Telefónica Tech

Julio de 2021

Informe sobre el estado de la seguridad 2021 H1

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.

tech.telefonica.com

Índice

1. 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.

El primer semestre de 2021 se ha visto marcado de nuevo por los efectos del SARS-CoV-2 pero desde un punto de vista más optimista gracias al avance global de la vacunación. Sobre el asunto que no se aprecia optimismo alguno es el avance del *ransomware*.

Este primer semestre hemos visto gran cantidad de compañías afectadas por este grave problema a nivel mundial. Desde ministerios hasta grandes compañías americanas. Desde pequeñas empresas hasta infraestructuras críticas.

El ataque de Colonial Pipeline en mayo ha representado un hito en el mundo del *ransomware* en general y de la ciberseguridad en particular, pues su efecto se dejó sentir en todo el país provocando diversas reacciones. **Entre el público general, se materializó la amenaza del *ransomware* como algo mucho más tangible que no solo afectaba a sus sistemas personales, a las pequeñas empresas o incluso a grandes compañías, sino que podía afectar a sus recursos de abastecimiento básicos.** También, a causa de las filtraciones sufridas durante este semestre de todo tipo de datos personales en compañías, los usuarios han percibido lo expuesta que puede estar su información.

En el plano de la política, el propio Joe Biden firmó una orden ejecutiva destinada a mejorar la ciberseguridad en general y tratar el *ransomware* como terrorismo. La guerra, en muchos ámbitos, se intensifica.

En el apartado de las vulnerabilidades, han destacado los 0-day encontrados en Chrome, cada vez más comunes y los FragAttacks, fallos de hace más de 20 años en las redes Wi-Fi que afortunadamente no han tenido mayor recorrido.

En el apartado del *malware* en móviles, hemos visto cómo cada vez con mayor sofisticación, los troyanos para Android han descubierto fórmulas para atrapar las notificaciones y atacar a los contactos de WhatsApp respondiendo automáticamente a los mensajes que llegan a la víctima.

Este semestre estamos de enhorabuena, porque inauguramos una nueva 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 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!

2. Los incidentes más destacados del primer semestre de 2021

A continuación, damos cuenta de aquellas noticias que mayor impacto han tenido durante el transcurso de este primer semestre de 2021.

ENERO

- ¿Parchear o no parchear los sistemas que han llegado a su fin de ciclo (EOL)? **Cisco vuelve a la polémica** por no querer parchear las últimas 74 vulnerabilidades en varios de sus dispositivos populares, porque han terminado su ciclo de vida, e invita a los usuarios a adquirir las versiones más recientes.
- Se encuentra **un APK fraudulento capaz de enviar mensajes a través de WhatsApp** a los contactos de la víctima. Aprovecha las notificaciones recibidas en el teléfono para responderlas rápidamente con un enlace que parece ser de la Play Store, pero que en realidad redirige otra URL desde donde descargar el *malware*.
- Google destapa una operación que supera cualquier otra actividad delictiva que hubiera tenido en su objetivo a expertos en ciberseguridad por su elaborada maquinaria para llegar a ellos. La campaña parece orquestada por el gobierno norcoreano y se tomaban la molestia de construir perfiles de supuestos investigadores de vulnerabilidades y *exploits* en Twitter, que apoyaban la labor de los otros, se daban a conocer en la comunidad y alardeaban de sus habilidades **mutuamente para ganar su confianza y más tarde intercambiar información con otros expertos reales.**
- El 11 de enero, la empresa noruega AKVA Group, dedicada a la piscicultura industrial (incluidos barcos), anunció que había sido atacada y parte de sus servicios de control habían sido bloqueados. El culpable, un ataque que terminó con un *ransomware* bloqueando sus sistemas. **En la contabilidad del primer trimestre AKVA cifró las pérdidas generadas por el ciberataque en 6 millones de dólares.**
- El 25 de enero, la empresa PALFINGER, con 25 ubicaciones en todo el mundo y más de 11.000 empleados, y que ofrece soluciones tecnológicas en el campo de la ingeniería y está especializada en grúas y sistemas de elevación, **sufrió un ataque a nivel global que dejó bloqueada gran parte de su infraestructura.** La producción estuvo parada durante dos semanas, en una empresa que genera más de 1.500 millones de dólares anualmente.

FEBRERO

- A partir de la versión 90, **Chrome muestra un error de certificado cuando un usuario intente acceder a cualquier web con un certificado firmado por Camerfirma**. Aunque quizás no sea la CA más popular, está muy presente en España en muchas organizaciones públicas.
- Tras el fallo en FreeType descubierto a finales de 2020 y que en realidad comprendía dos problemas (uno para explotar y otro para escapar de su *sandbox*), **vuelve a conocerse otro 0day de verdad (del que se encuentra siendo aprovechado por atacantes) en este navegador.** Es el sexto en apenas unos meses.

- Kenna Security ha estudiado 18.000 vulnerabilidades catalogadas con su CVE y concluye **que solo 473 fueron explotadas en 2019 de forma que supusieran una amenaza real para las compañías. Esto supone un 2,6%**. De estas, a su vez, apenas un 6% han llegado a ser populares en su explotación.
- Unos delincuentes acceden a una planta de aguas en Tampa, Florida, que da servicio a unas 15.000 personas. Aprovecharon la conexión a través de "Team Viewer" para acceder al sistema y **modificar la cantidad de hidróxido de sodio (lejía) para verter una cantidad muy superior a la utilizada normalmente** (para controlar la acidez del agua). El caso se puso en manos del FBI y del servicio secreto.
- El 28 de febrero, la empresa PrismHR, que gestiona más de **80.000 millones anuales de dólares en nóminas entre más de 80.000 empresas, reconoció un "ciberincidente" que afectó a su *software* de nóminas y beneficios para empleados.** Aunque no lo indicó expresamente, algunos medios lo situaron en el marco de un ataque con *ransomware*.

MARZO

- La gravedad de las últimas vulnerabilidades en Exchange (en concreto CVE-2021-26855, ProxyLogon) ha obligado a Microsoft a realizar un movimiento interesante: **incluye en Microsoft Defender, el "antivirus integrado" la mitigación del problema de seguridad de forma automática.** Con solo actualizar se mitigará la vulnerabilidad (no quedará corregida hasta que se parchee, pero los atacantes tendrán más dificultad para aprovecharla).
- Más ataques del tipo cadena de suministro, y esta vez a PHP. **Alguien entró en el GIT oficial del código PHP y añadido una puerta trasera**. Si se usa esta versión, un atacante tendría que entrar con la cadena "zerodium" en un User-Agent "falso" con una doble T al final y podría ejecutar código en el servidor.
- **Un ataque de *Ransomware* paraliza el Servicio de Empleo Español, SEPE durante días.** La Oficina de Reino Unido de Relaciones Exteriores, Commonwealth y Desarrollo comunicó la filtración de documentos confidenciales relacionados con proyectos de ayuda británicos, incluidos detalles relacionados con proyectos financiados por un fondo secreto de seguridad nacional.

ABRIL

- Se da otro paso dentro del plan para deshacerse de Emotet. En un principio se secuestraron los dominios y *command and controls* usados por el *malware*, para que fuesen en la medida de lo posible, "desactivados". **Ahora, la policía va a enviar desde esos servidores un mensaje al *malware* instalado en los sistemas para que se elimine por completo.**
- Se hacen públicos los datos de más de 13 millones de usuarios de Phone House.
- La central nuclear de **Natantz (Irán) sufre un ciberataque que provoca un apagón, 24 horas después de ser puesta en marcha**. En un primer momento, el gobierno iraní indicó que se trataba de un "accidente", pero tras las publicaciones de la prensa israelí asegurando que se trataba de un ciberataque, lo calificó como "terrorismo nuclear".
- El 24 de abril, una serie de ciberataques tumbó varios servicios nacionales españoles, como las webs de varios ministerios y del INE.

MAYO

- AXA toma una decisión en Francia: **la cobertura del ciberseguro no devolverá el dinero del rescate a los clientes que paguen por la extorsión.** Esta decisión se ha tomado en el contexto de una mesa redonda del senado en Francia que abordaba "la devastadora epidemia global de *ransomware*".
- La orden ejecutiva firmada por **Biden contra el ransomware pretende modernizar las defensas en ciberseguridad.** Esta orden ejecutiva se traducirá en que las empresas deberán cumplir unos estándares mínimos, se procedimentará, se auditará... se generará una industria más sana.
- Mathy Vanhoef, académico de seguridad de la Universidad de Nueva York en Abu Dhabi, descubre los ***FragAttacks*, una serie de 12 vulnerabilidades en WiFi que llevaban ahí desde prácticamente la implementación inicial de la tecnología.**
- Los días 4 y 5 de mayo, la empresa noruega **"Volue" sufrió un ciberataque con *ransomware* que bloqueo las instalaciones de aguas y aguas residuales que dan servicio al 85% del país.** Esto además provocó que la propia empresa, como medida preventiva, detuviera y pusiera en cuarentena cientos de dispositivos que tiene desplegados en toda Europa.
- El día 7 de mayo, la empresa **"Colonial Pipeline", que abastece de hidrocarburos a gran parte de la costa este de EEUU, se vio bloqueada por un ciberataque que cifró sus sistemas.** Esto provocó un encarecimiento medio del combustible del 4% y el bloqueo total duró 6 días. Las investigaciones apuntan a que una contraseña comprometida para el acceso a la VPN de la entidad pudo ser el punto de entrada de los delincuentes.
- El 14 de mayo el servicio público sanitario de Irlanda, el HSE, sufrió un ciberataque con un *ransomware* que obligó a cancelar citas y diagnósticos en varios hospitales.

JUNIO

- Se da a conocer ALPACA, **un nuevo tipo de ataque a TLS que permitiría redirigir el tráfico del navegador a un servicio diferente con el fin de acceder o exfiltrar información sensible.**
- El 4 de junio se publicó la noticia de que el **Departamento de Justicia de los Estados Unidos iba a equiparar los ataques de *ransomware* con los ataques terroristas**, en términos de prioridad en las investigaciones y prevención de estos delitos.
- El 8 de junio, **el FBI anunció que habían recuperado 63.7 Bitcoins de los 75 que se pagaron a los delincuentes que atacaron a "Colonial Pipeline".** Pese a recuperarse más de tres cuartos del total, el valor del Bitcoin en el momento de la recuperación hace que lo recuperado sume 2.3 millones de dólares, mientras que cuando se hizo el pago, esa misma cantidad superaba los 3.8 millones de dólares.

3. Móviles

3.1. Apple iOS

Noticas destacables

Dejamos el año 2020 con iOS 14.3 y no fue hasta el 26 de enero de un recién estrenado 2021 cuando la versión 14.4 vio la luz. Eso sí, **lo hizo cargado de parches de seguridad, en concreto, hasta 55 CVEs corregidos.** Casi la mitad de ellos para impedir la ejecución de código arbitrario, la joya de la corona de la explotación.

A medio camino entre iOS 14.4 y 14.5 tuvo que ser liberado un parche con carácter urgente el 8 de marzo: 14.4.1. Corregía una muy peligrosa vulnerabilidad (CVE-2021-1844) de ejecución de código arbitrario que podía ser explotada con tan solo visitar una página web maliciosa. El susto, proporcionado por los investigadores del Google Threat Analysis Group no quedó ahí y el 26 de marzo, del mismo modo, fue liberada con urgencia la versión 14.4.2. Se trataba de otra vulnerabilidad (CVE-2021-1879) con idéntico impacto.

Ahora sí, **el 26 de abril se publica iOS 14.5 una revisión mayor dentro del ciclo de vida de la versión 14. Hasta 60 vulnerabilidades corregidas, 12 de ellas con ejecución de código arbitrario.** Esta versión de iOS traía una interesante opción de desbloqueo basado en reconocimiento facial. En caso de disponer de un Apple Watch desbloqueado y a corta distancia, el usuario puede desbloquear el terminal si tiene puesta una mascarilla.

Además, iOS 14.5 trajo una nueva característica de protección de la privacidad. Por defecto, a menos que dispongamos de lo contrario en los ajustes, iOS bloqueará todo intento y petición de rastreo del usuario por parte de las aplicaciones. Otra opción nueva, permite activar la instalación automática de actualizaciones de seguridad. Es decir, el sistema no esperará a la decisión del usuario para instalar un parche (como, por ejemplo, los 14.4.1 y 14.4.2). Una vez iOS detecte que se trata de un parche de seguridad, optará por su instalación directamente.

El 3 de mayo se liberó una nueva versión menor antes de iOS 14.6. **La 14.5.1 corregía dos nuevos agujeros de seguridad en WebKit,** el motor de renderizado web de Safari, que podrían ocasionar la ejecución de código arbitrario con la visita a una web maliciosa.

Por último, el 24 de mayo es liberada la versión 14.6. La nueva versión viene con **43 vulnerabilidades corregidas, 8 de ellas de ejecución de código arbitrario.**

Evolución de vulnerabilidades en iOS durante el primer semestre de 2021

Un *exploit* que garantice la ejecución remota de código arbitrario en iOS se sigue cotizando a dos millones de dólares. Medio millón por debajo de su equivalente Android.

El primer semestre de 2021 se ha cerrado con más de 200 vulnerabilidades parcheadas, de las cuales, casi 50 son consideradas de alto riesgo, con posibilidad de ejecutar código arbitrario. Algunas de ellas afectan al propio núcleo del sistema.

VULNERABILIDADES EN IOS 2021-H1
Evolución de vulnerabilidades por año

Fragmentación de versiones durante el primer semestre de 2021

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 14 mantenía una cuota del 72% de dispositivos, seis meses después iOS 14 aumenta su población al 86% de dispositivos. Como es habitual, la versión saliente se coloca a una discreta, aunque significativa, segunda plaza con un 12%. En ese mismo lugar estuvo iOS 13 con un 18% seis meses antes.

Los números varían respecto a los de años anteriores en el sentido de que los dispositivos móviles de Apple adoptan con mayor grado de aceptación las nuevas versiones.

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

Fragmentación en Apple iOS 2020-H1 (Según los datos de la App Store)

3.2. Android

Noticias destacables

Falta poco para que Android 12 tome el relevo. Concretamente, si se sigue el mismo calendario de liberación de las últimas versiones, 12 verá la luz en septiembre de 2021. La beta de Android 12 fue anunciada y liberada el 18 de febrero. Será en el siguiente informe cuando demos un repaso a las novedades en el capítulo de seguridad y privacidad.

Respecto a Android 11, sistema operativo con el que llevamos desde septiembre de 2020, **ha publicado seis grandes parches acumulativos de seguridad.** Uno por mes, como es habitual, liberados en la primera semana.

Como avance en el capítulo de novedades de seguridad, Android 12 vendrá con un **cuadro de mandos en el que el usuario podrá comprobar que datos del dispositivo han sido accedidos y cada cuánto tiempo.** Por ejemplo, podremos ver que aplicación ha accedido al micrófono y cada cuanto tiempo.

Tal y como ocurre en iOS, Android mostrará un pequeño icono en la barra de estado cuando el micrófono o cámara esté activado en ese momento. Advirtiendo al usuario de los usos de estas funcionalidades. También se mostrará, en la nueva versión del sistema operativo móvil de Google, un mensaje que alerte al usuario de que la aplicación activa está leyendo el portapapeles.

Fragmentación en sistemas Android

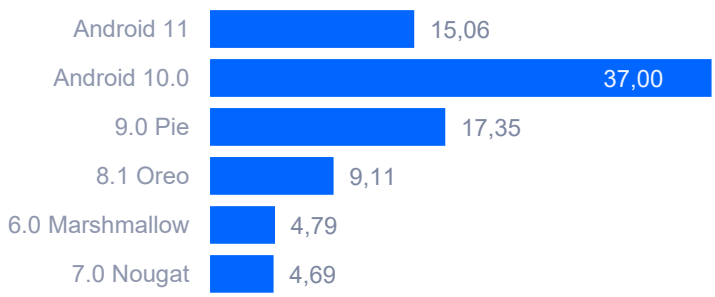
Android no publica estadísticas que muestren el estado de fragmentación entre versiones. Los datos obtenidos pertenecen a fuentes públicas, es decir, no están contrastados con las fuentes oficiales.

La última publicación de *Statcounter* a fecha de edición de este informe nos indican que la versión más implantada de Android sigue siendo la 10, con un share del 37%, solo tres puntos menos que la edición anterior. Le sigue Android 9 con un con algo más del 17% (pierde seis puntos).

Android 11, el sistema vigente tan solo despunta con un 15% a poco más de un trimestre de cumplir un año desde su publicación.

La porción restante se la reparten las versiones inferiores a la 9, donde ninguna supera el 10% de mercado. Aun así, sorprende que versiones de Android como la 8, 7 y 6 posean un share total de casi el 20%. Recordemos que Android 6 (o 5.1.1 "Lollipop") fue lanzado en 2015.

FRAGMENTACIÓN EN ANDROID 2021-H1



Evolución de vulnerabilidades en Android durante el primer semestre de 2021

Un *exploit* que garantice la ejecución remota de código arbitrario en Android continúa cotizando a dos millones y medio de dólares. No hay cambios respecto a la cifra de remuneración desde hace bastante tiempo.

Típicamente, Google libera un grupo de parches se seguridad cada mes. Por lo que han sido publicados seis boletines que suman un total de 246 CVEs o vulnerabilidades corregidas. **26 de ellas, críticas**.

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 los componentes afectados.

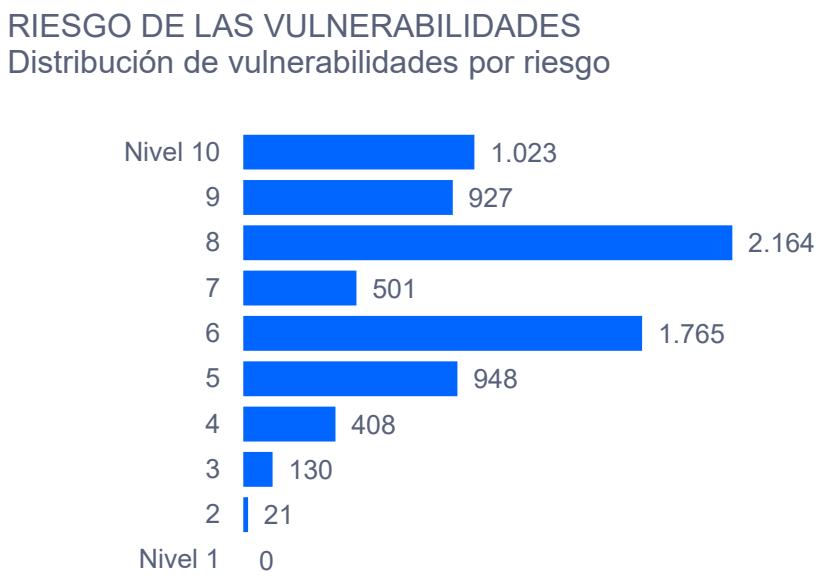
4. Vulnerabilidades destacadas

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

CVE ID	OBJETIVO	DESCRIPCIÓN	*SCORING*
CVE-2021-24092	Windows Defender	Una escalada de privilegios en BTR.sys a la hora de analizar archivos. Lo curioso es que había permanecido oculto durante más de 12 años. Quizás porque el fichero no permanecía siempre en disco, sino que se almacenaba y cargaba ocasionalmente cuando era necesario.	7.8
CVE-2020-9592 y CVE-2020-9596,	Adobe reader (aunque el problema es del estándar PDF)	El fallo también llamado “Shadow attacks”, permite realizar cambios en un PDF incluso después de estar firmado criptográficamente, dejando la firma intacta.	7.8
CVE-2021-21972	vCenter de VMWare	Con solo realizar una simple petición HTTP a la API de vCenter es posible explotar la vulnerabilidad y permitir a un atacante sin privilegios, acceder a todas las máquinas virtuales administradas por el sistema.	9.8
CVE-2021-22986	F5 BIG IP y BIG IQ	Combinando otras vulnerabilidades existentes para autenticarse, este fallo permitía un control total del sistema. Durante el primer semestre se detectaron escaneos masivos para encontrar servicios vulnerables gracias a la facilidad para explotar el problema.	9.8
CVE-2021-3604	Primion-Digitek Secure 8	Este dispositivo de control de acceso permite al atacante extraer información de usuarios y cuentas de administrador almacenados en la BDD a través de una Blind SQL Injection.	9.8
CVE-2021-28111	Dräger X-Dock	Estos detectores de gas almacenan credenciales embebidas y podrían ser explotadas por un atacante, pudiendo ejecutar código de forma remota.	8.8
CVE-2021-22667	Advantech BB-ESWGP506-2SFP-T	Se ha publicado un *0 day* sobre estos *Switches* industriales PoE. Permiten acceder a través de telnet a la contraseña de administrador que almacenan en claro	8.8
CVE-2021-28797	QNAP Surveillance Station 5.1.5.4.3 y 5.1.5.3.3	Una vulnerabilidad de desbordamiento en los NAS destinados a vídeo vigilancia permitiría a un atacante ejecutar código arbitrario.	9.6

4.1. Las vulnerabilidades en cifras

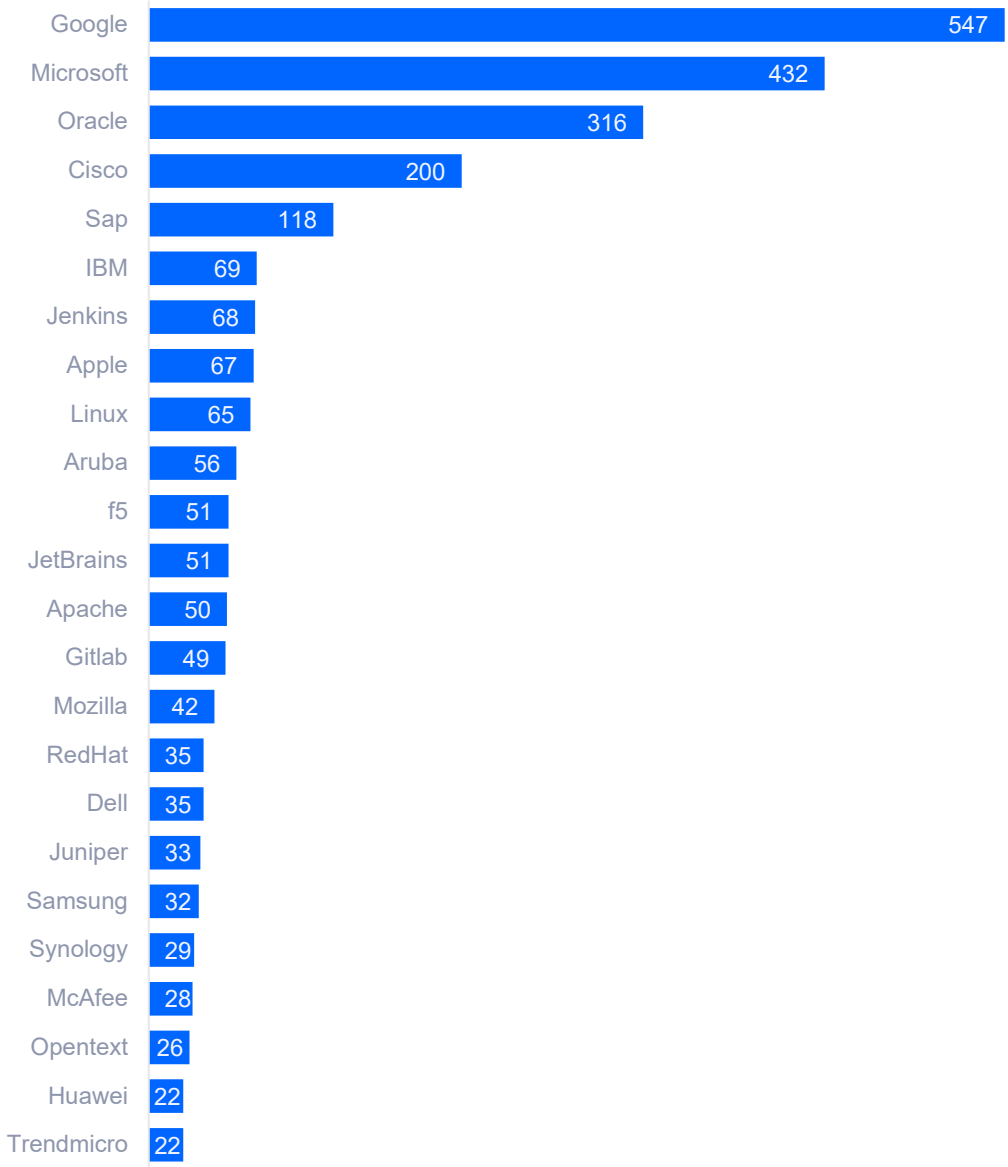
En números concretos de vulnerabilidades descubiertas durante este semestre, la distribución de CVE publicados por nivel de riesgo (*scoring* basado en CVSSv3), ha sido la siguiente:



Top 25 compañías con más CVE acumulados

Durante ese semestre, Google ha liderado por número de vulnerabilidades conocidas. Le sigue Microsoft y Oracle por número en este semestre.

Vulnerabilidades por fabricante (TOP 25 fabricantes por CVE acumulados)



5. 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.**

5.1. Metodología

Hemos realizado algo muy simple. Hemos recopilado y procesado toda la información de CVEs acreditadas durante el primer semestre de 2021. 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 384 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 440). 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 2021 H1.

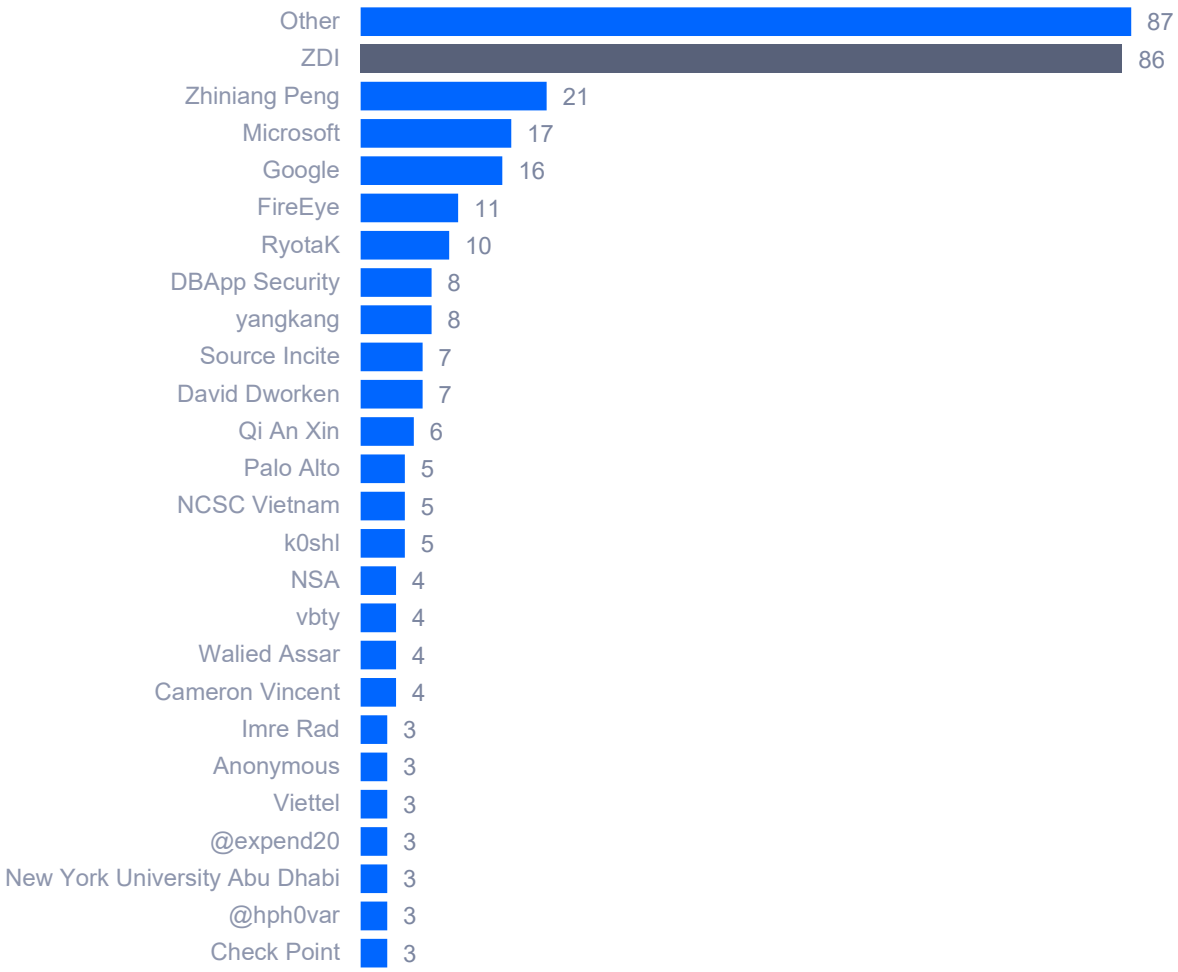
De los créditos, hemos extraído la compañía que ha descubierto la vulnerabilidad. **En el caso de que sean varios los descubridores, hemos contado solo al que aparecía en primer lugar, para simplificar los cálculos** y porque entendemos que se muestra como principal analista el que las reportó en primer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

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 de nuevo este trimestre Zhiniang Peng como un actor muy relevante con 21 fallos.

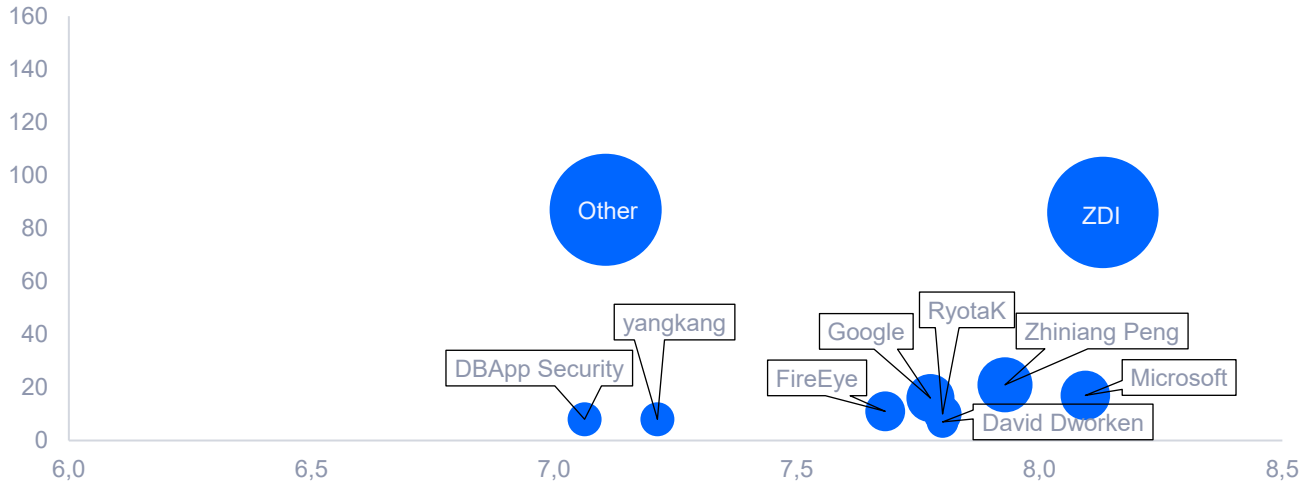
ZDI ES EL GRUPO QUE MÁS VULNERABILIDADES DESCUBRE EN PRODUCTOS DE MICROSOFT

Número total de vulnerabilidades por cada descubridor en el primer semestre de 2021



ZDI TAMBIÉN DESCUBRE LOS FALLOS MÁS GRAVES

Distribución de vulnerabilidades por gravedad y por descubridor; el tamaño de la burbuja es proporcional al número de vulnerabilidades descubiertas durante 2021 H1.



6. 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 2021

Pinchy Spider: Picadura mortal.

Este grupo, que ofrece su conocido *ransomware* "REvil" en modelo "RaaS" (*Ransomware-as-a-Service*), ha vuelto a la palestra porque su "servicio" ha sido utilizado recientemente en ataques como el que ha afectado a Quanta Computer, uno de los ensambladores oficiales de Apple. También fue utilizado contra la compañía JBS Food, el mayor empaquetador de carne a nivel mundial.

No es la primera vez que la araña pica. Su anterior creación, también en formato RaaS, fue GandCrab. Y eso fueron palabras mayores... GandCrab se detectó en 2018 y tras un año y medio dejó más de un millón de víctimas. En sólo dos meses cobró más de 600.000 dólares de entre 50.000 víctimas, aproximadamente.

Y por si todo esto fuera poco, según investigadores de Flashpoint, el *malware* que golpeó a la entidad Colonial Pipeline, y que puso en jaque al suministro de hidrocarburos de la costa este de los EEUU, estaría basado en REvil ¿Será el grupo "Darkside" afiliado de REvil? ¿Será una escisión de la araña? Lo cierto es que su red parece bastante extensa y difícil de detectar.

Judgment Panda: Juez, parte y panda.

En marzo, servicio de inteligencia y seguridad finés (SUPO), anunció que los ataques contra el parlamento de Finlandia, en otoño de 2020, fueron parte de una campaña de espionaje llevada a cabo por este grupo (conocido también como APT31) vinculado con el gobierno chino.

Si bien la noticia de la atribución sí es de 2021, los actos son de 2020.

Agrius APT: Nuevos en la ciudad (o no)

"Agrius" es un nuevo grupo, detectado en 2020, relacionado con Irán y otros países vecinos. Sus TTP incluyen el uso de un *wiper* compartido anteriormente por APT-33 y APT-34, dos grupos también con origen iraní.

Por cierto, según uno de los grupos de investigadores que han estado rastreando desde 2020 su actividad, la mayor actividad de este grupo en este año coincide con la vuelta de las tensiones en la franja de gaza y el lanzamiento de misiles entre Israel y Hamas (y otros grupos): a inicios de mayo.

¿Casualidad?

7. Análisis de amenazas OT

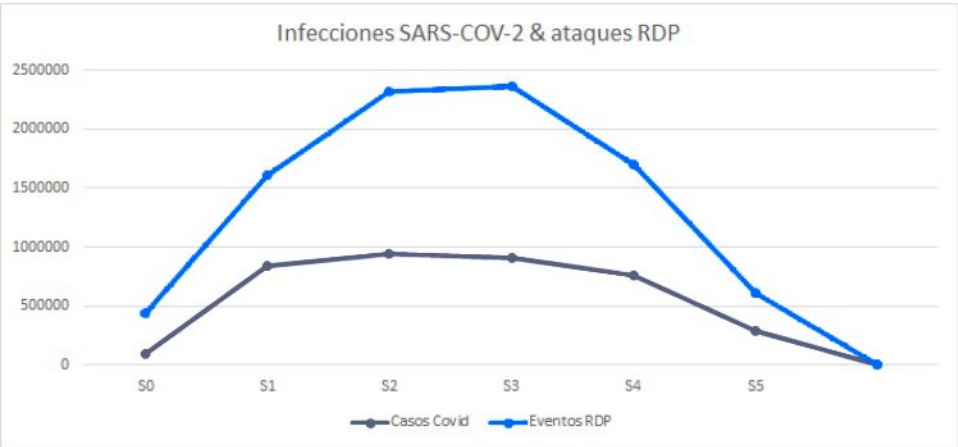
La siguiente información procede del sistema para la captura y análisis de amenazas en el ámbito OT, Aristeo. **Aristeo** incorpora una red de **señuelos, fabricados con hardware industrial real,** que aparentan ser sistemas industriales en producción real, **y se comportan como tales**, pero que están 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**

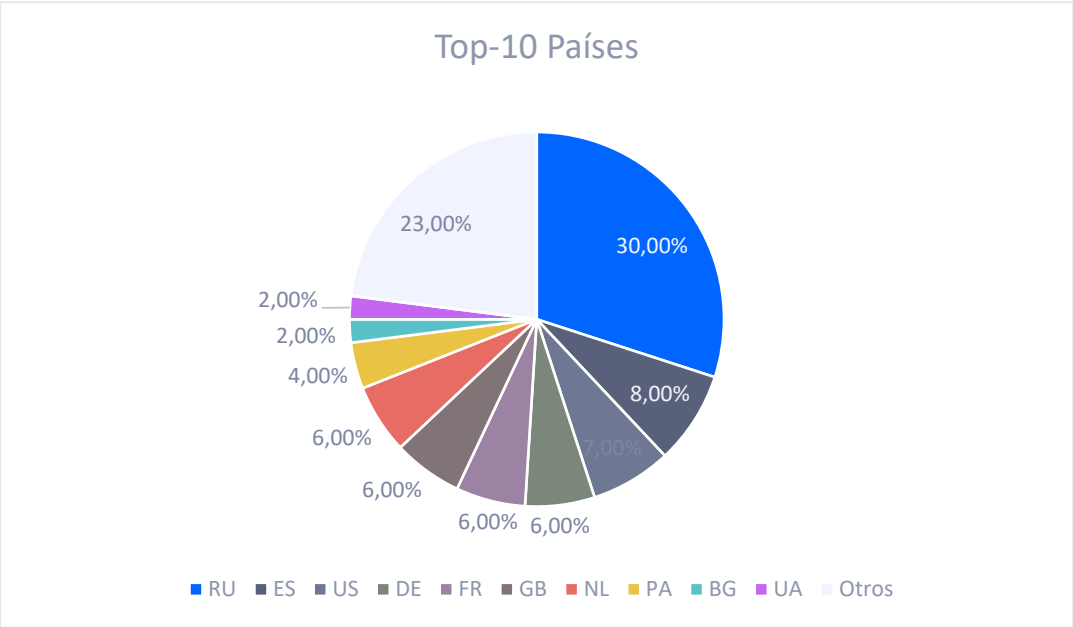
Análisis de la información

Inauguramos esta sección con uno de los temas candentes en los últimos meses. Ciberseguridad y COVID-19. Siempre se ha comentado que los delincuentes son los que mejor conocen la sociedad y sus realidades, su legislación... Cuando desplegamos el primer nodo de Aristeo, comenzamos a percibir una variación en los datos a medida que la pandemia iba aumentando o disminuyendo su incidencia. Decidimos analizar la información para comprobar si nuestra percepción era correcta. La respuesta es el siguiente gráfico, en el que se enfrentan los datos Covid con los datos de eventos de RDP en el mes de enero de 2021 separado por semanas. La S0 es la última de diciembre de 2020 (para observar el cambio desde el inicio de aquella ola).

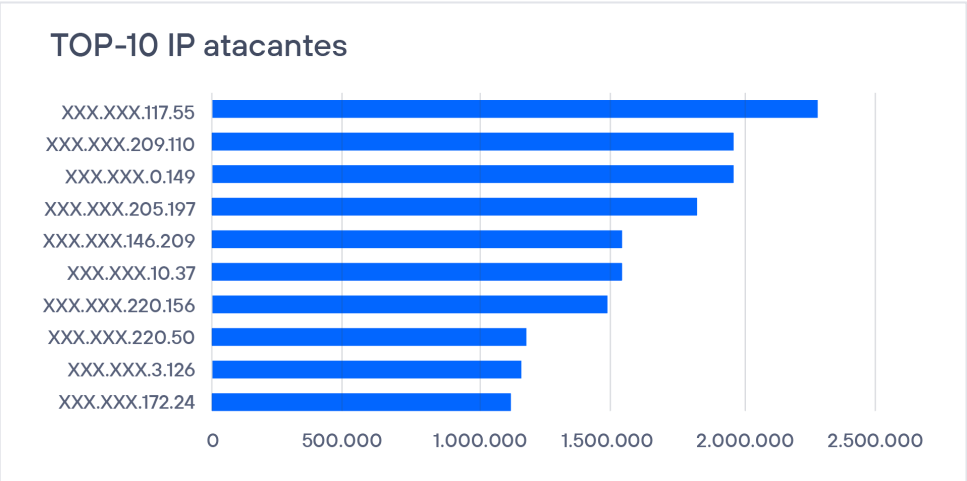


Los datos de las amenazas cibernéticas provienen en su totalidad de nuestro sistema, mientras que los datos sobre la amenaza que supone el SARS-COV-2 provienen de varios gobiernos y entidades investigadoras de reconocido prestigio. Aun así, dado que se han aglutinado datos de España, Francia, Alemania, Italia y Reino Unido, y que la actualización y trazabilidad de esta información no siempre es la mejor, la comparativa ha supuesto un gran desafío. No obstante, finalmente la gráfica sí muestra esa tendencia que nosotros intuíamos. **Los atacantes incrementaban el número de ataques contra los dispositivos que exponían un RDP (en nuestro caso, una bahía de ingeniería que controla el proceso industrial y sirve para administrar los dispositivos industriales en un nodo).**

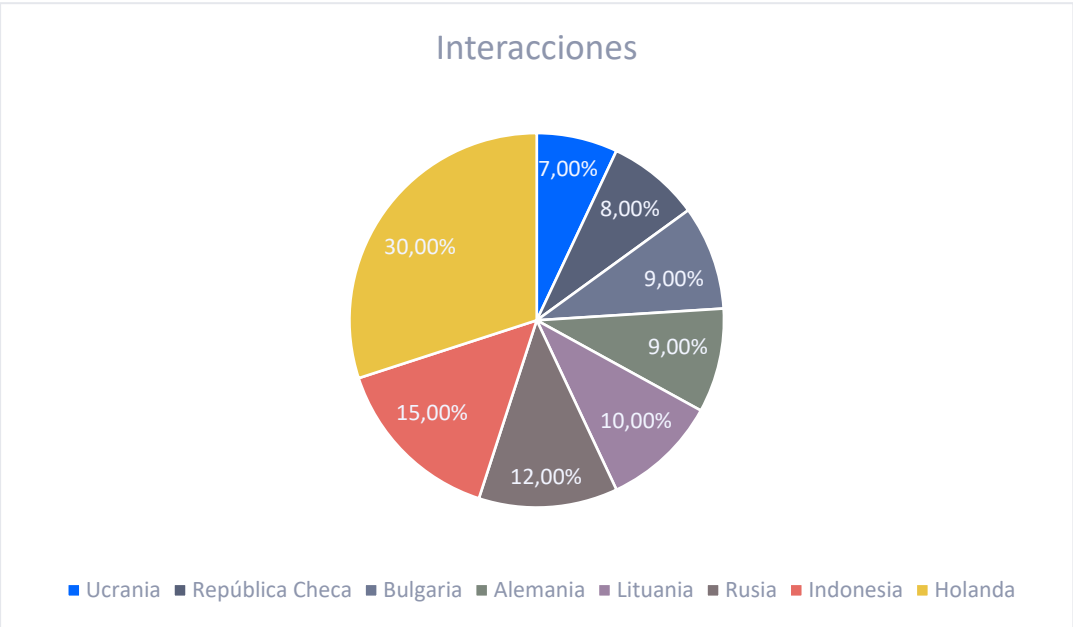
Pasamos a la estadística genérica de la información registrada. En el primer semestre de 2021 se detectaron **más de 246 millones de eventos de ciberseguridad**. Mayoritariamente, los eventos han estado relacionados con ataques de RDP más o menos sofisticados. La distribución por países sería la siguiente:



A continuación, podemos observar el Top-10 de las direcciones IP con más interacción con el sistema de Aristeo y sus países de referencia.



A continuación, observamos cómo se reparten las IP con más actividad. Como dato curioso, diremos que la dirección IP con más interacciones corresponde aparentemente a un entorno gubernamental de un país de los que figuran en el gráfico, (**y no es Rusia)**.



8. 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 en el primer semestre de 2021.

CRIPTOGRAFÍA

El cifrado plausiblemente negable o cómo revelar una clave sin revelarla

Criptografía chivata: cómo crackear dispositivos inviolables

Criptografía funcional: la alternativa al cifrado homomórfico para realizar cálculos sobre datos cifrados

El puzle por el que ofrecen un trillón de dólares a quien lo resuelva

La fiebre por los NFT: la última criptolocura que está arrasando Internet

Desenmarañando el enredo cuántico de la ciberseguridad: ordenadores cuánticos, criptografía cuántica y post-cuántica

El futuro de las credenciales universitarias apunta hacia Blockchain y Open Badges

Recupera el control de tus datos personales gracias a la Identidad Descentralizada sobre Blockchain

En Internet nadie sabe que eres un perro ni aunque uses certificados TLS

Las 26 razones por las que Chrome no confía en la CA española Camerfirma

MALWARE

El Malware Móvil, parte de la Generación Z

Usando a DIARIO la FOCA para análisis de malware

Fileless malware: ataques en crecimiento pero controlables

Ciberseguros y cibercrimen ante “la devastadora epidemia global de ransomware”. Se eliminan coberturas

Y el presidente dijo “ya está bien”. Las nuevas propuestas en ciberseguridad desde la Casa Blanca

Qué demonios está pasando con el ransomware y por qué no vamos a detenerlo a corto plazo

Tu sistema macOS también es objetivo del cibercrimen, ¡fortalécelo!

INTELIGENCIA ARTIFICIAL

Cómo engañar a las apps que usan Deep Learning para la detección de melanomas

Telefónica Tech

Sobre Telefónica Tech

Telefónica Tech es un holding de empresas propiedad del grupo Telefónica. La compañía cuenta con una amplia oferta de soluciones tecnológicas llegando a más de 5,5 millones de clientes en 175 países. Telefonica TECH podrá albergar otros negocios digitales a futuro, incluso del segmento B2C.

Más información

tech.telefonica.com