howlermonkey.io

Informe de Seguridad

Retrospectiva 2016

howlermonkey

Informe de Seguridad

Retrospectiva 2016

Introducción

Este 2017 hemos decidido mirar por el retrovisor y realizar un breve análisis de lo ocurrido en el 2016 en materia de ciberseguridad para entender en retrospectiva lo que sucedió y lo que posiblemente pueda esperarse este año, enfocándonos principalmente en analizar las vulnerabilidades reportadas durante el 2016, en cuales son las principales industrias preocupadas en corregir fallos de seguridad, algunas noticias importantes y las tendencias del mercado de ciberseguridad.

Queremos que este informe sea lo suficientemente comprensible. Es por eso que en lugar de presentarte un análisis muy exhaustivo, hemos querido hacerlo de forma simple pero a la vez claro y perceptible.

La seguridad informática es una preocupación compartida entre varios equipos de una organización, desde los directivos, profesionales de seguridad y profesionales de DevOps, hasta los equipos de desarrollo, redes e infraestructura. Es por eso que los datos presentados en este informe impactarán de forma diferente a cada uno de estos segmentos de público, con la idea de generar una conciencia colectiva en torno a la seguridad.

Recuerda que las vulnerabilidades van a seguir existiendo, por lo que una postura preventiva y toma de decisiones basadas en la buena información permitirán mejorar tus tiempos de corrección. Cada vez más las empresas se enfocan e invierten en la prevención, así que te recomendamos considerar la seguridad en todas las etapas de tu proyecto, esto evitará costos a futuro.

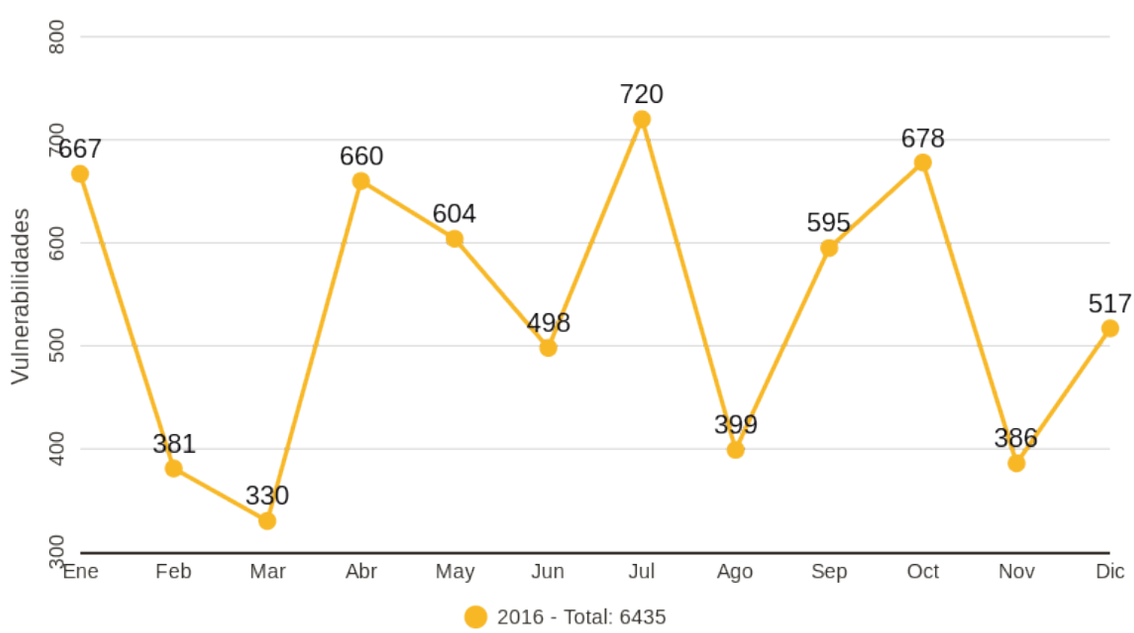
Informe de Seguridad

Retrospectiva 2016

Índice

Vulnerabilidades 2016

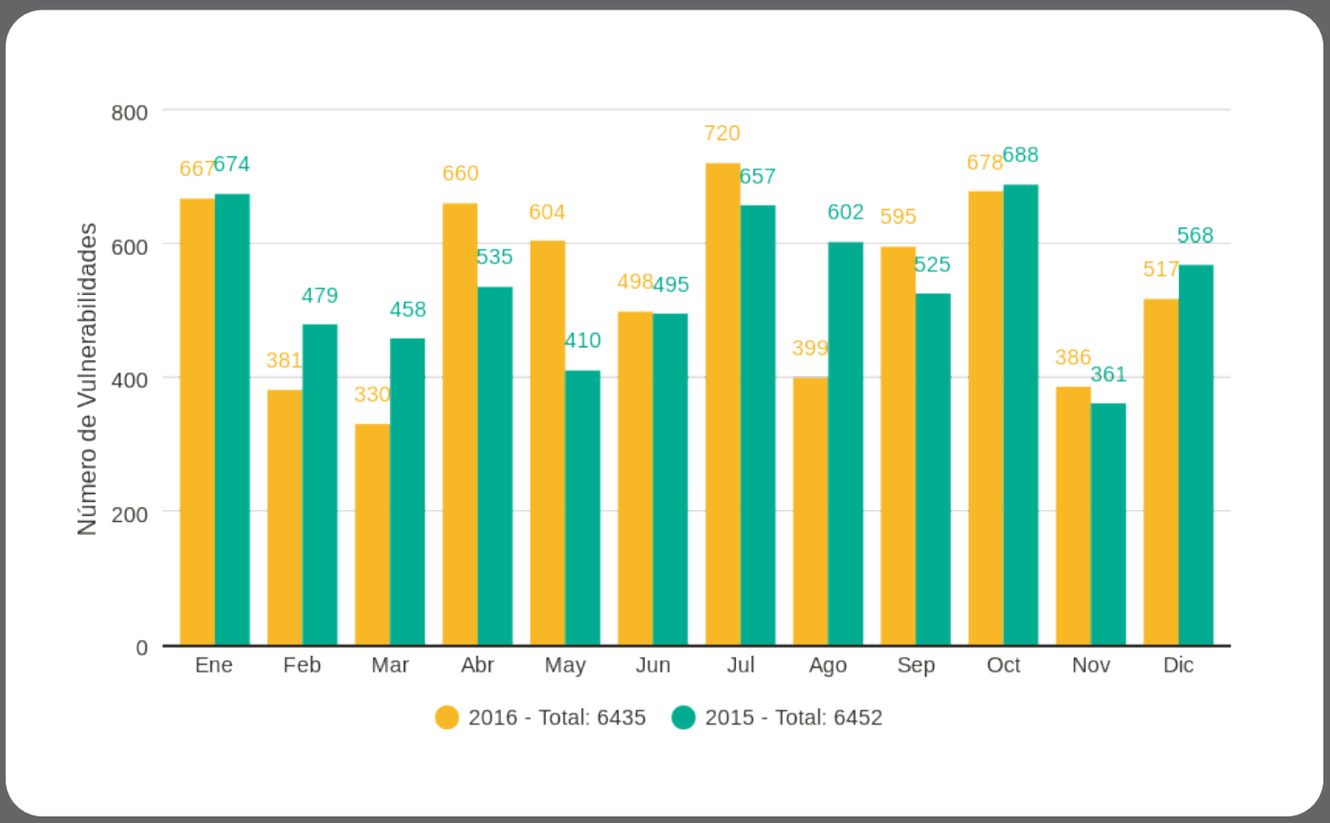
Un total de 6435 vulnerabilidades se registraron en el 2016, el cual inició con un número importante de vulnerabilidades en el mes de Enero motivado entre otras cosas por el boletín de seguridad de Oracle donde reportaba 248 vulnerabilidades en varios de sus productos. Julio llegó a alcanzar el mes con más registros en el 2016 con 720 vulnerabilidades reportadas.



Fuente: MITRE

Vulnerabilidades 2015/2016

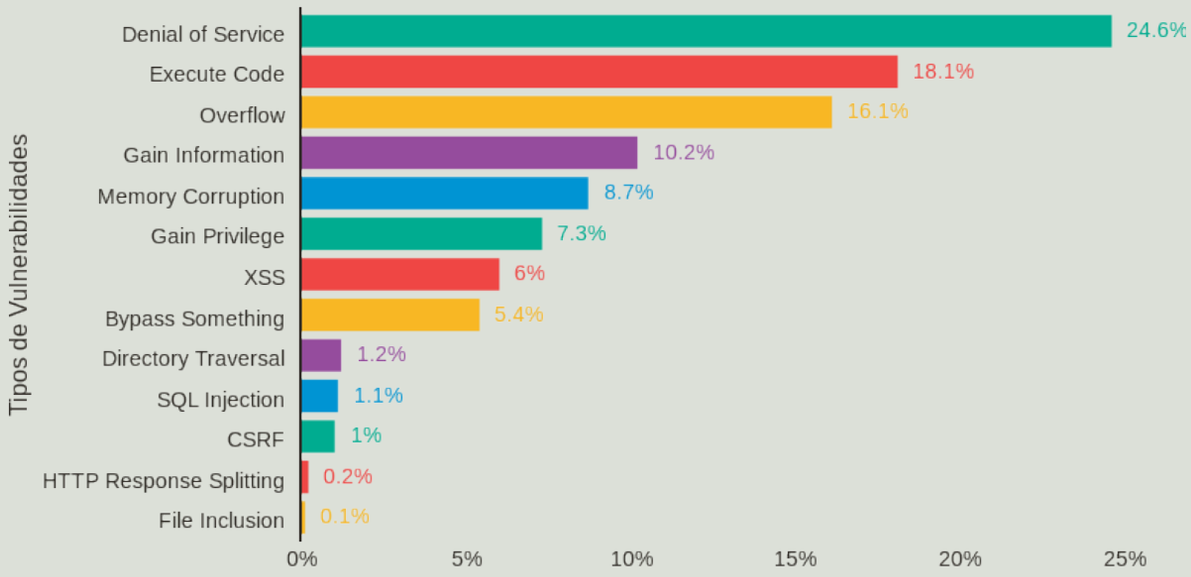
El 2015 y el 2016 fueron años muy parejos en cuanto al número de vulnerabilidades reportadas, el 2016 con apenas 17 registros menos en comparación con el 2015. Se puede observar notables variaciones en la distribución sobre todo en los meses de Marzo, Abril, Mayo y Agosto.



Fuente: MITRE

Tipos de vulnerabilidades

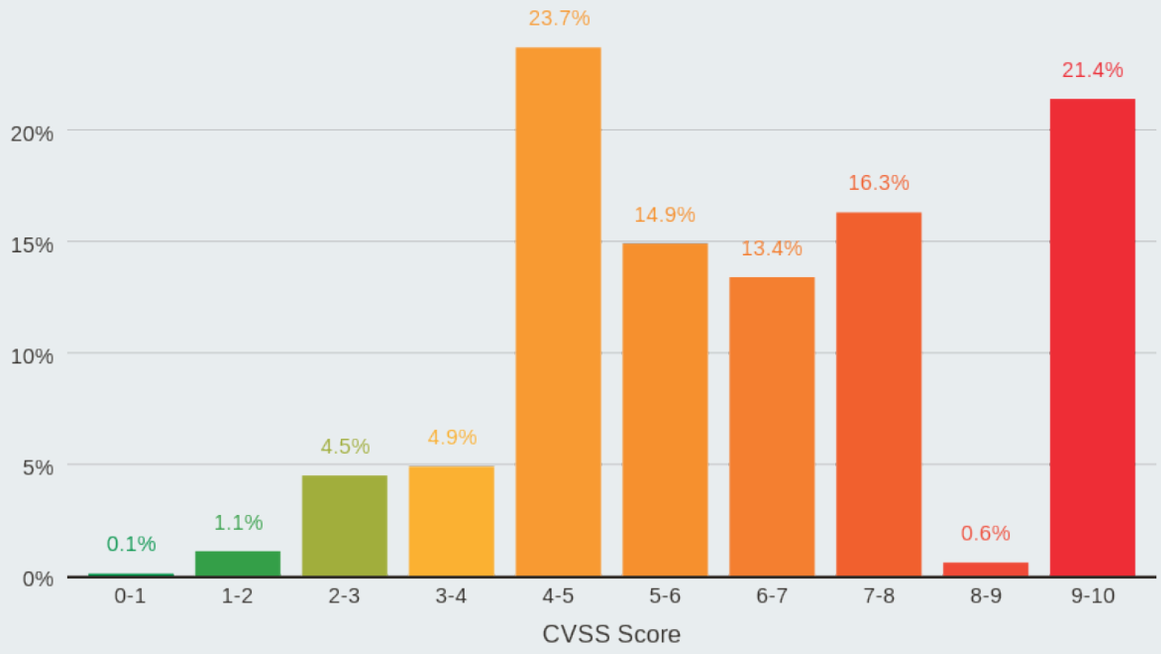
Las vulnerabilidades pertenecientes a la categoría de denegación de servicio fueron las más reportadas en el 2016 con un 24.6 %, seguidas por las vulnerabilidades de ejecución de código arbitrario y de desbordamiento. En los tres principales tipos de vulnerabilidades se mantuvo la tendencia con respecto a los años anteriores.



Fuente: MITRE

Distribución del impacto de las vulnerabilidades - CVSS Score 2016

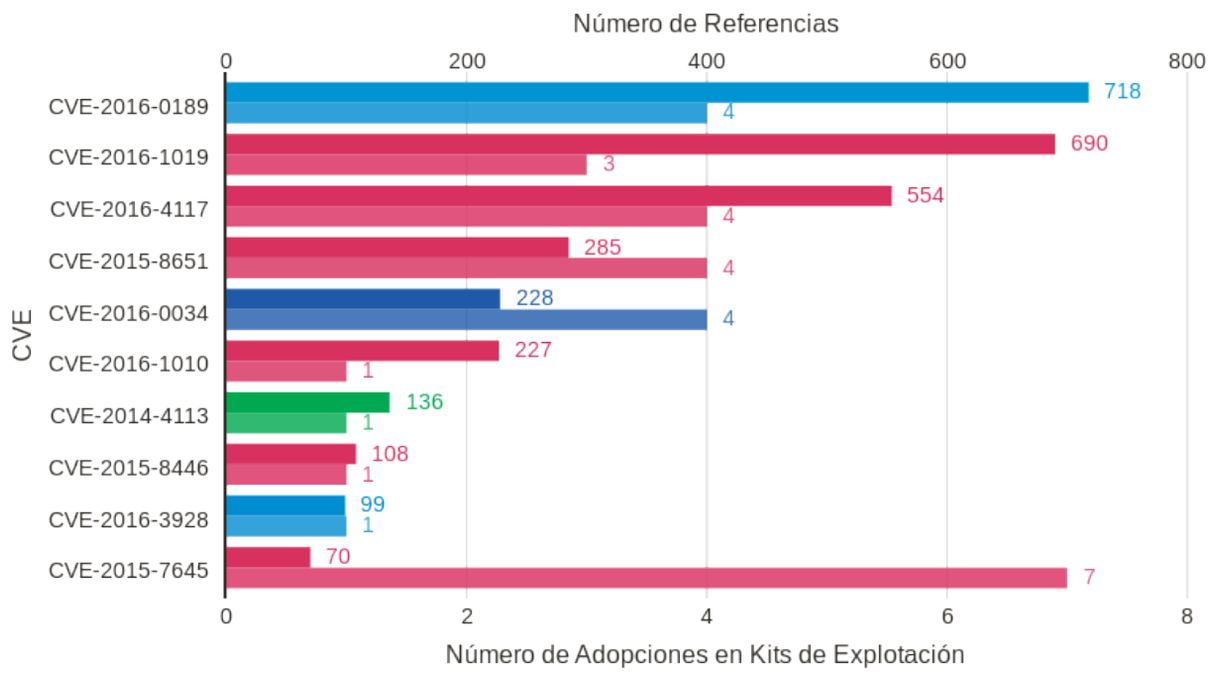
El CVSS Score permite estimar el impacto y cuantificar la severidad de una vulnerabilidad, a continuación vemos la distribución de las vulnerabilidades según su nivel de impacto. En el 2016 se registró una mayor cantidad en las vulnerabilidades comprendidas entre el CVSS score 4-5 (23.7%) y 9-10 (21.4%). El porcentaje de vulnerabilidades comprendidas entre el CVSS score 9-10 sigue siendo muy alto si entendemos que la explotación de una vulnerabilidad crítica o de CVSS score de 9 a 10 corresponde al compromiso total de un sistema.



Fuente: MITRE

Top 10 de vulnerabilidades con exploits más utilizados en el 2016

Que una vulnerabilidad aparezca en este ranking significa que para los ciberdelincuentes esta vulnerabilidad representa una gran oportunidad de negocio debido a la cantidad de posibles víctimas afectadas. Como se puede observar a continuación los afectados son viejos conocidos, destacando Internet Explorer y Adobe Flash, este último ocupando 6 de los 10 lugares del ranking.

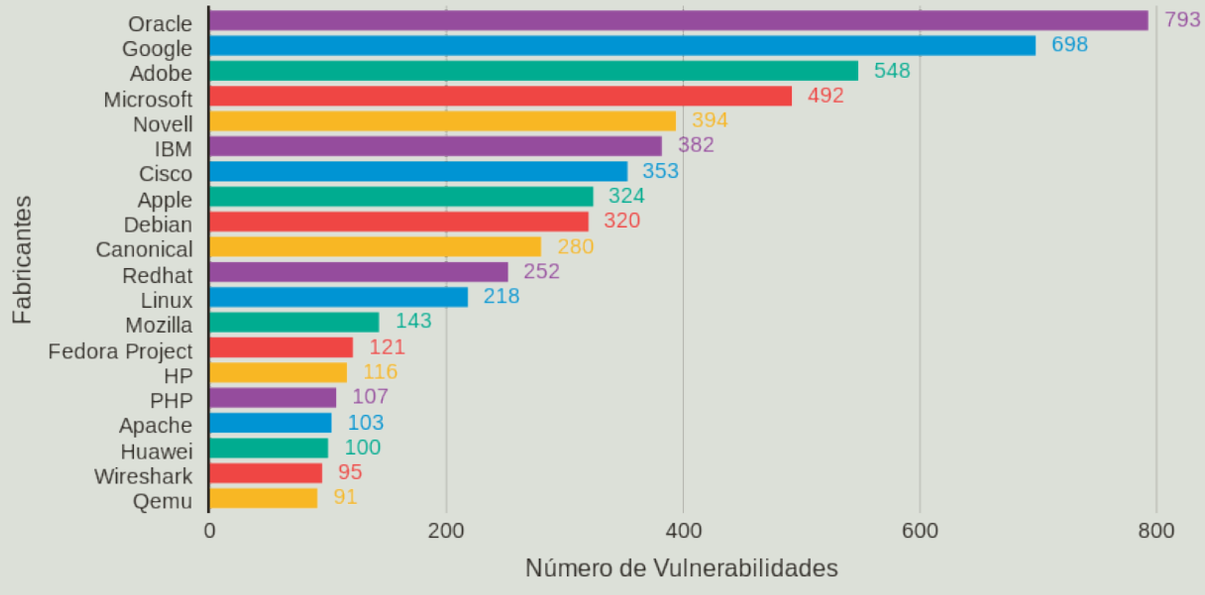


Fuente: Recorded Future

Los principales kits de exploits incorporan estas vulnerabilidades de manera casi inmediata a sus distribuciones, siendo CVE-2015-7645 del top 10 la más ampliamente adoptada en los kits de exploits analizados, debido a su efectividad multiplataforma (Windows, OS X, Linux).

Top 20 vendors con más vulnerabilidades reportadas en 2016

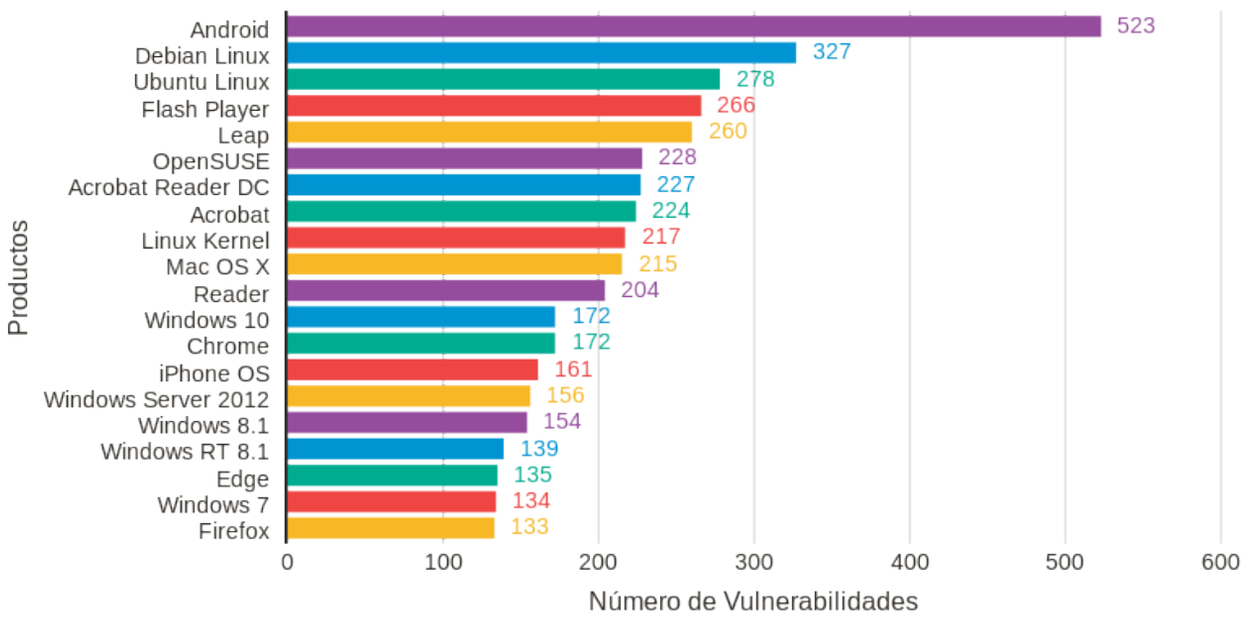
La empresa Oracle lidera la tabla del top 20 de vendors con mayor número de vulnerabilidades reportadas en el 2016, superando el número de vulnerabilidades registradas por ellos en el 2015 y pasando del puesto número 2 al 1. Por otra parte Google pasó del puesto número 6 al puesto 2, duplicando en cantidad el número de vulnerabilidades registradas en el 2015. Mientras que el resto de involucrados en los primeros lugares siguen sin grandes cambios en comparación al año anterior. Una incorporación interesante al top 20 del año 2016 fue el caso de Huawei que pasó del puesto 45 al puesto número 18 en tan solo un año.



Fuente: MITRE

Top 20 products con más vulnerabilidades reportadas en 2016

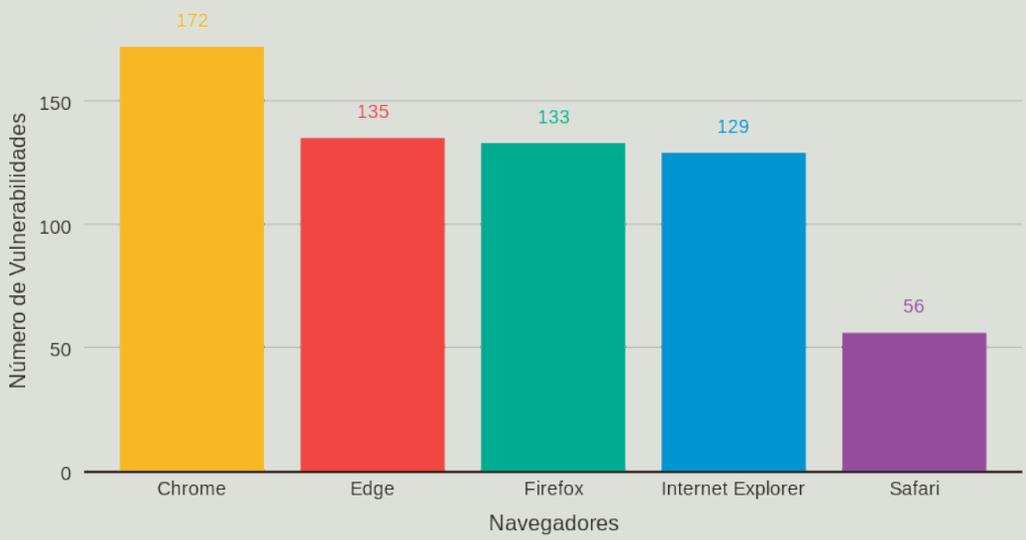
El 2016 no fue un buen año para Android, ya que incrementó en gran cantidad el número de vulnerabilidades reportadas y pasan del puesto 26 al número 1, liderando así el top 20 de productos más afectados. En su mayoría los productos afectados en el 2015 repiten nuevamente en el 2016, solo se registraron algunas variaciones entre ellos.



Fuente: MITRE

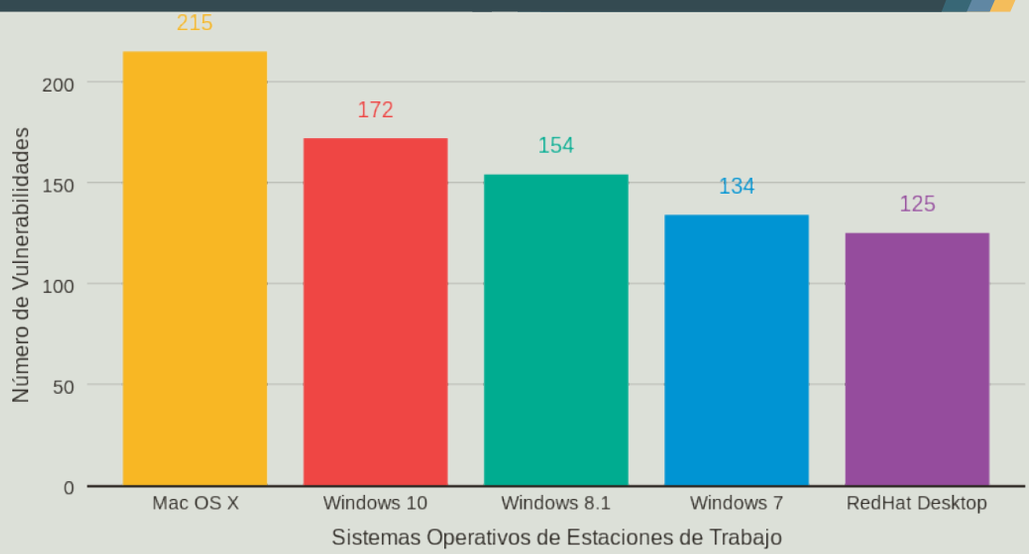
TOP 5 PARA USUARIOS

TOP 5 NAVEGADORES MÁS VULNERABLES EN EL 2016



Fuente: MITRE

TOP 5 SISTEMAS OPERATIVOS MÁS VULNERABLES EN EL 2016

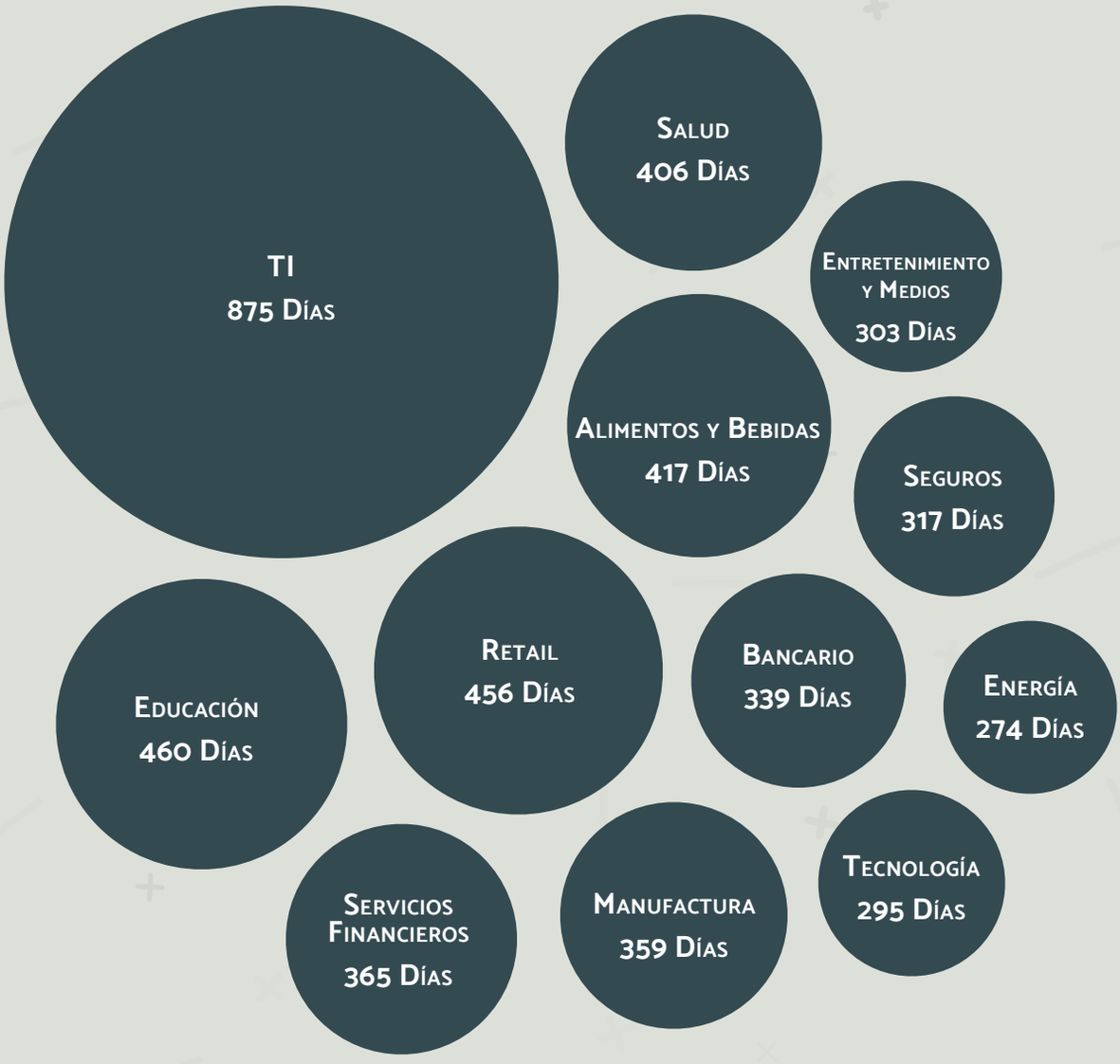


Fuente: MITRE

Promedio de tiempo de exposición de vulnerabilidades por sector

Los datos muestran que las vulnerabilidades permanecen abiertas durante mucho tiempo. Las vulnerabilidades críticas y de alto riesgo tienen un promedio de exposición entre 300 y 500 días, respectivamente.

La edad promedio de vulnerabilidades en diferentes industrias es similar. El sector de tecnología de la información (TI) es una excepción con el promedio más alto de 875 días.



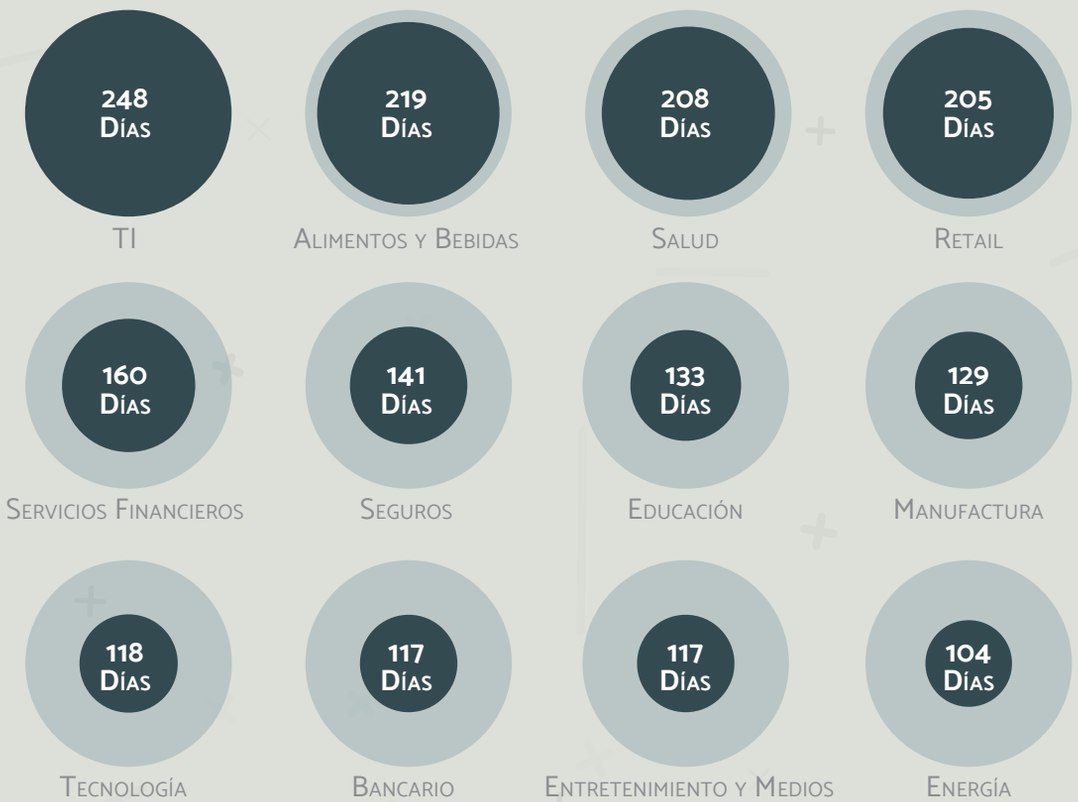
Fuente: WhiteHat Security

Promedio de tiempo de corrección por sector

Una vez encontradas las vulnerabilidades y los equipos de seguridad proponen solucionarlas, ¿en cuánto tiempo implementarán las correcciones?. El promedio de tiempo de corrección varía por industria aproximadamente de 100 días a 245 días.

El promedio de tiempo de corrección en los sectores de Retail y Salud es de alrededor de 200 días. Una vez más, el sector TI viene en aumento al abordar las vulnerabilidades con un tiempo promedio de reparación de aproximadamente 248 días.

Industrias altamente reguladas como Salud, Banca y Servicios Financieros cuentan con números muy altos de vulnerabilidades encontradas. Sin embargo tienen menores tasas de remediación (vulnerabilidades solucionadas del total de vulnerabilidades conocidas) en comparación con otros sectores.



Fuente: WhiteHat Security

Resumen de noticias más importantes en el 2016

Enero

- Se conoce que el causante de un apagón que dejó a más de medio millón de ucranianos sin energía eléctrica durante unas horas, fue un malware que afectó a varias centrales eléctricas del país.

- Mozilla publica Firefox 44 y corrige 17 nuevas vulnerabilidades, mientras que Oracle corrige un total de 248 vulnerabilidades diferentes en múltiples productos incluyendo Oracle Database hasta Solaris, Java o MySQL.

Febrero

- El Banco Central de Bangladesh sufre el robo de 100 millones de dólares.

- Dentro de su ciclo habitual de actualizaciones Microsoft publica 13 boletines de seguridad, que solucionan 67 vulnerabilidades. Adobe publica actualizaciones para Flash Player, Photoshop, Connect y Experience Manager, se solucionan 32 vulnerabilidades.

Marzo

- Se anuncia la vulnerabilidad DROWN CVE-2016-0800 que podría permitir a un atacante descifrar comunicaciones seguras con relativa sencillez.

- Se filtraron los datos de 93 millones de ciudadanos mexicanos, incluyendo la dirección postal, fecha y lugar de nacimiento. Esta brecha de seguridad se debió a una mala configuración de la base de datos MongoDB por parte del Instituto Nacional Electoral de México.

Abril

- El Sistema Internacional de Transferencias (SWIFT) atacado por malware.

- Adobe confirma la existencia de un 0-day en Flash Player que se está explotando en sistemas con Windows 10 (y anteriores), pocos días después lo soluciona junto con otras 23 vulnerabilidades que afectan al popular reproductor.

Mayo

- Banco ecuatoriano sufre el robo de $12M a través del sistema SWIFT.
- Panama Papers: Filtración de documentos confidenciales de la firma de abogados panameña Mossack Fonseca, revelando así el ocultamiento de propiedades de empresas, activos, ganancias y evasión tributaria de jefes de Estado y de gobierno, líderes de la política mundial, personas políticamente expuestas y personalidades de las finanzas, negocios, deportes y arte.

Junio

- Ether, una criptomoneda alternativa a bitcoin, ha sufrido el robo al equivalente de unos 50 millones de dólares.
- Mozilla publica Firefox 47 y corrige 14 nuevas vulnerabilidades. Dentro de su ciclo habitual de actualizaciones Microsoft publica 16 boletines de seguridad, que solucionan 36 vulnerabilidades.Adobe publica seis boletines de seguridad para anunciar actualizaciones que solucionan 43 vulnerabilidades en Flash (incluido un 0day), DNG Software Development Kit (SDK), Brackets, Creative Cloud Desktop Application, Cold Fusion y Adobe AIR.

Julio

- Entre las vulnerabilidades corregidas por Microsoft en sus boletines se incluye una actualización para los componentes del servicio de cola de impresión de Windows, existente en todos los Windows desde hace más de 20 años y que puede permitir la propagación de malware en una red.
- Se ha publicado el robo de 119.756 bitcoin, valorados en unos 64 millones de dólares, de la plataforma de intercambio Bitfinex (Hong Kong), el mayor operador mundial de intercambio de bitcoin basado dólares.

Agosto

- Investigadores de Check Point presentan un conjunto de cuatro nuevas vulnerabilidades, bautizadas como QuadRooter, que afectan a prácticamente todos los dispositivos del ecosistema Android. Hasta 900 millones de teléfonos y tabletas podrían verse afectados.
- Sale a la luz material de exploits usado por Equation Group, grupo vinculado supuestamente a la NSA. Todo son especulaciones sobre el origen de la información filtrada y la que supuestamente queda por exponer. Lo que es cierto es que se incluyen varios 0days que afectan a dispositivos Cisco y Fortinet.

Septiembre

- Investigadores de FireEye detectan una nueva muestra de malware para cajeros bancarios, que bajo el nombre de Ripper parece ser el culpable del robo de 12 millones de baths (algo más de 310.000 euros) de cajeros en Tailandia.
- Google ofrece detalles sobre las características de seguridad de la última versión de Android 7.0, también conocido como Nougat.

Octubre

- El servicio de gestión de DNS de la proveedora Dyn sufrió varios ataques de DDoS que lograron afectar e incluso interrumpir el servicio de sitios tan relevantes como New York Times, Reddit, Twitter, Spotify, eBay, Netflix o CNN.
- Google soluciona 78 vulnerabilidades en Android. Dentro de su ciclo habitual de actualizaciones Microsoft publica 10 boletines de seguridad, que solucionan 36 vulnerabilidades, incluidos cinco 0-days. Google publica Chrome 54 y corrige 21 vulnerabilidades. Oracle publica parches para 253 vulnerabilidades diferentes en múltiples productos pertenecientes a diferentes familias, que van desde el popular gestor de base de datos Oracle Database hasta Solaris, Java o MySQL.

Noviembre

- Se anuncia que el troyano bancario TrickBot empieza a afectar a bancos de la Unión Europea, incluyendo bancos irlandeses británicos y alemanes.
- Dentro de su ciclo habitual de actualizaciones Microsoft publica 14 boletines de seguridad, que solucionan 68 vulnerabilidades, incluidos dos 0-day. La habitual actualización para Adobe Flash Player en esta ocasión soluciona nueve vulnerabilidades. La Fundación Mozilla anuncia la publicación de la versión 50 de Firefox que corrige 28 vulnerabilidades.

Diciembre

- Confirmado el robo de los datos de 1.000 millones de cuentas de Yahoo.
- Check Point anuncia una nueva campaña de malware que, bajo el nombre de Gooligan, ha comprometido más de un millón de cuentas de Google, y continúa creciendo a un ritmo de 13.000 dispositivos infectados al día.

Fuente:Una al día

Reporte del mercado de ciberseguridad

Cybersecurity Ventures predice que los costos anuales de la ciberdelincuencia a nivel mundial crecerán de $ 3 trillones de dólares en 2015 a $ 6 trillones de dólares anuales para 2021, lo que incluye daños y destrucción de datos, dinero robado, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, malversación de fondos, la interrupción posterior al ataque en el curso normal de los negocios, la investigación forense, la restauración y eliminación de datos y sistemas infectados, y el daño a la reputación.

Se calcula que el gasto mundial en productos y servicios de seguridad cibernética para la defensa contra el cibercrimen superará $ 1 trillón de dólares en los próximos cinco años, de 2017 a 2021, según el Cybersecurity Market Report, publicado trimestralmente por Cybersecurity Ventures.

Hay algunas corporaciones que se han presentado con mayores presupuestos de ciberseguridad, JP Morgan Chase & Co. duplicó su presupuesto anual de ciberseguridad de $ 250 millones a $ 500 millones de dólares, mientras que Bank of America ha declarado que tiene un presupuesto ilimitado cuando se trata de combatir el delito cibernético. El gobierno de Estados Unidos ha aumentado su presupuesto anual de ciberseguridad en un 35%, pasando de $ 14.000 millones de dólares presupuestados en 2016 a $ 19.000 millones de dólares en 2017 .

Las actividades de seguridad atraviesan muchas áreas de negocios y en la actualidad la mayoría de las organizaciones intentan doblar sus presupuestos de seguridad.

Esto sin dudas son señales importantes en estos tiempos donde la preocupación en materia de ciberseguridad no pareciera tener un fin. Aumentos incrementales en el gasto en ciberseguridad no son suficientes. Esperamos que las empresas de todos los tamaños y los gobiernos a nivel mundial cobren conciencia.

84%

DE TODOS LOS CYBERATAQUES APROVECHAN VULNERABILIDADES COMUNES

En *HowlerMonkey.io* podrás consultar las vulnerabilidades de los productos que usas en tu plataforma tecnológica, y así poder tener la información necesaria para mitigarlas.

Ten otra postura, hazle frente a los ciberataques desde un enfoque preventivo y no seas una víctima más.

2016

howlermonkey

howlermonkey.io