Telefónica Tech

Informe sobre el estado de la seguridad 2022 H1

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

telefonicatech.com

Índex

RESUMEN EJECUTIVO

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.

Este primer semestre de 2022 se ha caracterizado por noticias interesantes relacionadas, cómo no, con vulnerabilidades destacadas y ataques importantes. Dos de los fallos más relevantes se han dado en Office, y están relacionados con fórmulas novedosas de ejecutar código en Word o Excel. La manipulación de las llamadas a protocolos incrustados permite la ejecución de código fuera del contexto de las macros. En enero teníamos todavía problemas con CVE-2021-40444 (protocolo MSHTML) y en mayo con el denominado Follina (protocolo MSDT) que de nuevo permitía la ejecución de código.

Esto daba qué pensar sobre si las macros empezaban a quedar obsoletas como vector de ataque en favor de técnicas más sofisticadas, menos detectadas y con todavía mucho recorrido por explorar (se cree que seguirán apareciendo vulnerabilidades relacionadas con el uso de protocolos incrustados en Office). Pero curiosamente, un movimiento de Microsoft ha descartado esta idea (en contra de toda lógica). En enero se anunció que, para junio de 2022, las macros serían bloqueadas completamente para los documentos descargados de la red. Y así era. Al abrir alguno, aparecía un mensaje en rojo mucho más llamativo para intentar que los usuarios no habilitaran las macros. Pero, precisamente en julio anunciaba que revertiría el cambio. Ahora volvía el viejo y peligroso "Habilitar contenido". No ha dado más explicaciones y por tanto, las macros como vector de ataque tenían una piedra menos en su camino... hasta finales de julio, cuando de nuevo cambió de idea y las volvió a bloquear. Esperemos que para siempre.

Con respecto a los ataques importantes, llama la atención que este semestre se hayan encontrado dos fallos importantes (abril y julio) en coches de la marca Honda. Los analistas pudieron arrancar y desbloquear ciertos modelos de forma remota. Esto ha vuelto a abrir el debate sobre la ciberseguridad en entornos críticos donde un ataque permitiría arriesgar la vida de los pasajeros.

Este semestre mantenemos nuestra sección especializada en el análisis de amenazas en el ámbito industrial. Esto es posible gracias a nuestro proyecto **Aristeo**, una red de **señuelos industriales** que emplean **dispositivos OT reales** para confundir a los atacantes y extraer la información necesaria para generar inteligencia que fortalezca las defensas de nuestros clientes.

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 PRIMER SEMESTRE DE 2022

A continuación, damos cuenta de aquellas noticias que mayor impacto han tenido durante el transcurso de este primer semestre de 2022.

ENERO

- El 2 de febrero el suministrador alemán de combustible, Deutschland GmbH & Co. KG, vio como su sistema de distribución se bloqueó por un ataque contra los sistemas automatizados de carga a los camiones de suministro. El sistema no se puede operar manualmente por razones de seguridad, por lo que **la empresa no pudo hacer nada**. Este suministrador surte de combustible a la empresa con más estaciones de repostaje de toda Alemania, 2300, por lo que tuvo que comenzar a utilizar fuentes alternativas de suministro. El ataque afectó a dos subsidiarias de la empresa matriz, que descubrieron el 29 de enero que habían sido atacadas. El ataque se extendió a varias terminales petroleras, localizadas en Bélgica y Holanda.

- **PwnKit**: **escalada de privilegios local** en PolKit afecta a distribuciones Linux. La vulnerabilidad se encuentra en el componente pkexec de PolKit, un binario SUID-root con una funcionalidad similar a sudo. Presente desde 2009 ha permanecido oculta todo este tiempo a pesar de estar en la **configuración por defecto de la mayoría de las distribuciones Linux**: Ubuntu, Debian, Fedora, CentOS. Es destacable la facilidad de su explotación ya que basta con manipular variables de entorno para poder realizar un exploit y se ha constatado su explotación activa.

- **EU bug hunt**: La comisión europea, a través de la oficina de programas de código abierto ha iniciado en enero 2022, la financiación de un programa de Bug Bounty para cinco aplicaciones open source, incluyendo **LibreOffice y Mastodon**. Este movimiento se encuadra en la estrategia europea asociada al código abierto.

- Meta, en un informe de finales de diciembre de 2021 mostraba el **crecimiento de la industria de espionaje de alquiler más allá de Pegasus**. Meta ha prohibido el acceso a su plataforma a siete servicios relacionados con esta industria de espionaje y que se estima que podrían haber afectado a más de 50.000 usuarios. La evolución de esta industria con nuevos actores confirmaba al espionaje como una tendencia en 2022.

FEBRERO

- **Vulnerabilidad crítica (CVSS: 10) encontrada en SAP**. Tanto la empresa de software empresarial SAP, como la agencia estadounidense CISA lanzaron, el martes 8 de febrero, una alerta para la urgente instalación de un parche para el componente SAP ICM (Internet Communication Manager) que proporciona un servidor HTTPS al resto de componentes de SAP que requieren acceso a internet. Una búsqueda en Shodan muestra más de 5000 servidores expuestos que podrían ser vulnerables.

- **Colonial 2.0**: Las operaciones de la compañía de almacenamiento de petróleo alemana Oiltanking GmbH Group se vieron fuertemente afectadas tras un ciberataque que, en palabras de la compañía,

afectó a los sistemas IT pero no a los industriales. Debido al ataque la carga y descarga de barriles de petróleo tuvo que pasar a modo manual altamente ineficiente.

- Muchas empresas comienzan a tener políticas robustas de protección ante el **ransomware**, lo que ha llevado a sus creadores a **innovar en sus modelos de negocio**, desde la petición de rescate inicial, pasando por la doble extorsión bajo amenaza de publicación de información sensible, o el uso de ataques DDoS para "borrarlos" de internet. La nueva vuelta de tuerca, que usa Lockbit, es invitar a los atacados a facilitar datos de terceros que ayude a los ciberdelincuentes a entrar en sus redes y a su vez a rebajar su "extorsión". Lockbit, poco después seguiría innovando: introduciría en su programa de "socios" un bug bounty. Pagará a quien encuentre fallos en su software o plataformas.

- Nuevo **ataque a una plataforma de criptomonedas**, en este caso la víctima fue Wormhole y los atacantes lograron robar un estimado de 322 millones de dólares. Los ataques a estas plataformas son cada vez más frecuentes lo que denota un lucrativo negocio detrás.

- En febrero, Toyota se vio obligada a cerrar todas sus fábricas de Japón debido a un ciberataque contra uno de sus proveedores principales. El proveedor Kojima Industries, provee de piezas de plástico a la marca, lo que hace imposible seguir funcionando a las 14 plantas del mayor fabricante de vehículos del mundo. Conviene recordar que en la industria de la automoción los fabricantes no suelen almacenar componentes para muchos días, sino que ahorran costes de almacenamiento recibiendo las piezas que necesitan casi a diario. Toyota dejó de fabricar **10.000 vehículos en un solo día**.

MARZO

- **Dirty Pipe: Nueva elevación de privilegios en el kernel de Linux**. Afecta al kernel de Linux a partir de la versión 5.8 extendiéndose también a Android. Está corregido en las versiones 5.16.11, 5.15.25 y 5.10.102 **permite escalar privilegios escribiendo en archivos bloqueados para solo lectura, aprovecharla en ficheros con SetUID, etc**. Desde 2016 la función splice que permite mover datos entre ficheros, no inicializa la variable donde se almacenan las flags. Llega 2020 y se define un nuevo flag *PIPE_BUF_FLAG_CAN_MERGE*, su función es indicar los datos de un pipe de una página puedan agruparse sin necesidad de rescribir los datos en memoria. Esto, en combinación con lo anterior genera la vulnerabilidad.

- **ContiLeaks: Los papeles de Panamá del ransomware**. Tras una discrepancia aparentemente interna y política, se publicaron dos años de mensajería privada del grupo Conti. La información desvela datos muy interesantes desde un punto de vista de inteligencia: por ejemplo, alias usados que coinciden con otros previamente vistos en otros grupos de ransomware, infraestructura que pertenece al famoso troyano bancario TrickBot, contraseñas, como está organizado el grupo, etc.

- **Nueva gasolina para la propagación de la botnet Muhstik**. Se ha encontrado un fallo en la base de datos Redis bajo Debían y Ubuntu, que permite escapar de la sandbox ejecutando código LUA y así controlando el sistema. Esto suma una nueva forma propagación para esta botnet, que ya se aprovechaba de Log4Shell y la vulnerabilidad de Confluence desde diciembre y septiembre del año pasado. Muhstik se encarga de, entre otras actividades, realizar ataques de denegación de servicio distribuido.

- **La información personal de más de 800.000 estudiantes de la ciudad de Nueva York ha sido comprometida**. Se deriva de un incidente de seguridad sufrido este enero por Illuminate Education, un proveedor de plataformas de aprendizaje ampliamente usadas en dicha ciudad. Se descubre ahora que **el atacante tuvo acceso a la base de datos que almacena los perfiles de los estudiantes** conteniendo, información sobre género, información racial, información identificativa, edad o incluso información de la situación financiera familiar.

- La CISA y el FBI publicaron un aviso sobre amenazas apuntando directamente al SATCOM, el sistema internacional de comunicaciones vía satélite de los Estados Unidos. Adjuntas a ese aviso, publicaron medidas de mitigación para los proveedores de servicios, y clientes, a través de SATCOM. Estas entidades también han considerado que algunos países podrían estar utilizando ya **ataques contra infraestructura satelital** de terceros países, conjuntamente con contras acciones físicas de índole militar. Es importante recordar, además, que las redes satelitales son compartidas en muchas ocasiones, por lo que un ataque contra satélites de un país repercute directamente en otros países cercanos.

ABRIL

- **0days everywhere**: En AppleAVD (librería de decodifiación de audio y video) y la segunda en el driver gráfico de Intel. Esta tendencia no afecta solamente a Apple ni mucho menos, **Chromium** (y por tanto Edge, Chrome y Opera) se han visto afectados desde hace tiempo por una insistente campaña de ataques. Es lógico, ahora el **motor está en dos de los navegadores más usados** por lo que la rentabilidad de cada fallo se multiplica.

- Project Zero, un grupo dedicado por Google a intentar encontrar y difundir 0days publica un interesante informe. En las conclusiones de su trabajo, podemos ver que en 2021 descubrieron **58 0days, un récord muy significativo desde el comienzo de su actividad en 2014 (el anterior récord fue en 2015 con 28)**. Observamos que la práctica totalidad de esos 0days siguen prácticas ya conocidas: basándose en exploits y vulnerabilidades existentes ya para desarrollar nuevos y exploits derivados. Esto es importante, ya que si usan métodos, técnicas o procedimientos conocidos, debería ser más fácil la detección y más rápida la respuesta.

- El 5 de abril, **Kaiser Permanente**, consorcio dedicado a la prestación de servicios sanitarios con gran presencia en Estados Unidos, descubrió un robo de información médica de miles de pacientes. Aunque actuaron rápidamente y cerraron el acceso, se calcula que casi 70.000 personas se han visto perjudicadas. El vector de entrada fue un acceso desde la cuenta de un usuario con permisos y acceso a e-mails con dicha información. No obstante, la empresa no ha querido garantizar hasta dónde llegó la intrusión. El anuncio de la filtración se produjo el día 3 de junio.

- **Psychic Signatures**: Error criptográfico en Java en el algoritmo de firma digital sobre curva elíptica (ECDSA). Este error es un gran candidato al error criptográfico (más bien de implementación criptográfica) del año por su facilidad de explotación y problemas derivados. Convierte la firma digital de archivos en una farsa, e incluso permitiría que las descargas maliciosas pasaran por contenido legítimo. Clásico ejemplo de refactorización sin suficiente análisis de impacto. En 2020, cuando se publicó Java 15, se omitió una comprobación que establece el algoritmo de verificación cuando se reescribió de C++ a Java el código relacionado con las curvas elípticas.

- Tras una larga espera el uso de un fichero security.txt, como primer paso para el contacto con una compañía, cuando se ha encontrado un fallo relacionado con/que afecta a su ciberseguridad, se ha convertido en un estándar. En el fichero se describe, de forma estandarizada, qué política prefiere seguir la compañía cuando alguien quiere reportarle un fallo en ciberseguridad. Cuenta con características como el punto de contacto, la caducidad de la política, claves públicas de encriptación de la compañía para cifrar los mensajes a intercambiar, etc. El estándar refleja que el fichero debe encontrarse dentro d la ruta /.well-known/ y no en la raíz donde muchas empresas lo situaban.

- Se descubre el uso del software de espionaje Pegasus, del grupo NSO, en multitud de instancias políticas europeas e internacionales, Reino Unido, Finlandia. **La comisión europea decide descartar una investigación propia sobre el maluso/abuso de estas tecnologías e indican que debe ser un asunto de cada estado miembro.**

MAYO

- **Follina: Vulnerabilidad crítica en tratamiento de documentos de MS Office**. Se detecta una nueva fórmula para ejecutar código en documentos Office que no necesita uso de macros y quizá más preocupante, **el documento puede no contener nada malicioso, sino que descarga la carga (payload) al vuelo**. Esta vulnerabilidad permite a un atacante ejecutar remotamente comandos maliciosos con solo abrir un documento de Microsoft Office. Por ejemplo, en los ejemplos iniciales se ve que los atacantes usaban un Word que trae un HTML de un servidor que a su vez utiliza el protocolo MS-MSDT para cargar código Powershell.

- **El Ransomware paraliza Costa Rica**: Rodrigo Chaves, el recién nombrado presidente de Costa Rica, tuvo que declarar el estado de emergencia nacional como de sus primeros actos de gobierno para poder mitigar y responder ante un masivo ataque de ransomware. El ataque comenzó en abril siendo el ministerio de economía el primero en detectarlo y comunicar impactos en el sistema fiscal y de aduanas.

- **Texas InfoLeak**: La información de más de **1.8 millones de personas** del estado de Texas en USA fueron expuestos tras un incidente de seguridad en el departamento de seguros del estado de Texas. Un error de configuración dejó expuesta públicamente una parte de la aplicación que debería ser privada desde 2019 a enero 2022. La Información expuesta incluía, nombres, fechas de nacimiento, direcciones, números de teléfono, y quizá más relevante, **información sobre las lesiones y solicitudes de bajas a las mutuas de los trabajadores**.

- **Disfraces creativos del malware**. Los antivirus normalmente detectan herramientas de cracking o parcheado como maliciosas. Los usuarios que realmente quieren usar estos programas desactivan el antivirus o crean excepciones para los mismos. Por ejemplo, con el conocido KMSauto, que necesita permanecer el Windows tras el parcheo, el usuario se habitúa a esa detección del antivirus. Los atacantes **Lazarus aprovecharon precisamente esto para esconder su ataque bajo el directorio y la apariencia de KMSAuto**. No es que el parche fuera malicioso, sino que disfrazaron su ataque de KMSAuto introduciendo un payload malicioso en él. El antivirus lo detectaba, pero todos los motores deducían que ocurría por tratarse de una herramienta de parcheo o crack y no por ser realmente malware.

- AGCO, **fabricante y distribuidor mundial de equipamiento agrícola**, fue afectado el 5 de mayo por un ataque de **ransomware** que **bloqueó su producción y gestión durante días**. Esta empresa facturó 11.000 millones de dólares el año pasado, siendo proveedor de varias marcas de tractores y otra maquinaria agrícola.

JUNIO

- La agencia americana CISA advierte que el déficit de comunicaciones de incidentes de ransomware afecta a la protección que ofrece la agencia a las organizaciones de Estados Unidos y su capacidad de represalias ante los grupos criminales que las lideran. La CISA estima que solamente sobre el 20-25% de los incidentes de ransomware son comunicados. Con los datos disponibles un informe revela que e**n 2021 más de 2300 ataques de este tipo han sido lanzados contra gobiernos locales, escuelas y proveedores de salud**. Se está iniciando un proceso legislativo para favorecer una mayor comunicación de incidentes, la legislación actual cubre solamente las infraestructuras críticas, pero podrían pasar años hasta su aprobación final.

- **Mozilla activa Total Cookie Protection por defecto en su última versión de Firefox**. El uso de cookies por terceros ha sido fruto de mucha controversia en los últimos años en particular su uso para perfilado de comportamientos de usuario. El problema reside en que existe un único contenedor para todas las cookies de un determinado dominio. Mozilla ha paliado este problema creando contenedores específicos para cada dominio que se visita y solamente ese contenedor es accesible desde el mismo, por lo que se limita la capacidad de recolección y análisis de cookies. Así, si un sitio web inserta una cookie de seguimiento, solo será accesible por y desde dicho dominio, sin posibilidad de acceder al resto de cookies.

- La empresa de análisis ambientales, Montrose Environmental Group con oficinas en 80 países , comunicó el 14 de junio que sufrió una brecha de seguridad que afectó a parte de su red de laboratorios, lo que ha generado retrasos en parte de sus análisis. Concretamente, la afectada fue su subsidiaria, Enthalpy Analytical, que opera en 11 laboratorios haciendo pruebas de entalpía.

- **Cloudflare detiene el mayor ataque HTTPS DDoS volumétrico hasta la fecha**. La compañía de infraestructura de internet Cloudflare asegura que ha detenido un ataque de más de 26 millones de peticiones por segundo. La botnet empleada no contaba según lo analizado con más de 5000 dispositivos lo que no es ni mucho menos un número alto, pero cabe destacar que en este ataque el **uso de infraestructura de cloud**, probablemente mediante el secuestro y uso de máquinas virtuales potentes en vez de dispositivos personales o IoT más numerosos, pero con menor capacidad de ataque.

MÓVILES

Apple iOS

Noticias destacables

Abrimos el año 2022 con iOS 15.2 y tan solo 12 días después se publica la primera revisión, 15.2.1, que arregla una denegación de servicio en HomeKit. Un curioso parche, lanzado por una única vulnerabilidad que ni tan siquiera es crítica. No obstante, el lanzamiento de este parche es atribuido a fallos de funcionalidad en la aplicación Messages y CarPlay.

No mucho después, el día 26 de enero es lanzada la versión 15.3 y esta vez con 10 parches de seguridad: la mitad de ellos de carácter severo en diversos componentes del sistema operativo móvil incluidos su núcleo.

Y ahora algo importante. Un parche urgente para el motor de renderizado de Safari, Webkit. Se sabe que existía una vulnerabilidad que estaba siendo explotada *in the wild*, por lo que el remiendo digital no se hizo esperar y se lanzó 15.3.1 el 10 de febrero.

Poco más de un mes después, Apple lanza iOS 15.4, con nada más y nada menos que 43 parches de seguridad, más de una decena correspondientes a vulnerabilidades que permiten la ejecución de código arbitrario.

Con 15.4 ocurrió exactamente lo mismo que con iOS 15.3. Apple se vio obligada a publicar un parche de emergencia debido a un nuevo fallo que estaba siendo activamente explotado en el componente AppleAVD (un codificador-decodificador de audio y video). Un bug peligroso, que afectaba al kernel del sistema operativo, con todas las consecuencias que eso conlleva (instalación de rootkits, interceptación de llamadas al sistema, etc)

Estamos a mitad de mayo y Apple libera la versión 15.5 con 38 parches de seguridad, 18 de ellos corrigiendo fallos que permitían ejecutar código arbitrario.

Terminamos el semestre con esta versión de iOS, la 15.5 sin revisiones menores. Un periodo quizás tranquilo, relativamente, hasta que llegue 15.6, pero eso será en el próximo semestre.

Evolución de vulnerabilidades en iOS durante el primer semestre de 2022

El primer semestre de 2022 se ha cerrado con 94 vulnerabilidades parcheadas, de las cuales, 36 son consideradas de alto riesgo, con posibilidad de ejecutar código arbitrario. Algunas de ellas afectan al propio núcleo del sistema.

VULNERABILIDADES EN IOS 2022-H1

Evolución de vulnerabilidades por año

Fragmentación de versiones durante el primer semestre de 2022

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.

A fecha de cierre de este informe, no se disponía de datos de fragmentación de versiones por parte de Apple, por lo que las cifras que relatamos a continuación proceden de StatCounter.

Como es habitual en el ciclo de versiones de Apple, la nueva versión alcanza la plenitud de usuarios en el siguiente semestre, con una cuota conjunta (15.5, 15.4, 15.3) que alcanza algo más del 75% de la tarta de versiones. Atrás que iOS 14 y curiosamente, un superviviente (aunque no inesperado): iOS 12.5

¿A qué se debe esto? Sin duda al iPhone 6 y 6+ que es una versión que poseen muchos usuarios y que solo soporta iOS 12.5. Este techo en el sistema operativo sobre este modelo en particular hace que un porcentaje relativamente alto del parque móvil de Apple, un nada desdeñable 2,33% aun siga estancado en la versión 12.5.

Todo debido a la popularidad y longevidad de un modelo de iPhone popular y duradero. Recordemos que el iPhone 6 salió en 2014, nada más y nada menos que hace 8 años.

FRAGMENTACIÓN EN APPLE 2022-H1	
iOS 15.5	57,43%
iOS 15.4	14,70%
iOS 14.8	4,31%
iOS 15.3	3,53%
iOS 12.5	3,23%
iOS 14.7	2,33%

Android

Noticias destacables

2022 abre con la versión ya consolidada de Android 12. Aún queda un largo camino hasta Android 13. La última versión de desarrollo fue publicada el 27 de junio, solo para desarrolladores.

Previsiblemente, Android 13 traerá mejoras en la privacidad, por ejemplo, en la selección que los usuarios pueden hacer acerca de las fotos y videos que las aplicaciones están autorizadas a manipular o un nuevo permiso para que las aplicaciones puedan detectar dispositivos WiFi cercanos.

Como curiosidad, Google liberó el 7 de marzo Android 12L, con número interno de API 32. Una versión refinada de Android 12 para dispositivos con pantallas más grandes, específico para las necesidades de los usuarios.

En total, se han publicado **230 parches** para corregir diversas vulnerabilidades repartidos en los seis boletines, los correspondientes a cada mes del semestre pasado. De esos 230 parches, **21 corrigen vulnerabilidades que han sido calificadas de críticas** y podrían facilitar la ejecución remota de código arbitrario.

Fragmentación en sistemas Android

La última publicación de Statcounter a fecha de edición de este informe nos indican que la versión más implantada de Android es la 11, con un share del 31.65%, seguida por la 10 con un share de 21.92%. Prácticamente, son los mismos números que la edición anterior.

Con estas versiones de momento copando los primeros puestos, Android 12 se conforma con el bronce en un tercer puesto, pero con un respetable 17.54%, un share superior al de Android 11 en su día con las mismas circunstancias.

Tradicionalmente, el ecosistema Android tarda tiempo en propagar las nuevas versiones, dado que los fabricantes han de adoptarlas a sus propias compilaciones, con aplicaciones y servicios inherentes a las distintas marcas.

La porción restante se la reparten las versiones inferiores a la 10, donde ninguna supera el 10% de mercado salvo la versión 9, que aún supone el 11.06% del mercado. La versión más antigua de Android con cuota significativa, un 2.64%, es Android Nougat o 7.0, un sistema que fue lanzado en agosto de 2016.

Estas últimas cifras son muy parecidas al semestre anterior, tal y como también ocurre con las nuevas versiones. El límite de vida útil de las versiones anteriores a la 10 se acerca y se van arañando porcentajes, aunque sean mínimos.

FRAGMENTACIÓN EN ANDROID 2022-H1	
12	17,54%
11	31,65%
10.0	21,92%
9.0 Pie	11,06%
8.0 Oreo	5,90%
7.0 Nougat	2,64%

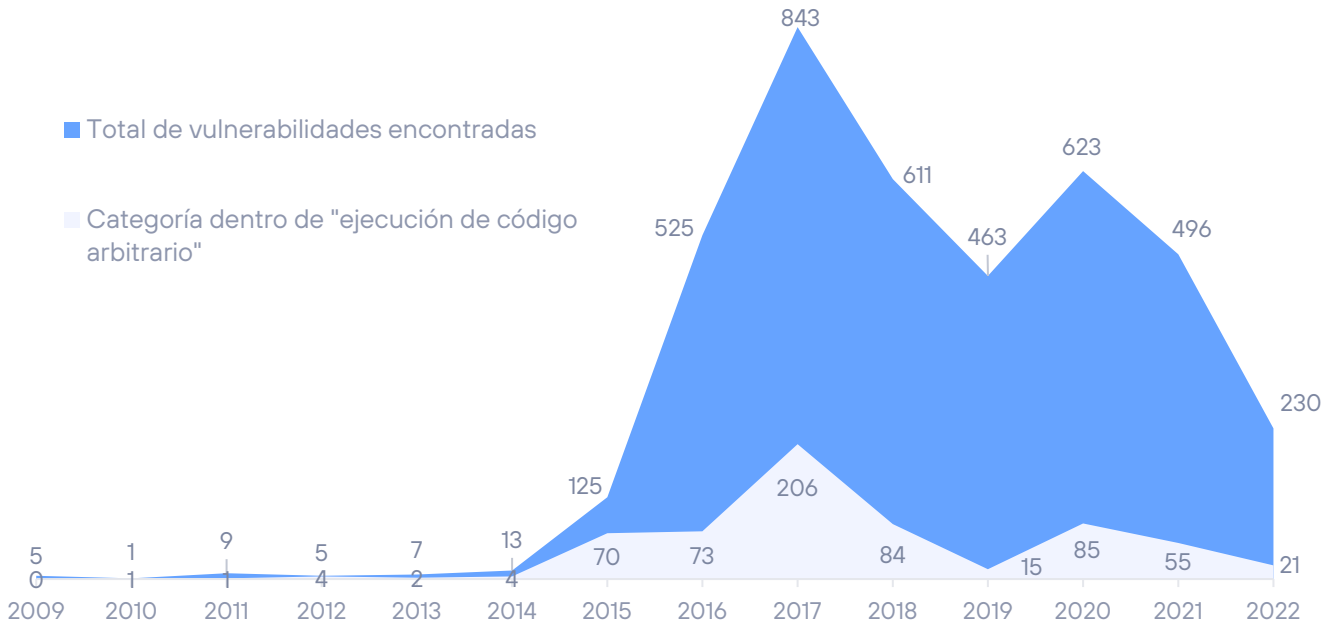
Evolución de vulnerabilidades en Android durante el primer semestre de 2022

Típicamente, Google libera un grupo de parches se seguridad cada mes. Por lo que han sido publicados seis boletines que suman un total de **230 CVEs** o vulnerabilidades corregidas ese semestre. **21 de ellas críticas**. Cifras muy similares al conjunto del semestre pasado. En la gráfica se observa lo acumulado hasta 2022, primer semestre.

No obstante, muchos de estos fallos afectan a software o firmware de ciertos fabricantes en particular, lo que significa que una misma vulnerabilidad no tiene por qué afectar a todo el parque de dispositivos Android, sino tan solo a aquellos con lo componentes afectados.

VULNERABILIDADES EN ANDROID 2022-H1

Evolución de vulnerabilidades por año



VULNERABILIDADES DESTACABLES

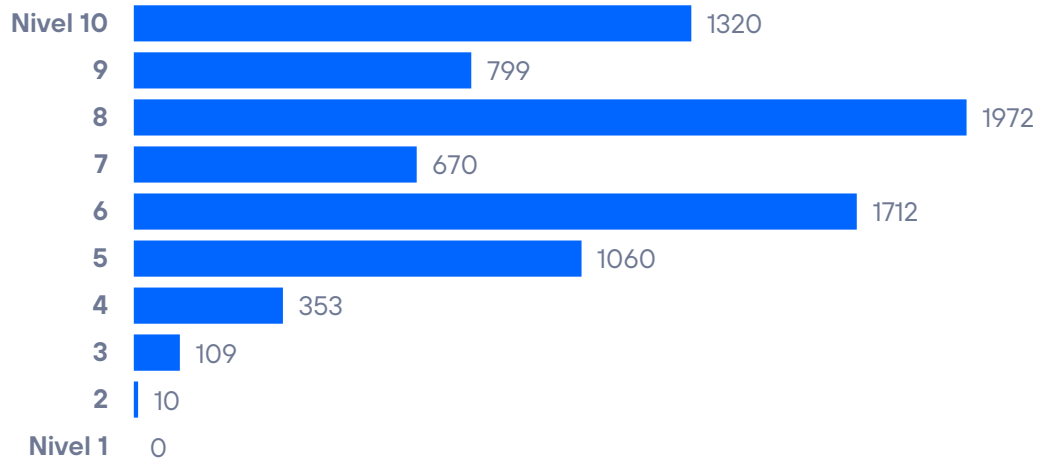
Comentamos en esta sección algunas de las vulnerabilidades notables a nuestro juicio, de este segundo semestre de 2021, es decir, aquellas que destacan por su especial relevancia o peligrosidad.

CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2022-26784	Philips: Varios	Philips publica una vulnerabilidad en Windows Cluster Shared Volume (CSV) que permite a un atacante ejecutar un ataque DoS en algunos dispositivos médicos, como el Holter Recorder DigiTrak XT	6.5
CVE-2022-1300	Trumpf: Varios	TRUMPF ha publicado una vulnerabilidad crítica que permitiría un acceso no autorizado, permitiendo ejecutar incluso una interrupción completa del servicio.	9.8
CVE-2022-22720	Apache Server 2.4.52	Se ha detectado una vulnerabilidad que permitiría acciones de "HTTP request smuggling" sobre productos de climatización de Mitsubishi.	9.8
CVE-2022-22965	Varios SCI	Spring4Shell afecta a varios sistemas de control industrial de varios fabricantes, permitiendo RCE sobre el Spring Framework de Java, ampliamente utilizado en el entorno Java y en ciertas aplicaciones de dispositivos industriales. Incluidos sistemas de autenticación.	9.8
CVE-2022-34265	Django	Vulnerabilidad de inyección SQL en la rama principal de Django	9.8
CVE-2022-1096	Chromium	Confusión de tipos en el motor de JavaScript V8	8.8
CVE-2022-0540	Altassian Jira	Salto de autenticación enviando peticiones HTTP	9.8

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

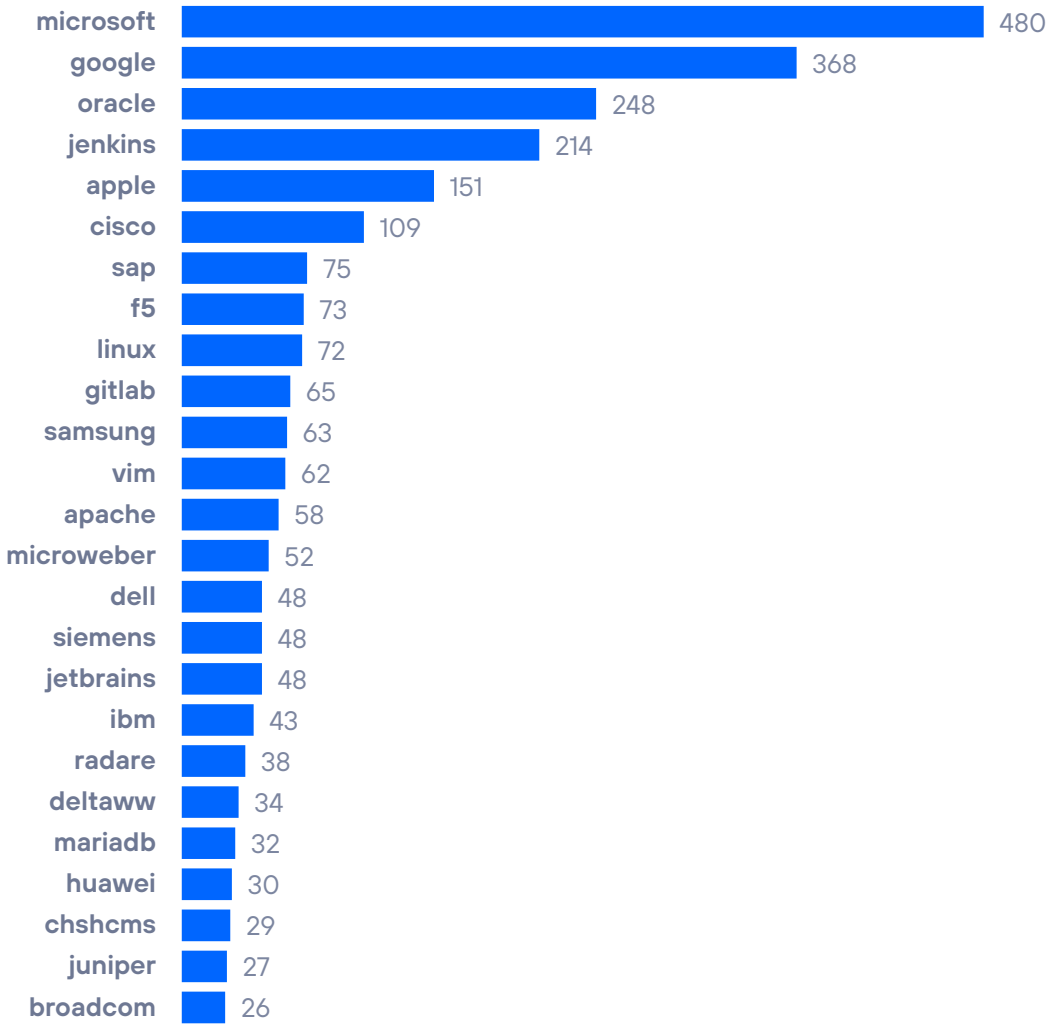


Top 25 compañías con más CVE acumulados

Durante el primer semestre de 2022, Microsoft ha liderado por número de vulnerabilidades conocidas.

VULNERABILIDADES POR FABRICANTE

Top 25 fabricantes por CVE acumulados



QUIÉN ES QUIÉN DESCUBRIENDO VULNERABILIDADES MICROSOFT

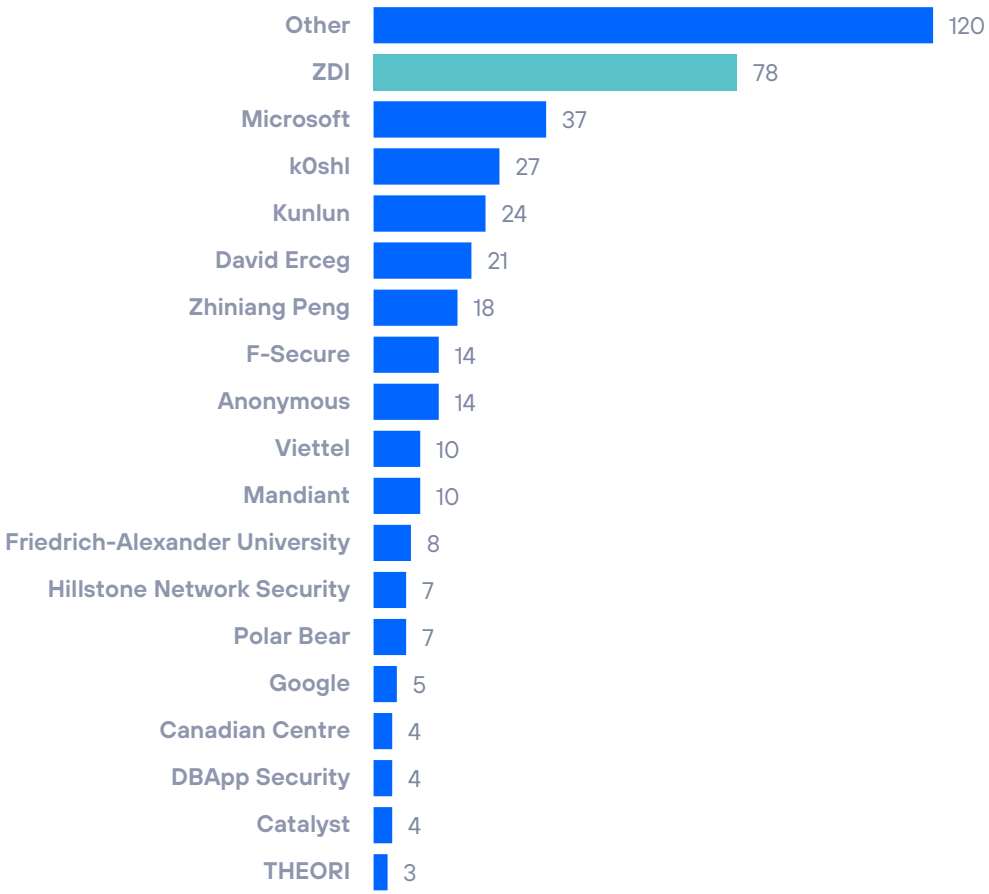
De los créditos de vulnerabilidades descubiertas en sistemas Microsoft, hemos extraído la compañía que ha descubierto la vulnerabilidad. **En el caso de que sean varios los descubridores, hemos contado solo al que aparecía en primer lugar, para simplificar los cálculos** y porque entendemos que se muestra 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.

La larga cola de "otros" es la que lidera la lista. La iniciativa ZDI, sigue siendo (cada vez más) la fórmula favorita para los investigadores. Baja considerablemente Google como descubridor, cuando en otros años ha sido clave. Se cuelan en este semestre muchos investigadores independientes.

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

Número total de vulnerabilidades por cada descubridor en el primer semestre de 2022



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 primer semestre de 2022.

Wicked Panda: Malos como ellos solos

Winnti (otro de los nombres de este grupo) es la definición pura de APT: "amenaza avanzada persistente", en español. Y sobre todo por lo de "persistente".

Tras una investigación de 12 meses, la empresa de ciberseguridad "Cybereason" ha concluido que el responsable de la operación "Cuckoo Bees" ha sido este grupo, de origen chino.

Esta operación, tan compleja que **comenzó en 2019** y no fue detectada hasta 2021, habría sido capaz de extraer "cientos de miles de gigas" de información relacionada con la propiedad intelectual de empresas muy relevantes en los sectores de energía, defensa, biotecnología, farmacéutica...

El impacto económico a presente y futuro... es incalculable (literalmente), aunque algunas fuentes lo estiman en billones de dólares.

Sobre APT41, el Departamento de Justicia de los Estados Unidos llegó en 2020 a identificar su estructura y a algunos miembros, varios relacionados con la empresa de ciberseguridad "Chengdu 404 Network Technology". Dicha empresa sería una tapadera que trabajaría en conjunto con otra de venta de dinero virtual para juegos en línea, SEA Gamer Mall, donde habrían sido identificados otros dos miembros del grupo.

Más información en: https://www.cybereason.com/blog/operation-cuckoobees-cybereason-uncovers-massive-chinese-intellectual-property-theft-operation

Lazarus: Siempre vuelve

Entre diciembre de 2021 y mediados de enero de 2022, este grupo desplegó una campaña de phishing enviando supuestas ofertas de trabajo en una empresa de renombre en el ámbito de la ingeniería y la defensa. Su intención, a juzgar por los receptores de la campaña, era comprometer a personal del ejército de los USA.

Los investigadores de Malwarebytes detectaron que el servidor de C&C era una cuenta de Github, con lo que discernir entre tráfico legítimo y no legítimo era mucho más difícil para los sistemas de seguridad.

Como último dato, los investigadores también observaron que los documentos son de abril de 2020, lo que nos vuelve a demostrar que el comportamiento profesional y empresarial de estos grupos es la tónica habitual.

Más información en: https://blog.malwarebytes.com/threat-intelligence/2022/01/north-koreas-lazarus-apt-leverages-windows-update-client-github-in-latest-campaign/

Aoqin Dragon: Emerge el rey de los mares del sur

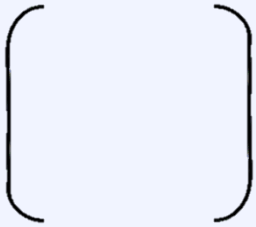
Desde 2013 llevaba el rey dragón de los mares del sur, Ao Qin, operando sin ser descubierto. Recientemente catalogado por los investigadores de Sentinel Labs, se le supone instalado en China y ha estado operando todo este tiempo en el sudeste asiático y en Australia sin levantar sospechas. Sus objetivos han sido entidades gubernamentales, instituciones educativas (posiblemente relacionadas con la investigación) y empresas de telecomunicaciones.

¿Cómo ha conseguido este grupo permanecer sin clasificar? Porque han ido cambiando de TTP precisamente para ello. En seguridad, "ciber" o no, identificar al criminal detrás del delito ayuda a conocer las aspiraciones y el impacto real de este. Hasta su ahora, estos ciberincidentes eran sólo elementos aislados sin un interés especial. Sin embargo, ahora forman parte de un "plan" ejecutado por alguien con intereses mucho más profundos de lo que se esperaba.

Más información en: https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/

Lapsus$: Vive rápido, muere joven...

... y deja un bonito cadáver. Esto debe haber sido lo que pensaron los integrantes de este grupo que tanto dio que hablar en marzo de este año.



Y no fue poco lo que hicieron:

- Robaron más de 70.000 credenciales de empleados de Nvidia, así como el código de desarrollo de su próximo modelo insignia de tarjeta gráfica.
- Publicaron 190GB de código de varios móviles de Samsung.
- Filtraron 37GB con código de varios servicios de Microsoft
- Accedieron al código fuente y datos de (300.000) usuarios de Mercado libre.

Y todo esto... en medio mes de marzo y publicando sus acciones en su canal de Telegram (con 48.000 suscriptores).

Aunque el grupo fue catalogado en diciembre de 2021, después de localizar al grupo en Brasil, a raíz de sus grandes éxitos, se puso la lupa sobre él y se descubrió que se trataba de un chico de 17 años que vivía con su madre en Oxford. El día 25 fueron detenidos (y liberados) en Londres varios miembros del equipo. No obstante, no se descarta que sí haya una pequeña ramificación en Brasil.

Este grupo es otra clara demostración de que lo difícil no es, desgraciadamente, hacer fechorías en el ciberespacio. Lo difícil es ocultarse. Sobre todo, cuando son de dimensiones tales que todos los ojos se posan sobre ti.

Más información en: https://www.xataka.com/seguridad/se-acabo-fiesta-policia-londres-arresta-a-siete-presuntos-lideres-lapsus

ANÁLISIS DE AMENAZAS OT

La siguiente información procede del sistema para la captura y análisis de amenazas en el ámbito OT, Aristeo. **Aristeo** incorpora una red de **señuelos, fabricados con hardware industrial real,** que aparentan ser sistemas industriales en producción real, **y se comportan como tales**, pero que están extrayendo toda la información sobre las amenazas que acceden al sistema. Con la información de todos los dispositivos desplegados en los distintos nodos-señuelos, Aristeo aplica relaciones e inteligencia para ir más allá del dato, pudiendo detectar proactivamente campañas, ataques dirigidos o sectorizados, vulnerabilidades 0-day, etc.

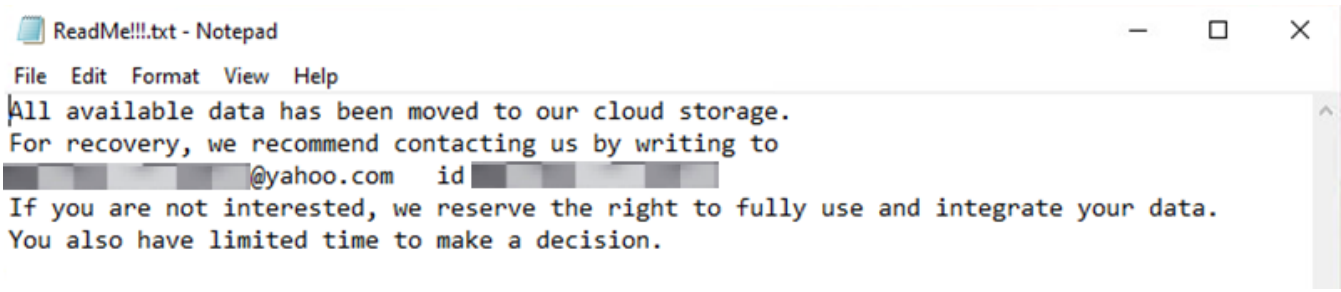
Cada nodo-señuelo dispone de sus propias características y reproduce un proceso distinto. Por lo tanto, los protocolos, dispositivos, sectores productivos... cambian en cada uno de ellos. Además, los nodos están vivos, lo que implica que pueden experimentar alteraciones en su configuración a gusto del equipo de investigadores que trabajan con ellos, o del cliente que dispone de su uso temporal o permanente. Esta variabilidad puede generar ligeras discrepancias en los datos mostrados en este apartado si se comparan entre semestres.

Más información en:
https://aristeo.elevenlabs.tech

Análisis de la información

Vamos dejando atrás poco a poco al SARS-COV2 y este semestre traemos un caso que refleja la importancia de reconocer a la ciberseguridad industrial como un ámbito distinto de la ciberseguridad de la información. Desde luego, los malos lo tienen claro y se comportan de distinta forma.

Hace unas semanas tuvimos un invitado en nuestro sistema que demostró que conocía dónde le dolía más al ecosistema industrial. Nos encontramos el sistema parado, todos los valores reseteados (incluidas contraseñas) y un escueto mensaje que decía:



Detenido, reseteado de fábrica, proceso "robado"... pero ¿y la estrella de todas las fiestas? ¿y el ramsonware? En ningún momento habla de "información cifrada". ¿Por qué no desplegó un ransomware? Por dos razones:

1. Vagancia o incapacidad (seguramente una mezcla de ambas). Una vez dentro, sería fácil ejecutar algún malware en el sistema, pero... ¿para qué? Esto se responde en el siguiente punto.

2. El atacante paró todo el sistema, reseteó todos los valores... robó la información de nuestro proceso. Y eso era todo lo que quería.

La explicación final es sencilla, si lo vemos con perspectiva y experiencia. La culpa es de la CIA. Nos referimos, obviamente, a los tres pilares de la seguridad de la información.

- **C**onfidentiality (confidencialidad)
- **I**ntegrity (integridad)
- **A**vailability (disponibilidad)

En un entorno en el que todo es "información", el ámbito TI, robar la información sólo puede afectar a la confidencialidad. La integridad y la disponibilidad se ven afectadas por otras maniobras (como por ejemplo el cifrado). Desde luego, una de las más efectivas y rápidas es ejecutar un ransomware. Recuperar el sistema es complicado, los ficheros con la información que pudiéramos tener en backup podrían no estar actualizados...

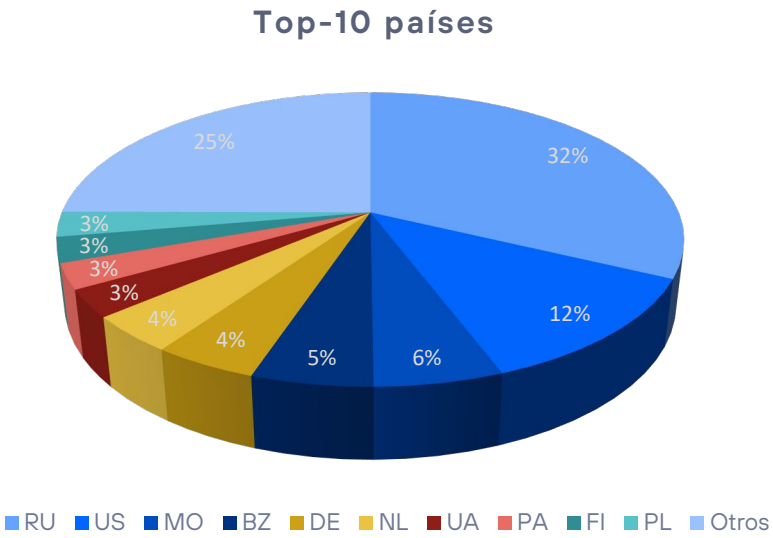
Sin embargo, en el ámbito TO lo más efectivo para afectar a la integridad y la disponibilidad del entorno industrial es, sencillamente, eliminar (o resetear) los valores que gobiernan el sistema. Por su parte, un ransomware afecta a medias al sistema industrial actual, porque en el ecosistema industrial hay dispositivos donde el ransomware no se puede ejecutar. Además, los valores de un sistema industrial no suelen variar por lo que la información de backup suele estar "actualizada". Por lo tanto, recuperar la información de un sistema industrial es más sencillo que en un sistema de información puro.

No conviene perder de vista el negocio: mientras que en un ecosistema TI, por lo que se paga más dinero es por recuperar los ficheros con la información más actualizada (y si pagas, todo queda "como antes"), en el ecosistema TO lo que más dinero vale es el proceso en sí, la operativa. Robar el proceso y vendérselo a la competencia, publicar sus detalles... eso es lo que tiene más valor (económico y operativo). Detener el sistema, inutilizarlo... es más o menos importante, pero es un daño que se hace previamente y que no se puede deshacer, con lo que de ahí los ciberdelincuentes ya no pueden obtener rédito. En resumen, en un entorno OT recuperar la información es relativamente sencillo por lo estable que resulta (un backup lo soluciona aunque no sea extremadamente reciente) y por tanto cifrar la información en un entorno OT, paradójicamente, no es tan dañino. El daño es parar la operativa o venderla a un tercero y eso no se puede recuperar.

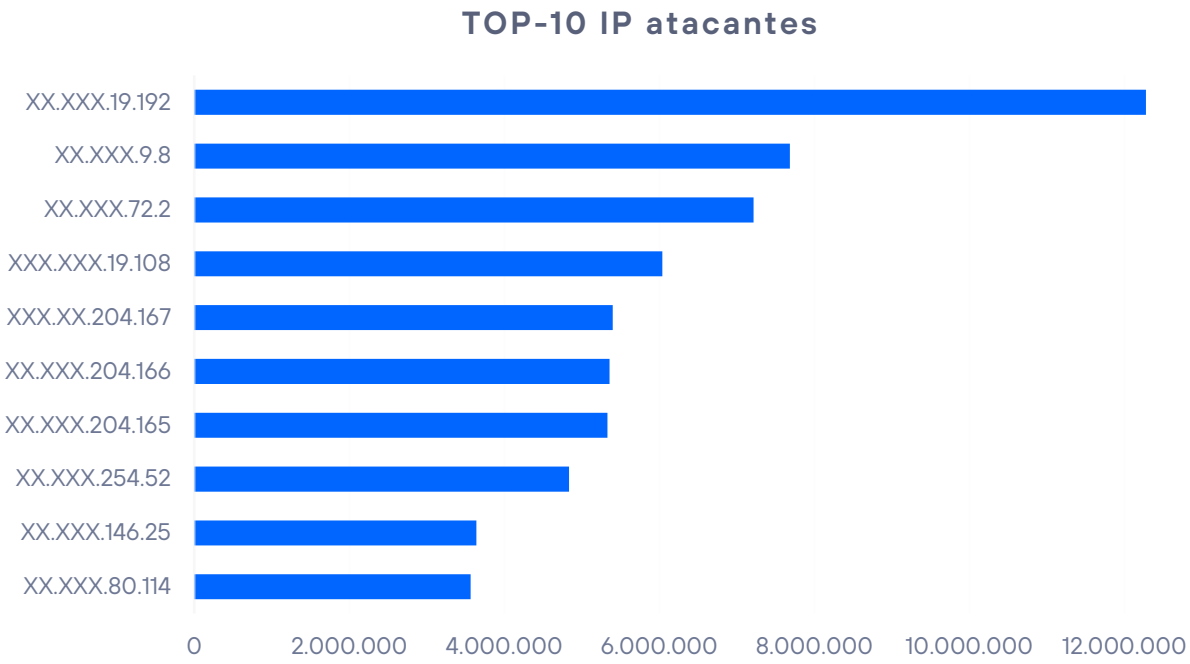
Y ahora, pasamos a la estadística genérica de la información registrada. En el primer semestre de 2022 se detectaron **más de 415 millones de eventos de ciberseguridad**. Esto supone un incremento de más del 160% respecto a los datos registrados en el primer semestre de 2021 y un 3% respecto a este semestre anterior.

Eso sí, la suma de eventos ha ido descendiendo mes a mes, viniendo de un enero en el que se registraron 105 millones de eventos y terminando con un junio en el que se detectaron algo más de 50 millones.

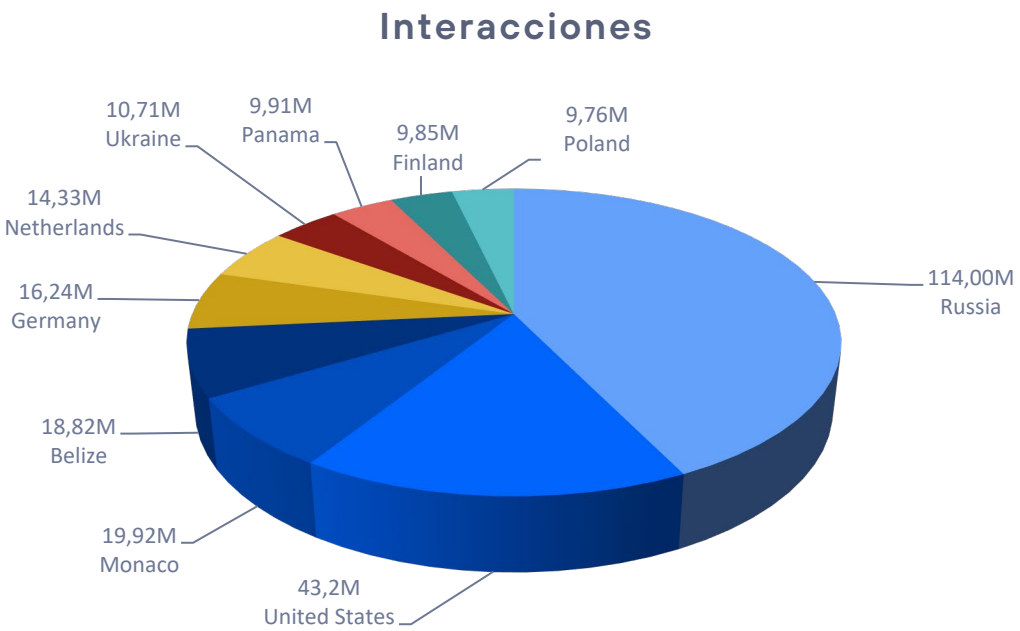
La distribución por países sería la siguiente:



Ahora vamos a ver el Top-10 de las direcciones IP con más interacción con el sistema de Aristeo. Del TOP-10, el 30% pertenecen al mismo proveedor de servicios de un país de Europa del este, y tiene delegada la administración de esas IP, un /24, en una entidad radicada a casi 10.000 km de ese país.



A continuación, observamos cómo se reparten la actividad los países con más presencia en nuestro Aristeo. Especialmente llamativa es la entrada de Belice (país con menos de 400.000 habitantes) en esta exclusiva lista.



RECAPITULACIÓN

Bajan por segundo semestre consecutivo los fallos corregidos tanto en iPhone como en Android. Mientras que en 2017 ambos sistemas operativos llegaron a un récord en vulnerabilidades corregidas con varios cientos de problemas, ambos han descendido considerablemente en los últimos años y marcan récords a la baja no vistos desde 2014.

Microsoft, Google y Oracle son las empresas con más fallos corregidos, como de costumbre. Jenkins se sitúa en cuarta posición por primera vez y entra fuerte en el ranking.

Google detecta muchas menos vulnerabilidades en sistemas Microsoft, mientras ZDI sigue como el bróker preferido por los descubridores. Algunos independientes siguen encontrando decenas de fallos.

Con respecto a la seguridad OT, el mundo del ransomware demuestra que sabe cómo economizar recursos cuando entra en uno de estos sistemas. No cifra, solo destruye, porque ahí radica el valor de la operativa.

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 ciberseguridad de Telefónica Tech tenemos mucha más información y noticias que pueden resultar de tu interés. Aquí van nuestros artículos más relevantes.

IDENTIDAD

Cuatro años de la RGPD: cómo mejorar la gestión de la privacidad

El nuevo final de las contraseñas

Digital Identity Wallets contra el fraude en identidad

Web3 y la evolución de la Identidad en Internet

CRIPTOGRAFÍA

Comprendiendo los certificados digitales

Google da un paso para mejorar el ecosistema de Certificate Transparency: No depender de Google

MALWARE

La hipocresía del doble lenguaje entre las bandas de ransomware