INFORME ANUAL PANDALABS 2015

panda

pandalabs

panda

pandalabs

1. INTRODUCCIÓN

1 Introducción

2015 ha sido un año en el que el mundo de la seguridad ha tenido un gran protagonismo. Por un lado, se han vuelto a batir todos los récords en la creación de malware, con más de 84 millones de nuevas variantes y, por otro, grandes empresas y páginas web de todo tipo han sido atacadas y sus datos de clientes robados. Por ello, millones de usuarios de todo el mundo se han visto afectados.

Mención especial merecen las cadenas hoteleras, que se han convertido en blanco de los ciberdelincuentes debido a la cantidad de datos que manejan, con millones de tarjetas de crédito utilizadas a diario.

Cryptolocker ha causado estragos en el mundo corporativo, ya que muchas de ellas están dispuestas a pagar un rescate para poder recuperar los datos secuestrados, lo que ha hecho que se multipliquen los ataques contra empresas.

Internet de las Cosas, (Internet of Things en inglés) comienza a tener mucho protagonismo en este informe, ya que parece que la seguridad en estos dispositivos es, en muchas ocasiones, bastante pobre.

A lo largo de 2015 hemos visto cómo diferentes especialistas han conseguido hackear coches, llegando a poder controlarlos de forma remota con las implicaciones que ello conlleva.

Pero no todo son malas noticias. Las empresas privadas y las fuerzas de seguridad de muchos países cada día colaboran de forma más cercana. Así se puede poner cerco a los criminales que circulan en la red. Es cierto que aún queda mucho trabajo por hacer, pero que los delitos no sean impunes es un buen síntoma.

Adobe Flash, una de las pesadillas en el mundo de la seguridad por todos los agujeros que tiene y que son utilizados para infectar a millones de usuarios de todo el mundo, parece que tiene sus días contados, ya que cada vez menos sistemas permiten su utilización.

Google es otra de las empresas que ha decidido dejar de soportar Flash (a través de su navegador Chrome), al igual que Amazon que ha decidido no permitir publicidad en su sitio web si se utiliza el hasta ahora popular formato.

2. EL AÑO EN CIFRAS

2

El año en cifras

2015 ha sido, otra vez, el año de la historia que más cantidad de malware se ha creado.

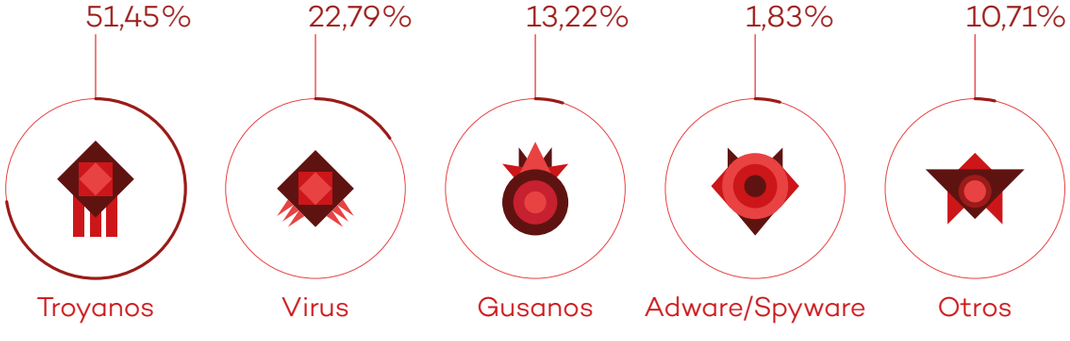
En total, han sido más de 84 millones de nuevas muestras detectadas y neutralizadas por PandaLabs, con una media de 230.000 al día.

Tenemos registradas 304 millones de muestras de malware, lo que significa que una de cada cuatro muestras de malware creadas en la historia de la informática, aparecieron el año pasado (27,63%).

Además de los troyanos, que siempre lideran las estadísticas en cuanto a creación de malware, cabe destacar los PUPs (Potentially Unwanted Programs, Programas Potencialmente No Deseados) y, cómo no, las diferentes familias de cryptolockers (o ransomware) que han estado causando estragos en todo el mundo secuestrando información y exigiendo un rescate a cambio.

Estos son los datos de la proporción de malware creado en 2015 por tipo:

NUEVO MALWARE CREADO
EN 2015, POR TIPO



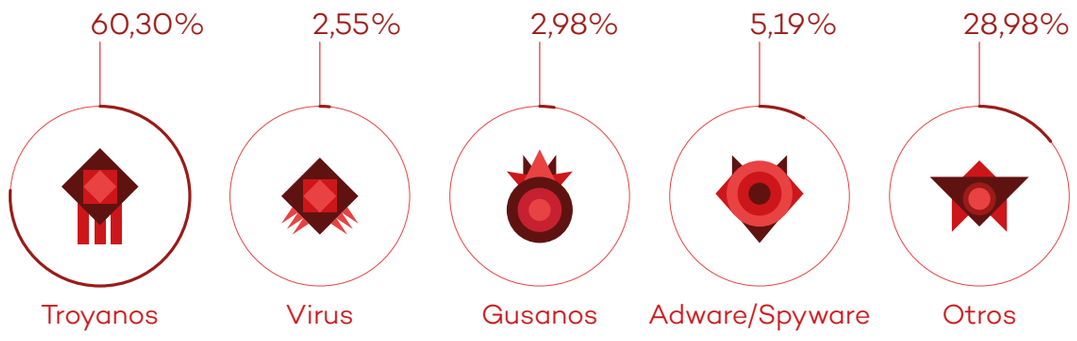
Los troyanos, como es habitual, están en primera posición con más del 50% de las muestras creadas a lo largo del año.

Sin embargo, la proporción respecto al año anterior ha disminuido a favor del resto de categorías, principalmente de virus (22,79%), gusanos (13,22%) y PUPs (10,71%).

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 60,30% de los casos.

Veamos cómo se reparten las infecciones en todas las categorías:

INFECCIONES POR TIPO DE MALWARE
2015



Podemos ver como los PUPs se posicionan en segundo lugar con casi un tercio de las infecciones, muy por delante del Adware/Spyware (5,19%), gusanos (2,98%) y virus (2,55%). Las técnicas agresivas de distribución junto a programas de software legítimos utilizadas por los PUPs hacen que consigan un alto ratio de instalación en los ordenadores de los usuarios.

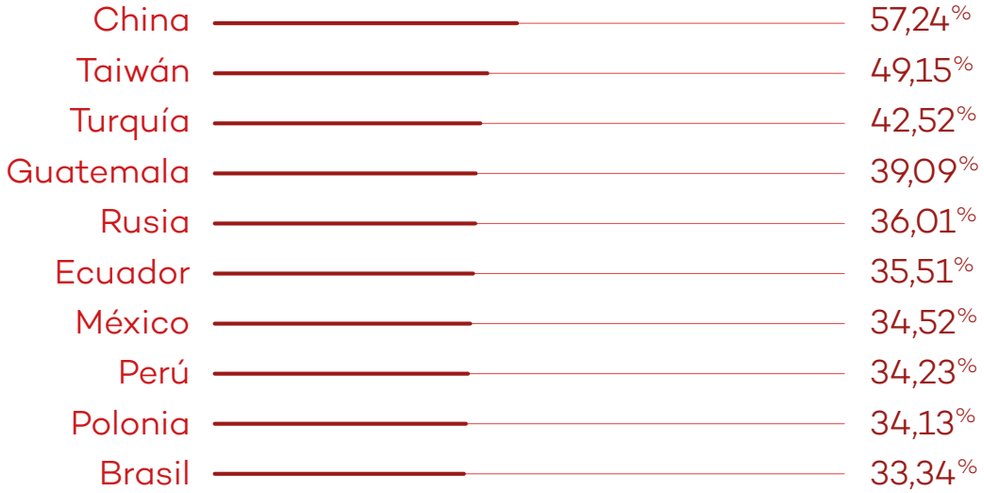
Si miramos al porcentaje global de ordenadores infectados, este es del 32,13%, cifra algo superior a la del año anterior, incremento debido a los PUPs.

Hay que destacar que se trata del porcentaje de ordenadores que han tenido algún tipo de encuentro con malware, lo que no significa necesariamente que se hayan infectado.

A nivel geográfico, los países más infectados del mundo están liderados por China, con un 57,24% de infecciones, seguida de Taiwán, con un índice de infección del 49,15%, y Turquía con un 42,52%.

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

PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN ESTE AÑO



Asia y Latinoamérica son las regiones con mayores infecciones. El resto de países, con un porcentaje mayor a la media mundial, son Colombia (33,17%), Uruguay (32,98%), Chile (32,54%) y España (32,15%).

Si analizamos los datos de los países mejor posicionados, aquellos cuyo índice de infección es más bajo, podemos observar que 9 de ellos son europeos, siendo Japón el único país no perteneciente al Viejo Continente. Los países escandinavos copan las primeras posiciones: Finlandia se sitúa a la cabeza, con un 20,32% de infecciones, seguido de cerca por Noruega con un 20,51%; y Suecia, con un 20,88% de infecciones.

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

PAÍSES CON MENOR ÍNDICE DE INFECCIÓN ESTE AÑO

El resto de países con un porcentaje menor a la media mundial son Australia (26,87%), Francia (27,02%), Portugal (27,74%), Austria (28,96%), Canadá (29,03%), Estados Unidos (29,48%), Venezuela (30,11%), Hungría (30,23%), Italia (31,84%) y Costa Rica (32,10%).

3. EL AÑO DE UN VISTAZO

3

El año de un vistazo

Cibercrimen

Si hay que destacar algún tipo de ataque durante 2015, sin duda alguna debemos hablar del ransomware, también conocido como Cryptolocker.

Este tipo de ataques afectan a todo el mundo, pero hemos visto cómo los delincuentes se centran en las empresas, ya que poseen información valiosa por la que están dispuestos a pagar un rescate.

Se sabe que las compañías infectadas, siempre que no cuenten con copia de seguridad, en muchas ocasiones acaban pagando el rescate para recuperar la información. En febrero supimos que una comisaría de policía de Illinois pagó hasta 500 dólares para recuperar la información de uno de sus ordenadores que había sido víctima de uno de estos ataques.

Los ciberdelincuentes utilizan diferentes técnicas para infectar y robar información de los usuarios. Una de las vías de entrada más comunes es la utilización de exploits, programas que explotan vulnerabilidades de programas instalados en las máquinas de sus víctimas.

En enero se supo que a su arsenal acababan de incorporar un nuevo exploit que afectaba a Flash Player. En este caso se trataba de una vulnerabilidad zero-day (día cero), lo que significa que era completamente desconocida y no existía actualización para corregirla en el momento de su descubrimiento.

Flash es uno de los componentes más atacados y que más vulnerabilidades tiene, casi al nivel de Java, otro de los grandes agujeros de seguridad presente en nuestros ordenadores.

Una de las "nuevas" técnicas (rescatadas del baúl de los recuerdos, ya que los primeros ataques de este tipo se registraron hace casi 20 años) por parte de los ciberdelincuentes para infectar a usuarios con ramsomware es el uso de macros en documentos de Office, principalmente de Word.

La mayoría de usuarios tienen una errónea sensación de seguridad ante un documento de texto porque piensan que no va a contener ningún tipo de amenaza. Sabiendo esto y siendo conscientes de que los filtros perimetrales no actúan contra este tipo de ficheros, se han incrementado de forma sustancial los ataques utilizando esta mecánica.

El punto débil de este ataque es que el usuario debe habilitar las macros, sin embargo los ciberdelincuentes son perfectamente conscientes de esto y han conseguido elaborar técnicas de ingeniería social realmente ingeniosas.

Una que descubrimos desde PandaLabs se trataba de un documento de Word que contenía una imagen difuminada.

En la parte superior del documento en mayúsculas y negrita aparecía un mensaje indicando que, por motivos de seguridad, la imagen estaba difuminada, y que si se quería acceder a la información se debían habilitar las macros, con una flecha apuntando al botón que se debía pulsar en Word para acceder a la activación de las mismas. Una vez activada la macro, te muestra la imagen sin difuminar mientras que al mismo tiempo te infecta con una variante de CryptoLocker.

Otro ransomware se ha hecho bastante popular, principalmente en Australia, aunque posteriormente se ha visto en otros países, debido a que usaba imágenes de la conocida serie de televisión Breaking Bad.

Cuando hablamos de phishing muchas veces lo relacionamos con mensajes que tratan de hacerse pasar por nuestro banco. Si bien los ataques de phishing comenzaron así, y aún hoy en día siguen siendo muy numerosos, las empresas cuyos clientes son objetivo de estos ataques no se limitan a entidades financieras.

En enero, ciberdelincuentes lanzaron un ataque de phishing haciéndose pasar por Apple. El remitente era "Apple Support", y como asunto utilizaba un truco recurrente: asustar al usuario con un supuesto problema de seguridad: "Tu ID de Apple ha sido suspendido".

El mensaje indicaba que alguien había tratado de acceder a tu cuenta desde un dispositivo no autorizado, y que iban a proceder a bloquearla. Para demostrar que efectivamente eras el usuario legítimo de la cuenta te proporcionaban un enlace que lleva a una página con el look & feel de Apple y en la que pedían gran cantidad de información: nombre completo, dirección, teléfonos, datos de tarjeta de crédito, etc.

En febrero la compañía norteamericana Anthem reconoció que fue víctima de un ataque en el que le robaron datos de 80 millones de clientes. Los ciberdelincuentes pudieron acceder a una base de datos gracias al uso de una contraseña robada con acceso al sistema. Se calcula que el coste del ataque para Anthem podría llegar a los 100 millones de dólares.

En marzo, la compañía norteamericana Slack envió un mensaje a todos sus usuarios indicando que habían detectado accesos no autorizados a una de sus bases de datos que contiene información del perfil de sus clientes. Aunque no fue robada información crítica (de hecho la compañía decía específicamente en su mensaje que no hacía falta cambiar la contraseña del servicio), se habilitó un sistema de doble factor de autenticación (2FA), recomendándose a todos sus usuarios que lo habilitaran para aumentar su protección.

Ryanair también fue víctima de un ataque en el que le sustrajeron cinco millones de dólares. Si bien no se han desvelado los detalles de cómo consiguieron los atacantes realizar el robo, se sabe que se produjo a través de una transferencia a un banco chino. La compañía denunció el caso e informó que habían conseguido congelar el dinero robado y que esperaban recuperarlo pronto.

La compañía norteamericana CareFirst BlueCross BlueShield, aseguradora médica, fue víctima de un ciberataque en el que le robaron información de 1,1 millones de clientes.

Cada vez las empresas están más en el punto de mira de delincuentes para robar información de forma masiva, y este simplemente es un ejemplo de los cientos de casos que suceden en todo el mundo.

AdultFriendFinder, una compañía de contactos online, sufrió un ataque en el que le robaron los datos de sus usuarios. Los atacantes la ofrecieron online al primero que pagara 70 bitcoins, unos 17.000 dólares al cambio en ese momento. Al poco tiempo, la base de datos al completo fue publicada en Internet.

LastPass, compañía líder en gestores de contraseñas, fue otra de las víctimas. Afortunadamente parece que los atacantes no lograron información de las contraseñas, aunque consiguieron los hashes de las claves de acceso maestras de sus usuarios. El complejo cálculo de estos hashes (salteados, con múltiples pasadas) hace muy complicado que los atacantes pudieran llegar a descubrir la contraseña real, a pesar de lo cual es

recomendable cambiarla si utilizamos una contraseña débil.

El Hard Rock Hotel & Casino de Las Vegas comunicó que han estado comprometidos durante ocho meses durante los que los atacantes pudieron robar información de sus clientes: nombres, números de tarjeta de crédito y débito y los códigos CVV de las mismas. Afectó a los clientes que pagaron en restaurantes, bares y tiendas del complejo, aunque no a los sistemas de pago del hotel y del casino. Este ataque recuerda a otros que hemos visto en el pasado (Target, Home Depot, UPS, Neiman Marcus) donde los terminales de punto de venta fueron infectados para robar la información de las tarjetas utilizadas por los clientes.

También ha habido rumores de que Uber había sido víctima de un ataque tras detectarse que usuarios de este servicio habían visto como desconocidos hacían uso de sus cuentas. Sin embargo, parece que todo fue debido a ataques de phishing donde los usuarios facilitaron sus credenciales a los atacantes tras ser engañados.

A finales de junio 1,4000 pasajeros de la aerolínea polaca LOT quedaron en tierra en el aeropuerto Chopin de Varsovia tras un ataque perpetrado contra el sistema informático de tierra de la compañía utilizado para confeccionar los planes de vuelo.

Uno de los mayores ataques sufridos por una empresa este año ha sido sin duda el de la empresa de contactos Ashley Madison. Los atacantes, autodenominados “Impact Team”, mostraron un mensaje en su página web exigiendo que cerraran el negocio o que publicarían toda la información robada.

Poco después, al no ceder la empresa al chantaje, publicaron un torrent con 10 Gb de información comprimida.

Entre la información publicada se encontraban los datos de sus 37 millones de clientes, transacciones realizadas, direcciones de correo, preferencias sexuales, etc. Además, también contenía todo tipo de documentación interna de la empresa.

Han sido descubiertas nuevas vulnerabilidades utilizadas por ciberdelincuentes como medio para acceder a sus víctimas. Además de las (tristemente) típicas aparecidas en Flash o en Java, el sistema operativo de Apple Mac OS X ha sufrido un par de ellas de mucha gravedad: la primera de ellas, descubierta por el investigador Stefan Esser, permitía tener acceso root y ya se ha visto utilizada por Adware como método de ataque en ordenadores Mac.

La segunda vulnerabilidad fue descubierta por investigadores de la compañía MyK. Se trataba de una vulnerabilidad en el sistema de administración de contraseñas que podría permitir a un atacante obtener todas las credenciales almacenadas.

Uno de los métodos de ataque que más se están popularizando es el que trata de comprometer routers de hogares y empresas, de tal forma que quedan bajo el control del atacante.

Se ha descubierto que routers de las empresas ASUS, DIGICOM, Observa Telecom, PLDT y ZTE incluyen credenciales predefinidas en su código. Esto permitiría a atacantes hacerse con el control de los mismos desde el exterior. Hay que recordar que los ataques que lanzaron un DDoS contra Xbox Live y PSN en navidades de 2014 utilizaron un ejército de routers infectados que tenían bajo su control.

Adobe Flash, conocido por sus casi infinitos agujeros de seguridad, podría morir en breve. iOS no permitía su ejecución desde los inicios del sistema operativo, en Android tampoco se ejecuta. Ahora Google ha ido un paso más y bloquea todo el contenido Flash que haya en una web si se navega desde su navegador Chrome. Y el gigante de las ventas online Amazon también ha anunciado que prohíbe en su plataforma cualquier anuncio que esté en este problemático formato. Aunque no vaya a desaparecer completamente, parece que la estocada dada a Adobe Flash este 2015 puede ser mortal, algo que, sin duda, mejorará la seguridad de todos los usuarios.

El FBI ha detenido a 5 individuos que estuvieron envueltos en el hackeo sufrido por JPMorgan en 2014. En este ataque consiguieron hacerse con las credenciales de un empleado, y luego fueron utilizadas para acceder a 90 servidores de la compañía y robar información perteneciente a 76 millones de individuos y 7 millones de empresas, todos ellos clientes de la entidad.

Microsoft, en su estrategia de mejora de la seguridad de sus productos y soluciones, ha decidido doblar la máxima recompensa que da a investigadores capaces de descubrir nuevos errores críticos en sus soluciones, pasando de 50.000 a 100.000 dólares.

Si bien este tipo de recompensas es habitual en empresas tecnológicas, aún no lo es tanto en otros sectores, aunque cada vez son más las empresas que recurren a ellas para que los investigadores que descubran algún problema se lo comuniquen antes de vender la información a otro postor.

Es el caso de United Airlines, la aerolínea con base en Chicago, que tiene la peculiaridad de dar recompensas en millas. Ha reconocido que ha llegado a dar hasta un millón de millas a investigadores que les han informado de errores para que pudieran ser solucionados.

El FBI también ofrece recompensas, aunque en este caso están dedicadas a quienes colaboren con información que ayude a detener a los ciberdelincuentes más buscados. La recompensa más alta es de 3 millones de dólares para cualquiera que pueda ayudar a capturar a Evgeniy Mikhailovich Bogachev, la mente criminal que está tras la red de bots Gameover ZeuS.

Las cadenas hoteleras están en el punto de mira de los ciberdelincuentes. Además del caso comentado anteriormente que afectó al Hard Rock Hotel & Casino de Las Vegas, ha habido otros: la cadena Hilton, la cadena Starwood (Westin, Sheraton, etc.), Las Vegas Sands Casino, Trump Hotels, Mandarin Oriental, FireKeepers Casino and Hotel, etc. Una larga lista que sin duda se irá incrementando, ya que si algo tienen los hoteles son millones de clientes que utilizan millones de tarjetas de crédito. Raro es el hotel que hoy en día no solicita a sus clientes la tarjeta de crédito por los gastos que pueda ocasionar en su estancia, así que los ataques no ya a los servidores de estas empresas, sino a sus puntos de venta, están en auge (algo que sabemos que funciona muy bien tras lo que le sucedió a Target, donde un malware de punto de venta robó 46 millones de datos de tarjetas de los clientes que compraban físicamente en sus tiendas).

La compañía juguetera VTech sufrió una brecha de seguridad en la que fueron comprometidos los datos de 4,98 millones de padres y 6,37 millones de niños. Semanas después de producirse el ataque la policía inglesa arrestó a una persona de 21 años en relación a este ataque.

Muchas otras empresas y páginas han sido víctimas de ataques similares, como T-Mobile, a quien le robaron datos de hasta 15 millones de clientes, sanriotown.com a quien le fueron robados los datos de 3,3 millones de fans de Hello Kitty, etc.

Redes sociales

En enero, al mismo tiempo que Obama daba a conocer una serie de iniciativas legislativas para ayudar en la lucha contra la ciberdelincuencia, un grupo de atacantes relacionados con ISIS se hicieron con el control de las principales cuentas de redes sociales del pentágono.

Uno de los ataques más extendidos que suceden hoy en día en Facebook es el que trata de regalarnos tarjetas de alguna empresa popular. En enero fuimos testigos de uno de estos engaños por el que en cuestión de horas cayeron miles de personas de todo el mundo. En este caso, crearon un evento en Facebook prometiendo repartir 430 tarjetas regalo de ZARA de 500€ cada una. Para participar en el supuesto sorteo debías unirte al evento, escribir en tu muro “Gracias Zara”, e invitar a 50 de tus contactos. En muy poco tiempo más de 5.000 personas se habían unido, enviándose más de 124.000 invitaciones.

Todas las conexiones del usuario con los servidores de Facebook, incluidos los mensajes que envías y recibes, se transmiten ya mediante el protocolo seguro HTTPS. Por si esto fuera poco, la red social también estableció su servicio en la red Tor para que los usuarios más exigentes en materia de privacidad pudieran estar tranquilos. Sin embargo, además de las conexiones que establecen los usuarios a través del propio servicio, hay otras comunicaciones que se realizan vía Facebook de forma indirecta, a través de correo electrónico. Son las notificaciones que te llegan, por ejemplo, cuando un amigo te ha enviado un mensaje directo (salvo que lo hayas desactivado).

Como la seguridad de estos mensajes no estaba tan garantizada, Facebook ha anunciado que, a partir de ahora, todos sus usuarios podrán recibirlos – si así lo deciden – protegidos por el popular software de cifrado Pretty Good Privacy (PGP).

PGP oculta los emails de cara a los posibles intrusos a partir de un sistema de claves basado en una pública (que debe tener el emisor del mensaje) y otra privada (que solo tienes el receptor).

El proceso de configuración es sencillo: Acceder a nuestro perfil, entrar en el apartado 'Información' e ir a 'Información básica y de contacto', donde podremos introducir aquí nuestra clave pública PGP (si no sabes qué es o cómo conseguirla, lo mejor es que leas un tutorial), que se mostrará en el perfil, a disposición de cualquiera que desee mandarnos un correo electrónico cifrado.

Debajo del cuadro veremos una casilla que tendremos que marcar si queremos que todos los correos que nos envíe Facebook, a partir de ahora, también incorporen esta capa de seguridad. Como siempre que se emplea el cifrado, es muy importante que recordemos la clave que establecimos para proteger nuestro correo electrónico con PGP. Si algún día la olvidáramos, no podríamos leer las notificaciones de Facebook, y podríamos llegar a perder nuestra cuenta en la red social.

WhatsApp es un gancho habitual para atraer usuarios y tratar de infectarles. Hemos detectado un bulo con el que pretenden enganchar a los usuarios de la aplicación de mensajería instantánea.

En concreto, se llama WhatsApp Trendy Blue. Una nueva "versión" que promete nuevas opciones de personalización de WhatsApp cuando, en realidad, lo único que hace es suscribir al usuario a un servicio de tarificación especial, no precisamente barata.

Este programa exige que la invitación de, al menos, 10 de nuestros contactos a los que les llegará nuestro mensaje para que se inscriban en esta web fraudulenta.

Facebook anunció que estaba estudiando incorporar un botón de “No me gusta”, y, como era de esperar, los ciberdelincuentes se pusieron manos a la obra para ser los primeros en darnos esta opción. En pocas horas comenzaron a aparecer todo tipo de engaños prometiendo añadir el famoso botón, buscando en todos los casos víctimas a las que poder robar información.

Móviles

Comenzamos 2015 con una amenaza que en buena medida nos recuerda a los antiguos gusanos de correo electrónico o de mensajería instantánea, apoyándose esta vez en los SMS.

El ataque comienza cuando recibes un SMS preguntándote si esa es tu foto, y un enlace a la supuesta fotografía. Dicho enlace realmente descarga un fichero .APK, aplicación para móviles Android. Si el usuario la instala, la aplicación maliciosa enviará un SMS idéntico al recibido a toda tu lista de contactos.

Fujitsu, en colaboración con la operadora japonesa NTT Docomo, ha lanzado su terminal Arrows NX F-04G basado en Android, y se ha convertido en el primer móvil Android que incluye como capa de seguridad el escaneo del iris, un método biométrico mucho más seguro y fiable que el popularizado lector de huellas dactilares que utilizan terminales populares de la competencia, como el Apple iPhone 6 o el Samsung Galaxy S6.

En junio detectamos una campaña de phishing dirigida a desarrolladores de Android que publican sus creaciones en Google Play, la tienda de apps oficial del popular sistema operativo. El campo “De” del mensaje dice “Play Developer Support”, con el asunto “Update your Account Informations”. Al pinchar en el enlace proporcionado, eres redirigido a una página web que parece de Google, donde te solicitan las credenciales.

Los ataques de phishing están diseñados para robar las credenciales y la identidad del usuario, por eso son extremadamente populares los ataques dirigidos a clientes de entidades

financieras y de todo tipo de plataformas de pago.

Este caso, sin embargo, es diferente ya que no están buscando vaciar la cuenta bancaria del usuario, quieren esas credenciales porque pueden usarlas para propagar malware a través de Google Play.

Lo más preocupante es lo fácil que resultaría para los delincuentes el automatizar todo este proceso.

Lo único que necesitan es:

- Construir una "araña" (crawler, hay unos cuantos proyectos de código abierto que les pueden ayudar en esta tarea) para descargarse información de todas las apps publicadas en Google Play.
- Analizar toda esa información para obtener las direcciones de correo de los diferentes desarrolladores.
- Enviar una campaña personalizada de phishing, incluso la página web podría ser personalizada para el desarrollador específico, hacienda que el engaño sea mucho más creíble y obtener un mejor "ratio de conversión".
- Como el atacante tiene la información de todas las apps publicadas por cada desarrollador, podría elaborar un sistema de alarma que le alertara cada vez que un desarrollador con una app popular (millones de descargas) hubiera caído en la trampa.

Desde este punto, uno de los más fáciles (y poco sofisticados) ataques sería publicar apps maliciosas desde esa cuenta. Imaginad que alguien consigue robar las credenciales de los desarrolladores de Candy Crush y publicaran Candy Crush 2 desde la misma cuenta...

Si los atacantes fueran más hábiles y encontraran una forma de modificar la aplicación sin utilizar la llave privada (que no puede ser obtenida con las credenciales robadas), podrían publicar y actualizar cualquier app. En el ejemplo anterior, imaginad que los atacantes crean una actualización de Candy Crush que incluye un troyano: cientos de millones de usuarios se lo descargarían e instalarían sin sospechar nunca que están siendo comprometidos.

Google ha creado crea un nuevo programa bajo el nombre de Android Security Rewards que recompensará las contribuciones de los investigadores de seguridad que descubran nuevas vulnerabilidades en Android.

La cuantía de la de recompensa se basa en la gravedad de las vulnerabilidades, la cantidad base son 2.000 dólares para vulnerabilidades críticas, 1.000 para las de gravedad alta, y 500 para las moderadas. Sin embargo, en función de la gravedad del problema, la calidad del informe, etc. pueden subir hasta los 38.000 dólares.

En julio, la empresa Zimperium dio a conocer una gravísima vulnerabilidad en Android que afecta a 950 millones de dispositivos con este sistema operativo. La gravedad no sólo reside en la cantidad de móviles, tablets y demás aparatos afectados, sino en lo sencillo que resulta comprometer de forma remota cualquiera de ellos. Simplemente enviando un MMS malicioso puedes hacerte con el control de cualquier teléfono, por lo que sólo haría falta poseer el número de

teléfono de la víctima. Ni siquiera es necesario abrir dicho MMS, ya que Android procesa las imágenes de forma automática, así que sólo con recibirlo ya puede infectar nuestro terminal.

Aunque se ha corregido el problema, la gran cantidad de diferentes fabricantes y versiones del sistema operativo que existen en el mercado hacía temer que la solución no fiera aplicada a un gran número de terminales. Sin embargo Google ha convencido a la mayoría de grandes fabricantes (Samsung, Sony, LG, Motorola, etc.) para que pongan esta actualización a disposición de sus clientes.

Además tanto Google como Samsung han anunciado que van a ofrecer actualizaciones mensuales a sus clientes para soluciones las diferentes vulnerabilidades que vayan apareciendo en Android.

De hecho, poco después dos investigadores del equipo XForce de IBM publicaron otro problema de seguridad que permitía a un atacante sustituir una aplicación legítima instalada por una maliciosa, de tal forma que esta última podría tener acceso a todos los permisos de la que estaba sustituyendo. Google ya ha publicado la actualización que soluciona este nuevo problema de seguridad.

Si bien estamos acostumbrados a ver ataques de ransomware en PC, ya se han visto algunos intentos en Android, de hecho uno aparecido durante estos meses llamó la atención por su originalidad a la vez que simpleza. Lo que hace la aplicación maliciosa es cambiar el código PIN del terminal y solicitar un rescate de 500 dólares. En cualquier caso, este tipo de estrategia tiene sus limitaciones. Por ejemplo, los usuarios del antivirus de Panda para Android pueden cambiar el código PIN de su móvil desde su panel de control web desde otro lugar, anulando el ataque de los ciberdelincuentes sin tener que pagar un solo dólar.

El sistema operativo móvil de Apple también ha sufrido numerosos ataques en este periodo.

La compañía Appthority ha descubierto una vulnerabilidad bautizada como Quicksand que afecta a las instalaciones y despliegues corporativos que hacen uso de sistemas MDM (Mobile Device Management) y que podría permitir el acceso a información confidencial de la compañía. Apple lo ha solucionado a partir de la versión de iOS 8.4.1.

Otra vulnerabilidad solucionada con esa actualización se llama Ims0mnia, que permite a una aplicación maliciosa evitar las restricciones de ejecución en segundo plano de Apple. Por ejemplo, se podría activar en segundo plano el micrófono y la cámara del usuario para espiarle.

Apple tuvo que retirar numerosas aplicaciones de su App Store debido a un ataque conocido como XcodeGhost. Los

atacantes publicaron una versión modificada del software de desarrollo de aplicaciones para iOS, de tal forma que aquellos desarrolladores que lo utilizaron para desarrollar sus apps incluían funcionalidad maliciosa sin su conocimiento.

Otro ataque sufrido por usuarios de Apple consiguió credenciales de iCloud de 225.000 usuarios. El ataque afecta a usuarios que previamente habían hecho un jailbreak de su dispositivo, lo que elimina controles de seguridad instalados en iOS y es utilizado por usuarios para instalar aplicaciones sin tener que hacer uso de la App Store.

Internet of Things

En julio HP Fortify publicó los resultados de un estudio realizado sobre smartwatches, donde encontraron que el 100% de los dispositivos analizados eran vulnerables.

Si bien cualquier dispositivo puede ser vulnerable a ataques en un momento dado, en este estudio daban pistas de los principales problemas encontrados. Por ejemplo, ninguno de los smartwatches disponía de doble autenticación a la hora de vincularlo a un móvil, y permitían meter contraseñas equivocadas de forma repetida.

Los investigadores de seguridad Charlie Miller y Chris Valasek hicieron una demostración en Julio que dejó a todo el mundo boquiabierto.

Convencieron a Andy Greenberg, periodista de Wired, para que condujera un Jeep Cherokee mientras los 2 investigadores le hackeaban el coche desde la casa de uno de estos.

El ataque comenzó mostrando la toma de control de algunos elementos del coche no críticos: encendieron el aire acondicionado al máximo, activar el limpiaparabrisas, cambiar la emisora de radio y subir el volumen, poner una foto suya en la pantalla del coche... hasta llegar a desactivar el acelerador, los frenos... llegando a tener un control total del vehículo.

Llevaban varios meses trabajando en estos ataques, y de hecho se los habían comunicado al fabricante en 2014, lo que le había dado la oportunidad de publicar una actualización que solucionara el problema. Los investigadores hablaron más en detalle del problema en la charla que dieron en agosto en la BlackHat, una de las conferencias de seguridad más importantes del año que tiene lugar en Las Vegas.

También en julio Land Rover avisó que debía actualizar 65.000 vehículos por un fallo en el software de determinados modelos que llevaban a la venta desde 2013 y que permitía que se pudieran desbloquear las puertas.

Los investigadores Kevin Mahaffey y Marc Rogers mostraron en Defcon, conferencia de seguridad que tiene lugar a continuación de la BlackHat, cómo hackear un Tesla Model S. Si bien necesitaban acceso físico al coche para poder llevar a cabo este ataque, decubrieron 6 nuevas vulnerabilidades que les permitían hasta parar el motor cuando se circulaba a baja velocidad. El fabricante ya ha publicado la actualización que

parchea las 6 vulnerabilidades.

Hiroyuki Inoue, profesor asociado en la Hiroshima City University's Graduate School of Information Sciences, llevó a cabo un experimento en el que conectando un Toyota Corolla a Internet, conseguñian hackearlo y hacer que remotamente se pudieran manipular las ventanillas del coche, manipular el medidor de velocidad, bloquear el acelerador, etc.

Si bien este experimento incluye añadir al coche conexión a Internet –algo que no tiene por defecto- es una llamada de atención para todos los fabricantes que están trabajando en soluciones que conectan a sus coches a la red de redes.

Ciberguerra

Por primera vez en la historia, Estados Unidos impuso sanciones a un país en respuesta a un ciberataque.

El país en cuestión era Corea del Norte, debido a su implicación en el ataque contra Sony a finales de 2014, que se cree motivado por el estreno de la película The Interview, una comedia donde la CIA pedía a unos periodistas asesinar al líder norcoreano.

Siguen publicándose nuevos datos de los documentos filtrados por Edward Snowden a la prensa. En enero, el diario alemán Der Spiegel daba a conocer que China se había hecho con Terabytes de datos sobre el caza F-35, incluyendo información sobre el sistema de radar, esquemas de los motores, etc.

El viceconsejero de Seguridad Nacional de la Casa Blanca, Ben Rhodes, comunicó que la Casa Blanca había sido víctima de un ataque informático. En una entrevista con CNN, Rhodes afirmó que los atacantes obtuvieron acceso no autorizado al sistema no clasificado de los ordenadores y robaron información de gran importancia, aunque el sistema clasificado no fue hackeado. Lo que no quiso confirmar Rhodes es si el ataque había sido realizado por hackers rusos ni cuándo había tenido lugar, pero sí dio a entender que no se había producido durante los últimos días. Sin querer entrar en más detalles, durante su intervención comentó que ya tomaron "una serie de medidas de seguridad para evaluar y mitigar los daños".

En junio supimos que la Office of Personnel Management (OPM), agencia del gobierno federal estadounidense de recursos humanos fue comprometida y robaron información personal de, al menos 4, millones de trabajadores públicos. El ataque tuvo lugar 2 meses antes, aproximadamente al mismo tiempo que la Casa Blanca fue comprometida. Sin embargo parece que ambos ataques no están conectados, ya que este último parece ligado claramente a atacantes chinos, aunque el gobierno no hizo ninguna declaración oficial al respecto.

Simpatizantes de ISIS atacaron a la cadena de televisión francesa TV5MONDE, consiguiendo sabotear la emisión. No sólo consiguieron esto, sino que tomaron el control tanto de su página web como de su página de Facebook.

El conocido grupo Syrian Electronic Army consiguió comprometer la página web de la armada de Estados Unidos, publicando contenido propagandístico a favor del régimen sirio de Assad.

El parlamento alemán fue víctima de un ataque donde consiguieron comprometer diferentes ordenadores y llegaron a robar información de los mismos. Se cree que el ataque vino de Rusia, aunque es difícil que se pueda llegar a demostrar quién estuvo realmente detrás del mismo.

Hemos conocido que la NSA utilizó una versión modificada de Stuxnet para sabotear el programa nuclear de Corea del Norte, aunque en esta ocasión no tuvieron éxito. Hay que recordar que con Stuxtet lograron destruir al menos 1.000 centrifugadoras de uranio de una planta en Natanz, Irán.

Hacking Team es una empresa conocida por ser proveedora de herramientas de ciberespionaje y ciberataque para multitud de gobiernos de todo el mundo.

En julio sufrieron un hackeo masivo en el que les robaron todo tipo de información. El ataque se dio a conocer a través de la propia cuenta de Twitter de Hacking Team, también comprometida por el atacante, en la que se cambió su nombre a “Hacked Team” y se daba un enlace para poder descargar por torrent la información sustraída:

Se hicieron públicos listados de clientes (agencias de policía y de inteligencia de multitud de países, desde Estados Unidos a Uzbekistán). Se hizo público un certificado corporativo de desarrollador utilizado por Hacking Team, contraseñas que utilizaban en sus sistemas más protegidos, listas de productos que vendían, código fuente de sus aplicaciones, datos financieros, etc. Incluso se publicó una web con un buscador que permitía hacer una búsqueda entre todos los correos electrónicos que tenían almacenados en Hacking Team.

Pocos días después se descubrió un Zero Day en Adobe Flash gracias a la información robada a Hacking Team.

James Comey, director del FBI, dijo en un foro de seguridad que habían detectado un creciente

interés por parte de terroristas sobre estrategias para lanzar ataques ciberterroristas contra Estados Unidos.

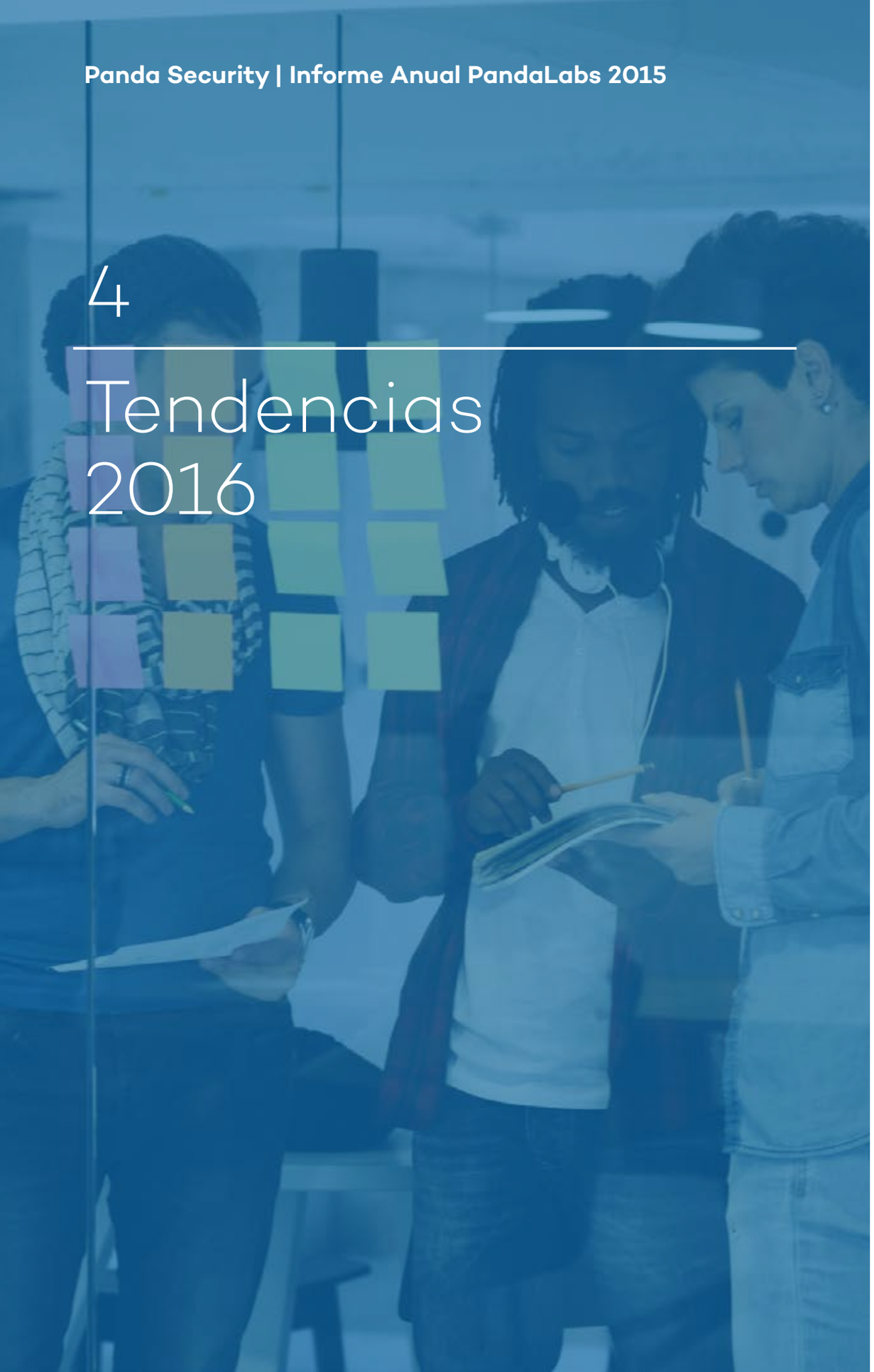
No especificó el tipo de ataques y dijo que parecía que estaban todavía en los inicios de planificación, tratando de ver cómo de efectivos podrían llegar a ser, pero que potencialmente se trata de un problema que puede ir a más.

El 25 de julio, hackers rusos consiguieron comprometer el sistema de correo electrónico no clasificado del Pentágono, del que robaron información. Según fuentes oficiales, se trató de un ataque muy sofisticado y que claramente había algún gobierno detrás del mismo.

En septiembre, investigadores de DGI publicaron un trabajo sobre la unidad del ejército chino 78020, donde mostraban que era quien estaba detrás del grupo conocido como Naikon, que está detrás de diferentes ataques de ciberespionaje con objetivos militares, diplomáticos y económicos en diferentes países de la zona. Entre sus víctimas a lo largo de cinco años se encuentran Camboya, Indonesia, Laos, Malasia, Myanmar, Nepal, Filipinas, Singapur, Tailandia, Vietnam, el Programa de Desarrollo de Naciones Unidas y la Asociación de Naciones del Sudeste Asiático.

Anonymous ha lanzado una campaña en contra de los terroristas de ISIS, hackeando y exponiendo sitios web y miles de cuentas de redes sociales pertenecientes a miembros del autoproclamado “Estado Islámico”.

4. TENDECIAS 2016



4 Tendencias 2016

A continuación vamos a tratar de ver cuáles son las principales tendencias que veremos a lo largo de 2016 en el ámbito de la seguridad informática.

1.- Exploit kits

Seguirán siendo la herramienta favorita de ciberdelincuentes para conseguir infecciones de forma masiva. Los exploit kits se pueden comprar en el mercado negro y además sus responsables ofrecen actualizaciones para incluir cualquier exploit que se descubra y pueda ser utilizado para conseguir nuevas víctimas. Muchas soluciones de seguridad aún no son capaces de combatir este tipo de ataques de forma eficaz, lo que hace que su ratio de conversión sea muy alto.

2.- Malware

El número de nuevos ejemplares de malware seguirá creciendo. Si bien la mayoría de ejemplares seguirán siendo ficheros de tipo PE (https://es.wikipedia.org/wiki/Portable_Executable), prevemos un aumento de malware de tipo no PE, principalmente scripts. No sólo el conocido javascript, sino que habrá un especial aumento del uso y abuso de Powershell, una herramienta de Microsoft que viene por defecto con Windows 10, permitiendo ejecutar scripts con todo tipo de funcionalidades. Se combinará también con ataques conocidos como “Fileless Attacks” (ataques sin ficheros), donde por ejemplo el código malicioso en lugar de estar en un fichero físico en el ordenador es un parámetro en la ejecución de un comando, o una entrada en el registro que contiene el script a ejecutar.

3.- Ataques dirigidos

Habrá un aumento de ataques dirigidos. El uso de técnicas de rootkit, que permiten al atacante ocultarse de la vista del sistema operativo y de las soluciones de seguridad se intensificará en este tipo de intrusiones. Las empresas se van a ver obligadas a tomar medidas de seguridad extra para estar protegidas ante esta amenaza real que puede dañar seriamente la imagen y las finanzas de las víctimas, teniendo en cuenta que puede tener como objetivo tanto información confidencial de la empresa (datos financieros, planes estratégicos, etc.) como datos de clientes de la misma.

4.- Malware Android

Aumentará el malware para móviles, especialmente para Android ya que es el sistema operativo con mayor cuota de mercado. Veremos cómo cada vez aparecen más amenazas que rootean el dispositivo, de tal forma que eliminarlo sea una tarea casi imposible para los antivirus, salvo aquellos que vengan instalados de fábrica.

5.- Plataformas de pago móvil

No está aún del todo claro que 2016 sea el año en el que definitivamente se popularicen las plataformas de pago móvil, lo que sí sabemos es que su uso va a ir aumentando y que van a estar en el punto de mira de los ciberdelincuentes, ya que puede ser una vía para robar dinero de forma directa. Si alguna de las plataformas se impone claramente sobre el resto, será la principal candidata a ser analizada por los atacantes para descubrir debilidades en el sistema que permitan su abuso.

6.- Internet of Things

Sabemos que 2016 no va a ser el año del Internet de las Cosas, pero cada vez vamos a tener más dispositivos conectados a Internet y veremos numerosas pruebas de concepto que mostrarán diferentes ataques que se pueden llevar a cabo, como los que hemos visto a lo largo de 2015 con el software de automóviles, permitiendo incluso el control remoto de un vehículo en marcha a kilómetros de distancia.

7.- Infraestructuras críticas

En ningún caso van a ser el blanco de ciberdelincuentes habituales, pero en el ámbito de la ciberguerra el poder sabotear infraestructuras críticas de un país de forma remota es algo tan valioso que sin duda los servicios de inteligencia de las naciones más poderosas del mundo tratarán de conseguirlo. Hace falta mucho dinero para poder realizar toda la investigación y desarrollo necesarios detrás de un ataque de este estilo, como nos demostró el caso de Stuxnet.

8.- Threat Intelligence en empresas

El crecimiento del número y complejidad de los ataques está transformando el uso de la información, y también cómo se comparte. Si bien las compañías que ofrecen soluciones y servicios de seguridad suelen compartir información para poder proteger de forma mejor a sus clientes se va a pasar a otro nivel donde estos mismos clientes (grandes empresas) por un lado demandando a sus proveedores de seguridad que les faciliten información de este tipo y, por otro, recopilando toda la información que llegue a sus redes y llegando a acuerdos para compartirla con otras empresas.

5. CONCLUSIÓN

5 Conclusión

2015 ha sido un año de infarto, donde los ataques han crecido más que nunca, y la verdad es que parece que 2016 va a venir aún más fuerte. Mucho de lo que hemos visto a lo largo del pasado año seguirá estando en este, como los ataques de cryptolockers a empresas que tanto dinero reportan a las bandas de ciberdelincuentes.

Deberemos prestar especial atención al Internet de las Cosas, ya que cada vez tenemos más dispositivos con conexión a Internet y con más capacidades, lo que los convierte en un objeto de deseo para todo aquel que quiere acceder a nuestra información, tanto personal como corporativa. Si bien es cierto que estos dispositivos no suelen almacenar mucha información, pueden ser la puerta de entrada perfecta para que los delincuentes consigan acceso a nuestra red, sea la de nuestro hogar o la de nuestra empresa.

Vistos los grandes robos de información que han tenido lugar, está claro que las empresas tienen un déficit de protección que es necesario atajar cuanto antes. Nadie debe asumir que está protegido y seguro, es más inteligente y actuar como si ya estuviésemos comprometidos, en lugar de esperar a enterarse meses o años después. Monitorizar y controlar todo lo que sucede en nuestra red es algo imprescindible a día de hoy.

Esperamos que este informe os haya sido de utilidad y seguiremos informando desde nuestro blog en http://www.pandasecurity.com/spain/mediacenter/ y en próximos informes.

6. SOBRE PANDALABS

6 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.

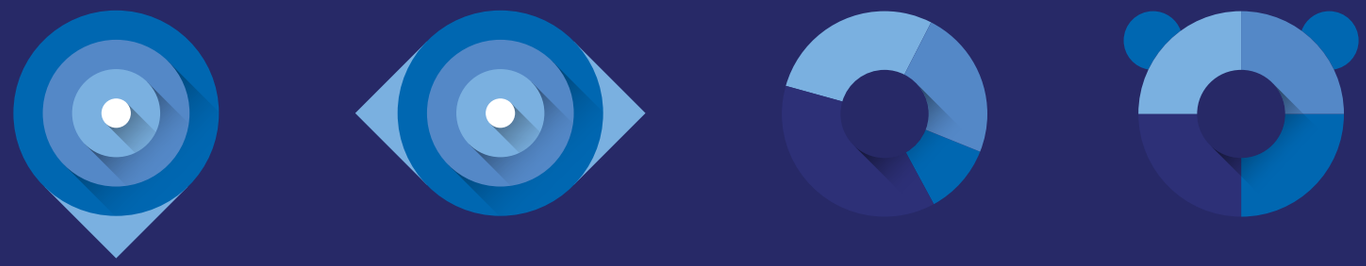
PandaLabs mantiene un continuo estado de vigilancia, siguiendo muy de cerca las diferentes tendencias y evoluciones acontecidas en el campo del malware y la seguridad.

El objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.

pandalabs

Queda prohibido duplicar, reproducir, almacenar en un sistema de recuperación de datos o transferir este informe, ya sea completa o parcialmente, sin previa autorización escrita por parte de Panda Security.

© Panda Security 2015. Todos los derechos reservados.



panda

pandalabs