**2016**

**1. Robo de 81 millones al Banco Central de Bangladés**    
  
Varios piratas informáticos lograron acceder a los sistemas del Banco Central de Bangladés y transferir 81 millones de dólares a varios casinos de **Filipinas**. Un error ortográfico evitó la catástrofe: el nombre mal escrito de uno de los destinatarios levantó las alarmas y permitió bloquear el ataque, planeado para obtener casi mil millones de dólares.   
  
**2. Robo de 64 millones en bitcoins a Bitfinex**   
  
El mayor operador mundial de intercambio de bitcoin basado en dólares, **Bitfinex**, radicado en **Hong Kong**, [fue el objeto de este ataque](https://www.economiadigital.es/tecnologia-y-tendencias/la-moneda-virtual-de-internet-desenmascara-todas-sus-debilidades_185585_102.html). La cotización del bitcoin superior cayó un 23% en los días posteriores.   
  
**3. Publicación de los datos de 154 millones de votantes de EEUU**

Los datos incluían información personal de los electores, como la dirección, el correo electrónico, el número de teléfono o enlaces a sus redes sociales.   
  
**4. Publicación de información personal de 93 millones de mexicanos**   
  
Un fallo en la configuración de la base de datos de **MongoDB**, utilizada por el Instituto Nacional Electoral de México, provocó una difusión masiva de datos personales en el país. Un hecho que provocó gran revuelo en México, donde los secuestros son un crimen relativamente habitual.   
  
**5. Robo de mil millones de cuentas de Yahoo**  
  
[Una piedra más en el nefasto año de la tecnológica](https://www.economiadigital.es/tecnologia-y-tendencias/yahoo-sufre-el-mayor-robo-de-datos-de-la-historia_187826_102.html). Además de fechas de nacimiento, direcciones de correo electrónico, números de teléfono, contraseñas en **MD5**, la información robada también contenía preguntas y respuestas de seguridad sin cifrar.   
  
**6. Robo de 500 millones de cuentas a Yahoo (en 2014)**  
  
Otro suceso relacionado con la misma compañía. Este ataque, según la información desvelada hasta el momento, podría haber sido respaldado por un Estado extranjero. Entre los datos robados, de nuevo se encontraban preguntas y respuestas de seguridad sin cifrar.    
  
**7. Robo de 400 millones de cuentas a Friend Finder Network Inc.**   
  
El masivo robo a Friend Finder Network Inc., compañía que gestiona diferentes páginas de citas, incluyó datos personales de sus usuarios, como el correo electrónico, los patrones de navegación, los patrones de compra y su orientación sexual.  
  
**8. Ataque de denegación de servicio (DDoS) a Play Station y Twitter, entre otros**  
  
Se trata del mayor ataque de **DDoS** producido hasta la fecha con dispositivos de Internet de las cosas (**IoT**). Producido por la botnet **Mirai**, compuesta por cientos de miles de cámaras IP junto a otros dispositivos IoT, [dejó fuera de juego a múltiples servicios de Internet](https://www.economiadigital.es/tecnologia-y-tendencias/un-ataque-informatico-lastra-twitter-y-spotify-durante-horas_186802_102.html), llegando a afectar a **Play Station Network** y **Twitter**, entre otros. Se sospecha que este ciberataque habría sido también una prueba de concepto para afectar al funcionamiento de los sistemas de voto electrónico de EE.UU., antes de las elecciones del 8 de noviembre.   
  
**9. Fallo en la implementación de la pila TCP en sistemas Linux**  
  
El fallo en la implementación de la pila TCP en sistemas Linux --posteriores a la versión de **Kermel 3.6.**-- permitió la infección de malware de forma remota o incluso el secuestro del tráfico de usuarios con sistema operativo Android y en televisores inteligentes. El ataque, además, degradó las conexiones a la red mediante el protocolo Https, redirigiendo el tráfico.  
  
**10. Fallo en los procesadores Qualcomm**   
  
El fallo en procesadores Qualcomm permitió a los piratas acceder a información cifrada sin que se activasen los mecanismos de borrados en millones de teléfonos. Esta vulnerabilidad en la generación de las claves de cifrado afectó aproximadamente al 60% de los móviles Android del mercado.

**2017**

**1. Ataque phishing a usuarios de Gmail**

“Sofisticado” fue uno de los adjetivos más utilizados por los medios y blogs especializados en tecnología para hablar de este suceso. En mayo, un grupo de cibercriminales lanzaron un ataque para hacerse con el **control de los correos electrónicos de los usuarios de Gmail**. Lo lograron, en al menos, [un millón de cuentas (el 0,1% de los usuarios de Gmail, según Google)](https://www.forbes.com/sites/thomasbrewster/2017/05/03/massive-google-gmail-phish-many-victims/#56997e442a1b).

Para ello, utilizaron un método muy popular: el phishing. Se trata de [un tipo de ingeniería social](https://opendatasecurity.io/es/ingenieria-social-cuando-blindar-sistemas-informaticos-no-lo-es-todo/)  en el cual el atacante se hace pasar por una persona o entidad de confianza para obtener cierta información o privilegios.

Los usuarios de Gmail recibieron un e-mail en cuyo asunto se podía leer: “(nombre de un contacto conocido) **ha compartido un documento** por Google Doc contigo”. Para poder verlo, había que seguir el mismo procedimiento que se lleva a cabo cuando nos comparten archivos por Google Drive: clicar sobre “Open in Docs” y elegir la cuenta de Gmail por la que se quiere abrir el documento (en caso de haber varias logueadas).

Tal y como se ve en la última parte del siguiente GIF, el daño se produce cuando aparece una ventana en la que **se pide que se concedan determinados permisos a una aplicación** para ver el documento compartido. Si el usuario pincha sobre “Allow” (permitir) entonces es víctima del phishing.

Concedidos los permisos, los hackers **podían gestionar a su antojo** el correo electrónico de sus víctimas, así como acceder a los contactos para que el ataque siga reproduciéndose. Google no tardó mucho en eliminar la aplicación phishing.

Por otra parte, los usuarios víctimas del ataque tuvieron que **revocar los permisos** que habían dado a esta aplicación para acceder a sus cuentas a través del enlace: [https://myaccount.google.com/permissions.](https://myaccount.google.com/permissions) Es recomendable que entre dentro de ese link, aunque no haya sido víctima del ataque. A más de uno le sorprenderá la cantidad de aplicaciones que pueden acceder a información personal.

**2. Judy, posiblemente el ataque más grande a dispositivos Android**

Seguimos en el mes de mayo, momento en el que los [investigadores de Check Point](http://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/) descubrieron el virus Judy, un malware que pudo haber afectado a una escandalosa cantidad de dispositivos Android: entre 8,5 y 36 millones de smartphones y tabletas.

Se especula con la idea de que el virus fue creado y extendido por hackers de Corea del Sur a través de una compañía llamada Kiniwini. Para ello, los desarrolladores de Judy, **colaron casi medio centenar de aplicaciones en Google Play**, todas ellas basadas en juegos: “Fashion Judy: Snow Queen Style”, “Animal Judy: Persian Cat Car” o “Chef Judy: Picnic Lunch Maker” son algunos de los nombres.

Muchas de estas aplicaciones **gozaban de una buena reputación** en la tienda oficial de Google, ya que estuvieron disponibles durante varios años y acumulaban entre 4 y 18 millones de descargas. De ahí que la popularidad de una aplicación no es garantía de seguridad.

Cuando un usuario se descargaba e instalaba algunos de los juegos de Judy, la aplicación abría una pasarela que conectaba el dispositivo con una web en la que se **pinchaba en enlaces de publicidad que generaban ingresos a los hackers** a través de la infraestructura publicitaria de Google. Todo esto de manera oculta y sin conocimiento del usuario.

Inexplicablemente, el virus [Judy también se encontró en aplicaciones de otros desarrolladores](http://www.independent.co.uk/life-style/gadgets-and-tech/news/judy-malware-latest-android-smartphone-infect-millions-virus-google-play-a7762766.html), no solo en las firmadas por Kiniwini. Desde que se descubrió este virus, Google retiró todas las aplicaciones Judy de Google Play.

**3. Ataque a las elecciones francesas y alemanas**

Atrás quedan los tiempos en los que se confiaba en los procesos democráticos de las democracias occidentales. El cibercrimen no solo persigue lucrarse a costa de particulares y empresas, hay una parte de él que busca **impactar sobre el destino de sociedades** como la de Estados Unidos.

A pesar de lo que ha llovido desde aquel 9 de noviembre de 2016, momento en el que Donald Trump ganó las elecciones de Estados Unidos, hoy en día siguen saliendo documentos clasificados que apuntan a que Rusia trató de **hackear un proveedor de software de las máquinas de votación** que se utilizaron en Norteamérica.

[Según la NSA](https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1), el gobierno de Putin también dirigió ataques spear-phishing (enfocados a obtener accesos a datos confidenciales) a funcionarios implicados en el proceso electoral justo antes de que se celebran las elecciones.

El documento de la Agencia de Inteligencia del gobierno americano no deja claro si estos ataques tuvieron éxito o influyeron de alguna manera en los resultados.

Pero este no fue el único suceso. El Kremlin está de nuevo en el punto de mira en la injerencia que se están produciendo en las elecciones francesas. Tanto la publicación de correos electrónicos del partido de centro, *En Marche!*, como la **propagación de una serie de noticias falsas** que dañan la imagen de Emmanuel Macron, tienen como objetivo influir en el duelo político entre Macron y Le Pen. [Según la firma de ciberseguridad, Trend Micro](https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts), los autores de estos ciberataques son un grupo ruso llamado *Pawn Storm.*

La motivación de estos ataques podría radicar en que la candidata del Frente Nacional, Marine Le Pen, defiende unas políticas que simpatizan con el gobierno de Putin. Además, se sabe que el pasado mes de marzo, [Le Pen se reunió en Moscú con el Presidente Ruso](http://www.independent.co.uk/news/world/europe/french-election-marine-le-pen-vladimir-putin-moscow-russia-a7647621.html), lo cual **pone en duda la neutralidad del Kremlin en estos comicios** a tenor de las sospechas de su injerencia en otros procesos electorales.

Alemania es otro país que se está preparando para posibles ciberataques en sus próximas elecciones que se celebrarán en septiembre de este año. Las agencias de seguridad del Estado alemán tienen indicios de que [Rusia podría dirigir ataques](http://www.independent.co.uk/news/world/europe/germany-spy-chief-russian-cyber-attacks-russia-elections-influence-angela-merkel-putin-hans-georg-a7718006.html) a instituciones, políticos y miembros del Ejecutivo con el fin de alterar el curso de los comicios a través de una **campaña de desinformación y desprestigio a través de noticias falsas.**

Aunque estos ciberataques están dirigidos a partidos políticos, no cabe duda de la magnitud de su impacto. Al fin y al cabo, el objetivo es **cambiar la intención de voto a favor de un candidato** cuya victoría podría no obedecer a la verdadera voluntad social, sino a los intereses políticos de quienes dirigen los ataques. Lo peor es que es no sabremos hasta qué punto estos ataques están influyendo en los resultados, y por tanto en el rumbo político de un país.

**4. Tercer hackeo a los usuarios de Yahoo**

Recientemente, la Comisión Nacional del Mercado de Valores de Estados Unidos (SEC por sus siglas en inglés) ha denunciado a través de [un informe](https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm) el supuesto hackeo de 32 millones de cuentas de Yahoo. La investigación que se llevó a cabo entre noviembre y diciembre de 2016 llegó a la conclusión de que **los atacantes utilizaron una técnica llamada *cookie-forging attack.***

Se trata de la inyección de cookies falsas en una página web que permite a los atacantes el acceso a la información de los usuarios sin que este proporcione su usuario y contraseña. En el caso Yahoo, el falseo e inyección de cookies permitía que los servidores de Yahoo entendieran que **el usuario que estaba tratando de acceder a su cuenta era legítimo y ya estaba identificado**, por lo que no pedía los datos de acceso. Esta es la manera por la cual los atacantes vulneraron la seguridad de miles de usuarios de Yahoo.

Lo cierto es que estos ataques se produjeron entre 2015 y 2016 y es ahora cuando se conoce la noticia y sus consecuencias. Uno de los motivos por los que el SEC ha estado investigando este suceso es porque las leyes estadounidenses obligan a las compañías víctimas de ciberataques que revelen **cuándo se ha producido una vulneración de su seguridad**, ya que podría afectar a las cotizaciones en bolsa. La cuestión es que [Yahoo ha tardado mucho tiempo en revelar los dos primeros ataques](https://techcrunch.com/2017/01/22/yahoo-hacking-sec/), y de no justificar debidamente esta decisión, el SEC podría terminar presentando una demanda.

Por parte de Yahoo, [la CEO Marissa Mayer, anunció en su Tumblr](https://marissamayr.tumblr.com/post/157876672644/update-on-yahoos-security-incident)  que es consciente de la gravedad del asunto y que ya han puesto en marcha medidas para solventar este grave fallo de seguridad.

**5. WannaCry, el ransomware que sacudió el mundo**

Basta con buscar “ciberataques de 2017” en Google para darse cuenta de que el [ransomware que se propagó por Internet el pasado 12 de mayo](https://opendatasecurity.io/es/wannacry-ransomware-sacudio-mundo/) ha sido el que más titulares ha generado. De hecho, hay quien opina que los medios de comunicación han atribuido más trascendencia al suceso de la que verdaderamente tuvo. Se estima que los creadores de WannaCry [consiguieron recaudar una cuantía ridícula: 20,000 dólares](https://www.theguardian.com/technology/2017/may/13/criminals-behind-cyber-attack-have-raised-just-20000-experts-say" \t "_blank) en todo el mundo. Pero **no por ello hay que restarle importancia al ataque** teniendo en cuenta lo que está por venir.

Expertos de seguridad prevén que **la frecuencia de los ciberataques y la virulencia irá en aumento**, pudiendo causar importantes pérdidas a las empresas y organizaciones que no tomen cartas en el asunto cuanto antes.

En ciberseguridad, la prevención es el mejor arma y hoy en día disponemos de métodos que van más allá de instalar un antivirus y un cortafuegos. Las [auditorías de redes](https://opendatasecurity.io/es/seguridad-de-red/), [de servidores](https://opendatasecurity.io/es/seguridad-para-servidores/), [de aplicaciones web](https://opendatasecurity.io/es/auditoria-seguridad-informatica/), así como la [formación de todos los miembros de una organización](https://opendatasecurity.io/es/formacion-en-seguridad-informatica/) son las **claves para no ser la siguiente víctima de los ciberdelicuentes** que atentan contra su privacidad desde el otro lado del mundo.

21/10/2017

DDoS

Twitter, Spotify, Airbnb, Amazon, Netflix o The New York Times