Eleven Paths

Informe sobre el estado de la seguridad 2020 H2

Desde la seguridad en móviles hasta el análisis de vulnerabilidades, desde las noticias más relevantes hasta el análisis de la privacidad, comprende los riesgos del panorama actual

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

ElevenPaths

ÍNDICE

El objetivo de este informe es sintetizar la información sobre ciberseguridad de los últimos meses (desde la seguridad en móviles hasta las noticias más relevantes y las vulnerabilidades más habituales), adoptando un punto de vista que abarque la mayoría de los aspectos de esta disciplina, para así ayudar al lector a comprender los riesgos del panorama actual.

El segundo semestre de 2020 se ha visto también marcado en el ámbito de la ciberseguridad por el mismo evento que ha sacudido al mundo entero: la aparición y efectos causados por el SARS-CoV-2. Por ejemplo, hemos podido observar **ataques a las infraestructuras informáticas en las que se sostenían el desarrollo de vacunas.**

En el mundo de las vulnerabilidades, dos de ellas han protagonizado los últimos meses. Por un lado, ZeroLogon, que ha permitido atacar a Windows de forma muy sencilla. Por otro, ha cobrado especial protagonismo el fallo en el producto de SolarWinds que se descubrió finalmente como culpable del ataque a decenas de compañías y organizaciones, FireEye incluida. La cadena de suministro es la palabra de moda. Como siempre, volvemos a las raíces. **¿Podemos controlar todos y cada uno de los puntos en los que confiamos para sostener nuestra infraestructura?**

Y hablando de infraestructura, SADDNS nos recuerda lo sencillo que puede ser atacar a una piedra angular de la red... el DNS. Como ya ocurrió en 2008 con el fallo de Kaminsky, el sistema operativo y el servicio en este caso permitían en conjunto envenenar las cachés de respuesta y redirigir a una víctima. **Un fallo ingenioso que nos recordaba, por enésima vez, la necesidad de reforzar el protocolo DNS con otros métodos de seguridad más robustos.**

Tanto si se es aficionado como profesional, es importante ser capaz de seguir el ritmo de las noticias relevantes sobre ciberseguridad: ¿qué es lo más relevante que está pasando? ¿Cuál es el panorama actual? El lector dispondrá con este informe de una herramienta para comprender el estado de la seguridad desde diferentes perspectivas, y podrá conocer su estado actual y proyectar posibles tendencias a corto plazo. La información recogida se basa en buena parte en la recopilación y síntesis de datos internos, contrastados con información pública de fuentes que consideramos de calidad. ¡Allá vamos!

LOS INCIDENTES MÁS DESTACADOS DEL SEGUNDO SEMESTRE DE 2020

A continuación, damos cuenta de aquellas noticias que mayor impacto han tenido durante el transcurso de este segundo semestre de 2020.

julio

CVE-2020-5902, vulnerabilidad del momento
Por gravedad y forma en la que se ha desarrollado el problema, desde el aviso hasta la existencia de un exploit plenamente funcional muy sencillo de lanzar con solo un comando curl. El fallo está en el TMUI de Big IP del fabricante F5. Un sistema que suele estar presentes en el perímetro de las compañías y que se utiliza con muchos fines, habitualmente críticos.

Problemas en Twitter
Twitter sufre un problema de seguridad en el que parece ser que los atacantes usaron ingeniería social con trabajadores con acceso a paneles de control que podían modificar el contenido de la cuenta de cualquier usuario. Perfiles relevantes promocionaban cuentas de bitcoin.

Protección contra los ordenadores cuánticos
El NIST anuncia los ganadores de la segunda ronda para la selección del nuevo estándar de criptografía post-cuántica: Classic McEliece, CRYSTALS-KYBER, NTRU y SABER, en las categorías de cifrado de clave pública y gestión de claves; y CRYSTALS-DILITHIUM, FALCON y Rainbow, en la categoría de firma digital.

Dos nuevos ataques contra el sistema de aguas de Israel
Los atacantes trataron de modificar los niveles de clorina del agua.

agosto

APT34 incorpora DoH
El grupo de atacantes Oilrig, también conocido como APT34, es el primero en incorporar DoH como parte de sus ataques. Algo que se preveía y que han hecho aprovechando herramientas de terceros.

Botnet Terracotta de Android
Una interesante botnet llamada Terracotta basada en Android y alojada (cómo no) en Google Play perpetraba ataques de tráfico y anuncios fraudulentos de una forma peculiar tanto en su tácticas como en sus técnicas. Consiguió en junio 2 mil millones de peticiones fraudulentas, con 65.000 teléfonos infectados.

Nueva versión de Emotet
La vacuna contra Emotet que se venía usando por investigadores deja de ser efectiva con la nueva versión del malware. Analistas descubrieron que escribía una rama del registro (codificada con XOR) para persistir. Pero también comprobaba su existencia antes de establecerla. Bastaba con crear en el sistema limpio esta rama del registro con un valor falso, y el malware tendría un desbordamiento de búfer cuando lo leyese. Dejaría de funcionar y no infectaría la máquina.

septiembre

Fallo en el Netlogon Remote Protocol
A pesar de que en agosto la vulnerabilidad se calificó como de "poco probable su explotación", ya existe una prueba de concepto para aprovechar el fallo conocido como ZeroLogon. Permite que cualquier usuario se haga con el control de la red interna de un sistema solo con tener acceso al controlador de dominio. Ya son cuatro las pruebas de concepto de CVE-2020-1472 que permiten aprovechar el fallo en el Netlogon Remote Protocol.

Fallo en Firefox para Android
Firefox para Android en su versión anterior a la 80 sufre un fallo de seguridad muy fácil de explotar. Permite a un atacante en la misma red WiFi abrir arbitrariamente cualquier URL en el navegador de la víctima, sin que esta deba generar ninguna acción, basta con estar en la misma red y que la víctima esté ejecutando Firefox.

Filtrado el código fuente de Windows XP
No es el único. En mayo de 2020 se filtró el código de la Xbox original y NT 3.5; en 2017, algunas partes de Windows 10; y en 2004, algunas partes de NT y 2000. El fichero más llamativo es Nt5src.7z, de 2,4 Gbs. Contiene el código del kernel 5 (compartido por 2003 y XP).

Irán identifica a los saboteadores de Natanz
Irán afirma haber identificado a los responsables de la explosión en la planta nuclear de Natanz el pasado 2 de julio.

octubre

Microsoft permite deshabilitar JScript en Internet Explorer 11
Con la actualización de octubre, Microsoft incluye una entrada en el registro que deshabilita JScript en Internet Explorer 11 para aquellos que sigan usándolo. Algo que siempre debió poder hacerse a través de la configuración de zonas de seguridad, pero que solo ahora es posible.

Solucionados fallos graves en Chrome
Lo difícil en Chrome no es encontrar vulnerabilidades sino convertirlas en algo útil. Y para ello es necesario eludir su sandbox, siempre un reto. Tras el fallo en FreeType que afectaba a Chrome y descubierto en septiembre, se soluciona CVE-2020-17087 en el driver Windows Kernel Cryptography (cng.sys) que en combinación con el fallo en Chrome estaba siendo usado por atacantes.

noviembre

Ataque SAD DNS
Se hace público un ataque apodado SAD DNS que permite envenenar la caché de los resolverdores DNS. Para poder falsear una petición DNS y devolverle al cliente una mentira, el cliente debe saber el TxID (transaction ID) y el puerto origen UDP. Esto suponía una entropía de 32 bits (adivinar dos campos de 16 bits). SAD DNS consiste en inferir el puerto UDP a través de un ingenioso método que se vale de los mensajes de vuelta de error ICMP. Esto deja de nuevo una entropía de 16 bits, asumible para un ataque.

Polémica en MacOS y la revocación de certificados
Se abre una polémica por la privacidad de MacOS y su intento de comprobar a través de OCSP si un certificado ha sido revocado. No es para tanto, según nuestros análisis, aunque Apple termina modificando alguna de sus políticas de acceso a información.

50.000 direcciones IP de dispositivos VPN de Fortinet vulnerables
Se hacen públicas casi 50.000 direcciones IP de dispositivos VPN de Fortinet vulnerables al fallo CVE-2018-13379 que había aparecido poco antes.

diciembre

Pfizer revela que el ciberataque a la Agencia Europea del medicamento, EMA, consigue acceder a información sobre la vacuna
Tanto las entidades como la agencia reconocen la intrusión y que los datos se encontraban en el servidor de la EMA.

Un ciberataque compromete a SolarWinds
El ataque al proveedor de servicios de agencias gubernamentales norte-americanas y grandes empresas reconoce el ataque y compromiso de su herramienta "Orion". Orion es una herramienta de monitorización y administración de redes, por lo que el impacto puede haber sido inimaginable.

¿Puertas traseras en el cifrado?
El Consejo Europeo adopta una Resolución sobre el cifrado en la que destaca la necesidad de que se garantice la seguridad a pesar del cifrado. El Consejo observa la necesidad de que se vele por que las fuerzas o cuerpos de seguridad y las autoridades judiciales competentes puedan ejercer sus facultades legítimas, tanto en línea como fuera de línea para proteger a la ciudadanía.

MÓVILES

Apple iOS

Noticias destacables

Ya tenemos iOS 14. Tras su anuncio en la conferencia de desarrolladores de Apple de finales de junio, el 16 de septiembre fue liberada la decimocuarta versión del sistema operativo móvil de la firma de Cupertino.

A los pocos días (aunque suele ser habitual) le siguió una revisión sin parches de seguridad. De hecho, la primera actualización que corregía agujeros de seguridad fue la 14.2, publicada el 5 de noviembre. Contenía más de veinte correcciones, muchas de ellas solventado vulnerabilidades de ejecución de código arbitrario, además de elevación de privilegios o relevación de información sensible.

Para finalizar el año, Apple liberó una nueva versión, la 14.3, el 14 de diciembre que corregía más de diez vulnerabilidades. Casi la mitad fallos que podrían permitir la ejecución de código arbitrario en caso de ser explotadas.

Muy reseñable, por su especial peligrosidad, es la vulnerabilidad que fue corregida a principios de este año (y cuyos detalles fueron publicados a principios de diciembre) **y que permitía ejecutar código arbitrario a través de AWDL (Apple Wireless Direct Link)** más conocido por su uso en AirDrop.

Descubierta por Ian Beer, de Project Zero (Google), la vulnerabilidad no se dio a conocer en su momento por la peligrosidad (podría desencadenar una infección masiva, al no requerir intervención del usuario). Una vez revelados los detalles y **la espectacular prueba de concepto, podemos alcanzar a ver lo que podría suceder si una vulnerabilidad de este calado fuese liberada públicamente o descubierta por atacantes.**

iOS 14: Novedades en seguridad

A partir de iOS 14, cuando una aplicación con los respectivos permisos use la cámara o el micrófono, el sistema indicará dicho uso mostrando un pequeño punto en la esquina superior derecha de la pantalla. **Verde cuando se esté usando cualquiera de las cámaras y naranja para el micrófono.**

Se añade un permiso adicional cuando una aplicación necesite usar la geolocalización. Ahora se podrá seleccionar que se solicite explícitamente permiso cada vez que se requiera tal uso. Además, se podrá controlar si la geolocalización se hace de forma precisa o aproximada.

El acceso a fotos también se ve mejorado en cuanto a granularidad de permisos. **Ahora podremos seleccionar a qué fotos exactamente puede acceder una aplicación y no todas las almacenadas.**

Respecto a las contraseñas que almacena iOS 14, el sistema nos señalará cuáles de ellas son consideradas inseguras debido a causas como haber sido halladas en robos de información o ya de por si débiles.

Una característica muy interesante, que ya se anunció en su día, **es la aleatorización parcial de la dirección MAC del dispositivo cuando este se conecta a nuevas redes WIFI.** Esta interesante opción permite que no se haga un seguimiento del dispositivo cuando se conecta, por ejemplo, a redes WIFI públicas. El hecho de cambiar la dirección MAC es un desafío a los sistemas de tracking que usan cualquier identificador posible para realizar un perfil del usuario.

Otra mejora sustancial respecto a la privacidad es la inclusión de un mensaje en la parte superior de la pantalla cuando una aplicación usa el portapapeles si este posee datos de otra aplicación. De este modo, el sistema avisa al usuario cuando una aplicación está accediendo a posibles datos sensibles a través del portapapeles.

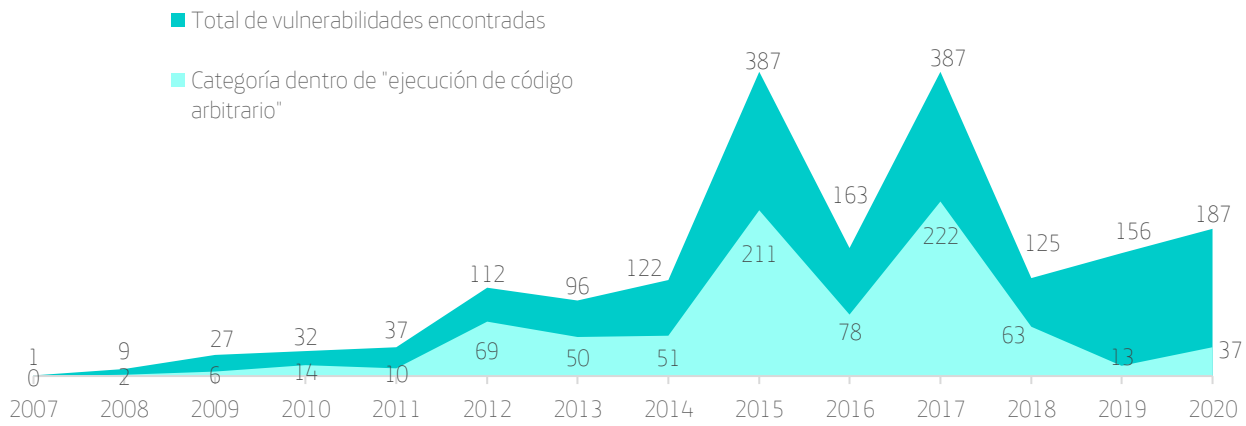
Evolución de vulnerabilidades en iOS durante el segundo semestre de 2020

Un exploit que garantice la ejecución remota de código arbitrario en iOS se sigue cotizando a dos millones de dólares.

El 2020 se ha cerrado con 187 vulnerabilidades parcheadas en el sistema operativo iOS, de las cuales, 37 son consideradas de alto riesgo, con posibilidad de ejecutar código arbitrario. Algunas de ellas afectan al propio núcleo del sistema.

VULNERABILIDADES EN IOS 2020-H2

Evolución de vulnerabilidades por año



Fragmentación de versiones durante el segundo semestre de 2020

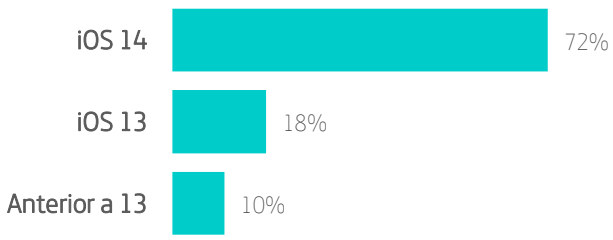
Como es tradición, la fragmentación nunca ha sido un problema para los desarrolladores de iOS. La ventaja de contar con una plataforma homogénea es incontestable y continúa arrojando cifras casi calcadas cada vez que revisamos la adopción por parte de los usuarios de iPhone de una nueva versión del sistema operativo.

Si el pasado semestre iOS 13 alcanzaba el 70% de dispositivos, seis meses después iOS 14 reemplaza al 13 y se coloca en primera plaza con una cuota del 72%, subiendo al 81% si contamos solo los dispositivos con menos de cuatro años. Como es habitual, el sistema operativo saliente se coloca a una discreta, aunque significativa, segunda plaza con un 18%. En ese mismo lugar estuvo iOS 12 con un 23% seis meses antes.

Además, iOS 14 seguirá siendo soportado desde los modelos de iPhone 6s y SE, terminales con cinco años de antigüedad en sus espaldas. Un tiempo considerable de longevidad en las plataformas móviles.

FRAGMENTACIÓN EN APPLE IOS 2020-H2

Según datos de la App Store del 15 de diciembre



Informe de Transparencia de Apple

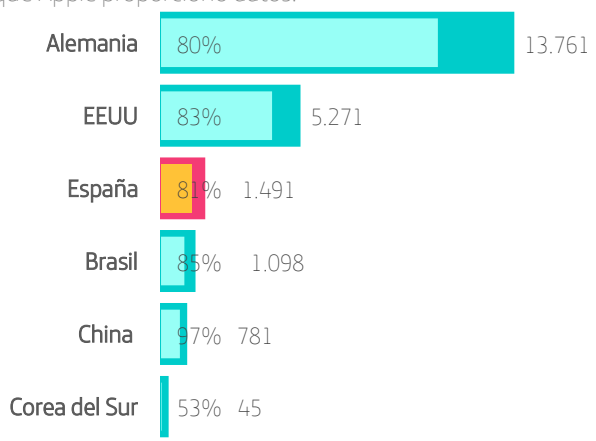
En ocasiones, los gobiernos necesitan apoyarse en las grandes corporaciones para poder llevar a cabo su trabajo. Cuando una amenaza pasa por conocer la identidad o tener acceso a los datos de un potencial atacante o de una víctima en peligro, la información digital que almacenan estas empresas puede resultar vital para la investigación y evitar una catástrofe. Apple publica semestralmente un completo informe sobre qué datos le piden los gobiernos, cuáles y en qué medida las peticiones se satisfacen. **Repasamos aquí algunos datos que hemos recopilado sobre las actividades y peticiones de los gobiernos a la compañía.**

Peticiones basadas en dispositivos

Representa **peticiones de agencias gubernamentales solicitando información de dispositivos Apple, como número de serie o número IMEI**. Por ejemplo, cuando las fuerzas del orden actúan en nombre de clientes a los que han robado el dispositivo o lo han perdido. También recibe peticiones relacionadas con investigaciones de fraude: solicitan normalmente detalles de los clientes de Apple asociados a dispositivos o conexiones a servicios de Apple.

ALEMANIA ES LA QUE MÁS PETICIONES SOBRE DISPOSITIVOS HA SOLICITADO

Peticiones basadas en dipositivos y % para las que Apple proporcionó datos.

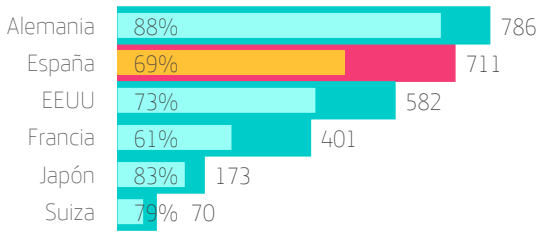


Peticiones basadas en datos financieros

Se producen estas peticiones cuando las fuerzas del orden actúan en nombre de clientes que requieren asistencia relacionada **con actividad fraudulenta de tarjetas de crédito o tarjetas regalo que se han usado para comprar productos de Apple.**

ESPAÑA ES EL SEGUNDO GOBIERNO QUE MÁS SOLICITUDES DE INFORMACIÓN POR FRAUDE HA SOLICITADO

Peticiones basadas en datos financieros y % para las que Apple proporcionó datos.

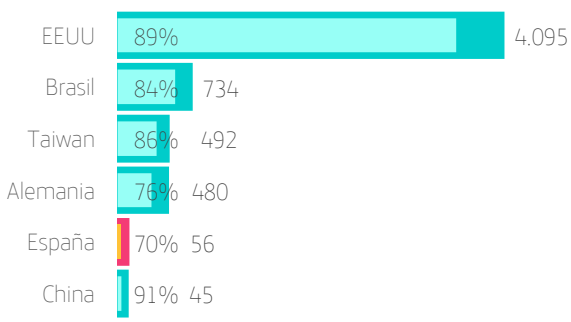


Peticiones basadas en cuentas

Se realizan **peticiones a Apple relacionadas con cuentas que pueden haber sido usadas en contra de la ley y términos de uso de Apple**. Se trata de cuentas de iCloud o iTunes y su nombre, dirección e incluso contenido en la nube (backup, fotos, contactos...).

EEUU ES, CON DIFERENICA, EL PAÍS QUE MÁS SOLICITUDES DE INFORMACIÓN DE CUENTA HA SOLICITADO

Peticiones basadas en cuentas y % para las que Apple proporcionó datos.

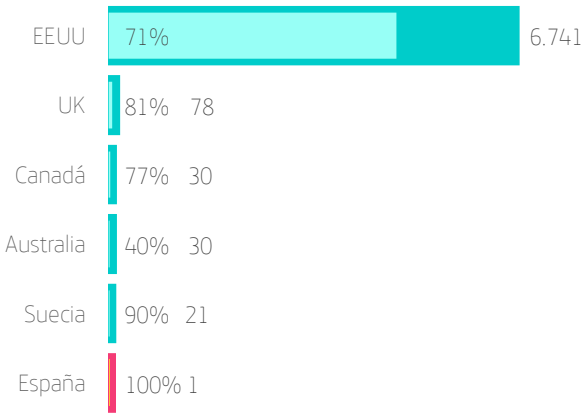


Peticiones relacionadas con la preservación de cuentas

Bajo el contexto de la U.S. Electronic Communications Privacy Act (ECPA), se puede solicitar a Apple que "congele" los datos de una cuenta y los mantenga desde 90 a 180 días. Este es un paso previo a petición de acceso a la cuenta, en espera de que se obtenga el permiso legal para solicitar datos y para evitar que la cuenta sea borrada por el investigado.

EEUU ES EL PAÍS CON MÁS SOLICITUDES DE PRESERVACIÓN DE CUENTAS

Peticiones relacionadas con la preservación de cuentas y % para las que Apple las preservó.

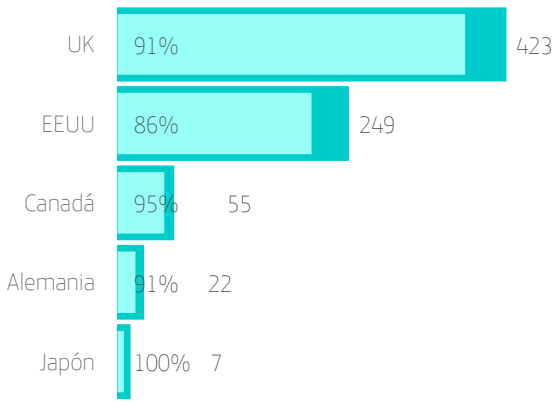


Peticiones por emergencias

También amparados bajo la U.S. Electronic Communications Privacy Act (ECPA), es posible solicitar a Apple que **proporcione datos privados de cuentas si en situaciones de emergencia se cree que esto puede evitar un peligro de muerte o daño serio a individuos.**

UK ES EL PAÍS QUE MÁS PETICIONES DE ACCESO A CUENTAS POR EMERGENCIA SOLICITA

Peticiones por emergencias y % para las que Apple proporcionó datos.

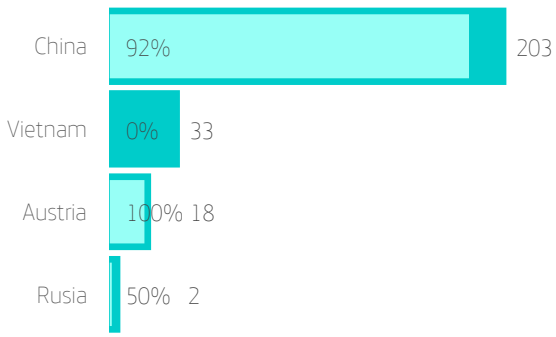


Peticiones relacionadas con la retirada de apps del market

Habitualmente tiene que ver con apps que se supone violan la ley.

CHINA SOLICITÓ 203 RETIRADAS DE APPS DEL MARKET

Peticiones de eliminación de apps y % para las que Apple proporcionó datos.



Conclusiones

Podríamos concluir que ciertos gobiernos solicitan «demasiado a menudo» acceso a datos, pero también argumentar que puede ocurrir que la Justicia funcione de manera más ágil en ellos, o que el fraude se base más en estas localizaciones. La interpretación es libre. Lo que sí parecen claras son algunas conclusiones basadas en los datos:

- El gobierno alemán es el que más solicitudes ha generado para obtener información sobre dispositivos y también para obtener información sobre potenciales fraudes.
- Estados Unidos solicita con diferencia más que cualquier otro país la preservación de cuentas y el acceso a los datos alojados en ella.
- Como de costumbre, China es el país que más retirada de apps solicita en el App Store.

Aclaración: en este ejercicio hemos representado en gráficas las tablas que publica la propia Apple. Es importante especificar que todas las peticiones se realizan por lotes. Por ejemplo, Apple contabiliza el número de peticiones de retirada de apps, y a su vez cada petición puede contener un número indeterminado de apps en ellas. Igual con las peticiones de cuentas y el número de cuentas en cada petición. Cuando Apple habla del porcentaje de peticiones satisfechas, habla de eso, de peticiones, pero no de cuentas concretas. Por ejemplo: Apple recibe 10 peticiones, con 100 cuentas entre todas las peticiones y luego dice que ha satisfecho el 90% de las peticiones, no sabemos cuántas cuentas individuales se le han proporcionado. Sin embargo, en las gráficas hemos contrastado números totales contra ese porcentaje. Es un ejercicio que si bien no es exacto, puede aportarnos una idea aproximada de la cantidad real de datos proporcionados.

Android

Noticias destacables

La noticia más relevante sin duda es el estreno de la versión 11 del sistema operativo móvil de Google, Android. El 8 de septiembre se liberó la esperada nueva iteración. Android 11 trae nuevas características de seguridad y privacidad. **Una de las más llamativas es la inclusión de permisos "de un solo uso"**. Una opción muy esperada y reclamada que permite a los usuarios dar permisos a las aplicaciones cuando soliciten acceder a un recurso del sistema. Es decir, el sistema preguntará al usuario cada vez que una aplicación intente acceder a la cámara o a las fotos, por ejemplo. Aunque esto pueda parecer engorroso para las aplicaciones en las que confiamos (en ese caso se podrá optar por permitir su uso siempre o cuando se use la aplicación) es una opción muy útil y razonable cuando estamos usando una aplicación de la que no se termina de confiar plenamente.

Se ha mejorado la compartimentalización del almacenamiento masivo, que permitirá a las aplicaciones acceder a este recurso de manera que no puedan tener permisos sobre los recursos de otra aplicación. Es decir, **permitir el acceso al almacenamiento no implicará que una aplicación pueda campar a sus anchas por todos los archivos del soporte.**

Otra de las opciones que nos permitirán mejorar nuestra exposición de datos personales es que el permiso para obtener la geolocalización cuando una aplicación está en segundo plano deberá ser explicito. Es decir, en vez de aprobar el permiso cuando se esté instalando la aplicación, el usuario deberá acceder al menú de la aplicación y desde ese lugar aprobar este tipo de uso.

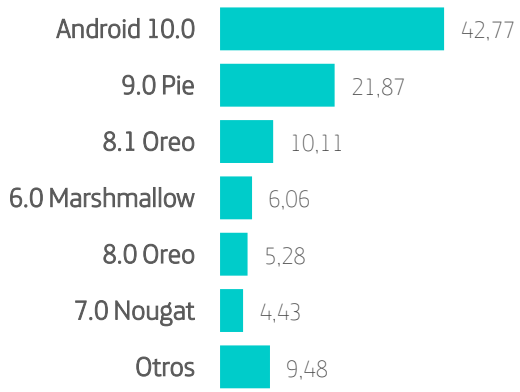
Respecto a los boletines de seguridad, Android puntualmente publica uno cada mes con información detallada respecto a los componentes afectados, gravedad e incluso en algunos casos, referencias directas al parche aplicado en la corrección de la vulnerabilidad. En total, se han corregido algo más de 250 vulnerabilidades de distinta gravedad y en diferentes componentes así como de fabricantes (MediaTek, Qualcomm, Broadcom, etc.).

Fragmentación en sistemas Android

Android no publica estadísticas en el portal de desarrolladores que muestren el estado de fragmentación entre versiones. Los datos obtenidos pertenecen a fuentes públicas, es decir, no están contrastados con las fuentes oficiales. No existen datos aún de la penetración en el mercado de Android 11, liberado el 8 de septiembre de este año.

La última publicación de *Statcounter* a fecha de edición de este informe nos indican que la versión más implantada de Android es la 10, con una cuota del 40%. Le sigue Android 9 con un con algo más del 22%. La porción restante se la reparten las versiones inferiores a la 9, donde ninguna supera el 10% de mercado.

FRAGMENTACIÓN EN ANDROID 2020-H2

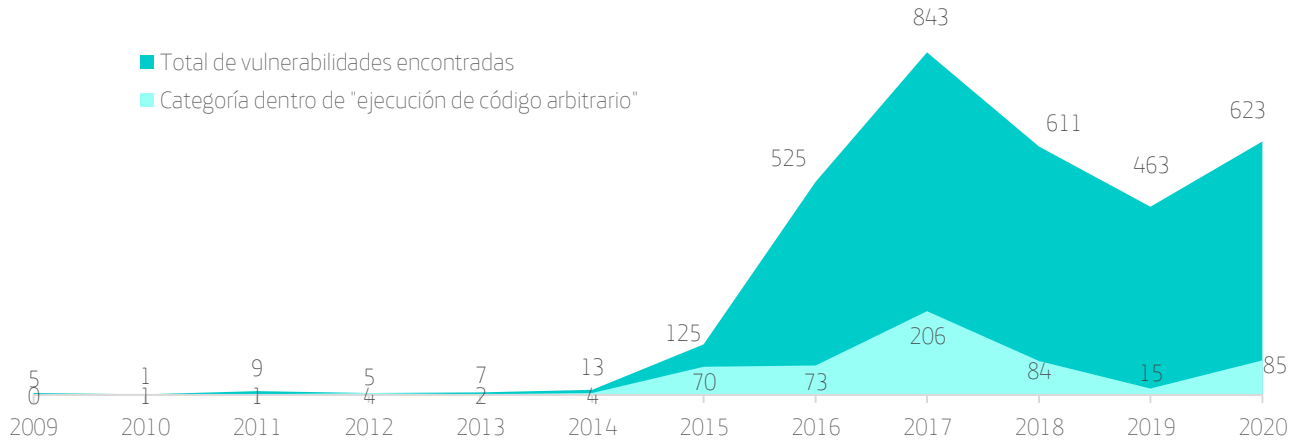


Evolución de vulnerabilidades en Android durante el segundo semestre de 2020

Un exploit que garantice la ejecución remota de código arbitrario en Android sigue cotizando a dos millones y medio de dólares. En general, **Android ha cerrado el año con 623 vulnerabilidades parcheadas, 85 de ellas consideradas de alto riesgo** dado que podrían permitir la ejecución de código arbitrario. Es necesario aportar aquí el dato de que muchos de estos fallos afectan a software de ciertos fabricantes, lo que significa que una misma vulnerabilidad no tiene por qué afectar a todo el parque de dispositivos.

VULNERABILIDADES EN ANDROID 2020-H2

Evolución de vulnerabilidades por año



VULNERABILIDADES DESTACABLES

Comentamos en esta sección algunas de las vulnerabilidades quizás no tan populares, pero notables a nuestro juicio, de este segundo semestre de 2020, es decir, aquellas que destacan por su especial relevancia o peligrosidad.

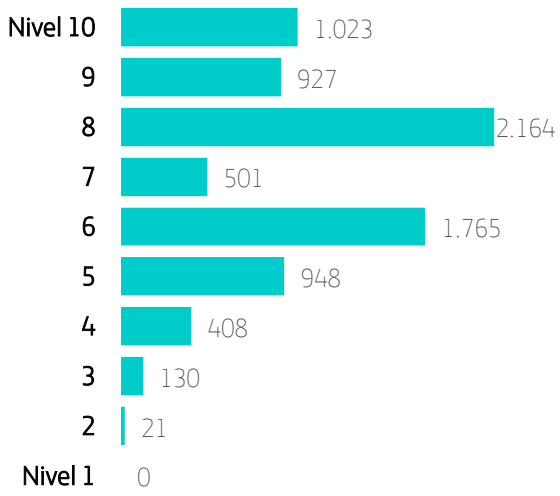
CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2020-12524	Sistemas de control industrial	Investigadores de la universidad de Birmingham han descubierto una vulnerabilidad que provoca que dispositivos como un HMI comiencen a consumir desmedidamente recursos hasta llegar a bloquearse. Teniendo en cuenta la importancia de los HMI a la hora de controlar los sistemas de control industrial a los que estén asociados esta vulnerabilidad no sólo es relevante por su calificación, sino por el potencial desastre que podría causarse si el atacante toma el control de un sistema industrial y bloquea el HMI para prevenir las primeras contramedidas o paradas del sistema.	7.5
CVE-2020-10148	SolarWinds Orion API	El fallo que se destapó tras lo que se suponía un ataque a FireEye, pero que derivó en un problema de seguridad a escala mundial. Un fallo en el control de autenticación permitía el acceso y con este problema llegaron a troyanizar el sistema que se distribuía por diferentes fabricantes y organizaciones.	9.8
Varios (Ripple20)	Pila TCP/IP	Se trata de 19 problemas de todo tipo en la implementación de la pila TCP/IP de la compañía Treck. Como esta implementación proporciona o licencia a infinidad de marcas (casi 80 identificadas) y dispositivos IoT, los afectados son, efectivamente, miles de millones. Y, por su propia naturaleza, muchos de ellos ni siquiera serán parcheados nunca. https://kb.cert.org/vuls/id/257161 Algo más tarde, en diciembre, se encontraron otros muchos fallos en las pilas TCP. https://kb.cert.org/vuls/id/815128 /	9.8
CVE-2020-1472	Directorios Activos en Windows	El problema es que se usa mal AES con el (lentísimo) modo CFB8. La función ComputeNetlogonCredential, en vez de aleatorizar los vectores de iniciación para cada byte, usa siempre un valor fijo... todo cero. El atacante envía una media de 256 intentos de bloques de ceros hasta que consigue autenticarse y en este caso la PoC deshabilita la contraseña. El problema se corregía en dos fases debido a la su complejidad para adaptarse a los diferentes escenarios.	10

Las vulnerabilidades en cifras

En números concretos de vulnerabilidades descubiertas, la distribución de CVE publicados por nivel de riesgo (*scoring* basado en CVSSv3), ha sido la siguiente:

RIESGO DE LAS VULNERABILIDADES

Distribución de vulnerabilidades por riesgo

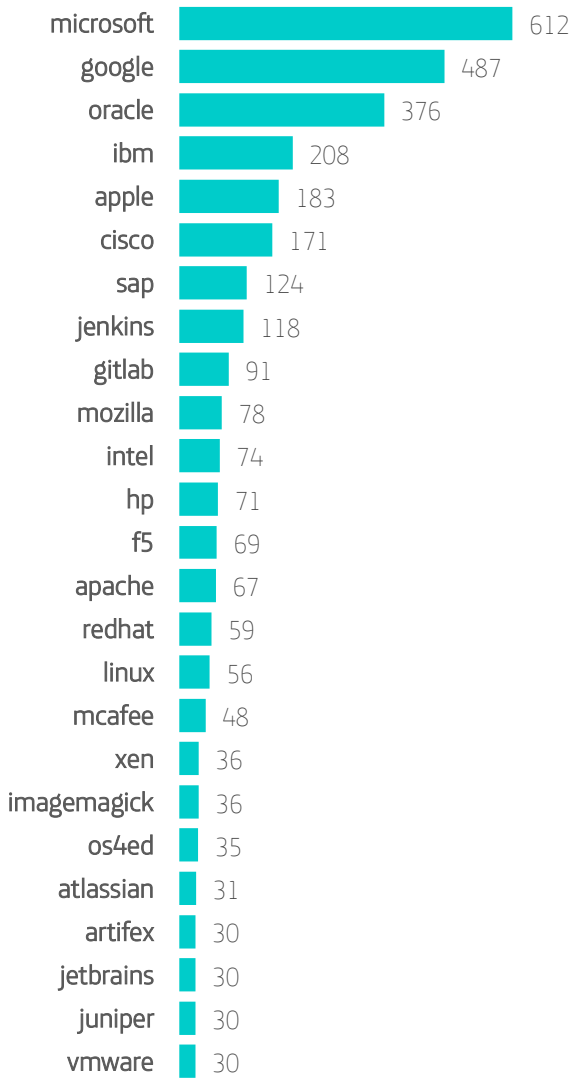


Top 25 compañías con más CVE acumulados

Durante 2020, Microsoft ha liderado por número de vulnerabilidades conocidas. La mayor parte de los meses ha superado los 100 fallos solucionados. Le siguen Google y Oracle por número en este semestre.

VULNERABILIDADES POR FABRICANTE

Top 25 fabricantes por CVE acumulados



Top 10 CWE más representativos

CWE (Common Weakness Enumeration) es una clasificación que agrupa todas las debilidades identificadas en productos informáticos. Similar al esfuerzo realizado con CVE para etiquetar las vulnerabilidades concretas, halladas por producto, CWE se centra en definir los tipos de forma abstracta. Esta definición permite realizar un mapeo directo entre CVE y CWE.

Esta lista comprende a los 10 CWE que más se han asignado por número de CVE. Esto nos permite observar qué tipo o clase de debilidades han sido más frecuentes en este periodo de estudio.

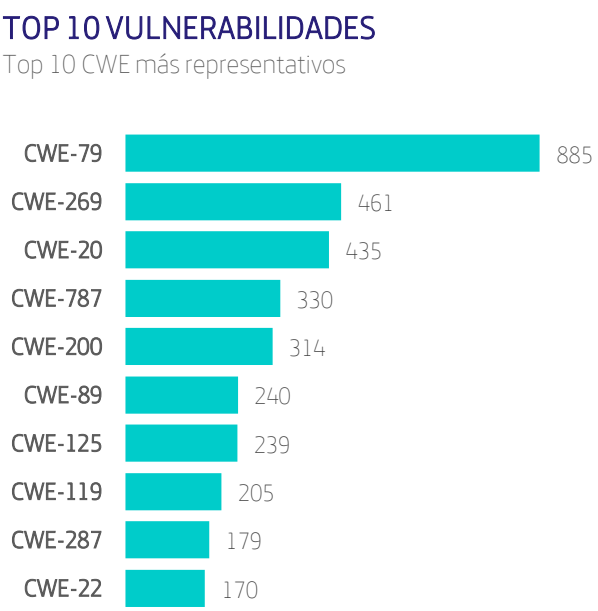


Tabla descriptiva de cada CWE

CWE	TÍTULO	DESCRIPCIÓN	CANTIDAD
CWE-79	Improper Neutralization of Input During Web Page Generation	Básicamente, recoge los tres tipos conocidos de vectores para realizar un Cross-site scripting: Reflejado, almacenado y basado en DOM.	885
CWE-269	Improper Privilege Management	La aplicación no gestiona adecuadamente los permisos y privilegios otorgados a un usuario.	461
CWE-20	Improper Input Validation	Categoría general para errores que consisten en un control deficiente o inexistente en entradas de datos procedentes de usuario.	435
CWE-787	Out-of-Bounds Write	Relacionada con CWE-125, agrupa aquellas vulnerabilidades que permiten escribir más allá de los límites designados a una región reservada de memoria intermedia.	330
CWE-200	Information Exposure	Recoge, de forma general, el compromiso de información sensible debido a la ausencia o deficiencia de controles que impidan la fuga de información.	314

CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Si no se procesan correctamente las cadenas antes de ser usadas como entrada para una base de datos, se puede modificar el estamento SQL y manipularla.	240
CWE-125	Out-of-bounds Read	Muy relacionada con CWE-119, recoge operaciones de lectura a memoria rebasando los límites de control de un búfer en concreto.	239
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	De forma general, recoge aquellos errores de programación donde no se está controlando la capacidad de un buffer de memoria, tanto en operaciones de escritura como de lectura.	205
CWE-287	Improper Authentication	Una validación pobre permite escaladas de privilegios.	179
CWE-22	Improper Limitation of a Pathname to a Restricted Directory	Es posible manipular las rutas a archivos que gestiona y usa la aplicación, posibilitando el acceso a recursos protegidos o no relacionados con el ámbito de la aplicación.	170

Conclusiones

Con respecto al semestre pasado, se cuelan en la lista CWE-89 basado en la inyección SQL, y CWE-287 que explota una autenticación pobre. Problemas de hace años que nunca terminan de desaparecer de entre las causas de las vulnerabilidades más graves conocidas.

Los primeros puestos de la lista siguen intactos en comparación con el primer semestre.

QUIÉN ES QUIÉN DESCUBRIENDO VULNERABILIDADES MICROSOFT

¿Quién encuentra más vulnerabilidades en los productos de Microsoft? **¿Qué porcentaje de vulnerabilidades son descubiertas por la propia Microsoft, empresas o brókeres de vulnerabilidades? ¿Cuántos fallos no se sabe quién los ha descubierto?** En este informe hemos analizado lo datos de los últimos tres años y medio para entender quién resuelve qué en el mundo de los productos Microsoft y la gravedad de estos fallos. Asimismo, **nos permite disponer de una visión interesante sobre quién investiga realmente los productos de Microsoft, los reporta de manera responsable, así como cuántas vulnerabilidades están acreditadas y cuántas no** (lo que podría suponer que son descubiertas por atacantes).

Cada segundo martes del mes Microsoft publica sus tradicionales parches de seguridad en un único paquete que actualiza Windows. Esa actualización resuelve una serie de CVEs o vulnerabilidades. Pero no siempre fue así. Durante muchos años se publicaron boletines que ocultaron varios CVEs, normalmente agrupados por producto.

Desde hace muchos años Microsoft viene incorporando en su política de desarrollo seguro la auditoría de su propio código con el objetivo de mejorar su seguridad. Hemos querido saber exactamente cuántos fallos de seguridad encuentra la propia compañía en sus auditorías internas, para **así hacernos una idea no solo de cuánto contribuye la propia Microsoft a la mejora de la seguridad de sus productos, sino de cuánto contribuyen también el resto de habituales *bug hunters*** de la industria.

Metodología

Hemos realizado algo muy simple. Hemos recopilado y procesado toda la información de CVEs acreditadas durante el primer semestre de 2020. La fuente de información ha sido principalmente esta página:

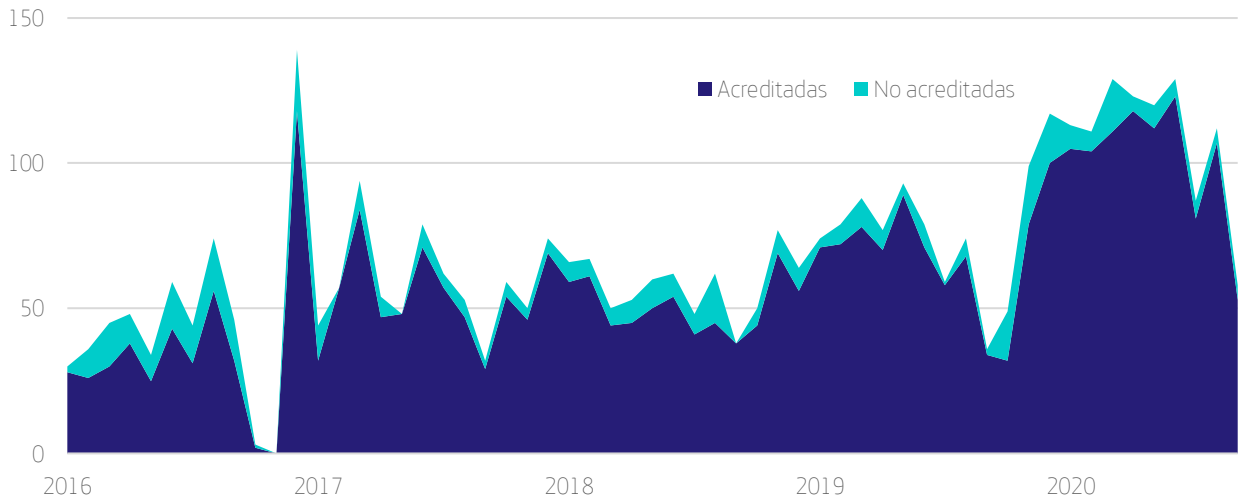
https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments

Estas son las vulnerabilidades acreditadas, esto es, reportadas por alguien identificable, ya sea particular o empresa. En este período hemos analizado 594 vulnerabilidades acreditadas. De todas ellas hemos extraído su gravedad a través del CVSS oficial del NIST.

Este número no suponen el total de fallos descubiertos (más de 600). Entendemos que la mayoría de los fallos no acreditados pueden venir de vulnerabilidades encontradas en 0-days u otras circunstancias en las que no se conoce al autor y no ha sido reportada de forma anónima. En estos casos, Microsoft no acredita a nadie en particular. Esta diferencia entre vulnerabilidades acreditadas y "no acreditadas", que no es lo mismo que anónimas, se ve reflejada en el siguiente gráfico.

NO TODAS LAS VULNERABILIDADES PROCEDEN DE FUENTES ACREDITADAS

Número de Vulnerabilidades Acreditadas y No-Acreditadas desde 2016 a 2020 H2.



De los créditos, hemos extraído la compañía que ha descubierto la vulnerabilidad. **En el caso de que sean varios los descubridores, hemos contado solo al que aparecía en primer lugar, para simplificar los cálculos** y porque entendemos que se muestra como principal analista el que las reportó en primer lugar. Si bien esto puede ser inexacto, da como resultado la fórmula más sencilla.

A partir de ahí, hemos realizado diferentes cálculos para poder analizar quién contribuye más y mejor a mejorar la seguridad de los productos Microsoft, de manera responsable.

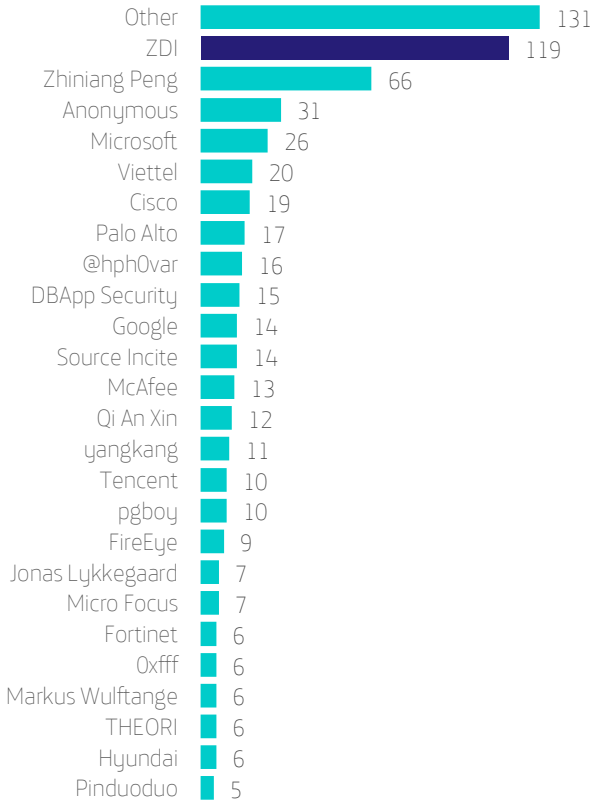
Los datos

Comparados con el semestre anterior, los datos resultan muy diferentes. La larga cola de "otros" es la que lidera la lista. Esto quiere decir que son descubiertas por investigadores con menos de 5 fallos acumulados. La iniciativa ZDI sigue siendo (cada vez más) la fórmula favorita para los investigadores. Se cuela este trimestre Zhiniang Peng como un actor muy relevante con 66 fallos.

Llama igualmente la atención que Qihoo, responsable de cientos de fallos descubiertos habitualmente, haya desaparecido por completo este semestre de la lista.

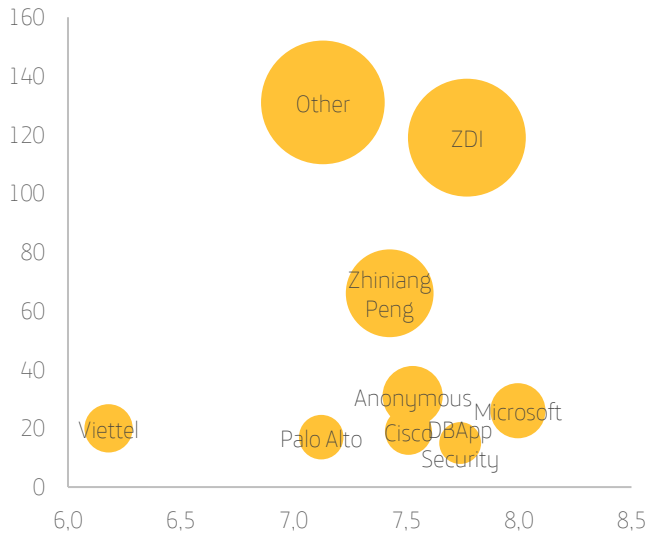
ZDI ES EL GRUPO QUE MÁS VULNERABILIDADES DESCUBRE EN PRODUCTOS DE MICROSOFT

Número total de vulnerabilidades por cada descubridor en el segundo semestre de 2020



ZDI SIGUE DESCUBRIENDO MÁS FALLOS, PERO LOS DESCUBIERTOS POR MICROSOFT SON MÁS GRAVES

Distribución de vulnerabilidades por gravedad y por descubridor; el tamaño de la burbuja es proporcional al número de vulnerabilidades descubiertas durante 2020 H2.



Conclusiones

De nuevo, de esta lista se concluye que si bien Microsoft no ha descubierto tantas vulnerabilidades como en semestres anteriores, sí que son las más graves según su CVSS.

OPERACIONES APT, GRUPOS ORGANIZADOS Y MALWARE ASOCIADO

Repasamos la actividad de los distintos grupos a los que se les atribuye la autoría de operaciones APT o campañas reseñables.

Advertimos que la atribución de este tipo de operaciones, así como la composición, origen e ideología de los grupos organizados es compleja y, necesariamente, no puede ser completamente fiable.

Esto es debido a la capacidad de anonimato y engaño inherente a este tipo de operaciones, en la que los actores pueden utilizar medios para manipular la información de modo que oculte su verdadero origen e intenciones. Incluso es posible que en determinados casos actúen con el modus operandi de otros grupos para desviar la atención o perjudicar a estos últimos.

Actividad APT notable, detectada durante el segundo semestre de 2020

Kimsuky (Aka"Velvet Chollima"): al pie del cañón

Si en el semestre anterior hablábamos de cómo este grupo "arrimaba el ascua a su sardina" utilizando el impacto del SARS-COV-2 a nivel mundial, este semestre ha vuelto a dar que hablar. En octubre, la CISA (Cybersecurity and Infrastructure Security Agency) publicaba un aviso alertando sobre el aumento de la actividad de este grupo. En este caso no fijaban un objetivo concreto, aunque sí que hacían referencia a organizaciones comerciales. Unos días más tarde, un grupo de investigadores combinó la información publicada por la CISA y la suya propia. El producto fue el descubrimiento de una suite no documentada previamente que Kimsuky utilizaba para operaciones de espionaje, así como un nuevo malware usado para evadir los análisis y para descargar *payloads* adicionales.

APT32 (Aka "OceanLotus Group"): Uncovered

Este conocido grupo ha sido "desenmascarado" (de una de sus máscaras) por Facebook. Parece que Facebook se ha metido en el papel de investigador (desde luego disponen de información para conseguirlo) y ha asociado la empresa vietnamita "CyberOne Security" con este grupo. Las TTP de este grupo incluyen la creación de sitios web falsos (y perfiles en Facebook) para engañar a los usuarios y conseguir dispersar su malware. La empresa en cuestión lo niega, aunque Facebook aseguró que tenía información sobre su infraestructura cibernética, código malicioso y otras herramientas y TTP. No obstante, no facilitó más datos amparándose en que si diera más detalles, el grupo se haría más difícil de rastrear en un futuro. Cabe recordar que la tensión entre Facebook y el gobierno vietnamita ha ido aumentando debido a que Facebook se negó en un principio a retirar publicaciones que fueran contra el gobierno. A principios de año, sin embargo, cedió a la presión y el gobierno vietnamita exigió un mayor nivel de censura, aumentando la presión con la desconexión de varios servidores de la compañía en este país.

APT36 (Aka "Mythic Leopard"): se atraen más moscas con miel que con vinagre

Este grupo pakistaní, detectado en 2013 y habitualmente relacionado con ataques a instituciones militares o gubernamentales de India, ha aumentado su actividad en el último semestre. Seleccionando a sus objetivos, desplegaban ante ellos honeytraps (perfiles falsos de mujeres atractivas) para que mordieran el anzuelo. Con este truco, han lanzado tres oleadas en las que enviaban al e-mail de los pobres ilusos que confiaban en el amor (o lo que fuera) y que no tenían reparos en abrir el documento que recibían y habilitar las macros. En ese instante se descargaba un RAT con el que podían tomar el control de la máquina atacada e intentar robar información confidencial o afectar a la infraestructura de defensa de India.

APT28 (Aka "Fancy Bear"): el oso más glamuroso ha vuelto

Fancy Bear es uno de los grupos con más solera en este ecosistema. Su referencia al oso lo sitúa en la órbita rusa, de la misma forma que los grupos con referencias a otros animales se vinculan al aparato estatal de otros países. Por ejemplo, los grupos con el apelativo "Panda" tienen que ver con... China.

En agosto se comenzó la detección de una campaña de Fancy Bear que tenía como objetivos (nada nuevo) los países de la OTAN y aquellos colaboradores con la alianza. El objetivo más claro fueron miembros concretos del gobierno de Azerbaiyán. Las muestras localizadas tenían un índice de detección bajo en los motores de antivirus. Además, más tarde se descubrió un servidor C&C activo en Francia.

Pero lo más interesante es que tras analizar el malware, los expertos de QuoIntelligence detectaron curiosas coincidencias con un ataque con malware de un supuesto nuevo grupo APT, ReconHell, hacia objetivos diplomáticos y de defensa de Bulgaria y Azerbaiyán. La dispersión de este malware se hacía a través de un documento enviado como adjunto en un e-mail. El título del documento hacía referencia a la conocida explosión del puerto de Beirut, que había sucedido **tan solo un día antes de su primera detección** y que acabó con el gobierno del Líbano dimitiendo en bloque entre protestas violentas seis días después de la explosión. El argumento de una novela de conspiraciones y geoestrategia.

RECAPITULACIÓN

En el ámbito de la seguridad para móviles, el número de vulnerabilidades en iOS sigue su tendencia al alza desde el bajón en 2018. En el marco de **Android, 2020 ha sido el segundo año con más vulnerabilidades** declaradas, tras el histórico 2017.

Respecto a las vulnerabilidades y debilidades, en la segunda parte de 2020 se ha observado un aumento considerable de vulnerabilidades de Nivel 10 de gravedad. **Los tres fabricantes con más CVE asociados siguen siendo los mismos: Microsoft, Google y Oracle.**

Respecto a las debilidades, **Con respecto al semestre pasado, se cuelan en la lista CWE-89 basado en la inyección SQL, y CWE-287 que explica una autenticación pobre.** Problemas de hace años que nunca terminan de desaparecer de entre las causas de las vulnerabilidades más graves conocidas. Los primeros puestos de la lista siguen intactos en comparación con el primer semestre.

Los grupos APT, por su parte, no han detenido su actividad. Kimsuky (Aka"Velvet Chollima") y Fancy Bear, continúan al pie del cañón, mientras que **OceanLotus Group han sido desenmascarados por parte de Facebook.**

En un semestre donde de nuevo casi todos los meses Microsoft ha rebasado las 100 vulnerabilidades solucionadas, Qihoo esta vez no aparece en la lista de fabricantes que más fallos han encontrado. **Sigue siendo ZDI la fórmula favorita para comunicar (y recompensar) los fallos graves.**

Enlaces de interés

No te quedes sólo en la capa superior del análisis de ciberseguridad, los informes semestrales son acumulativos y resumidos. En el blog de Elevenpaths tenemos mucha más información y noticias que pueden resultar de tu interés. Aquí van nuestros artículos más relevantes en el segundo semestre de 2020.

CRIPTOGRAFÍA

Retos y oportunidades de negocio de la criptografía postcuántica
El futuro de las firmas digitales para proteger tu dinero está en la criptografía con umbral
Cifrado que preserva el formato para garantizar la privacidad de datos financieros y personales
¿Eres cripto-ágil para responder con rapidez a ciberamenazas cambiantes?
Teletrabajo y pandemia: un análisis práctico respecto a la vulnerabilidad BlueKeep en España y Latinoamérica
Nonces, salts, paddings y otras hierbas aleatorias para aderezar ensaladas criptográficas

MALWARE

Conti, el ransomware más rápido del Oeste: 32 hilos de CPU en paralelo pero... ¿para qué?
El malware ClipBanker intenta detener nuestra herramienta de defensa CryptoClipWatcher
¿Qué recomiendan los criminales de la industria del ransomware para que no te afecte el ransomware?
¿Pagar cuando te infectas por ransomware? Demasiados grises

PRIVACIDAD

FaceApp y datos personales, ¿no habíamos hablado ya de esto?
Blockchain, criptomonedas, zkSTARKs y el futuro de la privacidad en un mundo descentralizado
Dime qué datos solicitas a Apple y te diré qué tipo de gobierno eres (II)
Escondiendo las claves debajo del felpudo los Gobiernos podrían garantizar la inseguridad universal

CORONAVIRUS

Ciberamenazas durante la COVID-19, una investigación de la Telco Security Alliance
Cómo protegerse de ciberataques pandémicos con herramientas gratuitas
Ciberseguridad en pandemia (I): las personas
Ciberseguridad en pandemia (II)
Análisis de APPs relacionadas con COVID19 usando Tacyt (II)
Teletrabajo y pandemia: un análisis práctico respecto a la vulnerabilidad BlueKeep en España y Latinoamérica

INTELIGENCIA ARTIFICIAL

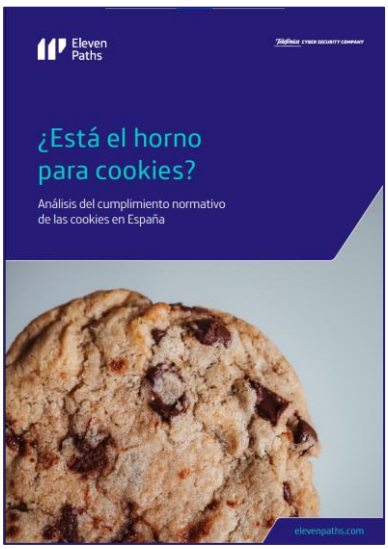
Adversarial Attacks, el enemigo de la inteligencia artificial
Adversarial Attacks, el enemigo de la inteligencia artificial II
Las primeras vulnerabilidades oficiales en Machine Learning, así, en general

Monográficos

Además, todos los años investigamos en profundidad diferentes aspectos de Ciberseguridad en nuestros informes. Este 2020 hemos analizado el comportamiento de SmartScreen en Windows y el cumplimiento normativo de las cookies.

SmartScreen es un componente de Windows Defender orientado a proteger a los usuarios contra ataques potencialmente dañinos, ya sea en forma de enlaces o ficheros. Cuando un usuario se encuentra navegando por Internet, el filtro o componente SmartScreen analiza los sitios que está visitando y, en caso de ingresar a uno considerado sospechoso, muestra un mensaje de advertencia para que el usuario decida si desea continuar o no. Pero también alerta sobre archivos descargados.

Durante los últimos meses, muchos departamentos de TI han estado ocupados realizando esta tarea de adecuación para dar **cumplimiento a la nueva normativa sobre cookies.** Cada vez que visitamos una página web nos encontramos ante un aviso que nos pregunta si queremos aceptar o (de manera casi siempre indirecta) si queremos rechazar las cookies. La mayoría de los usuarios que llegan a este mensaje buscando un servicio o una información concreta terminan aceptando todas las cookies sin conocer el impacto real en cuanto a seguridad y privacidad se refiere. ¿Cuántas cookies se aceptan habitualmente? ¿Durante cuánto tiempo? ¿Respetan las webs la nueva ley sobre cookies?



ElevenPaths

Acerca de ElevenPaths

ElevenPaths es la compañía de ciberseguridad de Telefónica, integrada dentro del holding Telefónica Tech, que aglutina los negocios digitales con mayor potencial de crecimiento de la compañía. En un mundo en el que las ciberamenazas son inevitables, como proveedores de servicios de seguridad gestionada inteligente, nos enfocamos en prevenir, detectar, dar respuesta y disminuir los posibles ataques a los que se enfrentan las empresas.

Garantizamos la ciber-resiliencia de nuestros clientes a través de un soporte 24/7 gestionado desde un i-SOC global con capacidad operativa global. Creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y, de esta manera, logramos ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Trabajamos para garantizar un entorno digital más seguro a través de alianzas estratégicas que nos permitan mejorar la seguridad de nuestros clientes, así como a través de colaboraciones con organismos y entidades líderes como la Comisión Europea, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, Europol, INCIBE, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Centro de Ciberseguridad Industrial (CCI) y APWG.