INFORME ANUAL PANDALABS 2014

enero 2015

panda

pandalabs

1. INTRODUCCIÓN

Introducción

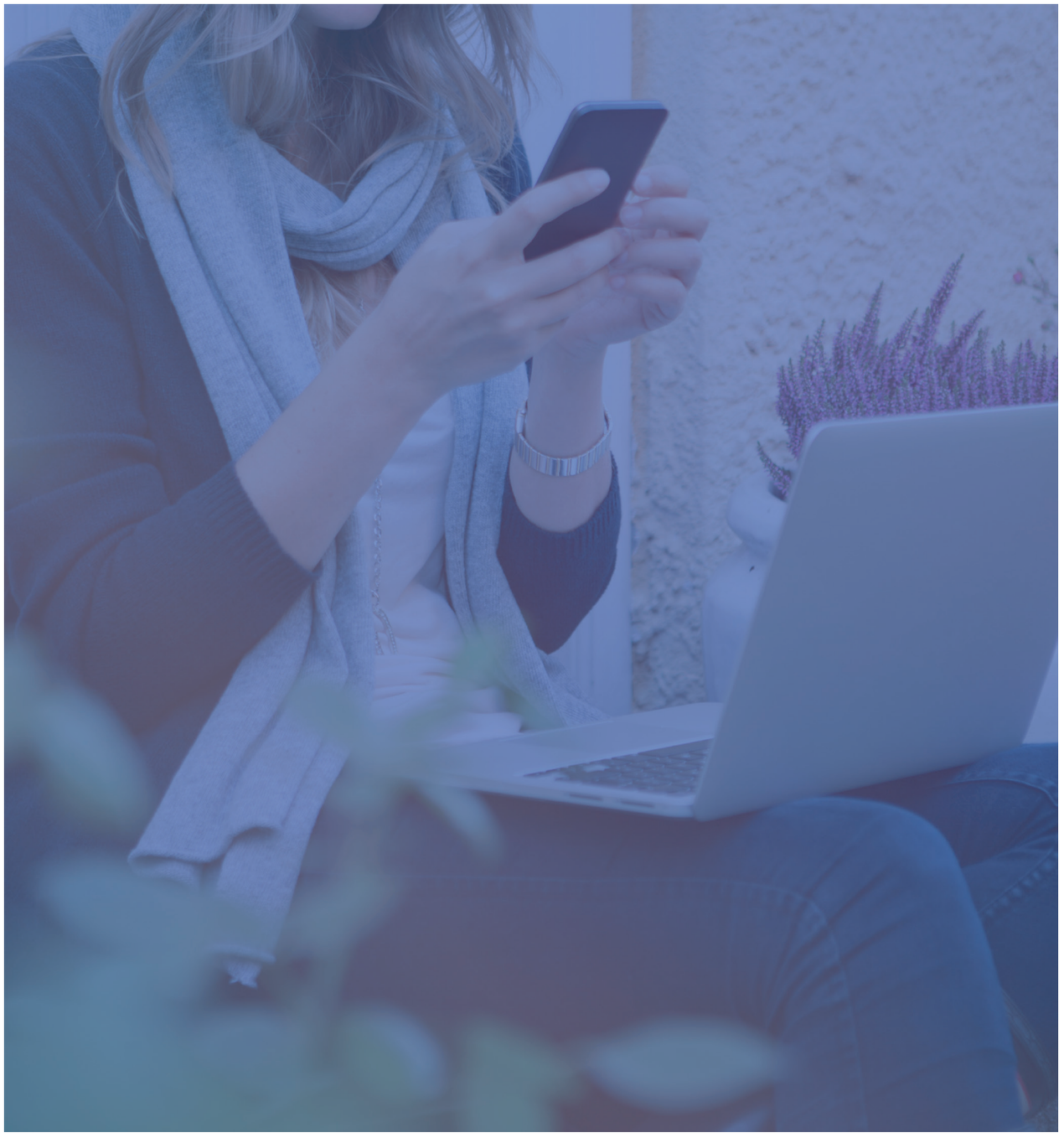
A lo largo de los 25 años de historia de Panda, hemos podido analizar la evolución del mundo de la seguridad informática, y hemos sido testigos y partícipes de los avances que han cambiado el mundo en pocos años.

Desde el inicio, cuando sólo unos pocos contaban con ordenadores de sobremesa, pasando por el triunfo de Windows como sistema operativo, la llegada de Internet, la popularización de los ordenadores portátiles, las conexiones WiFi, hasta la llegada de nuevos dispositivos que hoy forman parte fundamental en nuestro día a día como smartphones y tabletas.

El mundo que conocíamos ha evolucionado, y la seguridad de la información también ha pasado a formar parte de nuestras vidas.

Esto hace que todo se vuelva excesivamente complejo y difícil de entender. Tenemos toda la información a nuestro alcance, pero es tanta que nos desborda y no podemos estar al día de todo lo que sucede.

Con este informe queremos ayudar a aclarar el paisaje, analizando lo más relevante que ha ocurrido durante los últimos 12 meses. También aprovecharemos para ver qué es lo que nos deparará 2015 y saber a qué debemos atender para seguir seguros.



2014 puede ser considerado como el año de los grandes ciberataques.

Hemos sido testigos del robo de información a gran escala en algunas de las multinacionales más grandes del mundo, y al mismo tiempo, los ataques que normalmente no llegan a figurar con grandes titulares en los medios han ido amenazando a los inocentes usuarios de la red.

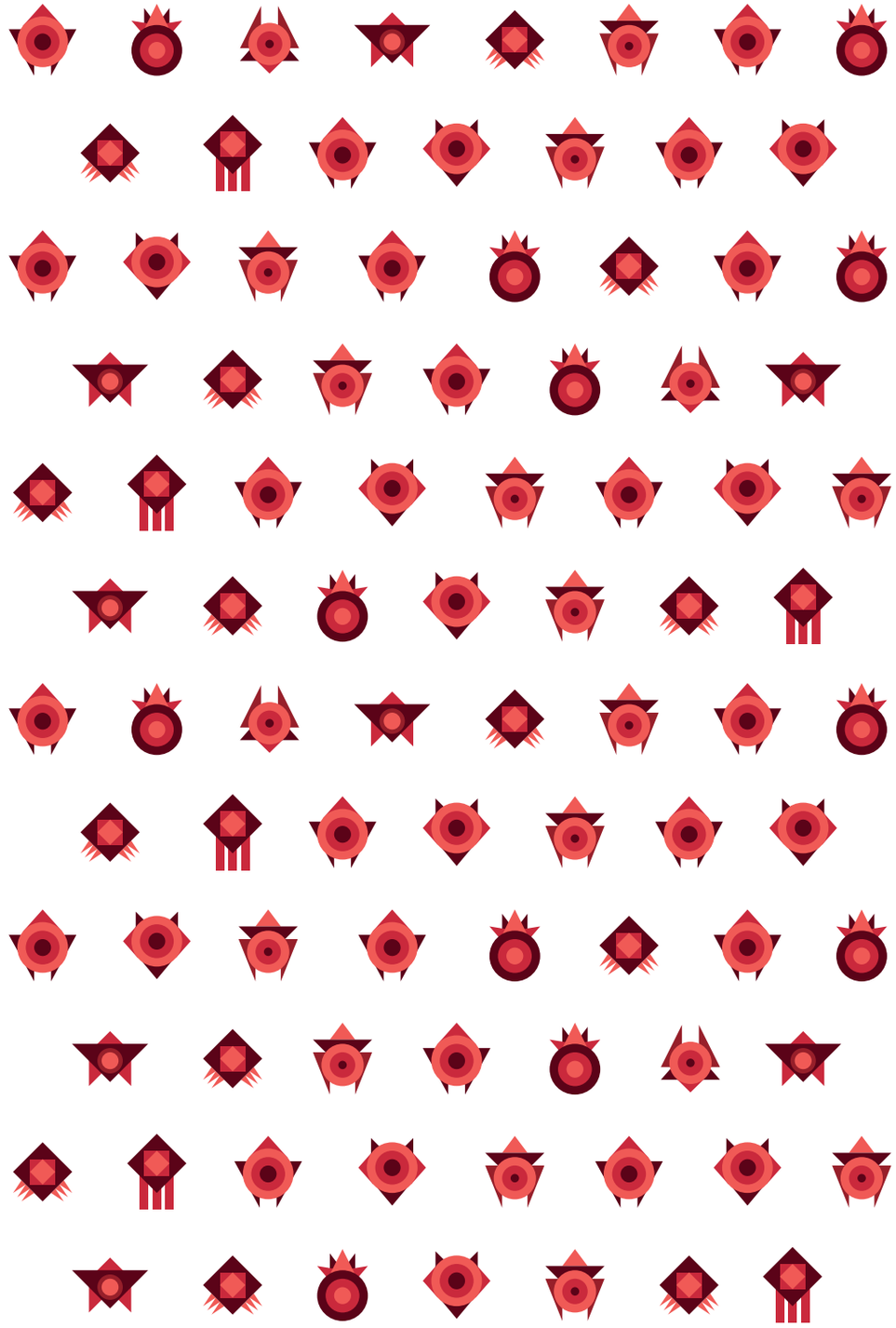
Uno de los tipos de ataques que más daño han causado son los protagonizados por malware de tipo ransomware -cuya familia más conocida es Cryptolocker- que cifran nuestros documentos y piden un rescate para poder recuperarlos.

Las víctimas se cuentan por miles, tanto usuarios domésticos como empresas que ven cómo su información es secuestrada sin apenas alternativas de poder recuperarla, salvo que cuenten con una copia de seguridad o que se ceda al pago del rescate.

Detallaremos los principales sucesos en el campo de la seguridad, los ciberataques, y analizaremos también las escalofriantes cifras que nos ha dejado 2014, año en el que se han batido todos los récords en cuanto a creación de malware.

Sobrepasando la marca de 200.000 nuevos ejemplares diarios capturados por PandaLabs.

En el mundo de los móviles analizaremos algunos de los ataques sucedidos y evaluaremos el estado de seguridad de las diferentes plataformas, donde Android sigue liderando -con diferencia- por cuota de mercado y por ser la elección predilecta de los ciberdelincuentes, con cientos de miles de nuevos ejemplares de malware aparecidos en 2014.



2. EL AÑO EN CIFRAS

El año en cifras

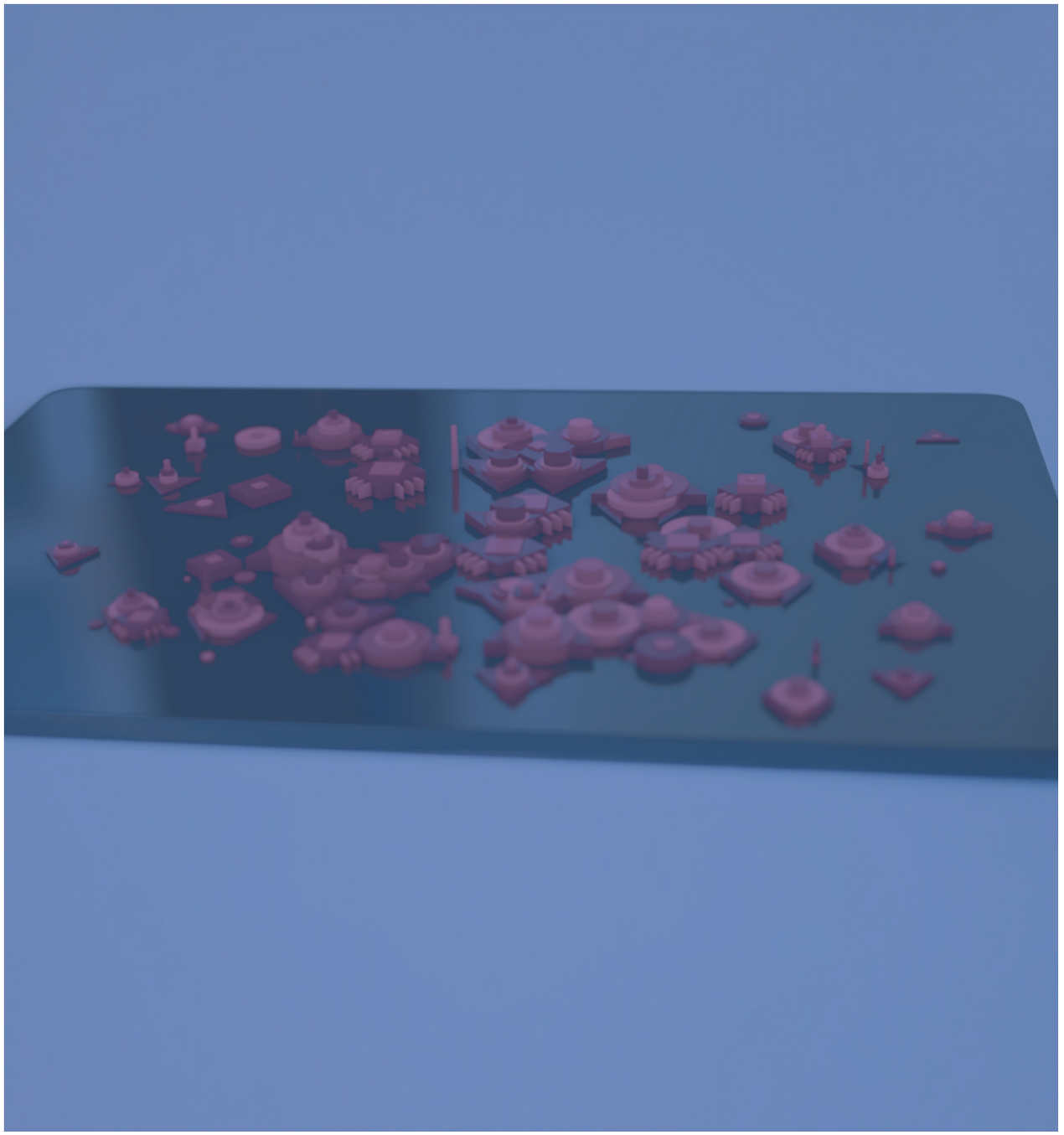
Nos encontramos ante el año de la historia que más cantidad de malware se ha creado, más de 75 millones de nuevas muestras detectadas y neutralizadas por PandaLabs, el laboratorio de Panda Security.

Esta cifra es dos veces y media más alta que la registrada el año anterior, que llegó a 30 millones de nuevos ejemplares.

En total contamos con 220 millones de muestras de malware detectadas, lo que significa que el 37,5% de todo el malware aparecido en la historia ha sido creado a lo largo de 2014.

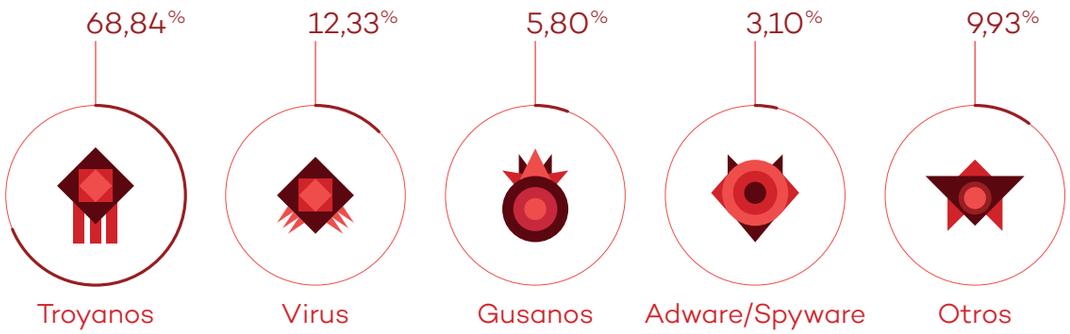
En un año donde los protagonistas han sido los ciberataques a grandes empresas, casi nadie se ha librado de tenérselas que ver con algún ataque.

Por ejemplo, los ransomware tipo Cryptolocker, que cifran los documentos del ordenador y piden un rescate para recuperarlos, han causado miles de infecciones por todo el mundo.



A continuación mostramos los datos della proporción de malware creado en 2014 por tipo:

NUEVO MALWARE CREADO EN 2014, POR TIPO



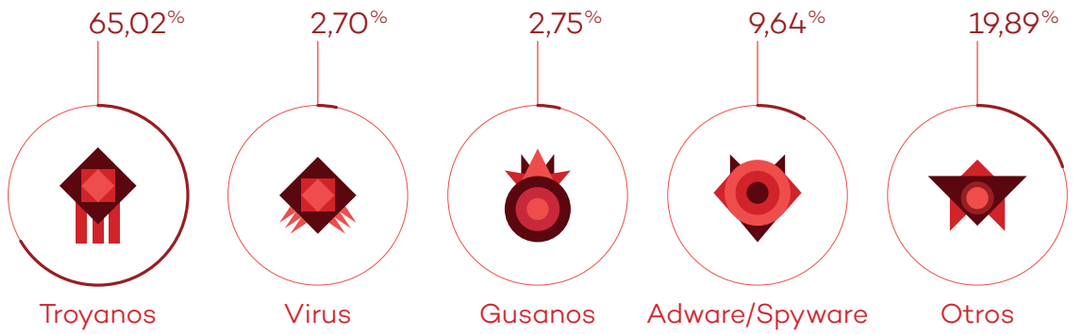
Los troyanos, como es habitual, siguen reinando sobre el resto de categorías con cerca del 70% de muestras creadas a lo largo del año. Si comparamos las cifras con las del año anterior, 2013, lo que más destaca es el aumento de la categoría “Otros”, con casi un 10% del total de muestras de malware registradas.

Esto es debido, como ya hemos explicado en anteriores informes, a los conocidos como PUP (Potencially Unwanted Program, Programas Potencialmente No Deseados), aplicaciones que sin ser maliciosas en sí mismas recurren a técnicas de engaño para conseguir instalarse en los ordenadores de los usuarios.

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 65,02% de los casos.

Veamos cómo se reparten las infecciones en todas las categorías:

INFECCIONES POR TIPO DE MALWARE EN 2014



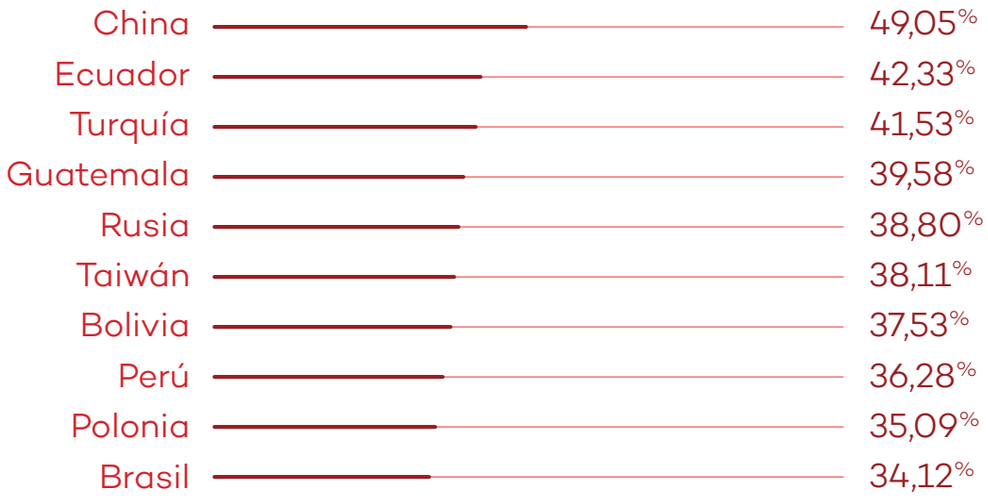
Además de la -por otra parte habitual- destacada posición de los troyanos, nos encontramos con que la categoría “Otros” vuelve a salir destacada, en esta ocasión, en segunda posición con un 19,89% de infecciones. De nuevo, tal y como hemos comentado anteriormente, se trata de los PUP. Sus técnicas agresivas de distribución junto a programas de software legítimos 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 30,42%, cifra menor a la del año anterior.

A nivel geográfico los países más infectados del mundo están liderados por China, con un 49,05% de infecciones, seguida de Ecuador -con un índice de infección sensiblemente más bajo, el 42,33%- y Turquía con un 41,53%.

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

PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN EN 2014



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

PAÍSES CON MENOR ÍNDICE DE INFECCIÓN EN 2014

Asia y Latinoamérica son las regiones con mayores infecciones. El resto de países, con un porcentaje mayor a la media mundial, son Colombia (33,27%), Uruguay (33,05%), Chile (31,27%) y España (30,90%).

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: Suecia se sitúa a la cabeza, con un 19,98% de infecciones, seguido de cerca por Noruega con un 20,31%; y Finlandia, con un 21,21% de infecciones.

El resto de países con un porcentaje menor a la media mundial son Australia (25,28%), Francia (25,68%), Portugal (26,84%), Austria (27,69%), Canadá (27,82%), Estados Unidos (28,96%), Venezuela (29,83%), Hungría (30,96%), México (31,00%), Italia (31,47%) y Costa Rica (31,50%).

3. EL AÑO DE UN VISTAZO

El año de un vistazo

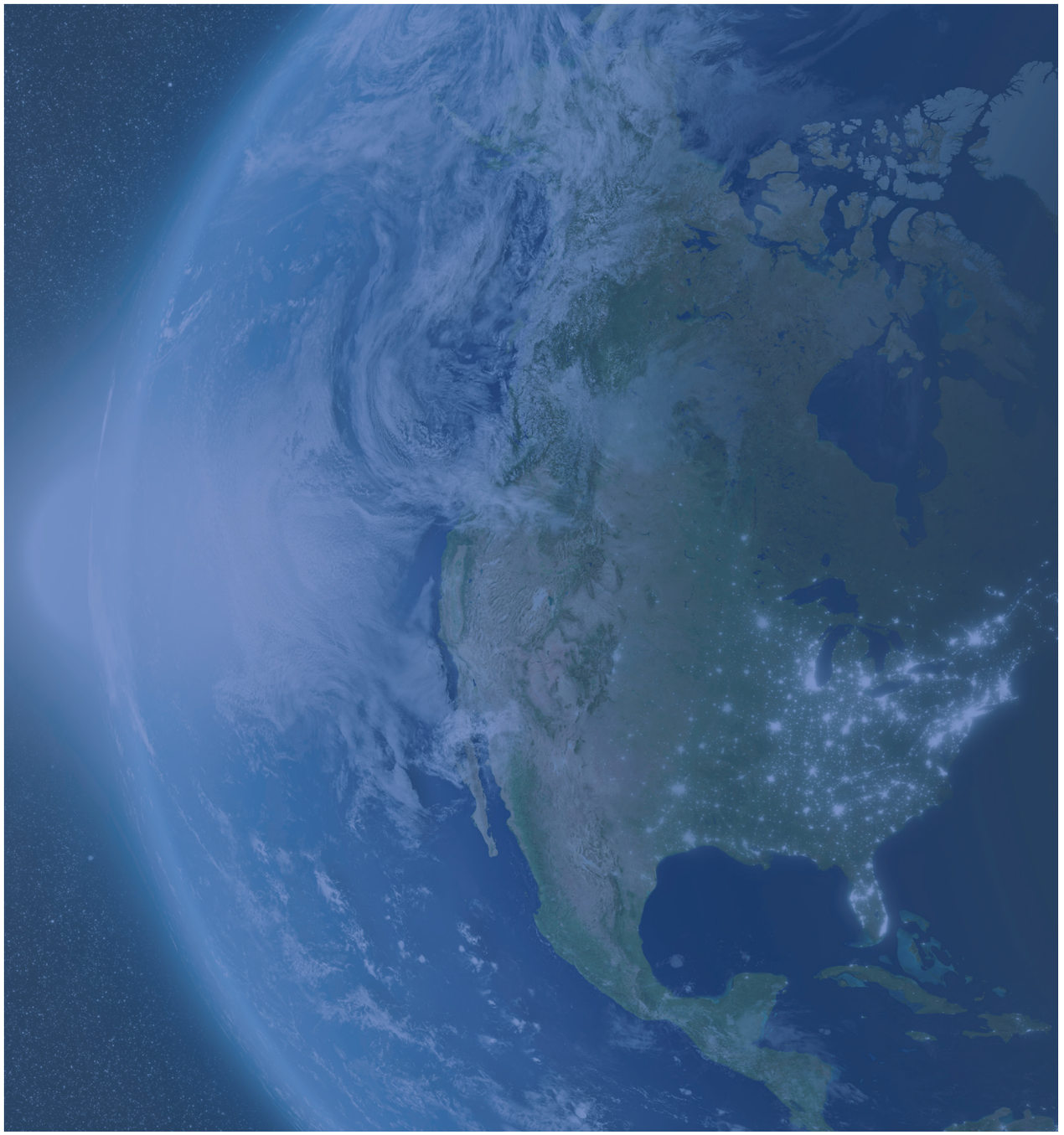
Cibercrimen

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. No hablamos 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 2014 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 datos.

Un trabajador del departamento antifraude de la compañía KCB 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 tuvieron 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 la empresa californiana no fue atacada ni sufrió robo de datos directamente.

Yahoo 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.

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.

¿Cómo puede entonces un sitio web validar a los usuarios? Es sencillo, bastaría con "saltear" la contraseña que elige un usuario al darse 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 predefinido (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 almacena como prueba de validación.

A partir de entonces, cuando 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 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 tuvo lugar este año 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 vimos muy claramente en el primer trimestre de 2014.

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.

El 8 de abril fue el día señalado por Microsoft para dejar de dar soporte a Windows XP.

Básicamente significa que dejará de recibir actualizaciones de seguridad, por lo que cualquier nuevo agujero que se descubra no se solucionará. Todo ello coincidió precisamente con la aparición de un grave agujero de seguridad de Internet Explorer que permitía a un atacante infectar un ordenador simplemente visitando una página web que abusara este error.

El pánico fue tal -se habían detectado ya ataques utilizando este problema- que Microsoft decidió publicar la actualización del navegador para la versión de Windows XP, a pesar de que ya se había dejado de dar soporte a este sistema operativo.

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

Al mismo tiempo que se producía el fin de ciclo de Windows XP, surgió un fallo de seguridad en la librería OpenSSL.

Heartbleed aprovechaba un agujero de seguridad en una librería que se utiliza para el cifrado de comunicaciones.

Las comunicaciones de los principales servicios de Internet como el correo web, redes sociales, banca online, etc. están cifradas con el propósito de proteger los datos que intercambiamos (credenciales bancarias, contraseñas, etc.). Aquellos servidores que utilizaban la librería vulnerable eran susceptibles de ser atacados.

El problema radicaba en un módulo que permite reutilizar conexiones ya abiertas (conocido como 'keep alive'), mediante el cual se podían obtener hasta 64 Kb de la memoria de la máquina atacada, y hacerlo repetidas veces. No todo era catastrófico, ya que al menos el atacante no podía elegir a qué parte de la memoria acceder, y, además, se publicó la librería que corrige este bug.

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

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

Los atacantes consiguieron credenciales de empleados de eBay que fueron utilizadas para acceder a la red corporativa de la empresa.

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

La polémica surgió no por el ataque, sino por cómo la propia compañía lo comunicó. Al inicio parecía que se trataba de restar importancia al mismo, y de hecho el incidente no se publicitó de forma visible en su página web. Sin embargo, ante la gravedad de los hechos, a eBay no le quedó más remedio que rectificar y añadir una advertencia muy visible en su página principal pidiendo a todos sus usuarios que cambiaran sus contraseñas.

PandaLabs detectó que los ciberdelincuentes están aprovechándose de este incidente.

Quienes lanzaron una campaña de correos de phishing haciéndose pasar por eBay, informando del problema de seguridad e incluyendo un enlace (malicioso) para cambiar la contraseña. Si accedemos a dicha página e introducimos nuestra información, estaremos dando nuestras credenciales de eBay a los ciberdelincuentes.

Spotify también fue víctima de un ataque similar para vulnerar su red corporativa.

Sin embargo, lo curioso de este incidente es que sólo se accedió a los datos de un único usuario de Spotify, algo realmente llamativo. Podría tratarse de un ataque dirigido a un único usuario, o bien de una prueba de los ciberdelincuentes para comprobar hasta dónde podían llegar.

La página web de Reuters fue comprometida por la Syrian Electronic Army.

En este caso no fue un problema de seguridad de Reuters el que dio pie al ataque, sino que la víctima del mismo fue un proveedor de servicios que la empresa utiliza, siendo ésta la vía de entrada de los delincuentes.

Domino's Pizza fue atacada por un grupo denominado "Rex Mundi".

Le fueron sustraídos datos de 650.000 clientes de Francia y Bélgica, solicitando un rescate por dicha información. Los responsables de la empresa dijeron que no estaban dispuestos a ceder al chantaje.

Hector Xavier Monsegur, alias Sabu, fue arrestado el 7 de junio de 2011 por el FBI. Muchos recordaréis a este personaje, uno de los líderes del movimiento de Anonymous y Lulzsec. Sabu se declaró culpable de numerosos delitos y ahora se enfrentaba a una pena de hasta 124 años de cárcel. No obstante, desde que fue arrestado estuvo colaborando con el FBI, ayudando a recoger evidencias y arrestar a otros ciberdelincuentes.

Gracias a la ayuda de Sabu se han evitado cerca de 300 ciberataques a lo largo de 3 años.

Tras ser arrestado, pasó siete meses en prisión y en estos momentos permanece a la espera de sentencia. Finalmente, en mayo de este año Sabu ha sido puesto en libertad, quedando su deuda con la justicia saldada gracias a la intensa colaboración mantenida con las fuerzas de seguridad.

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

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

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

Otra importante intervención contra el cibercrimen, de nuevo protagonizada por el FBI, fue la toma de control que tuvo lugar contra la red de bots GameOver Zeus

Estos son una familia de malware que utilizaba comunicación de tipo P2P, lo que hacía que su toma de control fuera realmente complicada al no depender de servidores que pudieran neutralizarse.

Además, el FBI presentó cargos contra quien controlaba la botnet, Evgeniy Mikhailovich Bogachev. Quien fue acusado de llevar a cabo infecciones con el conocido CryptoLocker y se añadió a la lista de los delincuentes más buscados.

iCloud también ha sido uno de los protagonistas involuntarios de un suceso ocurrido durante este año 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. 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.

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 el tercer trimestre fuimos 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 en la que robaron información 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 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 tuvo como víctima a Home Depot. El gigante minorista del bricolaje confirmó el ataque a sus servidores, en el que se comprometieron 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.

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 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.

USPS, United States Postal Service, informó que les habían robado de sus servidores datos personales de 800.000 empleados

Lo que llamó mucho la atención, ya el servicio postal de los Estados Unidos únicamente tiene medio millón de empleados. Parece que en los servidores había datos tanto de trabajadores en activo como retirados.

A finales de noviembre, trabajadores de Sony vieron cómo no podían poner en marcha sus ordenadores.

Un ataque de malware había empezado a borrar todo el contenido de los discos duros de los ordenadores. Pero éste sólo era el síntoma de un ataque a mucha mayor escala. El grupo responsable del ataque se autodenomina "Guardians of Peace", y dijeron haber robado más de 100TB de datos de Sony. De hecho, comenzaron a publicar en Internet datos personales de trabajadores de la compañía, de familiares, mensajes de correo electrónico entre empleados, salarios, copias de películas que aún no habían sido estrenadas, etc.

Ha habido mucha especulación sobre el origen de los atacantes, pero el FBI se involucró en el caso diciendo que tenían pruebas más que suficientes para saber que se trataba de un ataque realizado por Corea del Norte.

Días más tarde de hacerse público el ataque, se detectaron muestras de malware que estaban utilizando firmas digitales válidas que pertenecían a Sony y habían sido sustraídas durante el ataque.

Uno de los últimos grandes ataques que vimos antes de finalizar el año fue el que recibieron tanto Xbox Live como PlayStation Network.

En navidades, las fechas que estos servicios son más utilizados durante todo el año, fueron víctimas de un ataque de denegación de servicio que impedía a los usuarios acceder al sistema online de las dos gigantes de los videojuegos.

Si algo cabe destacar de este caso, es que en lugar de llevar a cabo un ataque DDoS utilizando ordenadores infectados, como suele ser habitual en estos casos, los ciberdelincuentes utilizaron routers comprometidos para llevarlo a cabo.

Redes sociales

En 2014 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 MH 370 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 cómo 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.

La Syrian Electronic Army se hizo con el control de cuatro cuentas de Twitter

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

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

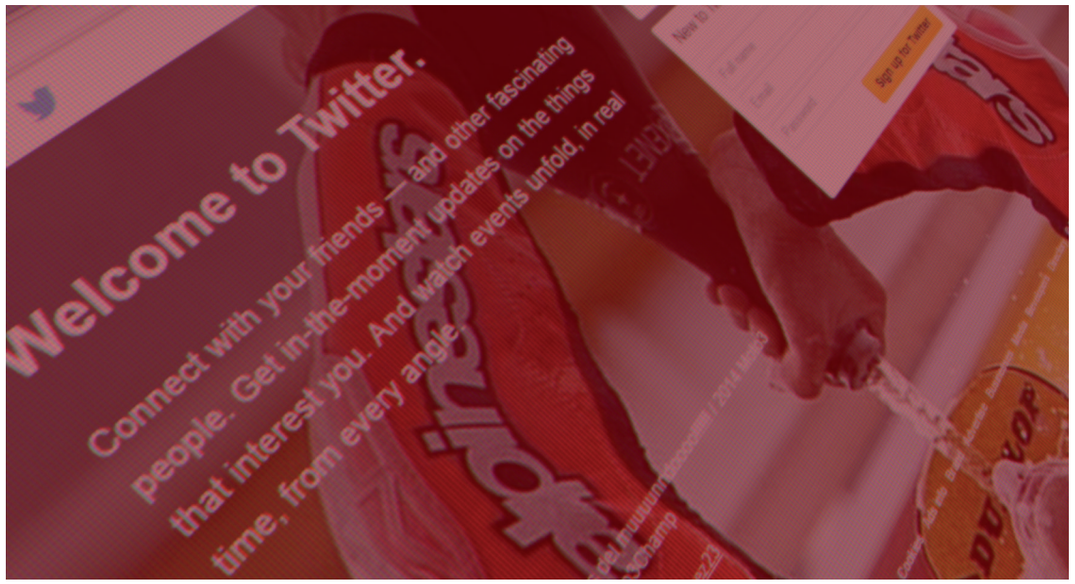
El pasado 12 de junio daba comienzo el Mundial de Fútbol en Brasil. Un ciberdelincuente aprovechó la oportunidad para robar credenciales de Facebook de los jugadores de Top Eleven: Be a Football Manager, uno de los juegos sobre managers de fútbol con más éxito, con más de 10 millones de seguidores en Facebook. Se trataba de un malware en Windows que actúa disfrazado de aplicación. En teoría, si se descarga permite ganar tokens para el Football Manager con los que comprar jugadores. Evidentemente esto no sucede, y si lo que hacemos es seguir las instrucciones indicadas, no solo no vamos a conseguir tokens gratis, sino que además podremos perder el acceso a nuestra cuenta de correo electrónico o de Facebook.

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 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

En febrero, PandaLabs destapó un caso de malware en Google Play. Cuatro aplicaciones de diferente temática (dietas, peinados, ejercicio y recetas) que al ser ejecutadas suscribían al usuario a un servicio de SMS Premium. Además, ocultaba los SMS recibidos, lo que provocaba que el usuario no se percatase del ataque hasta que recibiera la factura.

PandaLabs descubrió 4 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 Facebook.

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

En abril se descubrió una campaña de malware cuyo objetivo eran iPhones y iPads hackeados.

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

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

Todo parece indicar que los ciberdelincuentes han logrado las credenciales de Apple de algunos usuarios.

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

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

En el ecosistema de Android han aparecido todo tipo de noticias y ataques, aunque los más llamativos pertenecen a la categoría de falsos antivirus y ransomware.

Virus Shield consiguió aparecer en lo más alto de las aplicaciones populares de Google Play.

Un caso nunca visto hasta ahora ya que, aparentemente, se trataba de una aplicación antivirus de pago, con un coste de 3,99$. Sin embargo, realmente no ofrecía ninguna protección, únicamente tenía un interfaz que simulaba analizar y proteger el móvil. Tuvo más de 10.000 descargas antes de ser retirada, y Google repuso el dinero a los compradores timados.

Apareció también una nueva familia de malware para Android llamada Android/Koler.

Un "Virus de la Policía" dirigido a teléfonos móviles.

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

En esta ocasión, los ciberdelincuentes cometieron un pequeño error al configurarlo y dejaron la puerta entreabierta. Lamentablemente no pudimos acceder a toda la información que allí había (una base de datos -mysql- con información sobre infecciones, pagos, etc.).

Pero en PandaLabs pudimos descargar ficheros del servidor y echar un vistazo a su funcionamiento.

El método de funcionamiento desde el lado del servidor es muy parecido a los que tienen como objetivo ordenadores con Windows: varios scripts para geolocalizar el dispositivo y mostrar el mensaje en el idioma local y con imágenes de las fuerzas de seguridad locales. Guarda información de todos los dispositivos infectados en la base de datos y añade el MD5 del malware que lo ha infectado.

Al hacer esto es posible hacer un seguimiento del número de infecciones que consiguen con cada variante del malware y medir el éxito de las diferentes campañas de infección.

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

Otro malware del tipo ransomware apareció desde Rusia.

La novedad es que realmente cifraba información del móvil y solicitaba un rescate para recuperarla.

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

El número de muestras de malware para Android sigue subiendo exponencialmente y bate récords.

Android ha sido de nuevo el protagonista en este apartado por varios motivos. Por un lado, Adrian Ludwig, responsable de seguridad del S.O. 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 (velada mención a la App Store de iOS que tiene fama de ser mucho más exigente en este aspecto). Vino a decir que no es necesario el uso de 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 en Android que podrían ser explotadas de forma maliciosa:

- CVE-2013-6272: Afecta a las versiones anteriores a la 4.4.2 (KitKat) y puede permitir a una aplicación maliciosa realizar llamadas a números de tarificación especial.
- 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.

Wirelurcker es un malware para iPhone y iPad

Su técnica de infección es bastante curiosa. Primero infecta un ordenador, y una vez allí espera a que se conecte un dispositivo iOS por USB. Si el dispositivo tiene instalada una de las aplicaciones que son objetivo de este ataque, la infecta y la vuelve a instalar sin que el usuario sea consciente.

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 año han prevalecido las noticias de colaboración entre la NSA y el británico GC HQ (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.

Estados Unidos, Alemania, Bélgica, Reino Unido entre los países que confirmaron ataques dirigidos en 2014.

Uno de los casos más llamativos tuvo lugar en Bélgica. El Ministerio de Asuntos Exteriores del país europeo fue comprometido. Se especula con que el origen de dicha agresión podría ser Rusia, aunque debemos ser muy cautos, ya que la investigación aún está en curso y llevará bastante tiempo saber lo realmente sucedido.

En Reino Unido un alto cargo del gobierno confirmó que habían detectado un ataque detrás del cual se encontraba una potencia extranjera. Mediante dicho ataque consiguieron acceso a una cuenta de administrador de sistema de la "Government Secure Intranet", aunque lograron detectarlo a tiempo e impedir que se robara la información.

Sobre el espionaje realizado por el propio país, el director general de la Oficina para la Seguridad y Contraterrorismo, Charles Farr, asegur que las comunicaciones a través de redes sociales y buscadores extranjeros son interpretadas por el Gobierno británico como "externas", lo que implica que no necesita de orden judicial para acceder a la información y comunicaciones a través de Google, Twitter o Facebook.

Este tipo de declaraciones, unidas a todo el escándalo de espionaje protagonizado por la NSA en los últimos tiempos, han llevado a un cambio de comportamiento de usuarios. De hecho, según un estudio reciente, se ha más que doblado la cantidad de tráfico cifrado que circula en Internet desde que se desvelaran los casos de espionaje masivos.

Y ésta no ha sido la única consecuencia, el Gobierno alemán ha cancelado un contrato que tenía con la compañía de telecomunicaciones estadounidense Verizon, dentro del rediseño de las comunicaciones internas que están efectuando, tras descubrirse prácticas de espionaje por parte del gobierno norteamericano, que incluso había llegado a "pinchar" la línea de la canciller Angela Merkel.

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.

Seguimos en Estados Unidos, pero desde una perspectiva diferente. Hemos conocido mediante nuevos 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 a torrent que contenía el total de información sustraída.

CVE-2014-4114 es el identificador de una vulnerabilidad descubierta por la consultora de seguridad iSight Partners, hecha pública en octubre, la cual afecta a la mayoría de las versiones recientes de Windows, y que Rusia podría haber empleado en una reciente campaña de espionaje, bautizada como Sandworm.

Esta campaña se piensa que ha sido dirigida selectivamente sobre redes de la OTAN, operadoras de telefonía Europeas, universidades norteamericanas y varias agencias gubernamentales de Ucrania.

La vulnerabilidad permite a un atacante la ejecución de código mediante la apertura por parte de la víctima de un archivo de Powerpoint. La vulnerabilidad radica en que Windows permite al “OLE packager” (packager.dll) descargar y ejecutar ficheros INF, que pueden estar formados para ejecutar comandos específicos.

Esta vulnerabilidad afecta a las últimas versiones de Windows, desde Vista SP2 hasta el reciente Windows 8.1, incluyendo Windows Server 2008 y 2012.

Microsoft ya ha publicado un boletín de seguridad (MS14-060) que corrige esta vulnerabilidad:

https://technet.microsoft.com/library/security/ms14-060

4. TENDENCIAS 2015

Tendencias 2015

Cryptolocker

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

Una vez consigue entrar en un ordenador, cifra todo tipo de documentos que pueden tener 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 estos ficheros. El pago se reclama siempre en bitcoins, de tal forma que no pueda ser rastreado por la policía. Este tipo de ataque es muy jugoso para los ciberdelincuentes, ya que muchos usuarios deciden pagar para recuperar la información secuestrada.

APT

Las conocidas como APT (Advanced Persistent Threats) son un tipo de ataque dirigido cuyo objetivo suelen ser empresas o instituciones. Detrás suelen estar países que invierten mucho dinero en conseguir que el ataque permanezca mucho tiempo sin ser detectado. Son la versión virtual de James Bond.

Si bien no veremos ataques masivos de este tipo durante 2015, sí que saldrán a la luz nuevos casos que seguramente están actuando desde hace años.

Ataques Dirigidos

La mayoría de ataques están dentro de los millones de muestras de malware que aparecen todos los meses, pero un pequeño porcentaje 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.

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.

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 y que raramente son actualizados.

Así, en cuanto se encuentra un fallo de seguridad del software, comprometer dicho dispositivo se convierte en un juego de niños para el ciberdelincuente. Para empeorarlo, a su vez, estos dispositivos están conectados a redes internas, de hogares o empresas, por lo que se convierten en los puntos de entrada ideales para llevar a cabo ataques a mayor escala.

Terminales de Punto de Venta

Durante este año hemos visto cómo ha incrementado el ataque hacia estos terminales usados por 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 como pagar la compra del supermercado, que ningún usuario considera que pueda conllevar un riesgo, comienza a suponer un peligro del que han sido víctimas cientos de millones de personas en el mundo.

5. CONCLUSIÓN

Conclusión

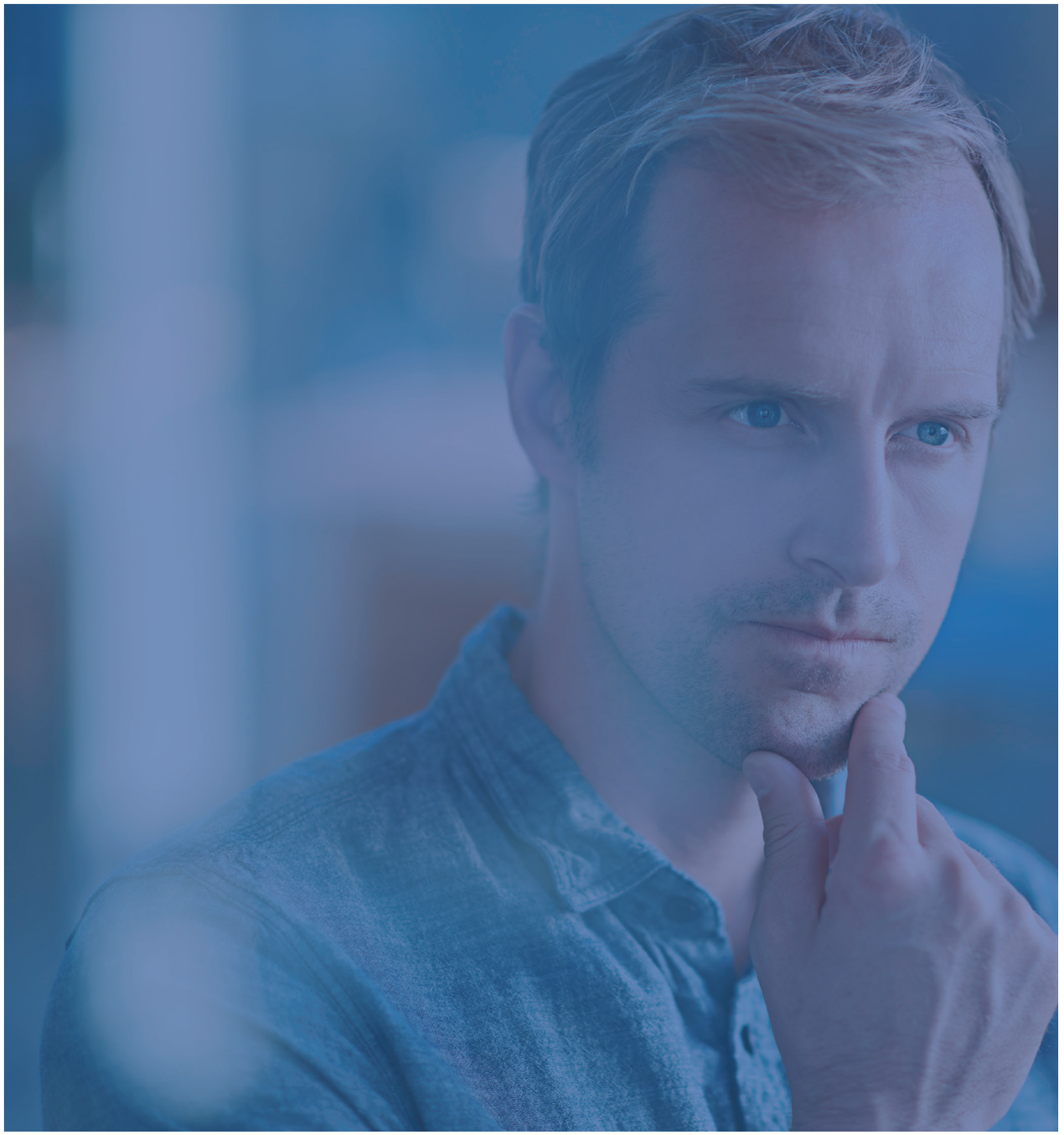
Vivimos en un mundo conectado a internet en todo momento, lo que hace que los riesgos a los que nos enfrentamos debido a los ciberataques nos afecten más que nunca en la historia.

Además, si algo sabemos seguro es que los riesgos siguen aumentando, los ciberdelincuentes están más activos que nunca y debemos estar preparados para hacer frente a los ataques que recibiremos.

Las empresas deben actuar como si hubieran sido comprometidas y que no esperen a enterarse meses o años después y porque un tercero les avisa. Monitorizar y controlar todo lo que sucede en tu red se va a convertir en algo imprescindible.

Esperamos que este informe os haya sido de utilidad y seguiremos informando en próximos informes y desde nuestro blog:

http://www.pandasecurity.com/mediacenter/



6. SOBRE PANDALABS

Sobre PandaLabs

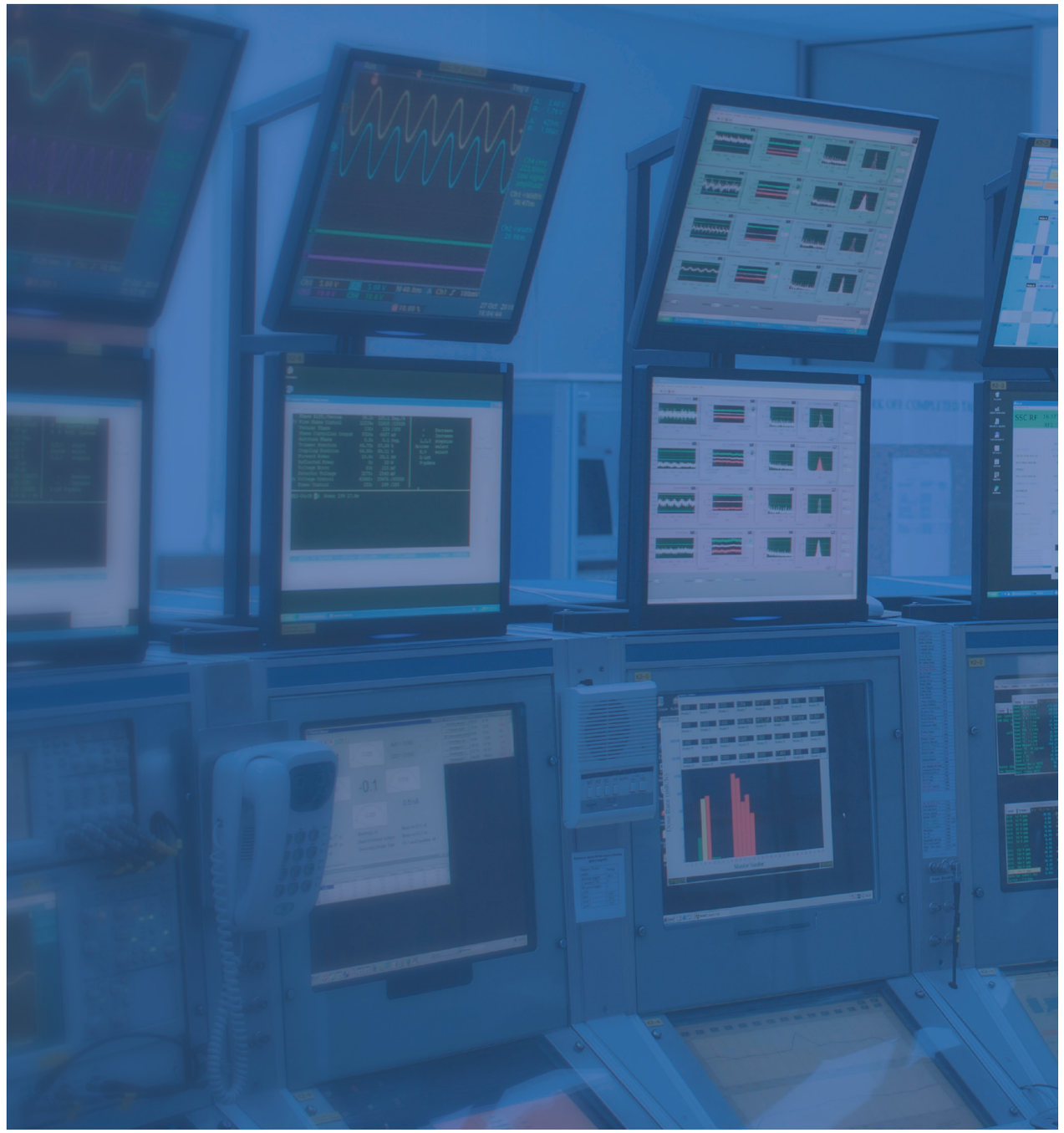
PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

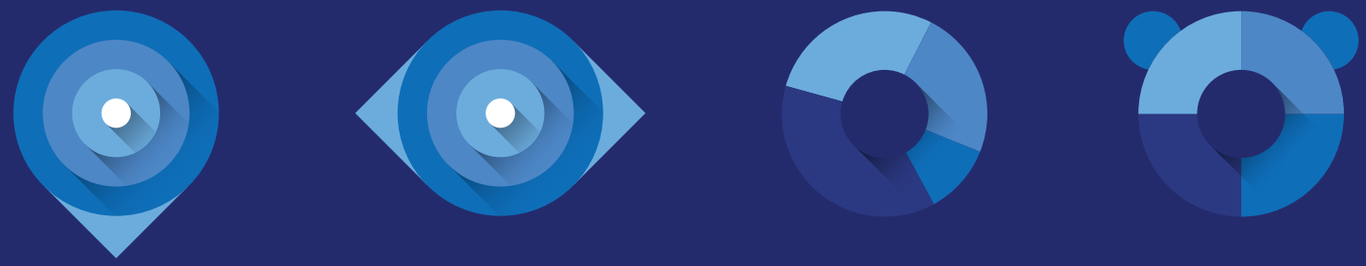
- Desde PandaLabs se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.

- 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.





panda

pandalabs