PANDALABS

THE EYE OF SECURITY

# INFORME TRIMESTRAL

T2 2014

PANDA SECURITY | *The Cloud Security Company*

INTRODUCCIÓN

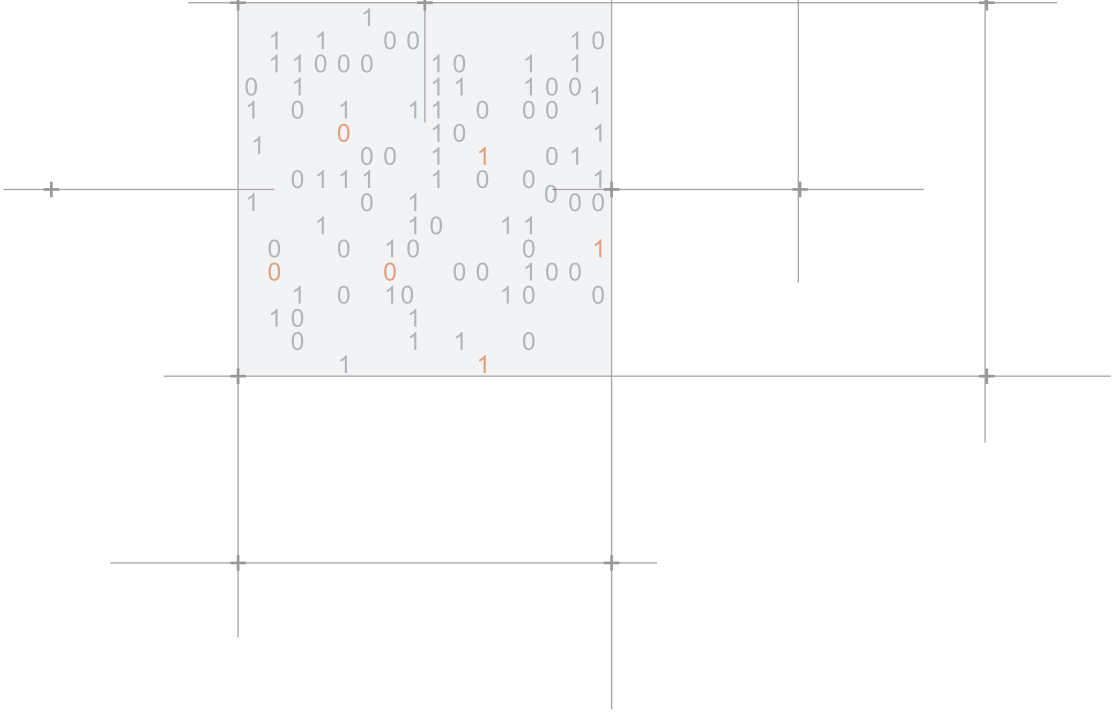
EL TRIMESTRE EN CIFRAS

EL TRIMESTRE DE UN VISTAZO

CIBERCRIMEN
REDES SOCIALES
MÓVILES
CIBERGUERRA

CONCLUSIÓN

SOBRE PANDALABS



# INTRODUCCIÓN

Analizamos en este informe lo sucedido en el mundo de la seguridad durante el segundo trimestre del año.

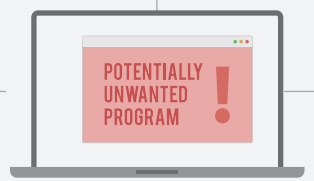
## La creación de malware a nivel mundial sigue la tendencia registrada a comienzos de 2014, alcanzando cifras récord nunca antes vistas

Los usuarios están sufriendo el ataque de numerosas aplicaciones que instalan software quizás no malicioso como tal, pero no deseado por ellos mismos. Se trata de **PUPs (Potentially Unwanted Programs)** cuyo impacto analizaremos algo más en detalle en este informe.

Analizaremos hackeos sufridos por grandes empresas como **eBay, Spotify o Domino's Pizza**, así como algunos ataques protagonizados de nuevo por el grupo Syrian Electronic Army (SEA).

Veremos que los ataques a móviles no sólo tienen como protagonista a los entornos **Android**, y que **iOS** se lleva también su parte en este trimestre.

En el campo del ciberespionaje repasaremos los últimos ataques conocidos, como el sufrido por el **Ministerio de Exteriores de Bélgica**, y las consecuencias que están teniendo los últimos casos de **espionaje** sobre Internet y las medidas tomadas por algunos gobiernos al respecto.



# EL TRIMESTRE EN CIFRAS

Si comenzamos el año batiendo récords de creación de malware, este segundo trimestre no ha ido a la zaga y sigue con la misma tendencia. Desde PandaLabs hemos registrado la creación de 15 millones de muestras de malware durante los últimos tres meses, más de 160.000 nuevas muestras generadas de media cada día.

Si bien los troyanos continúan siendo el tipo de malware más común, con un 58,20% de las nuevas muestras creadas, se trata de un porcentaje sensiblemente inferior al contabilizado el anterior trimestre. Esto no se debe tanto a que haya disminuido el número de nuevos troyanos como al incremento más que considerable de PUPs (Potentially Unwanted Programs, programas potencialmente no deseados en español).

Este crecimiento en la aparición de PUPs no es casual. Durante los últimos meses hemos visto un incremento notable en la creación de software bundlers, programas que instalan en los equipos programas potencialmente no deseados –además del programa que el usuario desea instalar- sin solicitar un consentimiento claro al usuario. Aunque este tipo de software bundlers existe desde hace tiempo, han comenzado a aparecer nuevas empresas que abusan de estos programas y se lucran instalando software no deseado por el usuario sin informarle adecuadamente.

Desde Panda Security hemos decidido proteger a nuestros clientes ante este tipo de ataque, lo que se refleja en los siguientes datos de malware creado.

## NUEVO MALWARE CREADO EN EL SEGUNDO TRIMESTRE DE 2014, POR TIPO

| 58,20% | 21,35% | 19,68% | 0,39% | 0,38% |
|---|---|---|---|---|
| TROYANOS | OTROS | GUSANOS | SPYWARE ADWARE | VIRUS |

Si analizamos las infecciones que han tenido lugar en el mundo, observamos cifras similares a las de nuevos ejemplares de malware creados:

## INFECCIONES POR TIPO DE MALWARE EN EL SEGUNDO TRIMESTRE DE 2014

| 62,80% | 24,77% | 7,09% | 2,68% | 2,66% |
|---|---|---|---|---|
| TROYANOS | OTROS | SPYWARE ADWARE | VIRUS | GUSANOS |

Los troyanos continúan a la cabeza, pero podemos ver cómo los PUPs se posicionan en segundo lugar acaparando un 24,77%, lo que demuestra que este tipo de técnicas están siendo empleadas de forma masiva.

El ratio de infecciones a nivel mundial ha sido del 36,87%, con un incremento significativo respecto a los últimos trimestres, de nuevo debido a la inclusión de los nuevos PUPs.

En cuanto a los datos registrados en los diferentes países, China continúa en primera posición, alcanzando un índice de infección del 51,05%. Le siguen Perú (44,34%) y Turquía (44,12%).

## PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN

| | |
|---|---|
| CHINA | 51,05% |
| PERÚ | 44,34% |
| TURQUÍA | 44,12% |
| BOLIVIA | 43,76% |
| ECUADOR | 43,13% |
| RUSIA | 42,89% |
| ARGENTINA | 40,57% |
| TAIWÁN | 39,63% |
| EL SALVADOR | 38,51% |
| ESLOVENIA | 38,25% |

El top de países con mayor ratio de infección está copado por países asiáticos y latinoamericanos. China, de nuevo, es el único país del mundo que supera el 50% de infecciones. Otros países con un nivel de infección que supera la media mundial son: Brasil (38,19%), Polonia (38,15%), Guatemala (37,99%), Colombia (37,86%), España (37,67%), Costa Rica (37,23%), Chile (37,05%) e Italia (36,88%).

## PAÍSES CON MENOR ÍNDICE DE INFECCIÓN

| | |
|---|---|
| PAÍSES BAJOS | 26,97% |
| PORTUGAL | 26,28% |
| BÉLGICA | 26,06% |
| SUIZA | 25,78% |
| REINO UNIDO | 25,45% |
| FRANCIA | 24,88% |
| JAPÓN | 24,21% |
| ALEMANIA | 22,88% |
| NORUEGA | 22,26% |
| SUECIA | 22,13% |

Europa es la zona del mundo donde el índice de infección es más bajo, con 9 países en este ranking. El único país no europeo entre los 10 más seguros es Japón, que se sitúa en cuarta posición, con un 24,21%.

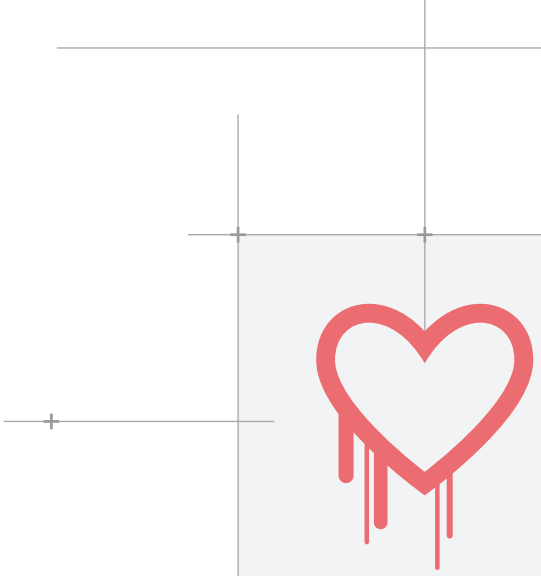
Otros países que han logrado situarse por debajo de la media mundial, son: Dinamarca (27,08%), Finlandia (27,19%), Panamá (27,25%), Canadá (27,58%), Austria (27,85%), Uruguay (28,45%), Venezuela (30,21%), Australia (31,45%), Estados Unidos (32,17%), Chequia (33,68%), México (33,99%) y Hungría (36,05%).

# EL TRIMESTRE DE UN VISTAZO

Éste ha sido un trimestre realmente activo en el mundo de la ciberseguridad. A continuación daremos un repaso a los hechos más relevantes ocurridos durante este periodo en todo el mundo.

Nada más comenzar abril, surgieron dos noticias que causaron muchísimo revuelo:

- El fin del soporte de Microsoft a uno de los sistemas operativos más populares de todos los tiempos, Windows XP, que aún es usado por millones de usuarios de todo el mundo.
- El descubrimiento de un peligrosísimo agujero de seguridad que afectaba a los más importantes sitios web de Internet, bautizado como Heartbleed.



CIBERCRIMEN

## El pasado 8 de abril era el día señalado por Microsoft para dejar de dar soporte a Windows XP

Básicamente esto significa que dejará de recibir actualizaciones de seguridad, por lo que cualquier nuevo agujero que se descubra no se solucionará. Todo ello coincidió precisamente con la aparición de un grave agujero de seguridad que afectaba a Internet Explorer y que permitía a un atacante infectar un ordenador simplemente visitando una página web que abusara de dicho error. El pánico fue tal -se habían detectado ya ataques utilizando este problema- que Microsoft decidió publicar la actualización del navegador para la versión de Windows XP, a pesar de que ya se había dejado de dar soporte a este sistema operativo.

La mayoría de compañías de seguridad, como es el caso de Panda Security, han decidido continuar ofreciendo soporte y actualizaciones a todos sus clientes que sigan utilizando XP, a pesar de lo cual recomendamos seriamente a los usuarios que se planteen la migración a una nueva versión del sistema operativo que ofrezca mayor seguridad, ya que no se trata de si se descubrirán nuevas vulnerabilidades o no, sino de cuándo sucederá. A partir de ese momento estaremos corriendo un peligro del que estaríamos a salvo si utilizáramos una versión más moderna de Windows.

Heartbleed surgió a principios de abril, al mismo tiempo que se producía el fin de ciclo de Windows XP.

## Se trataba de un fallo de seguridad en una librería, OpenSSL, que se utiliza para el cifrado de comunicaciones

Las comunicaciones de los principales servicios de Internet como el correo web, redes sociales, banca online, etc. están cifradas con el propósito de proteger los datos que intercambiamos (credenciales bancarias, contraseñas, etc.). Aquellos servidores que utilizaban la librería vulnerable eran susceptibles de ser atacados. El problema radicaba en un módulo que permite reutilizar conexiones ya abiertas (conocido como 'keep alive'), mediante el cual se podían obtener hasta 64 Kb de la memoria de la máquina atacada, y hacerlo repetidas veces. No todo era catastrófico, ya que al menos el atacante no podía elegir a qué parte de la memoria acceder, y, además, se publicó la librería que corrige este bug.

A los pocos días se arrestó a un joven estudiante canadiense de 19 años de edad por haber utilizado la vulnerabilidad de Heartbleed para robar información de Hacienda de unos 900 canadienses. La "Canada Revenue Agency" había denegado el acceso público a su servicio de impuestos online un día después de que el fallo se hubiera descubierto y hecho público, lo que, sin embargo, no evitó este ataque.

Uno de los mayores ataques -y más polémicos- sucedidos durante este trimestre tuvo a eBay como protagonista. La conocida empresa norteamericana pidió a todos sus usuarios que cambiaran sus contraseñas debido a un ciberataque del que habían sido víctimas.

## Parece que los atacantes consiguieron credenciales de empleados de eBay que fueron utilizadas para acceder a la red corporativa de la empresa

También accedieron a una base de datos que contenía los nombres de clientes, contraseñas cifradas, direcciones de correo electrónico, direcciones físicas, números de teléfono y fechas de nacimiento.

La polémica surgió no por el ataque, sino por cómo la propia compañía lo comunicó. Al inicio parecía que se trataba de restar importancia al mismo, y de hecho el incidente no se publicitó de forma visible en su página web.

Sin embargo, ante la gravedad de los hechos, a eBay no le quedó más remedio que rectificar y añadir una advertencia muy visible en su página principal pidiendo a todos sus usuarios que cambiaran sus contraseñas.

Por otro lado, PandaLabs ha detectado que los ciberdelincuentes están aprovechándose de este incidente y han lanzado una campaña de correos de phishing haciéndose pasar por eBay, informando del problema de seguridad e incluyendo un enlace (malicioso) para cambiar la contraseña.

## Si accedemos a dicha página e introducimos nuestra información, estaremos dando nuestras credenciales de eBay a los ciberdelincuentes

Otra conocida empresa tecnológica, Spotify, fue víctima de un ataque similar para vulnerar su red corporativa. Sin embargo, lo curioso de este incidente es que sólo se accedió a los datos de un único usuario de Spotify, algo realmente llamativo. Podría tratarse o bien de un ataque dirigido a obtener información de un único usuario, o bien de una prueba de los ciberdelincuentes para comprobar hasta dónde podían llegar.

Por otra parte, la página web de Reuters fue comprometida por la Syrian Electronic Army. En este caso no fue un problema de seguridad de Reuters el que dio pie al ataque, sino que la víctima del mismo fue un proveedor de servicios que la empresa utiliza, siendo ésta la vía de entrada de los delincuentes.

La conocida multinacional Domino's Pizza fue atacada por un grupo denominado "Rex Mundi", y le fueron sustraídos datos de 650.000 clientes de Francia y Bélgica, solicitando un rescate por dicha información. Los responsables de la empresa dijeron que no estaban dispuestos a ceder al chantaje.

Hector Xavier Monsegur, alias Sabu, fue arrestado el 7 de junio de 2011 por el FBI. Muchos recordaréis a este personaje, uno de los líderes del movimiento de Anonymous y Lulzsec. Sabu se declaró culpable de numerosos delitos y ahora se enfrentaba a una pena de hasta 124 años de cárcel.

No obstante, desde que fue arrestado estuvo colaborando con el FBI, ayudando a recoger evidencias y arrestar a otros ciberdelincuentes. Según reconoce la fiscalía, gracias a la ayuda de Sabu se han evitado cerca de 300 ciberataques a lo largo de tres años. Tras ser arrestado, pasó siete meses en prisión y en estos momentos permanece a la espera de sentencia. Finalmente, en mayo de este año Sabu ha sido puesto en libertad, quedando su deuda con la justicia saldada gracias a la intensa colaboración mantenida con las fuerzas de seguridad.

Durante este trimestre hemos presenciado también una de las mayores condenas de la historia a un ciberdelincuente. David Ray Camez, uno de los principales miembros de una página desde la que se comerciaba con tarjetas de crédito robadas, ha sido sentenciado a 20 años de cárcel. Además ha sido condenado a pagar 20 millones de dólares en concepto de daños causados.

## Una macrooperación policial a nivel mundial, liderada por el FBI, ha neutralizado al grupo Blacksades

Este grupo utilizaba una herramienta RAT (Remote Access Tool, Herramienta de Acceso Remoto) del mismo nombre para llevar a cabo diferentes delitos relacionados con robo de credenciales. Esta ha sido una de las mayores operaciones de la historia a nivel mundial contra este tipo de delincuentes.

Otra importante intervención contra el cibercrimen, de nuevo protagonizada por el FBI, fue la toma de control que tuvo lugar contra la red de bots GameOver Zeus, una familia de malware que utilizaba comunicación de tipo P2P, lo que hacía que su toma de control fuera realmente complicada al no depender de servidores que pudieran neutralizarse.

Además, el FBI ha presentado cargos contra quien controlaba la botnet, el ciudadano ruso Evgeniy Mikhailovich Bogachev. Bogachev, que ha sido añadido a la lista de los delincuentes más buscados y ha sido acusado también de llevar a cabo infecciones con el conocido CryptoLocker.


REDES SOCIALES

## La Syrian Electronic Army se hizo con el control de cuatro cuentas de Twitter pertenecientes al Wall Streel Journal

Las cuentas eran la de WSJ Africa (@wsjafrica), WSJ Europe (@wsjeurope), WSJ Vintage (@vsjvintage), y WSJ.D (@wsjd). WSJ se dio cuenta rápidamente del incidente y eliminó los tweets publicados por los atacantes.

La cuenta de Twitter de soporte de British Gas también fue comprometida. En este caso los atacantes comenzaron a publicar mensajes con diferentes enlaces, que llevaban a los usuarios a una página igual a la de Twitter donde se pedían las credenciales (usuario y contraseña). En caso de introducirlas, el usuario se las estaba facilitando a los delincuentes que podían acceder a sus cuentas y secuestrarlas.

El pasado 12 de junio daba comienzo el Mundial de Fútbol en Brasil. Un ciberdelincuente aprovechó la oportunidad para tratar de robar credenciales de Facebook de los jugadores de Top Eleven: Be a Football Manager, uno de los juegos sobre managers de fútbol con más éxito, con más de 10 millones de seguidores en Facebook.

Se trataba de un malware en Windows que actúa disfrazado de aplicación. En teoría, si se descarga permite ganar tokens para el Football Manager con los que comprar jugadores. Evidentemente, esto no sucede, y si lo que hacemos es seguir las instrucciones indicadas, no solo no vamos a conseguir tokens gratis para Top Eleven, sino que, además, podremos perder el acceso a nuestra cuenta de correo electrónico o de Facebook.

MÓVILES

Normalmente cuando hablamos de incidentes de seguridad en entornos móviles principalmente cubrimos el mundo Android, ya que es el sistema operativo más popular. Sin embargo, este trimestre hemos presenciado varios ataques que afectan al sistema operativo de Apple, iOS, y que tienen cierta relevancia.

## En abril se descubrió una campaña de malware cuyo objetivo eran iPhones y iPads que estuvieran hackeados

Es decir, dispositivos modificados por sus propietarios para poder instalar aplicaciones en los mismos sin tener que pasar por la App Store. Este malware tiene como objetivo el robo de credenciales y aparentemente es de origen chino.

Otro caso que tuvo como protagonista a los dispositivos móviles de Apple ocurrió en Australia. Un diario australiano publicó que se había producido un hackeo de algunos de los dispositivos Apple en ese país, sin desvelar el número exacto de afectados. Lo que sucedió es que varios usuarios se encontraron con un mensaje en el que se les pedía 100 dólares a cambio de devolver el control de sus respectivos dispositivos.

Todo parece indicar que los ciberdelincuentes han logrado las credenciales de Apple de estos usuarios, y las han utilizado para hacerse pasar por ellos y bloquear de forma remota los dispositivos, mediante la opción que permite localizar el teléfono en caso de pérdida o robo ("Find my iPhone"). Para recuperar el control de su dispositivo, la víctima tiene que pagar ese rescate. Sólo entonces los hackers enviarán la nueva contraseña que permite el desbloqueo.

Lo más probable es que los ciberdelincuentes hayan hackeado la base de datos de algún foro de fans de Apple, y que, tras robar las credenciales del mismo, hayan comenzado a probar si había usuarios que utilizaban la misma contraseña para los servicios de iCloud. En los casos de coincidencia se han bloqueado estos dispositivos y pedido un rescate por los mismos.

En el ecosistema de Android han aparecido todo tipo de noticias y ataques, aunque los más llamativos pertenecen a la categoría de falsos antivirus y ransomware. Un caso nunca visto hasta ahora fue el de la aplicación "Virus Shield", que consiguió aparecer en lo más alto de las aplicaciones más populares de Google Play. Aparentemente se trataba de una aplicación antivirus de pago, con un coste de 3,99 dólares. Sin embargo, realmente no ofrecía ninguna protección, únicamente tenía un interfaz que simulaba analizar y proteger el móvil. Tuvo más de 10.000 descargas antes de ser retirada, y Google repuso el dinero a los compradores timados.

Durante este trimestre apareció también una nueva familia de malware para Android llamada Android/Koler.

## Un ataque del tipo del "Virus de la Policía" parecido a los que hemos visto en ordenadores Windows, pero dirigido a teléfonos móviles

En este caso el malware no es capaz de cifrar los datos del teléfono, pero aún así es bastante molesto y difícil de eliminar si no cuentas con antivirus en tu móvil, ya que el mensaje que muestra en pantalla permanece encima de todo lo demás, y el usuario sólo dispone de unos pocos segundos para intentar desinstalarlo. Mientras lo estudiábamos en PandaLabs nos encontramos con una nueva variante, exactamente idéntica a la primera, pero que ahora se conectaba a un servidor diferente.

Y este servidor aún estaba activo… En esta ocasión, los ciberdelincuentes cometieron un pequeño error al configurarlo y dejaron la puerta entreabierta. Lamentablemente no pudimos acceder a toda la información que allí había (una base de datos -mysql- con información sobre infecciones, pagos, etc.), pero aún así fuimos capaces de descargar ficheros del servidor y echar un vistazo a su funcionamiento.

El método de funcionamiento desde el lado del servidor es muy parecido a los que tienen como objetivo ordenadores con Windows: varios scripts para geolocalizar el dispositivo y mostrar el mensaje en el idioma local y con imágenes de las fuerzas de seguridad locales. Guarda información de todos los dispositivos infectados en la base de datos y añade el MD5 del malware que lo ha infectado. Al hacer esto es posible hacer un seguimiento del número de infecciones que consiguen con cada variante del malware y medir el éxito de las diferentes campañas de infección.

Este malware está preparado para atacar a usuarios de 31 países de todo el mundo. 23 de ellos son europeos: Alemania, Austria, Bélgica, Chequia, Dinamarca, Eslovenia, Eslovaquia, España, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Noruega, Polonia, Países Bajos, Portugal, Reino Unido, Rumanía, Suecia y Suiza. El resto de países cuyos ciudadanos también son objetivos son: Australia, Bolivia, Canadá, Ecuador, Estados Unidos, México, Nueva Zelanda y Turquía.

Otro malware del tipo ransomware apareció este trimestre, en este caso de origen ruso. La novedad es que realmente cifraba información del móvil (fotografías y vídeos) y solicitaba un rescate para poder recuperarlo.

Por si no fuera suficiente con el malware que amenaza con infectar nuestros teléfonos desde el market o cualquier página web o tienda alternativa, ha aparecido un caso donde el malware venía instalado de fábrica. Se trataba de un fabricante chino, que incluía un troyano que robaba información y la enviaba a un servidor ubicado en China.

## CIBERGUERRA

Uno de los casos más llamativos tuvo lugar en Bélgica.

## El Ministerio de Asuntos Exteriores del país europeo fue comprometido

Se especula con que el origen de dicha agresión podría ser Rusia, aunque debemos ser muy cautos, ya que la investigación aún está en curso y llevará bastante tiempo saber lo realmente sucedido.

En Reino Unido un alto cargo del gobierno confirmó que habían detectado un ataque detrás del cual se encontraba una potencia extranjera. Mediante dicho ataque consiguieron acceso a una cuenta de administrador de sistema de la "Government Secure Intranet", aunque lograron detectarlo a tiempo e impedir que se robara la información. Sobre el espionaje realizado por el propio país, el director general de la Oficina para la Seguridad y Contraterrorismo, Charles Farr, asegur que las comunicaciones a través de redes sociales y buscadores extranjeros son interpretadas por el Gobierno británico como "externas", lo que implica que no necesita de orden judicial para tratar de acceder a la información y comunicaciones que van a través de Google, Twitter o Facebook.

Este tipo de declaraciones, unidas a todo el escándalo de espionaje protagonizado por la NSA en los últimos tiempos, han llevado a un cambio de comportamiento de usuarios. De hecho, según un estudio reciente, se ha más que doblado la cantidad de tráfico cifrado que circula en Internet desde que se desvelaran los casos de espionaje masivos. Y ésta no ha sido la única consecuencia, el Gobierno alemán ha cancelado un contrato que tenía con la compañía de telecomunicaciones estadounidense Verizon, dentro del rediseño de las comunicaciones internas que están efectuando, tras descubrirse prácticas de espionaje por parte del gobierno norteamericano, que incluso había llegado a "pinchar" la línea de la canciller Angela Merkel.

# CONCLUSIÓN

Este segundo trimestre de 2014 no nos ha defraudado, y, a pesar de la gran cantidad de ataques registrados, también hemos podido presenciar muchas buenas noticias en la lucha contra el cibercrimen, protagonizadas principalmente por el FBI. Entre las principales conclusiones de este estudio, destaca el hecho de que la creación de malware mantiene la cifra record alcanzada durante el trimestre anterior.

## 15 millones nuevos de ejemplares generados, siguiendo con una media de 160.000 nuevas muestras generadas cada día

En este contexto, si bien los troyanos continúan siendo el tipo de malware más común, con un 58,20% de las nuevas muestras creadas, se trata de un porcentaje sensiblemente inferior al contabilizado el anterior trimestre (un 71,85%). Esto no se debe tanto a que haya disminuido el número de nuevos troyanos como al incremento más que considerable de PUPs (Potentially Unwanted Programs, en español Programas Potencialmente No Deseados).

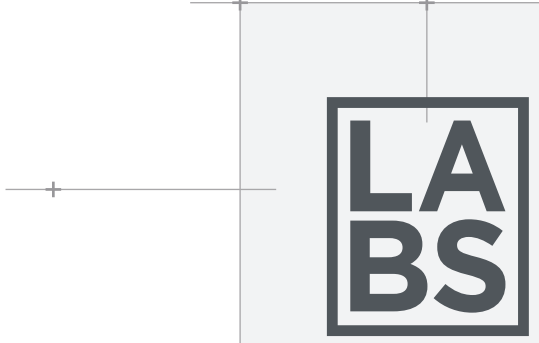
Tenemos por delante la segunda mitad del 2014 donde veremos la evolución del mundo de la seguridad, y donde seremos testigos de nuevos ataques dirigidos a empresas de sectores estratégicos que analizaremos en nuestros próximos informes.

# SOBRE PANDALABS

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

- 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.

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.




https://www.facebook.com/PandaSecurity
https://twitter.com/PandaComunica
https://plus.google.com
http://www.youtube.com/pandasecurity
http://www.linkedin.com/company/panda-security
http://mediacenter.pandasecurity.com