PANDALABS

THE EYE OF SECURITY

INFORME TRIMESTRAL

ENERO-MARZO 2014

CONTENIDOS

INTRODUCCIÓN
EL TRIMESTRE EN CIFRAS
EL TRIMESTRE DE UN VISTAZO
Cibercrimen
Redes Sociales
Móviles
Ciberguerra
CONCLUSIÓN
SOBRE PANDALABS
PANDA EN LA RED

INTRODUCCIÓN

Inauguramos el primer trimestre de lo que será un apasionante año en el mundo de la seguridad informática. En primer lugar, echaremos un vistazo a las cifras obtenidas desde PandaLabs en lo referente a malware, donde veremos cómo se vuelve a batir el récord de malware creado. Sobre los sucesos acaecidos durante estos tres meses de 2014 veremos cómo han tenido lugar grandes robos de datos en todo el mundo, con millones de ciudadanos afectados en cada uno de ellos.

En el mundo de la movilidad, Android ha sufrido diferentes ataques relacionados con la suscripción a servicios de SMS Premium, tanto a través de Google Play como mediante el uso de anuncios en Facebook utilizando la popular aplicación de mensajería WhatsApp como reclamo.

Hablaremos sobre las últimas andanzas del grupo Syrian Electronic Army (SEA), que ha tenido en su punto de mira a empresas como Microsoft e incluso ha intentado conseguir el control de todo Facebook (afortunadamente sin éxito).

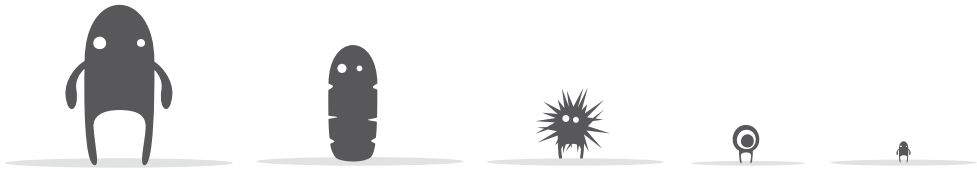
En el campo del ciberespionaje repasaremos las últimas revelaciones sobre operaciones llevadas a cabo por la NSA y la británica GCHQ (Government Communications Headquarters), con revelaciones que no dejan de sorprender e indignar, como el espionaje indiscriminado a millones de ciudadanos a través de sus propias webcams en una operación denominada “Optic Nerve”.

EL TRIMESTRE EN CIFRAS

El primer trimestre de 2014 ha batido todos los récords en lo que a creación de malware se refiere. PandaLabs ha registrado más de 15 millones nuevos de ejemplares durante estos tres meses, con una media de más de 160.000 nuevas muestras generadas cada día.

Los troyanos continúan siendo el tipo de malware más común, con un 71,85% de las nuevas muestras creadas, un porcentaje muy similar al identificado durante el trimestre anterior.

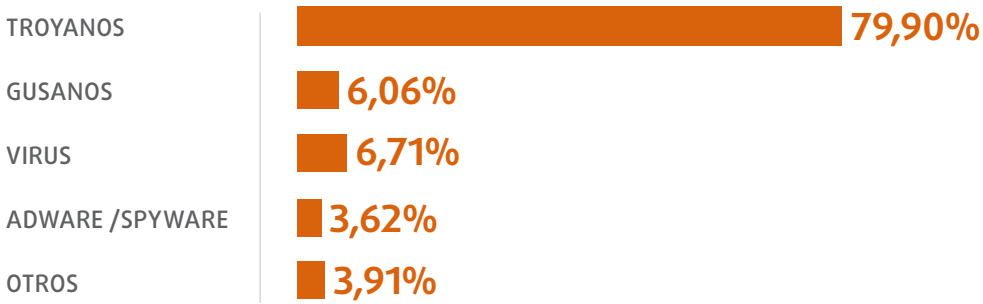
NUEVO MALWARE CREADO EN EL PRIMER TRIMESTRE DE 2014, POR TIPO



71,85%	12,25%	10,45%	5,26%	0,19%
TROYANOS	GUSANOS	VIRUS	ADWARE SPYWARE	OTROS

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 PRIMER TRIMESTRE

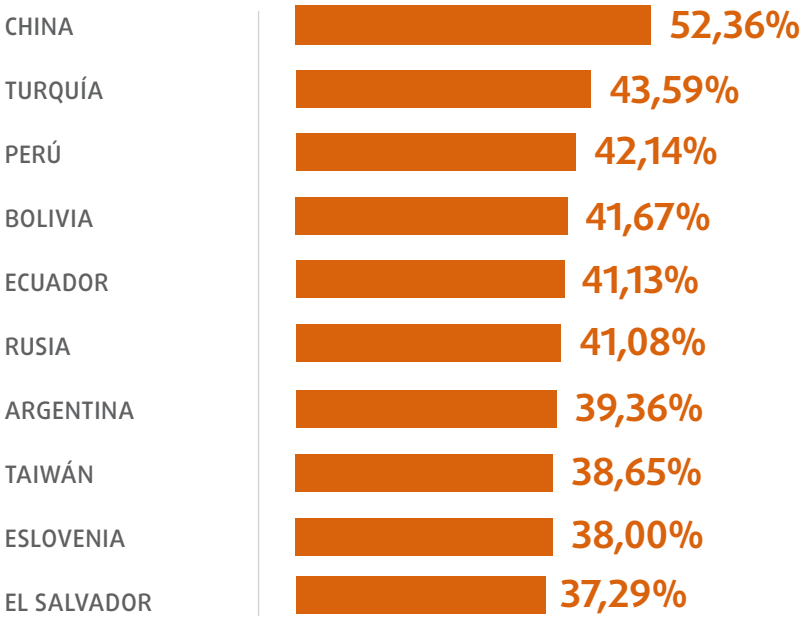


Las infecciones de troyanos se mantienen en la cima de este ranking, siendo el tipo de malware más utilizado por los ciberdelincuentes para infectar a los usuarios, y protagonizando casi cuatro de cada cinco infecciones que tienen lugar en el mundo.

Si realizamos un análisis geográfico de las infecciones, en este primer trimestre de 2014 el ratio de infecciones a nivel mundial ha sido del 32,77%, incrementando así respecto a los últimos trimestres. En cuanto a los datos de los diferentes países, **China continúa en primera posición**, alcanzando un índice de infección del 52,36%. Le siguen Turquía (43,59%) y Perú (42,14%).

A continuación, mostramos el top 10 de países con mayor ratio de infección.

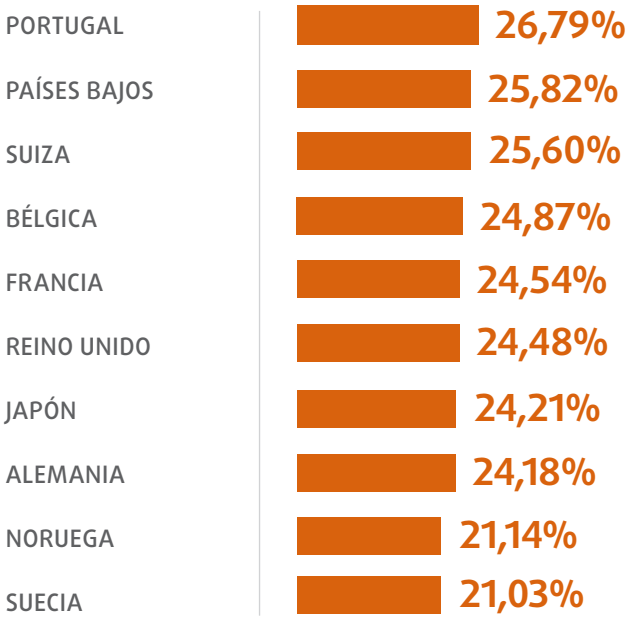
PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN



Como podemos observar, el top de países con mayor ratio de infección está copado por países asiáticos y de Latinoamérica. **China 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 (35,83%), Polonia (35,59%), Guatemala (35,51%), Colombia (33,86%), España (33,57%), Costa Rica (33,33%), Chile (33,22%) e Italia (32,77%).

Veamos a continuación los países menos infectados del mundo.

PAÍSES CON MENOR ÍNDICE DE INFECCIÓN



Europa es la zona del mundo donde el índice de infección es más bajo, con nueve países en este ranking. Suecia (21,03%), Noruega (21,14%) y Alemania (24,18%) son los países con un menor ratio de infecciones a nivel mundial. **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 no han conseguido posicionarse en este Top 10, pero que sí han logrado situarse por debajo de la media mundial de infecciones, son: Dinamarca (27,08%), Finlandia (27,16%), Panamá (27,52%), Canadá (27,54%), Austria (28,74%), Uruguay (28,89%), Venezuela (30,11%), Australia (30,45%), Estados Unidos (31,16%), Chequia (31,58%), México (32,25%) y Hungría (32,74%).

EL TRIMESTRE DE UN VISTAZO

Durante estos meses hemos sido testigos de algunos de los mayores robos de información desde la creación de Internet.

CIBERCRIMEN

A finales de 2013 se descubrió un caso de este tipo que afectó a **Target**, empresa norteamericana que vio cómo le era sustraída información de 40 millones de tarjetas de crédito y débito pertenecientes a clientes que habían comprado en sus **tiendas físicas.** Es decir, no estamos hablando de clientes que habían hecho sus compras a través de la tienda online, sino de personas que habían comprado físicamente en los establecimientos y habían pagado con su tarjeta de crédito. No sólo se descubrió el robo de esta información, sino también su inmediata venta en el mercado negro.

Target Corp sufrió el robo de datos de 40 millones de tarjetas de crédito y débito de compradores que visitaron sus tiendas

A comienzos de este año salieron a la luz más detalles que nos permitieron saber qué había sucedido. De acuerdo a los datos filtrados a Brian Krebs, un servidor web de la compañía habría sido comprometido. Desde allí, un troyano habría sido distribuido a los terminales de punto de venta.

El malware estaba específicamente diseñado para trabajar en estos terminales y robar información de las tarjetas de crédito directamente de la memoria RAM en cuanto se pasaba la tarjeta por el lector. Los ciberdelincuentes entraban regularmente a la red interna para recoger la información de los diferentes terminales comprometidos.

¿Cómo pueden protegerse las empresas ante este tipo de ataques? Los antivirus, obviamente, no son la solución, estamos hablando de ataques dirigidos, donde, para empezar, el malware ha sido especialmente diseñado con el propósito de evitar la detección del antivirus que se esté utilizando.

Como los terminales de punto de venta son normalmente plataformas cerradas, se podría pensar que una buena solución sería utilizar listas blancas o whitelisting. Este tipo de programas están diseñados para que sólo ciertas aplicaciones sean ejecutadas en un ordenador, y de hecho esta podría ser una buena estrategia ante cierto tipo de ataques como, por ejemplo, un ataque desde dentro, donde un empleado intenta infectar un terminal instalando algún tipo de software malicioso en él. Sin embargo, esa solución no cubre todos los flancos. En multitud de ocasiones las aplicaciones maliciosas son instaladas a través de la explotación de vulnerabilidades, y este tipo de instalaciones no son necesariamente detectadas por programas de whitelisting.

Los **terminales de punto de venta** son realmente un objetivo muy apetecible, y los ciberdelincuentes intentarán entrar. No es cuestión de suerte, tarde o temprano lo intentarán, y para estar protegidos necesitamos una solución que cubra los diferentes aspectos de los terminales y sea capaz de:

- Restringir la ejecución de software. Sólo se podrán ejecutar procesos confiables.
- Identificar aplicaciones vulnerables. Avisar ante cualquier software desactualizado.
- Hacer cumplir el comportamiento en procesos permitidos. En caso de que se intente explotar una vulnerabilidad en un proceso confiable.
- Trazabilidad. En caso de que ocurra un incidente, que nos facilite toda la información necesaria para contestar las cuatro preguntas básicas: desde cuándo se produce la intrusión y qué usuarios se han visto afectados, a qué datos se han vulnerado y qué han hecho con ellos, cómo han entrado los atacantes y desde dónde.

Estas no son todas las medidas de seguridad que se pueden tomar, pero al menos estos cuatro puntos deberían ser de obligado cumplimiento.

Si el robo sufrido por Target parece espectacular, aún lo fue más el que tuvo lugar en Corea del Sur. **Korea Credit Bureau (KCB),** compañía financiera coreana, fue víctima de un ataque en el que le robaron 105,8 millones de cuentas de usuarios que incluían detalles de tarjetas de crédito, nombre y apellidos, teléfonos, direcciones e incluso números de pasaporte. Cada coreano tiene una media de cinco tarjetas de crédito (la más alta del mundo), lo que significaría que al menos 21 millones de ciudadanos coreanos han visto cómo todos sus datos personales han sido robados. Para un país con menos de 50 millones de habitantes esto quiere decir que, como mínimo, un 42% de la población ha sido una víctima de este ataque, aunque el dato real tiene que ser mucho más alto, ya que no a todos los afectados les habrán comprometido todas sus tarjetas de crédito. Llegados a este punto sería más sencillo preguntar en Corea del Sur quién no ha sido víctima de este incidente de robo de datos.

Al contrario que en el caso Target, en el ocurrido en Corea del Sur no se ha utilizado malware para acceder a la información. El ladrón trabajaba para KBC –irónicamente en el departamento anti-fraude de la compañía-, y durante 11 meses simplemente copió toda la información y la vendió al mejor postor. Si la información hubiera estado debidamente cifrada, el daño causado habría estado limitado, sin embargo parece que no era el caso. Ser capaz de robar información durante 11 meses también indica una falta de supervisión y de control al acceso de los datos.

Un trabajador del departamento antifraude de la compañía Korea Credit Bureau robó datos de cuentas de más de la mitad de los habitantes de Corea del Sur

También existen medidas preventivas que podrían tomarse: es cierto que la persona involucrada en este incidente era parte del departamento anti-fraude, y, como tal, es probable que hubiera tenido acceso a los datos que fueron robados. ¿Qué se podría haber hecho? Bien, como hemos comentado antes, el cifrado de datos puede ayudar aquí, aunque es cierto que esta persona podría tener acceso a la información necesaria para descifrar los datos. Limitando la cantidad de información a la que es posible acceder cada vez podría mitigarse el daño producido en este tipo de robo de datos: si solo se puede acceder a un número limitado de entradas de la base de datos cada vez –digamos 10 registros-, esta persona habría necesitado repetir la misma operación más de 10 millones de veces. No sólo eso, también se puede limitar la cantidad de información a la que se accede en un periodo de tiempo dado, o incluso mejor: es posible contar con una serie de alarmas ligadas a reglas complejas que envíen un aviso cuando tiene lugar algún hecho inusual. Esto es algo que la mayoría de las entidades financieras ya tienen en marcha y que les permite detectar casos de fraude y de robo de identidad.

A lo largo del primer trimestre de 2014 han tenido lugar también otros robos de datos, aunque de menor impacto si los comparamos con los dos casos previamente descritos. Por ejemplo, en Alemania, la Oficina Federal para la Seguridad de la Información (BSI) lanzó una alerta indicando que el correo electrónico de 16 millones de personas había sido comprometido. Parece que en este caso una red de bots (botnet) se encontraba tras el ataque, lo que significaba que seguramente los ordenadores pertenecientes a los usuarios cuyas cuentas de correo habían sido comprometidas podrían formar parte de una red de bots controlada por ciberdelincuentes.

La Oficina Federal para la Seguridad de la Información alemana lanzó una alerta tras detectar que se habían comprometido 16 millones de cuentas de correo electrónico

BSI creó una página web que permite averiguar si tu cuenta de correo se encuentra entre las afectadas. Si figuras entre las víctimas, existen altas probabilidades de que tu ordenador esté infectado con malware, en este caso aconsejamos utilizar Panda Cloud Cleaner nuestra herramienta gratuita que analiza y elimina cualquier malware que puedas tener.

Por su parte, usuarios de **Yahoo** se vieron afectados por un incidente de seguridad, aunque Yahoo no fue atacada ni sufrió robo de datos directamente. La empresa californiana detectó que ciberdelincuentes habían conseguido información de sus usuarios para acceder a sus cuentas de correo. Al parecer, la información de los usuarios habría llegado a manos de los ciberdelincuentes tras hackear una base de datos de una tercera empresa sin relación con Yahoo.

Como medida preventiva, Yahoo cambió la contraseña de todos los usuarios afectados y utilizó el factor de doble autenticación para que los legítimos dueños de las cuentas de correo pudieran habilitar una nueva contraseña.

A diferencia de este caso de Yahoo, otro ataque sufrido por la compañía **Orange** sí tuvo lugar en una de sus páginas web. Una vulnerabilidad en la web de la multinacional francesa permitió a los atacantes hacerse con datos de cientos de miles de clientes, entre los que figuraban nombres, apellidos, direcciones y números de teléfono.

Orange sufrió un ataque en el que le robaron datos de 800.000 de sus usuarios

Por otro lado, afortunadamente, parece que Orange, a pesar del fallo que permitió el ataque a esta popular compañía, tenía sus sistemas lo suficientemente bien configurados como para que las contraseñas no fueran comprometidas, lo que limitó el daño a los más de 800.000 usuarios afectados en el caso. Parece ser que las contraseñas se encontraban almacenadas en otro servidor más seguro, según la información publicada.

Por tanto, de cara a proteger las contraseñas ante la eventualidad de un robo, la mejor política a seguir es no almacenarlas. Si no almacenas contraseñas no te las pueden robar, algo bastante obvio que lamentablemente no suele aplicarse.

Pero, ¿cómo puede entonces un sitio web validar a los usuarios? Es sencillo, bastaría con "saltear" la contraseña original que elige un usuario cuando se da de alta en un servicio web, y aplicar un hash a esa contraseña "salteada". Al "saltear" la contraseña original lo que hacemos es generar una nueva y diferente a partir de un patrón definido previamente (convertir letras en números, alterar su orden...). Es a esta contraseña alternativa a la que se le aplicaría ahora un hash para, mediante un algoritmo de codificación, convertirla en una compleja cadena de símbolos. Y sería este hash el que se almacenaría como prueba de validación del usuario. A partir de este momento, cada vez que el usuario vuelva a validarse, se le aplicaría el mismo patrón a la contraseña que introduzca, se calcularía su hash y se compararía con el almacenado. Si coinciden, significará que se ha utilizado la contraseña correcta y se podrá dar acceso al usuario sin necesidad de almacenar datos críticos, como es el caso de las contraseñas.

Otra medida que debería empezar a aplicarse de forma masiva es el doble factor de autenticación. Aunque puede resultar una molestia para el cliente, si se tiene la opción de utilizar este sistema resulta mucho más complicado que las cuentas de los usuarios puedan verse comprometidas. Esto es algo que las entidades financieras aprendieron hace tiempo pero que debería también extenderse al resto de servicios web.

Forbes sufrió un defacement por parte del grupo Syrian Electronic Army (SEA) y le sustrajeron datos de 1.057.819 cuentas de usuarios

El grupo **Syrian Electronic Army** (SEA) consiguió comprometer la página web de Forbes, y además robó datos de más de un millón de sus usuarios, entre los que se encontraban cientos de sus empleados. Dentro de la información sustraída se figuraban los nombres y direcciones de correo electrónico de los usuarios, así como las contraseñas (cifradas). Para empeorarlo aún más, SEA publicó los datos robados en Internet.

Cryptolocker, el dañino ransomware que cifra los ficheros de los ordenadores infectados y demanda un rescate para poder volver a acceder a los mismos, se ha seguido cobrando víctimas. Uno de los muchos casos que han tenido lugar este trimestre es el que afectó al despacho de abogados Goodson, en Carolina del Norte (EE.UU.), donde el troyano cifró todos los documentos legales contenidos en su servidor principal. Es importante recordar en este punto que las copias de seguridad son necesarias e imprescindibles en entornos empresariales, y que el daño sufrido en casos como éste quedaría minimizado con una copia de seguridad que permita restaurar toda la información.

Cryptolocker ha seguido causando estragos: una de sus últimas víctimas ha sido un despacho de abogados de Carolina del Norte al que le ha cifrado todos sus documentos legales

Cuando hablamos de ataques siempre pensamos en ordenadores principalmente, con otros dispositivos también en mente, como pueden ser smartphones o tablets. Sin embargo, hay más elementos de hardware vulnerables, y lo hemos visto muy claramente en el primer trimestre de este año. Una vulnerabilidad en routers Linksys permitía a un agresor externo hacerse con el control y realizar acciones como, por ejemplo, cambiar la configuración DNS, lo que es muy habitual para realizar ataques de phishing que nos redirijan a páginas falsas cuando estamos navegando.

Los troyanos bancarios son una de las amenazas más peligrosas y que mayor número de agresiones protagonizan. Su objetivo final es lograr vaciar las cuentas bancarias de sus víctimas, por lo que son ataques muy peligrosos y en los que los ciberdelincuentes invierten mucho, ya que pueden obtener pingües beneficios. En enero el Departamento de Justicia de Estados Unidos anunció que habían conseguido que el ciudadano ruso Aleksandr Panin se declarara culpable de fraude bancario. Se trata, ni más ni menos, del principal desarrollador y distribuidor de uno de los troyanos bancarios más conocidos: SpyEye.

Aleksandr Panin, la mente criminal detrás del famoso troyano bancario SpyEye, se ha declarado culpable de fraude bancario

REDES SOCIALES

Durante este trimestre tuvo lugar un triste suceso, la desaparición del vuelo de Malasia Airlines MH370. En cuestión de poco tiempo, los ciberdelincuentes explotaron la curiosidad que despertaba el caso y comenzaron a distribuir a través de Facebook supuestos vídeos del vuelo. Al tratar de acceder a los vídeos se solicitaba el usuario y la contraseña del usuario, que veía como su cuenta era comprometida. Al poco tiempo utilizaron la misma táctica a través de Twitter, empleando el supuesto vídeo como gancho del engaño.

Ciberdelincuentes utilizaron las noticias del vuelo de Malasia Airlines MH370 para lanzar ataques a través de Facebook y Twitter

Además de en redes sociales, también detectamos en PandaLabs malware distribuido a través de mensajes de correo electrónico utilizando el mismo reclamo. En este caso se adjuntaba la transcripción de las conversaciones entre la cabina del avión y una torre de control minutos antes de que se perdiera el contacto. Se trataba de un ejecutable que utilizaba un icono de ficheros PDF para engañar al usuario. Al ejecutar el fichero, por un lado, infectaba el equipo con un troyano, pero al mismo tiempo habría un documento con la transcripción prometida, haciendo que el usuario no tuviera sospechas de lo sucedido.

El grupo **Syrian Electronic Army**, al que hemos mencionado anteriormente en el informe, se ha mostrado muy activo en el campo de las redes sociales, principalmente comprometiendo cuentas de grandes empresas. Una de sus víctimas fue **Microsoft**, que vio como eran comprometidas las cuentas oficiales de Twitter de soporte de Xbox (@XboxSupport) y de noticias de Microsoft (@MSFTNews). Pero este no fue el primer ataque que sufrió la compañía de Redmond, ya que el mismo 1 de enero vio cómo las cuentas de Twitter y Facebook de Skype (propiedad de Microsoft) fueron hackeadas por el mismo grupo.

El grupo Syrian Electronic Army ha comprometido cuentas de Twitter y Facebook, y trató de hacerse con el control del dominio facebook.com en un ataque que fue parado a tiempo por MarkMonitor

Pero estos no han sido los únicos ataques de SEA, y de hecho trataron de comprometer directamente a Facebook en su totalidad: el grupo consiguió acceso al panel de control de **MarkMonitor**, proveedor de servicios DNS. Afortunadamente, el equipo de seguridad de MarkMonitor detectó la agresión según se estaba produciendo, y consiguieron pararlo antes de que cambiaran los registros DNS de facebook.com.

MÓVILES

En Febrero, PandaLabs destapó un caso de malware en **Google Play**. Se trataba de cuatro aplicaciones de diferente temática (dietas, peinados, ejercicio y recetas) que al ser ejecutadas en el terminal suscribían al usuario a un servicio de SMS Premium. Además, se ocultaban los SMS recibidos tras ser suscritos, lo que acarreaba que el usuario no pudiera percatarse del ataque hasta que recibiera la factura.

PandaLabs descubrió cuatro aplicaciones maliciosas en Google Play que tenían entre 300.000 y 1.200.000 descargas en poco más de un mes

Semanas más tarde, PandaLabs descubrió un ataque similar, aunque, en este caso, en lugar de utilizar Google Play los ciberdelincuentes habían creado una imitación de la tienda oficial de aplicaciones de Android, y para distribuir la aplicación utilizaban anuncios en la popular red social Facebook.

CIBERGUERRA

En este apartado han seguido apareciendo nuevas revelaciones sobre las tácticas de espionaje llevadas a cabo por la **NSA** que destapó Edward Snowden, como ya contamos en anteriores informes. Durante este trimestre han prevalecido las noticias de colaboración entre la NSA y el británico **GCHQ** (Government Communications Headquarters). Uno de los casos más escandalosos tiene que ver con el programa "Optic Nerve", a través del cual el GCHQ capturaba imágenes de la webcam de usuarios de Yahoo. No se sabe a cuántos usuarios en total ha podido afectar, aunque a lo largo de seis meses "pincharon" las webcam de 1.800.000 usuarios.

La NSA y el GCHQ espiaron a millones de usuarios capturando imágenes mediante sus webcams a través de una operación denominada "Optic Nerve"

En lugar de capturar vídeo, lo que hacían era tomar una imagen cada cinco minutos. De forma indiscriminada, de hecho, datos publicados indican que entre el 3% y el 11% de dichas imágines eran de desnudos. Yahoo acusó a las dos agencias de llegar a "un nuevo nivel en la violación de la privacidad de los usuarios".

En marzo, el diario alemán Spiegel reveló cómo de nuevo el GCHQ británico y la norteamericana NSA habían estado espiando a diferentes empresas e individuos en Alemania, entre los que se encontraba la canciller Ángela Merkel.

CONCLUSIÓN

Tal y como os prometíamos en la introducción, el año 2014 está resultando apasionante en el mundo de la seguridad informática.

Se han batido todos los récords registrados hasta la fecha en creación de malware, hemos sido testigos de robos masivos de datos a todo tipo de empresas, y también hemos recibido buenas noticias, como la declaración de culpabilidad lograda por el FBI del creador de SpyEye, uno de los troyanos bancarios más temibles.

Los ataques a dispositivos Android siguen aumentando y consiguen cada vez afectar a un mayor número de dispositivos. En próximos informes prepararemos información más detallada sobre el tema donde podremos analizar las amenazas más comunes y cuántos casos de infecciones tienen lugar.

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

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/

PANDA EN LA RED

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

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