del encuentro rusos consiguen detener múltiples trenes en Polonia con un ataque de lo menos sofisticado fallos de privacidad en el diseño de bluetooth low Energy en dispositivos Apple siguen dando la tabarra o como un investigador de seguridad causó pánico entre los asistentes de la Def con 31 pasajeros al tren que está a punto de comenzar 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 5 de septiembre de 2023 es el episodio número 105 yo soy Martín vigo y está conmigo no en directo pero sí presente Alexis porros Hola Alexis Qué tal cómo estamos muy buenas Martín Pues aquí bien bien esta semana Estamos un poco lejos pero siempre cerca de nuestros oyentes Espero que vayamos en sus corazones O al menos en sus orejas Mientras nos escuchan pero nada que ya estamos a primero de septiembre Cómo pasa el año no es increíble y cómo cómo seguimos dando lata barra siendo pertinentes con cada episodio semanal no me enrollo más para no seguir dando lata barra y nada comentar brevemente como siempre que nos podéis encontrar en todas las redes sociales más populares como tierra de hackers o arroba tierra de hackers ahora mismo si estáis ahora mismo como digo suscribiros a tierra de hackers en cualquiera de las plataformas de podcast estamos en la que os parezca mejor y más favorita es ahí estamos y también invitaros a uniros a nuestro canal de discord vía tierra de hackers.com barra discord Pues yo para no retrasarnos más darle las gracias que no podía faltar a eso siempre se hace tiempo a nuestros mecenas de patreon Muchas gracias por apoyarnos Y si tú estás interesado te gusta lo que hacemos pues apoyarnos en tierra de hackers.com/h patrón y a nuestros sponsor de hoy 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 con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y que 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 echar un vistazo a su web monat.com y mandarles vuestro currículum a tierra de hackers @monat.com comentaros antes de empezar con las noticias que voy a estar dando una charla o más bien participando una mesa redonda muy interesante de una conferencia organizada por europol en conjunto con la guardia Civil Española es un panel una mesa redonda donde voy a estar con otros tres interlocutores hablando de Inteligencia artificial privacidad Y cómo esto afecta a las investigaciones llevadas a cavas a cabo por fuerzas y cuerpos de seguridad del estado y yo estoy allí un poco pues para dar digamos la parte de Pro privacidad digamos esto es la conferencia Edén y se va a llevar a cabo el 18 y 19 de septiembre en Madrid y no os lo podéis perder Yo estaré por allí os dejo un enlace además con descuento en la entrada en las notas del episodio por si os apetece uniros también mencionar que esta semana nos sorprendió un oyente mandándonos un Deep fake de nuestra voz de Alexis y mía nos llegó por el correo la verdad no sorprendió bastante es algo que sabíamos y habíamos hablado alguna vez Alexis y yo de que iba a suceder pero he de decir que nos ha gustado un montón nos ha sorprendido lo fácil que puede llegar a ser clonar nuestra voz y la verdad sonaba muy realista sobre todo la de la de Alexis muy divertido Muchas gracias a ese oyente que no sé si quiere que le mencione o no pero bueno sí que quería quería comentar esto y también nos llegó un email de otro oyente Ya que en la noticia que yo cubrí en el episodio anterior donde hablaba sobre las trampas que se hicieron jugando al póker y sobre todo en concreto la demostración de cómo se puede comprometer hackear una máquina para barajar las cartas Pues nos comentaba que esta persona había trabajado en bueno en un grupo especializado que trabajaba Pues con casinos y bueno en general revisando que toda esta maquinaria que tiene que ver con los juegos sobre todo de azar en casinos y todo esto pues me comentaba que eso estaba muy regulado que se hacían chequeos incluso revisiones de seguridad por sorpresa en casinos y Bueno un poco

haciendo referencia cuando yo comentaba que bueno los propios casinos si no son los jugadores podrían también abusar estas vulnerabilidades para intentar llevarse digamos una comisión mayor entonces este oyente que se nota que tiene está muy experimentado en este tema pues no comentaba que eso estaba altamente regulado por supuesto puede suceder pero digamos que no es algo que podría ser abusado durante mucho tiempo porque acabarían cazándoles con alguna de estas revisiones sorpresas y que muchas gracias a ese querido oyente nos encanta es que que entre los miles y miles y miles de personas que nos escucháis hay de todo abogados expertos en hacking anarquistas gente políticos fuerzas y cuerpos de seguridad es perfecto Es un mix fantástico para que nosotros hablemos de temas y vosotros aportáis vuestro granito de arena que nosotros con gusto le damos altavoz aquí en en este nuestro humilde podcast y no me lío más que sé que estáis aquí para lo que estáis Así que vamos con la noticia mía como os decía transparencia Alexis no está en directo conmigo Pero ha preparado su noticia y os la pongo justo después de la mía la mía va sobre trenes y radiofrecuencias infraestructura crítica y señales críticas sistema de seguridad arcaico y una manera fácil y barata de hackearlo al alcance de cualquiera bueno que otro día en la oficina como como les gusta decir en Estados Unidos Cómo creéis vosotros os pregunto antes de comentar nada de la noticia Cómo creéis que funciona el sistema ferroviario Por ejemplo Cómo haces los trenes Cómo hacen los trenes para pues por ejemplo no sé evitar colisiones no es el maquinista que como si fuera digamos cuando vas conduciendo un coche va mirando y si ve un tren de frente pues pega un frenazo evidentemente no puede ser así tiene que haber un sistema de seguridad adicional no sobre todo bueno simplemente pensando lo que tardan de tenerse un tren lo que alcanza a ver un maquinista no sería suficiente distancia no para evitar un choque frontal Y cómo funcionan estos sistemas de seguridad ya que sabemos que tiene que haber alguno pues depende del país y de lo avanzado tecnológicamente hablando que esté pero básicamente los trenes están constantemente emitiendo información sobre sí mismos como su posición y velocidad al igual que hacen por ejemplo los barcos Pero además puede ser puede incluso comunicarse entre ellos Por así decirlo y esto sucede en muchas ocasiones mediante radiofrecuencia esto es el caso del sistema ferroviario polaco país de donde surge la noticia que os traigo hoy Y es que parece ser que unos delincuentes han decidido sabotear varios trenes explotando el sistema anticuado de comunicación usado por los trenes en Polonia y emitieron una señal de emergencia conocido como radio stop y consiguieron detener varios trenes 20 concretamente según las noticias que leía Parece ser que la motivación detrás de este ataque viene de hecho motivado por un apoyo a Rusia por parte de los atacantes y cuadra con el hecho de que Polonia ha estado enviando a Ucrania armamento recientemente por no decir que la señal falsa de emergencia enviada por radiofrecuencia incluía mayores sonidos correspondientes al himno Ruso y discursos de Vladimir Putin recordemos cuando hablamos de radiofrecuencia lo más próximo a ello que tienes pues por ejemplo la radio de tu coche las estaciones de radio transmiten mediante señales de radiofrecuencia las ondas correspondientes a tu música favorita y la antena encima del techo de tu coche es capaz de capturar esas señales al estar sintonizada en una frecuencia específica con frecuencia me refiero al numerito al que sintonizas tu radio para disfrutar de tu emisora emisora de preferencia por ejemplo pues no sé en FM la 92.1 no que a lo mejor pues tiene los 40 principales en España yo que sé esto lo explico porque tenemos que tener claro lo que es el canal de transmisión que es la radiofrecuencia y el estar sintonizado para escuchar una frecuencia específica Por qué Porque el arcaico sistema de comunicación de los trenes en Polonia utiliza básicamente lo mismo que tu coche solo que en una frecuencia diferente concretamente Cuando hablamos de alertas de emergencia la frecuencia es 150 megahercios de hecho un poquito más arriba del Rango de frecuencias de la radio FM tuya de tu coche que

oscila entre 87.5 megahercios y 108 megahercios En otras palabras si la radio de tu coche te permitiese subir sintonizar un poco más hasta de lo que ahora mismo permite que sería 108 podrías escuchar las transmisiones que emiten los trenes polacos especialmente las transmisiones de emergencia y Qué pasa si en vez de escuchar esas frecuencias pudieras emitir en esas frecuencias pues entonces pasarías a poder hablar con los trenes polacos especialmente para avisarles de una emergencia que tendría un efecto inmediato en forma de parada absoluta e inmediata Pero quizás estás pensando que para emitir en estas frecuencias se requiere de aparatos sofisticados No por nada más lejos de la realidad como ya hemos mencionado muchas veces en tierra de hackers y los hackers que nos escuchan conocen hay muchísimos gadgets de hacking como el jaque red y otros incluso mucho más baratos que te permiten transmitir en frecuencias de como puedes entre entre los 10 o 100 megahercios y los y los 6 gigahercios Por ejemplo yo mismo tengo varios de esos gadgets capaz de transmitir concretamente en los 150 megahercios que hablan los trenes de Polonia y además está el alcance de cualquiera comprarse una radio de este tipo cualquier amigo radioaficionado que tengas querido oyente estoy convencido que va a tener una llegados a este punto entendemos que en Polonia los trenes están sintonizados Por así decirlo y escuchando en la frecuencia 150 megahercios por si entra una señal de alerta por ejemplo de emergencia para que el tren Se detenga inmediatamente también sabemos que cualquiera puede comprar el Hardware necesario para transmitir la información necesaria la cuestión que nos queda es cómo averiguaron los atacantes el mensaje que había que enviar porque vale que puedan hablarle al tren y el tren los escuche Pero cómo le decimos al tren Oye emergencia Pon el freno magdaleno Pues esa señal se llama radio stop como os mencionaba antes y lo sabemos gracias a un documento público que es el estándar europeo que especifica el funcionamiento del sistema de interoperabilidad entre sistema ferroviarios en Europa es decir con la comunidad Europea deshaciéndose de las fronteras necesitamos que todos los países Pues a varios niveles puedan interactuar por ejemplo cuando se hablaba del tetra y el tetrapol y todo esto Pues justo hablábamos también de esto que varios países tienen diferentes sistemas y como en Europa queremos poder funcionar independientemente del país pues tenemos que poner sistemas que pueden interactuar entre ellos pues los trenes es lo mismo y se creó un estándar europeo que os dejo en las notas del episodio Y es ahí donde podemos encontrar información como os digo de este siguiente párrafo que traduzco literalmente el sistema de radio pkp descripción sistema de radio instalado en Polonia en las líneas en consideración para la interoperabilidad la radio en la banda de 150 megahercios de pkp Es una radio analógica que consta de equipos en la vía a bordo y portátiles el sistema de radio permite la comunicación de voz simplex y el uso de señales de operación tonos para llamadas selectivas Generalmente no se utiliza para la transmisión de datos el sistema cuenta con una función integrada de radio Stop Ok de este documento obtenemos información sobre el concepto de radio stop que tiene los trenes en Polonia y la frecuencia específica esos 150 megahercios que se emiten pues mira A mí mismo para prepararme para esta noticia me llevo menos de 5 minutos encontrar un paper académico hablando precisamente de los problemas del sistema polarco buscando Pues en Google con las palabras clave por radio stop y pkp que por cierto pkp son las siglas en polaco del sistema ferroviario de Polonia pues ese paper me dice exactamente que es lo que tengo que transmitir os dejo el paper en las notas del episodio pero osito textualmente después de traducirlo este párrafo la activación de la señal radio stop por parte del conductor se lleva a cabo al presionar el botón de alarma en el teclado del radio teléfono lo que resulta en el envío de una señal de sonido especial a través de la radio la señal de alarma es una combinación que en consta de tres tonos cortos consecutivos que varían en frecuencia y repetición periódica como resultado la señal portadora se modula mediante una secuencia

definida 3 cada 100 milisegundos de tres señales acústicas la primera en los 160 hercios la segunda en los 400 hercios y la tercera en los 670 hercios seguidos de un intervalo de 500 milisegundos es decir se repiten estos tres tonos diferentes se espera 500 milisegundos y se vuelve a transmitir perfecto he conseguido encontrar en unos 10 minutos toda la información que necesito para detener trenes en masa en Polonia Y eso que yo solo lo he hecho con fines educativos para traeroslo al podcast Imagínate si soy un delincuente Pro ruso lo que puedo llegar a encontrar pero voy más allá resulta que no tenéis ni que usar las frecuencias que vienen en el paper para generar los tonos vosotros mismos que se puede hacer con herramientas os lo podéis bajar directamente de YouTube ya que me he encontrado vídeos de maquinistas polacos demostrando el sistema de radio stop y con la señal Sonora perfectamente audible este momento esos tres tonos que escuchaba es el Tito es precisamente los tonos que describe el paper y es el tono que se envía en los 150 megahercios para detener un tren polaco quiero hacer hincapié en que todo lo que os acabo de contar es público no estoy contando ningún secreto y lo he sacado de fuentes totalmente abiertas insisto uno de ellos un paper académico por supuesto no os aventuréis ahora a probar según Qué cosas yo creo que a buen entendedor pocas palabras bastan o si queréis pues no lo probáis en producción Por así decirlo el sistema ferroviario se considera infraestructura crítica y cualquier tipo de interacción que intentéis llevar a cabo con esos sistemas por mucho que sea para testing para research o lo que queráis no solo puede ser potencialmente peligroso sino que se puede considerar hasta un acto de terrorismo Así que tontería la justas y dejemos esto en material educacional ok pero yo Después de ver todo esto me preguntaba qué pasa en otros países incluido España corremos peligro de que alguien pueda detener nuestros trenes con un aparatillo baratejo y enviando una señal Sonora no tan fácilmente España como muchos otros países de la Unión Europea utilizó un sistema de comunicación mejorado y digital para transmitir mensajes concretamente el gsmr sobre todo en trenes de alta velocidad Aunque es verdad que indagando un poquito más he visto que algunos trenes como los trenes de cercanía si utilizan un sistema más antiguo llamado tren tierra que sí es analógico como el polaco Aunque por lo que veo Parece ser que lo han estado pasando a digital y espero que no sea tan trivial mandarle órdenes a los trenes en España y que haya alguna no sé capaz de cifrado quizá de hecho alguno de vosotros queridos oyentes estén más puesto al día que yo en este tipo de sistemas de comunicación entre trenes y nos puede arrojar más luz ya sea en nuestro discord o mandándonos un email yo indagando un poco me da la impresión de que si es hackeable como el polaco me encontré un blog donde explican bien su funcionamiento el tipo de mensajes que se puede enviar que incluye uno de emergencia que detendría el tren y también en qué frecuencias específicas yo os dejo el blog en las notas del episodio para que le echéis un vistazo y recordar de nuevo que no hagáis tonterías Lo digo completamente en serio hasta aquí la noticia quería acabar con esa contundencia siempre es interesante este tipo de sistemas que se pueda interactuar de esta manera tan trivial con Hardware tan barato pero bueno una de las cosas que podéis hacer si queréis un poco jugar con esto en ese blog mismo Explica cómo se puede utilizar software libre para recibir las señales de que se envían entre los trenes y procesarlas y ver qué es lo que se están enseñando pero una cosa es recibir las señales y otra cosa muy diferente es transmitir Así que mucho cuidado con estas cosas como decía tenéis todas las notas en toda Perdón todos los enlaces a los papers a las noticias a los documentos que os estaba mencionando en las notas del episodio y bueno os dejo con Alexis que os recuerdo que no está en directo conmigo pero extrae una noticia también la más de interesante adelante Alexis bueno en este caso os Traigo una noticia que va un poquito de escalofríos con Bluetooth low Energy y vuestros dispositivos en este caso Apple os pongo un ejemplo un ejemplo de ficción escenario de episodio de cualquier serie hollywoodiense Mister

Robot o bueno la que sea no una cálida mañana de agosto en una conferencia en la que miles de personas están haciendo cola para recoger su entrada de repente muchos de ellos reciben notificaciones en sus teléfonos móviles pidiéndoles que conecten sus Apple ids o que compartan su contraseña con un dispositivo de Apple TV el popup dice conectando el texto del mensaje Dice Blue Devil requiere información adicional para conectar a esta red sale el logo del Apple TV y debajo sale un botón que pone continuar os pregunto queridos oyentes qué haríais en este caso darle a continuar desactivar el bluetooth de qué forma lo haríais no os voy a dar las opciones ahora porque os lo dejo ahí en el tintero y cuando acabemos Vais a saber la forma más segura y efectiva de hacerlo o de estar incluso protegidos para que esto no suceda en el futuro a pesar de que los Apple TV son útiles para compartir vídeo y audio entre dispositivos de Apple y televisiones normalmente no se utilizan en conferencias y menos en conferencias grandes porque normalmente se utilizan otros sistemas que han diseñado empresas que se dedican a el tema de videoconferencias de forma profesional no De todas formas los más avispados pensando que van a poder hacer Rick roll algunas televisiones aceptan la petición del Apple TV porque dicen Oye sabes qué pues hay una por aquí cerca voy a ver si me conecto y Pongo aquí unas unas fotos comprometedoras o algún vídeo así divertido no como digo un Rick roll similares pero al hacer eso lo que probablemente estés haciendo es compartiendo tu contraseña de bueno contraseñas de que estás utilizando en tus redes WiFi similares Y en este caso en este escenario que comento obviamente esta persona avispada que quería hacer un poco de juego no con esta conexión este Apple TV por el mensaje el popup que le sale en su dispositivo Apple al conectarse al supuesto Apple TV no le va a llevar a nada y bueno al fin y al cabo dicen le da conectar tarda un poco no lo típico porque todo esto radio bluetooth wi-fi en tema de propagación al estar lejos a veces no se conecta no porque te has movido y tal dices Bueno pues me despreocupo y Esto fue un fallo de conexión no por estar lejos o cualquier tema de conectividad pero de fondo se ve al cibercriminal riéndose que lanzó este ataque y que ha podido recopilar contraseñas que van a poder utilizar en futuros ataques esto queridos oyentes No es un episodio de Mister Robot no es un episodio de una serie hollywoodiense sino que es un escenario de la vida real y esto se dio en la conferencia defcon 31 de este año en Las Vegas Durante los días de la conferencia sobre todo los que estaban haciendo cola como digo para obtener su batch se sintieron confundidos y preocupados cuando sus iphones comenzaron a mostrar mensajes emergentes solicitándoles como digo esto de que conectaron su Apple ID o que compartieran una contraseña con un Apple TV cercano durante la conferencia nadie se proclamó nadie dijo ser el autor de este hecho y nadie tampoco publicó si esto estaba relacionado con actividad de algún actor de amenazas entonces la gente está un poquito ahí con la mosca en la oreja no como se dice en plan me tengo que preocupar o no el teléfono debería tirarlo a la basura y cambiar mis contraseñas Bueno si tienes doble factor y tal y una contraseña buena contraseña buena no porque te la han comprometido no pero doble factor y tal Pues igual igual estarías a salvo más o menos pero bueno al final resultó que estas alertas formaban parte de un proyecto de investigación por parte de Jake Box un investigador de seguridad que tenía dos objetivos uno era recordarle a la gente que para desactivar bluetooth en un iPhone hay que hacerlo desde el menú de configuración Bluetooth y darle al botoncito este para que se ponga gris oscuro no y que no no lo hagáis no desactives el bluetooth simplemente desde el centro de control de acceso rápido que normalmente se muestra al deslizar el dedo hacia abajo desde la esquina superior derecha del iPhone si claro se tiene configurado de esta forma el tema es que cuando se hace de esta forma no se Desactiva completamente y ahora voy a comentar un poquito más adelante porque es este comportamiento Ah y el otro objetivo obviamente era reírse de las reacciones de la gente mientras caminaba por la conferencia tan ancho y Pancho activando esas ventanas emergentes

en los iphones de la gente con un dispositivo que él había hecho A medida el investigador dijo que todo lo que necesitaba para llevar a cabo este experimento era un dispositivo que se componía de una raspberry Pay Hero 2w dos antenas un adaptador Bluetooth compatible con Linux y una batería portátil el dispositivo se podría hacer bastante pequeño ya que las dimensiones de la raspberry Pay 02w son de unos 6,5 por 3 centímetros pero para tener mayor alcance las dos antenas que utiliza hacen que su tamaño sea algo mayor incluso la batería también obviamente es un poquito más grande que la raspberry Pay 0 para que le dure bueno para que la diversión le dure un rato no pero es En definitiva es un dispositivo bastante portable que se podría llevar Sencillamente en el bolsillo del pantalón unos pantalones estos así anchitos no box el investigador estimó que esta combinación de Hardware excluyendo la batería cuesta alrededor de 70 dólares y tiene un alcance de 15 metros o 50 pies para aquellos que dominen los pies bueno Y como digo Por qué se da esto no porque esta persona se puede introducir se puede irrumpir en en la paz que tenemos en nuestros iphones No pues los protocolos de Apple para Bluetooth de baja energía o Bluetooth low Energy o el acrónimo ble permiten que los dispositivos de Apple se comuniquen entre sí el investigador dijo que se centró en las acciones de proximidad que aparecen en la pantalla de un Iphone cuando los dispositivos Apple están cerca unos de otros la proximidad está determinada por la intensidad de la señal Bluetooth lo Energy y parece que la mayoría de los dispositivos Apple usan intencionalmente una Potencia de transmisión baja bastante reducida para mantener el alcance corto no Esto está bien diseñado De tal forma para que al menos si alguien intenta hacer de las suyas con tu dispositivo y atacarte pues yo que sé lo puedas ver delante tuyo no más o menos porque así no tiene un alcance de kilómetros Digamos si no es de varios pies o metros sin embargo obviamente como os podréis imaginar el investigador no se limitó por el estándar y por como están configurados estos dispositivos de Apple y emitió a toda caña a toda potencia con las antenitas no Además las antenas que utilizó son también de mejor alcance y sensibilidad porque son más grandes que las que lleva un iPhone dentro y de esta forma podía alcanzar a más dispositivos de lo que podría haber hecho con un producto de Apple por defecto el investigador también dijo que creó una prueba de concepto que Construye un paquete de bluetooth luego Energy lo llaman advertisement se podría Traducir como anuncio personalizado que imita a lo que un Apple TV emite constantemente a Baja potencia simulando efectivamente un dispositivo de Apple que intenta conectarse repetidamente a dispositivos cercanos y que por tanto activa este mensaje de popup que salía a todos los asistentes de adefcon según el investigador no hubo robo de información o compromiso de dispositivos seguro que se está riendo ahora muja Jajaja Eso que he dicho no es del todo cierto no no sé según él dice él Esto es así pero bueno habría que fiarse o no Supongo que es una persona ética No si al fin y al cabo ha salido de forma pública y ha dicho que él fue el que hizo esto pero bueno ahí queda el tema dice que no recopiló ningún tipo de información confidencial o sensible de los dispositivos iPhone a los que con los que interactúo no y como digo a diferencia de los dispositivos Apple reales su cacharro no estaba programado para recopilar datos de iphones cercanos Incluso si la persona tocaba y aceptaba las indicaciones no el mensajito ese del Apple TV continuar pues según él dice no él no recopiló nada pero en teoría si hubiera querido podía haber recuperado recopilado cualquier tipo de datos expuestos por Bluetooth low Energy y ahora voy a comentar un poquito qué podría haber hecho y qué tipo de datos se filtran por Bluetooth lo Energy porque Bluetooth Love Energy carece de muchas protecciones de privacidad aunque no hubo compromiso de datos como dice el investigador muchos muchas personas han lanzado críticas contra su experimento entre comillas no ya que lo han encontrado un poquito de mal gusto Aunque a esto yo tengo un comentario queridos asistentes a este tipo de conferencias de hacking de alto riesgo que si realmente creéis que

cibercriminales van a comportarse y seguir las reglas o adherirse a la ley probablemente hubieran actuado como este investigador pero seguro que hubieran sido mucho más sigilosos estilo Ninja sin que nos enteraran enterásemos de este popup al menos este investigador mostraba amablemente una ventana de popup que te hace te hace un poco pensar sobre todo si ves que en el mensaje pone Blue Devil un nombre así un poco más sospechoso no dirías pues no me voy a conectar a diferencia de poder haber utilizado un nombre un poco más amigable no como Apple TV 1 o Apple TV living room o algo así y bueno siguiendo en este en esta línea de comentario también lo que recomiendan muchas personas Cuando asistes a este tipo de conferencias Como defones dejar tus dispositivos personales en casa eso lo hemos dicho alguna vez en el podcast en otros episodios y utilizar dispositivos de un solo uso como se llaman también en inglés los burner devices no Partner phones o que lo compras lo usas y luego lo tiras o lo devuelves o lo que sea no O probablemente tengáis en casa sean antiguos o vuestra empresa o incluso os puede facilitar y solo instalar aplicaciones de mensajería que incluyen cifrado extremo extremo por defecto Desactivar 2g y esos protocolos que son tan tan débiles Aunque Bueno hay muchas guías de mejores prácticas por internet para asistir a este tipo de conferencias así que bueno recomendable que antes de ir a una competencia tipo un poco investigues que son las mejores prácticas para su asistencia y que dejéis sobre todo los dispositivos personales en casa para evitar sustos mayores de todas formas vamos a comentar el impacto potencial si el investigador hubiera sido malicioso o si un actor de amenazas un grupo apt chino de esos que siempre hablamos no hubiera querido aprovecharse de la situación si un usuario interactuará con las indicaciones y si el otro extremo es decir el servidor el dispositivo Apple malicioso estuviera configurado para responder de manera convincente es decir que cuando haces conectar No pues siga el protocolo y se establezca que no solo sea el primer pop porque entonces te da sospechas No pero si todo va bien y se emula digamos este protocolo el investigador cree que se podría lograr que la víctima transfiera su contraseña en datos sensibles el investigador dijo que estos problemas ya se conocen desde un estudio académico publicado en 2020 que estudió el protocolo Bluetooth de baja energía de Apple y concluyó que existen varias fallas que filtran datos del dispositivo y de comportamiento de los dispositivos Bluetooth lo Energy cercanos que permiten recuperar el número de teléfono el correo electrónico de Apple ID o incluso a sus usuarios en ese estudio publicado por investigadores de la Universidad de León en Francia descubrieron que los dispositivos de Apple filtran información privada a través de los mensajes Bluetooth lo Energy que emiten estos problemas están relacionados en concreto con los servicios de continuidad de Apple y afectan a todos los dispositivos de Apple así como dispositivos compatibles con la funcionalidad de continuidad Los investigadores hicieron ingeniería inversa de este protocolo o funcionalidad que se llama continuidad o en inglés continuity e identificaron que los mensajes de bluetooth lo Energy emitidos por dispositivos de Apple incluyen datos no cifrados que exponen información privada y se pueden recolectar para rastrear usuarios monitorear actividades en una casa inteligente obtener los números de teléfono direcciones de correo electrónico y comandos del asistente de voz de Apple City en Bluetooth lo Energy los dispositivos transmiten mensajes cortos llamados paquetes de o anuncio para comunicar su presencia y características a dispositivos cercanos estos paquetes de anuncios pueden incluir el nombre de dispositivo su tipo y también datos personalizados en un campo utilizado por cada fabricante en concreto y por lo general los fabricantes utilizan este campo para transmitir datos de aplicaciones Apple Utiliza este campo en concreto para incluir datos de sus protocolos de continuidad o continuity como digo Bueno y qué son estos protocolos de continuidad de Apple pues estos protocolos están diseñados para aumentar la usabilidad de sus productos características concretas incluyen transferencia de actividad transferencia de archivos como el conocido airdrop

compartir contraseñas de WiFi y similares esto de las contraseñas de wifi si tenéis a alguien en vuestra agenda y está poniendo la contraseña de una WiFi en concreto de la que tenéis también la contraseña pues os sale un POP si estáis cerca de dicha persona porque Bluetooth también se como digo vía Bluetooth Energy y os dice Oye queréis compartir la contraseña con esta persona que está a punto de escribir una contraseña de Wifi en su iPhone y puedes compartirla directamente la comunicación entre dispositivos cercanos a través de el protocolo de continuidad se realiza mediante Bluetooth lower Energy como digo Bueno pues el tema es que está diseñado de tal forma que aunque algunos mensajes algunos elementos estén cifrados la mayoría de los datos enviados en estos mensajes de continuidad se envían en texto claro y estos datos se pueden recolectar de forma pasiva con snipers Bluetooth lo Energy tienes que estar cerca o con equipos sensible o con antenas potentes para recibir estas señales Pero eso lo que digo exponen la privacidad de estos usuarios de estos dispositivos de Apple por ejemplo se pueden utilizar esos mensajes para rastrear a los usuarios ya sean dispositivos iPhone iPad airpods o cualquiera que este protocolo de continuidad porque a pesar de que este protocolo incluye una funcionalidad para evitar este rastreo que es utilizar direcciones randomizadas hay varios elementos que permanecen constantes con el tiempo o que pueden debilitar el mecanismo de esta función anti rastreo que es la randomización de direcciones por ejemplo Los investigadores dicen que hay mensajes emitidos por los airpods que incluyen información como niveles de batería y el contador de apertura de la tapa que pueden ser explotados para rastrear estos ipods es decir pues si tienes un airpod que tiene batería 88 pues te puedo puedo ir monitorizando este dispositivo en concreto Aunque cambie la dirección y si sigue con 88 luego va a seguir a 87 o si se va a cargar pues seguirá 89 podría inferir un poquito el a ver con Siempre hay que tener en cuenta que esto no es 100% preciso pero ayudaría a rastrear a estos dispositivos también lo que se puede hacer es determinar inferir relacionar los dispositivos que están asociados con una misma cuenta de iCloud este ataque se basa en la repetición de mensajes que provocan una respuesta solo de los dispositivos asociados a la misma cuenta de iCloud un atacante podría aprovechar esto para identificar todos los dispositivos pertenecientes a una persona y podría deducir su ubicación o su hogar si estos dispositivos Allí se encuentran y se pueden identificar De todas formas comentar que este ataque es activo A diferencia de los otros que estoy comentando que son pasivos que es solo snifar digamos los mensajes Bluetooth Energy de anuncio también podemos monitorizar las actividades en una casa inteligente hay mensajes emitidos por dispositivos compatibles con homekit que pueden revelar la actividad que está sucediendo en una casa inteligente homekit es un marco de protocolos de hogares domóticos no hogares inteligentes desarrollado por Apple y se encuentra en dispositivos de obviamente Apple y también otros fabricantes como digo no estos fallos o estas fugas de privacidad no solo se limitan a apple son los más afectados Pero también es otros dispositivos que utilizan protocolos diseñados por Apple como homekit están afectados estos dispositivos que utilizan homekits Qué pasa que utilizan Bluetooth Energy para evitar emitir continuamente mensajes que incluyen un indicador que refleja el estado del dispositivo por ejemplo en el caso de una bombilla este indicador cambia solo cuando se enciende o se apaga de forma similar en un detector de movimiento infrarrojo el indicador también cambia solo cuando una persona cruza el campo de detección cuando hay movimiento experimentos en laboratorio por estos investigadores mostraron que un atacante pasivo puede aprovechar los mensajes de bluetooth lo Energy de homekit para monitorizar la evolución de dispositivos en una casa y de esta forma abrir o monitorizar la actividad de la misma qué más pues voy a comentar el tema de que hay varios mensajes de bluetooth loner y de anuncio que exponen una amplia variedad de información sobre las características y el estado del dispositivo emisor en concreto modelo al dispositivo versión del sistema operativo

color de dispositivo conectividad celular nivel de batería actividad actual y temas similares esto como digo es bastante muy por diseño para que los dispositivos sepan con quién se va a comunicar cada dispositivo y pues ajustar un poquito los protocolos las comunicaciones de esta forma podemos capturar también como he dicho antes direcciones de correo electrónico y números de teléfono esto por qué pues cuando se utilizan funciones como airdrop y Nere los dispositivos emiten mensajes de los que se pueden extraer direcciones de correo electrónico y números de teléfono estos servicios de continuidad permiten compartir recursos con dispositivos cercanos airdrop para compartir archivos near para compartir credenciales de red WiFi el caso del escenario que mencionado anteriormente Cuando alguien que tienes en tu libreta de direcciones está introduciendo la contraseña WiFi y tú se la puedes compartir previo al intercambio de esta información los dispositivos establecen su identidad mediante el intercambio de identificadores a través de bluetooth low Energy se intercambian direcciones de correo electrónico y o números de teléfono Eso es identificadores no se envían en texto claro sino que se envían en forma de Hash que se puede abusar se podría digamos crackear para los datos originales y finalmente ya paró el último tema de privacidad sería los comandos del asistente de voz City porque cuando se activa por voz este asistente crea un mensaje que incluye una huella digital del Comando Aunque la señal de audio sin procesar no se puede reconstruir a partir de ella es decir el mensaje de audio que tú le has dicho a Siri por ejemplo Siri suscríbete al podcast tierra de hackers en Apple podcasts Ah Y también en Google Play y en Spotify y en ivoox pues no se puede reconstruir esto y obtener el audio pero sí que se podría aprovechar esta huella digital para inferir el comando que es total que hay muchos mini fallos podríamos decirlo así o de poca importancia algunos no son de tan poca importancia no pero individualmente cada fallo filtra un pequeño dato una pequeña cantidad de información pero si agrupamos todo esto estos datos se pueden usar para identificar y rastrear dispositivos durante largos periodos de tiempo y bueno también como he dicho el tema de que algunos en algunos casos se pueden comprometer contraseñas no como el tema de la contraseña de la WiFi a ver que lo del tema de la WiFi parece poco importante pero obviamente si es si alguien sabe dónde vives y sabe tu red WiFi y luego tú desvelas la contraseña de tu red WiFi y estás apañado porque entonces bueno obviamente ya sabéis no entrarían a vuestra red WiFi de vuestra casa y de ahí pues podrían hacer lo que quisieran Y por qué pasa todo esto os preguntaréis incluso ya desde el 2020 el estudio se publicó en 2020 pero ya del 2019 es cuando empezaron a analizar e identificar todos estos detalles estos digamos los fallos de diseño pues Apple de hecho reconoció estos digamos estos estas fichas como él diría estas funcionalidades y dijo que no que esto está diseñado de esta forma tal y como ellos han querido y dijo que no iban a arreglar nada de esto porque esto es de tal forma es Cómo funciona el protocolo que ellos han diseñado para que los productos de Apple puedan ser lo más A menos lo más user friendly posibles Bueno pero que me voy por la rama no el tema Por qué está diseñado de tal forma Pues por todo lo que mencionado anteriormente no para compartir temas por airdrop para compartir la contraseña WiFi también temas interesantes que probablemente usemos más que es como el tema de seguir utilizando dispositivos de Apple como los Apple watch o los auriculares airpod vuelvo a recordar el escenario inicial esto sucede porque el bluetooth lo Energy está activado no entonces antes os he hecho la pregunta de cómo lo desactivaríais Pues el tema que normalmente todos hacemos es desde deslizar el dedo si lo tienes en el en el control de acceso rápido desde arriba a la derecha deslizas el dedo y te sale este menú de varias opciones no una de ellas es Bluetooth el icono de bluetooth tienes al lado el icono de la WiFi y también el icono del modo avión que incluso en el episodio anterior hable de un potencial ataque de persistencia después de una de un compromiso de teléfonos dispositivos iPhone falseando un poquito este este modo avión no pero bueno es desde ahí donde

normalmente desactivamos el bluetooth o pensamos que se Ha desactivado pero realmente no se Ha desactivado porque realmente el bluetooth lo Energy Sigue estando activado y de esta forma dispositivos como digo como el Apple watch y los airpods todavía pueden conectarse a tu teléfono iPhone y aquí vengo un poquito con la moraleja de la historia no lo que hay que hacer para desactivar Bluetooth y Por ende Bluetooth lo Energy y evitar todos estos datos de fuga de datos y atento contra vuestra privacidad es Desactivar Bluetooth yendo al menú de configuración y Bluetooth y de esta forma Vais a poder dormir mucho mejor e ir tranquilos a conferencias como la Def con Gracias Alexis Bueno yo este año no pude ir a la defcon tuve que verlo Desde la distancia y la verdad muriéndome de envidia pero bueno ya he visto esto que era bastante trending en Twitter todo el troleo este de todas las la gente recibiendo eso que sobre todo para los que van por primera vez a Def con o Bueno todavía no no están tan acostumbrados en general en torno a Def con hay como ese miedo de que te van a hackear de que si está en las fuerzas del cuerpo de seguridad del Estado ahí dropeando cero days de que te espían seguro que asustó a más de uno y seguro que mucha gente apagó el móvil directamente hasta aquí Hemos llegado queridos oyentes como siempre Esperamos que hayas aprendido algo nuevo si es así déjanoslo saber coméntanoslo en redes sociales en los comentarios Y de paso déjanos una review que ya sabes que nos ayuda un montón y a ti te cuesta prácticamente nada nos haces un gran favor Y así seguimos creciendo Muchas gracias por estar ahí como siempre semana a semana nosotros volvemos para la semana sin falta es septiembre Hay que volver al trabajo los delincuentes no han parado así que nosotros tampoco os mando un abrazo Muchas gracias por escucharnos y ya sabéis hasta la próxima semana Adiós adiós 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 la tierra de