Noviembre, 2017

Informe Anual PandaLabs 2017

panda

pandalabs

Introducción.

Luis Corrons
Director Técnico de PandaLabs

En el Corazón de la Compañía.

En una empresa de ciberseguridad, el laboratorio es el cerebro desde donde se coordinan las actividades de investigación de las amenazas, y de desarrollo de las técnicas de ciberdefensa.

Sobre nuestros hombros recae el peso de la responsabilidad de preservar la seguridad de nuestros clientes. Si uno de ellos por algún casual se infecta, hemos fallado. La buena noticia es que **el número de incidentes de malware escalados a PandaLabs a lo largo de 2017 tiende a cero**.

Una forma de medir si realmente estamos haciendo bien nuestro trabajo, es ser evaluados por una entidad independiente. Seguramente la mejor prueba que se realiza hoy en día para medir la efectividad de una solución ante amenazas reales, es el **test Real World de AV-Comparatives**. El "Advanced+" es el máximo galardón que conceden y, entre todos los que trabajamos por conseguir un mundo más seguro, nos lo han otorgado a nosotros:

¿Cuál es el Secreto?

En la conclusión de este informe lo veremos en detalle, pero en definitiva, se trata de conseguir "olvidarse" del malware. Si nos centramos en luchar contra el malware, será una batalla perdida de antemano, siempre iremos por detrás.

Contar con tecnología Machine Learning para proteger a nuestros clientes, implica que los técnicos de PandaLabs dispongan de más tiempo para investigar.

Estas son muy malas noticias para los atacantes: hemos formado nuestro equipo de Threat Hunting que analiza y va a la caza de cualquier comportamiento anómalo que se pueda dar, por muy inocente que pueda parecer. Y han destapado numerosos casos de ataques, algunos de los cuales describimos en este informe.

La combinación de tecnologías avanzadas y servicios gestionados, nos permite clasificar el 100% de los procesos activos y saber qué está pasando en el momento que está pasando. Visibilidad sin límites de lo que ocurre, y control absoluto de lo que ocurre para reducir a cero el impacto de cualquier amenaza.

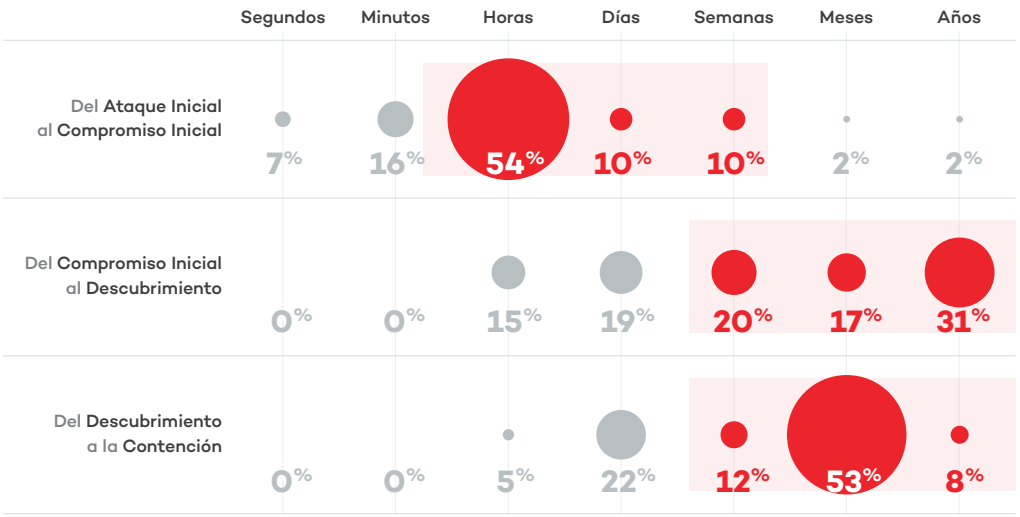
Evolución de los Ataques.

Hay **más atracos y extorsiones que nunca antes en la historia**, con la peculiaridad de que ahora los atacantes pueden estar a miles de kilómetros sin nunca haberse acercado a sus víctimas.

De hecho, ni siquiera es necesario que el ordenador comprometido tenga acceso a la información o a los recursos que busca el ciberdelincuente, ya que simplemente lo utilizarán de punto de partida.

Usarán movimientos laterales para desplazarse por la red corporativa hasta que dan con la información que les interesa, o con el sistema que quieren sabotear.

Así, las nuevas técnicas para penetrar las defensas y la ocultación del malware están permitiendo que las amenazas permanezcan en las redes corporativas durante largos períodos.



Datos del DBIR de 2016.

En la Actualidad.

El Cibercrimen es un negocio atractivo y muy lucrativo. Los atacantes cuentan con más y mejores recursos -tanto técnicos como económicos- lo que les permite desarrollar ataques cada vez más sofisticados.

Casi cualquiera puede lanzar un ataque avanzado gracias a la democratización de la tecnología, el mercado negro y herramientas de código abierto. Como consecuencia, todas las empresas se convertirán en el objetivo de un ataque avanzado. Es necesario asumir este hecho para comenzar a trabajar en acciones y políticas de seguridad efectivas. Contar con los mecanismos para detectar, bloquear y remediar cualquier tipo de amenaza podrá salvaguardar los activos y la reputación de las organizaciones.

La práctica totalidad de estos delitos tiene una base económica. Los atacantes irán a por víctimas que les reporten beneficios. Es por ello que debemos poner todas las medidas posibles para complicar y entorpecer su llegada al objetivo, de tal forma no les sea productivo.

En la mayoría de los casos si un ataque se vuelve complejo y no consiguen llegar a su objetivo final, optarán a ir a por otra víctima que les ofrezca un mejor retorno de inversión.

Para que nos hagamos una idea de la complejidad de los ataques, en el 62% de las brechas de seguridad que han tenido lugar en empresas se han utilizado técnicas de hacking. Lo que es más, **sólo en el 51% de los casos los atacantes han utilizado malware**, en el resto se han valido de otras herramientas contra las que la mayoría de empresas no están protegidas.

En el caso de sufrir un ciberataque, es importantísimo poder disponer de información forense del mismo, de tal forma que podamos tomar las medidas necesarias sabiendo a qué nos estamos enfrentando.

Así podemos saber por dónde han venido, qué técnicas han utilizado, qué movimientos han realizado, qué han hecho, cómo evadieron defensas, etc.

Otras Motivaciones.

Si bien la mayoría de los ataques tienen un objetivo económico, también existen otros casos en los que hay motivaciones claramente distintas.

Un caso claro que hemos visto este año ha sido el ataque a empresas con oficinas en Ucrania a través del **Petya/Goldeneye**, con un motivo claramente político donde el propio gobierno ucraniano acusó abiertamente al gobierno ruso de estar detrás del mismo.

Pero no se trata de un caso puntual. Estamos en plena carrera armamentística en el ciberespacio, las naciones están creando cibercomandos ya que saben que es clave no sólo como método de ataque, sino que necesitan reforzar de forma inmediata sus defensas ante cualquier ataque a empresas o infraestructuras de interés nacional.

Por ejemplo, el plan de ciberseguridad del presidente Obama solicitaba a su sucesor que entrenara a 100.000 nuevos expertos en seguridad informática para el año 2020. De hecho, el objetivo para 2018 es contar con **133 equipos militares para acciones cibernéticas**.

Todos los países han incluido esta prioridad en sus ejércitos como una unidad operativa más. De hecho y a menudo, son las unidades con mayor dotación presupuestaria.

Distribución de la Inversión en Cyber-Ejércitos

PAÍS	PRESUPUESTO ANUAL	NÚMERO DE CIBER-TROPAS
	$7.000M	9.000
	$1.500M	20.000
	$450M	2.000
	$300M	1.000
	$250M	1.000
	$200M	4.000

Fuente: RBTH

Tendencias.

Conociendo a tu Enemigo.

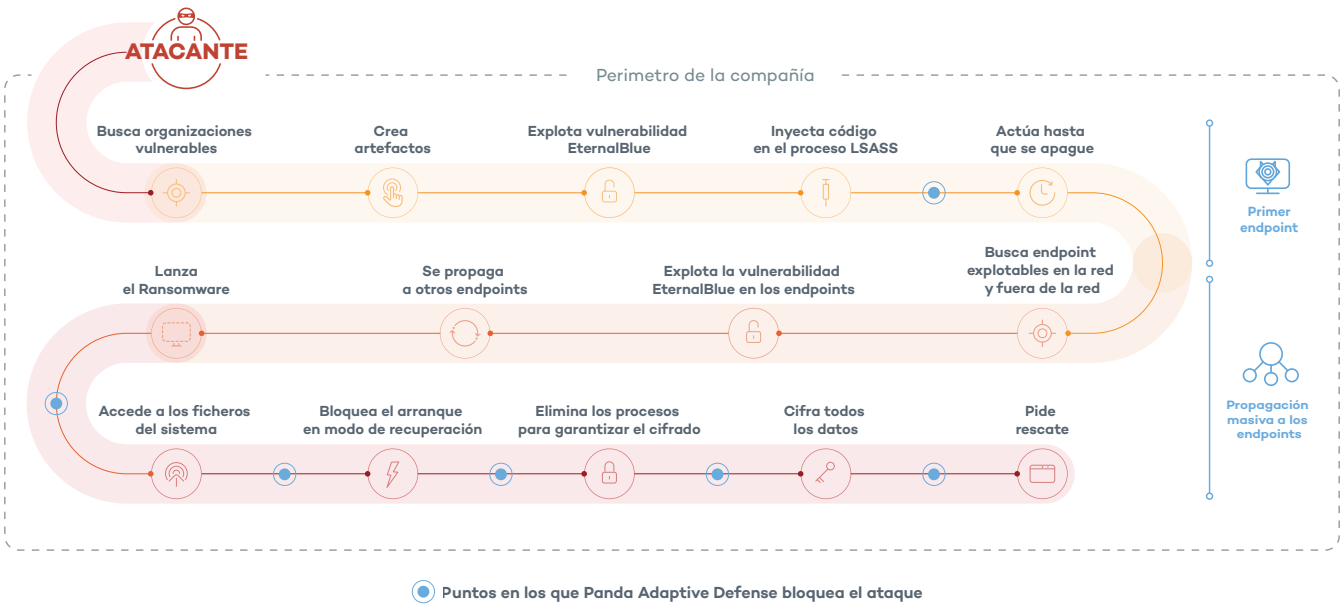
Aprovechando las vulnerabilidades, los ciberatacantes crean nuevas herramientas para explotarlas, además y para complicarlo aún más, buscan el éxito de su ataque al margen de la acción humana.

Esto implica un estudio minucioso de sus víctimas, una reacción armada de explotación de agujeros de seguridad muy concretos, y una distribución automática y exponencial sin intervención del propietario del dispositivo, evitando así delegar en la intervención humana el éxito de la amenaza.

Interactúan en tiempo real con la red de la víctima y las defensas que están desplegadas, para adaptarse a ellas y conseguir su objetivo.

Es fundamental saber a qué nos enfrentamos, cómo piensa y como actúa.

Así, y para familiarizarnos con los atacantes, hemos creado esta Cyber-Kill Chain para analizar los diferentes pasos que siguen desde la etapa de reconocimiento hasta la consecución de su objetivo:



Esta secuencia de acciones y su extensión, es una excelente herramienta para entender cómo las organizaciones pueden aumentar significativamente sus capacidades de defensa detectando y bloqueando las amenazas en cada fase del ciclo de vida de los ataques.

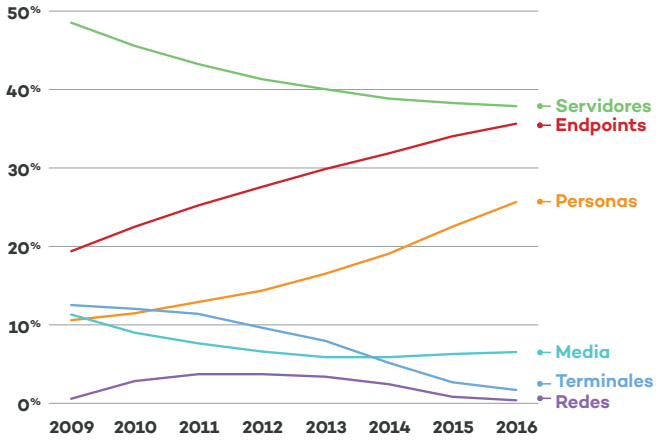
La Cyber-Kill Chain nos explica cómo mientras los adversarios deben progresar completamente a través de todas las fases de la cadena para su éxito, nosotros necesitamos “sólo” detener la cadena en cualquier punto del proceso para romper el ataque.

La explicación detallada de cada uno de las fases, está disponible **aquí**, y también puedes ver el **vídeo**.

El Objetivo es el Endpoint.

Hay un punto crítico que merece la pena destacar cuando hablamos de la evolución de los ataques. En muchas ocasiones los propios fabricantes de soluciones de seguridad invertimos mucho tiempo hablando del perímetro, Internet de las Cosas y demás vectores donde necesitamos protección, pero quizás no se hace foco en lo realmente importante: el endpoint.

¿Por qué es tan importante? Los atacantes necesitan alcanzarlo porque desde allí pueden acceder a otros objetivos, exfiltrar información, robar credenciales, reunir datos sobre la red o desplegar nuevos ataques. La tendencia nos la muestra claramente la siguiente gráfica:



Fuente: Verizon Data Breach Investigations Report.

Sin embargo, las empresas dedican la mayor parte de su presupuesto de seguridad en el perímetro, descuidando **la parte clave, el endpoint**.

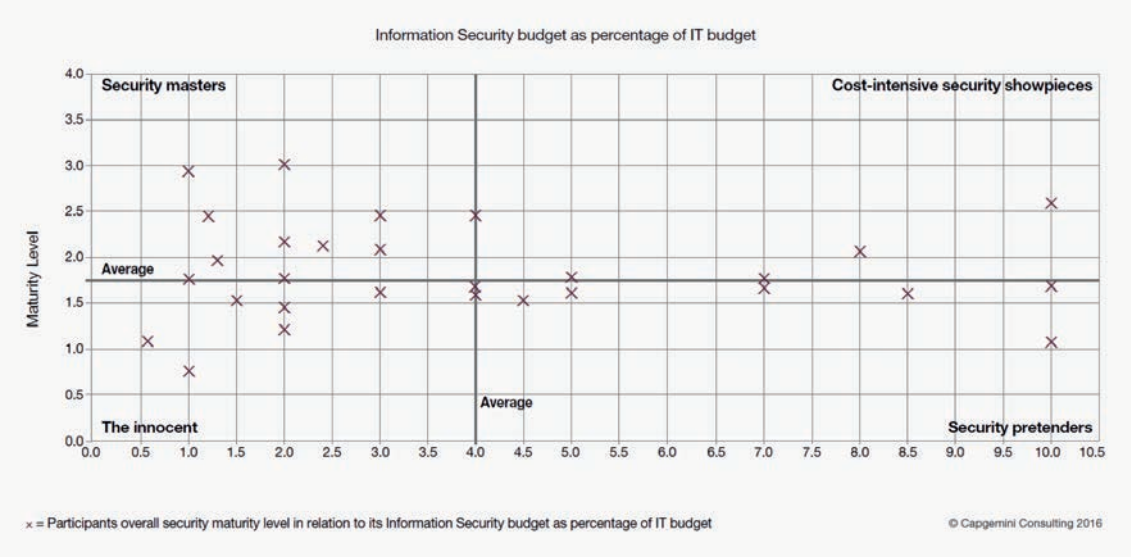
Esto no sucede por ignorancia o negligencia, al fin y al cabo, en el pasado tenía sentido este enfoque de centrarse en el perímetro: como los endpoints estaban seguros dentro de las redes corporativas, lo que había que hacer era reforzar las defensas contra los posibles atacantes externos, que debían pasar por el perímetro.

PRODUCTOS		SERVICIOS	
Perímetro	$11,9B	Consultoría	$21B
Identidad	$4,6B	Integración	$20B
Endpoints	$3,8B	SOC: • Prevención • Detección • Respuesta	$20B
Web	$2,6B		
Otros	$11,0B		

Hoy en día la situación ha cambiado: el perímetro se ha difuminado, la movilidad está en el día a día de cualquier compañía, y la transformación digital ha extendido la superficie de ataque a una velocidad casi incontrolable para las empresas.

Y así, los atacantes van a por los equipos. Saben que si logran llegar a uno de ellos la probabilidad de poder llevar a cabo sus acciones antes de ser detectados son muy altas.

Por tanto, es cuestión de establecer prioridades y no de invertir más, sino de invertir en donde realmente es necesario. Como demuestra este estudio de Capgemini, donde compara el nivel de inversión en seguridad con el nivel real de protección de los activos empresariales:



Cifras.

Una de las consecuencias más evidentes que ha conllevado la profesionalización de los ataques es que la cantidad de malware se ha multiplicado de forma exponencial. Hasta en un **50% más según Verizon, solo en ataques con Ransomware**.

Pero esto no es debido únicamente a que el número de ataques ha aumentado –que también-, principalmente se debe a las técnicas utilizadas.

Hace más de 10 años publicamos un artículo donde dábamos cuenta de esta tendencia. Haciendo un análisis retrospectivo veíamos como en 2002 los 10 ejemplares de malware más prevalente causaban un 40% de todas las infecciones, y en 2006 descendía hasta el 10%.

¿Cuál es la Situación en 2017?

Como todas nuestras soluciones se comunican con nuestra nube, podemos obtener datos con los que analizar si se ha agudizado esta tendencia.

Para calcular las cifras hemos tomado todo aquel malware (ficheros PE) que nunca habíamos visto antes del 1 de enero de 2017. Hasta el 20 de septiembre nos han preguntado por **15.107.232 ficheros de malware distintos**, hablamos sólo de los que nunca antes habíamos visto. El número total de malware creado es mucho mayor. Hay que sumar todos los tipos de ficheros (scripts, documentos, etc.) y todos aquellos que no han intentado infectar a nuestros clientes. Estamos hablando en **total de unos 75 millones, 285.000 nuevos ejemplares de malware al día**.

Estos son los 10 ficheros malware más consultados a nuestra nube:

POSIC.	VISTO	TIPO	NOMBRE
1	15/8/17	Trj/HackCCleaner.A	HackCCleaner
2	5/1/17	Trj/CerberCrypto.A	Cerber
3	15/5/17	Trj/RansomCrypt.I	WannaCry
4	15/8/17	Trj/HackCCleaner.A	HackCCleaner
5	17/5/17	Trj/Agent.SM	Downloader
6	24/2/17	Trj/Genetic.gen	Bot
7	15/5/17	Trj/RansomCrypt.I	WannaCry
8	12/5/17	Trj/RansomCrypt.K	WannaCry
9	15/5/17	Trj/Agent.PS	Downloader
10	12/5/17	Trj/RansomCrypt.K	WannaCry

Tiene todo el sentido que dentro de este top 10 aparezcan ficheros relacionados con los casos más graves ocurridos durante este año, como WannaCry (3ª, 7ª, 9ª y 10ª posición) y la versión backdorizada de CCleaner (1ª y 4ª posición). El resto son downloaders (troyanos que se utilizan como elemento intermedio para instalar todo tipo de malware) y un bot.

Y de todo este malware (15.107.232), ¿cuánto ha sido visto 1 única vez? **El 99,10%, 14.972.010**.

Si miramos las cifras desde el otro extremo, vemos que efectivamente una insignificante parte de todo el malware está realmente extendido. **Sólo hemos visto 989 ficheros de malware en más de 1.000 ordenadores, el 0,01%.**

Esto viene a confirmar lo que ya sabíamos, que salvo contadas excepciones -como WannaCry o HackCCleaner- la mayor parte del malware cambia cada vez que infecta, por lo que cada ejemplar tiene una distribución muy limitada.

Al agruparlo por familias o tipos podemos ver cómo el ransomware está muy presente, algo que tampoco nos coge por sorpresa ya que es uno de los ataques que más beneficios está dando a los ciberdelincuentes, motivo por el que se ha popularizado tanto en los últimos años.

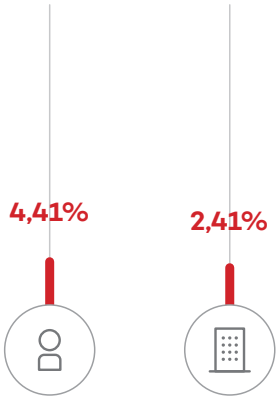
En cualquier caso, si lo que queremos es saber a qué riesgo de infección nos estamos enfrentando, el total de nuevo malware no es tan relevante, sino la frecuencia con el que nos podemos enfrentar al mismo. Para calcular este dato lo que hacemos es medir únicamente los intentos de infección de malware no detectado ni por firmas ni por heurísticos, tanto los ataques protagonizados por malware como por los ataques sin fichero (fileless) o aquellos realizados a través del abuso de herramientas legítimas del sistema, algo cada vez más habitual en entornos corporativos, como vimos en el caso de Goldeneye/Petya en junio.

Para medir esto utilizamos datos obtenidos de una serie de tecnologías propias, englobadas en lo que llamamos “Inteligencia Contextual”, que nos permite revelar patrones de comportamiento malicioso y generar acciones de ciberdefensa avanzada contra amenazas conocidas y desconocidas.

A continuación pasamos a analizar los datos de ataques que hemos obtenido.

No todos contamos con las mismas medidas de protección, ya que mientras un ordenador doméstico o de una pequeña empresa suele contar con protecciones más básicas (lo que acarrea que corran más riesgo), las medianas y grandes empresas cuentan con muchos más recursos dedicados a la protección de su información.

Aquí únicamente contabilizamos aquellos ataques que se saltan todas las protecciones, no son detectados y los paramos en el último momento antes de llegar a comprometer el ordenador. Quien dedique más recursos debería conseguir que llegaran menos de estos ataques, y efectivamente las cifras así nos lo muestran. Mientras que los **usuarios domésticos y pequeñas empresas tienen un 4,41% de ataques, en las medianas y grandes coporaciones la cifra baja hasta el 2,41%**.



Aunque estos datos puedan darnos una sensación de tranquilidad si estamos en una empresa, no debemos engañarnos: un atacante no necesita atacar todos los ordenadores de la red corporativa para causar un daño mayor. De hecho, atacará el mínimo número de ordenadores posibles para pasar desapercibido y así minimizar el riesgo de detección y así conseguir su objetivo.

Distribución Geográfica de los Ataques.

Hemos calculado el porcentaje de máquinas atacadas en cada país. A mayor porcentaje, mayor probabilidad de sufrir un ataque de nuevas amenazas en esos países:

Irán	11,96%
Argelia	11,81%
India	10,96%
Egipto	7,89%
Bolivia	6,88%
Rep. Dominicana	6,88%
Pakistán	6,43%
Sudáfrica	6,30%
Malasia	5,99%
Bangladesh	4,71%
Tailandia	4,59%
Indonesia	4,48%
Marruecos	4,28%
Moldavia	4,22%
Brasil	4,22%
Armenia	4,14%
El Salvador	3,98%
Paraguay	3,88%
Honduras	3,82%
Kazajstán	3,70%
Ucrania	3,63%
Venezuela	3,55%
Uruguay	3,50%
China	3,42%
Túnez	3,42%
Guatemala	3,32%
Filipinas	3,29%
Arabia Saudí	3,28%
Bielorusia	3,25%
Emiratos Árabes	3,22%
Chile	2,98%
Colombia	2,89%
Rusia	2,86%
Vietnam	2,82%
Ecuador	2,66%
Chipre	2,56%
México	2,39%
Georgia	2,34%
Macedonia	2,14%
Brunei	2,14%
Taiwán	2,08%
Perú	2,07%
Singapur	1,85%
Bosnia Herzegovina	1,82%
Costa Rica	1,82%
Bulgaria	1,81%
Turquía	1,79%
Italia	1,71%
Panamá	1,68%
Argentina	1,63%
Portugal	1,58%
Corea	1,53%
Serbia	1,51%
Puerto Rico	1,44%
Lituania	1,42%
Letonia	1,39%
Reino Unido	1,33%
Croacia	1,30%
Irlanda	1,26%
Eslovaquia	1,16%
España	1,14%
Estonia	1,09%
Alemania	1,06%
Rumanía	1,03%
Austria	1,01%
Israel	0,99%
USA	0,99%
Noruega	0,94%
Polonia	0,94%
Francia	0,93%
Australia	0,91%
Chequia	0,88%
Hong Kong	0,86%
Hungría	0,82%
Nueva Zelanda	0,79%
Suiza	0,78%
Malta	0,77%
Suecia	0,75%
Dinamarca	0,67%
Grecia	0,64%
Japón	0,64%
Eslovenia	0,62%
Canadá	0,60%
Bélgica	0,54%
Países Bajos	0,53%
Finlandia	0,51%

El año de un vistazo.

Hacer un seguimiento de los mayores ataques registrados a lo largo de todo 2017 es como viajar en una montaña rusa: no ves el camino que tienes delante y no puedes saber lo alto que subirás ni cómo será la bajada. Pero a pesar de la incertidumbre, sabes que nunca te has visto antes en una situación igual y que no lo olvidarás fácilmente.

Equifax, CCleaner, Sabre, WPA2, Vault7, CIA, KRACK, NSA, hackeo de elecciones... son algunos de los protagonistas analizados a continuación. Protagonistas de infecciones masivas, robos de datos, ataques de ransomware, aplicaciones hackeadas para lanzar ataques contra un país, para llevar a cabo ataques dirigidos contra grandes empresas concretas, hasta vulnerabilidades que afectan a miles de millones de dispositivos.

Pero hay dos ataques que destacan especialmente por el impacto y el daño causados: WannaCry y GoldenEye/NotPetya.

WannaCry apareció en mayo, propagándose y causando estragos en las redes de empresas de todo el mundo, resultando ser uno de los mayores ataques de la historia. Si bien por número de víctimas y velocidad de propagación hemos visto ataques en el pasado mucho más potentes (como el Blaster o el SQLSlammer, por poner sólo un par de ejemplos), lo cierto es que el daño que causaban era colateral a su propagación. Sin embargo, WannaCry es un ransomware con funcionalidad de gusano de red, por lo que cada ordenador infectado acababa con sus documentos secuestrados.

En este enlace podéis acceder al webinar impartido por Luis Corrons, Director Técnico de PandaLabs, donde realiza un análisis detallado de lo sucedido y de las medidas que se deben tomar para estar protegido ante ataques de este tipo.

Goldeneye/NotPetya ha sido el segundo ataque que más repercusión ha tenido este año, como **una réplica al terremoto 'WannaCry'**. A pesar de que sus víctimas estaban en principio limitadas a una zona geográfica concreta (Ucrania), acabó afectando a empresas en más de 60 países.

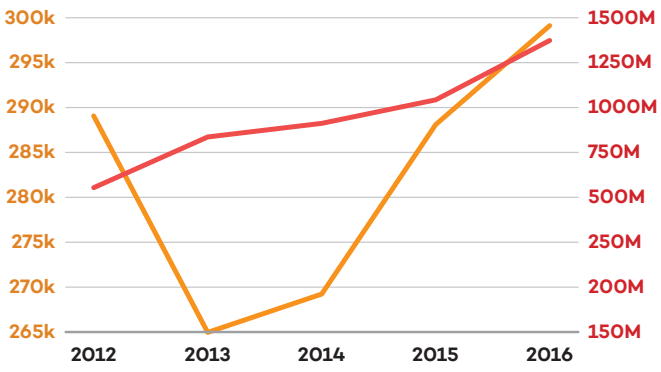
El ataque, cuidadosamente planeado, se llevó a cabo a través de una aplicación de contabilidad muy popular entre empresas en Ucrania, M.E.Doc. Los atacantes comprometieron el servidor de actualizaciones de dicho software, de tal forma que todos los ordenadores con M.E.Doc instalado pudieron ser infectados de forma automática.

Además de cifrar los ficheros, en caso de que el usuario que tiene la sesión iniciada en el ordenador tenga permisos de administrador, el malware va a por el MBR (Master Boot Record) del disco duro. En principio aparentaba ser un ransomware al estilo de WannaCry, pero tras analizarlo a fondo uno se percata de que realmente sus autores no tenían intención de dejar que la información secuestrada fuera recuperada.

Días después, el gobierno ucraniano acusó abiertamente a Rusia de estar detrás del ataque. Luis Corrons, Director Técnico de PandaLabs, desgrana las claves de este ataque y de sus autores en la presentación que puedes ver aquí.

Cibercrimen.

Según el informe "2016 Internet Crime Report" publicado por el Internet Crime Complaint Center (IC3) del FBI, **las pérdidas debidas al cibercrimen aumentaron un 24%, superando los 1.300 millones de dólares**. Hay que tener en cuenta que esto contabiliza sólo la cantidad reportada por víctimas estadounidenses al IC3, que estima que se trata de un 15% de las mismas, por lo que la cifra total (sólo para Estados Unidos) aumentaría hasta las **9.000 millones de dólares de pérdidas en 2016**.



Los exploits más codiciados para lanzar ataques son los conocidos como "0-day". Desconocidos por el fabricante del software afectado y que permite a los atacantes comprometer a los usuarios aunque tengan todo su software actualizado.

En abril se descubrió una de estas vulnerabilidades que afectaba a diferentes versiones de Microsoft Word. Se sabe que, al menos desde enero de este año, había estado siendo utilizada por atacantes.

El mismo mes de abril Microsoft publicó la actualización correspondiente para proteger a sus usuarios de Office.

Un ejemplo claro de profesionalización del cibercrimen es RDPatcher, un **ataque** descubierto por PandaLabs, cuya finalidad es dejar el equipo de la víctima listo para **ser alquilado** al mejor postor en el mercado negro.

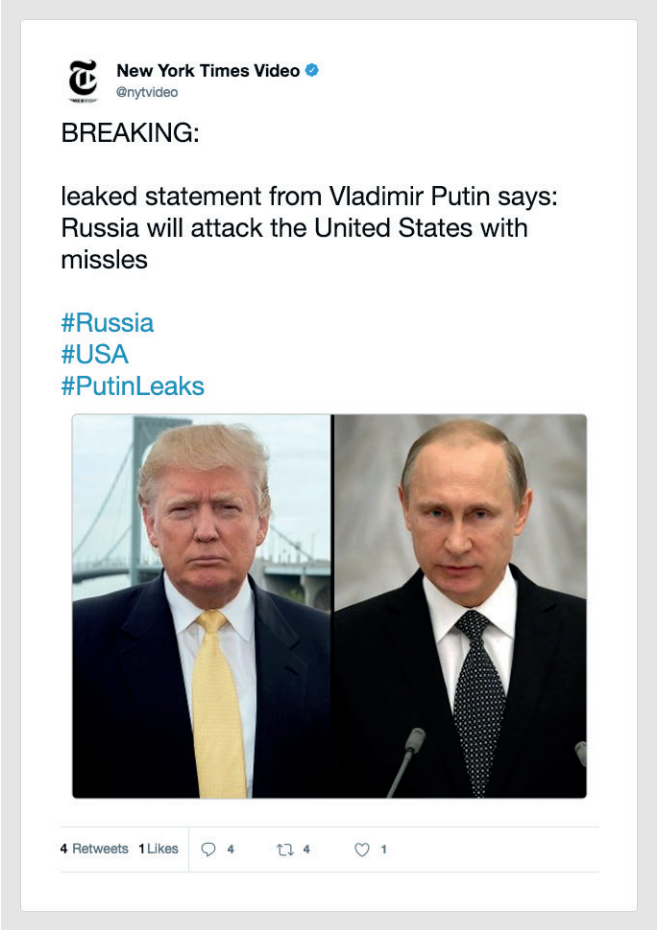
Los ciberdelincuentes tratan de evitar ser detectados, y uno de los métodos más efectivos para conseguirlo es no utilizar malware. Por tanto, los ataques malwareless se han popularizado, como en **este caso** descubierto por PandaLabs, dónde se ve cómo tras llegar a un equipo los atacantes dejan abierta una puerta trasera por la que entrar al mismo sin tener que instalar malware con ayuda de las "**Sticky keys**".

En la segunda mitad de 2016 vimos varios **ataques DDoS** muy sonados, y en 2017 se han visto más ataques de este estilo aunque no tan brutales. Clientes de Lloyds tuvieron problemas para acceder a sus cuentas online como consecuencia de un ataque DDoS lanzado contra la entidad que saturó sus servidores.

La policía de Estado italiana desarmó en enero una central de ciberespionaje, bautizada como **Eye Pyramid** creada por dos hermanos italianos con el objetivo de controlar instituciones y administraciones públicas, estudios profesionales, empresarios y políticos.

El **hackeo de cuentas de redes sociales** es un habitual, y uno de los casos más llamativos sucedió en enero, cuando la cuenta de Twitter oficial de vídeos del New York Times fue comprometida. En cuanto recuperaron el control de la misma borraron los tweets que había publicado los atacantes:

Este es uno de los tweets que el grupo publicó, anunciando que Rusia iba a lanzar un ataque con misiles a Estados Unidos:



El mismo grupo es conocido por haber hackeado otras cuentas de empresas como Netflix o Marvel.

Un grupo de ciberdelincuentes denominado "**Turkish Crime Family**" chantajeó a Apple, pidiéndole un rescate para evitar borrar remotamente los datos de los iPhones, iPads y Macs de más de 250 millones de usuarios. Apple se negó a ceder al chantaje.

Robos de Datos a Empresas.

Los robos de datos también han protagonizado titulares a lo largo de este año. Empezamos con un caso muy irónico: Cellebrite, compañía israelí que se dedica a facilitar el hackeo de teléfonos -concretamente la extracción de información de los mismos-, fue hackeada y le robaron 900Gb de datos. Entre la que se encuentran datos de clientes, bases de datos e información técnica sobre los productos de la compañía.

Historiales médicos de al menos 7.000 personas han sido comprometidos por una brecha de seguridad en el Bronx Lebanon Hospital Center en Nueva York.

Otro tipo de incidentes de seguridad donde no hay atacantes directamente implicados son aquellos en que debido a un error o negligencia, datos que deberían estar protegidos se exponen a que cualquiera pueda acceder a ellos. Esto sucedió en EEUU. Unas empresas de marketing contratadas por el partido republicano **dejaron accesible a todo el mundo datos de 198 millones de votantes** registrados, lo que supone casi la totalidad de votantes.

Dow Jones sufrió un error mediante el que dejaron acceso a través de la nube de Amazon datos de 2 millones de sus clientes debido a un error de configuración. Entre la información comprometida hay nombres, direcciones de correo, e incluso los últimos números de la tarjeta de crédito.

22 personas han sido detenidas en China por traficar con datos de clientes de Apple en el país asiático. Todo parece indicar que se trata de un trabajo desde dentro, ya que algunos de los detenidos trabajaban para empresas subcontratadas por Apple y que tenían acceso a la información con la que los detenidos estaban traficando.

HBO ha sufrido este año varios ciberataques. En uno de ellos le comprometieron servidores robándole **episodios** completos aún no estrenados de diferentes series de televisión, así como información interna.

InterContinental Hotels Group (IHG) fue víctima de robo de información de sus clientes. Si bien la empresa dijo en febrero que el ataque únicamente había afectado a una docena de sus hoteles, se ha sabido ahora que tenían TPVs (Terminales de Punto de Venta) **infectados en más de 1.000 de sus establecimientos**. Entre las diferentes marcas de hoteles que posee el grupo se encuentran Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels, y Crowne Plaza.

Sabre Corporation es una empresa estadounidense que gestiona reservas para 100.000 hoteles y más de 70 aerolíneas de todo el mundo. Un atacante consiguió las credenciales para acceder a uno de los sistemas de reserva de la compañía, accediendo a información de pago y detalles de reservas gestionados desde el mismo.

Este sistema en concreto gestiona las reservas de particulares y agencias de viajes para 35.000 hoteles y establecimientos de alojamiento. **Estuvieron comprometidos desde el 10 de agosto de 2016 al 9 de marzo de 2017, 7 meses**.

De este incidente se han derivado diferentes noticias de ataques a hoteles, aunque en esta ocasión no habían atacado los sistemas de los mismos, sino que se han visto afectados por el ataque a Sabre. **Entre algunas de las cadenas hoteleras afectadas se encuentran Four Season Hotels & Resorts, Trump Hotels, Kimpton Hotels & Restaurants, Red Lion Hotels Corporation, Hard Rock Hotels y Loews Hotels**.

Taringa, una popular red social en Latinoamérica, sufrió una brecha de seguridad en la que le fue extraída información de más de 28 millones de sus usuarios, incluyendo el nombre de usuario, correo electrónico y el hash (MD5) de la contraseña.

Pero la mayor brecha de seguridad del año, y de las peores de la historia, llegaría algo más tarde, cuando se supo que el gigante especializado en informes crediticios, **Equifax, había sido comprometido**. Debido al trabajo que debe realizar la empresa posee cantidad abundante de información confidencial de millones de personas.

El ataque se llevó a cabo a través de una **vulnerabilidad en Apache Struts** presente en uno de los servidores de la empresa. La vulnerabilidad se hizo pública, junto a la correspondiente actualización que la solucionaba, el 6 de marzo. Pocos días más tarde los atacantes dieron con el servidor de la empresa, que estuvo comprometido hasta finales de julio, cuando descubrieron el ataque. **Los datos de unos 200 millones de personas se han visto comprometidos**, un 70% de los mismos de EEUU y el resto de Reino Unido y Canadá. Más tarde la lista de países afectados se amplió a Argentina, Brasil, Uruguay, Perú, Paraguay, Ecuador y Chile.

Para empeorar la situación se supo que 3 ejecutivos de la firma aprovecharon el periodo que pasó desde que se descubrió la brecha de seguridad y se hizo pública para vender acciones de la empresa por un valor de 1,8 millones de dólares. La responsable de seguridad de la firma fue despedida y apenas un mes después Richard Smith, CEO de Equifax desde 2005, anunció que se retiraba.

Caballos de Troya.

Después de Goldeneye/NotPetya, la empresa **Netsarang** sufrió un ataque mediante el cual versiones de 5 de sus programas (Xmanager Enterprise 5.0, Xmanager 5.0, Xshell 5.0, Xftp 5.0, or Xlpd 5.0) incluían un backdoor. El fichero comprometido tenía firma digital válida de la empresa, lo que significa que los atacantes les habían comprometido completamente. Entre los clientes de esta empresa se encuentran bancos y compañías energéticas.

El caso de software comprometido más sonado este año es sin duda el de **CCleaner**. Las versiones comprometidas fueron instaladas por más de 2 millones de usuarios. El software comprometido se quedaba a la espera de recibir órdenes y aparentemente no llevó a cabo ninguna acción maliciosa. Sin embargo, investigadores de Cisco descubrieron que los atacantes tenían una lista con las empresas cuyos ordenadores querían comprometer, se trataba de 20 compañías de alto perfil entre las que se encontraban Samsung, Cisco, Sony, Intel y Microsoft.

Estos tres ataques tienen un claro perfil extremadamente profesional que apunta a que podría haber países detrás de los mismos. De hecho, la misma OTAN declaró que detrás del ataque del Goldeneye/NotPetya se encontraba alguna nación.

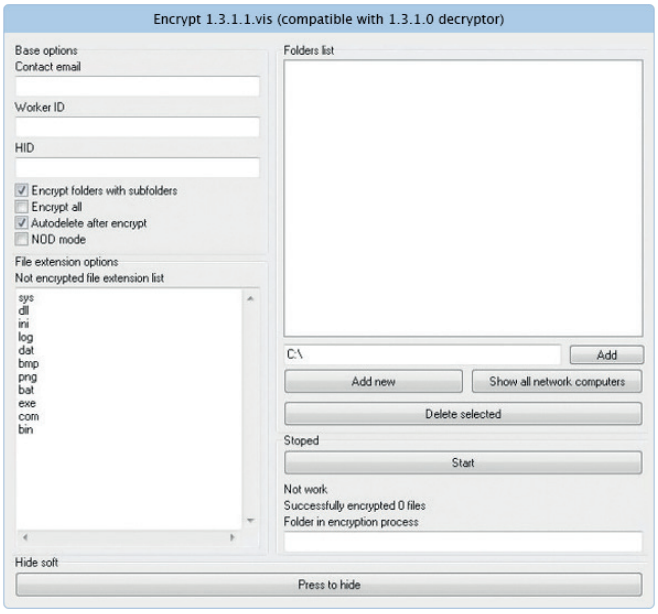
Impacto global de los ataques

Ransomware.

Los ataques de ransomware siguen en auge, y así seguirán mientras las víctimas sigan pagando los rescates.

Además de las conocidas familias de ransomware (Locky, Cerber, etc.) aparecen soluciones más personalizadas para este tipo de víctimas.

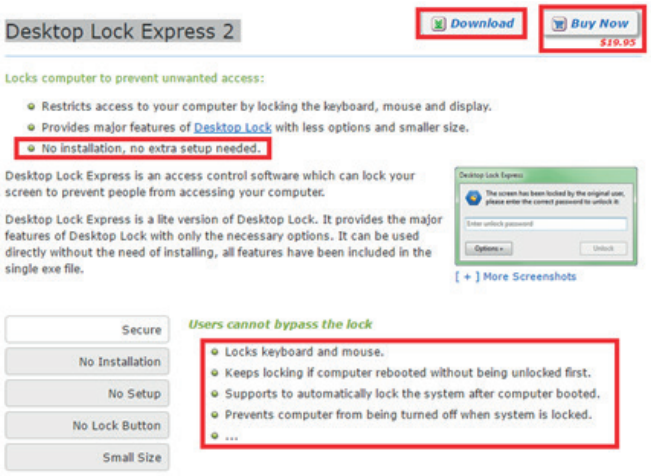
Uno de ellos fue descubierto por PandaLabs, se trata de un ransomware con interfaz propia, bautizado como **WYSIWYG**, que permite al delincuente seleccionar las carpetas cuyo contenido se cifrará, los ordenadores de la red, auto-borrado, la dirección de email a la que deben dirigirse las víctimas, etc.:



Uno de los métodos más populares, y relativamente sencillos, de **penetrar en una red corporativa es a través de ataques de fuerza bruta a través de RDP**, el popular Escritorio Remoto que viene con Windows. Los atacantes van escaneando Internet en busca de ordenadores que lo tienen activado y una vez encuentran una potencial víctima, lanzan un ataque de fuerza hasta que dan con las credenciales correctas.

Hemos visto a lo largo de 2017 numerosos ataques de este tipo con atacantes de origen ruso. Todos sigen un esquema similar: una vez acceden al ordenador tras el ataque a través de RDP instalan software de minería de bitcoins, como método para obtener beneficios añadidos, y luego bien cifran ficheros o bloquean el acceso al ordenador.

No siempre utilizan malware para esto, por ejemplo, en uno de los casos que **analizamos** utilizaron la aplicación comercial "Desktop Lock Express 2" para llevar a cabo el bloqueo del ordenador:



Las consecuencias inmediatas de un ataque de ransomware son claras, pierdes el acceso a tus ficheros. Sin embargo los casos de secuestro digital pueden ir mucho más allá de esto, como pudieron comprobar los clientes de un **hotel en Austria,** que tras ser atacado por ciberdelincuentes éstos bloquearon las puertas de las habitaciones e inutilizaron el software de programación de las tarjetas de entrada a las habitaciones.

La empresa de alojamiento de páginas web Nayana, de Corea del Sur, fue atacada y el ransomware cifró información de 153 servidores Linux. **Los atacantes exigieron un rescate de 1,62 millones de dólares**. La empresa negoció con los delincuentes y rebajó la cifra a 1 millón de dólares, a pagar en 3 veces.

Internet Of Things (IoT).

Desde hace años se está alertando del peligro que los dispositivos de Internet de las Cosas tienen debido a que no se tiene en cuenta la seguridad en el diseño de muchos de ellos.

O porque, en ocasiones, simplemente son aparatos que sin conexión a la red no suponen un riesgo, pero cuando se les añade una conexión a Internet quedan accesibles a todo el mundo pudiendo ser objetivo de ataques.

Parece que este llamamiento ha ido calando y en EEUU un grupo de senadores demócratas y republicanos se han unido para crear una legislación que solucione en parte esta situación. La idea es exigir a los fabricantes de productos con conexión a Internet que éstos sean actualizables (para poder así corregir fallos de seguridad), prohibir que vengan con contraseñas que no se puedan cambiar o que se pongan a la venta dispositivos que tienen agujeros de seguridad conocidos, entre otras medidas.

Edificios Inteligentes.

De un tiempo a esta parte, la mayoría de edificios se han ido adaptando para registrar el consumo eléctrico de hogares y oficinas mediante los 'smart meters' o **contadores inteligentes**. Más allá del posible efecto en la factura de la luz que algunas asociaciones de consumidores ya han denunciado, lo cierto es que la generalización de este tipo de aparatos entraña algunos riesgos menos conocidos en materia de seguridad.

Tal y como explicó el investigador Netanel Rubin durante la pasada edición del Chaos Communications Congress, celebrada en Hamburgo (Alemania), estos contadores suponen un peligro en varios frentes. En primer lugar, como registran todos los datos de consumo de hogares y oficinas para mandarlos a la compañía eléctrica, un atacante que lograra tomar el control podría ver la información y utilizarla con fines maliciosos.

Por ejemplo, podría averiguar si la vivienda u oficina está vacía para perpetrar un robo. Incluso, dado que todo dispositivo electrónico deja un rastro en la red eléctrica, podrían detectar las variaciones para averiguar qué dispositivos de valor tendrán a su alcance cuando accedan al lugar.

Smart TV.

Otro dispositivo cada vez más común es la Smart TV o **televisión inteligente**. Algunos utilizan versiones de Android como sistema operativo, lo que tiene sus ventajas y también sus inconvenientes. Darren Cauthon daba cuenta de ello en Twitter revelando que el televisor de un miembro de su familia había sufrido un ataque. Según explicó, todo sucedió después de que la víctima instalara una aplicación para ver películas en internet, al parecer desde un sitio de terceros.

Se trataba de un modelo de la marca LG, fabricado en el 2014, que funciona con Google TV, una versión de Android específica para televisores. Una vez hubo infectado el dispositivo, el 'software' malicioso **pidió al afectado 500 dólares** (unos 471 euros) por el desbloqueo en una pantalla que simulaba un aviso del Departamento de Justicia estadounidense.

Paralelamente, se están gestando ataques mucho más peligrosos, que pueden darnos una idea de lo que está por llegar en este terreno. En febrero, durante el European Broadcasting Union Media Cyber Security Seminar, fue mostrado el exploit creado por el consultor de seguridad Rafael Scheel, el cual permite tomar control de una Smart TV sin acceso físico a la misma mandando el ataque a través de la señal TDT.

Smart Cities.

En Australia, **55 cámaras de tráfico** ubicadas en semáforos y controles de velocidad se vieron afectadas después de que un trabajador de una subcontrata conectara un ordenador infectado a la red donde éstas se encontraban.

El pasado 7 de abril en Dallas, Texas, 156 sirenas de emergencia se pusieron a sonar al unísono desde las 23:40 de la noche. Funcionarios lograron pararlas 40 minutos después, tras echar abajo todo el sistema de emergencias. Aún se desconoce quién fue el responsable.

Automoción.

Se ha dado a conocer una nueva vulnerabilidad afectando a coches, en este caso de la marca Mazda. Sin embargo, al contrario que en ocasiones anteriores, para poder comprometer el sistema del coche se necesita introducir un USB mientras el motor está en marcha en un modo de funcionamiento determinado.

Si bien los coches y demás vehículos son elementos habituales que no sorprende que puedan llegar a tener conexión a Internet, hay otros relacionados con el sector en los que claramente esto es impensable. Este es el caso de los lavacoches.

Los investigadores Billy Rios y Jonathan Butts presentaron en la conferencia Black Hat en Las Vegas cómo habían conseguido **hackear lavacoches automáticos** que se encuentran conectados a la red, secuestrando el sistema de tal forma que podían atacar físicamente al vehículo y a sus ocupantes.

Más allá de los coches y continuando en el sector automoción, **los Segways pueden ser hackeados de forma remota**, pudiendo llegar a ser controlados de forma total por un atacante.

El investigador Thomas Kilbride de IOActive demostró diferentes vulnerabilidades y problemas de seguridad. Uno de los más graves es que el Segway no comprobaba las actualizaciones que se le aplicaban, de tal forma que cualquiera podría en un momento dado actualizar el aparato con un firmware malicioso a merced del atacante.

Infraestructuras Críticas.

El investigador holandés Willem Westerhof ha estado analizando convertidores de corrientes utilizados en **paneles solares** para transformar la corriente en alterna y poder así volcarla a la red general de una de las empresas líder en este sector, SMA Solar Technologies.

En total ha encontrado 21 vulnerabilidades que permitirían a un atacante, por ejemplo, controlar la cantidad de electricidad que se vuelca en la red. Son vulnerabilidades que se pueden explotar de forma remota a través de la red.

Un atacante malicioso que comprometiera estos dispositivos podría ocasionar daños incalculables. En esta **web** se puede encontrar todos los detalles.

Hospitales y Salud.

Sin duda el hackeo de la red eléctrica es algo muy grave que puede afectar a las vidas de innumerables personas, aunque palidece con el riesgo que supone que **un atacante pueda controlar un marcapasos** y material hospitalario como si se tratara de una **ciber-pandemia**, lo que permitiría en el peor de los casos matar de forma remota a una persona.

La FDA (Food and Drug Administration) norteamericana avisó a casi medio millón de pacientes para que acudieran a su médico para realizar una actualización del firmware de sus marcapasos, diferentes modelos pertenecientes al fabricante Abbott.

Móviles.

La creación de nuevo malware para dispositivos móviles sigue siendo muy inferior al que vemos en PCs, aunque sigue los mismos pasos. El popular ransomware, que tan buenos resultados está dando a los delincuentes, y su traslado a este tipo de dispositivos es una clara prueba de ello.

Malware para Móviles.

Un buen ejemplo es un nuevo malware para Android, conocido como "Charger", que tras ser instalado en el teléfono roba los contactos y mensajes de SMS. A continuación bloquea el terminal, solicitando un rescate o amenazas con comenzar a vender parte de tu información en el mercado negro cada 30 minutos. El rescate solicitado es de 0,2 bitcoins.

Las grandes compañías muestran su preocupación y lanzan iniciativas como la de Google, propuesta en junio, que consiste en aumentar las recompensas para quien encuentre los fallos de seguridad más graves que se pueden dar (no ha sido descubierto ninguno en los últimos años). La primera recompensa aumenta de 50.000 a 200.000 dólares, y la segunda de 30.000 a 150.000.

Vulnerabilidades.

Una vulnerabilidad (CVE-2017-6975) en el firmware de los chips Broadcom Wi-Fi HardMAC SoC cuando se renegocia una conexión a la red WiFi obligó a Apple a lanzar una actualización de iOS (10.3.1). Esta vulnerabilidad, sin embargo, no sólo afecta a iPhones y iPads, sino también a dispositivos móviles de otros fabricantes como Samsung o los mismos Nexus de Google, que recibieron en abril su actualización de seguridad para solventar este problema.

Pero si una vulnerabilidad se lleva la palma es la conocida como KRACK, que afecta al protocolo WPA2. No es única de dispositivos móviles, ya que afecta a todo tipo de dispositivos que implementan WPA (ordenadores personales, routers, etc.), pero sí es de destacar el problema que conllevará principalmente para los usuarios de móviles con sistema operativo Android.

El problema de seguridad fue descubierto en 2016 por los investigadores belgas Mathy Vanhoef y Frank Piessens, pero no fue hasta octubre de 2017 cuando se hizo público.

Una de las implementaciones del protocolo en código libre, "wpa_supplicant" utilizada tanto por Linux como por Android, es especialmente vulnerable a este ataque.

Si bien Google publicará el parche de seguridad correspondiente para su sistema operativo, son muchos los fabricantes de dispositivos que tienen que implementar su versión de las actualizaciones, y hay muchos dispositivos (cientos de millones) en uso cuyos fabricantes ya no dan mantenimiento, por lo que nunca recibirán las actualizaciones necesarias. Un problema recurrente en este ecosistema.

Ciberguerra.

Hay sospechas detrás de los 2 grandes ataques del año (**WannaCry y Goldeneye/NotPetya**) podría haber gobiernos (Corea del Norte en el caso del WannaCry y Rusia en el de Goldeneye/NotPetya), pero estos son únicamente un par de casos dentro de la ciberguerra más o menos encubierta que está teniendo lugar en el ciberespacio.

Los protagonistas principales se repiten de forma constante: Estados Unidos, Rusia, Corea del Norte, China e Irán. Aunque en la mayoría de ocasiones no es posible asegurar con certeza quién está detrás de un ataque. Por un lado teniendo medios, es relativamente sencillo ocultar tus huellas, e incluso dejar pruebas que apunten a otro, es algo que sucede cada vez con más frecuencia.

Más que nunca los ciberataques y la política están relacionados. Tras la resaca de las elecciones estadounidenses del pasado año, las acusaciones de ciberataques de EEUU a Rusia han dado paso a sanciones. Antes de abandonar su cargo, Obama anunció sanciones al país acusándolo de orquestar **ataques informáticos para dañar la campaña de la demócrata Hillary Clinton** y favorecer a Donald Trump, expulsando a 35 diplomáticos rusos y cerrando 2 centros propiedad del Gobierno ruso.

Todo esto ha tenido repercusión en otros países del mundo. **En Francia han descartado el uso del voto electrónico** por parte de sus ciudadanos residentes en el extranjero ante el riesgo "extremadamente elevado" de que tengan lugar ciberataques.

En Holanda han ido aún más lejos, y sus autoridades anunciaron que contabilizarían a mano los votos en la noche electoral y comunicarían los resultados por teléfono para evitar el **riesgo de un posible ciberataque**.

De hecho Holanda pidió en febrero la creación de una alianza internacional de defensa cibernética, a través de la OTAN, que tenga capacidades de defensa, control y ataques de respuesta contra la creciente amenaza de los ciberataques.

La canciller alemana Angela Merkel dijo en marzo que proteger las infraestructuras alemanas de potenciales ciberataques era una de las mayores prioridades del momento. Poco después se supo que **el ejército alemán formará su propio cibercomando para reforzar sus defensas online**. En principio contará con 260 empleados, que irán aumentando hasta alcanzar los 14.500 en 2021.

Uno de los eventos más remarcables este año en lo que respecta al ciberespionaje es el protagonizado por la CIA, muy a su pesar.

El 7 de marzo, **Wikileaks comenzó a publicar una serie de documentos bajo el título "Vault 7"** que contenían detalles de técnicas y herramientas de software utilizadas para entrar en smartphones, ordenadores e incluso televisores con conexión a Internet. Wikileaks está publicando los documentos en una **sección de su página web**.

Lo bueno es que el conocimiento publicado, puede ser utilizado para protegerse mejor contra; lo malo es que otros actores pueden aprender para poner en práctica tácticas similares que busquen violar la privacidad de sus ciudadanos.

En Estados Unidos están claramente preocupados ya que sus instituciones son el objetivo de muchos atacantes. El Comité de Inteligencia del Congreso llevó a cabo una audiencia para tratar **el impacto del hackeo por parte de Rusia de las elecciones** presidenciales de 2016. Allí el antiguo Secretario del DHS bajo la administración Obama, Jeh Johnson, reiteró que el presidente ruso Vladimir Putin había ordenado el ataque con la intención de influir en el resultado. También confirmó que estos ataques no habían conseguido manipular votos.

En junio el gobierno norteamericano lanzó una alerta en la que culpaba al gobierno de Corea del Norte por **una serie de ciberataques ocurridos desde 2009**, y advirtiendo que es probable que cometan aún más.

La advertencia, que vino del DHS y del FBI, se refería a un grupo de atacantes, "Hidden Cobra", que han atacado a medios de comunicación, sectores como el aeroespacial y el financiero, así como infraestructuras críticas tanto en EEUU como en otros países. **Hay evidencias que relacionan el reciente ataque de WannaCry con el grupo Hidden Cobra**, o más recientemente conocidos como "Lazarus Group".

Una de las implicaciones del número de ataques atribuidos a este país es el aumento de sanciones por parte de la ONU al gobierno norcoreano. Lo que, a su vez, les habría llevado a buscar nuevas fórmulas de financiación.

Durante la 'Gartner Security & Risk Management Summit' que se celebró en Washington en junio, el exdirector de la CIA, John Brennan, comentó que la **supuesta alianza entre el gobierno ruso y cibedelincuentes para llevar a cabo el robo de cuentas de Yahoo** se trata sólo de la punta del iceberg, y que futuros ciberataques llevados a cabo por gobiernos se incrementarán y seguirán este tipo de fórmula.

Miembros del parlamento británico han sido objetivo de intentos de ataques para hackear sus cuentas, según publicó el Financial Times, en lo que se cree que es un ataque patrocinado por una potencia extranjera.

FINANCIAL TIMES

Cyber Warfare

British MPs targeted by hackers in co-ordinated attack

An armed police officer outside the Houses of Parliament © AFP

MAY 17, 2017 **Sam Jones**, Defence and Security Editor 5 comments

Toda esta vorágine está afectando a empresas tecnológicas. El FSB ruso está demandando a compañías como CISCO, SAP o IBM el código fuente de sus soluciones de seguridad para buscar **posibles puertas traseras (backdoors).** Poco después, el gobierno de Estados Unidos prohibió a todas las agencias federales del país que utilicen soluciones de Kaspersky, debido a su cercanía al gobierno ruso y al FSB.

theguardian

US government bans agencies from using Kaspersky software over spying fears

Federal agencies have been barred from using cybersecurity software made by Kaspersky Lab over fears the firm has ties to state-sponsored spying programs

Aunque no hay pruebas tangibles que atestigüen la actividad maliciosa de Kaspersky, es comprensible que en el actual clima de tensión que viven las dos potencias, el gobierno estadounidense esté preocupado. No por una actitud sospechosa de Kaspersky, sino simplemente porque se trata de una empresa rusa. País cuyo gobierno es más cercano al lado autoritario que al democrático, y así anticipan que **el gobierno ruso podría, en un momento dado, forzar a Kaspersky a utilizar su software para lanzar un ataque o robar** información, en el caso de que el conflicto escale en intensidad.

Threat Hunting, la Investigación Detrás del Ataque.

Iñaki Urzay
Chief Security Strategist de Panda Security

Asistimos a un crecimiento exponencial en el número de expertos en ciberseguridad en todo el mundo. Este movimiento está auspiciado, en primer lugar, por los propios gobiernos que necesitan involucrarse (por iniciativa propia o de forma reactiva) en un conflicto virtual del que nadie puede permanecer al margen.

Los gobiernos de todo el mundo llevan tiempo creando organismos gubernamentales especializados en ciberdefensa, con exponentes tan claros como el recién creado nuevo cuerpo del **ejército alemán con más de 13.000 ciber soldados, los más de 100.000 proyectados por la administración americana para el 2020, los más de 6.000 con los que parece cuenta Corea del Norte** y los otros tantos en los ejércitos de Rusia, China, UK, Francia, España, Israel, Irán, etc.

A estos números debemos sumarles los de los especialistas con los que cuentan contratistas y vendedores de soluciones de seguridad en todo el mundo. Todos ellos cuentan con expertos en ciberseguridad, en todos los países. Y finalmente, los números de los ciberdelincuentes que fruto de esta explosión de expertos e interés global en ciberseguridad, con sus correspondientes cursos de formación, herramientas, etc; son capaces de encontrar recursos capacitados con mucha mayor facilidad.

Este incremento de capacidad humana altamente cualificada crea un ecosistema que hace posible el descubrimiento sistematizado de vulnerabilidades en el software. También favorece el desarrollo de herramientas profesionales de ataque e incluso la sostenibilidad y escalabilidad de los **ataques directos basados en personas que no utilizan malware y que permiten una adaptabilidad total al entorno** y el más alto grado de sigilo.

Tal y como nos demuestra nuestra solución Panda Adaptive Defense, **los ataques basados en malware pueden controlarse perfectamente** con soluciones basadas en el modelo positivo estricto creado por Panda Security.

En el momento en que se clasifican todas las aplicaciones que intentan ejecutarse en un equipo y sólo se permiten ejecutar aquellas que son realmente confiables, **el "gap de detección" que caracteriza a los modelos antivirus clásicos desaparece bajo este nuevo paradigma**. El malware ya no puede ocultarse entre los ficheros desconocidos que una solución tradicional de seguridad tiene que ignorar.

La potencia para detener los ataques de este tipo de modelos no es algo que el mercado en general pueda permitirse ignorar y el crecimiento de cuota de mercado del modelo es una consecuencia fácilmente previsible. A medida que este paradigma sustituya a los modelos antivirus tradicionales los atacantes adaptarán sus técnicas para intentar sortearlos. Y en este caso, una posibilidad verosímil sería la ejecución de ataques no basados en malware.

Los ataques malwareless se caracterizan por la utilización exclusiva de las herramientas usadas habitualmente por el administrador legítimo de la red para realizar sus labores; por ejemplo mecanismos para la instalación de software de forma remota o para realizar copias de seguridad de los datos, etc. En este tipo de operaciones **el atacante asume la identidad del administrador**, después de haber conseguido de una forma u otra sus credenciales de red y a todos los efectos para un observador externo aparenta ser el administrador de la red realizando su trabajo diario.

Al no utilizar malware de ningún tipo, los sistemas de seguridad deben ser capaces de distinguir un ataque de este tipo **basándose en el comportamiento exhibido por los usuarios de la red** corporativa. Las tecnologías capaces de realizar estas labores se engloban dentro del concepto de Threat Hunting.

Las plataformas de Threat Hunting deben ser capaces, entre otras cosas, de monitorizar el comportamiento de los equipos, las aplicaciones que se ejecutan en los mismos y sobre todo de los usuarios de la red. Para cada uno de estos elementos deben definir perfiles de comportamiento esperado de forma dinámica y, en tiempo real, cotejar los modelos contra los datos reales buscando desviaciones sobre el comportamiento indicativas de que puede estar produciéndose una suplantación de identidad.

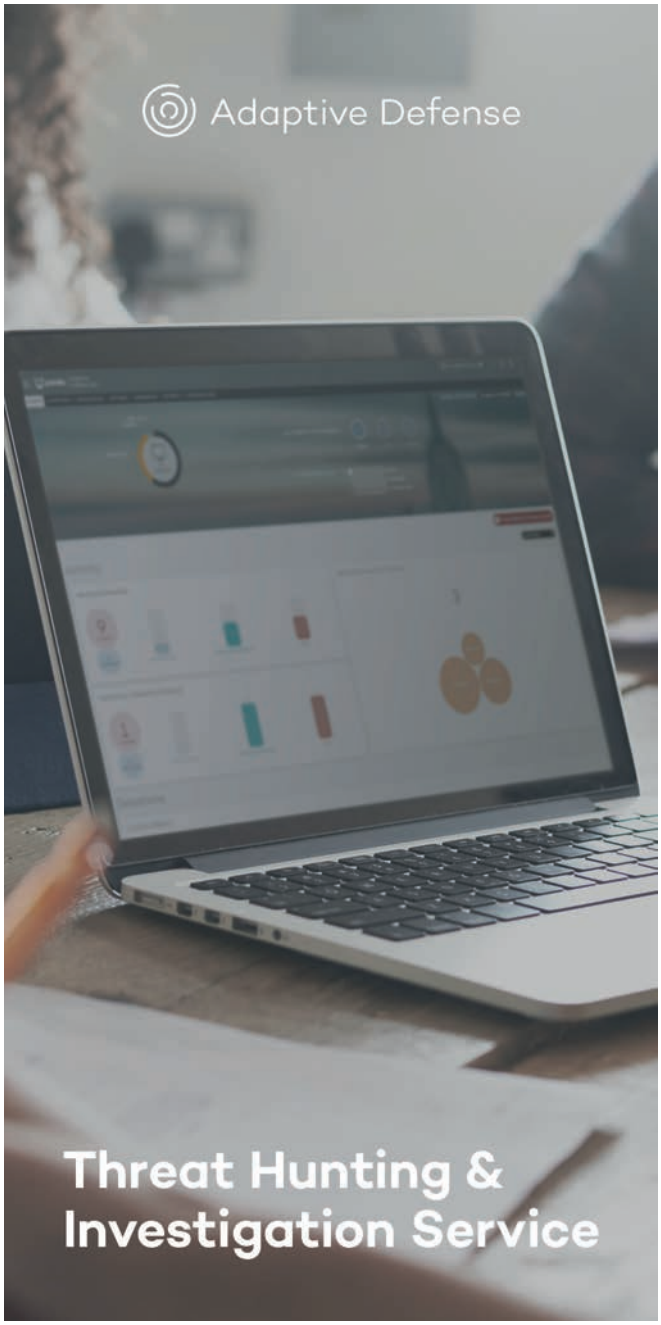
Técnicamente, el proceso de Threat Hunting se fundamenta en un inmenso almacén de datos con todo el comportamiento de las entidades monitorizadas actualizado en tiempo real a medida que suceden los nuevos eventos. Sobre este lago de información, la plataforma debe ofrecer la **capacidad de exploración libre sobre los hechos para encontrar nuevas hipótesis de ataque**, definir patrones de búsqueda sobre conjuntos parciales de los datos a modo de back-testing antes de activarlos sobre la corriente principal de datos en tiempo real, junto con los modelos basados en la búsqueda de anomalías en los perfiles de comportamiento. En ese momento **los sistemas de machine learning priorizarán los potenciales incidentes** que, una vez detonados, deberán ser analizados en detalle mediante herramientas de análisis forense remotas integradas en la plataforma.

Estas herramientas permiten a los analistas realizar exploraciones personalizada en los equipos afectados con capacidad para situarse en cualquier punto del tiempo en el historial de eventos de cada equipo o cada usuario analizado y reconstruir sus pasos permitiendo así confirmar el ataque.

En el futuro, que ya está llegando, **el malware tradicional en forma de programas concretos claramente maliciosos se ve reemplazado por operativos que no usan malware**, donde el atacante suplanta la identidad de los usuarios de la red y realiza sus operaciones amparado en una cobertura aparentemente legítima.

En este contexto, será imprescindible que las soluciones de seguridad, además de ofrecer la capacidad de implantar estrictos modelos positivos gestionados, proporcionen servicios y plataformas escalables de caza de amenazas.

Panda Adaptive Defense es la primera solución de mercado que ofrece simultáneamente ambas capacidades, un servicio desatendido de Threat Hunting y herramientas en forma de APIs y consolas que permiten a los clientes realizar labores de exploración y reconocimiento de sus redes en busca de atacantes ocultos detrás de las identidades de los usuarios corporativos.



Situaciones Comprometidas.

Han evolucionado. Los objetivos han cambiado, las técnicas se han sofisticado, los vectores de entrada se han multiplicado y las herramientas se diseñan de forma más específica.

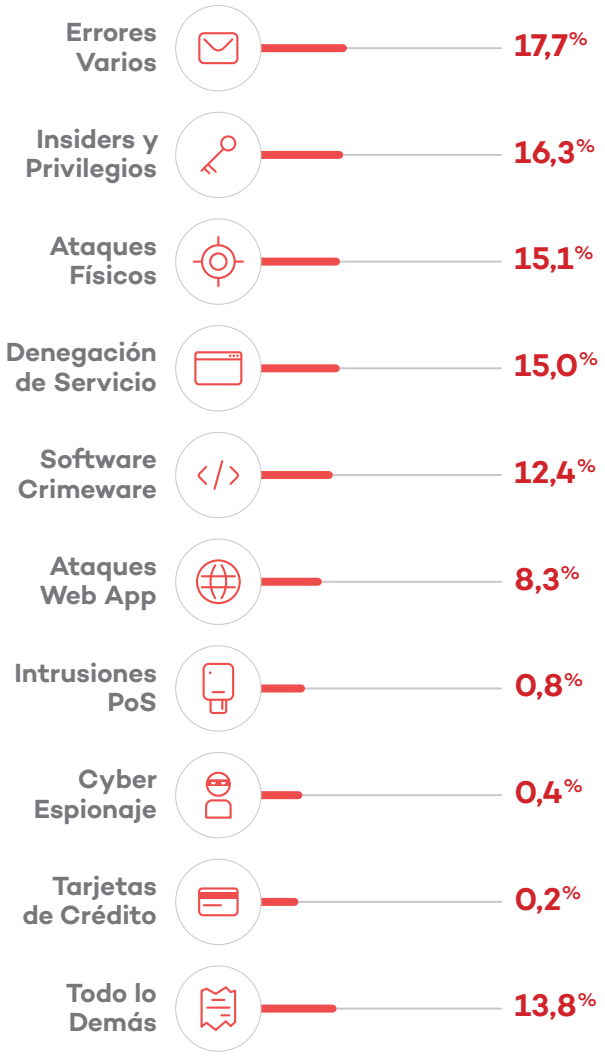
Los atacantes estudian minuciosamente a sus víctimas para adaptar su estrategia de ataque y conseguir provocar el mayor impacto posible. Así, detrás del **62% de las amenazas aparecen hackers que han analizado a sus víctimas** y han adaptado sus ataques cuidadosamente.

- Ataques de Hackers
- Ataques solo con Malware
- Otras técnicas

Eficiencia, eficacia, efectividad y rentabilidad que quedan demostradas por el recuento de hasta 100.000 casos de nuevas brechas e incidentes de seguridad en los entornos corporativos durante el último año.

A lo largo de este informe, hemos comprobado cómo lo hacen y qué han conseguido durante este año. Con todo esto, parecería que ahora es más fácil que nunca ser víctima de un ciberataque. De algún modo así es, pero también los sistemas de prevención, detección, respuesta y remediación son cada vez más eficaces. Combinando, como en el caso de Panda Adaptive Defense, soluciones y servicios para **optimizar la protección, reducir la superficie de ataque y minimizar el impacto de las amenazas**.

Gracias a esta evolución de las técnicas de protección, presentamos una serie de casos en los que Panda Security abortó el ataque a tiempo. Aquí jugaron un papel determinante las investigaciones forenses, que demostraron cómo se cumplen esas nuevas tendencias y técnicas de ataque, y se confirma el estudio de Verizon que establece que **el 95% de los agujeros de seguridad, y el 86% de los incidentes, se enmarcan en solo 9 patrones de acción**.



De esta forma, Panda ayuda también a mejorar los protocolos y estructuras de defensa de las compañías, incluso en aquellos puestos y sistemas que no contaban con la protección directa de Panda Adaptive Defense.

Movimientos Laterales.

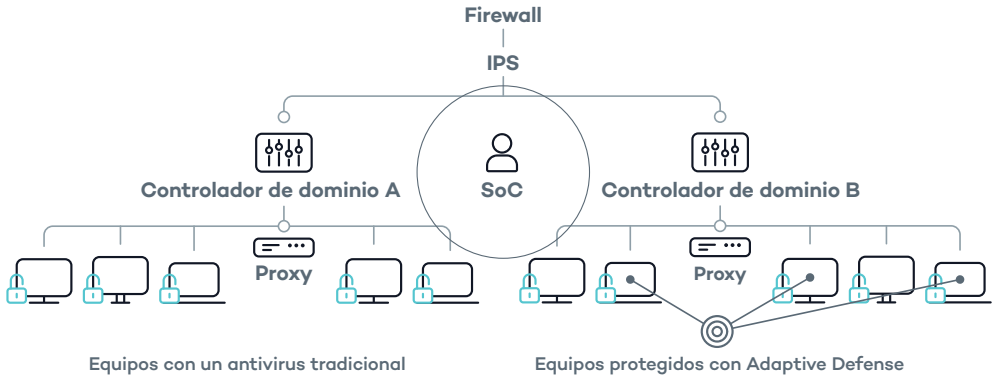
Así, y como muestra de ambas evoluciones, se presenta en primer lugar un ataque oculto con movimientos laterales adaptativos, uno de los tipos de ataque que se está haciendo demasiado común. En esta ocasión la compañía contaba con una batería realmente completa de sistemas de detección y protección (firewall, IPS, SoC, controladores de dominio, proxis, etc.).

Pero ninguna advirtió el movimiento lateral que podría haber supuesto el ataque perfecto contra sus activos.

Los criminales no contaban con que esta empresa disponía de los servicios de Panda Adaptive Defense que descubriría sus intenciones y abortaría su plan de ataque:

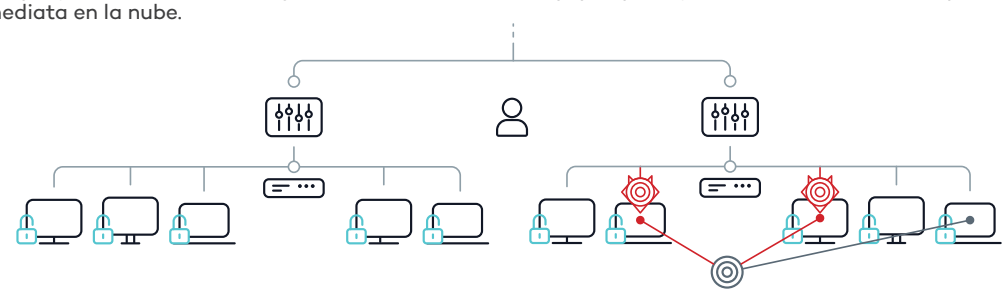
1 Una red aparentemente protegida

Entorno de Gran Cuenta con miles de equipos repartidos en dos dominios, algunos controladores de dominio, firewall, IPS, antivirus y un SoC. El despliegue de Adaptive Defense comienza por unos pocos equipos del dominio B.



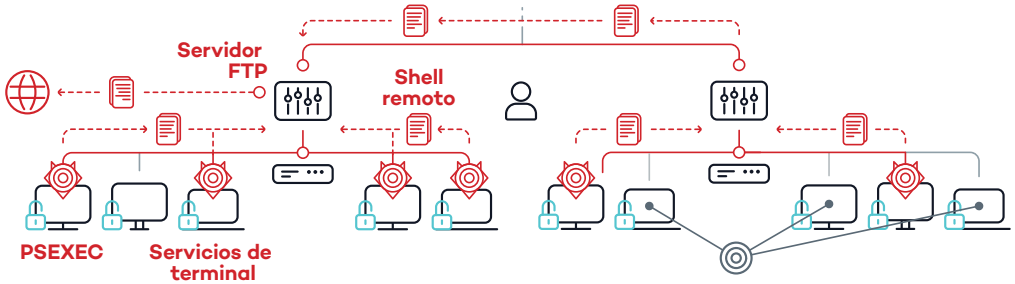
2 Modelo de seguridad de Adaptive Defense

Bloquea los programas no confiables y envía telemetría de los equipos protegidos. Dicha telemetría es procesada de forma inmediata en la nube.



3 Detección de amenazas e investigación

Los Cazadores de Amenazas relacionaron eventos retrospectivos y descubrieron que, detrás de una red que parecía protegida, el dominio A había sido comprometido mediante herramientas administrativas con el fin de obtener y enviar información del perfil de los equipos a sus servidores.



El ataque es descubierto por el Threat Hunting Team

Los movimientos laterales del atacante para hacerse con el control del dominio B fueron descubiertos y remediados por Adaptive Defense antes de que pudieran comprometer los equipos de la red.

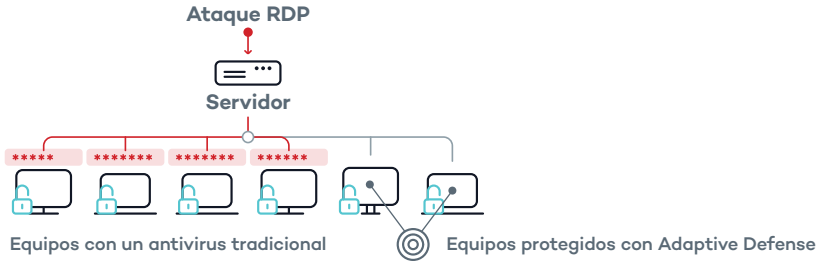
RDP: Ataques sin Malware.

El ataque sin malware se ha convertido en una de las amenazas preferidas por los atacantes. De hecho, apenas un **51% de las brechas de seguridad registrados este año utilizaban algún tipo de malware** como maniobra de ataque. Prefieren permanecer invisibles a las protecciones tradicionales y no necesitar de la interacción humana por parte del atacado y, como en este ejemplo, poder incrementar la rentabilidad al duplicar el efecto del ataque.

Una vez localizadas sus víctimas, desplegaba un **ataque RDP** para monetizar la ofensiva de dos formas distintas: generar tráfico online que se vendía a páginas de terceros, o vendiendo al mejor postor el acceso a las máquinas comprometidas. Casos contemplados con cierta frecuencia y resumidos en esta infografía:

1 Acceso y persistencia

El atacante escanea Internet en busca de víctimas potenciales con el Escritorio Remoto habilitado. Las encuentra, y utiliza un ataque de fuerza bruta para acceder al sistema. Una vez en el sistema, consigue que el ataque sea persistente modificando la entrada del registro correspondiente a la función de Teclas especiales. A partir de ese momento, activar las Teclas especiales (ej. pulsando Bloq Mayús 5 veces), abrirá una puerta trasera en el equipo de la víctima que permitirá al atacante acceder al sistema incluso aunque se cambien las credenciales de Escritorio Remoto.

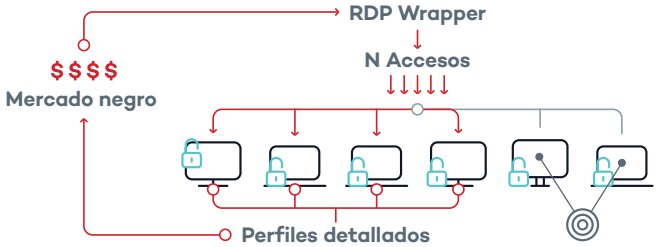


2.1 Monetización de los equipos comprometidos: Generación de tráfico online

El hacker descarga "Traffic Spirit", una aplicación "legal" de generación de tráfico que se utiliza para obtener dinero de los equipos comprometidos. Como vemos, el atacante no utiliza ningún tipo de programa malicioso.

2.2 Monetización de los equipos comprometidos: Venta del acceso a las máquinas

Una vez que los atacantes consiguen acceder a una máquina, obtienen un perfil detallado de todos los equipos de la red. A continuación, venden el acceso a dichas máquinas en el mercado negro para distintos fines (extorsión, robo de información, redes de equipos zombi, bots, etc.).



El ataque es descubierto por el Threat Hunting Team

Descubrimos el ataque gracias a la continua monitorización y a la visibilidad de las actividades en los equipos. Los datos descubiertos por el equipo de Threat Hunting de Panda, revelaron un comportamiento anómalo de los equipos que habían sido comprometidos (cientos de intentos de inicio de sesión en un corto espacio de tiempo).

Extorsión de un Ex-empleado.

A continuación, se revelan algunas de las motivaciones más extendidas para iniciar el ataque contra una empresa: el rencor y la necesidad de revancha.

Y es que, a lo largo de este año, se han visto varios casos de exempleados que intentaron extorsionar a sus antiguas empresas, hasta el punto de que **los ataques iniciados por actores internos ya suponen el 25%** de las amenazas mundiales.

El denominador común de estos casos suele ser la laxitud de las políticas de protección y acceso a los recursos corporativos. **El 81% de los accesos ilícitos tuvieron éxito gracias al robo de contraseñas o a contraseñas poco seguras**.

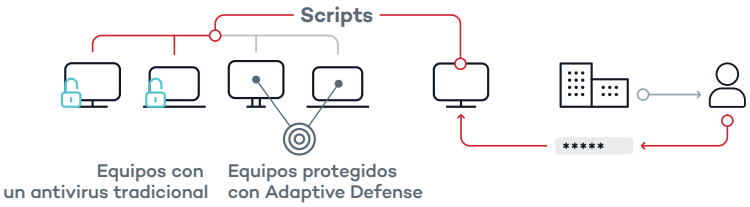
A pesar de ello, una vez dentro, los empleados utilizan estrategias de expansión y control para evadir el resto de sistemas de seguridad y conseguir hacer daño a la compañía, tanto en su reputación como a su economía:

1 El empleado es despedido

Pero no se revocan sus credenciales de acceso, por lo que todavía es capaz de acceder a su equipo de forma remota.

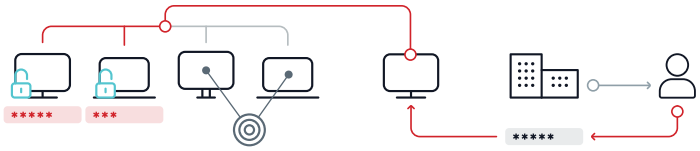
2 Obtención de perfiles detallados

El empleado utiliza varias herramientas del sistema operativo para obtener la lista de equipos conectados a la red. Posteriormente, lanza un script con un comando de Microsoft para descubrir a los usuarios del dominio.



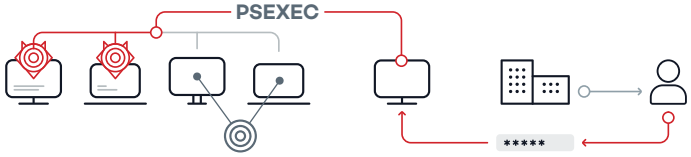
3 Ataques de fuerza bruta

Durante los siguientes días lanza ataques de fuerza bruta y finalmente consigue acceder a varios equipos.



4 Ataque de ransomware

Crea un ejemplar de ransomware que compila el día antes de su despliegue. Desde su antiguo equipo, y tras ejecutar PSEXEC, lanza un script para eliminar todas las copias de seguridad existentes. A continuación, ejecuta el ransomware.



El ataque es descubierto por el Threat Hunting Team

Adaptive Defense bloquea el ataque en todas las máquinas donde está instalado. Tras el primer intento de ataque sobre un equipo protegido con Adaptive Defense, el Threat Hunting Team investiga todos los procesos y comportamientos, descubriendo todos los detalles del ataque así como la identidad del atacante.

Coincidencias.

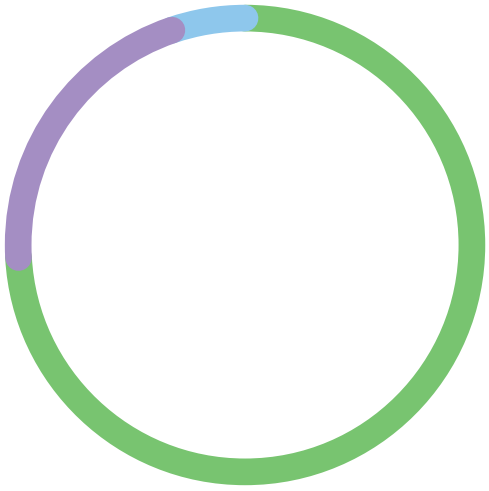
Aun siendo diferentes entre sí, todos estos casos tienen ciertas similitudes:

Un **estudio previo** de las debilidades de la compañía antes al ataque.

La planificación y **adaptación de la ofensiva** a esas debilidades, un acceso sigiloso que no levante sospechas ni alerte a los sistemas de seguridad tradicionales.

Y **movimientos internos** muy estudiados y programados para alcanzar sus objetivos.

Incluso este objetivo suele ser compartido, el dinero. Según Verizon, el **objetivo económico se comparte en el 73% de los ataques**, mientras que el 21% de las motivaciones están relacionadas con el espionaje.



El otro denominador común que comparten estos casos es que todos fueron detectados y abortados por el equipo de Threat Hunting y las soluciones avanzadas de Panda Security.

El Precio de los Ataques.

Hemos visto como la democratización de los ciberataques ha sido facilitada por variables como la profesionalización de los atacantes, la evolución tecnológica, o la facilidad de acceso a los datos.

Aunque algo que, sin duda, ha ayudado a popularizar este tipo de amenazas, es la rentabilidad que suponen sus acciones.

Ciber-armas que se venden a precios muy económicos, y con las que el atacante puede conseguir una suculenta recompensa.

		Desde	Hasta
Herramienta de Ataque	Malware	$50	$200
	Ransomware	$1	$400
	Software	$100	$700
	Pagos y Log-ins	$1	$25
Datos	Información Personal	$3	$150
	Registros de BBDD	$25	
Servicios	Hacking	$100	$300
	Usuarios	$20	$150
	Malware	$1	$25
	Spam	$20	$400
	Documentos Falsos	$15	$25

Fuente: Recorded Future.

GDPR.

El nuevo Reglamento General de Protección de Datos (GDPR) responde a la tendencia alcista de los ciberataques, y a la búsqueda de colaboración entre las entidades públicas y privadas para remediarlo.

A pesar de ser ya una norma vigente, el Reglamento General de Protección de Datos **comenzará a funcionar con toda su fuerza de ley en mayo de 2018**. Las compañías han comenzado una carrera a contrarreloj por ajustar sus prácticas y departamentos a la nueva disposición.

La nueva ley emplaza a las empresas a adecuar sus herramientas y departamentos a unas exigencias mucho más restrictivas y punitivas que obligan, por ejemplo, a informar de cualquier brecha que afecte a datos personales a la Agencia de Protección de Datos bajo pena de **sanciones que pueden alcanzar el 4% de la facturación**.

Las organizaciones también han recibido el imperativo de implantar cifrado y sistemas de doble factor de autentificación en todas las capas de datos. A partir de dicha fecha saldrá caro saltarse las barreras del legislador europeo que, como elemento estrella, introduce también la figura del 'Delegado de Protección de Datos' (DPO, por sus siglas en inglés) si se dan las circunstancias necesarias.

En cualquier caso, la GPDR ha iniciado una carrera entre las empresas españolas, que puede ser a contrarreloj de no comenzar ya a preparar su acogida, por poner coto a uno de los ámbitos que más preocupa a toda firma que ya opera digitalmente: la fuga de datos.

En resumen, el GDPR:

- Establece de forma más precisa cómo tratar los datos de los residentes de la UE, incluso en países de fuera de la Unión.
- Requiere el consentimiento expreso de los residentes en relación con los datos que se recopilarán y claridad respecto al uso que se puede hacer de ellos.
- Define el alcance de lo que son los datos personales para incluir datos de medios sociales, fotos, direcciones de correo electrónico e incluso direcciones IP.
- Aborda la transferencia de datos a través de formatos de archivo abiertos y populares.
- Contempla el «derecho al olvido», que permite eliminar permanentemente o rectificar los datos de una persona a petición.
- Establece que organizaciones de todos los tamaños deben designar responsables de protección de datos, que responderán ante las autoridades de protección de datos.
- Obliga a rediseñar los procesos y los flujos de trabajo para «integrar la privacidad en el diseño».
- Exige que cualquier posible violación de seguridad de los datos se notifique a los pocos días de haberse detectado.
- Contempla sanciones cuantiosas de hasta 20 millones de euros o, si fuera superior, hasta el 4% del volumen de negocios global.

Afectará a empresas con datos personales de ciudadanos de la UE

Obligación de notificar en 72 horas los incidentes sobre datos

Hasta 20.000.000€ en multas por incumplimir la normativa

El DPO se encargará de informar y supervisar el cumplimiento del GDPR

Caso Práctico.

En la gran mayoría de estados de Estados Unidos existen legislaciones que obligan a comunicar las brechas de seguridad a clientes, reguladores y personas afectadas. Por eso es que los casos de brechas de segruidad en empresas estadounidenses dominan los medios de comunicación.

Hasta la entrada en vigor en 2018 del GDPR, en muchos países de la Unión Europea no existe tal obligación.

Para hacerse una idea, basta remitirse a un caso tan impactante como el de **Equifax**, considerado como el mayor hackeo de datos personales sensible de la historia, y que de haberse producido en Europa con la legislación actual, probablemente no se hubiese sabido nada: ni los clientes afectados, ni los reguladores.

De haber ocurrido en Europa, y con el nuevo reglamento en vigor, Equifax se enfrentaría a una demanda por parte de la Unión y de los usuarios afectados. Con una facturación aproximada de $500M netos, **Equifax se enfrentaría a la máxima penalización impuesta por la Unión Europea, €20M**; sin tener en cuenta las compesaciones por daños y perjuicios que se sentenciasen a favor de los afectados.

A partir de la entrada en vigor del GDPR esto va a cambiar, siendo obligado el reporte sobre la incidencia en datos personales, por lo que veremos cómo las publicaciones sobre casos de robo de información en empresas en la Unión Europea se disparan.

Básicamente, la diferencia radica en que, a partir de entonces, nos enteraremos. Porque, en realidad, los casos de robo de información ya están teniendo lugar.

Predicciones.

De los anteriores análisis se desprende que los problemas de ciberseguridad son cada vez más acuciantes, sobre todo en el ámbito empresarial, donde la mayor parte de las organizaciones sufre fugas de datos. Con el agravante de que el intervalo entre una fuga de datos y su detección es cada vez mayor y el método habitual de prevención de pérdidas de datos es cada vez menos eficaz.

Estos son sólo algunos de los problemas acuciantes en seguridad informática en la actualidad pero, **¿cuáles son las amenazas que se presentan para el 2018?** A continuación desvelaremos las predicciones para el mundo de la ciberseguridad en el próximo año.

Ciberguerra y sus Consecuencias.

En lugar de una guerra abierta donde se puede diferenciar cada bando, estamos ante una estrategia de ataques aislados cuyos autores nunca acaban de revelarse claramente.

Freelancers al servicio del mejor postor.

Los principales potencias mundiales ya tienen legiones enteras de cibersoldados, decenas de miles de "combatientes" entrenados con capacidades ofensivas en este terreno. Con el tiempo, algunos de ellos se convertirán en freelancers, ofreciendo su experiencia y capacidades al mejor postor. Las bandas de ciberdelincuentes profesionales podrán encontrar aquí una cantera de profesionales muy bien preparados con acceso a ciber-armas y un conocimiento muy valioso de cara a lanzar ataques. Como consecuencia, **veremos cómo crece la cantidad de ataques avanzados y complejos**.

Operaciones de bandera falsa.

Si hay una característica atractiva para las naciones que llevan a cabo ciberataques es el anonimato que les da Internet. Es cierto que siempre hay sospechas de quién podría estar detrás de un determinado ataque, analizando por ejemplo la víctima y sacando conclusiones sobre quién podría beneficiarse. También averiguando pistas que se hayan podido dejar los atacantes: características en el código malicioso utilizado, servidores a los que se conecta para llevar a cabo sus comunicaciones, etc.

Sin embargo, este anonimato es un arma más en estos ataques: **es muy sencillo llevar a cabo un ataque haciéndolo pasar por un ataque de un tercero** que nada tiene que ver con quien realmente lo está perpetrando. Este tipo de operación de bandera falsa será cada vez más común y averiguar quién está realmente detrás de un ciberataque promovido por una nación será aún más difícil.

Víctimas colaterales.

WannaCry nos mostró en 2017 que hay ataques que están teniendo lugar en el mismo terreno donde las empresas llevan a cabo su día a día: en sus propias redes corporativas, atacando de forma indiscriminada a cualquier víctima vulnerable.

Pero hay también ataques quirúrgicos, donde el objetivo está muy bien definido. Este fue el caso de Petya/GoldenEye, su objetivo claramente eran empresas públicas y privadas de Ucrania. Sin embargo la realidad es que en Internet no existen fronteras, y empresas de decenas de países de todo el mundo se vieron afectadas por este ataque, convirtiéndolas en víctimas colaterales de un conflicto con el que no tenían ninguna relación.

El Enemigo en Casa.

Una de las mayores pesadillas que podemos imaginar es que nos ataquen en un entorno protegido y en el que nos sentimos seguros, como puede ser nuestro hogar. Es una situación para la que no estamos preparados, ya que en primer lugar, confiamos en las personas invitadas a nuestra casa, y segundo, aunque un cuchillo pueda utilizarse como un arma de ataque, todos lo tenemos como utensilio de cocina. Sirva esta analogía para ilustrar al tipo de ataques a los que nos vamos a tener que enfrentar:

Malwareless.

Una de las tendencias que veremos a lo largo de 2018 es cómo aumentará la cantidad de ataques que no utilizan malware (aquellos conocidos como malwareless: sin malware) y mal usan herramientas no maliciosas para llevar a cabo sus ataques. En 2017 hemos visto cómo en el **62% de las brechas de seguridad producidas en empresas se habían utilizado técnicas de hacking** y en la mitad (49%) de estos incidentes no se había utilizado malware.

Aplicaciones comprometidas.

Lo hemos visto en el caso de Petya/Goledenye, donde se comprometieron versiones del software de contabilidad M.E.Doc (y anteriormente a este caso se utilizó la misma vía para infectar a víctimas con ransomware). Otro caso de especial mención es el del CCLeaner, modificado por atacantes desconocidos en lo que parece ser un ataque dirigido a víctimas específicas de grandes empresas tecnológicas.

Dispositivos Móviles.

¿Hasta qué punto debemos preocuparnos por las amenazas en el entorno móvil? En su justa medida. Hay que tener en cuenta que hay más smartphones que ordenadores en el mundo y, sin embargo, la cantidad de ataques a los que se tienen que enfrentar es ínfima comparada con la que tienen que luchar los PCs.

Esto no significa que debamos despreocuparnos por la seguridad de nuestros dispositivos móviles. Seguirán sucediendo ataques, pero parece que Google ha tomado nota de cuáles son los principales problemas y poco a poco está tomando medidas para securizar su sistema operativo (**Android, que cuenta con la mayor cuota de mercado del mundo en el sector móvil**) y para cerrarlo, sin llegar a los extremos de Apple en iOS.

En cualquier caso existen ya millones de amenazas para Android por lo que necesitamos protección que nos proteja toda la información a la que tenemos acceso desde nuestro dispositivo.

Internet of Things.

Es un hecho que el número de dispositivos conectados a Internet no deja de aumentar, pero ¿qué implica de cara a nuestra seguridad? Ya existen redes de bots compuestas de miles de dispositivos IoT, desde cámaras IP a impresoras, que permiten lanzar ataques masivos. Pero este no es el único problema al que deberemos enfrentarnos el próximo año.

En general, los dispositivos IoT no están en el punto de mira de los ciberdelincuentes como objetivo final. Lo que sucede es que estos dispositivos aumentan la superficie de ataque, por lo que utilizarlos como vía de entrada a la red de nuestra empresa va a ser cada vez más frecuente.

Todo por la Pasta.

Ransomware.

Está claro que el principal objetivo de las bandas de delincuentes es el dinero, no hay dudas al respecto. Los ataques de ransomware seguirán siendo muy prevalentes a lo largo de 2018, ya que tienen un retorno de inversión muy alto con un riesgo muy bajo.

Más Ataques, Más Avanzados.

Los ataques serán profesionalizados, sobre todo en aquellos casos en los que el premio (el dinero a obtener) es mayor. Una de las características de Internet y la tecnología digital es que cuando algo tiene éxito enseguida surgen seguidores de estos métodos que tratan de utilizarlo. Y el caso de la ciberdelincuencia no es ninguna excepción. Es por ello que la cantidad de ataques avanzados aumentará de forma notable en 2018. Manteniendo la tendencia de los últimos años, **en 2018 el incremento superará en un 50%** los ataques sufridos durante este año.

El Año de los Ataques a Empresas.

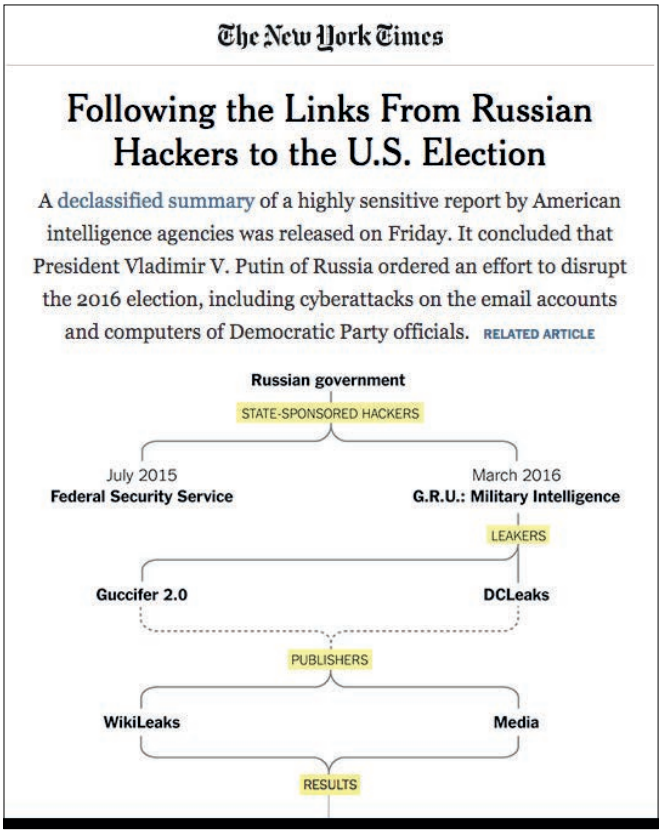
Es cierto que ya hemos vivido grandes ataques en el pasado, con robo de información de todo tipo y en números enormes. Todos recordamos el caso de la intrusión en Yahoo con el robo de cientos de millones de credenciales, o por irnos a casos más cercanos en el tiempo tenemos los casos de Sabre o Equifax que hemos tratado en este informe. ¿Por qué motivo entonces creemos que 2018 va a ser el año de los ataques a empresas? La respuesta viene en forma de siglas: **GDPR.**

Esto no significa que en 2018 las empresas vayan a ser más atacadas, sino que por primera vez el público será consciente de los ataques que se producen y que en muchos casos se esconden.

Redes Sociales y Propaganda.

Nunca en la historia el ser humano había tenido acceso a tanta información. Irónicamente, nunca ha sido tan complicado encontrar información veraz como lo es ahora.

Las redes sociales no dejan de ser herramientas donde podemos intercambiar información, y al ser utilizadas por miles de millones de personas son un objetivo claro de quienes quieren influir en la opinión pública tomando, en cierta forma, el papel que en el pasado tenía la prensa. Hemos sabido que el mismo Presidente **Obama avisó personalmente a Mark Zuckerberg**, fundador y CEO de Facebook para que la red social se tomara muy en serio la amenaza que supone la propagación de noticias falsas en el ámbito de las elecciones a la presidencia de EEUU.



Facebook, está tomando ya cartas en el asunto. Si una página de Facebook distribuye repetidamente noticias falsas, será bloqueada. Además han publicado anuncios en su red y en medios de comunicación dando consejos a los lectores para que puedan identificar noticias falsas. También están cambiado su política en lo que respecta a publicidad relativa a campañas electorales, para que ésta sea lo más trasparente posible.

Criptomonedas.

El uso del bitcoin y demás criptomonedas se utilizan cada vez más como medio de pago digital. Si bien es cierto que existe mucha especulación, cada vez hay más comercios que aceptan pagos en estas monedas. Otro de los motivos del éxito de estas monedas es que los ciberdelincuentes hacen un uso extensivo de las mismas, ya que les permite mover de forma sencilla y anónima grandes cantidades de dinero.

Un ejemplo claro lo vemos en el ransomware, ya que la práctica totalidad de estos ataques piden el rescate para recuperar la información en bitcoins.

El uso de las criptomonedas seguirá creciendo, y también crecerá de forma notable toda la ciberdelincuencia que lo rodea:

- Infecciones de equipos con software de minería de criptomonedas.
- Infecciones de páginas web para convertir en mineros a todos los visitantes.
- Robos a empresas de cambio de criptomonedas.
- Robos de wallets de usuarios.

Conclusiones.

Después de ver los ataques que han golpeado empresas e instituciones de medio mundo este, es importante saber cómo podemos salvaguardar nuestra privacidad y seguridad en Internet.

Las actualizaciones de seguridad deberían formar parte de un proceso prioritario dentro de todas las empresas. Cada día que pasa sin parchearse un sistema vulnerable está en riesgo tanto la reputación de la compañía, como la integridad de la información propia, de clientes y proveedores. Incluso la producción puede ponerse en peligro e incurrir en pérdidas millonarias. Un ejemplo: el grupo AP Moller-Maersk fue una de las víctimas del ataque de GoldenEye/NotPetya, y calcula que las pérdidas sufridas están entre los 200 y 300 millones de dólares.

Los países están invirtiendo cada vez más en capacidades defensivas y ofensivas, con el punto de mira en infraestructuras críticas. Poder lanzar un ataque de forma remota que cause un apagón no es una teoría: ya ha sucedido en Ucrania y podría repetirse en cualquier país del mundo. El conocimiento de diferentes las herramientas utilizadas para perpetrar estos ataques hace cada vez más viable que grupos con financiación más limitada que aquellos patrocinados por estados puedan llevar a cabo acciones similares contra objetivos concretos. Grupos terroristas, como el ISIS, están claramente dispuestos a utilizar todos los medios a su disposición para causar terror.

2018 dibuja un entorno más peligroso, lo que obliga a **implantar un cambio de mentalidad y estrategia para conseguir las mayores cotas de seguridad** y proteger los activos en la red. Ir en busca de malware sólo protege parcialmente. Cualquier proceso nuevo que quiera ejecutarse en cualquier dispositivo conectado a la red deberá ser previamente aprobado, y aquellos en los que confiamos tendrán que ser vigilados de cerca para poder detectar cualquier comportamiento anómalo en el menor periodo de tiempo posible.

Tanto en el ámbito empresarial como particular, la **formación y concienciación son aspectos clave** en estos momentos para mejorar la situación en lo que a ciberseguridad se refiere. De cara a las empresas esto lleva a plantear la necesidad de una mayor inversión en los puntos críticos de ciberseguridad.

El conocimiento de los ataques debe ser la base para establecer las defensas apropiadas. Una **seguridad basada en la detección y respuesta en tiempo real**, que aporte un informe forense y al detalle de cómo se ha producido el ataque, es fundamental para evitar futuras intromisiones. Las reseñas dejadas en el **Gartner Peer Insights** avalan en esta línea la solución Panda Adaptive Defense, a la cabeza de las soluciones EDR contando con el mayor número de análisis de todo el mercado.

Los ficheros de firmas ya no sirven y las cifras hablan por sí mismas: más del 99% de todo el malware no vuelve a aparecer nunca más en ningún otro lugar. Añadir firmas para su detección es ya una labor insuficiente e ineficiente. La mayoría de las compañías de seguridad las añaden simplemente por si más adelante algún laboratorio de pruebas decide hacer una prueba de detección de malware por firmas (algo cada vez menos común), o para aquellos que creen que esos resultados se traducen en si un producto puede detectar una amenaza, o no.

Hay un problema de enfoque: aquellas **soluciones que siguen centradas en luchar contra el malware, están condenadas a extinguirse** si no cambian de estrategia, y estas son la mayoría de las que se encuentran disponibles en el mercado. La cantidad de ataques malwareless, sigue creciendo. Y ante esta realidad se ven completamente perdidos e indefensos, tanto ellos como sus clientes.

Y por supuesto, no podemos olvidar la **cooperación internacional** y la creación de un marco legislativo común, como será el GDPR; como algunos de los aspectos clave de una estrategia de ciberseguridad. La existencia de un plan de acción y el respaldo político y económico permitirá hacer uso de los últimos avances tecnológicos de la manera más segura.

Porque, al fin y al cabo, de lo que se trata de es de seguir **reinventado la ciberseguridad**.

panda

pandalabs