se contaba cómo Wen Jiabao -primer ministro chino- y su familia habían amasado una fortuna de miles de millones de dólares.

El New York Times, The Wall Street Journal y The Washington Post denunciaron haber sido víctimas de ataques con motivaciones políticas con origen en China

Un día más tarde, el diario económico **The Wall Street Journal** anunció que también habían sido víctimas de un ataque similar por parte de lo que parecían ser hackers chinos. El gobierno chino, ofendido por lo que consideran como ataques injustificados, protestó y Hong Lei - Ministro de Asuntos Exteriores de China- hizo unas declaraciones alegando que insinuar que los ataques venían de China "era algo irresponsable y poco profesional", ya que todo estaba basado en meras especulaciones (*"It is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence"*).

Curiosamente, en estos incidentes los atacantes lograron acceder a todo tipo de información de los medios (datos de clientes, etc.), sin embargo, se centraron únicamente en acceder

a información de periodistas y empleados tratando de encontrar cualquier referencia a investigaciones periodísticas sobre China, principalmente buscando las fuentes utilizadas para elaborar los artículos de investigación sobre el país asiático.

El día siguiente a la revelación de The Wall Street Journal, otro gigante de los medios norteamericanos, **The Washington Post**, hizo público que ellos también habían sufrido un ataque similar en 2011, con origen de nuevo en China.

Semanas más tarde, la compañía norteamericana Mandiant publicó un demoledor informe de 76 páginas (APT1: Exposing One of China's Cyber Espionage Units, *http://intelreport.mandiant.com/*) donde detallaba cómo la Unidad 61398 del ejército chino estaba especializada en ataques de ciberespionaje. El informe revela más de 3.000 evidencias que demuestran cómo esta unidad llevaba en marcha al menos desde el año 2006, robando información en, como mínimo,141 organizaciones de todo el mundo.

Es posible que no nos percatemos de la importancia que tiene este informe de Mandiant y de las repercusiones que puede tener a medio / largo plazo. Demostrar quién está detrás de cualquier ataque es algo muy complejo, incluso en casos de ciberdelincuencia normales. Cuando hablamos de ciberespionaje es aún más complicado por el simple hecho de que quien está detrás del ataque es gente altamente cualificada y con medios más que suficientes para ir cubriendo su rastro.

Desde hace años, todas las miradas se volvían a China cada vez que se daba un caso de este tipo, pero sin pruebas reales de que realmente el gobierno chino estuviera detrás de los mismos. Ahora, por primera vez, se ha demostrado que el ejército chino está activamente realizando labores de espionaje a nivel mundial, infiltrándose en empresas de todos los sectores y robando información.

La semana siguiente a la publicación del informe de Mandiant siguieron apareciendo noticias de casos de ciberespionaje que apuntaban a China: EADS (European Aeronautic, Defence and Space Company), fabricante del avión de combate Eurofighter y dueña de Airbus, fue atacada por hackers de origen chino, según el diario alemán Der Spiegel *(http://www.spiegel.de/international/world/digital-spying-burdens-german-relations-with-beijing-a-885444.html*). En la misma noticia se hablaba también de otro ataque similar del que había sido víctima el gigante alemán ThyssenKrupp.

Hackers de origen chino consiguieron acceder a planos de más de dos docenas de sistemas de armas norteamericanos. El Washington Post consiguió acceso a un informe interno del Defense Science Board (DSB) del Pentágono donde se detallaba cómo habían obtenido acceso de misiles Patriot o de diferentes cazas en desarrollo, como el F-35.

> Hackers chinos robaron planos del caza F-35, entre otros sistemas armamentísticos

En cualquier caso, no es algo nuevo que ataques cuyo origen es claramente chino tengan como objetivo Estados Unidos. De hecho, el mismo Pentágono en su informe anual en el Congreso acusó a China de estar detrás de numerosos ataques cuyo objetivo es hacerse con secretos norteamericanos.

Según un informe de la Oficina de Seguridad Nacional de Taiwán, la "ciberarmada" china no deja de crecer y cuenta ya con unos 100.00 efectivos.

Todos estos ataques causan gran preocupación en los diferentes gobiernos, que tratan de tomar medidas. Uno de los últimos en anunciar la creación de un cibercomando fue Indonesia; su ministro de defensa anunció que el principal objetivo de la nueva unidad será protegerse de ciberataques dirigidos a webs gubernamentales.

NSA y la violación de la privacidad en nombre de la seguridad

El 6 Junio de 2013 fue cuando la noticia saltó a las portadas de los principales medios de comunicación de todo el mundo: la **NSA** se dedicaba a espiar de forma indiscriminada tanto a individuos como a empresas. Y había pruebas.

Según el Washington Post, la Agencia de Seguridad Nacional norteamericana, NSA en sus siglas en inglés, había estado espiando "a todo el mundo" a través de un programa llamado PRISM, y para ello había contado con la ayuda voluntaria de nueve gigantes del sector tecnológico: Microsoft, Apple, Google, Yahoo, Facebook, Youtube, Skype, AOL, y PalTalk. Según se decía, la NSA podía obtener todos los datos que quisiera de todos los clientes de esas compañías. Rápidamente, medios y agencias de todo el mundo se hicieron eco de lo publicado por el diario norteamericano.

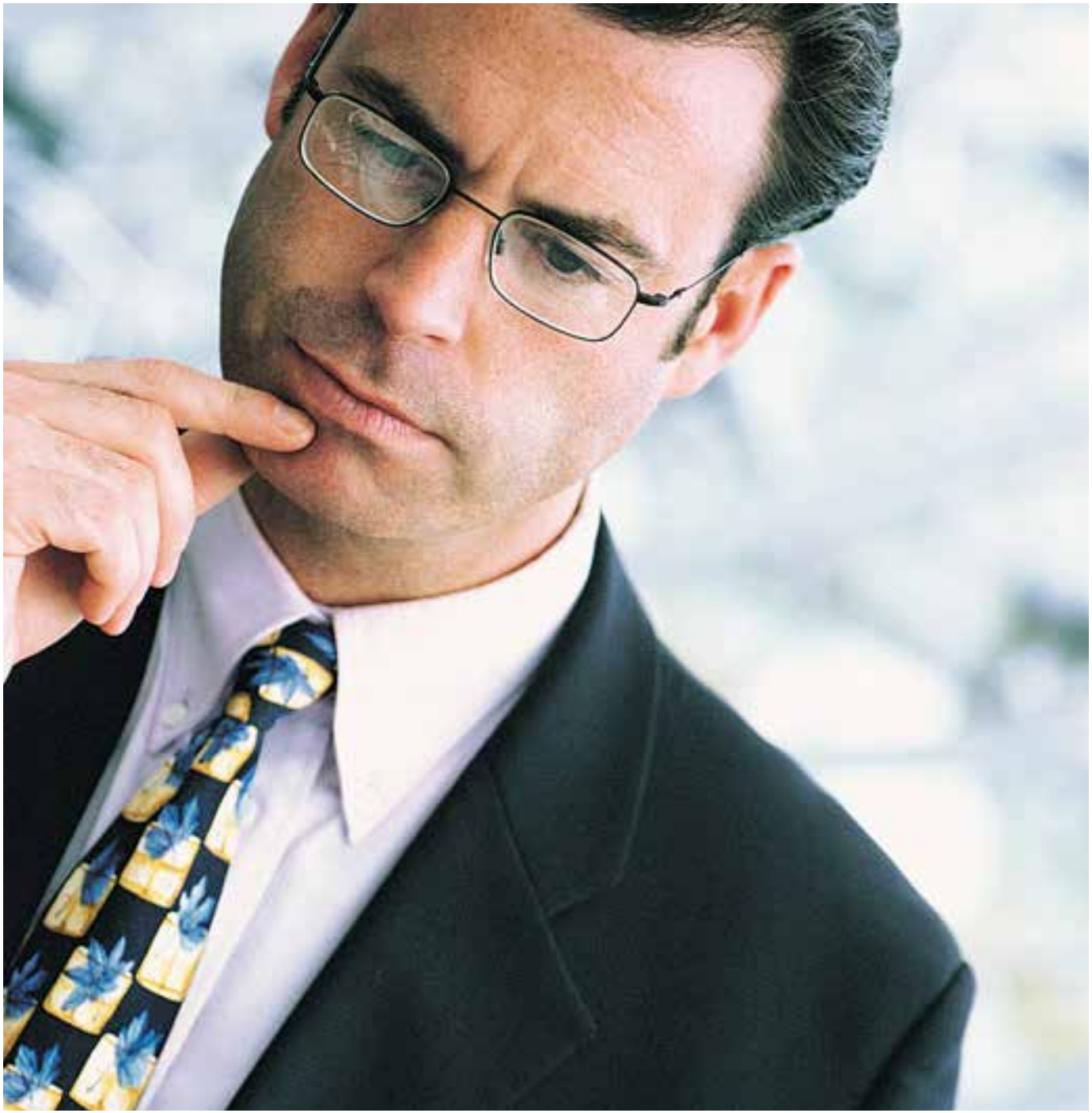
> La NSA fue protagonista al hacerse público su programa PRISM mediante el que puede obtener datos de usuarios de las más populares plataformas online

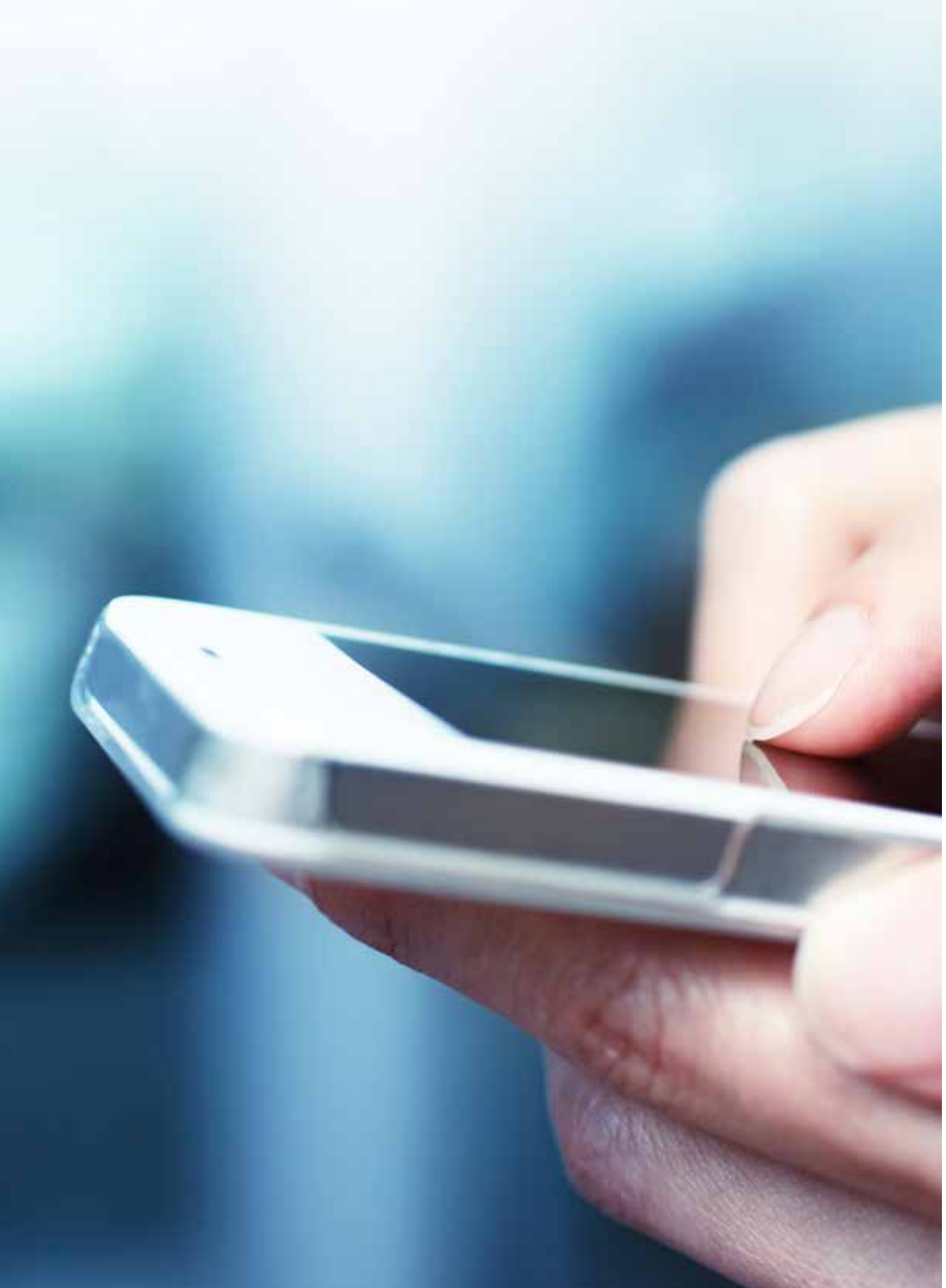
Dichas compañías negaron categóricamente esto. De hecho, el mismo Washington Post cambió la noticia publicada el día anterior, modificando el titular y eliminando partes como en la que se decía que las empresas estaban voluntariamente facilitando todo tipo de datos de sus clientes a la NSA. Ante el escándalo del espionaje realizado por la NSA, grandes empresas han demandado al gobierno norteamericano una mayor transparencia en los programas de vigilancia. En concreto, están pidiendo que les dejen hacer pública la cantidad de peticiones de información que reciben del gobierno, y diferente información relacionada con estas peticiones.

La NSA incluyó un backdoor en un conocido algoritmo de generación de números pseudoaleatorios, cuyo uso era recomendado por importantes organismos oficiales

Dentro de las revelaciones que han sido dadas a conocer desde junio, se ha sabido que la NSA había incluido un backdoor en el Dual EC_DRBG, un algoritmo de generación de números pseudoaleatorios que había sido certificado por los más importantes organismos internacionales. De hecho, días más tarde, la compañía de seguridad RSA envió un comunicado a sus clientes para que no utilizaran dicho algoritmo, que estaba implementado por defecto en dos de sus productos. Pero esto no era todo: el escándalo fue mayúsculo cuando se publicaron informaciones que indicaban que RSA había cobrado 10 millones de dólares de la NSA a cambio de incluir la mencionada puerta trasera en el algoritmo.

Pero los escándalos no quedan aquí. Si quisiéramos detallar los diferentes casos desvelados, haría falta publicar un libro, y parece que cuando crees que no han podido llegar tan lejos, los hechos hacen ver cómo nuestros peores temores se hacen realidad. Han recopilado información de miles de millones de llamadas telefónicas, hackeado empresas como Google para obtener acceso a sus datos, infectado decenas de miles de ordenadores de todo el mundo para robar información, e incluso han llegado a espiar las llamadas de la canciller alemana Angela Merkel… Nada es suficiente y las consecuencias de lo que ha sucedido se notarán durante años





04| Tendencias 2014

Creación de malware. 2014 será el año de la historia en el que más malware se cree. La mayoría de este nuevo malware serán variantes conocidas que mediante diferentes técnicas cambian de forma para evitar que los productos de seguridad puedan detectarlas.

Vulnerabilidades. Java ha sido la causa de la mayoría de infecciones ocurridas a lo largo de 2013, y todo indica que lo seguirá siendo a lo largo del año 2014. El hecho de que se encuentre instalado en miles de millones de ordenadores y que tenga un número aparentemente infinito de agujeros de seguridad, hace que sea una de las elecciones predilectas por parte de los ciberdelincuentes. No existe en el mercado negro un Exploit Kit que se precie que no incluya al menos un puñado de vulnerabilidades de Java en su "menú".

Ingeniería Social. La ingeniería social es un apartado en el que los ciberdelincuentes han brillado por su creatividad. Tras el uso de vulnerabilidades, la segunda causa de las infecciones que sufren los usuarios son ellos mismos, tras caer víctimas de algún engaño. Aunque muchos de ellos llegarán a través de emails, la mayoría tendrán lugar en redes sociales.

Móviles. Android seguirá siendo el principal objetivo de los ciberdelincuentes, y se batirá un nuevo récord de amenazas para esta plataforma.

Ransomware. Junto con los troyanos bancarios y bots, los protagonistas de los ataques que amenazarán a los usuarios serán aquellos que utilizan técnicas de ransomware: pidiendo un rescate para volver a utilizar el equipo, poder recuperar información (CryptoLocker), eliminar una supuesta infección (Falso Antivirus) o incluso pagar una supuesta multa (Virus de la Policía). Es un método mediante el que los ciberdelincuentes pueden obtener una ganancia económica directa, motivo por el que estos ataques aumentarán e incluso se extenderán a otro tipo de dispositivos, como los smartphones.

Seguridad en empresas. Ante ataques cada vez más agresivos (como los llevados a cabo por Cryptolocker), las empresas demandarán medidas extras de seguridad que vayan mucho más allá de la protección que les proporciona un antivirus "tradicional".

Internet of Things. El número de dispositivos conectados a Internet no deja de aumentar, y va a seguir por este camino. Cámaras IP, televisores, o reproductores multimedia ya forman parte de Internet, y en muchos casos además cuentan con una característica que los diferencia de los ordenadores, móviles y tabletas: raramente son actualizados por parte de los usuarios. Esto significa que son extremadamente vulnerables a agujeros de seguridad, por lo que es muy probable que comencemos a ver ataques que tengan como objetivo este tipo de dispositivos.

05| Conclusión

Durante los próximos 12 meses vamos a tener que estar especialmente atentos a las amenazas para dispositivos Android, ya que están en pleno auge y veremos nuevos ataques con el objetivo claro de robar dinero e información a los usuarios.

Las revelaciones llevadas a cabo por Edward Snowden aún no han finalizado, y seguramente veamos nuevas noticias sobre diferentes programas de espionaje a los ciudadanos de forma indiscriminada. Esta violación continua de la privacidad de los ciudadanos seguirá acaparando titulares en la prensa, aunque aún están por ver las consecuencias que tendrá.

Las empresas son las "presas" más deseadas por los ciberdelincuentes. Ya no sólo tienen que preocuparse de infecciones producidas por comportamiento imprudente de un trabajador, sino que saben que van a ir a por ellas para tratar de robar información. Es por esto que van a tener que desplegar medidas de seguridad más completas, que les permitan tener un control de todo lo que está sucediendo en su red, controlando la ejecución de todo el software en el parque informático y vigilando el acceso a los datos, con un control de quién y cuándo accede a qué información.

En el blog de PandaLabs, *http://pandalabs.pandasecurity.com/* podréis tener acceso a todos los avances y descubrimientos que haremos desde el laboratorio.

06| 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 de 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/

07| Panda en la Red

facebook
https://www.facebook.com/PandaSecurity

twitter
https://twitter.com/PandaComunica

google+
https://plus.google.com/b/114692356211770437886/114692356211770437886/posts

youtube
http://www.youtube.com/pandasecurity1

linkedin
http://www.linkedin.com/company/panda-security