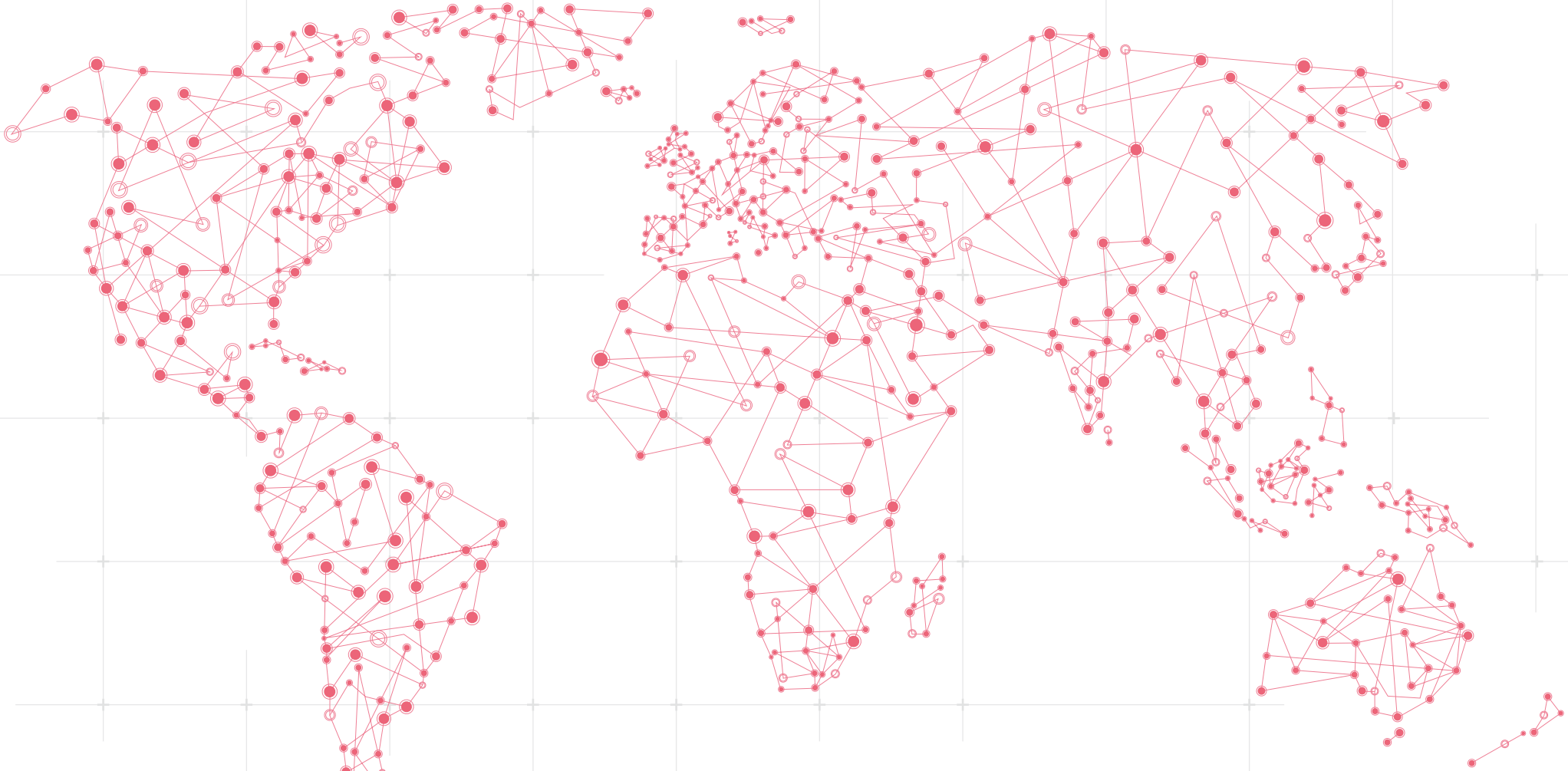
PANDALABS

THE EYE OF SECURITY



INFORME TRIMESTRAL

T3 2014

PANDA SECURITY | *The Cloud Security Company*

INTRODUCCIÓN

El tercer trimestre coincide con la época veraniega, por lo que se suele pensar –equivocadamente- que se trata de una época tranquila y sin sobresaltos. No sólo no ha sido una época tranquila sino que veremos a lo largo del informe que los ataques en el mundo no dejan de aumentar.

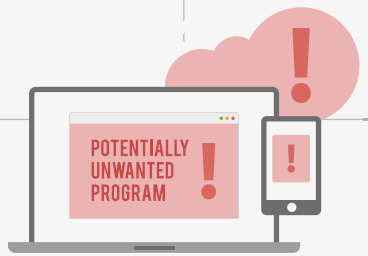
Se han batido todos los records de creación de malware, con una media de más de 227.000 nuevos ejemplares al día.

Por un lado, nuevamente se han batido todos los records de creación de malware, con más de 20 millones de muestras aparecidas durante estos tres meses, con una media de más de 227.000 nuevos ejemplares al día.

En el mundo móvil, mientras vemos cómo responsables de seguridad de Android en Google dicen que no hay que preocuparse y que no son necesarios los programas antivirus, aparecen nuevos agujeros de seguridad que pueden ser fácilmente utilizados por ciberdelincuentes para infectar nuestros dispositivos.

Hablando de ciberdelincuentes, analizaremos el caso #celebgate donde fotos íntimas de 100 actrices y modelos han sido robadas y publicadas en Internet, y qué papel jugó en el mismo iCloud. También veremos algunos de los ataques masivos que han sufrido todo tipo de empresas, desde UPS a JPMorgan Chase, pasando por Home Depot.

Por otro lado, el mundo del ciberespionaje sigue dando noticias a raíz de nuevos documentos filtrados por Edward Snowden, el antiguo trabajador de la NSA.



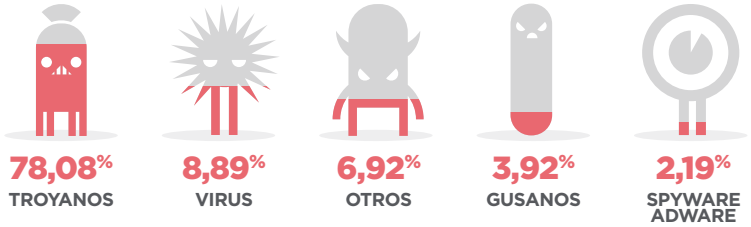
EL TRIMESTRE EN CIFRAS

La primera mitad del año comenzó con un aumento notable del número de nuevos ejemplares de malware, doblando la cifra del pasado año y alcanzando las 160.000 muestras diarias. En el tercer trimestre de 2014 el número se ha disparado aún más. Desde PandaLabs hemos capturado durante estos tres meses más de 20 millones de nuevos ejemplares de malware, con una media de 227.747 al día.

Gran parte de este malware no procede de nuevas familias creadas de cero, sino de variantes conocidas de malware que son modificadas por sus creadores parar tratar de evitar su detección por parte de los laboratorios de antivirus.

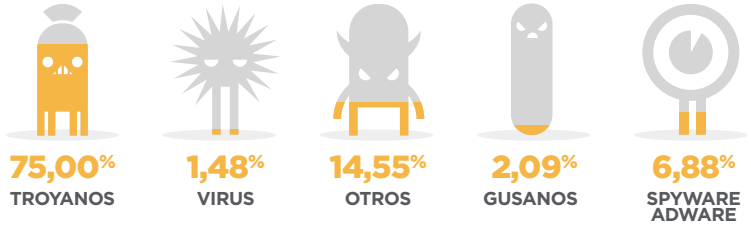
Una vez más, los troyanos son el tipo de malware más común, sumando un 78,08% de todas las muestras de malware aparecidas durante este periodo. En segundo lugar –a gran distancia- están los clásicos virus, que alcanzan un 8,89%. A continuación, los datos de malware creados en este trimestre:

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



Si analizamos el porcentaje de infecciones que han tenido lugar en el mundo por tipo de malware, observamos cifras similares a las de nuevos ejemplares de malware creado, aunque se puede observar cómo la categoría "Otros" del ranking de infecciones por tipo supera en más del doble el porcentaje de ejemplares creados:

INFECCIONES POR TIPO DE MALWARE EN EL TERCER TRIMESTRE DE 2014

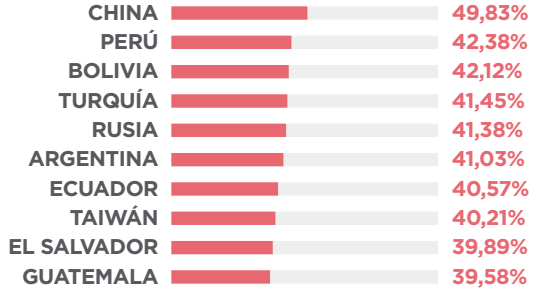


Las categorías de "Otros" -que incluye PUPs (Potentially Unwanted Programs) y de "Adware/Spyware" son las que más rentabilizan sus ejemplares, al lograr llegar a más PCs con un número más contenido de muestras. No debemos olvidar que en la mayoría de los casos hablamos de software legal que utiliza métodos muy agresivos para su distribución, desde su inclusión dentro de aplicaciones gratuitas hasta instaladores que distribuyen software libre de cualquier amenaza, pero que tratan de instalar otro software en los equipos de los usuarios.

El ratio de infecciones a nivel mundial ha sido de un 37,93%, que supone un ligero incremento respecto a los últimos trimestres. En cuanto a los datos registrados en los diferentes países, China continúa en primera posición, alcanzando un índice de infección del 49,83%, bajando por primera vez en mucho tiempo del 50% de ordenadores infectados. Le siguen Bolivia (42,12%) y Perú (42,38%).

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

PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN

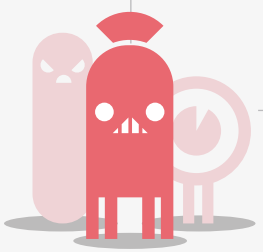


Como podemos observar, el top de países con mayor ratio de infección se localiza en Asia y Latinoamérica. China, de nuevo, es el único país del mundo que supera el 50% de infecciones. Otros países con un nivel de infección superior a la media mundial son: Polonia (39,48%), Brasil (39,21%), Eslovenia (39,05%), Colombia (38,86%), España (38,37%), Costa Rica (38,19%), Chile (38,05%) e Italia (37,97%).

Veamos a continuación los países menos infectados del mundo:

PAÍSES CON MENOR ÍNDICE DE INFECCIÓN

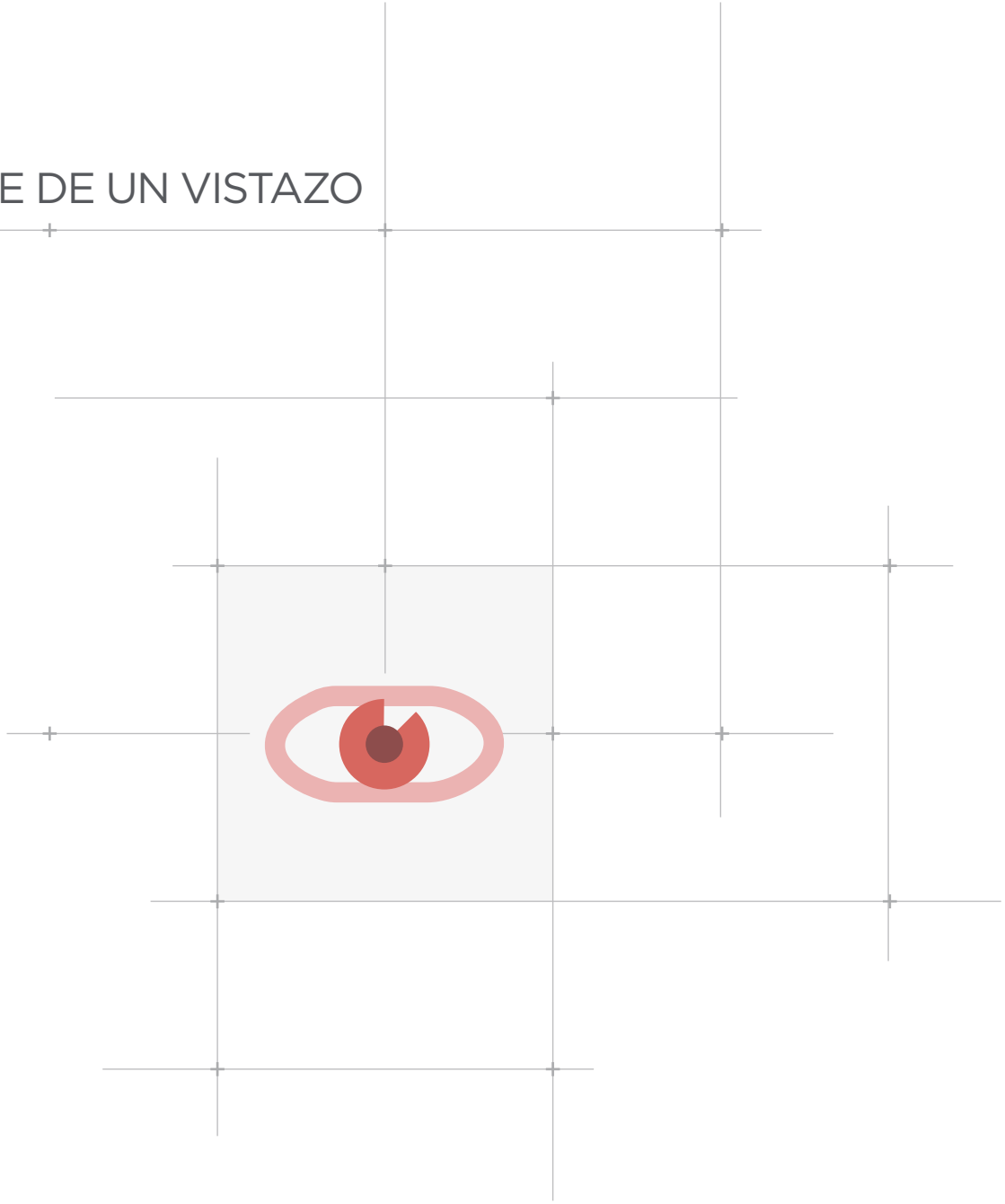
PORTUGAL	27,83%
BÉLGICA	27,39%
PAÍSES BAJOS	26,96%
ALEMANIA	26,52%
FRANCIA	25,87%
REINO UNIDO	25,11%
SUIZA	24,61%
JAPÓN	24,02%
SUECIA	23,44%
NORUEGA	23,07%



Europa es la zona del mundo donde el índice de infección es más bajo, con nueve países en este ranking. Noruega (23,07%), Suecia (23,44%) y Japón (24,02%) son los países menos infectados a nivel mundial. 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 (28,18%), Finlandia (28,59%), Panamá (29,77%), Canadá (30,03%), Austria (30,55%), Uruguay (31,15%), Venezuela (32,35%), Australia (32,54%), Estados Unidos (33,03%), Chequia (34,46%), México (36,31%) y Hungría (36,99%).

EL TRIMESTRE DE UN VISTAZO

El tercer trimestre de este año, a pesar de coincidir con la época veraniega, no nos ha dejado ni un minuto de descanso. Vamos a repasar a continuación los hechos más relevantes ocurridos en el mundo durante este periodo en el panorama de la seguridad informática.



CIBERCRIMEN

__ iCloud también ha sido uno de los protagonistas involuntarios de un suceso ocurrido durante este periodo y que es conocido como el caso #celebgate. __

Una de las formas más prácticas de mitigar el riesgo de que nuestras contraseñas sean utilizadas por terceros es utilizar sistemas de doble factor de autenticación. La mayoría de las grandes compañías (Google, Microsoft, Facebook, etc.) ya ofrecen este tipo de servicios. Este trimestre Apple, que ya tenía implementada esa tecnología en sus servicios iCloud, la amplió para poder utilizarla desde apps que hagan uso de dicho servicio en dispositivos como el iPhone o el iPad, mejorando así la seguridad.

iCloud también ha sido uno de los protagonistas involuntarios de un suceso ocurrido durante este periodo y que es conocido como el caso #celebgate. Se trata de un incidente en el que se han robado imágenes y vídeos íntimos a más de 100 actrices y modelos, con su posterior publicación en Internet. Actrices como Jennifer Lawrence, Kirsten Dunst o Kate Upton han sido algunas de las víctimas de este ataque, y todas tienen algo en común: el robo se ha producido en iCloud, donde se pueden guardar copias de fotografías y vídeos tomados con nuestros dispositivos.

De hecho, en un principio, se especuló con que el ataque pudiera venir por algún fallo de seguridad en iCloud, pero la compañía ha asegurado **a través de un comunicado** que, después de 40 horas de investigación, ha descubierto que las cuentas de estas celebrities "fueron comprometidas por un ataque muy específico sobre los nombres de usuario, contraseñas y preguntas de seguridad". Una práctica "que se ha vuelto muy común en Internet".

Está claro que los culpables en este caso son los atacantes que han robado las imágenes, pero debemos tomar nota y aprender de lo sucedido:

- Nunca subir a Internet imágenes que en ningún caso vamos a querer compartir.

- Activar el doble factor de autenticación de nuestras cuentas online.

CNET ha sido víctima de un ataque por parte de un grupo de origen ruso autodenominado w0rm, robando una base de datos con nombres de usuario, direcciones de correo y contraseñas cifradas. Este mismo grupo ha perpetrado en el pasado ataques a otras empresas, como la BBC, Adobe o Bank of America.

Durante este trimestre, hemos sido testigos de grandes robos de información a importantes empresas y organismos. Community Health Systems, una de las más grandes redes hospitalarias de EEUU, fue víctima de una intrusión en su red por la que robaron información personal de 4,5 millones de clientes .Supervalu, cadena de tiendas de alimentación, anunció también el robo de datos pertenecientes a clientes que habían comprado en 180 establecimientos diferentes a lo largo del país. Por su parte, UPS comunicó que la información de tarjetas de crédito y débito de clientes de 51 de sus establecimientos podía haber sido comprometida en otro ataque.

La entidad financiera JPMorgan Chase fue también víctima de una agresión similar. En este caso se trató de un ataque dirigido a varios de sus empleados para conseguir acceso a sus ordenadores y así acceder a la red interna de la entidad. Se desconoce quiénes fueron los atacantes, aunque algunas fuentes han apuntado que lograron acceder a información interna y que han podido alterarla e incluso borrarla. El FBI y el Servicio Secreto están investigando el caso.

Uno de los más grandes ataques sucedidos este trimestre tuvo como víctima

a Home Depot. El gigante minorista del bricolaje ha confirmado el ataque informático a sus servidores y ha reconocido que se han comprometido 56 millones de tarjetas. Según asegura The Wall Street Journal, la compañía también ha reconocido que, en algunos casos, se han vaciado las cuentas asociadas a estas tarjetas.

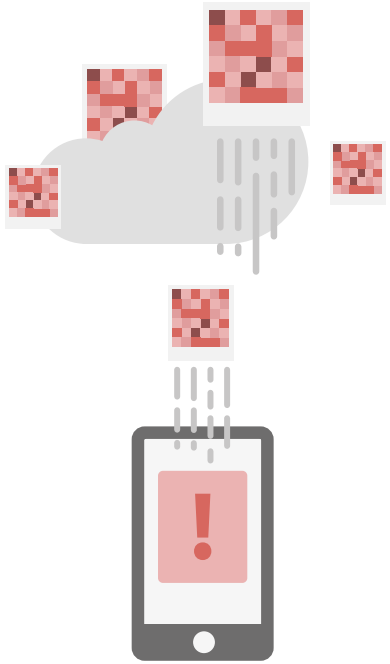
Además, las transacciones fraudulentas que se están produciendo en Estados Unidos se deben a que los criminales están empleando la información robada para comprar tarjetas prepago, o realizar compras en tiendas de electrónica o comestibles.

El hackeo llega unos meses después del que se produjo contra Target, y ambos podrían estar conectados ya que se utilizó la misma herramienta para explotar la vulnerabilidad, conocida como "BlackPOS". Esta brecha de seguridad ha afectado potencialmente a los clientes que compraron en cualquiera de las casi 4.000 tiendas que la compañía tiene en Estados Unidos y Canadá, entre abril y septiembre.

El anuncio de un posible hackeo a Google apareció en las portadas de medios de comunicación de todo el mundo tras saberse que se había publicado un archivo con más de cinco millones de nombres de usuario y contraseñas pertenecientes a cuentas de Gmail. En un comunicado, Google afirmó no tener evidencia de que sus sistemas hayan estado comprometidos, si bien explica que "cada vez que un usuario ve comprometida su cuenta nosotros tomamos acciones para ayudarle a proteger sus datos". De hecho, parece que un 98% de los datos eran antiguos y no estaban actualizados, y podían provenir de la recopilación de diferentes ataques de phishing o a través de infecciones de malware.

Se ha descubierto un agujero de seguridad en Bash que pone en peligro la seguridad informática de los usuarios Linux y Mac. Esta vulnerabilidad, bautizada como "Shellshock", afecta al intérprete de comandos de estos sistemas operativos. Para que nos hagamos una idea, este bug permite a un ciberdelincuente acceder a un sistema que emplee Bash de forma remota y colocar, por ejemplo, un programa espía que robe datos o información confidencial del usuario, así como obtener el control total del mismo.

Una de las consecuencias más graves de esta vulnerabilidad son todos aquellos dispositivos que utilizan Linux y cuyo software no suele ser actualizado por parte de sus usuarios, como es el caso de multitud de routers en todos los hogares, lo que podría permitir a un atacante tomar control del dispositivo.



REDES SOCIALES

__ Twitter se une a las compañías que premian la labor de todos aquellos usuarios que dedican parte de su tiempo a descubrir y revelar fallos de seguridad en sus creaciones.__

En el mundo de la tecnología es habitual que las compañías premien la labor de todos aquellos usuarios, de un nivel avanzado, que dedican parte de su tiempo a descubrir y revelar fallos de seguridad en sus creaciones.

Algunas no suelen confiar en la eficacia en este tipo de recompensas, pero otras muchas piensan que, visto lo visto, pueden resultar sumamente útiles, no solo para descubrir nuevos errores que pasaron desapercibidos en su día, sino para tener a los expertos de su lado y evitar sobresaltos indeseados. Una de las firmas que aún no había desembarcado en este escenario era Twitter. La red social se resistía a recompensar a los expertos que encontraran 'bugs' en su servicio.

Sus responsables han fijado 140 dólares como la compensación mínima para todos aquellos que encuentren algún fallo de seguridad en Twitter.com, ads.twitter, mobile Twitter, TweetDeck, apps.twitter, así como en las aplicaciones tanto para iOS como para Android. El montante está lejos de lo que otras compañías destinan a este fin. Los 'bounty programs' de empresas como Facebook o Google premian a los usuarios que encuentran vulnerabilidades con sumas que superan los 500 y los 1.000 dólares respectivamente.

MÓVILES

__ El número de muestras de malware para Android sigue subiendo de forma exponencial y batiendo récords. __

Android ha sido de nuevo el protagonista en este aportado por motivos muy variopintos. Por un lado, Adrian Ludwig, responsable de seguridad del sistema operativo de Google, declaró que se tenía una idea equivocada de cómo son analizadas y validadas las aplicaciones que se suben a Google Play en comparación a otras tiendas equivalentes (velada mención, sin nombrarla, a la App Store de iOS que tiene fama de ser mucho más exigente en este aspecto). En este contexto, vino a decir que no es necesario el uso de software antivirus en Android.

Mientras tanto el número de muestras de malware para Android sigue subiendo de forma exponencial y batiendo récords, siendo este el año de la historia en el que más malware de móviles ha aparecido.

Además siguen apareciendo diferentes vulnerabilidades que podrían ser explotadas de forma maliciosa por atacantes en Android:

- CVE-2013-6272: Afecta a todas las versiones de Android anteriores a la 4.4.2 (KitKat) y podría permitir a una aplicación maliciosa realizar llamadas a números de tarificación especial sin que el usuario se percate de ello y aun sin permisos para ello.

- CVE-2014-N/A: Afecta a las versiones de Android 2.3.3 y 2.3.6, y tiene los mismos efectos que la anterior.

CIBERGUERRA

En julio el diario norteamericano The New York Times publicó una exclusiva en la que revelaba cómo atacantes chinos consiguieron acceder a bases de datos en los que la oficina de personal federal almacena la información personal de los funcionarios que solicitan un pase para acceder a información de alto secreto. El Gobierno confirmó que, efectivamente, dicho ataque había tenido lugar, pero que no había constancia de que se hubiera sufrido ninguna pérdida de información sensible. A pesar de que se siguió el rastro de los atacantes hasta China, tampoco hay pruebas de que actuaran en nombre del gobierno chino.a

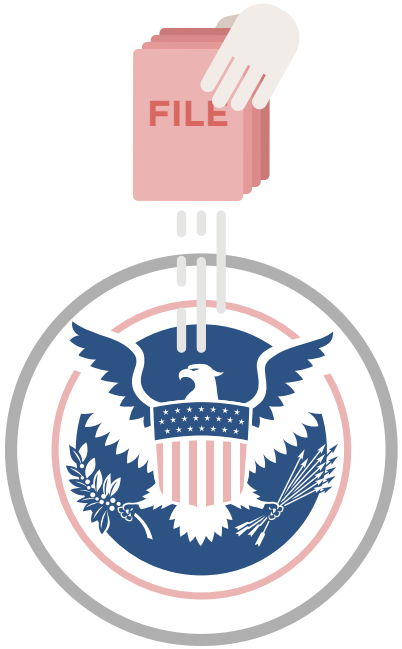
Durante este trimestre, hemos sido testigos de grandes robos de información a importantes empresas y organismos.

Seguimos en Estados Unidos, pero desde una perspectiva diferente. Hemos conocido mediante documentos secretos filtrados por Edward Snowden, pertenecientes a la NSA y a la británica GHCQ, el programa "Treasure Map" (Mapa del Tesoro). Aunque ya se había hablado anteriormente de este programa, lo que se ha conocido es que habrían entrado sin consentimiento en las redes internas de diferentes compañías de cara a cumplir su objetivo (crear un mapa de todos los dispositivos que se conectan a Internet). Una de estas empresas es el gigante alemán Deutsche Telekom, que tras ser avisado por el diario alemán Spiegel, analizó su red sin ser capaz de hallar pruebas de la infiltración.

Otros documento filtrado por Snowden puso de nuevo en el punto de mira al GHCQ, donde se mostraba que la agencia de espionaje británica tenía capacidad de vigilar en tiempo real las comunicaciones que se hacen sobre Skype sin que los usuarios sean conscientes de ello.

En agosto un hacker hizo público que fue capaz de infiltrarse y robar 40 Gb de documentos de la empresa Gamma International (http://en.wikipedia.org/wiki/FinFisher). Esta compañía se dedica a desarrollar software espía para los principales gobiernos del mundo. El atacante creó una cuenta en Twitter llamada @GammaGroupPR en la que comenzó a publicar los documentos robados, además de proporcionar un enlace al torrent que contenía el total de información sustraída.

.

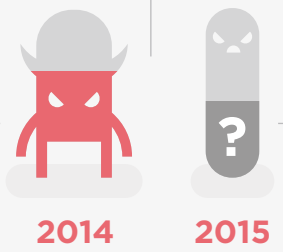


CONCLUSIÓN

Este trepidante tercer trimestre de 2014 no nos ha dejado indiferentes. De hecho, se ha producido el mayor número de muestras de malware creadas en la historia, así como ataques sufridos por grandes empresas comprometiendo decenas de millones de tarjetas de crédito utilizadas por sus clientes en sus establecimientos físicos, todo tipo de credenciales robadas, etc.

Viendo cómo han transcurrido los últimos nueve meses, la última parte del año promete ser aún más apasionante. ¿Seguirá la creación de malware batiendo records, o ha llegado ya a su techo? ¿Qué nuevos ataques veremos en el mundo de los dispositivos móviles? ¿Qué otras empresas serán atacadas? ¿Seguirá Snowden filtrando nuevos documentos que vuelvan a poner en evidencia a la NSA?

Todo esto lo veremos en el próximo informe, que cubrirá los principales hechos acaecidos durante todo el año, y donde daremos también las pinceladas de nuestras previsiones sobre lo que sucederá a lo largo de 2015 en materia de seguridad.



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