Telefónica Tech

Informe sobre el estado de la seguridad 2022 H2

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

Índice

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 segundo semestre de 2022 se ha caracterizado por varios ataques a grandes compañías que han dado mucho que hablar. Por ejemplo, a Uber, en el que se usó una forma muy humana de eludir el segundo factor de autenticación: la "fatiga" del administrador al recibir decenas de mensajes pidiendo confirmación de acceso, en un corto periodo de tiempo y además en horas poco adecuadas. Otro ataque sonado en LastPass ha puesto en duda, de nuevo, la seguridad del uso de gestores de contraseñas en la nube. Otras muchas empresas e incluso países han sufrido ataques, aunque solo los hemos visto reflejados en sus consecuencias: los *leaks*. En este último semestre de 2022. Cisco, Microsoft, Toyota, Revolut... E incluso se han filtrado datos personales de la población China.

En contraposición, los ataques con las macros de Office como vector de ataque han disminuido. La razón es que cada vez Microsoft le ha puesto más difícil para su ejecución por defecto y los atacantes han agotado buena parte de todas las posibilidades técnicas para eludir los controles, alertando así a los EDR y sistemas de protección para poder cazar las nuevas fórmulas de ejecución. De ahí que los atacantes estén buscando nuevas fórmulas, más complejas pero quizás efectivas como pueden ser los *zero days* en Chrome, que a pesar de su dificultad para encontrarlos y desarrollarlos, han sido nueve en 2022.

Pero en este panorama, el ransomware profesional se mantiene como la joya de la corona de los atacantes, porque sigue siendo un negocio lucrativo. Pero, ¿cuánto? Existen muchas estimaciones, y todas pueden ser más o menos exactas. A finales de 2022, el FBI ofreció un dato concreto que parece bastante fiable: Hive, una de las organizaciones de ransomware más activas, había ganado 100 millones de dólares de 1300 víctimas. Y todo desde junio de 2021, momento en el que se comenzó a observar actividad. Durante un tiempo compartieron recursos con la banda Conti. Este dato nos da una media de unos 77.000 dólares por víctima. La media es tentadora pero no refleja la realidad, porque Hive ha dado golpes muy lucrativos y sonados cuyo botín se sale mucho de esa media. De hecho, Hive publica en su web junto con cada víctima, el número de empleados y los beneficios de la empresa. Ofrece una pista de cuánto pueden llegar a extorsionar en función de estos parámetros. De media resulta en 81 víctimas por día todos los días. Algunos de estos ataques habrán requerido meses de preparación, otros golpes serán más rápidos. Pero la conclusión cierta de estos números (que tampoco podemos garantizar, porque habrá víctimas que nunca salen a la luz) es que el trabajo de Hive en particular y las bandas de ransomware en general está engrasado. Esa infraestructura requiere inversión en captar víctimas, atacarles (entrar en sus sistemas), tiempo en red, atención a la víctima para el cobro, lavar dinero, etc. También cabe destacar que las bandas no suelen ser muy numerosas, al menos en su core técnico, por tanto concluimos que son muy productivos por atacante.

Este semestre, además de mantener nuestra sección especializada en el análisis de amenazas en el ámbito industrial gracias a nuestro proyecto Aristeo, añadimos Maltiverse como plataforma de consulta para analizar los principales IoC de la industria.

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 2022

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

JULIO

- Maddie Stone, una de las principales investigadoras del equipo Project Zero de Google, encargado de encontrar, analizar y tratar de colaborar con fabricantes para solucionar las temidas vulnerabilidades 0-day, publicó un duro informe donde señala que durante el **primer semestre de 2022 más de la mitad de las vulnerabilidades 0-day son variantes de vulnerabilidades ya conocidas.** Esto demuestra una falta de análisis de causa raíz por parte de los fabricantes en la resolución de las vulnerabilidades.

- Microsoft sigue recapacitando sobre las macros y su impacto. En menos de dos semanas pasa de bloquearlas completamente para documentos descargados de internet a revertir el cambio para finalmente volver a instaurarlo.

- China sufre la primera fuga de información a gran escala, al menos la primera que ha visto la luz pública. Varios medios internacionales han contrastado la autenticidad de la muestra publicada en un foro de la DarkWeb que parece formar parte de una base de datos de la policía Nacional de Shangai y que según el anunciante ChinaDan consta de **datos de más de 1.000 millones de ciudadanos chinos** con información sensible como nombres, direcciones, números de identidad, de teléfono móvil y registros policiales y médicos.

- **Prestashop**, la plataforma de e-commerce de código abierto más popular en Europa y Latinoamérica, utilizada por alrededor de 300.000 clientes en todo el mundo, detecta un ataque que utilizando una combinación de vulnerabilidades, incluido un **0-day de inyección SQL, permitía la ejecución de código con el objetivo de robar información de pago de los clientes.** PrestaShop han publicado una serie de comprobaciones para verificar la afectación y recomendaciones como deshabilitar la función MySQL Smarty Cache que fue empleada para realizar los ataques.

- **"Rolling-PWN"**: El fabricante de vehículos **Honda va a rediseñar los automóviles** más recientes para eliminar una vulnerabilidad que aparentemente afecta a **modelos desde 2012 hasta 2022**. El problema está relacionado con la apertura a distancia con mando. Se descubre una vulnerabilidad en el sistema de rotación de claves del generador aleatorio de claves que los fabricantes utilizan para evitar ataques de repetición y que les permite volver a usarlos para abrir el coche o incluso arrancarlo.

- El SEMAE (Servicio Municipal de Agua y Alcantarillado) del municipio de São Leopoldo, en Brasil, sufre un ciberataque la semana del 4 de julio. Se ejecutó un ransomware que cifró incluso las copias de seguridad. Este municipio tiene más de 230.000 habitantes.

AGOSTO

- **Twilio**, un gigante de la gestión de los SMS así como otros canales de contacto con cliente sufre un ataque de phishing que afecta a 163 clientes. No parece muy relevante siendo un 0,06% de su base de clientes, pero su rol particular en el ecosistema digital hace que la importancia del ataque sea mucho mayor y evidencie su sofisticación. Un **ataque dirigido a una compañía que da servicios de SMS** que pueden servir como **segundo factor de autenticación** para sus clientes corporativos, como Signal , Okta o Authy **es significativo ya que puede desencadenar múltiples ataques de cadena de suministro.**

- Google informa del **mayor ataque DDoS** (denegación de servicio distribuido) **de la historia**. Un cliente de Google Cloud Armor recibió una serie de ataques HTTPs que alcanzaron los 46 millones de solicitudes por segundo y tuvo una duración de algo más de una hora. El ataque se ejecutó usando solicitudes desde más de 5000 direcciones IP distribuidos en más de 100 países. Los investigadores señalan por las características del ataque que puede estar **relacionado con la botnet Mēris.**

- Los dueños de servidores on-premises de confluence (Confluence Server and Data Center) en particular aquellos que usan una de sus aplicaciones más populares llamada Questions for confluence, deben actualizar debido a una vulnerabilidad crítica (CVSS 9.9) producida por unas **credenciales incrustadas que daban acceso a dichos servidores y que fueron publicadas en Twitter solamente un día después de que Atlassian publicase el parche** que deshabilitaba a ese usuario.

- Un desarrollador llamado Stephen Lacy descubre un curioso ataque de malware en Github. Un atacante creó más de **35.000 repositorios con copias de repositorios muy populares a los que añadió malware**. Si un usuario utilizase la copia modificada en vez del original el atacante obtendría sus variables de entorno y una puerta trasera a sus sistemas. Github eliminó los repositorios identificados como maliciosos en el periodo de una semana.

- **La autenticación multi-factor se asienta como requerimiento en las plataformas de desarrollo y publicación de software**. Este mes RubyGems (Ruby), se une a npm (javascript), NuGet (.Net) and PyPi (Python) en anunciar la obligación de usar un doble factor de autenticación (al menos para las librerías con más descargas) para poder publicar librerías o paquetes de software. Esta tendencia puede formar parte del empuje de una mayor seguridad en la industria del software pero también puede derivar del rápido incremento de incidentes en proyectos opensource relativamente pequeños que desencadenaron enormes ataques de cadena de suministro.

- Un atacante consigue utilizar una URL olvidada en el proceso de instalación del panel de administración web de cajeros de bitcoin gestionados por Crypto Application Server (CAS) de la compañía General Bytes. Así consiguió **acceso como administrador y reconfiguró el cajero** para que cuando un usuario enviase dinero al cajero para ser recogido en persona, este dinero fuese redirigido a la cartera (wallet) del atacante.

- El grupo CL0P publica en su sitio en TOR un anuncio en el que asegura haber atacado con éxito a la compañía Thames Water, llegando incluso a los sistemas SCADA y paneles de control. Sin embargo, este anuncio incluye información de esa empresa y además de otra llamada South Staffordshire PLC. Esta última empresa reconoció el ataque, indicando que el suministro de agua no se vio afectado gracias a “los sólidos sistemas y controles sobre el suministro y la calidad del agua” que

tienen implementados. Por su parte, este grupo de ciberdelincuentes publicó imágenes del HMI y afirmó que "sería fácil cambiar la composición química de su agua, pero es importante tener en cuenta que no estamos interesados en causar daño a las personas".

SEPTIEMBRE

- Trellix publica los detalles técnicos de una vulnerabilidad a un ataque de "**path traversal" en el módulo *tarfile* de Python** conocida desde hace 15 años. Curiosamente, **en este caso no es que la vulnerabilidad pasara desapercibida, sino que no se le dio la importancia que merecía** y con la globalización del SW y las dependencias de las cadenas de suministro el impacto es mucho mayor del esperado.

- La tecnológica financiera **Revolut es víctima de un ciberataque** que afecta a algo más de **50.000 clientes**. Aunque los detalles exactos no se conocen todo indica a un ataque de ingeniería social para lograr el acceso a una base de datos de clientes que contenía información personal de los clientes como dirección, teléfono y números de cuenta. Revolut informa que los saldos de sus clientes no se han visto comprometidos y que no se accedió a contraseñas, PINs o información de tarjetas bancarias.

- Dinamarca sigue los pasos de Austria, Francia e Italia al declarar el uso de Google Analytics como ilegal dentro del país ya que incumple la normativa GDPR. La agencia de protección de datos danesa insta a las empresas a ajustar la herramienta usando un *proxy inverso* para pseudonimizar la información antes de enviarla a los servidores de Google en USA o a dejar de usarlo.

- Hasta ahora una detección del uso de *Cobalt Strike* era un claro indicador de un ataque en curso. Desde este septiembre los equipos de defensa tendrán que añadir el uso de ***Brute Ravel*** otra herramienta de *redteam* de coordinación de comunicaciones post-explotación como indicador de una operación después de que una **versión crackeada de este software fuera puesto a disposición de los cibercriminales** en múltiples foros *underground*.

- Se acabó la relativa calma en **MS Exchange** después de lo ocurrido con *ProxyShell*. En septiembre se detectan **dos vulnerabilidades críticas que estaban siendo explotadas activamente**. la presencia y combinación de ambas vulnerabilidades de forma encadenada da lugar a la ejecución remota de código, elevación de privilegios y poder finalmente hacerse con el control del servidor. Se estima que **afecta a más de 200.000 servidores de correo**, Microsoft estuvo trabajando fuera de ciclo para parchear las vulnerabilidades dada la urgencia de la situación.

- El Estado Mayor General de las Fuerzas Armadas de Portugal reconoce dos ciberataques que fueron detectados a través de los documentos encontrados por los USA a la venta en la Darkweb. El Presidente del Observatorio de Seguridad Interior indicó que se trata de un "daño reputacional irreparable" y urgió a contratar más personal en ciberseguridad.

OCTUBRE

- El **gusano *Raspberry Robin*** que se propaga mediante dispositivos USB infectados ha ido acaparando noticias en los últimos meses infectando a un alto número de sistemas Windows. El CERT de Deutsche Telekom detectó que muchas de las infecciones podrían ser rastreadas hasta el uso de dispositivos USB en tiendas de impresión y fotocopias. El *framework* que usa el malware

Raspberry Robin post-infección utiliza **técnicas avanzadas de ofuscación, anti-sandboxing y evasión de herramientas de seguridad, incluso realiza la instalación de malware falso** para confundir a los investigadores sobre lo que están analizando.

- Una v**ulnerabilidad crítica en OpenSSL pone** en alerta a los principales equipos de administración de sistemas durante una semana este octubre. Algunos compararon con Heartbleed, finalmente baja su criticidad de crítica a alta. Sigue siendo una vulnerabilidad importante porque **puede dar lugar a ejecución de código arbitrario** o una denegación de servicio en determinadas condiciones. **La explotación, de todas formas, no es sencilla** ya que se cuenta con poco espacio útil para lanzar el ataque y es necesario que el certificado digital esté firmado o sea aceptado por el usuario.

- Un experto en criptografía americano Nicky Mouha descubre una vulnerabilidad de **buffer overflow** en la implementación de **SHA-3** en una **conocida librería opens ource llamada XKCP** que proporciona varios esquemas criptográficos. Los atacantes podían ejecutar código arbitrario y eliminar propiedades criptográficas esperadas en SHA-3. Se generan parches para las distribuciones de XKCP para Python, Ruby y PHP.

- Se publica un primer draft de especificación para **nuevo estándar** del W3C (World Wide Web Consortium) **para estandarizar la URL de cambio de contraseña** con un formato como el que sigue: *https://example.com/.well-known/change-password.* La idea propuesta por dos ingenieros de Apple es permitir a herramientas automatizar el descubrimiento de las páginas de cambio de contraseña y por tanto facilitar al usuario el cambio de contraseñas en varios servicios de forma automática.

- La popular **plataforma de e-commerce Magento**, ahora llamada Adobe Commerce, se ve afectada por dos vulnerabilidades, una de ellas calificada como **crítica de Cross-Site Scripting**, que usadas de forma combinada permitía a un atacante ejecutar código arbitrario. Adobe publica parches para las versiones afectadas, sin embargo, algunas firmas de seguridad especializadas en Magento como Sansec sugieren realizar una actualización a nuevas versiones de la plataforma en vez de aplicar los parches disponibles siempre que sea posible, lo que denota que el parche no soluciona la causa raíz del problema.

- Un informe de Symantec descubre que el **grupo de espionaje *The Wichetty* ocultó *mlaware* en un viejo logo de Windows** que se descargaba de una fuente pública confiable para no levantar sospechas y que posteriormente se extraía el backdoor mediante el tratamiento de dicha imagen. Symantec describe los ataques analizados estaban dirigidos a dos gobiernos de Oriente Medio y una bolsa de un país africano, **victimas relevantes para un ataque con el uso de técnicas sofisticadas como esta**.

- El Centro Nacional de Energías Renovables sufre un ciberataque que deja sin acceso a los sistemas a toda la plantilla localizada en la localidad navarra de Sarriguren. En abril, el fabricante de aerogeneradores, Nordex, también sufrió un ciberataque que dejó sin acceso a un número indeterminado de los aproximadamente 1000 trabajadores que tiene la empresa en Navarra.

NOVIEMBRE

- Investigadores de Kaspersky identifican una **campaña de phishing** que emplea una novedosa técnica de ocultación, **a través de enlaces de Google Translate**. Desde el punto de vista del usuario, este verá un enlace a un servicio aparentemente legítimo de Google que se encarga de traducir al vuelo el sitio web y servir el contenido, en este caso, malicioso, a través de una conexión aparentemente inocua. **Evadiendo así una de las defensas tradicionales de comprobación de dominios que un usuario tiene para detectar phishing**.

- La policía nacional emitió un comunicado anunciando la detención de 6 integrantes de una **banda de criminales que habían estafado mediante phishing más de 12 millones de euros a un total de casi 300 víctimas**. La investigación comenzó con una denuncia de una entidad financiera española que estaba siendo suplantada para ofrecer **falsas operaciones financieras de renta variable y criptomonedas** a clientes franceses.

- **La atribución del origen de un grupo de ciberatacantes siempre es complicada** y rara vez se indica de una manera categórica en los informes de investigadores de seguridad**.** Este noviembre se filtraron los chats internos de la banda *Yanluowang* y se pudo evidenciar que sus miembros no eran ciudadanos de origen chino sino ruso.

- Con el rápido crecimiento de usuarios que la red social **Mastodon** ha experimentado como resultado del éxodo de *twitter* era una cuestión de tiempo que **alguien utilizase la infraestructura** de dicha red social, en este caso distribuida, **para configurar las comunicaciones de un *Command & Control***. El atacante utilizaba la página "about me" para indicar al malware que se conectaba al servidor de mastodon *ioc.exchange* donde encontrar el C2 real.

- **Github** añade una funcionalidad que permite a los investigadores de seguridad **informar de vulnerabilidades en repositorios públicos a sus respectivos dueños a través de un canal privado**. Esta funcionalidad ayudará a los investigadores a no tener que utilizar el sistema de incidencias que es visible para el público en general incluyendo potenciales atacantes. Otro paso más en la **securización del código de fuente abierta que está tan en el punto de mira tras los graves incidentes de cadena de suministro como Log4Shell**.

- El equipo Project Zero de Google advierte de que existe un **importante retraso en el parcheo de vulnerabilidades en el ecosistema de Android**. En concreto, tras detectar cinco vulnerabilidades explotables en el **driver de GPU de ARM Mali** y trabajar con ARM en la generación de los parches a nivel de usuario final estas vulnerabilidades siguen siendo explotables ya que **los fabricantes de telefónos Android como Googlem Samsung, Xiaomi, etc. no los han trasladado aún a los usuarios de sus teléfonos**.

- Un actor malicioso denominado Ryushi pone a la venta en un conocido foro clandestino una **base de datos de 400 millones de usuarios de Twitter**. El vendedor afirma que los datos fueron extraídos a través de una vulnerabilidad e incluyen correos electrónicos y números de teléfono de usuarios de la plataforma. Esta noticia salta después de que a **principios de año** Twitter ya reconociese la autenticidad de un *leak* que fue puesto a la venta en la DarkWeb con **datos personales de 5.4 Millones de usuarios y por los que la agencia de protección de datos irlandesa mantenía una investigación en curso por incumplimiento de GDPR**.

- Los investigadores de Microsoft se encontraban investigando una serie de ataques contra la red eléctrica india cuando advirtieron el uso del Webserver Boa como vector de acceso en los ataques. Este software se utiliza en routers, cámaras de seguridad y otros dispositivos IoT relacionados con el mundo OT... y carece de soporte desde 2005. Estos investigadores aseguraron también que han identificado más de un millón de componentes de este tipo.

DICIEMBRE

- Los **certificados de sistema de Android de Samsung, LG, mediatek y otros fabricantes** son **usados para firmar *apps* maliciosas con *malware***. Esto es un problema grave ya que los certificados de sistema son considerados por Android como fuertemente confiables y por tanto tienen acceso a casi todo el sistema. Tras el hallazgo investigadores de seguridad de Rapid7 puntualizaron que, aunque la firma de malware suele asociarse con cibercriminales esponsorizados por estados en este caso **algunas de las apps firmadas eras simple adware lo cual puede denotar que esos certificados han estado ampliamente disponibles en foros** *underground***.**

- **Noveno 0-day publicado para Google Chrome**, en este caso una vulnerabilidad de confusión de tipos. La explotación de este fallo de seguridad podría permitir a un atacante remoto explotar potencialmente la corrupción de la pila a través de una página HTML manipulada. Desde un tiempo a esta parte la cantidad de fallos graves en Chrome ha ido aumentando de forma significativa. Google da sus razones para ello, pero también es cierto que **la rentabilidad de las vulnerabilidades en el motor *chromium* es mucho mayor ahora ya que afecta a los navegadores Chrome, Edge, Opera**. En definitiva, se trata de un punto crítico muy apetitoso para los atacantes.

- Tras un año de **Log4Shell**, la plataforma de gestión de vulnerabilidades Tenable, publica que tras una serie de pruebas concluye que **el 72% de las organizaciones todavía es vulnerable** a Log4Shell y que **desde mayo de 2022 hasta octubre de 2022 las organizaciones que han remediado la vulnerabilidad se ha doblado pasando a formar el 28% restante.**

- Dos investigadores de seguridad de Kaspersky y Stairwell publican un **plugin para IDA Pro que usa el famoso modelo de lenguaje de inteligencia artificial *chatGPT* para explicar las funciones decompiladas**. Una gran **advertencia: las explicaciones pueden no ser precisas**, sin ir más lejos StackOverflow ha prohibido las respuestas generadas por ChatGPT debido a la gran cantidad de errores que contenían.

- **Tras innumerables incidentes de seguridad accidentales, por fin el servicio de almacenamiento en la nube AWS S3 ha decidido finalmente cambiar sus opciones por defecto de "público" a "bloquear el acceso público"**. Esto revela la importancia de los valores por defecto y el principio de privacy-by-default. A partir de abril de 2023 si realmente se quiere tener un contenido en S3 abierto al público en general se deberá desplegar una ACL (Access Control List) para hacerlo efectivo.

- LastPass anuncia que su sistema de almacenamiento en la nube fue vulnerado mediante claves de acceso robadas en un incidente del pasado mes de agosto, donde los atacantes tuvieron acceso a información técnica y código fuente de la compañía. **Aprovechando estas claves, los autores del ataque lograron robar información de cuentas de clientes y datos almacenados en el *vault*, incluyendo contraseñas y notas**. Si bien los datos del *vault* están cifrados, la empresa ha avisado

a sus clientes que los que **atacantes podrían intentar hacer fuerza bruta contra sus contraseñas maestras y obtener acceso a toda la información almacenada**. Además, en su último comunicado LastPass admite que las urls de un determinado cliente no están cifradas sino simplemente ofuscadas en un formato propietario binario, esto es un problema ya que un atacante sabiendo las webs que usas puede lanzar un ataque de phishing dirigido con muchas más posibilidades de éxito.

- La NSA, la CISA y ODNI, publican un documento donde se presenta tanto los beneficios como los riesgos asociados con la división de redes 5G. También proporciona estrategias de mitigación que abordan las posibles amenazas a la división de redes 5G. La guía se basa en los vectores de amenazas potenciales para la infraestructura 5G de ESF, publicados en 2021. La técnica de Network Slicing es especialmente útil para redes 5G en usos profesionales e industriales.

MÓVILES

Apple iOS

Nuevas características de seguridad

Cerramos el año 2022 con iOS 16.2 (segunda revisión de la versión 16) publicada el 12 de septiembre de 2022. Vamos a reseñar las principales características de seguridad que nos ha traído iOS 16.

La nueva versión de iOS ya incluye el anunciado "Lockdown Mode", un modo especial de funcionamiento en el que el sistema restringe varias funcionalidades que contribuyen a aumentar la superficie de exposición frente a nuevos exploits. Por ejemplo, en este modo la aplicación "Messages" bloquea todos los adjuntos a excepción de imágenes o la creación de vista previa en enlaces. No es un modo dirigido al usuario medio, sino a un público expuesto a ataques muy concretos.

iOS 16 incorpora una nueva funcionalidad para aliviar el uso de contraseñas y sus múltiples errores conceptuales: "Passkey" permite el uso de autenticación sin contraseñas en servicios que implementen el protocolo WebAuthn, apoyándose en la verificación biométrica que ya proporcionan los dispositivos, esto es: Face ID y Touch ID.

Una de las funcionalidades que más pueden llamar la atención es la que se denomina "Rapid Security Responses". Es una nueva capacidad del sistema operativo para instalar actualizaciones de seguridad de modo que no sea necesario realizar una actualización completa sino más frecuente según estén disponibles los parches, tal y como se venía haciendo hasta ahora. Aunque opcional, se trata de una muy interesante opción para quienes deseen aplicar los parches de seguridad tan pronto como estén disponibles sin necesidad de esperar.

Vulnerabilidades

Respecto a la publicación de versiones en el segundo semestre de 2022, se abría el ciclo durante agosto con una actualización de emergencia: 15.6.1 corregía dos gravísimos problemas asociados y que en combinación podrían permitir el control del dispositivo víctima de un ataque.

Por un lado, se parcheaba una vulnerabilidad en WebKit (el motor de renderizado del navegador Safari) que permitía la ejecución de código arbitrario. Por otro, se arreglaba un fallo en el kernel del sistema que permitía idéntico impacto. Ambas vulnerabilidades han sido detectadas mientras estaban siendo activamente explotadas.

Ya en septiembre, justo cuando se estrenaba iOS 16, se publicó paralelamente iOS 15.7, la séptima revisión del sistema que venía con un lote de veinte parches de seguridad, tres de ellos de ejecución remota de código arbitrario. Llama la atención el fallo de seguridad en el "Neural Engine", un componente físico del sistema encargado de acelerar los cálculos de procesos relacionados con machine learning entre otros.

iOS 16 en su estreno llevaba consigo hasta 46 parches de seguridad, una cifra bastante abultada para el inicio de su singladura. Cuatro de los fallos corregidos permitían la ejecución de código arbitrario.

Pocos días después se liberaba un pequeño parche, 16.0.2 pero no contenía ninguna actualización de seguridad. Del mismo modo, (ahora sí con un parche de seguridad), se publica la 16.0.3 el 10 de octubre. Se

daba un problema en la aplicación Mail que podría causar una denegación de servicio al procesar correos manipulados de forma maliciosa.

El 24 de octubre nos trae la primera gran revisión de iOS 16. La versión 16.1 contenía 38 parches de seguridad, siete de ellos corrigiendo vulnerabilidades que podrían ocasionar la ejecución de código arbitrario. Para la versión 15.7 se publicaba unos días después la revisión 15.7.1 con 18 parches; dos de ellos corrigiendo ejecución de código arbitrario.

En noviembre se publicaba una actualización de emergencia debido a dos fallos críticos en la popular librería libxml2, usada por múltiples aplicaciones para el tratamiento de archivos xml.

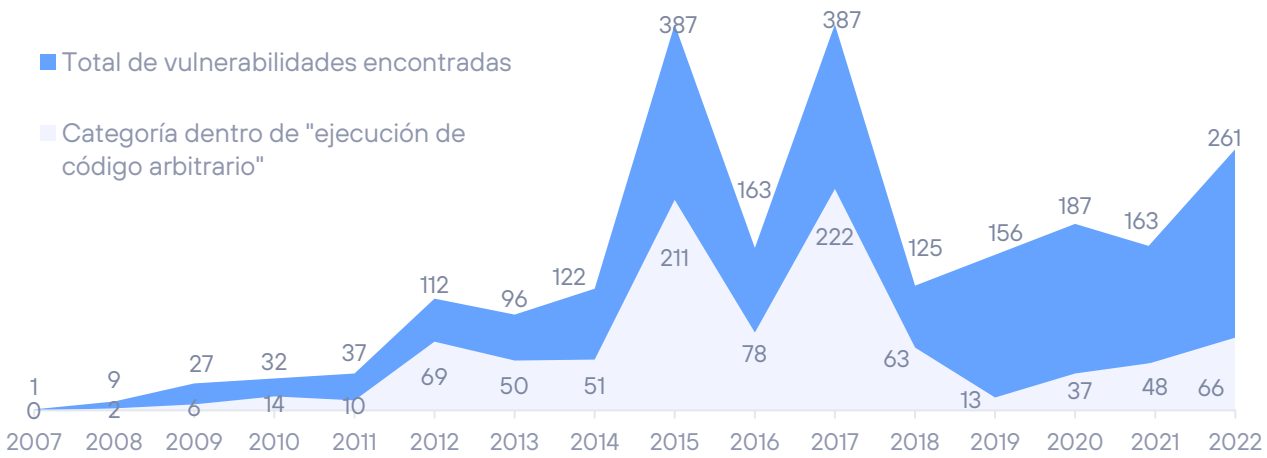
Se cerró noviembre con un susto: un parche de emergencia para Webkit que estaba siendo explotado activamente. Saltamos a iOS 16.1.2.

A mediados de diciembre, y para cerrar el año 2022, son publicadas las revisiones: iOS 16.2 y 15.7.2 respectivamente. La primera con 37 parches, 11 de ellos relativamente graves y 17 para iOS 15 con siete de ellos cerrando ejecuciones de código arbitrario.

Evolución de vulnerabilidades en iOS durante el segundo semestre de 2022

El segundo semestre de 2022 se ha cerrado con 167 vulnerabilidades únicas parcheadas, alrededor de la treintena consideradas de alto riesgo, con posibilidad de ejecutar código arbitrario. Algunas de ellas afectando al propio núcleo del sistema operativo. Se cierra así 2022 con 261 fallos corregidos. El número de fallos anual no deja de crecer desde el pico de 2017.

VULNERABILIDADES EN IOS 2022-H2
Evolución de vulnerabilidades por año



Fragmentación de versiones durante el segundo 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 indiscutible 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 (iOS 16) alcanza la plenitud de usuarios en este semestre, con una cuota conjunta (16, 16.1, 16.2) que alcanza casi el 60% de la tarta. Atrás queda iOS 15 con una resistencia aún del 25% que irá desvaneciéndose durante el semestre. Las versiones anteriores a iOS 15 representan ya una cantidad mínima y despreciable.

Actualmente, Apple da soporte a iOS 15 y iOS 16, abarcando dispositivos desde el iPhone 6S (presentado hace más de siete años) al iPhone 14.

Informe de Transparencia de Apple

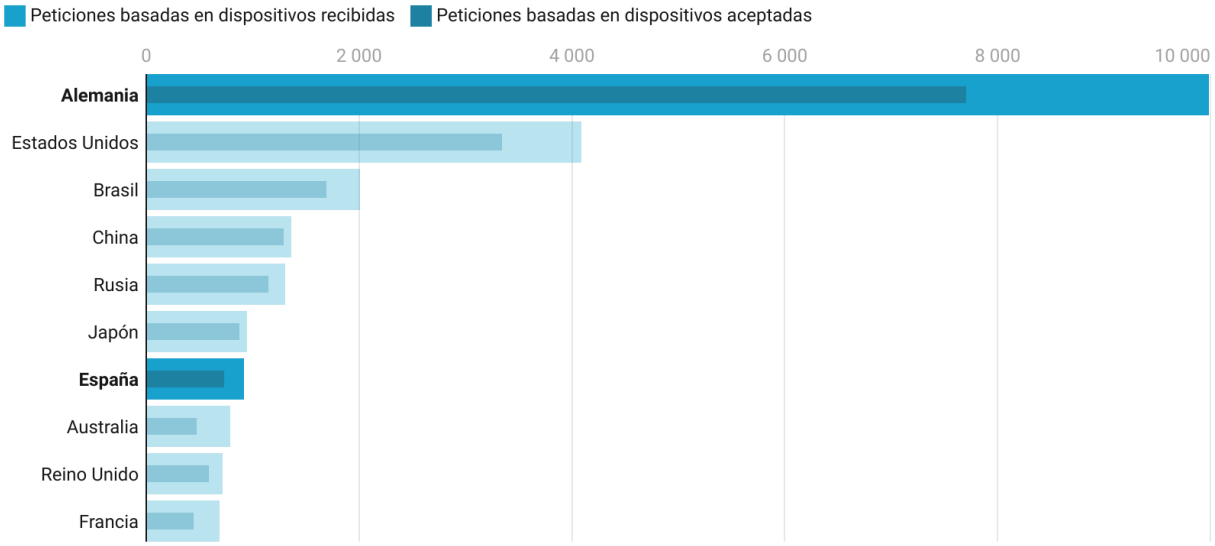
En ocasiones, los gobiernos necesitan apoyarse en las grandes corporaciones para poder llevar a cabo su trabajo. Cuando una amenaza pasa por conocer la identidad o tener acceso a los datos de un potencial atacante o de una víctima en peligro, la información digital que almacenan estas empresas puede 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. Actualizamos aquí algunos datos que hemos extraído de la información publicada por Apple para **el primer semestre del año 2021 (el último publicado por Apple)** 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 el país que más solicitudes de información de dispositivos ha realizado en el primer semestre de 2021

Se muestran el número total de peticiones realizadas y aquellas que han sido aceptadas por Apple.



El grado de aceptación varía desde el 60% para las peticiones de Australia al 94% para las correspondientes a China.

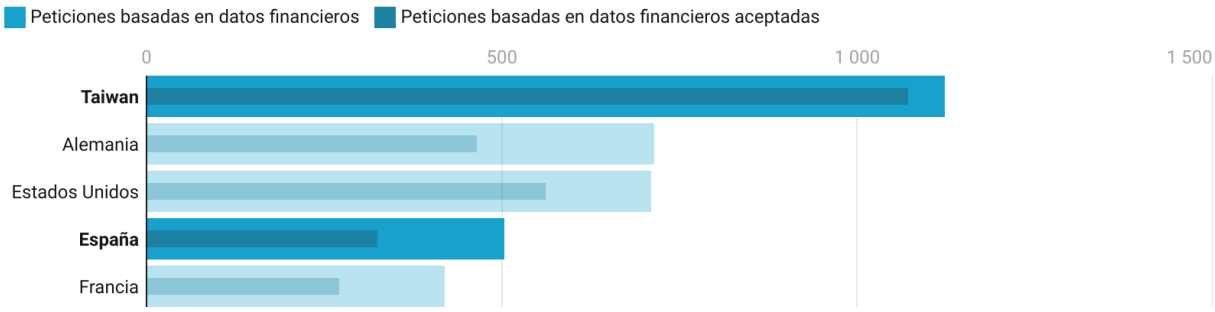
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

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.

Taiwan duplica a cualquier otro país en solicitudes de información por fraude en los primeros seis meses de 2021

Se muestran el número total de peticiones realizadas y aquellas que han sido aceptadas por Apple.



El grado de aceptación entre los 5 paises con mayor volúmen varía desde el 64% para las peticiones de España al 95% para las correspondientes a Taiwan.

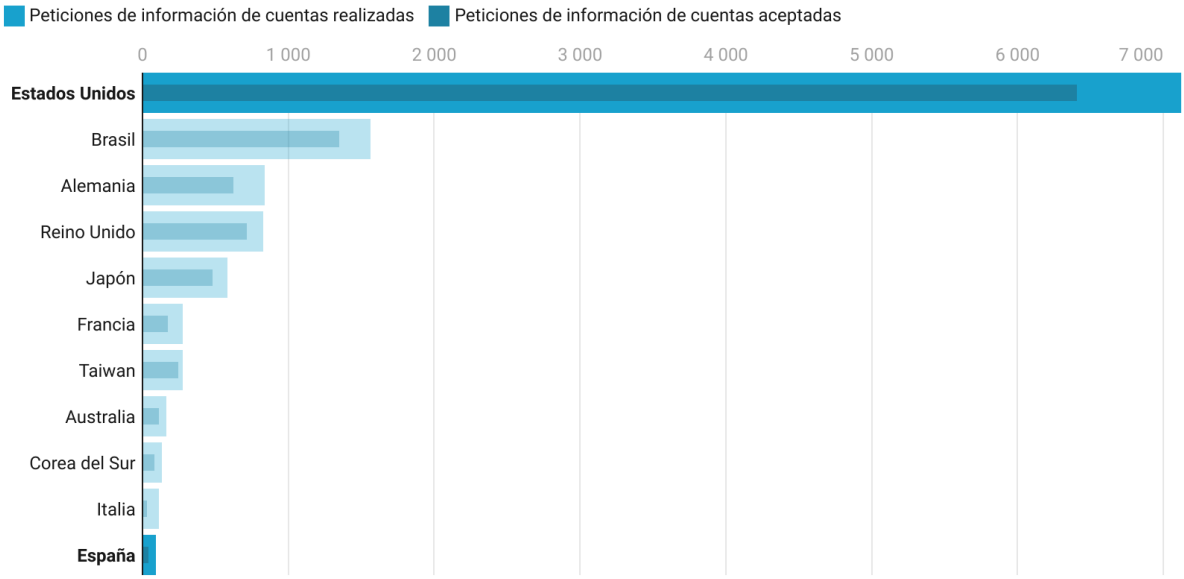
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

Peticiones basadas en cuentas

Se realizan, desde los gobiernos, 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 diferencia, el país que más solicitudes de información de cuenta ha realizado en el primer semestre de 2021

Se muestran el número total de peticiones realizadas y aquellas que han sido aceptadas por Apple.



De las 93 peticiones realizadas por España en los primeros meses de 2021 solamente 41 fueron aceptadas (44%).

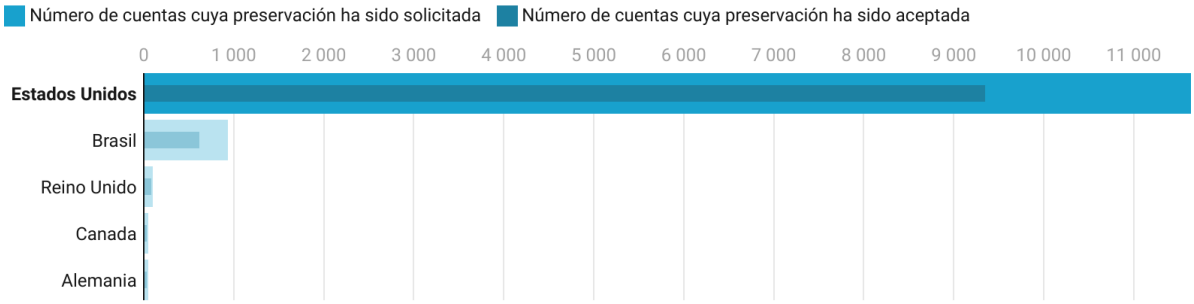
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

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 que más cuentas ha solicitado preservar en los primeros seis meses de 2021

Se muestran el número total de cuentas cuya preservación ha sido solicitada y aquellas cuya preservación ha sido efectivamente realizada por Apple.



España, que ocupa el puesto 30 en número de solicitudes, solamente emitió una solicitud de preservación de una cuenta que fue rechazada en este periodo.

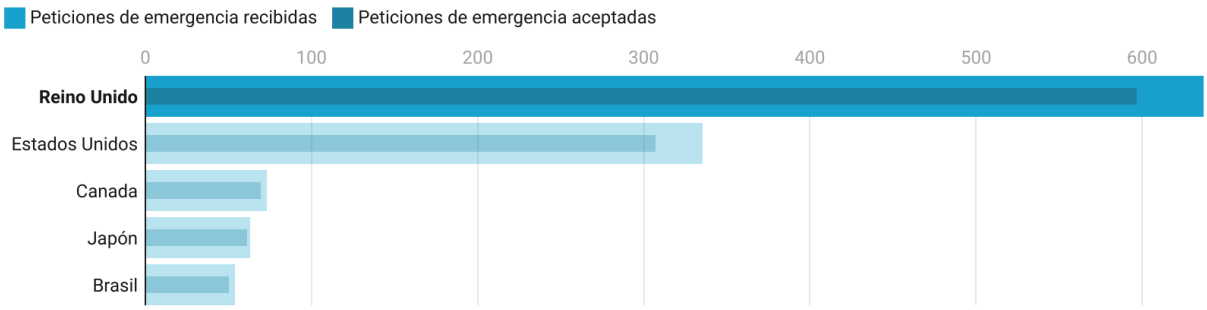
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

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 en el primer semestre de 2021

Se muestran las peticiones de acceso a cuenta por emergencia realizadas y aquellas aceptadas por Apple.



España, que ocupa el puesto 33 en el ranking, solamente emitió 1 solicitud de acceso a cuenta por emergencias y fue aceptada (100%).

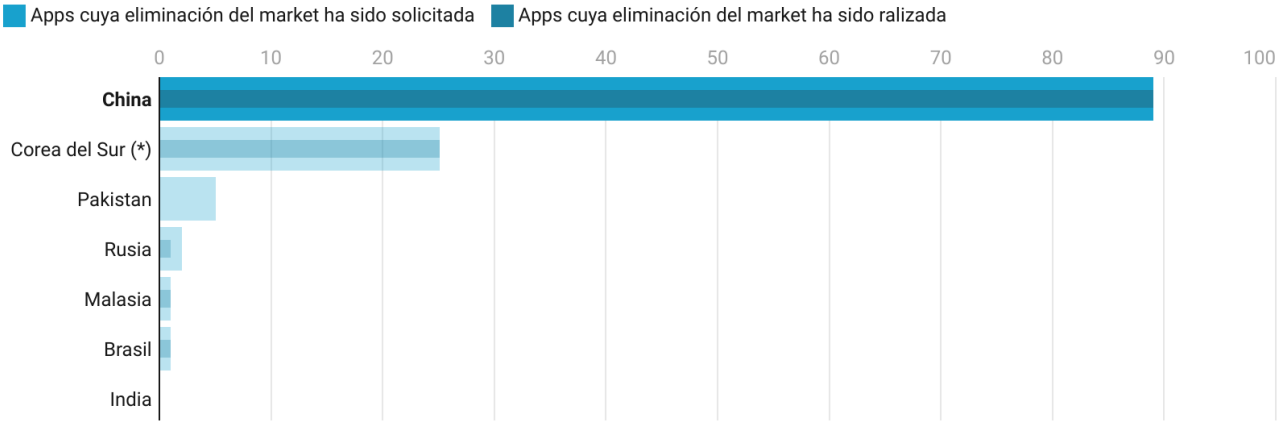
Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

Peticiones relacionadas con la retirada de apps del market

Habitualmente tiene que ver con aplicaciones que se supone violan la ley soberana.

China solicitó 89 eliminaciones de Apps del market en los primeros seis meses de 2021 y todas fueron aceptadas.

Se muestran las Apps cuya retirada del respectivo market ha sido solicitada y aquellas Apps efectivamente eliminadas.



Una App cuya retirada fue solicitada por Corea del Sur, finalmente fue apelada su retirada y se restauro en el market.

Gráfico: Juan Elosua • Fuente: Apple • Creado con Datawrapper

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.
- **Taiwan ha aumentado de forma sustancial las solicitudes de información de cuentas por fraude** que ha realizado, solamente en seis meses de 2021 lleva más solicitudes (1.124) que en todo el 2020 (1.030).
- Estados Unidos solicita con diferencia más que cualquier otro país la preservación de cuentas y el acceso a los datos alojados en ella. Lo que destaca de nuestro análisis es que **Brasil está en segundo lugar de una forma muy destacada con 10 veces más solicitudes de preservación y acceso respecto al tercero**.
- **Reino Unido lidera desde 2020 las solicitudes de acceso a información de cuentas por situaciones de emergencia**, aquellas donde se puede evitar un peligro de muerte o daño serio a individuos. Resulta sorprendente a raíz de los volúmenes de acceso a cuentas de EEUU. ¿Existirá un procedimiento pre-establecido de lanzamiento de este tipo de solicitudes por parte de su departamento de exteriores?

- De manera poco sorprendente, China es el país que más retirada de apps solicita en el App Store, Desde lo observado en 2020 vemos que se ha reducido de forma significativa el número de países que solicitan la retirada de aplicaciones, principalmente en Europa.

Aclaración: en este ejercicio hemos representado en gráficas las tablas que publica la propia Apple. Es importante especificar que las peticiones se realizan por lotes que pueden incluir más de una cuenta o dispositivo. Por ejemplo, Apple contabiliza el número de peticiones de información de dispositivos, y a su vez cada petición puede contener un número indeterminado de dispositivos 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 dispositivos entre todas las peticiones y luego dice que ha satisfecho el 90% de las peticiones, no sabemos cuántos dispositivos individuales se han proporcionado. Por lo que se trata de un ejercicio que puede aportarnos una idea aproximada de la cantidad real de dispositivos proporcionados para el ejemplo expuesto.

Android

Nuevas características de seguridad

Android 13 sale a la luz el 16 de agosto. Internamente se a esta versión se la conoce como "Tiramisu". Las novedades de esta gran revisión del sistema operativo móvil de Google en el apartado de la seguridad están sobre todo orientadas a la privacidad (siempre bajo la lupa por las numerosas críticas), tal y como comentamos en el informe anterior.

A partir de esta versión es posible seleccionar de manera personalizada las fotografías que se pueden compartir por aplicación. Ahora se puede elegir qué fotografías pueden ser accedidas por cada aplicación en vez del acceso completo a toda la fototeca o galería.

Otro aspecto mejorado en privacidad es la eliminación del requisito de acceso a la geolocalización del usuario cuando ciertas aplicaciones necesitan conectar a un punto Wifi cercano. A partir de ahora las aplicaciones podrán examinar y conectarse a puntos de conexión inalámbricos cercanos sin necesidad de tener que obtener la comentada geolocalización.

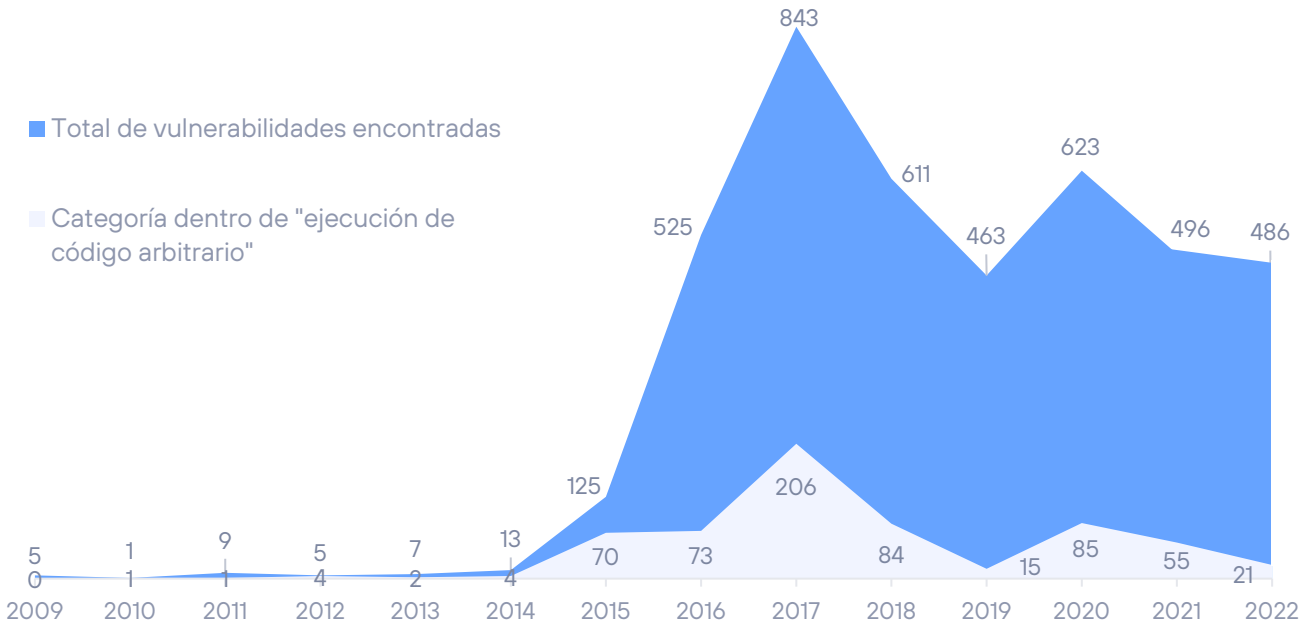
Vulnerabilidades

Android publica un conjunto de parches cada mes, generalmente durante la primera semana. En total, se han publicado **256 parches** para corregir diversas vulnerabilidades repartidos en los seis boletines. De esos 256 parches, **14 corrigen vulnerabilidades que han sido calificadas de críticas** y podrían facilitar la ejecución remota de código arbitrario. Esto sitúa en casi 500 las vulnerabilidades corregidas en 2022. Parecido al año pasado aunque menos graves en general.

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-H2

Evolución de vulnerabilidades por año



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 12, con un share del 28.29%, seguida por la 11 con un share de 23.6%. Prácticamente, son los mismos números que la edición anterior. Es típico en Android que las nuevas versiones del sistema operativo tarden bastante en ser adoptadas debido sobre todo a que cada fabricante debe personalizar y adaptar los cambios a las particularidades del dispositivo e idiosincrasia de la marca.

La nueva versión, Android 13, tan solo está disponible en un pobre 6.72%, debido sobre todo al efecto que comentamos en el párrafo anterior: se tarda muchísimo tiempo en propagar y adoptar las nuevas versiones al parque de dispositivos.

La porción restante se la reparten las versiones inferiores a la 11. Sorpresivamente, Android 10 posee aun un 18.38% de cuota. Una cantidad sorprendente para una versión del sistema operativo que posee tres años y aun, afortunadamente, recibe actualizaciones de seguridad.

Algo alarmante es que Android 9.0 y 8.1 aun poseen una cuota conjunta de casi un 14%. Decimos alarmante porque son versiones del sistema operativo que no reciben actualizaciones de seguridad; lo que equivale a decir que el 14% del parque de Android (sin contar los porcentajes de versiones incluso anteriores) es vulnerable.

VERSIÓN	PORCENTAJE DE USO
13	**6,72%**
12	**28,28%**
11	**23,60%**
10	**18,38%**
9	**8,71%**
8	**4,90%**

VULNERABILIDADES DESTACABLES

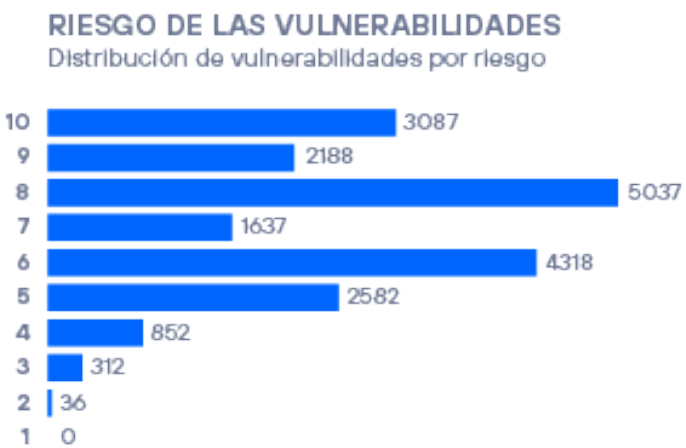
Comentamos en esta sección algunas de las vulnerabilidades notables a nuestro juicio, de este segundo semestre de 2022, es decir, aquellas que destacan por su especial relevancia o peligrosidad.

CVE ID	OBJETIVO	DESCRIPCIÓN	SCORING
CVE-2022-34265	Django framework	Inyección SQL en las funciones Trunc() y Extract() permitían tomar el control del sistema.	9.8
CVE-2022-2385	Kubernetes	Un fallo en el proceso de autenticación IAM usado en Kubernetes podría permitir a un atacante evadir las protecciones existentes frente a *replay attacks*.	8,1
CVE-2022-26138	Confluence	Confluence usaba una contraseña "hardcodeada" en el sistema que se podía explotar en remoto para iniciar sesión en Confluence y acceder a cualquier página a la que el grupo confluence-users tenga acceso.	9.8
CVE-2022-27255	Realtek	Ejecución de código en los chips Realtek RTL819x relacionados con dispositivos de red, gracias a un desbordamiento de búfer en el tratamiento de SIP.	9.8
CVE-2022-36804	Bitbucket	Inyección de comandos a través de HTTPs	9.9

CVE-2022-40684	Productos Fortinet	Salto de restricciones a la hora de autenticar a través de API	9.6
CVE-2022-4135	Chrome	Nuevo 0day en Chrome, el octavo del año. Ejecución de código con salida de la sandbox.	9.6
CVE-2022-37300	Siemens: Varios	El mecanismo de recuperación de contraseñas olvidadas podría permitir a un atacante el acceso no autorizado al controlador, en modo de lectura y escritura, cuando se comunica a través de Modbus.	9.8
CVE-2022-40674	Profinet SDK	Se han identificado una vulnerabilidad en la librería del analizador XML Expat (libexpat) que podría permitir la ejecución de código arbitrario.	9.8
CVE-2022-3214	Delta Industrial Automation: DIAEnergy	Este sistema industrial de gestión de energía permite emplear credenciales en texto plano que permitirían la ejecución remota de código mediante la subida de ficheros ejecutables en ciertos directorios.	9.8
CVE-2022-3485	IFM: Moneo Appliance	Un atacante sin autenticar podría resetear la contraseña de administrador con sólo indicar el número de serie del dispositivo y además ganar control total sobre éste.	9.8

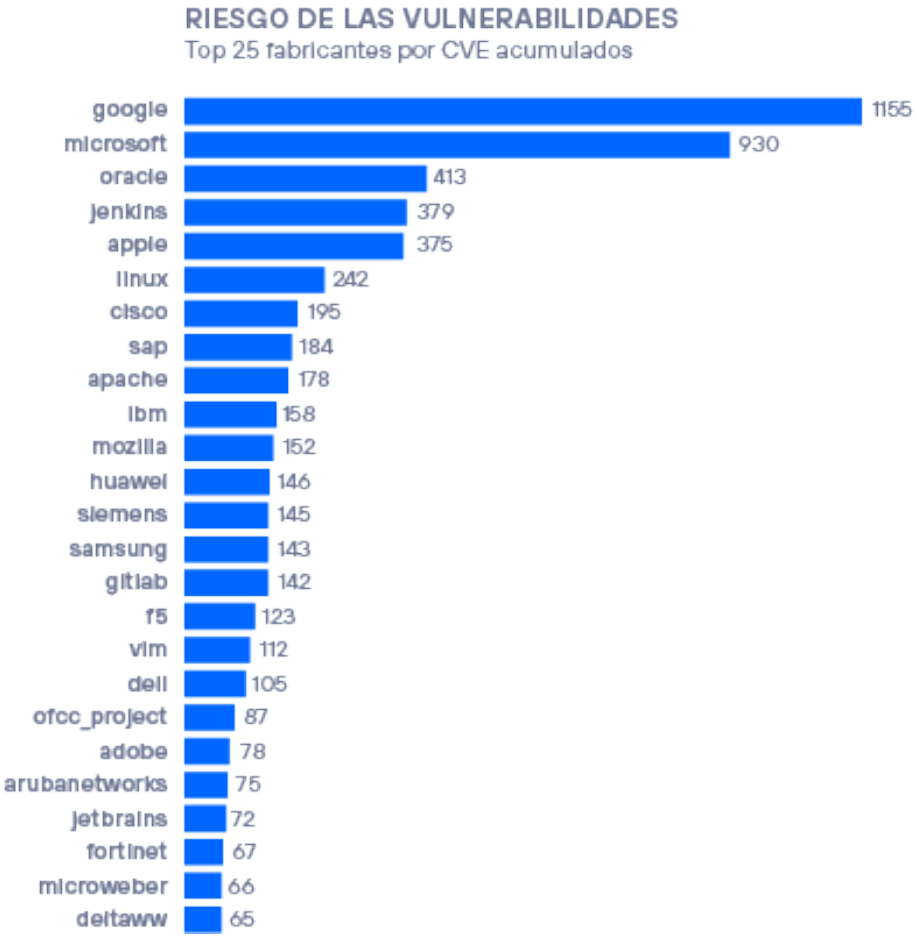
Las vulnerabilidades en cifras

En números concretos de vulnerabilidades descubiertas, la distribución de CVE publicados por nivel de riesgo (*scoring* basado en CVSSv3), ha sido la siguiente. El número de vulnerabilidades en general se ha disparado con respecto al primer semestre.



Top 25 compañías con más CVE acumulados

Durante el segundo semestre de 2022, Google ha liderado con diferencia por número de vulnerabilidades conocidas, seguido de Microsoft. En general, es habitual que los tres grandes estén siempre entre los primeros en número de vulnerabilidades.



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.

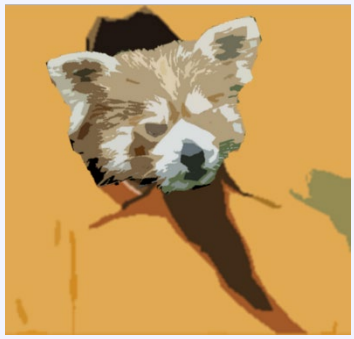
Advertimos que la atribución de este tipo de operaciones, así como la composición, origen e ideología de los grupos organizados es compleja y, necesariamente, no puede ser completamente fiable. Esto es debido a la capacidad de anonimato y engaño inherente a este tipo de operaciones, en la que los actores 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 2022.

Emissary Panda: Nunca traen buenas noticias

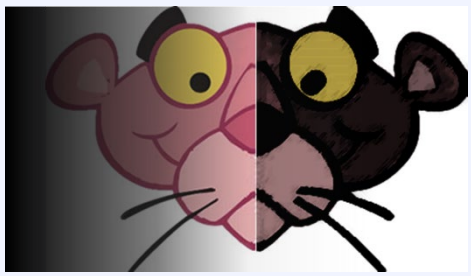
El ministro de Relaciones Exteriores de Bélgica indicó en julio que varios grupos respaldados por el gobierno chino habían atacado los ministerios de Defensa e Interior de su país.

El representante del gobierno belga señaló a varios grupos APT, aunque uno de ellos ya había sido mencionado a principios de año. Concretamente, este "Emissary Panda", que había sido detectado por los servicios alemanes de inteligencia utilizando el RAT HyperBro en varias organizaciones comerciales con el fin de espiar, infiltrarse en las redes de clientes y robar secretos comerciales y propiedad intelectual.



Más información en: https://diplomatie.belgium.be/en/news/declaration-minister-foreign-affairs-malicious-cyber-activities

Dark Pink: Smooth criminals



Este grupo ha sido descubierto por el equipo de investigadores de Group-IB. El análisis, basado en la segunda mitad de 2022 (aunque se sospecha de acciones desde mediados de 2021), ha detectado TTPs diferentes al resto de grupos existentes, herramientas personalizadas y un claro enfoque hacia objetivos militares, ministerios y agencias gubernamentales.

Por el momento, la actividad que se les ha adjudicado han sido acciones contra organismos militares en Filipinas, Malasia (tres veces en dos meses) y organizaciones gubernamentales de Bosnia y Herzegovina, Camboya e Indonesia.

No obstante, por mucha novedad que presenten, el vector inicial de ataque no es novedoso: un spear-phishing bien cocinado.

Más información en: https://www.group-ib.com/media-center/press-releases/dark-pink-apt/

Polonium: Venenoso y siniestro

Este grupo, supuestamente localizado en el Líbano, pero que trabaja en coordinación con otros grupos esponsorizados por Irán, fue documentado por primera vez en junio de 2022 por investigadores de MSTIC (Microsoft).

Sus objetivos han sido organizaciones de Israel, registrándose actividad desde septiembre de 2021 y durante todo 2022 en más de 20 organizaciones de distintos sectores, entre los que está Defensa. Aunque emplea herramientas propias (CreepyDrive, CreepyBox, Creepysnail...), comparte TTP (y objetivos) con algunos grupos iraníes, como Mercury.

Este grupo utiliza principalmente (por el nombre de las herramientas se puede intuir) los servicios de almacenamiento de OneDrive y DropBox para las acciones de C&C y la exfiltración de la información.

Más información en: https://www.bleepingcomputer.com/news/security/hacking-group-polonium-uses-creepy-malware-against-israel/

GhostSec: ¿A quién vas a llamar?

Como ilustración de este grupo, no se nos ocurre nada mejor que un auténtico fantasma. Alguien que se autodefine como "experto en ciberseguridad".

No obstante, este grupo palestino tiene unos buenos conocimientos. En septiembre fue detectado varias veces atacando objetivos israelíes. Primero, el grupo de investigadores de Otorio informó de que este grupo afirmaba haber hackeado 55 PLC de Berghof en territorio israelí.

Quince días más tarde, volvieron a anunciar un ataque con éxito. El compromiso de una planta de depuración de aguas. Publicaron además capturas de pantalla del sistema y aseguraron que podrían ir mucho más lejos y envenenar el agua si quisieran, pero que ese no era su objetivo.

Más información en: https://www.securityweek.com/hacktivist-attacks-show-ease-hacking-industrial-control-systems

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

Este semestre, como caso concreto, vamos a comentar una situación interesante y que nos llamó la atención durante la prestación de un servicio a un cliente del norte de Europa. Concretamente vamos a comentar cómo percibimos el cambio en el eje mundial de los ciberataques dependiendo de la localización de los activos atacables. El proyecto requirió que cambiáramos la localización (a nivel lógico) de uno de nuestros nodos a la sugerida por el cliente, en un país del centro-este de Europa. En este relato, nos centramos en uno de los principales vectores de ataque, por su sencillez y rentabilidad: acceso por fuerza bruta contra RDP.

A continuación, vamos a señalar una comparativa entre los intentos de acceso a la bahía de ingeniería (el PC de control del sistema industrial) del nodo mientras estuvo desplegado en España y en su estancia (temporal) en Francia. Las listas se han confeccionado a 7 días y se muestran los 10 mayores valores por número de intentos.

ESPAÑA	FRANCIA
scada1\ad	scada1
scada1\us	administr
administr	hello
hello	scada1\ad

scada1\sc	user cont
admin	usercontr
user	user.cont
raquel	u.control
david	domain
laura	test

Sobre el TOP 10, varias circunstancias resultan llamativas:

- La similitud salta a la vista. Un 30% de las contraseñas intentadas son idénticas aunque en diferentes orden.
- Un 40% guardan cierta relación o similitud entre ellas.
- Un 30% son... ¿nombres de persona?

Efectivamente, cuando empezamos a descender en la lista, dejamos de ver contraseñas "genéricas" y empezamos a encontrar nombres propios. En cuanto localizamos el nodo en Francia, los nombres empezaron a cambiar. Así, a partir del décimo resultado, empezaron a verse los "emanuel", "guillaume", "isabelle", etc. propios del país galo. Algunos de ellos figurarían en el TOP 10 de no ser por los resultados que muestran distintas iteraciones entre "user" y "control".

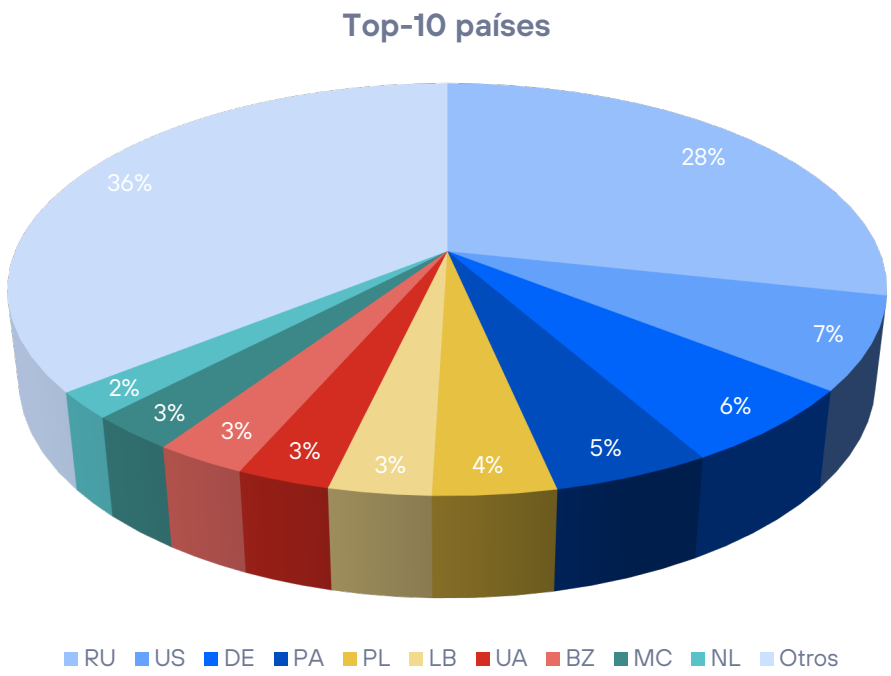
Sobre el país donde nuestro cliente pidió localizar el nodo no podemos dar datos concretos, pero sí podemos afirmar que los cuatro primeros nombres que encontramos eran los cuatro nombres más utilizados en ese país, según su propio "INE" (Instituto Nacional de Estadística) según consultamos oficialmente en el organismo del país para respaldar nuestra teoría.

Este tipo de circunstancias, además de ser muy curiosas, deslizan algo que hemos destacado en otros informes. El atacante sabe muy bien lo que hace, contra quién lo hace y dónde está su objetivo. De hecho, aunque la bahía de ingeniería no deja de ser un PC, los intentos de acceso denotan que los atacantes tenían muy claro que era un elemento embebido en un sistema industrial. Estas son ventajas de utilizar sistemas industriales reales.

A medida que se desciende por la lista de intentos de acceso, también se comienzan a observar credenciales por defecto de varios dispositivos industriales y de IIoT (Industrial IoT) que no están presentes en nuestro sistema industrial. Esto nos da una muestra muy clara de las TTP de los atacantes a nivel general: las labores automatizadas de reconocimiento pasan en gran medida, aunque no mayoritariamente, primero por una identificación del sistema (OT-IIoT) y después por un ataque de fuerza bruta genérico. No llegan a indagar en qué tipo de sistema se han encontrado. Seguramente porque **tienen tantos aciertos que no necesitan mejorar la eficacia ni la eficiencia de sus sistemas automatizados**.

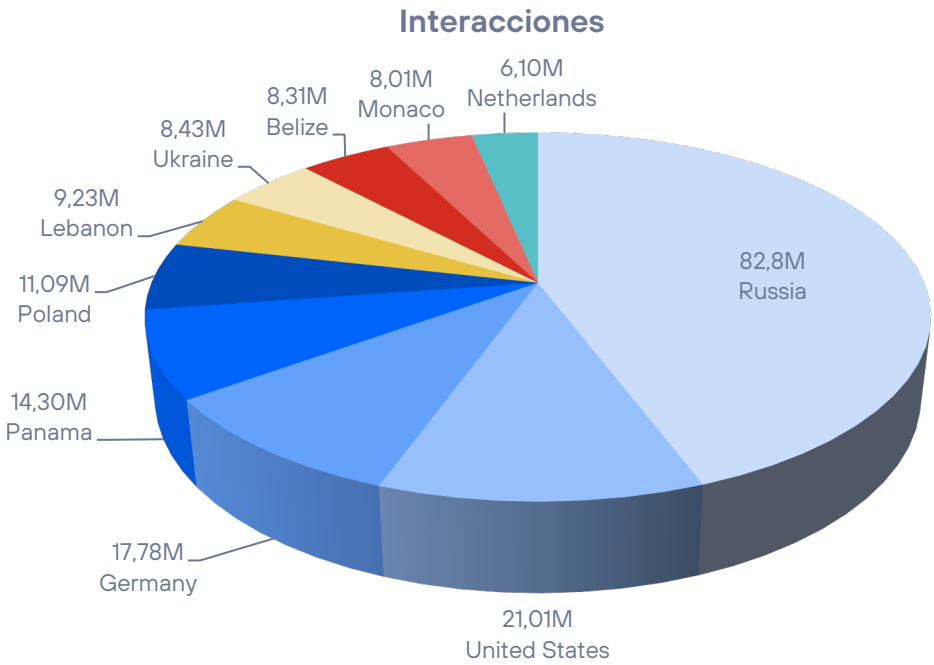
Y ahora, pasamos a la estadística general de la información registrada. En el segundo semestre de 2022 se detectaron **más de 291 millones de eventos de ciberseguridad**. Esto supone un descenso respecto a los datos registrados en el primer semestre de 2022 y un 30% menos respecto al mismo periodo del año pasado.

Aun así, la cifra total de eventos detectados en 2022 ha sido de más de 706 millones, cifra superior a la detectada en 2021. La distribución por países sería la siguiente:



Ahora vamos a ver las diez direcciones IP con más interacción con el sistema de Aristeo. El 70% provienen de varios países de Europa del este. Ni una sola de las IP pertenecen a un país fuera de la localización geográfica europea. Esto es especialmente llamativo porque es habitual que las direcciones IP de nodos tan importantes para el tráfico de internet como los Estados Unidos.

A continuación, observamos cómo se reparten la actividad los países con más presencia en nuestro Aristeo. La entrada de Belice en esta lista el semestre anterior ya fue llamativa, pero la presencia de Líbano tampoco se queda atrás en el ranking.



ESTUDIO DE AMENAZAS POR INDICADOR

En colaboración con **Maltiverse**, hemos realizado un estudio clasificatorio de los indicadores de compromiso detectados en su plataforma. Esto es, indicar atributos interesantes sobre *maliciosidad* detectada en direcciones IP, nombres de dominio y URLs de los últimos seis meses.

¿Qué tipo de funcionalidad relacionada con los ataques conllevan las URL estudiadas?

De más de 650.000 urls estudiadas, casi un 66% eran puntos de descarga de malware. Es decir, una vez visitada la URL el recurso obtenido era malware: bien un troyano, exploit o cualquier binario catalogado como tal.

Por detrás del malware, **muy relacionado siempre con urls se encuentra el phishing con un 30%.** Son URLs que en algún momento han estado relacionadas con phishing. Una URL que enviaba a la víctima a algún sitio falsificado a la espera de que entregara sus credenciales, claves financieras o engaños similares.

URL	
Malware download	66%
Phishing	30%
Beacons	4%

El resto de URLs, se encaja en el concepto de infraestructura relacionada con malware. Por ejemplo, casi un 4% de las URLs pertenecían a beacons del framework de pentesting Cobalt Strike. Entrarían en el capítulo de alojamiento de malware, pero especificando más su uso.

¿Qué podemos encontrar respecto al registro de dominios asociados a actividad maliciosa?

Existen momentos clave en la vida de un dominio malicioso, por ejemplo: cuando aparece en alguna infraestructura y no está registrado; cuando se registra, pero no está activo y, finalmente; cuando ha está activo y provee alguna capacidad maliciosa. **Casi un 72% de los dominios detectados o envueltos en campañas de infección estaban activos en el momento de su detección.**

La mayoría de los dominios se han empleado para operaciones relacionadas con ataques o campañas de phishing. **Un 40% de los dominios estaba implicado en falsificación de sitios para robar credenciales.**

Casi un 30% de los dominios estudiados pertenecían a centros de control de bots. El centro de control es el servidor al que acuden los nodos o sistemas infectados para la obtención de órdenes para coordinar acciones conjuntas, entre otras operaciones.

DOMINIOS	
Bots	29%
Distribución malware	26%
Phishing	39%
Otros	6%

¿Dónde se geolocalizan las direcciones IP maliciosas?

El destino final del tráfico producido por una arquitectura de malware siempre será una dirección IP. Ya sea de forma directa, indicando en la dirección URL la propia IP o a través de la resolución de un dominio, siempre nos toparemos con un servidor alojado en algún sitio que responde en una dirección IP concreta.

Dado que las direcciones IP están vinculadas a sus redes y estas poseen una localización física, es bastante fácil poder extraer concusiones acerca de la distribución geoposicional de las direcciones IP sobre las que se han detectado actividad maliciosa.

De un total de más de 450.000 direcciones IP recopiladas, los 10 países donde se ubican más direcciones IP que aparecen en estas posiciones son:

IP PAÍSES	
Estados Unidos	18,08%
India	10,90%
China	10,32%
Taiwan	4,48%
Rusia	3,67%
Alemania	3,33%
Brasil	3,05%

Vietnam	2,34%
Pakistan	2,27%
Tailandia	2,26%
Resto	39,30%

Este grupo representa el 60% del conjunto, mientras que el resto, el 40%, sostiene porcentajes no significativos o menores al 2%.

Tipología

Aunque una misma dirección IP puede tener más de una clasificación (esto es, una misma dirección IP puede contener, por ejemplo, un sistema de spam y tiempo después o de forma concurrente puede servir de C2).

Algo más de un 68% de detecciones son las direcciones IP que se consideran bots. Es decir, máquinas o sistemas infectados. Un bot es un ordenador infectado por malware que se haya bajo el control de una botnet. El uso que se le puede dar a esta red de bots es discrecional: desde minar criptomoneda, atacar con peticiones masivas un objetivo para crear una denegación de servicio o simplemente alojar malware o phishing para posteriores ataques.

Un 20% de las IP ha sido vista realizando algún tipo de fuerza bruta contra sistemas de autenticación. Esto es, por ejemplo, realizando miles de peticiones con combinaciones de usuario y password contra un servidor SSH. Si una de estas combinaciones es aceptada por el servidor significaría el compromiso de este o al menos el acceso con las credenciales y permisos otorgados por la cuenta secuestrada. Es un claro aprovechamiento de un simple y caro olvido: cambiar credenciales por defecto o contraseñas débiles por otras más robustas.

Un 8% de estas IP han sido catalogadas como distribuidoras de malware. Es decir, alojan malware disponible para su descargar por las víctimas que han sido infectadas. Cuando se trata de infecciones, es común que en primer lugar la víctima sea infectada por un downloader que una vez dentro del sistema realiza la descarga del malware definitivo. Estas IPs han sido observadas alojando malware o formando parte de puntos de descarga.

Casi un 3% de las IP está envuelta en algún caso de SPAM o lo que es igual: distribución masiva de correos no solicitados. Es decir, en algún momento, el 7% de las direcciones IP han sido catalogadas como servidores de correo. Un mal incansable y siempre rentable para las organizaciones criminales. Además de ser uno de los vectores principales por donde entra el malware.

IP	
Bots	69,00%
Brute force	20,00%
Malware download	8,00%
SPAM	3,00%

Debemos recordar que dentro de la propia categoría de bots es posible hallar direcciones que en un momento dado sirvan de punto de descarga de malware, alojamiento de phishing o envío de correos no solicitados o de igual forma: spam a lo largo de una línea de tiempo. Es decir, un nodo o máquina infectada es al final un servicio multipropósito bajo el control de una organización criminal que decide, en según qué necesidades posee dicha organización, a qué dedica los sistemas bajo su control.

RECAPITULACIÓN

Aumentan en general el número de vulnerabilidades corregidas en iPhone. De 125 en 2018 a 261 en todo 2022. También aumenta el número de fallos graves hasta los 66. En Android la tendencia es estable por el contrario, con números similares desde 2021 en torno a los 500 fallos. 2022 ha sido uno de los años con menor número de vulnerabilidades críticas.

Con respecto al informe de transparencia de Apple, debemos hablar de datos del primer semestre de 2021 (el último publicado por la compañía). Interesante como Alemania es el país que más solicitudes de información de dispositivo ha realizado, mientras que, con diferencia, es Estados Unidos el país que más peticiones de información de cuentas ha realizado. Como de costumbre, China es la que más solicita eliminar apps del mercado.

Microsoft, Google y Oracle son las empresas con más fallos corregidos, como es habitual, aunque a veces intercambiando orden. Jenkins se situó el semestre anterior en cuarta posición por primera vez y se mantiene. Le sigue Apple de cerca.

Con respecto a la seguridad OT, demostramos cómo los atacantes tienen muy en cuenta dónde se sitúan las máquinas potencialmente víctimas, y utilizan la idiosincrasia propia del país. Por ejemplo, en el uso de nombres propios para fuerza bruta, tienen muy en cuenta las estadísticas de uso para maximizar las probabilidades de éxito.

Inauguramos en este informe la colaboración con Maltiverse. De sus sistemas podemos concluir que la inmensa mayoría de la infraestructura considerada maliciosa se utiliza para descargar malware (un 66%) y que la mayoría de dominios también maliciosos están relacionados con centros de control de bots (el 30%). La infraestructura, en su mayoría, suele estar en EEUU. Esto puede estar relacionado con el abuso de infraestructura legítima que está de moda entre los atacantes, para evitar precisamente se bloqueado por las medidas de seguridad impuestas.

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

Cómo proteger tus cuentas en las redes sociales

¿Realmente estamos comprando de forma "segura" en Internet?

CRIPTOGRAFÍA

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

MALWARE

DGA o no DGA, esa es la cuestión

Dime qué malware tienes y te diré a qué botnet perteneces

Entendiendo la dinámica de los incidentes de seguridad con Ransomware