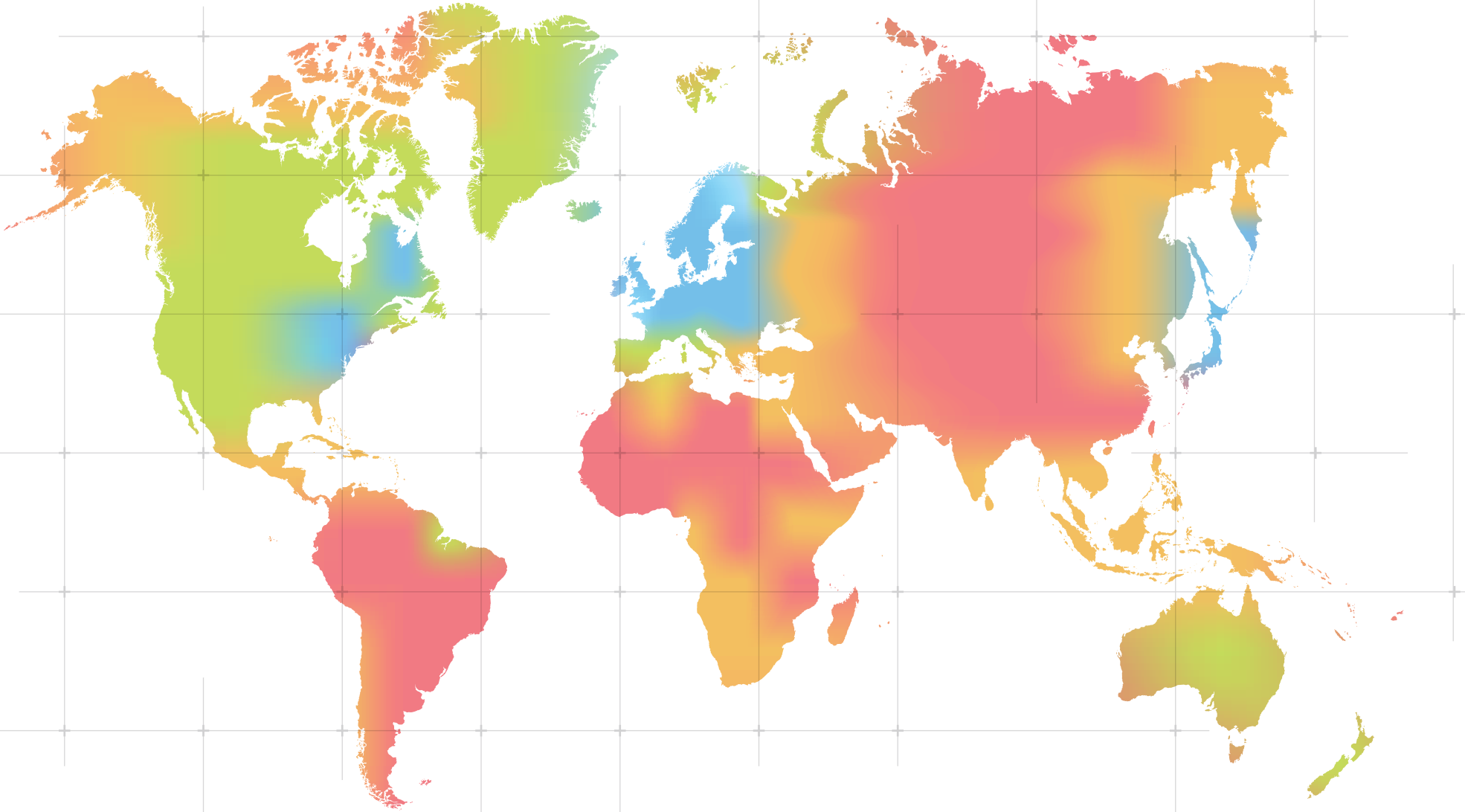
PANDALABS
THE EYE OF SECURITY



# INFORME ESPECIAL: PREDICCIONES 2015
## Y ATAQUES MÁS DESTACADOS EN 2014

PANDA SECURITY | *The Cloud Security Company*

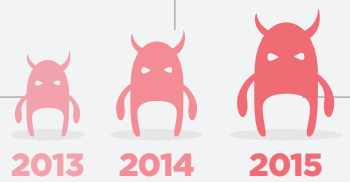
# INFORME ESPECIAL: PREDICCIONES 2015

## Y ATAQUES MÁS DESTACADOS EN 2014

# INTRODUCCIÓN

Según las estimaciones de PandaLabs, la creación de malware volverá a batir records durante 2015.

## La gran mayoría de este malware estará diseñado para plataformas Windows, pero veremos un incremento significativo en otras como Android o Mac OSX.




**Veremos un aumento de Cryptlocker**, un malware que ya ha tenido protagonismo en este 2014, y que seguirá ocasionando quebraderos de cabeza en 2015.

Los **ataques dirigidos serán más populares** a lo largo del año que viene, y **seguiremos conociendo casos de Amenazas Persistentes Avanzadas** (APTs).

Los dispositivos móviles, sobre todo Android, volverán a estar en el punto de mira de los ciberdelincentes.

Por otra parte, y si nos centramos en 2014, si algo puede destacarse de lo sucedido a lo largo de este año es la cantidad de ataques sufridos por grandes empresas de todo el mundo, en los que han estado implicados desde gigantes tecnológicos como Dropbox, Paypal, o Google, hasta empresas financieras, medios de comunicación o famosas personalidades del mundo.

En este informe de PandaLabs, resumimos los principales incidentes de seguridad sucedidos durante este periodo, así como las predicciones de seguridad que debemos tener en cuenta para estar protegidos durante 2015.

# PREDICCIONES SEGURIDAD 2015

2013 fue el año en el que más ejemplares de malware fueron creados. 2014 ha batido de lejos dicho récord, y todo indica que durante 2015 seguiremos con un crecimiento que volverá a batir todas las marcas registradas hasta la fecha.

La gran mayoría de este malware estará diseñado para plataformas Windows, pero veremos un incremento significativo en otras como Android o Mac OSX.

## CRYPTOLOCKER

Este tipo de malware ha tenido mucho protagonismo durante 2014, y todo hace prever que durante 2015 estos ataques irán en aumento.

El funcionamiento es bastante directo: una vez consigue entrar en un ordenador, cifra todo tipo de documentos que pueden tener algún valor para el usuario (hojas de cálculo, documentos de texto, bases de datos, fotografías, etc.) y chantajea a la víctima para que pague un rescate si quiere recuperar dichos ficheros.

El pago se reclama siempre en bitcoins, de tal forma que no pueda ser rastreado por la policía, lo que hace que este tipo de ataque sea muy jugoso para los ciberdelincuentes, pues muchos usuarios deciden pagar para poder recuperar la información secuestrada.

## ATAQUES DIRIGIDOS

Si bien la mayoría de ataques protagonizados por malware están dentro de los millones de muestras de malware que aparecen todos los meses, un pequeño porcentaje de las mismas son creadas para atacar a objetivos previamente definidos. Estos son los conocidos como ataques dirigidos, cada vez más comunes y que tendrán un gran protagonismo durante 2015.

Uno de los mayores riesgos que afrontar es que muchas empresas no creen que puedan ser objetivo de ataques dirigidos, por lo que no disponen de las medidas adecuadas para detectarlos y pararlos, o al menos para poder detectar cualquier anomalía y mitigar el daño lo antes posible.

## TERMINALES DE PUNTO DE VENTA

Durante este año hemos visto cómo se ha incrementado el ataque hacia estos terminales, usados por todos los establecimientos comerciales para cobrar a sus clientes.

Los ciberdelincuentes están consiguiendo atacar de forma eficaz estos entornos, posibilitando el robo de información de tarjetas de crédito utilizadas por los compradores en dichos establecimientos. De esta forma, una actividad que ningún usuario consideraba que conllevaba un riesgo inherente, como es pagar la compra del supermercado, la gasolina, ropa, etc. comienza a suponer un peligro potencial del que ya han sido víctimas cientos de millones de personas en todo el mundo.

## APT

Las conocidas como APT (Advanced Persisten Threats) no dejan de ser un tipo de ataque dirigido cuyo objetivo son empresas o instituciones estratégicas. Detrás de estos ataques suelen estar países que invierten mucho dinero en conseguir que el ataque dirigido sea capaz de permanecer un largo tiempo sin detectar. Son la versión virtual de James Bond.

Si bien no veremos ataques masivos de tipo APT durante 2015, sí se descubrirán nuevos casos que seguramente llevan ocurriendo desde hace años pero que ahora salen a la luz.

## INTERNET OF THINGS

El número de dispositivos conectados a Internet está creciendo de forma exponencial, y no estamos hablando de ordenadores o teléfonos móviles, sino de otros dispositivos.

Desde cámaras IP a impresoras, todos estos "nuevos" dispositivos que forman parte de la red tienen una característica que los hace muy propicios como objetivo de los ciberdelincuentes: son dispositivos a los que los usuarios les prestan muy poca atención, por lo que raramente son, por ejemplo, actualizados.

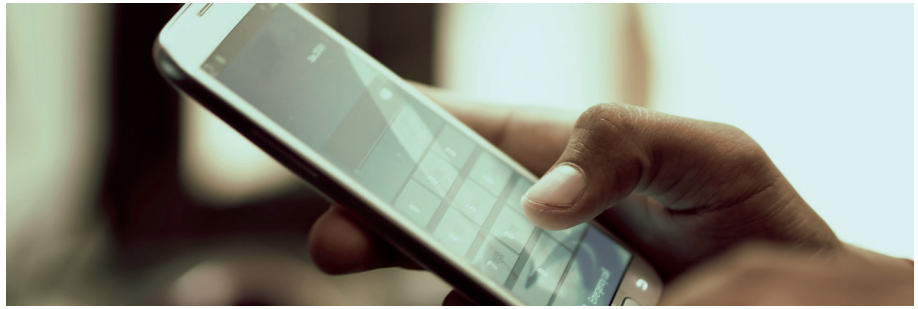
De esta forma, en cuanto se encuentra un fallo de seguridad que afecte al software de uno de ellos para cualquier ciberdelincuente, comprometer dicho dispositivo se convierte en un juego de niños.

Para empeorarlo aún más, estos dispositivos, a su vez, están conectados a redes internas, bien sea en hogares o empresas, por lo que se convierten en los puntos de entrada ideales para llevar a cabo todo tipo de ataques a gran escala.

## MÓVILES

Los ataques a smartphones, más concretamente a aquellos que utilizan Android, van a pasar a un nuevo nivel.

No sólo aumentarán los ataques sino que también lo hará la complejidad de los mismos, con un objetivo común: el robo de credenciales. Cada vez tenemos más información en nuestros smartphones, y los ciberdelincuentes van a tratar de obtenerla a cualquier precio.



Si bien hace apenas un par de años el malware en móviles era aún algo anecdótico, sólo en 2014 han aparecido más muestras de malware para Android que todas las aparecidas en la historia para cualquier dispositivo móvil.

Todo hace apuntar que durante 2015 el crecimiento será exponencial, aumentando también el número de víctimas, por lo que el uso de productos antivirus para estos dispositivos va a ser imprescindible.

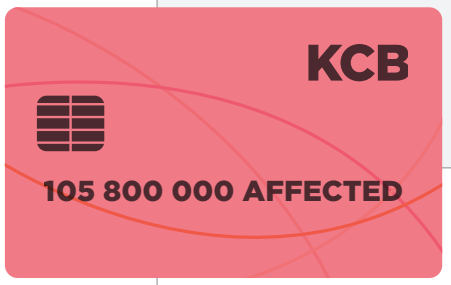
# PRINCIPALES ATAQUES DE 2014

## KCB

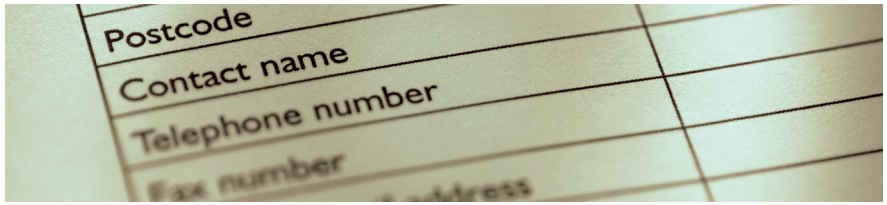
Korea Credit Bureau (KCB), compañía financiera coreana, fue víctima de un ataque por el que le robaron 105,8 millones de cuentas de usuarios que incluían detalles de tarjetas de crédito, nombre y apellidos, teléfonos, direcciones e incluso números de pasaporte.

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 vieron cómo todos sus datos personales fueron robados. Para un país con menos de 50 millones de habitantes esto quiere decir que, como mínimo, un 42% de la población fue 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.

En este caso, no se utilizó malware para acceder a la información. El ladrón trabajaba para KCB -irónicamente en el departamento anti-fraude de la compañía-, y durante 11 meses copió toda la información y la vendió al mejor postor. Si la información hubiera estado debidamente cifrada, el daño causado hubiese 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.

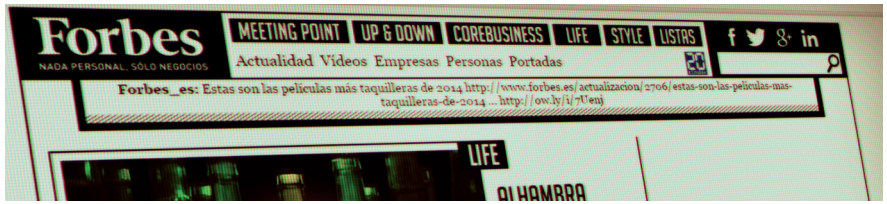


## ORANGE




Una vulnerabilidad en la web de la multinacional francesa Orange permitió a los atacantes hacerse con datos de cientos de miles de clientes, entre los que figuraban nombres, apellidos, direcciones y números de teléfono. 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.

## FORBES




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 figuraban los nombres y direcciones de correo electrónico de los usuarios, así como las contraseñas (cifradas). Y peor aún, SEA publicó los datos robados en Internet.

## EBAY Y PAYPAL


En mayo, eBay nos sorprendía pidiendo a los usuarios de PayPal en la página web de pagos online de su propiedad que cambiaran sus contraseñas de acceso.

Parece que la compañía había confirmado que los ciberdelincuentes habían accedido, un par de meses antes, a las cuentas de algunos empleados.

Esto les habría dado acceso a la red interna de la empresa y, desde allí, a la base de datos con nombres de usuarios, teléfonos, direcciones de correo electrónico y contraseñas.

Eso sí, aseguraron que ni los datos bancarios ni las tarjetas de crédito de sus clientes se habían visto comprometidos.

## DOMINO'S PIZZA

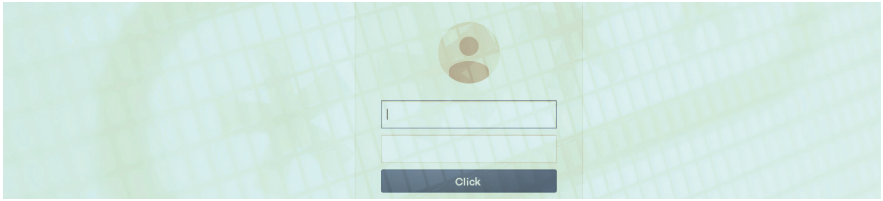

La conocida multinacional Domino's Pizza fue atacada por un grupo denominado "Rex Mundi", y le fueron sustraídos datos de 650.000 clientes de Francia y Bélgica, solicitando un rescate por dicha información. Los responsables de la empresa dijeron que no estaban dispuestos a ceder al chantaje.

## CELEBGATE: IMÁGENES DE HOLLYWOOD EN LA RED


En septiembre se produjo el ataque del que más se ha hablado durante este 2014: el CelebGate.

La filtración de imágenes íntimas de la ganadora del Óscar en 2013, Jennifer Lawrence, así como de otras modelos y actrices a través del foro /b/ de 4Chan, dio mucho de qué hablar. Apple aseguró 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". De esta manera, Apple negó que el hackeo a estas cuentas se produjera por una vulnerabilidad en servicios como iCloud o 'Find my iPhone'.

## GMAIL, ROBO DE CINCO MILLONES DE CONTRASEÑAS



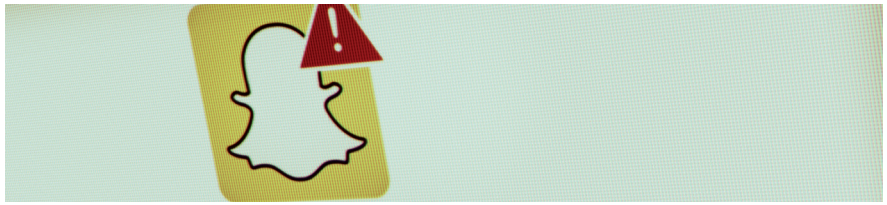

Un foro de ciberseguridad ruso publicó el mes de septiembre un archivo con más de cinco millones de cuentas de Gmail. Según varios expertos, más del 60% de las combinaciones de usuarios y contraseñas eran válidas. Sin embargo, Google afirmó que esta información estaba "desactualizada", es decir, que estas cuentas o no existían o sus usuarios no accedían a ellas. Al igual que Apple, aseguró no tener evidencia de que sus sistemas fueran comprometidos.

## VIATOR

También en septiembre, Viator sufrió un ataque de seguridad mediante el que los ciberdelincuentes consiguieron acceder a datos bancarios de sus usuarios. Según aseguró la compañía, el ataque se produjo entre el 2 y 3 de septiembre. Parece ser que Viator fue consciente del hackeo debido a las quejas de sus clientes sobre cargos no autorizados en las tarjetas utilizadas en su servicio.

Como siempre y, para evitar en lo posible el robo de más datos, Viator les pidió que cambiaran su contraseña de acceso a la cuenta, y que prestasen atención a los movimientos de las tarjetas de crédito.

## SNAPCHAT



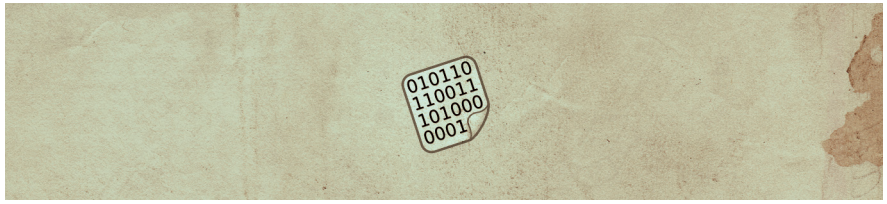
Tras las modelos y actrices, en octubre fueron las personas registradas en Snapchat quienes vieron comprometida la seguridad de sus archivos.

Snapchat es una aplicación móvil con la que se pueden enviar fotos y mensajes que se eliminan entre uno y diez segundos después de haberlos leído. Aunque Snapchat no guarda las imágenes de sus usuarios, otra aplicación, Snapsave, disponible para Android e iOS, sí lo hace, lo que permitió el robo de 200.000 fotografías.

## HOME DEPOT

Home Depot, gigante minorista del bricolaje, confirmó el ataque informático a sus servidores, reconociendo que se comprometieron 56 millones de tarjetas. Según asegura The Wall Street Journal <http://online.wsj.com/articles/fraudulent-transactions-surface-in-wake-of-home-depot-breach-1411506081>, la compañía también reconoció que, en algunos casos, se vaciaron las cuentas asociadas a estas tarjetas.

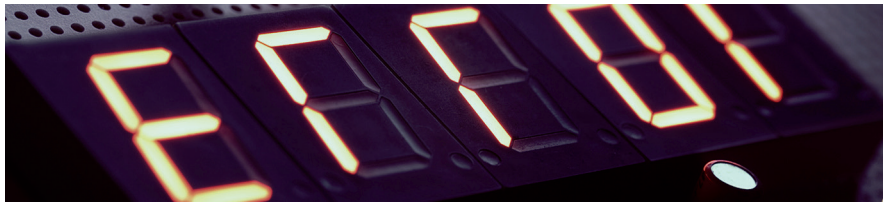
## DROPBOX




Un usuario de la web Pastebin, punto de encuentro para hackers y especialistas en seguridad informática, aseguró disponer de las contraseñas de siete millones de usuarios de Dropbox y, para demostrarlo, compartió una parte de ellos.

A través de su Blog oficial, Dropbox no tardó en anunciar que sus servicios no fueron hackeados, sino que esos datos fueron robados de otros servicios y que serían los mismos empleados para acceder a su plataforma. ¿Las recomendaciones de Dropbox? No utilizar la misma contraseña para todos los servicios y activar la verificación en dos pasos.

## SONY



A finales de 2014 se produjo uno de los ataques más importantes dirigidos contra una compañía.

Aún se desconoce mucha información sobre el incidente, pero sus efectos han causado estragos a la firma japonesa: una semana sin poder conectar los ordenadores, borrado masivo de información, robo de todo tipo de información interna de la empresa... Los atacantes han publicado cinco películas aún sin estrenar, y amenazan con ir publicando información confidencial a discreción.

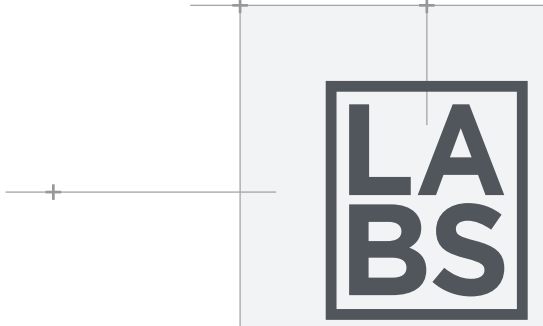
Además ha comenzado a aparecer malware con firma digital de Sony, cuyas claves fueron robadas junto al resto de los datos.

# SOBRE PANDA**LABS**

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.




facebook.com/PandaSecurityES
twitter.com/PandaComunica
plus.google.com/+pandasecurityES
youtube.com/PandaSecurity
linkedin.com/company/panda-security
www.pandasecurity.com/spain/mediacenter/