64. Fog Reveal

los departamentos de policía de eeuu han estado utilizando la plataforma foc review para vigilar a usuarios móviles de forma masiva gracias a datos de aplicaciones móviles comunes que brokers de información han comprado y re vendido por un precio anual de unos 7500 dólares americanos viento en popa ya toda vela os traemos otro episodio de tierra de hackers comenzamos hola hola y bienvenido a esa tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 4 de septiembre de 2022 este es el episodio número 64 yo soy alexis porros y en este episodio no tenemos al gran martín ya que se encuentra fuera del ciberespacio lamentablemente pero lo vamos a tener de vuelta en el próximo episodio así que quedamos sentados hasta que venga en el próximo así que en este episodio estamos tú y yo querido oyente bueno y las noticias que te traigo pero primero de todo como siempre agradeceros a todos vosotros nuestros queridos oyentes el seguimiento que nos hacéis en redes sociales donde nos comenta y si nos enviáis vuestras sugerencias y preguntas y me refiero a twitter instagram y facebook donde estamos como el handle a tierra de hackers donde nos podéis seguir y escribir comentarios y lo que queráis también en si no estáis suscritos a nuestro podcast en vuestra plataforma de escucha favorita y ahora mismo a suscribiros para que cuando salga el nuevo episodio lo tengáis tengáis esa notificación de que ya para escucharlo también nos podéis seguir nos podéis enviar vuestros mensajes de sugerencias en linkedin youtube y tuits ahí estamos como tierra de hackers y por supuesto nos podéis enviar nuestros correos electrónicos a podcast a tierra de hackers puntocom bueno y también tenemos un servidor de discordia al que podéis acceder vía tierra de hackers puntocom dischord donde tenemos ya una gran población cibernética digámoslo así de unos 700 usuarios casi ya así que muy muy agradecidos por todos los que os habéis unido ahí a compartir vuestros conocimientos enviar preguntas dudas está está muy interesante la verdad así que os invitamos a uniros también y finalmente antes de entrar en el episodio en sí comentar agradeceros primero de todo vuestro apoyo a la pregunta del episodio que publicamos siempre en twitter y comentarla brevemente en la pregunta del episodio anterior fue la siguiente quién crees que está diciendo la verdad en la confrontación entre twitter y su ex responsable de seguridad twitter match chat ccoo con un aplastante 92% tenemos que nuestros oyentes han elegido a match como el que está diciendo la verdad y un 8% a twitter la verdad es que hay que comentar que match tiene una reputación de ser bastante fiable una persona con moral y ética así que bueno vamos a ver cómo se va desarrollando la historia pero así apuntan las votaciones agradecer también a nuestro patrocinador monat que nos apoya y que nos permite seguir adelante con el podcast monat una empresa que comparte los mismos valores que nosotros hace la seguridad más accesible y transparente nosotros a través de un podcast y mona a través de una herramienta de gestión y visualización de telemetría y datos de seguridad una empresa fundada en sillicon valley y que está buscando muchos ingenieros sobre todo con algo de experiencia en seguridad para ayudarles a construir y hacer realidad su misión lo mejor de todo es que están contratando en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web monet puntocom m o n de un tocón y les podéis contactar al correo tierra de hackers monat puntocom para más información y así ellos saben que venís de nuestra parte y con todo esto un bizcocho comenzamos bueno y que os traigo pues nada más y nada menos que un caso más de abuso a nuestra privacidad queridos oyentes y si así tal y como lo escucháis es que los departamentos de policía locales estatales y federales de eeuu han estado utilizando una

herramienta llamada fox review que sería traducida así como desvela la niebla o revela a la niebla ese plan tenemos una cortina de humo pues con esta herramienta se va el humo y ves la realidad claramente algo así supongo que se inspiraron en llamar a la herramienta foco review pero bueno esta herramienta como digo la están utilizando los cuerpos de policía de eeuu para vigilar a millones de personas en eeuu lo que les ha permitido a rastrear dispositivos individuales sin una orden judicial esto es muy muy importante gracias a información basada en datos recopilados de aplicaciones comunes de teléfonos móviles inteligentes que cualquiera como vosotros queridos oyentes o como yo incluso puede haber instalado en su teléfono estas aplicaciones incluyen aplicaciones del tiempo incluso se mencionan un par bastante populares en la investigación que son starbucks supongo que todo el mundo la conoce para pedirme desde la cafetería de starbucks no perdí café y similares y weiss esta aplicación que es si no me equivoco es propiedad de google ahora y se utiliza para bueno para ubicarte en un mapa y en tener la ruta a tu destino no todo esto viene de investigaciones de la organización activista electronic frontier foundation efe efe y el grupo de noticias a sus 73 y es que estamos acostumbrados a escuchar sobre cómo la agencia de seguridad nacional la n sea la agencia central de inteligencia la cia e incluso la oficina federal de investigaciones fbi todos estos han analizado ilegalmente cantidades masivas de datos sobre personas que viven en eeuu e incluso en el mundo con aliados en otros países como hemos comentado en algún episodio anterior en alemania y similares pero bueno la organización del conjunto de los cinco ojos mundiales verdad pero de lo que no se habla tanto desde que la policía al menos la de eeuu está haciendo lo mismo y ahora lo hemos podido comprobar gracias a correos electrónicos documentos que incluyen incluso manuales publicados al respecto de esta herramienta fox y build y bueno antes de seguir quiero hacer un inciso sobre foc review quien ha creado esta herramienta pues una empresa que se llama fox data science que es un broker de información cuyo producto principal es como digo foc review esta empresa foc teira science tiene su sede en virginia en estados unidos y también tiene entidades relacionadas en nueva jersey ohio y texas fue fundada en 2016 por robert liscovsky quien dirigió la división de seguridad cibernética nacional del departamento de seguridad nacional en la administración del presidente george bush su colega broderick es un ex general de brigada de la marina de eeuu que dirigió el centro tecnológico de de hs el departamento de seguridad nacional durante el huracán katrina en 2005 bueno y cuál es el modelo de negocio de foc teira saints pues esta empresa lo que hace es comprar miles de millones de puntos de datos de unos 250 millones de dispositivos móviles en eeuu originalmente obtenidos de decenas de miles de aplicaciones móviles de los iphone ipad y android como he mencionado anteriormente aplicaciones del tiempo starbucks y weiss por mencionar unas de las más populares los datos provienen de empresas de tecnología y torres de telefonía celular y se recopilan en la herramienta foco review luego por una tarifa de suscripción anual de entre unos siete mil y nueve mil dólares bastante asequible para ciertos cuerpos de policía locales y estatales los que probablemente las grandes ciudades foc deira saints proporciona acceso a una base de datos masiva que permite realizar búsquedas de dónde se encuentran las personas gracias a una interfaz web amena en fácil de usar y muchas veces como digo sin orden judicial o bueno creo que casi todos los escenarios que se han visto en base a los correos electrónicos y documentos obtenidos son todos sin orden judicial las fuerzas del orden analizan estos datos de foc review para crear patrones de vida de los usuarios geolocalizados es decir con estos al fin y al cabo una persona normalmente en su vida real semana a semana repite sus actividades no se puede crear un patrón de vida por la mañana sale de casa y va al trabajo al mediodía va a algún

sitio a comer pues en una zona de restaurantes y luego vuelve al trabajo y a la tarde vuelve a su casa y bueno así así es la vida no si se se va repitiendo y las fuerzas del orden como digo pueden crear estos patrones de vida y bueno y monitorizar a los usuarios según investigaciones the associated press docter science vendió sus software a en unos 40 contratos a casi dos docenas de agencias según una empresa que se llama cops en español sería algo como gastos gubernamentales que controla los gastos del gobierno los registros y los informes de asse siret press muestran el primer relato público del uso extensivo de foc review por parte de la policía local un dato curioso es que hace 73 intentó contactar starbucks e incluso a weiss sobre sobre estas revelaciones estas dos empresas de negaron cualquier relación con factoría science así que estas empresas no dan directamente los datos a fock teira science como digo les vienen los compran estos datos a otra empresa tercera que ahora voy a entrar en detalle en qué empresa es los siguientes de tierra de hackers no se deberían sorprender de este tipo de empresas ya que hemos comentado noticias similares en episodios anteriores y ya en el episodio 52 tenemos el caso del broker de información anormal y six en el episodio 61 tenemos el caso de los brokers de información safe graf y play ser él vamos que no paran de surgir empresas que venden nuestra información para que otras empresas o cuerpos de la ley nos rastreen hoy en día lo que más vale incluso yo creo más que el oro y el petróleo es son nuestros datos así que tendríamos que protegerlos bastante bien aunque nos compensarán si los utilizan sin nuestro consentimiento verdad y con esto voy a está esto permitido alguien se preguntará supongo pues claramente en la respuesta es no en eeuu de hecho está la cuarta enmienda que es un grupo de leyes que protege a los ciudadanos americanos sobre búsquedas o incautaciones de forma no justificada o de forma forzada y esto todo lo que comentó fox review of their a sign si el uso de estos datos por parte de los grupos policiales en eeuu es una clara violación de la cuarta enmienda no sólo si se busca un individuo en particular que es esto sería obvio sino que la cuarta enmienda prohíbe las búsquedas generales y no particulares de los datos de ubicación de todas las personas que estén presentes en un lugar en particular por esta razón los tribunales de hecho dicen que las búsquedas mediante el concepto de jehová ya geof en zinc en inglés también viola en la cuarta enmienda el tema del geof en zinc lo hemos comentado anteriormente anteriormente pero brevemente comentar que es definir una zona geográfica en la que quieres buscar datos sobre personas que están en esa zona en 2018 la corte suprema de eeuu dictaminó que la cuarta enmienda requiere que la policía obtenga una orden judicial antes de incautar datos de ubicación históricos llamados información de ubicación del sitio celular de las empresas telefónicas también se teme que el seguimiento de la ubicación que ofrece foc de iras services es no sólo esta empresa sino muchas otras verdad pueda tener otros usos más aplicados a la vida real o más concretos como controlar a las personas que buscan abortos en estados donde ahora es ilegal y esto como digo lo hemos comentado en el episodio 61 así que si queréis refrescar vuestra memoria escuchando esos episodios ok y cómo se consiguieron estos correos electrónicos y documentos en reveladores la electronic frontier foundation esta organización activista realizó su investigación a través de más de 100 solicitudes de registros públicos presentados durante varios meses y se consiguieron correos electrónicos y documentos de foc de irak science entre estos documentos también se consiguió el manual de usuario de 30 páginas de la herramienta review y luego comentó algunos detalles del manual que son interesantes pero quería comentar una conclusión que obtuvieron los investigadores no decían literalmente que esos registros muestran que foc teira saints y algunas fuerzas del orden policías no creían que la vigilancia de foc de ir a science violar a los derechos de

la cuarta enmienda de las personas y que hiciera falta que las autoridades obtuvieron una orden judicial para poder utilizar la herramienta fox review me parece una conclusión bastante interesante para reflexionar sobre la capacidad de lógica de estas entidades del orden de no saber si la información que están tratando necesita una orden judicial o no pero bueno ahí lo dejo rock tale signs menciona que tiene un socio de información y de hecho es desde esta empresa desde donde obtiene la información para ofrecerle a sus clientes y esta empresa se llama ventel con dos enes vn tl que provee de datos que consume y vende a sus clientes vent él obtiene datos publicitarios globales de su empresa matriz llamada web y analytics los datos en sí proveen como he dicho antes de aplicaciones instaladas en los teléfonos inteligentes de las personas los desarrolladores de hecho de estas aplicaciones a menudo firman acuerdos para vender la información de ubicación de sus usuarios a terceros y de hecho éste es digamos el modelo de negocio que utilizan los desarrolladores que ofrecen aplicaciones gratuitas de alguna forma supongo que tienen que ganarse el pan de cada día y en lugar de cobrar a los usuarios que a veces es una entrada bastante difícil para usuarios que se descarguen la aplicación que la compren pues oye de forma gratuita y a cambio sin que el usuario se dé cuenta o bueno algunos aunque se den cuenta se está compartiendo la ubicación y es lo que estos los desarrolladores recopilan de sus aplicaciones y esto lo pasan a empresas como digo 20 el barra grade y analytics inventen luego lo vende a otras empresas como font era science la información de geolocalización se basa en números de identificación publicitarios lo que se llama en inglés advertising aid y por ejemplo en los sistemas a los que según los funcionarios de fontellas service es se extraen de aplicaciones populares como he dicho anteriormente esta información luego se ven empresas como fonteide saints como he dicho pero también interesante es que se vende a agencias gubernamentales incluida la oficina de aduanas y protección fronteriza de hecho sobre 20 él sí nos habéis seguido cada episodio ya hablamos por primera vez en el episodio 16 allá en noviembre de 2020 cuando cubrimos la noticia que ponía en entredicho de aduanas y protección fronteriza de eeuu pudiera estar abusando de los datos de ubicación de los residentes americanos para ubicarlos y arrestarlos de nuevo si no os acordáis de esta noticia podéis ir a refrescar vuestra mejor memoria y escuchar el episodio 16 por poner un poquito en perspectiva en tema de precio de licencias hemos comentado que una licencia de annual de foc review cuesta entre 7.000 y 9.000 dólares pues la oficina de aduanas y protección fronteriza de estados unidos pago a 20 el casi medio millón de dólares en agosto de 2020 por su software para poder geolocalizar a personas en eeuu se entiende que los cuerpos de policía prefieren ir con folk review que es mucho más barato que con 20 el directamente y por eso creo que en el futuro van a seguir surgiendo empresas de este tipo que venden datos de geolocalización porque van a competir supongo que en precio y bueno van a van a seguir surgiendo de estas empresas hasta que se regularicen un poco el tema bueno y aparte de es dar seguimiento o poder determinar dónde se encuentra un usuario en tiempo real qué es lo que ofrece digamos foc review pues según los materiales de marketing obtenidos foc ctera science también ha promocionado su herramienta folk review con la capacidad de ofrecer análisis predictivos a la policía una palabra un concepto de moda últimamente que se usa para describir herramientas de alta tecnología digamos utilizando mazinger ning inteligencia artificial y similares que para predecir los puntos críticos del crimen no con esto lo que se puede hacer es determinar casi en tiempo real los movimientos diarios de las personas y estar un paso adelante de ellas como he dicho anteriormente no se puede determinar un patrón de vida de estas personas personas pueden ser criminales no pues se podría incluso decir oye pues en base a su historia hoy lunes

suponemos que va a ir a esta zona para cometer un crimen o no o ahí lo podemos ir a interceptar y arrestar así que esta función predictiva también es muy atractiva para los policías rockville se ha utilizado desde al menos el 2018 en investigaciones criminales algunas con resoluciones exitosas como casos de protección infantil y abusos de menores y también como el asesinato de una enfermera de 25 años en newport arkansas se pudieron encontrar los teléfonos de personas que habían estado cerca de ella cuando se la vio por última vez y de alguna forma identificaron al criminal y también se ha utilizado en otras investigaciones criminales como el rastreo de los movimientos de un posible participante en la insurrección del 6 de enero en el capitolio la herramienta foto review rara vez o nunca se menciona en los registros judiciales durante las investigaciones legales algo que los abogados defensores dicen que les dificulta defender adecuadamente a sus clientes en los casos en los que se utilizó esta tecnología foc review permite a la policía y a otros de sus clientes interactuar con la herramienta para realizar distintas tareas por ejemplo dibujar un cuadro una geo vaya a una geofences y ver y anti de identificadores que representan cada dispositivo dentro de esas área geográfica en un periodo de tiempo determinado y también usar la identificación de un dispositivo para rastrear el historial de ubicación preciso de ese dispositivo durante hasta 5 años en el pasado fue previo en sus documentos menciona que sigue rastrea los dispositivos a través de él y de publicidad del advertising aid y estos son números únicos asignados a cada dispositivo que bueno de todas formas se pueden recetar de tanto en cuando desde las opciones del teléfono móvil pero si no las resetea pues es fácil seguir a estos identificadores estos números de identificación de publicidad no contienen el nombre del usuario del teléfono pero se pueden rastrear hasta los hogares y lugares de trabajo para ayudar a la policía a establecer análisis de como digo de patrones de vida y determinar al menos el tipo de persona que hay detrás está detrás de este dispositivo móvil rastreando bueno y sobre el manual unas pinceladas que dicen o cuando inician sesión por primera vez en la interfaz web de foc review los usuarios reciben un mensaje que les recuerda que los datos a los que a punto de acceder son confidenciales y que deben protegerse adecuadamente a partir de ahí un usuario puede comenzar a buscar datos históricos sobre qué dispositivos se encontraban en un área en particular a través de un cuadro de búsqueda que acepta direcciones y coordenadas de latitud y longitud como he dicho los usuarios también pueden dibujar geo bayas geofences para ver qué dispositivos estaban en un área el manual indica que es posible vigilar a una gran cantidad de personas a la vez aunque esto puede no ser útil por la gran cantidad de datos que es que devuelve la herramienta entonces vas a tener muchos datos y no puedes identificar cuál es tu objetivo luego los usuarios pueden etiquetar un dispositivo en concreto para marcarlo como un dispositivo de interés a partir de ahí pueden consultar ese dispositivo en particular y el sistema mostrará un patrón de actividad de unos 180 días o unos seis meses en el pasado y de hecho según uno de los fundadores en la documentación y en los correos electrónicos intercambiados como digo puede permitir búsquedas de hasta cinco años en el pasado el manual también incluye una de pantalla que enumera lo que describe como grupos de usuarios mostrando diferentes usuarios éstos incluyen arkansas el departamento de policía de atlanta el departamento de policía de massachusetts barnstable el departamento de policía del estado de connecticut el departamento de policía del estado de delaware y algunos más algunos dicen la ff y hd 3 que ya se conocían pero otros son nuevos y es una revelación esta lista también incluye una referencia a una empresa privada que se llama eyeworks corp que según dicen podría referirse a iwork corporation que es un contratista del gobierno federal hasta incluso el gobierno federal directamente está usando pudiera estar

abusando de esta información algunos departamentos de policía les gusta mucho la rapidez con la que pueden acceder a estos datos ya que no requieren órdenes judiciales como he dicho por lo general se ha demostrado no que google podría proporcionar información sobre qué dispositivos estaban presentes en un área en particular en un momento específico pero las autoridades necesitarían obtener llamada orden judicial de ubicación inversa que puede llevar tiempo con foco review es tan simple como hacer login y buscar a tu objetivo y esto marca un antes y un después porque según bennett site first que dirigió el trabajo de registros públicos de la electronic frontier foundation en contra de foc their a science dijo que no ha habido ningún registro oficial anterior de empresas que vendan este tipo de datos granulares directamente a las fuerzas del orden local así que esto es una gran revelación y esto viene sobre todo por el precio de lo gratuito no cuál es este precio pues bien quede oyente tu privacidad tenemos que pensar nos lo bien dos veces antes de utilizar aplicaciones gratuitas que puedan poner en peligro nuestra privacidad sobre todo esas que piden información de geolocalización gratuitas y no gratuitas también algunas que pagues incluso pueden ser tan malas como las gratuitas en conclusión piénsatelo dos veces querido oyente antes de darles permiso o si no de vez en cuando puedes analizar los permisos que has otorgado a las aplicaciones y deshabilitar los que pienses que no son necesarios igual te preguntas querido oyente tiene foco de ira saints mis datos y como lo detengo si es así pues es bastante difícil saber si te irá saints y por extensión la policía tiene acceso a tus datos si descargarse una aplicación de terceros cualquier aplicación digámoslo así en tu móvil y otorga este acceso a los datos de ubicación en los últimos cinco años es posible que la respuesta sea así es bastante posible aunque bueno como digo mencionan 250 millones de dispositivos hay muchos más dispositivos en eeuu así que podrías calcular la probabilidad en función a todos los dispositivos móviles que hay en eeuu los residentes en california pueden enviar una solicitud de derecho a saber en base a la ley de privacidad del consumidor en california a la fuente de datos de forma de ir a science event el para saber qué es lo que tienen sobre sobre vosotros y si lo sé no lo sé si sospecho que igual tienen mi información que puedo hacer al respecto pues lo primero el seguimiento de anuncios identificador de anuncios móviles este en años por ejemplo se llama advertising aid y esto se puede desactivar o resetear de vez en cuando así pues se rompe un poco el seguimiento no es que sea infalible y perfecto porque probablemente igual viendo el mismo patrón en dos distintos advertising idish podrían correr y decir estos dos advierta de simitis son el mismo la misma persona el mismo dispositivo móvil pero bueno eso es una forma de ponerse lo más difícil no está esta gente a esas empresas que venden nuestros datos y los recopilan en segundo lugar se puede intentar limitar cuántas aplicaciones en el teléfono tienen permiso a recopilar datos de geolocalización como he dicho antes deshabilita las aplicaciones que no lo necesiten y permíteles a las que lo necesiten como por ejemplo aplicaciones de mapas para orientarse en el espacio aunque como he dicho una de esas aplicaciones que ha proporcionado datos a este tipo de empresas es ways según mi experiencia la utilizan muchísimos taxistas al menos en nueva york y en todo eeuu así que bueno no es tan fácil aplicar esta recomendación pero lo más importante es que que todos podemos hacer bueno al menos desde estados unidos pero también en cualquier otro país es hacer presión al congreso y al gobierno en sí para que protejan nuestra privacidad la supervisión federal de empresas como foc de ir a sainz es un panorama legal en evolución y de hecho recientemente un caso relacionado a la comisión federal de comercio demandó a un broker de información llamado con chava que al igual que font tale signs ofrece información de usuarios móviles en base a identificaciones publicitarias los tribunales también están sopesando el uso que

hace el gobierno de los datos de ubicación y de hecho ahora ya hay proyectos de ley ante el congreso que de ser aprobados regularían la industria recordemos que en 2018 la corte suprema dictaminó que la policía generalmente necesita una orden judicial para revisar los registros que revelan dónde han estado los usuarios de teléfonos celulares esto bueno esto es normal verdad que lo necesiten pero vemos cómo están estos cuerpos de policía se los saltan un poco a la torera así digámoslo utilizando foc review y con esto queridos oyentes llegó a la pregunta del episodio cuál crees que sería la medida más efectiva para evitar el abuso de información de geolocalización de usuarios obtenida a partir de aplicaciones móviles que siguen tus movimientos os vamos a ofrecer cuatro opciones de respuesta la primera es pues bueno el gobierno con la legislación debería tratar este tema la segunda sería que los fabricantes deberían aplicar más restricciones aún para evitar que aplicaciones pudieran acceder de forma ilimitada a accesos de ubicación la tercera es que los desarrolladores deberían tener un poquito más de moral decidir no vender toda esta información de geolocalización a otras empresas y la última somos nosotros queridos oyentes los usuarios de estas aplicaciones móviles que podríamos intentar bueno de alguna forma enviar ubicaciones falsas o no utilizar el gps como he dicho desactivarlo resetear el advertising aid y este que he dicho es todo más desde la parte del consumidor del usuario así que ahí planteamos la pregunta del episodio y votad por favor en twitter y bueno antes de acabar el episodio también quería comentar brevemente una noticia que me ha parecido muy interesante y bastante relacionada sobre este tema de geolocalización no están en relacionado con un tema a nivel global oa nivel de todo un país como eeuu es un tema más concreto pero bueno durante la conferencia de la blanca de este año en las vegas a la que pudimos asistir martín y yo en calidad de prensa en representación de tierra de hackers los investigadores de nozomi networks que es una empresa que se enfoca en seguridad de sistemas de control industrial mostraron un nuevo ataque contra los sistemas de localización en tiempo real construidos con tecnología de radio de banda ultra ancha ultra white man en inglés lo que consiguieron los investigadores fue uno monitorizar estos dispositivos de rastreo sin el conocimiento de su objetivo de la persona que lo lleva y dos incluso hacer que cualquier dispositivo de rastreo en tiempo real pareciera que se moviera voluntad de sus atacantes y ubicarlo en lugares falsos brevemente entrar explicar que es el ultra wide band para los oyentes que no sepan lo que es es una tecnología de radio de banda ultraancha es una tecnología que no es nueva muchos productos la utilizan el caso más popular es el de apple que lo ha integrado en dispositivos móviles a partir del iphone 11 así como en los modernos relojes apple home potts y probablemente lo que más conozcáis son los airbags estos se utilizan esta tecnología ultra wide band para identificar dónde se encuentra este dispositivo en todo momento en gracias a bluetooth también se está utilizando en proyectos de infraestructura a gran escala como el del sistema de señalización del metro de la ciudad de nueva york ultra wide band se puede aplicar a cualquier tecnología es simplemente que el ancho de banda utilizado para emitir la señal específica es más ancho de lo normal como digo ultra white los beneficios son menos errores de transmisión y recepción con incluso mayores velocidades de lo normal protección contra interferencias o jamming e incluso se puede compartir el canal con más usuarios y para que se utilizan estos sistemas pues por ejemplo tres casos de uso el primero es seguimiento de empleados en industrias en fábricas donde mucha maquinaria peligrosa también en entornos médicos para el seguimiento de pacientes para aplicarle las medidas del tratamiento que requieran en cada momento el segundo caso es definición de jehova jazz para detener maquinaria peligrosa si sale debe una definida y el tercer caso de uso sería el seguimiento de contacto por

ejemplo como el de la pandemia del cobi 19 pero cuál es el problema que identificaron los investigadores pues la tecnología de radio de banda ultraancha sea utilizado en sistemas de localización en tiempo real no ok hasta aquí todo bien el tema es que aunque existe un estándar del iec hubo el institute of electrical and electronics engineers el instituto de ingenieros eléctricos y electrónicos y que como digo han definido un estándar para estos sistemas de localización en tiempo real no cubre ese estándar la sincronización o el intercambio de datos lo que entonces depende de la implementación de los proveedores algo que crea oportunidades para la explotación y con esto me refiero a sincronización e intercambio de datos pues son los datos que están en movimiento los datos que se envían este estándar del y okubo no define cómo se deben proteger estos datos no define los niveles de confidencialidad e integridad y disponibilidad de estos datos no define si se tienen que cifrar o no esto todo depende del fabricante que pone a la venta sus dispositivos de ubicación en tiempo real los investigadores de hecho se enfocaron en dos sistemas de localización en tiempo real de tecnología de radio de banda ultraancha uno es el guión indoor tracking y el otro es el kit empresarial avalúo de nit y artemis estos sistemas que son como los stacks de apple llamemos los de forma genérica etiquetas radio se comunican con un servidor de localización en tiempo real a través de un sistema intermedio que son llamados anchors en inglés a los que me voy a referir como puntos de acceso en lugar de centrarse en la comunicación entre de hecho las etiquetas y el punto de acceso en lugar de centrarse en el entorno radio los investigadores analizaron las comunicaciones que normalmente van por un medio cableado o no pero más en él en la parte de la infraestructura entre los puntos de acceso y el servidor de localización en tiempo real donde ocurre todo el procesado y cuáles son los escenarios de ataque que demostraron estos investigadores pues me mostraron unos ataques de suplantación de ubicación como los siguientes primero mostraron cómo pudieron rastrear objetivos utilizando los sistemas de ubicación en tiempo real existentes ya hemos visto los casos de abuso y la preocupación por los usos maliciosos de el 'tax en los que un mal hecho rastrea una persona escondiéndole un nerd tag en una mochila chaqueta o vehículo verdad pues en este ataque el equipo no necesitaba ocultar un dispositivo metérselo en la mochila chaqueta o vehículo simplemente arrastraron la etiqueta que su objetivo ya usaba todo esto gracias al análisis de los datos interceptados entre el punto de acceso y el servidor de ubicación en tiempo real también demostraron cómo falsificar los movimientos de una etiqueta en un escenario de rastreo de contactos de kobe 19 podría crear una alerta de exposición falsa o evitar que el sistema detecte una exposición y finalmente otro caso de ataque fue la demostración sobre una maqueta de una instalación de fabricación donde los datos de localización en tiempo real se usan para apagar las máquinas para que un trabajador puede entrar de manera segura a la zona de máquinas y que no sea dañado de forma física los investigadores pudieron modificar los datos y detener la producción en la maqueta de la fábrica engañando al sistema para que pensara que había un trabajador cerca lo contrario incluso podría ser más grave al hacer que parezca que el trabajador se ha ido del área de esta peligrosa con maquinaria cuando en realidad todavía está ahí la máquina podría reactivarse y lesionar potencialmente al trabajador una de las limitaciones del ataque es que un atacante necesita haber comprometido un sistema dentro de la red en la que se encuentra el servidor de localización en tiempo real para poder interceptar y manipular las comunicaciones en el caso de la investigación esto lo realizaron a nivel de red mediante ataques de hombre en el medio the man in the middle con spoofing de erp o suplantación del protocolo a erp que es un protocolo que se utiliza para la asociación y resolución entre direcciones mac y direcciones ip y

gracias al abuso de este protocolo pudieron suplantar por ejemplo a los sistemas en esta infraestructura ya fuera el servidor de ubicación en tiempo real o los puntos de acceso las implicaciones las fallas de seguridad de esta tecnología identificadas por los investigadores y se implementan si se materializan y se abusan por atacantes son bastante graves especialmente en entornos industriales ya que podrían ser incluso mortales cuales son las mitigaciones que pudiera haber al respecto pues los investigadores añadieron capacidades de cifrado al sistema de ubicación de localización en tiempo real pero descubrieron que esto creaba mucha latencia tanta quien utilizaba el sistema para darle la capacidad de tiempo real entonces no era una mitigación válida la mejor solución los investigadores sugirieron fue que se revisara el estándar del ie cubo para cubrir la sincronización y el intercambio de datos lo que significa que los fabricantes tendrían que implementar funciones de seguridad en sus dispositivos y si fuera posible distribuirlas en forma de una actualización de firmware no para que sea más barato sino en el peor de los casos habría que reemplazar el hardware y con ello el dispositivo físico en conclusión que no te puedes fiar de estos sistemas de localización en tiempo real porque su ubicación puede ser falsificada fácilmente bueno como digo tienen que los atacantes necesitan tener un sistema comprometido en la misma red en la que se encuentra el servidor pero es posible esto también está muy relacionado con la noticia que comenté en el episodio 62 sobre los sistemas gps de esta empresa china microbús que tenían vulnerabilidades y que podían usarse para también falsificar la ubicación gps de estos dispositivos que se utilizan para gestión y control de flotas de vehículos y nada como digo como siempre acabamos diciendo a estos episodios parece que es el fin del mundo al menos en el tema cibernético pero bueno nada nosotros siempre queremos traer las noticias tal y como son esperamos que el episodio sea instructivo informativo para todos vosotros y que hayáis disfrutado de un buen rato así que nada como siempre agradeceros por escucharnos en cada episodio y nos escuchamos en el siguiente probablemente con martín de vuelta muchas gracias chao chao 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 una valoración donde nos estés escuchando también puedes seguirnos en twitter instagram y facebook te esperamos en el próximo episodio de tierra de hackers