la cámara de un iPhone 13 es todo lo que necesitas para robar las claves criptográficas de un móvil Galaxy s8 según un paper publicado recientemente un borrador aprobado por el consejo de los estados europeos pretende debilitar la ley Europea de libertad de los medios de comunicación y conceder Carta blanca a gobiernos para utilizar spyware contra periodistas justificando asuntos de seguridad nacional a las puertas de los 100 Aquí tienes un nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 27 de junio de 2023 el episodio número 99 yo soy Martín vigo y está conmigo por casi 100 veces todavía 99 Alexis porros Hola Alexis qué tal Pues muy bien Martín aquí venimos con un descuento el 99 episodios a punto de que lleguemos al 100 el gran premio para nuestros oyentes que se han quedado hasta los 100 y que Esperamos que se queden más allá no y nada también quería comentar brevemente que ya hemos pasado el solsticio de verano Martín no sé aquellos que les guste el verano se pueden ir despidiendo No mentira Todavía queda verano pero a partir de ahora los días se van haciendo más cortos hasta el solsticio de invierno este espacio meteorológico lo ha patrocinado tierra de hackers querido sirvientes fuera bromas os queremos dar las gracias a todos vosotros por apoyarnos online por reíros de nuestras bromas o es cero y sobre todo por escucharnos si aligerando que es gerundio estamos en todas las redes sociales más populares en las que no os podéis encontrar como tierra de hackers o arroba tierra de hackers en el 99% de las plataformas de podcast donde debería estar suscritos y si no lo estáis ya estáis tarda ndo y os invitamos a formar parte de nuestra comunidad de discord vía tierra de hackers.com barra discord el episodio anterior el 98 no tenía preguntas y que nada nos vemos en el próximo o en el siguiente Pero bueno para comentar las siguientes preguntas más allá así que ahí vamos perfecto efectivamente 99 me pregunto Cuántos oyentes habrán escuchado los 99 episodios que me Conste que son varios el episodio número 100 va a ser pensábamos como como lo íbamos a celebrar y nos basamos en mucho de lo que nos escribís que es Oye molaría que contestáis preguntas de los oyentes y tal pues vamos a hacer eso lo que se conoce como un ama no lo del askyne hemos pensado que lo que podéis hacer es contactarnos por email en podcast.com por redes sociales o incluso mejor os invitamos a mandarnos audios que Twitter pues puedes mandarnos un audio en instagram puedes mandarnos un audio creo que por discord también puedes mandarnos un audio porque así si nos haces una pregunta podemos ponerla directamente en el podcast y así por nosotros contestarla Entonces La idea es hacer algo especial en el episodio 100 preguntarnos lo que queráis bueno Esto siempre de hackers que tenemos nuestro digital es un poco genérico pero bueno ya me entendéis con lo que queráis pero nosotros gustosamente puede ser sobre ciberseguridad puede ser sobre nuestra vida personal un poco como Hemos llegado a Estados Unidos ves así no sé se me ocurre habrá algunas cosas que no vamos a contestar y Alexis ni yo pero la idea es acercarnos un poco más a nuestra audiencia preguntarnos lo que queráis y nosotros gustosamente daremos esas respuestas celebrando esos 100 episodios yo por mi lado darle las gracias de todo a nuestros mecenas de patreon por estar apoyándonos económicamente día a día y a nuestros sponsors en este caso brawler Pro una herramienta muy completa de seguridad en aws empresas de todos los tamaños se apoyan diariamente en brawler pro para que sus equipos puedan confiar en su modelo de seguridad de aws puedes probar brawler Pro hoy mismo y de manera totalmente gratuita y vas a obtener paneles y gráficas con información concisa y accionable con todo lujo detalles además sobre la madurez de tu modelo de seguridad y una visión completa de tu infraestructura en todas las regiones de aws y tendrás todos los resultados en apenas unos minutos Así que a qué estás esperando empieza a usar brawler pro y benefíciate de los resultados visitando tierra de hackers.com barra brawler Pro prw l e r o y también queremos dar las gracias a otro de nuestros

patrocinadores en este caso monat una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y monat a través de una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web monat.com y en mandarles vuestro currículum tierra de hackers arroba monat.commod.com perfecto Pues yo antes de comenzar con la noticia solo mencionar que la semana pasada como os mencionaba estaba desde Cyber World que di allí una charla sobre red teaming a temas de reputación que fue muy Guay pero Alexis tío Tienes que empezar a venir a conferencias porque la cantidad de oyentes de tierra de hackers que estaban por allí era una pasada y como digo Siempre agradecidísimo de que la gente viniese a saludar fue una pequeña cagadita que me quedé sin pegatinas y no tenía Para repartir lo cual es un Preciado tesoro cuando voy a las conferencias les pillaste la dirección a los aquellos que no tenías pegatinas para luego no no no no ninguno ninguno está dispuesto no es preciado pero no para tanto pero nada la verdad como siempre fue es que es increíble tío viene viene la gente Te saluda te comenta muy Guay un especial saludo a la gente con lo que me fui a comer y que me ayudó a describir hay gente con muchos skills en el tema de Austin tío porque saqué en la conversación un tema de una película de pequeño que que había visto y que solo me acordado de una escena y allí entre Chuletón y Chuletón de Ávila tío estos compañeros que son fieles oyentes de tierra hackers y que le mando un saludo enorme que me eché una buena risa con ellos me sacaron la peli allí entre charge petes búsquedas buenas de Google saber lo que buscar una pasada estos tíos quilapelli era el pequeño Einstein y yo solo me acordado de una escena de que un tío deshabilitaba una bomba con una guitarra eléctrica y a que había algo relacionado con cerveza tío y mira que lo había buscado Eh pues estos tíos en 5 minutos pum ya me habían dado el hecho son mejores que echar gpt tío Qué grande me suena el juego este bueno juego que la gente popular el Gio que es ser este no que sale una imagen Sí sí sí Ya te digo Sí eso es de las fotos también son una pasada porque es en plan no la silueta tiene 45 grados a la hora que por el brillo del cristal se puede ver que el sol se está poniendo y además la vegetación es la típica de Australia que me estás contando tío que me estás contando no es genios como Einstein sí Ya ves pues bueno nos vamos a la noticia vengo con un nuevo paper que me he encontrado la semana pasada hablaba de uno Pues esta semana a otro esta vez para un ataque contra sistemas de cifrado pero la verdad me interesa porque traeros lo porque es de una como de una manera física un vector de ataque todavía complicado ya llevar a cabo un escenario real pero que en pruebas de laboratorio funciona la perfección y parece imposible Incluso en pruebas de laboratorio se trata del robo de claves privadas de llaves privadas de cifrado mediante el análisis del comportamiento de los leds de varios dispositivos electrónicos me explico seguro que todos tenéis por casa el típico aparato que bueno tiene una Lucecita normalmente roja no cuando está apagado y cuando lo enciendes por la lucecita Pues cambia de color se pone azul o verde pensad por ejemplo en vuestra televisión cuando la pagáis desde el mando de la televisión en vez de digamos quitando El enchufe no en realidad pues queda en un estado que se llama como Stand By y suele saberse porque la lucecita el led está en rojo Pues esa lucecilla consume energía aunque sea muy poquita y os voy a explicar cómo gracias a ese detalle se puede robar el secreto mejor guardado de los dispositivos electrónicos de seguridad sus llaves criptográficas vídeo base cryptoanálisis extractic criptography Kiss from vídeo fouresh of a divise Power elid Ese es el título que le han puesto a este paper y cuyos autores son bennassi etay luz ofeg Boyer orcohen dudonassi borishi me gusta siempre hacerlo un guiño a los autores de papers que me han sorprendido que porque se lo merece no por el currado que lleva tipo Este descubrimiento este

tipo de descubrimientos tú conoces al Ben este no al Ben nace no Alexis sí Ese es el nuestro querido amigo que nos ha llenado tantos episodios de risas como el lanfon y el glow warm ese esos ataques el danzón aquel que era apuntando con un láser a una bombilla y calculando midiendo las vibraciones del puntero de la luz láser en función de lo que hablaba la gente en esa habitación podía recuperar el audio y el otro el Glock World era algo parecido pero atacando inyectando comandos de voz así tipo dispositivos estos asistentes como la Google home mi similares pero sí sí un crack Pues sí la verdad el Ben así este va a haber que seguirlo de cerca porque siempre está involucrado en todo este tipo de ataques hollywoodienses que la verdad son una pasada y este caso es otro más ya que este paper que por cierto van a presentarlo en Blackjack y Def con este año que como ya sabéis son conferencias de ciberseguridad muy muy importantes Pues nos explican más que un nuevo vector de ataque una manera de mejorarlo que lleva pues como decía el robot de información confidencial de dispositivos como móviles y lectores de tarjeta de tarjetas de alta seguridad bueno con esto de tarjetas de seguridad me refiero a las tarjetas rfid que usa mucha gente pues para abrir puertas no entrar a sus oficinas etcétera Ya sabéis pues bueno que sepáis que estas tarjetas también utilizan criptografía pues para dificultar en parte ataques de clonación que no sea fácil que alguien se te acerque y te pueda clonar la tarjeta no con acercar pues una antena o algo así utilizan un ataque tipo Side Channel o de canal lateral basando basándose en el análisis del consumo de energía que pueden inferir por como parpadea el ID la lucecita este tipo de ataques No son nuevos leían un artículo como uno de los primeros ataques de este tipo de canal lateral Data de 2008 cuando unos investigadores se dieron cuenta que cuando utilizaban un dispositivo militar para cifrar y descifrar mensajes para enviarlos evidentemente de manera segura cada vez que cifraba una letra se podía captar esa actividad con un osciloscopio que estaba muy cerca para los que no conocéis lo que es un osciloscopio Pues nos permite analizar el comportamiento de Señales eléctricas en el tiempo no como vacilando Pues resulta que estaba captando las emisiones electromagnéticas que irradiaba el dispositivo militar un hallazgo por pura casualidad pero que les permitió inferir la clave de cifrado privada mediante el análisis de esas emisiones electromagnéticas ahí es nada en 2019 hubo otro ataque que nombraron Minerva y con el cual pudieron robar las claves privadas de cifrado de un lector de tarjetas de alta seguridad utilizado una vez más en el ámbito militar una clave de más de 256 bits que es lo que a día de hoy consideramos como seguro y que consiguieron robar mediante el análisis de patrones del tiempo durante el proceso de cifrado Y tenemos otro ataque más en 2020 que es el caso de hearts blit que también permite recuperar claves Privadas del sistema de cifrado post cuántico conocido como psique midiendo en este caso las variaciones del consumo eléctrico de chips de la cpu en concreto de Intel y amd cuando llevan a cabo ciertas operaciones relacionadas con la criptografía Qué sucede con estos ataques que os acabo de mencionar Pues que requieren de equipos muy caros y muy sofisticados para llevar a cabo estos ataques pues ya decía que hablábamos de osciloscopios pero otro tipo de Hardware para el desarrollo de circuitos electrónicos también Es necesario por no mencionar que además estos ataques requerían acceso físico a los dispositivos a comprometer hasta el punto de tener incluso que en el caso del lector de tarjetas tener que conectarse directamente a la placa base para ser más concretos en el caso de Al ataque de Minerva había que previamente comprometer El lector de tarjetas de manera que necesitabas acceso físico a ella durante un tiempo prolongado imaginemos que si estás en una base militar Pues claro ahí va a haber cámaras refrigerando las las puertas no entonces pues es un poco difícil de llevar a cabo este tipo de ataque y en el caso de hearts si bien no había que comprometer previamente el dispositivo se tardaba 18 días interactuando con el dispositivo para llegar a robar la clave criptográfica lo dicho ataques teóricos muy difícilmente ejecutables en un escenario real Pues

esta nueva investigación que os traigo hoy permite eliminar todas estas Barreras y llevar a cabo estos ataques con dispositivos como la cámara de un iPhone de último modelo un iPhone 13 o una cámara de vigilancia esto es como un cambio brutal porque sobre todo cuando pensamos en cámaras de seguridad que están en todos lados es una especie como de shoulder surfing no pero que en vez de intentar grabar cuando metes una contraseña o El pin del teléfono está grabando el led de tu dispositivo ya no necesitamos componentes electrónicos especializados y caros ya no necesitamos estar físicamente cercanos al dispositivo a comprometer ya no necesitamos conectarnos físicamente a él todo lo que necesitamos es poder grabar el dispositivo en vídeo desde una distancia la verdad es que una gran mejora este tipo de ataques y un claro ejemplo Esto me gusta destacarlo de cómo vemos que los ataques más locos y sofisticados que parecen imposibles en principio empiezan como prueba de concepto en laboratorio y luego se van mejorando y abaratando hasta hacer los posibles en la vida real Ok entonces ya sabemos que al grabar Cómo varía de intensidad o color los leds de nuestros dispositivos se puede inferir las claves criptográficas debido a que el consumo eléctrico pues hace que varía con una intensidad o con otra os ahorro por eso lo explico así toda la matemática de cómo exactamente funciona Porque ni la entiendo yo Después de leer mi paper y además os dejo el paper en sí las notas del episodio porque seguro que soy mucho más inteligentes que yo lo que me interesa destacar es cómo es posible hacer esto con una cámara de un iPhone porque esto es un poco lo que lo que me atrajo a traeros esta noticia o una cámara de videovigilancia si hace tan solo unos años se requería de equipo electrónico altamente preciso y conectarse directamente a la placa para poder leer ya os podéis imaginar esas oscilaciones en el led tan sutiles no esos cambios esas variables en el conducto eléctrico tan tan mínimas Bueno pues esto es debido a que las nuevas cámaras disponen de una tecnología llamada Rolling shader OK Y como no me tuve que leer exactamente que era esto Pues mira me fui a echar gpt y os pongo lo que me dijo Charles ppt es un método utilizado en cámaras digitales y en algunos dispositivos de capturas de imágenes para registrar la imagen en diferentes momentos en lugar de capturarla de manera instantánea en un solo momento a diferencia de las cámaras con obturador mecánico tradicional que capturan toda la imagen de una manera simultánea el Rolling shutter divide Las capturas en líneas o secciones que se leen secuencialmente comenzando desde la parte superior hasta la inferior o de izquierda a derecha es decir básicamente el Roly shader en vez de sacar una foto en ese instante en el tiempo en el en el tiempo cero te la saca durante Digamos como unos nanosegundos y se va sacando como de arriba abajo digamos no un poco como se cargaban los videojuegos de los 80 esto porque os lo cuento Pues por un detalle muy importante normalmente las cámaras teniendo en cuenta que aquí hablamos a grabar vídeo graban al frame rate que tienen 24 frames por segundo 30 60 120 Esto bueno ya sabéis que lo que significa es que en el caso de 120 pues toman digamos 120 instantáneas fotos por segundo digamos para crear el vídeo si recordáis esas típicas imagen del cine en los años 80 que no con el con el aparatito donde Pues un poco como cuando se revelaban las fotos antiguamente pues van pasando los fotogramas a toda velocidad Pues esa velocidad es precisamente que pasen 24 fotogramas por segundo y al ser fotos con cambios mínimos por ejemplo en el movimiento de una persona para nuestro ojo lo percibimos como que hay movimiento y que es vídeo esto todo para decir que realmente el vídeo se puede hacer A través de pasar instantáneas comparaciones mínimas a una velocidad específica que es lo que representa esto de 24 30 60 120 Ok el Rolling shuter permite subir el frame rate de manera digamos artificial y llegar a captar hasta 60.000 instantáneas por segundo en vez de 24 o 30 60 o 120 60.000 esto es muchísimo y lo que se necesita precisamente para llegar a tener la granularidad suficiente para captar cambios mínimos en la intensidad de un led o incluso el propio cambio de color si si por ejemplo hacemos suma tope

enfocando al LED que es en este caso pues en el vídeo que demuestran Cómo se hace pues lo que hacen hacer sumas led Precisamente es esta tecnología y esos 60.000 instantáneos es precisamente el iPhone 13 lo que es capaz de hacer gracias a este Rolling shutter teniendo la manera de capturar estas alteraciones ya nos permite analizar minuciosamente esos cambios e inferir la clave criptográfica como decía os dejo de hecho los enlaces a los vídeos de demostración donde no solo se muestra cómo lo hacen lo del zoom que os comentaba pero también el propio Setup no que está muy curioso en uno de los ataques son capaces de hacerlo a 20 metros de distancia con una cámara de seguridad con suficiente zoom para enfocar de lleno el led y de hecho lo que Proponen que esto se queda para para una escena de peli de Hollywood como decíamos o de serie de Netflix unos tíos podrían hackear una cámara de seguridad para utilizarla para hacer zoom a la puerta de entrada concretamente al lector de tarjeta así sacar en la llave criptográfica del lector de tarjeta y poder clonarla desde su casa Sin haber pisado el lugar de alta seguridad o sea esto es perfectamente posible porque lo que es hackear cámaras de seguridad prácticamente muchas de ellas las podemos comprometer a día de hoy utilizando shodam o con contraseñas en claro para un ataque un atacante un poco sofisticado si ese sistema de videovigilancia está de alguna manera conectado a internet pues podrías comprometerlo y una vez en la cámara de seguridad ya tenemos ahora Gracias a este paper que Sería posible al menos en condiciones de laboratorio insisto el poder hacer zoom al led del lector de tarjeta interpretar los cambios de color o intensidad como de manera que podemos inferir la clave criptográfica debido al consumo eléctrico de las operaciones criptográficas guapísimo guapísimo ahora que acaban de sacar la nueva temporada de Black mirror Es que yo creo que aquí tenemos varios episodios de Black mirror el otro ataque lo hacen contra un Samsung Galaxy s8 que esto también nos interesa porque ya hablaba de cómo se podía comprometer teléfonos Android en el episodio anterior Pues aquí volvemos a tener algo parecido pero en este caso el Samsung Galaxy s8 está conectado a un altavoz por USB ya que normalmente si lo pensáis como aquí tenemos que grabar el digamos la actividad de un led claro los teléfonos móviles no suelen tener este tipo de leds pero los altavoces Sí así que es como el orden que Insisto que os dejo el vídeo ya para terminar la noticia recordar de nuevo que si bien estos investigadores han mejorado muchísimo este tipo de ataques de Side channer sigo siendo bastante improbable que suceda en el mundo real y os doy esta vez los detalles en su propia prueba contra El lector de tarjetas tenían que capturar la imagen del led haciendo la operación criptográfica durante 65 minutos a ver ya no son 18 días como eran 2018 pero que realmente como tienen que ser 65 minutos grabándose en la operación criptográfica Esto es algo imposible porque cuando una persona va a entrar en un edificio y pasa digamos la tarjeta por el lector eso qué es menos de un segundo Por tanto todavía no Sería posible realmente este vector de ataque en cuanto a la prueba contra el Samsung Galaxy s8 para extraer las claves de privadas Samsung contexto que el algoritmo vulnerable a este tipo de ataques que os mencionaba que era el psique ha sido retirado ya y de hecho ya no le dan soporte y esto es debido a que otro ataque fue reportado hace un añito en donde también se podía Robar claves criptográficas Solo que de otra manera así que de momento ataques a nivel académico pero con pasos de gigantes sin duda para hacerlos cada vez más probables en la vida real sí de nuevo como siempre Netflix o quien sea aquí estamos para dar ideas de episodio de lo que sea Black mirror o películas de Hollywood muy interesante lo que tú decías No qué operaciones criptográficas tardan 65 minutos o más está preguntándome Qué puede haber por ahí la usabilidad sería sería terrible ahí la verdad Y esto es que en plan Bueno A partir de la lección aprendida tienes que cubrir tu el led del dispositivo sí es marca reader como cuando vas a un cajero automático tapa tapa el código pin no me sea que te lo vayan a pillar con la Cámara pues Algo similar Sí tal cual de hecho sé que en Amazon porque a veces tenemos estos típicos

dispositivos cargadores o así en la habitación y tienen un led súper fuerte y la gente le molesta para dormir y venden en Amazon pegatinas para tapar los leds de dispositivos electrónicos pues Oye en la primera vez que en tierra de hackers damos una defensa tan sencilla y barata tío pegatinas las pones y ya está o esas típicas no de la yo tengo también pegatinas de estas para cubrir la cámara del portátil Pues lo mismo de eso similares y el tema del Samsung s8 cuál era exactamente que pudieron obtener del Samsung las claves criptográficas que estaba utilizando Sí a ver lo que no especificaba en el paper lo que entonces es posible que sean claves criptográficas de la negociación por Bluetooth bueno no porque era por USB entonces claro los dispositivos electrónicos tienen su propia digamos clave raíz no que es la que está en el chip Pero luego con esa cifran y descifran otras claves que se utilizan para para cosas específicas no Entonces yo quiero entender que la clave que podrían extraer al tener un altavoz enchufado es una clave criptográfica que no es la clave criptográfica raíz que viene digamos en el chip especial este que no se puede extraer no en Android suele ser el tee en el iPhone es el Security eso es lo que yo quiero pensar porque no tendría sentido que se bueno es que tal como tengo entendido aquí hay gente que sabe muchísimo más que yo en temas de móviles pero yo tengo entendido que la clave que sería la crítica la más crítica de que viene en el chip especializado no en el Security o en el te esa se utiliza para cifrar y descifrar otras claves privadas que se generan Entonces yo quiero pensar que esa es la que se filtra Pero bueno no sé no venía especificado Ok si no era por aclarar un poco bueno Estaba pensando también que como tú dices un ataque no muy práctico Pero oye no sé igual en el futuro hay procesos que tardan más está pensando que no sé si si al ser 65 minutos si se repitiera un proceso es en plan si la misma persona va a hacerlo va a pasar su tarjeta en un lector de tarjetas estos de acceso físico no sé el primer minuto de cada 65 minutos igual si se va repitiendo y pueden sacar extraer eso no sé o igual lo vemos en el próximo stacks de 2 pero bueno es un poco bastante bastante particular el ataque así que bueno parece que lo van a publicar durante la blajara este año algo así he visto Sí aparte en las dos en tanto en Blackjack como lo cual es señal de que recordemos que hay ahí una serie de expertos que son los que verifican Y aprueban si una charla va a aparecer la conferencia no no los Cold paper reviewers es muy raro que una charla la acepten en ambas O sea que cuando la aceptan en ambas porque recordemos que Black es el martes y el miércoles y Def con escorpio viernes sábado domingo claro es en la misma semana cuando acepten una charla en ambas es porque es espectacular Así que promete Pues los que vayáis ya sabéis a verla y si no al final siempre acaban las charlas en online Así que esto significa como dice Martín que hay que verla en cuanto salga publicada o en cuanto tengáis la oportunidad porque debe ser Interesante pero todavía mejores Escuchar tierra de hackers y antes de que haya salido la charla ya la tenéis os acabamos de ahorrar 5000 pavos de iros a Las Vegas Así que apuntados ahí a patreon y darnos un eurillo muy buena cuña Martín me ha gustado soy un hacha haciendo publicidad subliminal tío un hacha bien afilada y luego estaba pensando en el nombre de este tipo que digo algo me suena este nombre Cómo se llama de nuevo Martín ven así digo Este es el tío de la canción está de sí sí sí sí tío A mí que me va la música electrónica Qué buena Sí sí debe ser el hijo predilecto tío de fondo en tu noticia la podríamos poner ahí eso cuando tengamos editor otra vez que ahora me lo como yo editar esto y me lleva mucho tiempo Pues nada bueno Martín como decimos de capítulo de Black mirror o de película de esta de una escena de hacking guapísima tío comprometer la cámara para leer los leds para extraer los las claves criptográficas post-análisis del consumo electrónico brutal en plan sí estoy estoy aquí cerca de la puerta OK un momento pum puerta abierta Muchas gracias aparte mira ahora que van a sacar Dentro de poco la de emisión imposible que tiene siempre mucho de hacking Pues hay una escena de esas estaría muy guapo sí sí sí sí Ok pues nada vamos con la siguiente noticia os Traigo una con implicaciones de privacidad

bastante graves y voy a empezar con la siguiente afirmación la Unión Europea legaliza el uso de software espía contra periodistas tal cual Europa da Carta blanca a los países de la unión para que puedan espiar a periodistas siempre y cuando se deba a un asunto de seguridad nacional entre comillas antes de entrar en detalle en este nuevo desarrollo voy a poner la noticia en contexto tenemos la ley Europea de libertad de los medios que se abrevia como del inglés emfa y european media freedom act que fue aprobada en septiembre de 2022 todo esto obviamente por todos los casos que hemos cubierto en tierra de hacker sobre pegasos y tal escucharon los episodios y dijeron Uy tenemos que emitir una ley de estas para proteger a los ciudadanos europeos no igual escucharon el podcast pero probablemente sea por todas las noticias No pues este reglamento Busca proteger a los periodistas y proveedores de servicios de medios de ser atacados por los estados miembros de la Unión Europea mediante el uso de spyware y como digo fue presentado por primera vez por la comisión europea en septiembre del año pasado aún así se ha ido realizando investigaciones de Incluso un año o sea que solapa con la publicación de esta ley pero en base a una investigación de un año sobre el uso de pegasus y Software espías similar los eurodiputados argumentan que el uso ilícito de software espía ha puesto en juego la democracia misma literalmente tal cual lo dicen y piden investigaciones creíbles cambios legislativos y una mejor aplicación de las normas existentes para abordar el abuso esta este movimiento o esta llamada a la acción a estas modificaciones fue aprobada con 411 votos a favor 97 en contra y 37 abstenciones esto pinta genial no podríamos decir ciudadanos 1 o periodistas uno empresas de software espía 0 o gobiernos cero Pero antes de cantar Victoria en este partido que estamos jugando sigamos comentando una noticia para ver si realmente ganamos para detener de inmediato las prácticas ilícitas de software espía los eurodiputados argumentan que el software espía solo debe usarse en los Estados miembros donde las denuncias de abuso de software espía se hayan investigado a fondo donde la legislación nacional esté en línea con las recomendaciones de la comisión de Venecia y la jurisprudencia del tribunal de justicia de la Unión Europea y donde se hayan hecho cumplir las normas de control de las exportaciones de este tipo de software quieren normas de la Unión Europea sobre el uso de software espía por parte de las fuerzas del orden que solo deberían autorizarse en Casos excepcionales para un propósito predefinido y por un tiempo limitado los eurodiputados argumentan que los datos que se encuentran bajo el privilegio abogado cliente o que pertenecen a políticos médicos o medios de comunicación deben protegerse de la vigilancia A menos que haya evidencia de actividad delictiva también Proponen notificaciones obligatorias para las personas objetivo y las personas no objetivo a cuyos datos se accedió como parte de la vigilancia de otra persona también una supervisión independiente después de que haya ocurrido la investigación y una definición legal común del uso de la seguridad nacional como base para la vigilancia sobre el primer punto mencionar que recientemente Apple O sea hay empresas que no solo gobiernan sino que empresas notifican a sus usuarios sobre ataques a nivel apt a nivel de gobierno y de hecho Apple ha enviado notificaciones recientemente sobre unos ataques de apts a ciudadanos de ahora no recuerdo el país pero era creo que por el este de Europa De hecho no solo eso voy más allá tienen una página donde hacen un tema transparencia y ponen públicamente todos los todas las veces que les han contactado y como lo han hecho o sea como lo han hecho Perdón de respecto a qué O sea no ponen todos los detalles ni la persona en concreto Pero eso Mola un como un reporte de transparencia lo valoran mucho la privacidad es uno es creo que es uno de sus puntos de venta con los que te convencen porque la verdad es en ese aspecto lo hacen bastante bien y para ayudar a descubrir vigilancia ilícita estos eurodiputados incluso Proponen la creación del iu teclab o laboratorio tecnológico europeo un instituto de investigación independiente con poderes para investigar la vigilancia y brindar apoyo tecnológico incluida la

detección de software espía en dispositivos y la investigación forense esto Me parece muy interesante no he encontrado más detalles pero Oye si se van a si se va a montar un lava así en Europa no sé yo creo que sería bastante interesante trabajar en ese laboratorio hasta aquí todo pinta muy bien Ahora entramos en la parte más oscura de la noticia recientemente ha habido desarrollos preocupantes en el proyecto de reglamentos sobre esta ley que comento la ley Europea de libertad de los medios emfa el consejo de los estados de la Unión Europea aprobó el 21 de junio hace muy poco su borrador de ley Europea de libertad de los medios de comunicación en él el consejo debilitó significativamente la protección prevista de los periodistas de la vigilancia Estatal la federación Europea de periodistas advierte que esta excepción en blanco por la que gobiernos pueden utilizar spyware contra periodistas justificando que se trata de asuntos de seguridad nacional y otros cambios en el texto hacen que la ley de libertad de los medios sea lo dicen literalmente como un caparazón vacío y la hacen efectivamente pues sin efecto básicamente valga la redundancia es una ley que Su contenido no no aplica porque la modificación que le van a aplicar pues la anula completamente y por lo tanto temas de privacidad y derechos de los periodistas se quedan descubiertos en respuesta a esto se ha publicado un comunicado o Carta abierta de 65 organizaciones de libertad de prensa y derechos fundamentales que advierte que el este último texto de compromiso así se le llama o Esta última modificación de la ley Europea de libertad de medios plantea graves riesgos para los principios democráticos fundamentales de la Unión Europea y derechos bueno civiles y humanos en particular las libertades de prensa la libertad de expresión y la protección de los periodistas la reforma de ley está liderada por los gobiernos de Francia Alemania y los Países Bajos así estos tres países son los que están más interesados en poder espiar a los periodistas en toda la Unión Europea el texto de compromiso mantiene y agrava la propuesta de la comisión que establece una excepción de seguridad nacional a la prohibición general de desplegar software espía contra los periodistas la modificación de la también aumenta la lista de delitos que permiten la vigilancia contra los periodistas y las fuentes periodísticas es decir no me he leído la lista pero añaden más casos posibles en los que se puede determinar se puede argumentar que este caso en concreto es de seguridad nacional y voy a instalarle un pegasus o el que sea en el teléfono de este periodista de este periódico o de este de este podcast o de lo que sea no Y también elimina las salvaguardas legales que protegen a los periodistas contra el despliegue de software espía por parte de los estados miembros al Añadir la excepción de seguridad nacional a la ley los estados que han pedido esta modificación se aseguran que puedan espiar a cualquier periodista simplemente argumentando que el periodista estaba atentando contra la seguridad Nacional del país y todos sabemos Obviamente que nunca se ha usado evidencia falsa en ningún caso en cortes o que la evidencia no se puede falsificar verdad pues la 65 organizaciones que firman esta carta abierta incluyen asociaciones de prensa Defensores de las libertades civiles y Derechos Humanos y están ubicadas en países como España Hungría Rumanía eslovenia Suecia Noruega Italia Croacia Finlandia Serbia Montenegro hay algunos más pero incluso también la wikimedia de Europa lo curioso es que también estas organizaciones incluyen algunas que están ubicadas en Francia Alemania en los Países Bajos que son los gobiernos que han liderado la reforma de la ley y los que quieren tener Carta blanca para espiar a periodistas europeos lo que se pide en esta carta es eliminar la excepción de seguridad nacional esa justificación por la que los gobiernos podrían tener Libertad para determinar contra qué periodista lanzar el software espía e infectar sus teléfonos sus dispositivos móviles segundo sería restringir la lista de delitos que permiten medidas represivas contra periodistas y fuentes periodísticas y prohibir el despliegue de spyware o sea como justo ahora la han ampliado la esta lista de potenciales situaciones en las que se puede encajonar la situación como seguridad nacional

pues hoy reduzcamos esta lista porque no son tantos los casos y el tercer punto que esta carta pide es incluir fuertes salvaguardas legales para proteger y respetar el trabajo periodístico libre e independiente y de esta forma pues poder garantizar que La regulación proteja a los periodistas y sus derechos fundamentales en este caso como en muchos otros debido a la condición de excepción de tema asociado seguridad nacional uno se puede preguntar Bueno pero esto tendría que aprobarlo un juez no el tema de Quién determina si esto es se trata de algo de nivel de seguridad nacional o no pues el tema sería así y no un juez lo aprobaría normalmente Sí pero en este caso al haber una excepción o Carta blanca por este motivo los estados pueden ignorar las decisiones del tribunal de justicia de la Unión Europea esto es bastante fuerte el Gobierno Federal descendió su posición y enfatizó que no quería legalizar el espionaje a los periodistas y que la excepción general sólo pretende garantizar que las competencias de los estados miembros no se vean afectadas en el área de la seguridad nacional es decir no no nosotros no queremos marcar precedente y que todo el mundo Ahora Pueda espiar a cualquier periodista y queremos hacer y no queremos hacer legal el tema del spyware lo único que queremos es asegurarnos es que si hay algún tema de seguridad nacional pueda podamos llamarlo terrorismo similar Pues que Oye que los gobiernos tengan libertad de actuar Supongo de forma rápida y contundente el consejo de estado de la Unión Europea debe ahora acordar una versión final de la ley de libertad de los medios con el parlamento de la Unión Europea y la comisión el parlamento por su parte aún no ha adoptado una posición propia pero como ya digo el borrador ha sido aprobado Así que es algo preocupante Todo esto lo comento porque han habido casos sonados de espionaje de ciudadanos por parte de gobiernos utilizando software espía para refrescar nuestra memoria quiero recordar eventos recientes en los que gobiernos han utilizado software espía contra periodistas e incluso ciudadanos o incluso políticos como el escándalo pegasus en Hungría el caso Predator en Grecia o el catalángate en España y ahora recientemente Kaspersky ha publicado más detalles sobre un nuevo exploit Bueno lo han ido investigando desde hace poco más de un mes han ido publicando detalles pero han vuelto a publicar más detalles ahora está estos últimos días y me refiero al exploit o el implante este de cero de y de teléfonos móviles de Apple iphones iOS llamado triángulo divi otro más Añadir a la lista de exploits utilizados por software espía como digo como pegasus pre editor Rain y otros la mayoría de estas plataformas de software espía infectan dispositivos encadenando múltiples exploits por ejemplo el exploit para escapar de la zona restringida o sandbox de imessage la aplicación de mensajería de mensajes de texto al procesar un archivo adjunto malicioso o también un exploit de kernel para escalar privilegios a usuario root y digo que algo hincapié en esto de que se utilizan diferentes exploits Encadenados porque a día de hoy los dispositivos móviles que utilizamos la verdad que implementan medidas de seguridad en capas que es un modelo de seguridad en profundidad que hace que el correr exploits y comprometer los dispositivos sea más difícil aunque no imposible no porque ya vemos que pegasus corre muchos teléfonos han sido infectados con pegasus similares por lo tanto quería comentar esto porque caspersky dice que no siempre es posible seguir la cadena de todos los exploits utilizados en el compromiso en la infección y obtener todos estos payloads muchas veces es difícil porque los servidores intermedios que han estado ofreciendo el segundo Pilot o el tercer pelo si hay dos o tres componentes en la cadena pues ya no están sirviendo dichos archivos maliciosos o no están activos o bueno el FBI los ha tumbado o lo que sea no para el caso de esta operación triangulación que es como se le ha llamado la operación de este grupo de ciberdelincuentes cibercriminales que está utilizando exceso Levy se fijó como objetivo recuperar tantas partes de la cadena de explotación como fuera posible y después de seis meses de investigaciones han publicado un análisis inicial digo inicial porque Todavía siguen investigándolo y van a publicar más detalles en las próximas

semanas que incluye dos exploits de día cero y de hecho estos dos exploits Apple los ha parcheado en la versión 15.7.7 de tanto de iOS como iPad o es así que ya sabéis si no tenéis vuestro dispositivos parcheados ahora mismo y a parchearlos a ipsofacto Aunque Bueno si no sois objetivo así muy interesante muy VIP os podéis esperar a que acabe la noticia del episodio y luego ir a parchearlos como digo este implante llamado triángulo divise implementa después de que los atacantes obtienen privilegios de root en el dispositivo iOS objetivo al explotar una vulnerabilidad de kernel a través de la plataforma imessage lo que le otorga un control total sobre el dispositivo y los datos del usuario a los al grupo cibercriminal este malware en concreto se ejecuta en memoria lo que significa que todos los rastros del implante se pierden cuando se reinicia el dispositivo por lo tanto si la víctima reinicia su teléfono los atacantes deben volver a infectarlo enviando un mensaje un mesege con un archivo adjunto malicioso iniciando así nuevamente toda la cadena de explotación en caso de que no se reinicie el teléfono el implante se desinstala después de 30 días es como viene configurada por defecto A menos que los atacantes prolonguen este periodo caspersky le puso el nombre de triángulo divi a este implante porque se pueden encontrar numerosas referencias a terminología de base de datos en el código del exploit por ejemplo se refieren a directorios como tables se refieren a archivos como Records se refieren a procesos corriendo en el teléfono en el sistema operativo iOS como esquima luego por ejemplo al servidor de command en control lo llaman divi server servidor de base de datos y similares no es curioso que hayan utilizado estos términos en el código del malware esta operación es interesante porque estaba dirigida a funcionarios del gobierno ruso diplomáticos extranjeros que estaban en Rusia y empleados de carski y de hecho lo curioso es que Cars pesqui dijo que identificó este nuevo exploit porque estaban monitorizando el tráfico de red de la WiFi corporativa de su empresa usando un producto suyo caspersky unify monitorning en análisis platform y descubrieron una campaña apt contra móviles iOS que previamente no tenían conocimiento sobre sobre este tipo de ataque y de ahí fue que la identificaron me parece me parece interesante también el otro aspecto a Resaltar es que el servicio de inteligencia ruso el fsb que sería el equivalente del FBI en Rusia vínculo este ataque a la nsa y afirmó que Apple cooperó con la agencia de espionaje estadounidense Apple negó las afirmaciones del fsb y bueno de la nsa no he encontrado declaraciones y bueno esto Esto es interesante no sé si el tema de que encontraron el exploit en su red WiFi corporativa lo han utilizado un poco como gancho también para vender su producto de que gracias a él detectaron este este ataque este implante o bueno o se la ha inventado y realmente sí que fueron atacados y bueno para decir sí Igualmente lo hemos detectado nadie nos ha dicho nada al respecto en cualquier caso es interesante que sigan saliendo exploits en este caso es un exploit que a primera vista vamos a ver qué más Comenta caspersky pero no está relacionado con ningún software espía en concreto no está relacionado con pegasus no está relacionado con cualquiera otro este de esos que se utilizan para comprometer teléfonos móviles Así que no quiero decir que podemos estar calmados y relajados sino a ver a ver qué más pero es que o quien sea que vaya a analizar este exploit en breve en el futuro y con esto queridos oyentes llegamos a la pregunta del episodio estás A favor o en contra de la excepción de Carta blanca por la que gobiernos podrían utilizar spyware contra periodistas justificando asuntos de seguridad nacional os damos cuatro opciones la primera es a favor si es por tiempo limitado a favor si hay registros de auditoría en plan no se pueden modificar como tipo blockchain no que es de zona se guardan en una base de datos inmutable que no se puede modificar y bueno Luego si alguien que quiere investigar algo pues puede determinar si ha habido abuso o no la tercera opción es en contra podría extenderse a ciudadanos no quiero no quiero que esto se tome como precedente y la última es en contra en cualquier caso me niego a esto Pues yo creo que la respuesta sea contundente esto de que los gobiernos espían a periodistas que los

periodistas son precisamente los que mantienen a raya a los gobiernos a través de informar a la población de los tejemanejes de los menudeos Yo espero que sea un rotundo No claro luego está la parte de esto de asuntos de seguridad de estado críticos y todo lo que tú quieras pero eso es tan genérico que claro se puede abusar perfectamente y no tiene que ser pensado como abusado por los líderes que tenemos hoy en día cargo cualquier año puede salir elegido alguien a ver no quiero hacer declaraciones aquí políticas pero digamos líderes como a lo mejor en algunos países como Estados Unidos hemos visto que salieron líderes digamos inesperados no en su modus operandi entonces claro no no tenemos que pensarlo como bueno los líderes no nunca van a abusar Esto bueno sería como muy grave son muchos los países que tienen dictadores y las dictaduras normalmente pues aprovechan de saltarse la ley pero lo que no vamos a hacer es ponérselo en bandeja y poner leyes que luego interpretan a su Merced y ponen como excusa que no Esa es la constitución eso es como está escrito en las leyes y se puede y todo es asunto de estado y ya está así que Cuántas veces hemos visto a periodistas desvelar desde desde Imagínate lo de snowden es lo primero que se me ocurre no saldría porque eso es un asunto de seguridad del estado y sí yo estoy abierto a debatir si fue bueno o malo o mucha gente que estaba no sé sobre el terreno de manera secreta Pues por los links de snowden se puso podemos hablar de 50.000 cosas pero lo que es verdad Al fin y al cabo y al final del día es que había un programa de espionaje que entraban conflicto directo con la Constitución de los Estados Unidos O sea que estaba espiando su propia población por tanto si ahora decimos que todo eso no puede salir a la luz porque es un asunto de seguridad del estado Pues esa sería la primera consecuencia no sé otra cosa que se me ocurre los papeles de Panamá famosos no que muchísimos políticos pues esto sería una herramienta para utilizar para que nada de eso saliera la luz yo vamos votaría totalmente en contra Sí sí Buen punto yo si tenemos algún algún oyente que es periodista Pues nada que esté un poquito al loro y me consta que tenemos que estuve en la Cyber World con como un periodista muy bueno y que Escucha le gusta le gusta el podcast así que sería interesante obtener su postura quien haya creado el qué Perdona Espera espera vamos a dejar una pausa aquí es que no sé por qué te escucho bajísimo he escuchado un montón de ruidos si no te preocupes Espera voy a dejar una pausa vale que así sé dónde editar el aparatito ese va a faltar es que se escucha fatal dime ahora repite lo que decías digo Sí digo estos estados que quieren aprobar la carta blanca esta la excepción a espiar a periodistas por temas de seguridad nacional digo que que no nos consideren periodistas a nosotros que no lo había pensado así que hoy en día Ya Con evidentemente todo el respeto claro claro justo justo Con todo el respeto al colectivo de periodistas que se han marcado la carrera y están ahí al pie del cañón en redacción pero sí hoy en día Todo todo el mundo es periodista en Twitter Entonces nosotros que tenemos yo no sé se considera tierra de hacker es un medio de comunicación a ver por un lado Pues sí no por eso es muy especializado en temas de ciberseguridad pero no son cuatro podcast los que llevamos llevamos tres años somos dos personas que hacemos nuestras investigaciones o bueno o digamos más que investigaciones nos miramos al dedillo las noticias cubrimos la actualidad hombre en ese sentido medio de comunicación A lo mejor somos insisto Con todo el respeto al colectivo de periodistas Sí sí Yo por eso decía no sé cómo cómo estamos considerados por ahí sobre todo por gobiernos O sea que ya sabes Martín si vas a Francia mucho cuidado porque son los que están liderando Este cambio en la ley Pues Mejor no hablemos de los franceses mejor que no bueno queridos oyentes hasta aquí ha llegado este episodio 99 lo más importante recordad celebrar con nosotros el episodio número 100 enviándonos vuestras preguntas lo podéis hacer a nuestro correo electrónico podcast arroba tierra de hackers.com lo podéis hacer A través de nuestras redes sociales Twitter Instagram Facebook linkedin lo que queráis también nos lo podéis preguntar a lo mejor enviándonos un mensaje privado en

discord Y todavía más chulo sería si nos enviáis una nota de voz un audio haciéndonos la pregunta que tengáis porque así pues la puedo recortar y poner en el podcast directamente que sería muy interesante los lo podéis enviar por Instagram tw también lo permite en mensajes privados como queráis la cuestión es conocer a nuestra audiencia preguntarnos lo que queráis es vuestra oportunidad episodio especial para celebrar los 100 juntos Muchísimas gracias por estar ahí con nosotros sí sí Martín y he dicho audios pero si alguien no se atreve no quiere dejar su voz ahí pues también puede enviarnos alguna pregunta por mensaje Claro claro por mensaje como decía redes sociales email en podcast arroba tierra hackers en discord lo que queráis cualquier medio de contactarnos nosotros iremos recopilando las preguntas Supongo que entrarán muchas que están duplicadas Y las iremos contestando las leemos o los que nos mandéis un audio pues podemos poner alguno de vuestros audios para hacerlo un poco más más chulo Pues nada y esperemos vuestras preguntas y vuestros audios y nada si nos enviáis algún Alguna algún mensajillo gracioso también todos nos reunimos juntos venga para adelante pues nos vemos y nos escuchamos en el episodio 100 Muchísimas gracias Adiós adiós Chau chau nos vemos en el centenario si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers