Noviembre, 2018

Informe Anual PandaLabs 2018

panda

pandalabs

Introducción:
El estado de la Ciberseguridad

El estado de la Ciberseguridad

2017 fue el año en el que la palabra ransomware dejó de estar reservada solo para especialistas en ciberseguridad y departamentos TI. La enorme relevancia mediática que adquirieron ataques como WannaCry o Petya/GoldenEye convirtieron a este tipo de amenaza en una de las principales tendencias del pasado año a nivel empresarial. Sin embargo, como saben los profesionales del sector, los eventos altamente publicitados nunca deben servir como indicación del riesgo ni influir en una decisión relacionada con la seguridad.

En este informe anual de 2018 desde PandaLabs, el laboratorio anti-malware de Panda Security, hemos revisado los datos de amenazas recopiladas en el laboratorio a partir de nuestras fuentes de sensores. Incluimos datos de las soluciones de seguridad para endpoints implementadas en los dispositivos de nuestros clientes, las tendencias observadas por nuestros analistas mientras proporcionaban servicios de clasificación de ficheros y búsqueda de amenazas; así como los incidentes de ciberseguridad más relevantes reportados a nivel mundial.

Y la información recopilada este 2018 sigue reflejando la prevalencia de los ataques de malware, con 9 millones de URLs maliciosas y 2,4 millones de ataques prevenidos por millón de endpoints, por mes. El 20,7% de las máquinas objeto de estudio recibió al menos un ataque de malware durante el periodo analizado.

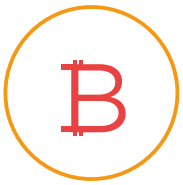
Pandalabs constata que las amenazas de malware basadas en ficheros no son un problema para Panda Security con niveles de infección tendientes a 0.

Esto se debe a la adopción del modelo de clasificación al 100% de todos los procesos de malware ejecutables en los sistemas, que permite bloquear cualquier programa desconocido para Panda, hasta que sea clasificado. Como contrapartida, los cibercriminales evolucionan hacia ataques más insidiosos, abusando de herramientas de software existentes, una vez que consiguen infiltrarse en la red. Esto nos lleva a pensar que este tipo de ataque se incremente en el futuro.

Tipos de ataque contra empresas más exitosos en 2018:

Prevalencia de ataques de malware

Ataques al protocolo RDP

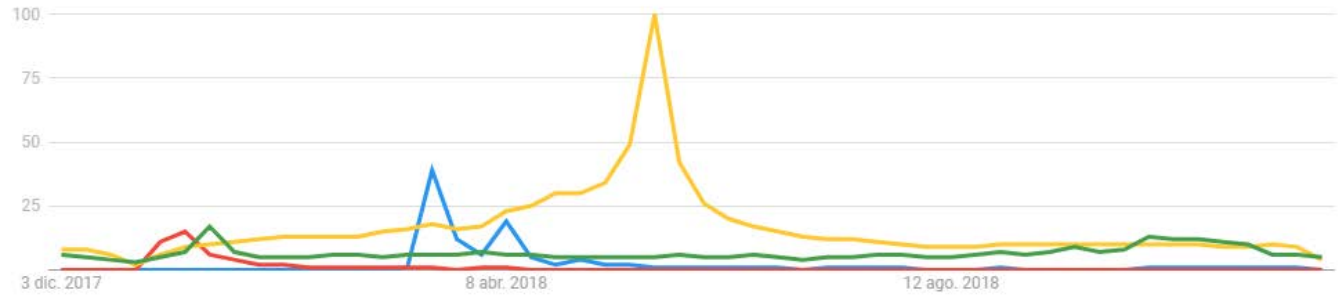


Boom del Cryptojacking y Ransomware As a Service

Y mientras las técnicas tradicionales –phishing, ransomware, o el compromiso de cuentas de correo empresariales- parecen ser tan fructíferas como siempre, el auge de los ataques al protocolo **RDP**- combinado con otras técnicas de ingeniería social- se consolida como vector de entrada para los atacantes. Si a esto le sumamos el boom de este año en torno al **Cryptojacking y el Ransomware As a Service, tenemos los tres principales tipos de ataque que han vulnerado con éxito las redes de las empresas durante 2018.**

El objetivo principal de los atacantes sigue siendo el endpoint. Ahí es donde encuentran la información más sensible, y donde comprometen los credenciales que les permiten ir realizando movimientos laterales y atacando otras redes y sistemas. internamente de un sistema a otro.

Sin embargo, el presupuesto de seguridad destinado a proteger el endpoint es aproximadamente un tercio del destinado a la seguridad de la red. -Fuente: Gartner- **No es de extrañar por tanto que la mayor parte de los endpoints corporativos sigan protegidos por tecnologías "tradicionales", no adecuadas a los retos de la ciberseguridad de hoy en día.** Tampoco resulta sorprendente el éxito de muchos atacantes, que tardan mucho menos tiempo de media en comprometer los sistemas que en ser descubiertos. Esta asimetría y falta de equilibrio, junto a la escasez crónica de profesionales en el sector, seguirán constituyendo un año más los principales desafíos para las organizaciones en materia de ciberseguridad.



Google trends:

GDPR
Cambridge Analytica
Meltdown y Spectre

Esta figura sirve para reafirmar que probablemente GDPR haya sido el tópico de más interés este año en cuanto a volumen de búsquedas.

PandaLabs:
Datos de amenazas en 2018

Datos de amenazas en 2018

Las soluciones para endpoint de Panda Security integran múltiples capas de tecnologías y servicios diseñados para proteger contra el malware de distintos tipos (basado en ficheros), pero también contra ataques en memoria, por medio de exploits o técnicas *fileless*. Muchos ataques combinan *varias técnicas* para maximizar las posibilidades de éxito y, a la vez, minimizar los costes para los atacantes.

En este informe, presentaremos los datos de amenazas correspondientes a las capas de protección más significativas, según informa nuestra base de productos corporativos basados en endpoints, y que son: firmas (específicas y genéricas), heurística, análisis basado en comportamiento/contexto, en memoria, anti-exploit y servicios 100% Attestation y Threat Hunting & Investigation. Estas capas de protección se ofrecen tanto a nivel local como desde la nube. La figura 1 representa el conjunto de técnicas utilizadas según el método de ataque.

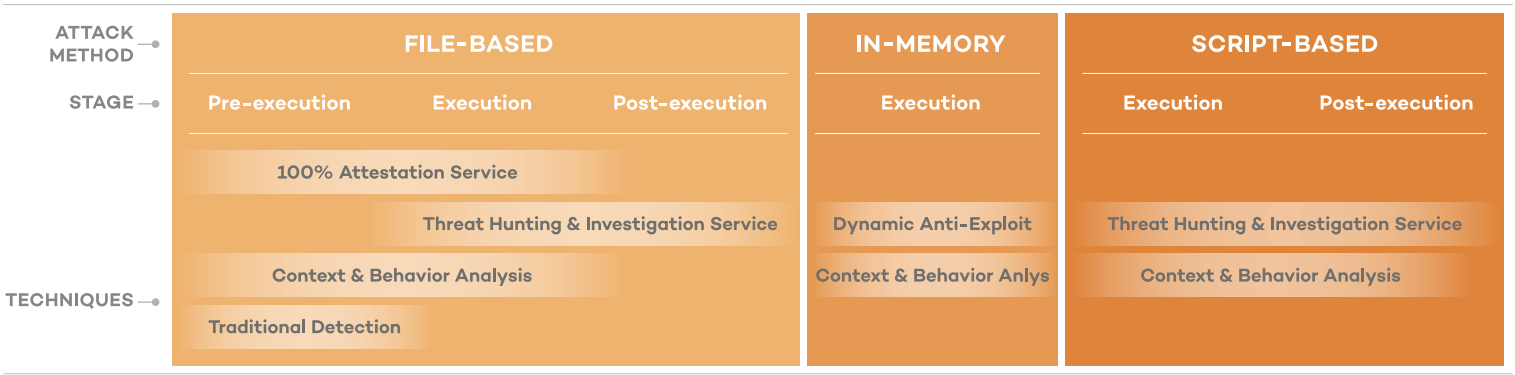


Figura 1.: Tecnologías de protección, métodos y fase de ataque.

Detecciones

La mayoría del malware que se detecta en los endpoints protegidos en las empresas se identifica a través de las firmas y la heurística. Sin embargo, se evita que la mayoría del malware llegue a ejecutarse en el endpoint porque los emails de phishing y las URL relacionadas con el malware, los vectores de entrada más comunes, los tenemos muy controlados en Panda Security. Mientras **la cantidad total de ficheros de malware que llegan al endpoint sigue creciendo constantemente (más del 60% del principio al final del periodo), el riesgo que suponen para nuestros clientes las amenazas basadas en ficheros ha disminuido** de manera significativa, hasta alcanzar niveles marginales. Esto es debido a la eficacia de las capacidades integradas a través de productos y servicios, y en particular debido al enfoque «100% atestación» de Panda Security, lo cual previene por defecto la ejecución de ejecutables desconocidos hasta que PandaLabs los clasifique.

De promedio, se detectaron **más de 2,4 millones de ficheros de malware y más de 9 millones de URLs de malware bloqueadas cada mes, por millón de endpoints**. La mayoría de ellos se vieron sólo una vez.

Analizando el malware, los vectores de ataque y códigos maliciosos en auge durante el 2018 vemos que la prevalencia de las categorías de malware detectadas en esta etapa no ha cambiado mucho en el último año. **Troyanos y ransomware representan la mayoría de estas amenazas**. Relativo a esto, **el bloqueo de URL relacionados con malware** (a través de interacciones directas en webs o a través de URL incrustados en emails) ocurre con una **frecuencia 3,7 veces más alta** que las detecciones de ficheros de malware, lo cual **representa el vector de entrada más significativo para amenazas al endpoint**, junto con los ataques de fuerza bruta como los predichos a principio de año contra RDP.

2,4 MILLONES — Ficheros de malware

URLs de Malware bloqueadas cada mes por millón de endpoints , por mes — **9 MILLONES**

Creemos que la **conexión RDP con acceso a Internet representa una amenaza creciente** para muchas organizaciones que no son conscientes de que están expuestos. Ser víctimas de esta técnica de ataque supone ser continuamente escaneados por los cibercriminales que buscan oportunidades fáciles para infiltrarse en las redes de la empresa. Los datos registrados en el laboratorio corroboran que aproximadamente **el 40% de nuestros clientes medianos y grandes son sujetos a este tipo de ataque contra RDP todos los meses.**

En cuanto a vectores de entrada y códigos maliciosos más comunes en este año que finaliza, corroborar que **el email sigue siendo uno de los vectores más popular para campañas de ataque**, aunque muchos de ellos acaban en la carpeta de spam antes de llegar al endpoint. Los usuarios, especialmente al usar dispositivos móviles, están más expuestos a URLs maliciosas o webs infectadas.

En este contexto, **las webs infectadas con código de CoinHive son una amenaza cada vez más generalizada**, como forma menos agresiva de minar criptomonedas. CoinHive, inicialmente diseñado para permitir a los propietarios de las webs el hecho de generar ganancias extra sin recurrir a anuncios, se ha posicionado a lo largo del año como la principal amenaza, con su código instalado sin el conocimiento de los propietarios en las webs hackeadas. La minería de criptomonedas no autorizada agota los ciclos de CPU y la energía de los dispositivos durante todo el tiempo que el usuario visite la web infectada. De hecho, **la minería de criptomonedas ha tenido un crecimiento de 3,5 veces más en comparación con el mismo periodo del año pasado**, mientras el ransomware todavía creció 2,5 veces en el mismo periodo. En 2018, los mineros de Monero representan casi el 70% del número total de mineros de criptomonedas identificados.

Clasificaciones previas a ejecuciones.

Ya que nuevos tipos de malware se crean y se publican más rápidamente de lo que se añaden maneras de detectarlos, siempre existe un gap de detección. Esto genera **infecciones inevitables de algunos usuarios «paciente-cero» que no cuentan con una protección más robusta** o completa.

Para poder cerrar ese gap y minimizar el riesgo de infección para sus clientes, Panda Security introdujo en 2015 el servicio "100% Attestation", el cual asegura que todos los procesos que se ejecutan en los endpoints deben ser clasificados como confiables por PandaLabs antes de que se permita su ejecución. Este servicio de seguridad actúa como la última línea de defensa contra el malware basado en ficheros.

En el periodo de enero-noviembre, un promedio mensual de 5,8 millones de ficheros ejecutables distintos fueron observados por millón de endpoints. Mientras la mayoría de los ficheros se repiten de un mes a otro, aproximadamente un 20% de ellos cada mes eran desconocidos la primera vez que intentaron ejecutarse. Dichos ficheros fueron clasificados automáticamente casi al 100% (99,98%), y de ellos, un promedio de 1,3% fueron clasificados como malware.

PandaLabs Identificó

5,8 MILLONES al Mes

De ficheros ejecutables

Por millón de endpoints

La detección de ataques mediante el análisis del contexto y de comportamiento

El módulo de análisis de comportamiento, que bloquea acciones según el contexto de ejecución, es capaz de reconocer cientos de combinaciones de procesos, relaciones entre estos, acciones, etc...; que son indicativos de los ataques de fase temprana de distintos tipos (ransomware, mineros, ataques basados en script, entre otros). Paradójicamente, debido a la prevención temprana de la amenaza, es imposible que determinemos la naturaleza final de la amenaza, dado que **los atacantes también podrían usar una combinación de técnicas dentro del mismo ataque**. La introducción de estas técnicas preventivas representó un éxito importante en la lucha contra las amenazas peligrosas para nuestros clientes, como el ransomware.

Durante el periodo observado, **el módulo de análisis previno más de 15 mil acciones maliciosas** (ej., una secuencia de eventos indicativa de un ataque en su fase temprana). **por cada millón de endpoints, por mes** El abuso de PowerShell para ataques filess (ya están dentro cuando usan powesell) en el sistema fue clasificado como la principal técnica, representando casi más de un 26% % de estos bloqueos.

Detección de exploits en memoria.

Los ataques «en memoria», que se aprovechan de las vulnerabilidades en aplicaciones en ejecución, se detectan mediante un **módulo anti-exploit** dinámico e integrado. Este módulo **detectó de media más de 8.100 intentos de explotación durante el periodo analizado, por millón de endpoints, por mes. Internet Explorer, Outlook fueron las aplicaciones que más ataques sufrieron.**

PandaLabs Detectó

Por millón de endpoints

El módulo de análisis de contexto y de comportamiento bloquearon

De Acciones Maliciosas

Por millón de endpoints

Búsqueda proactiva de amenazas o Threat Hunting.

Los ataques que buscan abusar de herramientas legítimas ya presentes en el entorno, y que pueden ser utilizadas con fines maliciosos, como herramientas administrativas para la gestión de sistemas,representan una de las amenazas más importantes a día de hoy. La capacidad aumentada de cibercrimen de grupos o estados que utilizan hacking en vivo, técnicas malwareless, y la dificultad (o más bien, la imposibilidad) de detectar estas infiltraciones con medios convencionales nos hace creer que estos ataques se convertirán en el principal reto para los departamentos de seguridad informática.

Una falta de profesionales de seguridad cualificados agrava el problema. Según ciertos cálculos, -Cybersecurity Jobs Report 2018-2021, de Cybersecurity Ventures- habrá un déficit de 3,5 millones de trabajos para 2021. Creemos que es el reto más importante en la ciberseguridad hoy en día.

El Servicio de Threat Hunting and Investigation de Panda Security, como componente integrado de las soluciones de Panda Adaptive Defense, **tiene como objetivo identificar estos ataques**. El servicio, proporcionado por el equipo de expertos de PandaLabs, depende de sus propias herramientas para crear y, retrospectivamente, probar y validar las hipótesis contra toda la actividad que se monitoriza en toda la base instalada, para investigar potenciales incidentes y para ayudar a clientes a remediar incidentes confirmados.

En el periodo analizado, se confirmaron y se investigaron aproximadamente **90 incidentes**.

Casos investigados

Caso #1. Compañía de servicios grande

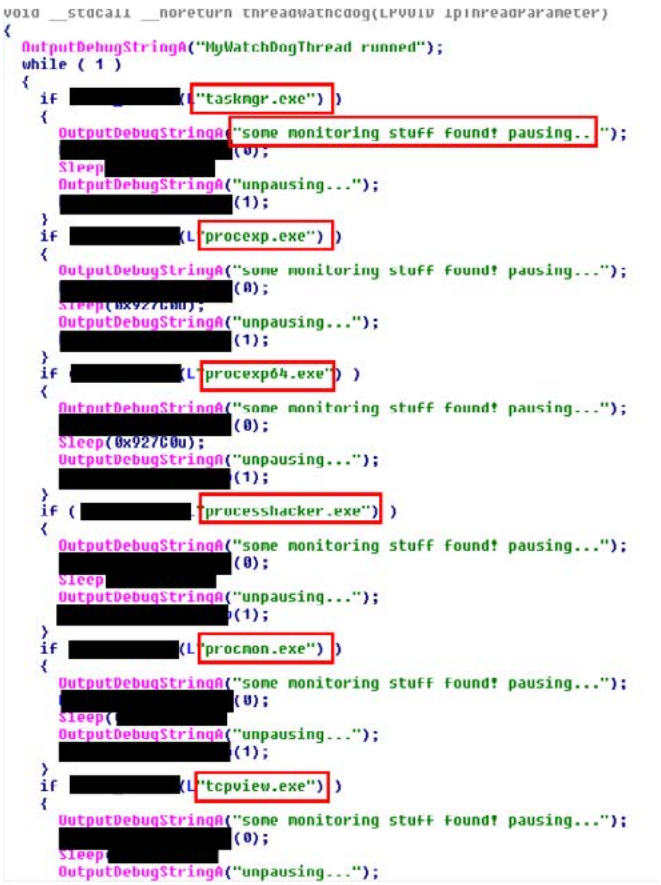
Se detectaron Conexiones salientes hacia China sospechosas en un sistema no protegido por Panda, utilizando telemetría de sistemas protegidos. Las investigaciones llevaron a la neutralización de un troyano dirigido, diseñado para exfiltrar datos sensibles. El troyano «se compiló/auto-compiló» más de 100 veces, creando variantes de sí mismo para intentar, sin éxito, evitar ser bloqueado.

Caso #2. Múltiples clientes.

Un usuario recibió un correo dirigido con un documento Word, utilizado para lanzar un script que, a su vez, llamó a PowerShell para que descargara una herramienta de red legítima (socat.exe) y Tor. La herramienta de conectividad se utilizaba para crear un relay con Tor utilizando puertos locales para esconderla de las herramientas de monitorización de red. Se ha informado de esta técnica antes, en relación con troyanos de banca.

Caso #3 Cliente del mercado medio

La vulnerabilidad EternalBlue se utilizó para ejecutar un fichero directamente en memoria, incluido un código para conectarse a un servidor C&C y para recopilar información sobre el sistema (versión del OS, productos de seguridad instalados, etc.), y robar las contraseñas de los usuarios. El bot dirigido también intentó añadir su propia ubicación a las exclusiones en Windows Defender para evitar ser detectado, e incluyó su propia implementación del protocolo Tor. En una instancia, el bot descargó e instaló un driver, un rootkit «Necurs» con una funcionalidad para deshabilitar numerosos productos de seguridad y para buscar la presencia de herramientas para la monitorización de procesos, y para parar su actividad para evitar ser detectado. En este caso, el bot también descargó y ejecutó un cryptominer de XMRIG modificado, como servicio, sin tocar el disco.

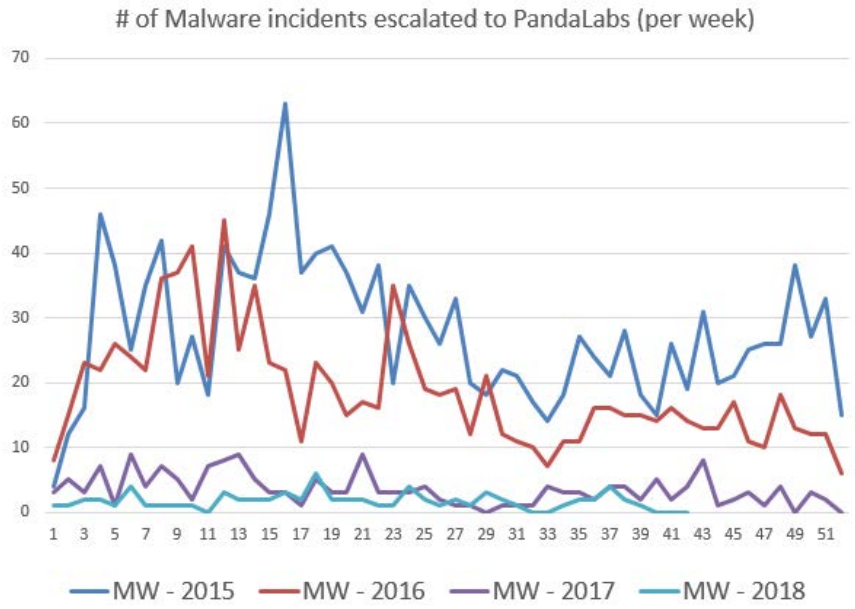


El driver detecta la presencia de programas de seguridad y de herramientas de monitorización de procesos, para pausar su actividad.

Incidentes Escalados

La misión de Panda Security es mantener a sus clientes libres de amenazas de seguridad. Toda la información anterior acerca de amenazas, técnicas, tecnologías y servicios no tendría sentido si, al final, nuestros clientes no pudieran proteger sus activos informáticos, y se convirtieran en presa para los atacantes. Así pues, como métrica crítica para medir nuestro éxito en la lucha contras los ciberataques, incluimos el número de incidentes escalados a PandaLabs por clientes, y su evolución en los últimos 4 años. La siguiente figura muestra el número de tickets escalados cada semana, para 2016, 2017 y 2018 para todos los productos, tanto de corporativo como de consumo.

Como podemos ver, **en 2018 el número de incidentes escalados por infecciones de malware tienden a cero**. La clasificación de todos los ficheros ejecutables, la visibilidad de todos los programas en ejecución, la eficacia del análisis de comportamiento en tiempo real al ejecutar aplicaciones autorizadas y los servicios continuos de Threat Hunting proporcionados por el laboratorio, han contribuido a esta situación de tendencia hacia 0 infecciones en clientes.



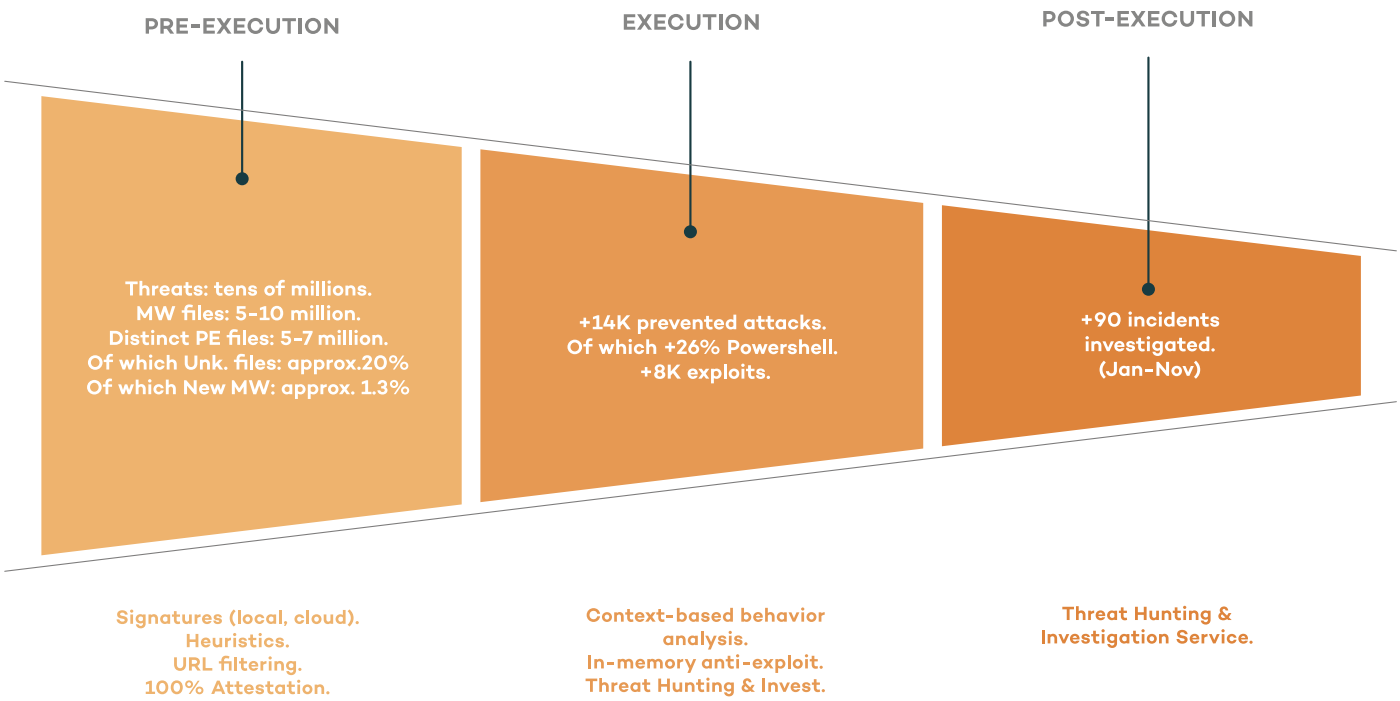
El «Embudo de mitigación de amenazas»

Las amenazas que se dirigían hacia el endpoint pueden ser caracterizadas por su categoría o su tipo (ransomware, cryptominer, troyano, fileless, etc...; aunque muchos ataques utilizan una combinación de técnicas), pero también según el nivel de sofisticación o personalización del ataque. **Proteger contra ataques altamente sofisticados o personalizados requiere un nivel más alto de madurez de las capacidades de protección del endpoint**. Aunque la medida de mitigación más eficaz que puede tomar cualquier organización es parchear, no esperamos cambios significativos en la velocidad media con la que las organizaciones despliegan incluso los parches más críticos, debido a restricciones de tiempo o de recursos, y debido también a los inconvenientes y a la oposición de los usuarios.

No obstante, **las amenazas de hoy en día pueden mitigarse en gran medida con el uso de protección avanzada de nueva generación endpoint de próxima generación**. Los datos muestran que utilizar «un enfoque basado en la clasificación al 100% de las aplicaciones desconocidas, o que no son confiables, que llegan al endpoint, junto con un servicio manejado que resuelve rápidamente su clasificación, puede reducir el riesgo de malware basado en ficheros a niveles marginales, con una transparencia absoluta y conveniencia para los administradores y los usuarios.

La gráfica de debajo representa la mitigación de las amenazas observadas en el conjunto de endpoints analizado, mientras la tecnología y las capas de servicio filtran las amenazas caracterizadas por su nivel de sofisticación o de personalización.

«Embudo de mitigación de amenazas»



Ciber-noticias de 2018:
mes a mes

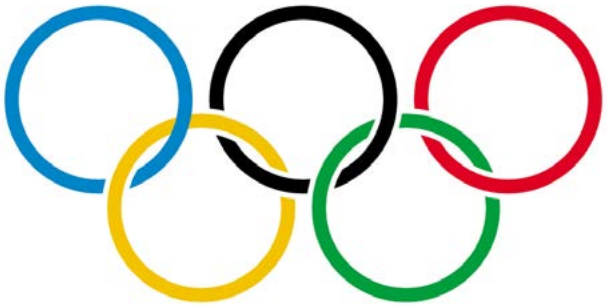
Enero

Vulnerabilidades Meltdown y Spectre

El año empezó con un gran susto: el anuncio de las vulnerabilidades «catastróficas», **Meltdown y Spectre** (CVE-2017-5754), afectando a la mayoría de los microprocesadores modernos. No entraremos en los aspectos técnicos ya que hay mucha información disponible sobre este aspecto. Sencillamente diremos que podemos respirar tranquilos ya que, hasta el momento, no hemos visto ningún ataque real, y sus efectos se han limitado a unos problemas de rendimiento que puedes consultar **aquí**. Existen **herramientas gratuitas** para que los usuarios comprueben si sus sistemas están protegidos contra estas vulnerabilidades.

Ciberataque en los Juegos Olímpicos

Durante la ceremonia de inauguración de los Juegos Olímpicos de Invierno en Corea del Sur, **hubo un ciberataque** que afectó la conexión de Internet, el servicio de televisión y la web de los juegos. Aunque inicialmente se culpó a Coreo del Norte por el ataque, más tarde los servicios de inteligencia de Estados Unidos **atribuyeron el ataque a agentes rusos**.



Febrero

Foro de cibercrimen, «Infraud» eliminado de Internet

El Departamento de Justicia estadounidense imputó a 36 personas y arrestó a 13 en relación con la eliminación del foro de cibercrimen, **«Infraud»**. El grupo fue responsable de la pérdida de más de 530 millones de dólares de consumidores. Bajo el lema «*In Fraud We Tust*» (En el fraude confiamos), la organización lideraba un foro de negocios ilegales para sus 11.000 miembros, comerciando con identidades robadas, tarjetas de crédito y de débito comprometidas, información personalmente identificable, información financiera y bancaria, malware, y otro contrabando. Puedes ampliar **aquí** la información.

Marzo

El creador de los malware «Cobalt» y «Carbanak», detenido en España

De especial importancia fue el arresto de un ciudadano ucraniano en España en el mes de marzo. Según **la noticia,** se cree que es el autor de los malware Carbanak y Cobalt. El ciberdelincuente y sus socios infectaron a más de 100 bancos con los malware, que fueron utilizados para hackear cajeros automáticos de manera remota, robando más de mil millones de dólares en menos de un año, según los organismos policiales responsables de su arresto.

Se descubren backdoors en sistemas utilizados por el gobierno británico

En marzo, investigadores descubrieron **múltiples backdoors** en los sistemas de un contratista del gobierno británico que se diseñaron para robar datos militares y del gobierno. Este ataque está vinculado al grupo APT15, Se sospecha que el grupo usó la herramienta Mimikatz para obtener credenciales de los administradores del sistema.

Abril

CoinHive surge como una de las principales amenazas

El *cryptojacking* consiste en el uso no autorizado de los dispositivos de un usuario para minar criptomonedas. Básicamente, los atacantes hacen uso del malware para secuestrar esos ordenadores, tablets o smartphones, y aprovechan parte de su poder de procesamiento para minar criptomonedas de manera encubierta. Una de las técnicas más comunes consiste en apropiarse de la CPU o GPU de la víctima desde una página web infectada con malware para minar criptomonedas, como ha ocurrido recientemente con YouTube. En este caso, la plataforma de anuncios DoubleClick fue la víctima de un ataque que ocultaba en el código de los anuncios de YouTube el script de *cryptojacking* Coinhive. Precisamente, Coinhive es el script más utilizado para desarrollar estos ataques. Un estudio del investigador de seguridad Troy Mursch ha detectado 50.000 nuevos sitios web infectados con scripts de *cryptojacking, con un 80%* de ellos recurriendo a Coinhive.

Mayo

VPNFilter – Un ataque patrocinado por un estado sobre routers SOHO

El FBI y el Departamento de Justicia de Estados Unidos anunciaron **«acciones»** para interrumpir el botnet VPNFilter que afectaba a cientos de miles de routers domésticos de múltiples fabricantes. Se cree que un grupo de actores patrocinados por un estado controla el botnet. Se descubrió más tarde que el malware tiene la capacidad de entregar exploits a endpoints a través de una capacidad de «intermediario». Puedes ampliar **aquí** la información.

GDPR y algunas consecuencias imprevistas

En mayo el muy esperado Reglamento General de Protección de Datos (**GDPR**) entró en vigor. Tal vez el efecto más evidente para los usuarios, mientras se asentaba el polvo, fue la marea de mensajes con la petición de consentimiento; algo de que los cibercriminales se aprovecharon para lanzar **compañas de phishing.**

Otra consecuencia inesperada del nuevo reglamento europeo fue la restricción de los esfuerzos de la investigación de seguridad para los que utilizaban WHOIS, el sistema utilizado para consultar los datos de registro de nombres de domino y el rango de las direcciones IP. La Corporación de Internet para la Asignación de Nombres y Números (ICANN), la organización que supervisa y gestiona el sistema de los nombres de dominio, propuso borrar cierta información clave de los registros públicos para cumplir con el GDPR y de este modo limitar los esfuerzos de los investigadores de seguridad. En junio, ICANN publicó una propuesta: ofrecer el acceso a todos los datos de WHOIS para propósitos legítimos, como acciones de organismos policiales, y, a la vez, tener una protección adecuada para datos personales según el GDPR. ICANN está ahora buscando respuestas acerca de la propuesta.

Business Process Compromises en México y Chile

También en mayo, unos ciberataques contra algunas instituciones financieras pasaron desapercibidos para muchas organizaciones de seguridad. En México, unos cibercriminales atacaron las aplicaciones y la infraestructura utilizada por varios bancos para conectarse al Sistema de Pagos Electrónicos Interbancario, SPEI, y pudieron transferir de manera ilícita más de 400 millones de pesos (aprox. 18 millones de euros). Unos días más tarde, se lanzó un doble ataque contra el Banco de Chile. Se cree que el primero, un ataque de ransomware, sirvió como distracción e hizo colapsar miles de PC y cajeros automáticos y tuvo un efecto dominó sobre muchos sistemas de terceros. El segundo, el ataque «verdadero», tuvo como objetivo el sistema SWIFT del banco, y los atacantes consiguieron transferir aprox. 10 millones de dólares de las cuentas operativas del banco a unas cuentas en Hong Kong. No han salido detalles acerca de las técnicas utilizadas por los atacantes.

Junio

Productos prohibidos en las instituciones de la Unión Europea

Tras decisiones parecidas en Estados Unidos, el Reino Unido y los Países Bajos, el día 13 de junio, el **Parlamento Europeo aprobó la resolución sobre ciberdefensa** lo cual, entre muchas otras recomendaciones, pidió a la UE «que lleve a cabo una revisión exhaustiva de los programas, los equipos y las infraestructuras informáticas y de comunicaciones que se utilizan en las instituciones, a fin de excluir programas y dispositivos potencialmente peligrosos y prohibir aquellos que hayan sido confirmados como malintencionados, como los de Kaspersky Lab». Inmediatamente después de que se conociera la noticia, Kaspersky canceló su colaboración con Europol y la iniciativa *NoMoreRansom*.

La decisión de la Unión Europea atraerá incluso más atención a los riesgos geopolíticos que deberían considerar las organizaciones de seguridad al tomar decisiones de compra.

Ciberataque a satélites

En el mes de junio, se descubrió un **ciberataque** que según los investigadores que lo descubrieron, fue lanzado desde ordenadores chinos, a satélites estadounidenses y de países del sudeste de Asia. Los satélites pertenecían a compañías de defensa y operadores de telecomunicaciones. El objetivo del ataque era claro: espionaje, específicamente la interceptación de comunicaciones militares y civiles. Según los investigadores, los hackers pudieron infectar los ordenadores que controlaban los satélites, lo cual significa que teóricamente podrían haber alterado las ubicaciones de los satélites.

Julio

Mensajes falsos de WhatsApp provocan linchamientos en La India

Como explica un reportero, «Las noticias falsas están siendo culpadas por engañar a votantes y posiblemente influir las elecciones en occidente. Pero en la India, están causando muertes». Al menos cinco personas fueron apaleadas hasta la muerte después de que se difundiesen a través de Whatsapp falsos rumores sobre el secuestro de niños. También hubo reportajes sobre otros apaleamientos por todo el país. El problema ha obligado a la policía india a lanzar una campaña anti-noticias falsas, y el Gobierno indio ha exigido a la app de mensajería instantánea que bloquee estos mensajes. La empresa incluso incluirá una nueva funcionalidad en el país para impedir que los usuarios reenvíen mensajes a más de cinco personas o grupos.

Espías rusos imputados por al hackeo del DNC (Comité Nacional Demócrata)

El día 13 de julio, el Departamento de Justicia de Estados Unidos imputó a 12 espías rusos por **delitos de hackeo** relacionados con las elecciones presidenciales de 2016. Proporcionó un informe detallado sobre las tácticas utilizadas y las operaciones llevadas a cabo por el equipo de agentes, miembros de GRU, un organismo de inteligencia ruso, según dice la acusación. Se utilizó spear phishing para robar los credenciales a numerosas personas, sustrayendo el contenido de emails, entrando en sus ordenadores y colocando cientos de ficheros con código malicioso. Para conseguir esto, **instalaron el malware X-Agent**, que es capaz de grabar las teclas pulsadas, robar archivos, y hacer capturas de pantalla.

Sextortion

La Policía Española advirtió sobre renovadas campañas de *sextortion*, con 6.000 víctimas declaradas desde 2014. Las campañas recurren a contraseñas obtenidas en brechas de datos que están disponibles en foros de cibercrimen, y que los usuarios siguen utilizando a pesar de haber sido filtradas. Luego, se hace creer a la víctima que el hacker puede haber comprometido el sistema y que ha utilizado la webcam para grabar un vídeo mientras la víctima miraba pornografía, con la amenaza de publicar el vídeo si no se paga un rescate. Según la Policía Española, el rescate que se pide (en bitcoin) puede variar entre 50 y 6.000 euros.

Facebook multado por el escándalo de Cambridge Analytica

La Information Commissioner's Office (ICO), el organismo de privacidad de Reino Unido, impuso a Facebook una multa de 500.000£, la sanción máxima, por dos violaciones de la Ley de protección de datos del Reino Unido. Muchos consideran que esta sanción es un castigo mínimo para la empresa, ya que tuvo ingresos de más de 40 mil millones de dólares en 2017. Bajo el nuevo reglamento del GDPR, es probable que la multa hubiera sido mucho más alta.

Rutas marítimas y navieras en peligro

Se ha revelado que muchos de ellos siguen utilizando sistemas anticuados – algunos siguen utilizando Windows NT, de 1993 –, junto con terminales de comunicación por satélite expuestos, interfaces de usuario accesibles mediante protocolos inseguros, y credenciales predeterminadas que nunca fueron modificadas.

Los agujeros de seguridad de las embarcaciones pueden provocar daños sustanciales tanto en industrias nacionales como en el entorno marítimo, incluyendo puertos, canales y muelles. Los analistas señalaron que, entrando al ECDIS (El Sistema de Información y Visualización de la Carta Electrónica – el sistema electrónico que permite que estos buques naveguen), también se puede obtener acceso a los sistemas que avisan al capitán de un posible escenario de colisión. Controlando estas alarmas de choque, los atacantes podrían bloquear rutas tan importantes como el canal de la Mancha y perjudicar toda la oferta y demanda de todo un país.

Agosto

Comportamiento Inauténtico Coordinado - Manipulación de opiniones

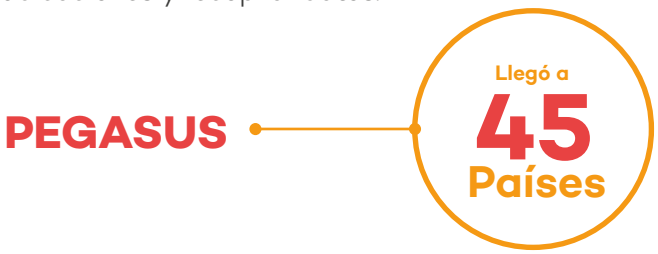
El 21 de agosto, actuando en base de una pista recibida de la empresa de ciberseguridad FireEye, Facebook anunció que había borrado de Facebook y de Instagram 652 páginas, grupos y cuentas que participaban en «comportamiento inauténtico coordinado» - en algunos casos provenientes de Irán y Rusia - que se utilizaban para engañar a otros sobre quiénes eran y qué hacían.

El mismo día, Microsoft anunció que había frustrado planes para atacar las elecciones legislativas de los Estados Unidos de noviembre. Según la empresa tecnológica, hackers del grupo Fancy Bear habían creado seis dominios web, haciéndose pasar por webs del International Republican Institute, que se iban a utilizar en campañas de spear phishing.

Septiembre

Spyware llega a 45 países

El 18 de septiembre, se reveló que un peligroso spyware llamado Pegasus había llegado a 45 países – 6 de los cuales en el pasado ya han utilizado spyware para abusar de los derechos humanos. Desarrollado por la **empresa israelí NSO Group**, el spyware tiene como objetivo iPhones y dispositivos Android, llegando a ellos a través de phishing para, seguidamente, lanzar una serie de ataques zero-day y evadir así los mecanismos de seguridad. Se utiliza para vigilar los SMS y las llamadas, recopilar contraseñas, rastrear ubicaciones y recopilar datos.



Acusación por WannaCry

En septiembre, el **Ministerio de Justicia estadounidense** tomó una medida poco común: acusó oficialmente a un hacker norcoreano por llevar a cabo los ataques de WannaCry, así como por estar implicado en el hackeo de Sony Pictures en 2014, y el robo del Banco de Bangladesh en 2016.

Octubre

Ciberataque en Países Bajos

El 4 de octubre, el gobierno holandés denunció que oficiales holandeses y británicos interrumpieron un ciberataque a la sede de la Organización contra la Proliferación de las Armas Químicas en La Haya. Se cree que esta organización fue el objetivo debido a sus investigaciones del uso de armas químicas de parte de Rusia en Siria y el Reino Unido. En este caso, acusan a cuatro agentes rusos que dicen son agentes del equipo de ciberguerra del GRU. Supuestamente, viajaron a los Países Bajos con pasaportes diplomáticos. Su intención era entrar en la red de la Organización utilizando equipamiento escondido en un coche que se aparcó cerca de la sede, e interrumpir los ordenadores en la oficina.

Cierre Google Plus

El 8 de octubre, Google anunció que cerraba su red social, Google Plus debido a un fallo de seguridad que había dejado expuestos los datos personales de al menos 500.000 usuarios. La empresa aseguró que ningún hacker había accedido a estos datos.

Noviembre

Nueva versión de Stuxnet

El gusano Stuxnet fue descubierto en 2010 en Irán. Se cree que fue desarrollado específicamente para atacar las centrales nucleares iraníes. El 2 de noviembre, Gholamreza Jalali, el jefe de la agencia de la Defensa Civil de Irán dijo que se había descubierto lo que se cree que es una nueva versión de este ataque. Fue descubierto intentando entrar en las redes estratégicas y las infraestructuras críticas del país.

Hackeo a Amazon en el Black Friday

Horas antes del Black Friday, y con el Cyber Monday a la vista, Amazon alertó a algunos clientes sobre un "Error Técnico" en su sitio web que exponía el nombre y la dirección de correo electrónico de los usuarios. El gigante del comercio electrónico confirmó la autenticidad del mensaje de aspecto sospechoso con varias publicaciones, diciendo solo que ha solucionado el problema e informando a los clientes que pueden haber sido afectados. A diferencia de esta filtración, la que sufrió el mes pasado fue causada por un empleado de Amazon que fue sorprendido vendiendo datos de clientes y que Amazon despidió al descubrir lo que estaba haciendo. A pesar de la seguridad de Amazon, siempre es una buena idea cambiar tu contraseña después de un incidente de seguridad.

Fugas de datos.

El año del GDPR

El pasado 25 de mayo fue el día D, la fecha desde la que el **GDPR**, el **nuevo Reglamento General de Protección de Datos,** es obligatorio en toda la Unión Europea. Con ello llegaba una normativa que, pese a gozar de dos años de adaptación, al final, en la mayoría de casos, se acabó implementando en el último minuto.

El nerviosismo y la preocupación por parte de muchas empresas era evidente, sobre todo si tenemos en cuenta que **las consecuencias de incumplir el GDPR eran severas**, con **multas de 10 millones de euros** o el 2% de los ingresos anuales (Nivel 1) o de 20 millones o el 4% de los ingresos anuales (Nivel 2).

Una de las consecuencias inesperadas fueron las prisas de último momento para cumplir con los nuevos reglamentos. Los consumidores notaron este apuro con la avalancha de correos enviados por empresas que pedían permiso para seguir teniendo estos datos en sus bases. Sin embargo, muchos expertos advirtieron que estos correos no eran necesarios ya que las empresas ya tenían permiso de estos usuarios, lo cual significó que se perdieron muchos contactos.

A pesar del margen de tiempo para la preparación con el que jugaban las organizaciones, un mes después de la llegada del GDPR, varias agencias de protección de datos **reportaron** un aumento significativo en la cantidad de quejas y reportes de brechas de datos en el seno de las empresas.

Y las consecuencias no se han hecho esperar. La primera multa a una organización según las obligaciones marcadas por el nuevo reglamento vino a finales de octubre cuando **el Hospital do Barreiro** en Portugal fue sancionado con 400.000€ de multa por dos violaciones de las normas.

Multas Nivel 1

10.000.000 €

2% **De Ingresos anuales**

Multas Nivel 2

20.000.000 €

4% **De Ingresos anuales**

Redes Sociales: Facebook

Este año, la red social más utilizada del mundo, ha tenido que enfrentarse a múltiples problemas derivados de la protección de datos y la privacidad de sus usuarios.

Lo primero que se reveló en marzo fue **el escándalo de Cambridge Analytica.** En varios periódicos se publicaron los detalles de cómo se usaron sin permiso los datos de carácter personal (PII) de al menos 87 millones de usuarios para intentar influir en el resultado de las elecciones en Estados Unidos. Como resultado, Mark Zuckerberg fue obligado a comparecer ante el Comité Jurídico del Senado en Estados Unidos.

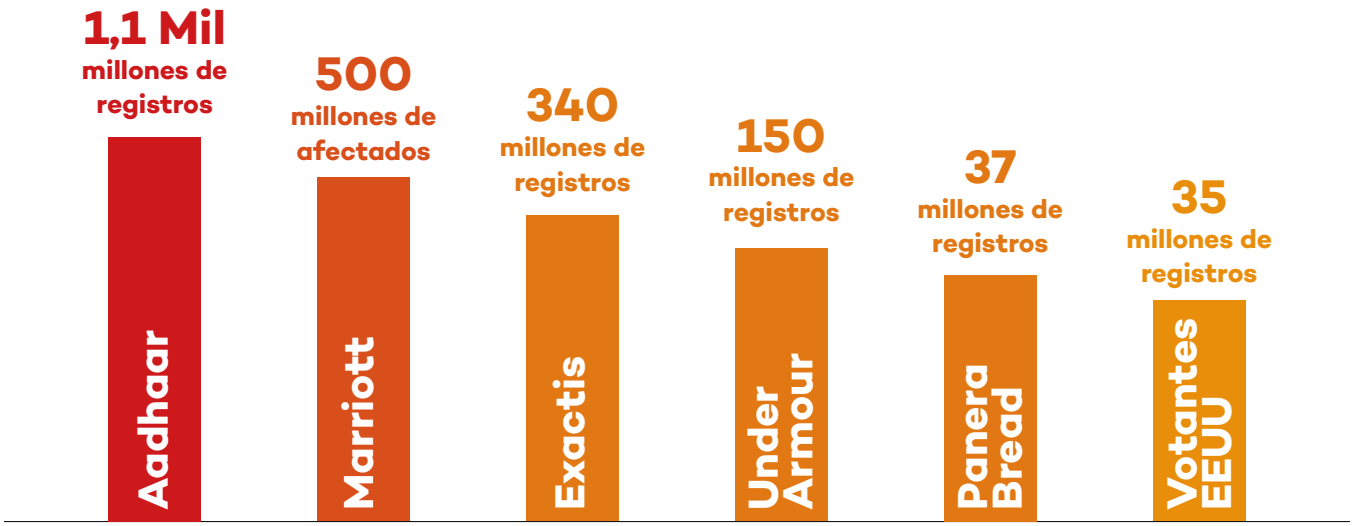
Como resultado del escándalo, la Oficina del Comisionado de Información (ICO) de Reino Unido **le impulsó una multa** de 500.000£, la máxima sanción posible antes del GDPR.

Ya en el mes de septiembre, cerca de **50 millones de cuentas quedaron expuestas** en ciberataque a la red social. Los atacantes explotaron una vulnerabilidad que les permitió robar los tokens de acceso del usuario, y en este caso, el proceso de notificación y las consecuencias ya han sido otras.

Siguiendo las reglas del GDPR, Facebook notificó el incidente al Comisario de Protección de Datos (DPC) de Irlanda, donde tiene su sede europea, y todavía queda por ver si recibe una multa que podría alcanzar los **1,63 mil millones de dólares** (1,4 mil millones de euros).

Y si parecía que no podía suceder nada más, en noviembre se **descubrió** una web que vendía mensajes privados de al menos 81.000 cuentas hackeadas. Según decían los dueños de la web, tenían los detalles de un total de 120 millones de cuentas, que pretendían vender. Facebook, sin embargo, se defiende advirtiendo que su seguridad no ha sido comprometida y que lo más probable es que se utilizaran extensiones de navegador maliciosas para acceder a estas cuentas.

Desafortunadamente, las brechas de datos siguen copando titulares de manera regular. Aquí proporcionamos un **ranking de los 6 casos más graves**, reportadas entre enero y agosto según la cantidad de registros afectados (o potencialmente accedidos):



1. Aadhaar (India).

Potencialmente 1,1 mil millones de registros.

Aadhaar, la base de datos de identificación nacional india, contiene registros sobre 1,1 mil millones de ciudadanos, incluida su información de identificación biométrica. En enero, periodistas de un periódico nacional informaron de que pudieron **obtener el fichero de cualquier individuo en Aadhaar por 500 rupias** (casi 6 euros) desde un grupo de WhatsApp. También obtuvieron el software de impresión de AadHaar por 300 rupias adicionales.

La Autoridad de Identificación Única de la India (UIDAI), la agencia que gestiona el sistema, niega contundentemente estas alegaciones acerca de la brecha. Meses más tarde, en junio, un investigador de seguridad informó que una filtración de datos en un sistema vulnerable permitió que cualquier persona pudiera descargar la información privada de todos los titulares de un Aadhaar, exponiendo sus nombres, sus números únicos de 12 dígitos de identificación, e información sobre servicios a los que están conectados, como sus datos bancarios y otra información privada. La UIDAI también ha negado que sea verdadera la afirmación, y afirmó que la base de datos seguía «segura».

2. Cadena hotelera Marriott.

500 millones de clientes afectados.

El 30 de noviembre la empresa hotelera Marriott International reveló que el sistema de reservas de muchas de sus cadenas de hoteles había sido hackeada, exponiendo los datos privados y personales de hasta 500 millones de clientes, constituyendo una de las fugas de datos más grande de la historia. El valor potencial de la información expuesta es de tal magnitud que ha alimentado la especulación de que se trate de un ataque perpetrado por un estado, con el fin de espiar los movimientos de diplomáticos, espías, autoridades militares y ejecutivos. El acceso no autorizado al sistema de reservas de Starwood Hotels, que incluye cadenas como St. Regis, Westin, Sheraton, Aloft, Le Meridien, Four Points y W Hotels,tuvo lugar desde el año 2014 en adelante.

3. Exactis (EE.UU).

Aproximadamente 340 millones de registros.

En junio, el investigador de seguridad llamado Vinni Troia descubrió que **Exactis, una compañía estadounidense de marketing,** había expuesto los ficheros de aproximadamente 340 millones de personas en un servidor de acceso público. Según Troia, cada registro contiene hasta 150 campos de información que describe una persona, incluidos nombres, direcciones físicas, y números de teléfono. Además, alrededor de la mitad contenía direcciones de correo electrónico.

También muchos de los registros comprometidos contienen datos como el número de niños en una casa, las edades de los niños, el tipo de tarjeta de pago que tiene esa persona, una estimación del valor de su casa, si tiene acciones, sus hobbies, la empresa con la que tiene su hipoteca, grupo étnico o religión, entre otras muchas más. Aunque los registros no contienen números de seguridad social ni detalles bancarios, sería muy útil para cometer fraude o para ataques de phishing.

Para este caso, y otros de los más sonados este año, no hay un veredicto todavía. De hecho, el supervisor Europeo de Protección de Datos, Giovanni Buttarelli, ha **comentado recientemente** que las primeras multas y amonestaciones se verán a finales de este año.

4. Under Armour (EE.UU).

Aproximadamente 150 millones de registros.

En marzo, **Under Armour protagonizó la que ha sido una de las mayores brechas de seguridad** sobre datos personales de usuarios registrados de la historia, con el anuncio de la exfiltración de 150 millones de usuarios de su popular aplicación de alimentación y nutrición, MyFitnessPal, cuya web y App había sido comprometida. La empresa descubrió que en febrero, un tercero no autorizado había accedido a los nombres de usuario, las direcciones de correo, y las contraseñas encriptadas de los usuarios que estaban dados de alta.

5. Panera Bread (EE.UU).

Hasta 37 millones de registros (o más).

En abril, Brian Krebs, tras ser contactado por el investigador de seguridad Dylan Houlihan, informa que **el sitio web de la cadena de restaurantes Panera Bread** ha dejado al descubierto millones de registros y datos de carácter personal de sus clientes — incluidos sus nombres, direcciones físicas y de correo, sus cumpleaños y los último cuatro dígitos de las tarjetas de crédito de los clientes. Según el investigador, los datos llevaban expuestos ocho meses, a pesar de notificaciones repetidas a la empresa después del descubrimiento de la filtración.

6. Votantes en Estados Unidos.

Hasta 35 millones de registros

En octubre, a pocas semanas de las elecciones legislativas de Estados Unidos del 6 de noviembre, se descubrieron hasta **35 millones de registros electorales a la venta en un popular sitio web de hackeo.** Se temía que estos registros podrían emplearse para perjudicar las elecciones – incluida la manipulación de los listados de votantes en las urnas para impedir que la gente votara. La filtración afectó a 19 estados.

Otras brechas de datos relevantes este 2018:

British Airways.

En septiembre, la aerolínea británica reveló que entre el 21 de agosto y el 5 de septiembre, **cibercriminales habían podido robar los datos personales y financieros de más de 380.000 clientes.** Un grupo llamado MageCart fue el responsable de la infección del sitio web con un código malicioso que le permitió recolectar la información personal de los clientes de British Airways. Las última cifras que hacen balance del incidente y correspondientes a finales del mes de octubre hablan de 185.000 usuarios afectados.

Orbitz

En marzo, el sitio web de reservas de viajes Orbitz, reveló que la i**nformación relacionada con hasta 880.000 tarjetas de pago se había filtrado,** y que era posible que el atacante tuviera acceso a más datos de carácter personal e información sensible de los afectados.

Ticketmaster

En junio, la web de venta de entradas, Ticketmaster, **informó de una brecha de datos** que afectó a hasta 40.000 clientes británicos y de otras nacionalidades. Entre la información sustraída se encontraban los detalles de tarjetas de pago, direcciones físicas, y números de teléfono. Según Ticketmaster, la inserción de malware dentro de su servicio de atención al cliente fue la causa de esta brecha.

Adidas

En junio, la marca de ropa deportiva Adidas, **anunció** que clientes de su web estadounidense podrían haber sido afectados por una brecha de datos. Aunque la empresa no reveló muchos detalles técnicos, este incidente potencialmente afectó a millones de personas.

T-Mobile

En agosto, la empresa telefónica T-Mobile experimentó un ciberataque en el que los datos personales de unas dos millones de personas **fueron robados**. Se incluían nombres, números de teléfono, números de cuenta y códigos postales.

SingHealth de Singapur

En julio, Singapur sufrió la **brecha de datos** 'más seria' en la historia del país hasta el momento, cuando los **datos personales de 1,5 millones de pacientes de SingHealth**, el grupo de instituciones de servicios de sanidad más grande del país, fueron robados. Entre los **datos robados se encontraban los del Primer Ministro del País, Lee Hsien Loong**. Según el gobierno de Singapur, el ataque 'no fue obra de hackers normales y corrientes, ni de bandas criminales. Los atacantes tuvieron como objetivo claro los datos personales de Lee Hsien Loong", pudiendo hablar de un ataque dirigido.

Timehop

En julio, se reveló una brecha de datos de **usuarios de la app Timehop**, que afectó a **21 millones de personas**. Se robaron números de teléfono, nombres y direcciones de email, y es posible que pudieran acceder a las cuentas de los afectados. Según Timehop, la brecha fue posible debido a una falta de medidas de seguridad en su cuenta en la nube.

No quieras ser uno de ellos

Nadie quiere que su compañía aparezca en las noticias como la última damnificada por una brecha de seguridad. Por lo que supone para su reputación, para sus usuarios y para su negocio. Y más aún con la obligatoriedad del GDPR, cuyo principal objetivo es proteger los datos de los ciudadanos europeos y controlar cómo las organizaciones procesan, almacenan y utilizan estos datos, garantizando su seguridad, trazabilidad y su gestión, incluyendo el derecho a ser olvidado digitalmente. Una mala praxis en cualquier de esos procesos, ahora conlleva una serie de consecuencias extras, como las **multas de hasta 20 millones de euros** o el 4% de la facturación global anual de la empresa.

Para evitar estar en esa tesitura, el primer paso es ser consciente de la importancia de implantar medidas y políticas de seguridad efectivas. La prevención por parte de las organizaciones que tratan datos es el aspecto base del Reglamento. Es importante trabajar con visión y antelación como ventaja competitiva en la estrategia empresarial.

Soluciones como **Panda Data Control** son capaces descubrir, auditar y monitorizar los datos de carácter personal y sensible desestructurados en los endpoints, desde el dato en reposo, hasta las operaciones sobre ellos y su tránsito. De esta forma se evitan los accesos incontrolados a los datos sensibles de tu empresa, se garantiza el registro y la trazabilidad de todos los datos personales y te ayuda a cumplir con los reglamentos de protección de datos como GDPR o PCI-DSS.

El control de los datos que ofrece **Panda Data Control** es fundamental para demostrar a los responsables, al DPO y a las autorizadas, que tu empresa tiene un dominio exhaustivo de los PII ubicados en tus equipos. La herramienta decisiva para justificar cualquier gestión que debas hacer sobre esos datos: modificación, confirmación o cancelación.

Predicciones de ciberseguridad 2019.

1. Hacking "en vivo".

Aunque los tipos de malware "tradicionales", como troyanos o gusanos, siguen siendo muy utilizados por los atacantes, las nuevas técnicas de ataque "*sin fichero de malware*" crecerán a un mayor ritmo. Esto se debe, por una parte, a la mayor dificultad para detectarlos, y por otra, a la mayor capacidad ciberofensiva mundial, tanto por parte de estados como de bandas criminales, asociadas o no a estados.

2. En 2019 el concepto de soberanía digital se extenderá también a la seguridad.

En 2018 la geopolítica en el ámbito digital ha tomado un papel más relevante, como consecuencia de las posiciones más proteccionistas en occidente (Estados Unidos, Reino Unido), y de las reacciones por parte de otras potencias (Rusia y China principalmente), habiéndose incrementado el clima de desconfianza mutua entre ellas. **Países como Francia están tomando medidas** para proteger su soberanía digital. **Pensamos que esta tendencia se fortalecerá en 2019, sobre todo en Europa (que caminará hacia una soberanía digital europea)**, que se irá configurando como un cuarto bloque, frente al bloque Americano (USA), China y Rusia. Esto tendrá un efecto importante en cuanto a las estrategias y políticas de ciberseguridad, así como a las decisiones de compras de productos en este ámbito.

3. Incremento de ataques a la cadena de suministro (Supply Chain Attacks).

Posiblemente uno de los tipos de ataque más peligrosos, los ataques a la cadena de suministro implican la infiltración en el proceso de desarrollo de empresas o proyectos de software legítimo, en el cual los atacantes plantan código malicioso, que es distribuido con las actualizaciones de dicho software a sus usuarios. **Recientemente se detectó un caso** de este tipo en un Proyecto de código abierto en GitHUb, y que se une a otros descubiertos durante el año. Durante el 2019 es muy probable que se produzcan más casos como éste, dada su efectividad, el mayor impacto que puede tener, ya que se puede expandir rápidamente a millones de sistemas, y dado que el ataque se vale de la confiabilidad en un software legítimo, lo cual incrementa la dificultad para prevenirlo.

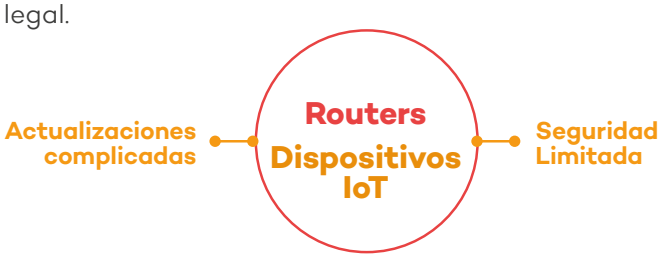
4. La inteligencia artificial será cada vez más utilizada por los atacantes.

Las mismas herramientas y conocimientos usados para analizar grandes volúmenes de datos y producir algoritmos inteligentes será cada vez más utilizada por los atacantes, con propósitos maliciosos. Esto se explica por la democratizacion de dichas herramientas, su disponibilidad, así como por la disponibilidad de información sobre los productos de seguridad, lo cual permitirá diseñar algoritmos que descubran automáticamente nuevas formas de ataque.

5. Se descubrirán nuevas vulnerabilidades catastróficas, similares a las que descubrieron hace casi un año (Meltdown y Spectre). A mediados de noviembre, y con poca repercusión, un equipo de investigadores descubrió **7 nuevos ataques** contra procesadores. Dos de ellos eran variaciones del ataque Meltdown, y los otros cinco, de Spectre. Pensamos que la mayor atención que dichas vulnerabilidades recabaron entre los investigadores, dado su impacto, y la poca investigación realizada hasta la fecha en comparación con las vulnerabilidades en aplicaciones (lo que significa que aún queda mucho por descubrir), hará que probablemente tengamos más noticias en este sentido, con el consiguiente riesgo de que se desarrollen exploits funcionales que acaben en manos de los cibercriminales.

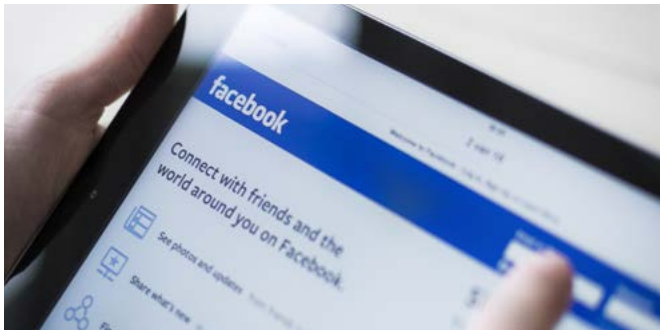
6. Más ataques a routers y dispositivos IoT:

Relacionado con el punto anterior, y continuando con la tendencia apuntada por ataques como **VPNFilter**, que se estima afectó a aproximadamente medio millón de routers de un buen número de fabricantes, en todo el mundo, en 2019 deberíamos ver también un aumento de ataques, no solo contra routers, sino contra dispositivos IoT. **Las razones principales son dos: por una parte, la seguridad por defecto de dichos dispositivos deja mucho que desear**, con contraseñas de fábrica o directamente sin contraseña por ejemplo; por otra parte, **son dispositivos más difíciles de actualizar**, en los que muchos usuarios ni siquiera saben cómo hacerlo, por lo que su nivel protección es mucho menor que otros dispositivos (PCs, portátiles). Esto hace que se puedan convertir en un objetivo fácil para los atacantes, tanto para realizar ataques DDoS, como para distribuir software de tipo criptominero por ejemplo, con bajo coste y riesgo para el atacante, especialmente ahora que el valor de las criptomonedas ha caído notablemente y ha disminuido la rentabilidad de su minería de forma legal.



7. Abuso de datos y noticias falsas.

En marzo de 2018 saltó el escándalo de Cambridge Analytica, en el que se estima que los datos de aproximadamente 87 millones de usuarios de Facebook fueron utilizados sin su consentimiento con fines politicos. El análisis masivo de datos, mediante herramientas de Big Data fácilmente disponibles, permite extraer perfiles detallados de las preferencias y tendencias personales de los usuarios en muchos ámbitos, no solo el político. Al igual que las noticias falsas buscan influenciar la opinión y el comportamiento político de las personas, la información personal diseminada en redes sociales de varios tipos (Facebook, Twitter, LinkedIn, etc), debidamente analizada y correlacionada, puede permitir el desarrollo de ataques de ingeniería social muy sofisticados y personalizados, con fines maliciosos. Por ejemplo, a través de información extraída de esta forma, se puede impersonar a alguien o a una empresa de forma más efectiva, para engañar a las víctimas a realizar acciones o comportamientos no deseados (como por ejemplo, realizar transferencias a cuentas del atacante bajo engaño). Este tipo de ataques (phishing, Business Email Compromise), que se han incrementado en 2018, crecerán aún más en 2019, dada su efectividad (se estima que, de media, un 4% de los receptores de emails destinados a engañar al usuario hacen click en ellos), y la mayor dificultad en detectarlos.



Precisamente la seguridad sobre estas predicciones para 2019 y cualquier otro tipo de acciones ilegítimas radica en la concepción del modelo de Panda Adaptive Defense, puesto que es capaz de monitorizar, clasificar y categorizar absolutamente todos los procesos activos (100%) en todos los equipos de la red corporativa. Incluyendo aquellas herramientas aparentemente legítimas pero que desarrollan comportamientos sospechosos o que se convierten en vectores de entrada a la red, como el RDP.

Panda Adaptive Defense no es un producto, es una suite de ciberseguridad que integra soluciones Endpoint Protection y Endpoint Detection and Response (EDR), con los servicios de 100% Atestación y Threat Hunting and Investigation, siendo la combinación perfecta de soluciones y servicios para proporcionar una visibilidad detallada de toda la actividad en todos los endpoints, el control de todos los procesos ejecutados en la red y la reducción de la superficie de ataque.

Panda Adaptive Defense clasifica automáticamente el 99,985% de los procesos, pero detrás de ese 0,015% hay personas. Analistas cualificados de PandaLabs que, gracias al servicio de 100% Atestación, acaban con el Gap de Detección, asegurando la confiabilidad de todos los procesos en ejecución y permitiendo reaccionar en términos de prevención, detección y respuesta contra el malware conocido y desconocido; así como los ataques que no siguen los patrones tradicionales como los fileless o aquellos que se ejecutan en memoria.

Además, el servicio de Threat Hunting e Investigación perfeccionan nuestro sistema de Machine Learning, alertando de actividades y comportamientos anómalos de usuarios, aplicaciones y dispositivos.

Prevención, detección y respuesta para ataques con y sin malware, en un solo agente.

Visibilidad Real-Time e Histórica de toda la actividad de los endpoints de la red corporativa.

Clasificación del 100% de los Procesos: 99,98% mediante Machine Learning, y el otro 0,02% por analistas de Panda.

Threat Hunting y Análisis Forense: los expertos de Panda y de nuestros MSSPs investigan en profundidad los ataques.

Bibliografía.

2. PandaLabs: datos de amenazas

https://www.pandasecurity.com/spain/mediacenter/malware/sin-secuestro-no-hay-rescate/

https://www.pandasecurity.com/spain/mediacenter/seguridad/ciberataques-evolucion-2017/

https://www.pandasecurity.com/spain/mediacenter/seguridad/que-es-el-cryptojacking/

https://www.pandasecurity.com/spain/mediacenter/seguridad/boom-ataques-fileless-malware/

3. Ciber- noticias 2018

https://www.pandasecurity.com/spain/mediacenter/seguridad/meltdown-y-spectre-fallo-seguridad/

https://arstechnica.com/gadgets/2018/01/heres-how-and-why-the-spectre-and-meltdown-patches-will-hurt-performance/

https://www.grc.com/inspectre.htm

https://www.pandasecurity.com/spain/mediacenter/pandalabs/ciber-sabotaje-juegos-olimpicos-invierno/

https://www.theverge.com/2018/2/25/17050868/winter-olympics-2018-russia-north-korea-cyberattack-opening-ceremonies

https://en.wikipedia.org/wiki/Infraud_Organization

https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible

https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

https://threatpost.com/china-linked-apt15-used-myriad-of-new-tools-to-hack-uk-government-contractor/130376/

https://thenextweb.com/hardfork/2018/03/07/wordpress-cryptocurrency-mining-malware/

https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

https://www.pandasecurity.com/spain/mediacenter/panda-security/gdpr-1980-2018/

https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/

https://www.pandasecurity.com/spain/mediacenter/seguridad/whois-protocolo-gdpr/

https://www.pandasecurity.com/spain/mediacenter/seguridad/ciberdefensa-parlamento-europeo/

https://www.eltiempo.com/tecnosfera/dispositivos/ciberataque-a-satelites-fue-lanzado-por-computadores-en-china-233268

https://www.npr.org/2018/07/18/629731693/fake-news-turns-deadly-in-india?t=1536657722588

https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

https://www.bleepingcomputer.com/news/government/us-charges-12-russian-intelligence-officers-for-hacking-dnc-running-dcleaks/

https://www.pandasecurity.com/spain/mediacenter/seguridad/gdpr-multa-facebook/

https://www.pandasecurity.com/spain/mediacenter/seguridad/peligros-industria-maritima/

https://www.zdnet.com/article/microsoft-weve-just-messed-up-russian-plans-to-attack-us-2018-midterm-elections/

https://threatpost.com/dangerous-pegasus-spyware-has-spread-to-45-countries/137506/

https://www.pandasecurity.com/spain/mediacenter/noticias/hacker-acusado-wannacry-corea/

https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body

https://www.pandasecurity.com/spain/mediacenter/mobile-news/googleplus-cierre-seguridad/

https://www.infosecurity-magazine.com/news/stuxnet-returns-striking-iran-with/

https://www.adslzone.net/2018/11/22/amazon-error-datos-clientes/

4. Brechas de datos

https://www.pandasecurity.com/spain/mediacenter/seguridad/gdpr-cuenta-atras/

https://www.pandasecurity.com/spain/mediacenter/adaptive-defense/gdpr/

https://www.theguardian.com/technology/2018/jun/26/european-regulators-report-sharp-rise-in-complaints-after-gdpr

https://www.itpro.co.uk/data-protection/28029/latest-gdpr-news-uk

https://www.pandasecurity.com/spain/mediacenter/seguridad/gdpr-multa-facebook/

https://www.pandasecurity.com/spain/mediacenter/seguridad/gdpr-multa-facebook/

https://www.bbc.com/news/technology-46065796

https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/

https://www.wired.com/story/exactis-database-leak-340-million-records

https://www.computerworld.es/tendencias/la-union-europea-espera-que-las-primeras-multas-de-gdpr-se-apliquen-antes-de-fin-de-ano

https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html

https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/

https://threatpost.com/up-to-35-million-2018-voter-records-for-sale-on-hacking-forum/138295/

https://www.pandasecurity.com/spain/mediacenter/noticias/british-airways-hackeada/

https://www.cnet.com/news/possible-orbitz-data-security-breach-affects-880000-payment-cards/

https://thehackernews.com/2018/06/ticketmaster-data-breach.html

https://www.bloomberg.com/news/articles/2018-06-28/adidas-says-millions-of-u-s-customers-being-alerted-of-breach

https://www.theverge.com/2018/8/24/17776836/tmobile-hack-data-breach-personal-information-two-million-customers

https://www.zdnet.com/article/singapore-suffers-most-serious-data-breach-affecting-1-5m-healthcare-patients-including-prime/

5. Predicciones

https://www.businessinsider.es/timehop-breach-21-million-users-2018-7?r=US&IR=T

https://www.wired.co.uk/article/google-france-silicon-valley

https://boingboing.net/2018/11/26/candy-from-strangers.html

https://www.zdnet.com/article/researchers-discover-seven-new-meltdown-and-spectre-attacks/

https://en.wikipedia.org/wiki/VPNFilter

panda

pandalabs