es la nueva técnica presentada por investigadores de la Universidad de waterloe Illinois que permite Localizar a personas dentro de un edificio abusando el del protocolo WiFi investigadores académicos alemanes desvelan el misterio de cómo los soldados rusos han podido identificar la ubicación de los operadores de los drones dji que bombardeaban sus bases y sus tanques gracias a la interceptación de las comunicaciones radio y al análisis del protocolo drone ID de conferencias y un par de días más tarde pero sin faltar a nuestra cita semanal aquí tenéis 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 16 de marzo de 2023 este es el episodio concretamente 86 yo soy Martín vigo y está conmigo el irrepetible e inigualable Alexis porro sol Alexis qué tal Muy bien aquí contigo Martín esta semana fue el día de pi ese número tan interesante de las Matemáticas hubiera sido chulo publicar ese día pero bueno no pudimos pero desde aquí Muchas felicidades a todos esos afanes en las matemáticas es el lenguaje que es de la naturaleza de todo lo que nos rodea y nada pues muy interesante así que tenemos que hacer un día del día de tierra de hackers no así para también hacer algo así sí lo podíamos hacer el 12 de abril que es cuando publicamos el primer episodio 12 de abril oficialmente lo en el calendario día de tierra de hackers pues ya está listo mira listo qué ideas y totalmente sin planificar me encanta pues nada para no enrollarnos que nos ha llegado ese feedback esos comentarios muy interesantes y muy buenos decir que no os voy a montar el rollo a través de las redes sociales Porque si episodio 86 no lo sabéis todavía Ya os hago un friend en Facebook y en todo y en todas hay oyentes nuevos no en este episodio pero sí seguro que muchos se lo sabe si no sabes lo que donde podéis ir veis a tierra de hackers.com y ahí están todos los enlaces a todas las redes sociales comentaros también uno interesante que igual no sale así tan visible que es discord que tenemos una comunidad muy muy rica muy interesante comentarios charlas muy muy muy útiles Y entonces podéis entrar vía tierra de hackers.com barra discord y ya con esto como siempre agradecemos vuestro apoyo en todas las redes sociales como ha dicho los comentarios para mejorar el podcast y para llevarlo más allá pero también os agradecemos el apoyo a la pregunta del episodio que cada episodio publicamos en Twitter y la del episodio anterior fue la siguiente De qué forma crees que se podría evitar que empresas de vigilancia puedan recopilar información de usuarios online esto venía en referencia Bueno a las múltiples empresas que hemos cubierto en episodios anteriores pero en concreto a la empresa de auror empresa auror de Nueva Zelanda Y tenemos cuatro respuestas la más votada sería educar al usuario para evitar que esto suceda con un 38%, seguida de pues tener leyes proactivas que un poco vigilen de este problema con un 27% seguida de redes sin perfiles algo un poco interesante con un 20% y finalmente un 15% medidas antibot porque sabemos que todas estas empresas son muy automáticas para extraer la información y utilizan Bots para bueno para hacer el scripping de toda esta información Así que ahí lo dejamos perfecto y yo aprovecho a dar las gracias a nuestros mecenas de patreon tenemos cuatro esta semana nuevos estoy súper contento platanito canario que me hizo mucha gracia Non que esto es nada y a Alba Muchísimas gracias por formar parte de la familia de tierra de hacker es el próximo el próximo episodio uno va a ser mojo picón o algo así cierto Hola guagua y también agradecerle a nuestros sponsors en concretamente Tenemos uno nuevo Muchísimas gracias a A3 sech que es una empresa española de ciberseguridad con presencia en España pero también México y Colombia y que lleva más de 10 años en el sector focalizada en dar respuestas a tres Pilares principales prevención detección y respuesta cubren servicios ofensivos como red Team pen testing auditoría de código etcétera y también dan servicios gestionados de monitorización Avanzada respuesta entre incidentes y red hunting con un enfoque diferenciador en el mercado siempre están buscando profesionales para incorporar a su equipo ofensivo y de seguridad y vigilancia

digital para trabajar en un ambiente colaborativo y con enfoque muy técnico así que ya sabéis ir a su web que es A3 sech.com y les decís también que vais de nuestra parte muy bien y también lo mismo darle las gracias a otro de nuestros patrocinadores en este caso prowler Pro Gracias por apoyarnos en el podcast y decir que brawler pro es la herramienta más completa de seguridad en aws empresas de todos los tamaños se apoyan diariamente en prawler pro para que sus equipos puedan confiar en su modelo de seguridad de aws puedes probar prauer Pro hoy mismo y de manera totalmente gratuita obtendrás paneles y gráficas con información concisa y accionable con todo lujo de detalles sobre la madurez de tu modelo de seguridad y una visión completa de tu infraestructura en todas las regiones de aws además tendrás todos los resultados en apenas unos minutos empieza a usar brawler pro y beneficiarte de sus resultados visitando tierra de proswllrprpro muy bien perfecto Pues antes de comenzar solo solo recordaros que estuve que tierra de hackers estuvo en la ruta y la verdad fue súper divertido y me lo pasé muy bien con mucha gente pero quería mandar un saludo a Jordi murgo que es un tío con el que me eché muchas risas y me lo pasé muy bien y sé que es un fiel oyente del podcast y se lo prometí probablemente cuando Hagamos una ronda de entrevistas nos lo traeremos y también a Oscar y Daniela de micro hackers que se portaron Alexis conmigo de lujo No solo son unos tíos cojonudos sino que además hicieron de fueron mi Uber particular Así que muchas gracias a micro hacker Está bien qué bueno fueron de micro a Uber Sí exactamente Exactamente Bueno sabes con la noticia que si no nos alargamos hoy os traigo el análisis de otro paper que fue publica de tan solo unos meses en la conferencia acm mobycom en Australia y esto lo hago en parte porque cuando despedimos feedback para que sepáis que tanto Alexis como yo prestamos mucha atención a lo que nos pedís fuisteis varios los que nos comentabais que os gustaba cuando desgranábamos papers sobre temáticas interesantes y desde luego ésta Lo es publicado por aliadevil Y deepack basic esto es Los investigadores Proponen un nuevo ataque contra las redes wi-fi que permitiría la localización física de dispositivos conectados a la red esto implicaría también de personas si lo pensáis porque ya que se podría localizar la localización de los móviles que normalmente la gente lleva los bolsillos por tanto al fin al cabo lo que estás localizando es el móvil que esa persona tiene guardado y por tanto localizas a la persona recordemos las implicaciones para nuestra privacidad y seguridad de ataques como este o sea el poder más que geolocalizar localizar dentro de un edificio Tú desde fuera a una persona donde está en ese edificio cualquiera desde la calle podrías haber dónde estamos no en el propio paper plantean Como por ejemplo delincuentes podrían saber la localización de guardias de seguridad en todo momento si saben que cuando están haciendo la ronda en ese momento están en la planta de abajo podrían entrar por la primera planta por ejemplo al edificio No simplemente monitorizar por donde se están desplazando para poder evitarles mientras cometen un robo asalto a una persona que requiere de este tipo de seguridad la localización física de personas y dispositivos dentro de un edificio usando como digamos vehículo las redes WiFi No es algo novedoso son varios los ataques propuestos en el pasado que de alguna manera ya sea mediante análisis de Señales ruido o tráfico podría dar indicaciones de la localización física de los dispositivos uno de estas investigaciones previas es radar y mediante que mediante el uso de varias estaciones mide la propagación de la señal de radiofrecuencia que se verá afectada pues al chocar con objetos y con eso se podría llegar a determinar Pues dónde hay personas físicamente dentro de un edificio el problema de Esta técnica es precisamente que necesitas montar varias estaciones para emitir señales y recibir señales desde distintos ángulos sail sail es otro sistema este se centra en medir el tiempo que requieren los paquetes en viajar del router a los dispositivos el problema aquí es que no es un sistema que puedes desplegar de manera encubierta si lo pensáis y que además requiere estar conectado a la WiFi donde están conectados tus objetivos

por tanto tienes ese otro problema y otro que mire ese array que utiliza un sistema multiantena para triangular la posición de un dispositivo Aquí el problema una vez más es que tienes que ser el router para empezar que usa la víctima o sea es decir que tu objetivo esté conectado a una red wifi tú estés controlando router y además necesitas varios puntos de acceso desplegados en la zona no son técnicas que fueron propuestas como posibilidad de abuso a nuestra privacidad básicamente los sistemas hasta día de hoy requieren que previamente hagas mucho finger printing para tener un baseline no que le dicen con el que comparar los datos o requiere desplegar como decía múltiples antenas en la escena donde se encuentra tu objetivo o simplemente requiere estar conectado a la misma WiFi a la que está conectada el móvil de tu objetivo y quiero matizar que cuando digo que estas investigaciones tienen estas investigaciones previas digo tienen problemas no me refiero a que realmente tengan un problema estas técnicas no se han no han sido diseñadas o estudiadas con el objetivo de rastrear la localización de dispositivos de manera secreta el objetivo de estas propuestas es que legítimamente se necesita saber la localización en Casos pues como por ejemplo centros comerciales si quieres pues monitorizar por donde se mueve la gente en oficinas por si quieres pues tener localizado dispositivos wi-fi y cosas así pues bien wip elimina todos los requerimientos y permite la localización de las personas por cierto que no sé si lo mencioné antes wipip es como llamaron a esta investigación académica y en general Pues a la metodología mecanismo o digamos modos operando y porque no realmente una herramienta en sí Sino una manera de llegar a hacer este vector de ataque vamos a llamarle wipi va al vector de ataque que Proponen estos investigadores de los que os voy a hablar y esto lo que permite es Localizar a personas sin asociarte a la red WiFi sin desplegar múltiples antenas y sin ningún tipo de finger printing previo Y es que wipi sí que explora los problemas de privacidad esto Comparado con las investigaciones previas de hecho el título del paper en concreto es Non cooperative WiFi localization and It's privadas y implications es decir la localización de dispositivos en WiFi No cooperativas y sus implicaciones de la privacidad Aquí vemos que este estudio académico sí se centra en eso y por eso nos interesa a nosotros y os lo traemos aquí a tierra de hackers Así que vamos a ver qué es lo que Proponen estos investigadores primero vamos a deshuesar no las diferentes partes del ataque y luego veamos cómo lo hace lo primero es que son capaces de generar tráfico en un dispositivo sin estar asociado a la misma WiFi que está ese dispositivo es decir que yo soy capaz según este paper de hacer que tu teléfono que está conectado a la WiFi de tu casa genere tráfico de manera que yo lo pueda ver sin que yo esté conectado a la WiFi de tu casa Solo la verdad Alexis me está mirando un poquillo es muy interesante Y cómo hacen esto que Alexis me mira con cara de cómo hacen esto de hecho pregunta Alexis y cómo hacen esto Martínez Explícame a ver un poquito más pues abusando particularidades del diseño del protocolo hecho 02 11 o dicho de otra manera aprovechándose de debilidades en Cómo funciona la red wi-fi paso 1 necesitaremos el ssid de la WiFi objetivo qué es esto del ssd Alexis me has pillado porque no me acuerdo el acrónimo pero ese Station su scribe ID no sé es él básicamente Bueno bueno yo te digo que está muy bien el acrónimo Pero tú que eres un experto de desgranar términos y conceptos tan complicados para nuestra querida audiencia que a veces no es altamente técnica procede a contarnos qué es esto del ses ID Pues sería el nombre de la red WiFi por ejemplo efectivo default que hay muchas redes WiFi que son así Open o abierta sí o aeropuerto Madrid o todo esto o Starbucks o todas estas vale es el nombre de la WiFi el ese ID pues esto es Es lo único que es requerido Es decir si yo por ejemplo quiero ir a robar a tu casa pues necesitaría para llevar a cabo este ataque el nombre de la WiFi que no la contraseña solo el nombre de la WiFi que recordemos que tu router lo está gritando A los cuatro vientos y yo puedo escucharlo No solo eso tenemos servicios también como google.net donde yo desde mi casa puedo ver nombres de la WiFi de zonas que me

pueda interesar Entonces paso 2 identificar los dispositivos que hay en la red objetivo concretamente las direcciones Mac Qué quiere decir esto ahora que yo tengo el nombre de la WiFi de tu casa ahora tengo el paso 2 que identificar las direcciones Mac de los dispositivos que están conectados a esa red Pero aquí es donde en principio chocamos con el problema Cómo cómo puedo hacer eso Si yo no estoy asociado a la red no y recordamos que la dirección Mac es por decirlo de alguna manera un identificador único para tu dispositivo móvil en concreto es un identificador único para la tarjeta de red Pero bueno lo podemos ver como la matrícula de tu móvil que es única no y es un poco pues como se utilizan los protocolos para poder dirigirse a ello el equivalente a una persona pues sería tu nombre no y apellidos que sería sería digamos la matrícula de una persona pues bien poniendo el ejemplo de si yo quiero robar un banco y quiero saber dónde están los guardias de seguridad en todo momento pues utilizamos vamos a empezar a utilizar ese caso de uso No yo quiero robar un banco por lo primero sería irme de noche a las cercanías del banco para que esté dentro de la zona de cobertura de la WiFi No pues por ejemplo puedo aparcar mi coche enfrente del banco no en la calle y desde el coche puedes hacer todo tipo de operaciones sin levantar sospechas lo siguiente que quiero hacer es encontrar los dispositivos conectados a la red WiFi del banco ya dijimos que yo pues simplemente con estar cerca puedo saber el nombre de la wifi al igual que cuando estás cerca de un Starbucks pues miras tu móvil para conectarte una red WiFi y ves el Starbucks ahí pues ahora lo siguiente estando en cercanía pero no dentro del banco Yo quiero saber qué dispositivos están conectados y esto esto lo quiero hacer yo sin tener que Conectarme a la red WiFi porque como decía no es no es requerimiento tener la contraseña de la WiFi esto es importante remarcarlo porque si estuviera conectado a la misma red sería trivial encontrar los otros dispositivos conectados si yo estoy en la red WiFi de tu casa para mí es muy sencillo saber qué otros dispositivos están conectados a esa red pero como no lo estoy Pues aquí viene la triquiñuela si bien nuestros dispositivos transmiten de vez en cuando paquetes al aire no a pesar de estar un estado de modo de ahorro de batería pruebas de estos investigadores mostraron que algunos dispositivos tardan mucho tiempo en enviar dicha información y si intentamos robar un banco pues queremos poder actuar rápidamente Qué quiere decir esto tú cuando no estás usando tu móvil y está en tu bolsillo como es el caso que estamos utilizando de los guardas de seguridad la pantalla se apaga se pone en modo de ahorro de batería pero también hay muchas funcionalidades que se están ejecutando en segundo plano que dejan de funcionar porque ya no es tú si no estás navegando por internet Pues hay muchos procesos que no requieren estar activos porque tu móvil está bloqueado no eso no quiere decir que la radio de tu teléfono de repente se apague pero vamos que disminuye muchísimo la actividad y ellos hicieron pruebas y se dieron cuenta que el móvil al no estar transmitiendo pues no podemos nosotros interceptar ese tráfico por tanto lo interesante sería poder hacer algo para poder interceptar ese tráfico o más bien dicho poder hacer que el teléfono genere tráfico aquí es donde entra una de las particularidades chulas de esta investigación ellos Proponen abusar el mecanismo de ahorro de batería que os está diciendo implementado en el protocolo WiFi para detectar dispositivos conectados a esa red de manera inmediata forzando que transmitan paquetes que podemos interceptar y con ello identificar las direcciones Mac parémonos aquí un momento para que entendamos mejor cómo hacen esto porque a mí la verdad que me gustó mucho porque desconocía este vector de ataque y me trajo ideas para líneas de investigación no de algunas cosillas que tenía pensado mirar recordar que lo que os voy a explicar ahora es una manera en la que tú puedes hacer que el móvil de otra persona sin estar conectado a la misma WiFi empieza a transmitir tráfico de manera que tú lo puedes interceptar y ver la dirección Mac que tiene Ok esto Es como ir por la calle se me ocurre así ahora y que tú puedas hacer que una persona diga su nombre y apellidos en alto es

como como fuerzas a una persona hacer eso Si no eres amigo de él no Pues un poco eso sería la analogía Pues resulta que para ahorrar batería los dispositivos Como por ejemplo nuestros móviles que era nuestro caso de uso relevante insisto mientras los dispositivos están durmiendo como decía el punto de acceso que para dicho de otra manera el router no que no siempre tiene que ser un router o así pero vamos a llamarle el router puede guardar temporalmente en un buffer la información que debería enviarse al dispositivo hasta que se despierte para enviársela en ese momento Esto es lo mismo que si yo quiero hablar con Alexis y Alexis se va a echar una siesta Y en vez de seguir hablándole Yo empiezo a memorizar todo lo que le quiero decir y cuando se despierta le digo Ay Alexis mira que te quería comentar que mañana grabamos el episodio y tal y cual y cuál pues esto sería lo mismo estás dialogando Alexis se va a dormir Yo me yo voy memorizando todo lo que le quería decir y cuando se despierte se lo digo todo entonces así permito que Alexis pueda irse a dormir porque yo tengo la capacidad del almacenar en un buffer es decir mi memoria todas las cosas que me van llegando que le quiero decir a Alexis y aquí viene la clave hay un paquete especial que envía el punto de acceso el router a todos los dispositivos que viene a decirles Oye tú que tengo información almacenada aquí para ti esperando a que te despiertes y este paquete se llama Traffic indication map o Team para nuestros oyentes más técnicos esto qué quiere decir que yo ahora en el protocolo WiFi que representamos entre una entre Alexis y yo yo puedo despertar Alexis hay una manera en la que yo le puedo enviar un paquete es decir decir Alexis despierta que tengo algo que decirte y tengo la memoria llena y si no se me va a olvidar entonces Alexis desperté me dice Ah vale vale Te escucho dime Y le suelto todo lo que tengo en la memoria Vale pues hay un paquete especial que me permite despertar los dispositivos móviles en una red WiFi para decirlos Oye tengo tengo datos almacenados Y qué pasa cuando un dispositivo Recibe un paquete del router diciendo lo que tiene información almacenada para él pues como decía Pues en este caso mando un paquete de vuelta cuando está listo para recibir diciendo Hey router cuando tú quieras soy todo oídos no es como si yo le digo Alexis despierta que tengo que decirte algo de Access me dice o se empieza a desperezar se frota los ojos y dice pero es para un segundo vale vale dime dime ahora que ya te presto atención Pues eso yo despierto Alexis con y Alexis me tiene que contestar diciéndome vale Ya he despertado Háblame ahora Vale pues ese paquete contiene la dirección Mac del dispositivo dicho de otra manera nuestra analogía Alexis diría Hey soy Alexis Espérate un segundin que ya ya estoy despierto dime entonces Alexis acaba de decir quién es en nuestra equivalencia la dirección Mac y por tanto yo estoy escuchando y ahora sé cómo se llama Alexis justo no sé si no sé cuánto tiempo es el que el que se estipula el protocolo eso va por fabricante que es Supongo que debe ser un minuto o 30 segundos o como sea hay oportunidad no el atacante básicamente no tiene que tirarse ahí 24 horas para para identificar a un dispositivo exactamente Es una cuestión de segundos por lo que dicen hicieron un análisis por ejemplo con un Galaxy 7 sin generar estos paquetes y tuvieron que esperar más de 10 minutos para que el teléfono en modo ahorro de batería algún paquete que ellos pudiesen interceptar y contuviese la dirección Mac pero generando paquete steam a los dos segundos ya había contestado por tanto eso es un avance muy grande voy a comentar algo así me ha venido a la mente no es completamente relacionado con el tema este de la privacidad y la geolocalización pero me ha venido a la mente esto de ataques para despertar a dispositivos estamos acostumbrados a que nuestros dispositivos tienen batería y va a decir larga pero es dura 24 horas Así que tampoco Ese es que sea muy larga dura 24 horas el tuyo el mío tío no me llega ni un día es verdad que que siempre estoy mirando algo de YouTube pero Y eso eran los Nokia los Nokia 3210 una semana y la pantalla blanco y negro en verde pero y nuestro dispositivo tampoco son tan críticos pero imaginaos lo que pasaría con dispositivos médicos por ejemplo

marcapasos y de hecho yo en el 2017 se publicó una vulnerabilidad de una empresa que se llama Met sec de hecho llevo digamos un poco le sacó los colores a otra empresa que se llama senjut Medical que fabricaba marcapasos y los tenían implantados mucha gente ahí en su corazón Pues entonces esto marcapasos normalmente duran siete años no pues con este ataque que los investigadores descubrieron podían hacer que el marcapasos se despertara más rápido porque hay un lo puedes Digamos si estás a cierta distancia física no sean 10 metros algo así puedes hacer que el marcapasos se active como para el modo de programación Y eso hace que se vaya cortando la batería más rápido que en modo de operación normal Entonces eso hacían que estos estos pacientes que tenían plantado marcapasos tuvieran que ir a emergencias o requiere una operación a corazón abierto en menos de siete años para reemplazar el marcapasos así que solo quería dar ese comentario que me parece interesante es un apunte buenísimo Alexis porque de hecho voy entrar en brevemente en el tema de ataques de de me salen inglés de desgaste de batería a través de enviar tráfico y hacer que esté despierto que el equivalente aquí sería Alexis No te duermas Alexis No te duermas Alexis Alexis ahí con la cara toda rechupeteada porque no le dejo dormir sería un poco eso no te estoy acortando la vida en realidad al no dejarte al no dejarte dormir justo justo Sí sería un caso igual que el marcapasos pero aplicada a los teléfonos o a las personas Sí sí pues bueno pues como decía de esto se aprovecha precisamente el ataque wipi para descubrir dispositivos en una red a la que no está conectada abusa la funcionalidad de ahorro de energía y envía un paquete haciéndose pasar por el router a todos los dispositivos diciéndoles que tiene información para ellos consiguiendo Así que cada uno de los dispositivos conteste y así obtener su dirección Mac Y si os preguntáis pero un momento un momento Martín quieto quieto parado cómo es posible Enviar un paquete a todos los dispositivos si no sabes qué dispositivos hay es un poco el huevo y la gallina Pues bueno el paquete puede formarse de una manera especial que indica todos los dispositivos no tienes que saber cuáles hay digamos que tú puedes construir un paquete haciéndote pasar como que lo envía el router en el que en el que en vez de decir Alexis despierta digo todo el mundo que me está escuchando Despierten para la gente más técnica esto sería poniendo el beatmap del paquete Team con todo fff que es un clásico pues este es un truquillo muy bueno porque ahora es como estar gritando despierta en todos y todos los dispositivos se despiertan de hecho la analogía aquí militar que se me ocurre es eso el sargento entrando en la barraca donde están todos los soldados durmiendo sería un poco es decir Despierta despierta y todo se ponen de pie no no ha dicho a quienes pero ahora todos dicen Alexis a la orden Martín a la orden Manolo a la orden que siempre sale siempre tiene que salir Manolo en un episodio de tierra hackers pues ahí estamos es exactamente cómo funciona este protocolo yo como atacante he entrado como el sargento diciendo simplemente que todos Despierten y luego cada uno de los soldados Es decir de los dispositivos me ha ido diciendo su nombre mientras me decía que estaba a la orden esperando instrucciones pues es así como funciona paso 3 ahora que tenemos todas las direcciones Mac de los dispositivos en la red recordemos todo esto sin hacernos conectado a esta WiFi lo siguiente es medir Cuánto tiempo tarda un paquete en ser entregado esto también se conoce como el Time offline no básicamente pues imaginaros la velocidad en la que se propaga el sonido que si yo recuerdo que a lo mejor digo Aquí una burrada y me asesináis pero era rollo de 1000 km por hora no que es cuando se rompe la Barrera del sonido los aviones cuando van a mil kilómetros por hora yo creo que sí pero bueno el más chuno no Este sí puede ser y decir otra burrada Alexis me Mola porque me estás me quieres apoyar como buen amigo mío que eres estás mirando con cara no tengo ni idea pero no me quieres dejar en ridículo bueno da igual la velocidad el sonido Pues bien si digo lo de la velocidad del sonido porque si Alexa y se halla más lejos de mí yo cuando le digo Alexis despierta pues el sonido se prepara a una velocidad y tarda más en llegar a los

oídos de Alexis Cuanto más lejos esté esto Es evidente no Entonces esto sería el Time offline el tiempo que tarda en llegar el sonido de mi voz a los oídos de Alexis en la versión que nos concierran aquí del protocolo WiFi pues es el tiempo que tarda yo como atacante en enviar el paquete de despierte y que le llegue que esto evidentemente pues es radio se transmite por las ondas del aire pues lo que tarda en llegar al dispositivo pero claro yo no voy a saber cuándo llega el dispositivo a no ser de que ese dispositivo me diga me ha llegado que ahora vamos Así que para medir esto tienes que poder comunicarte con el dispositivo pero recordemos volviendo lo de antes que no estamos conectados a esa WiFi por lo que cómo hacemos para hablar con un dispositivo que esté conectado a una WiFi a la que nosotros no estamos conectados y que incluso esa WiFi puede estar cifrada o sea ahora vamos una vuelta más allá ahora ya no es que yo digo esto el equivalente sería que yo entro pegando un grito o sea Alexis es que se me va ocurriendo sobre la marcha pongamos que Alexis habla chino y yo solo hablo español vale Yo puedo despertar Alexis simplemente pegando un grito no porque eso es como digamos internacional y Alexis despierta vale Ok pero ahora yo no puedo comunicarme con Alexis porque yo no hablo chino entonces es en el punto donde estamos yo consigo despertar a Alexis con ese paquete Team porque es internacional digamos Pero cómo puedo yo ahora hablar con Alexis si él solo habla chino el equivalente sería Cómo puedo yo comunicarme con un dispositivo que está conectado a una WiFi a la que yo no estoy conectado pues quizás os sorprenda como a mí pero una vez más Hay ciertos paquetes que puedes enviar utilizando la dirección Mac es decir el paquete Team nos da la dirección Mac es decir nos da el nombre de Alexis y ahora hay una manera en la que yo puedo comunicarme con Alexis concretamente ahora que ya sé su nombre a pesar de que habla chino y yo no es decir en una red WiFi yo puedo hablar con un dispositivo en concreto en vez de chillarla a todo el mundo a pesar de que no estoy ni conectado a su wifi y este me va a contestar tú esto te sorprende no Alexis porque a mí me sorprendió pues estos investigadores mostraban Cómo era posible comunicarse con dispositivos ajenos de manera que te contestasen con el famoso ack no y lo llamaron po light wi-fi y en su día lo mostraban como una manera en la que podías agotar la batería de los dispositivos ajenos con este tipo de ataques como bien explicaba Alexis en el caso de del marcapasos no básicamente ya tenemos que podemos enviar paquetes a dispositivos específicos conectados a una WiFi Ajena con solo saber su dirección Mac me da la impresión que me estoy un poco repitiendo un montón con todos los matices pero es que es muy importante entenderlo Entonces cómo hacemos ahora para estimar Dónde están esos dispositivos físicamente porque ahora yo puedo despertar a Alexis con un grito Alexis le puedo hablar por su nombre para que me haga a pesar de que yo no hablo chino y me contesta pues ahora y resumiendo mucho para que no se alargue más esta noticia se aprovechan de que el estándar de la WiFi indica que la respuesta tiene que enviarse a lo exactamente a los 10 nanosegundos de recibirla es decir pegó un grito Alexis se despierta ahora yo le hablo de una manera que aunque no hable chino él me va a contestar pero es que aparte él va en cuanto me escuche va a esperar 10 nanosegundos y me va a contestar y siempre va a esperar 10 nanosegundos por tanto usando esta constante la velocidad de la luz y ciertos modelos para lidiar con pequeños márgenes de error diseñar un sistema para medir lo que os comentaba antes el Time offline pero de manera muy precisa es decir poder detectar a la distancia que se encuentra Alexis cuando como yo le hablo a pesar de que no hablo chino Pero sabiendo que va a tardar diez segundos después de recibir esa respuesta y por tanto la única variable que queda es precisamente Cuántos tarda en llegar mi voz a la suya y la suya a la mía si puedes medir el Time offline de manera precisa entonces puedes calcular como de lejos está ese dispositivo al que estás enviando información hasta aquí todo muy bonito pero como siempre suena ciencia ficción bueno quizá no a ciencia ficción pero digamos de momento es un paper es un estudio

académico además aunque esto funcione bien y sea fácil como implementamos esto en un caso real cómo hacemos volviendo al caso del banco yo ahora cojo este paper y como robo ese banco como más bien detecto Dónde están los guardias de seguridad Pues bien estos investigadores no se quedaron en la teoría o experimentos de laboratorio sino que demostra la eficacia de su vector de ataque con un dron y esto Me alegra porque nos gustan los drones una de las noticias que más le gustó a la gente que nos dijo en el Twitter era la del dron que se utilizó para acceder a una red corporativa de una empresa sobrevolándolo por el tejado pues esto se hicieron algo igual queridos oyentes estos cracks usando un mini drone dji equipado con el mítico chipestl esp8232 este Alexis me dice que sí no recuerdo era el número pero el mítico que se utiliza para temas de WiFi que vale nada vale céntimos pues equiparon ese mini drone porque no pesa nada además de hecho pusieron dos por temas de cálculo de que no voy a entrar al tema según me leí al paper pero básicamente pusieron un chip capaz de mandar paquetes en el protocolo WiFi a un Mini drone y sobrevolaron un edificio y eran capaces de detectar dónde estaban físicamente todos los dispositivos conectados a la red objetivo físicamente dentro del edificio desde un dron con solo tener la el nombre de la WiFi nada más espectacular se acabó así tan rápido como cuando vi venir el dron y se fue pim Pam a ver hablan de que de que tiene que mandar pues unos 100 200 paquetes no para medir un poco el Time offline y ir comparando con el modelo que tiene Y tal Pero pero me parece una pasada que porque insisto las desventajas de los otros papers académicos que veíamos que no estaban centrados en privacidad Pues tienes que poner varias antenas o tienes estos problemas o estar asociado la WiFi pero no no a esto el Setup comentaron que les costaba como 50 dólares y el dron es lo más caro y sobrevolando una red pum puedes estar monitorizando a los guardias de seguridad por dónde están haciendo la ronda en qué planta están y ya te metes ahí a robar el banco hasta la cocina un comentario que iba a hacer porque estaba pensando mientras lo ibas diciendo es que un ajuste de esa velocidad que calculan es la de la luz no la del sonido verdad sí sí no sé por qué es que antes habla del sonido cuando hablaba del tema de hablarte a ti no un poco para medir esa distancia Pero es verdad que las ecuaciones en las ecuaciones utilizaban la de la luz que ahora que me lo dices Claro que es así que me la sabía 3 por 10 a la ocho a 300 Por 300.000 kilómetros no por segundo pero sí que es verdad que en el paper mencionan la velocidad de la luz pero ahora que me ahora me pillas porque porque no así a vote pronto no sé por dónde entra el tema de la velocidad de la luz porque deberías a por la pero claro es que no no es el sonido lo que se propaga radio o es que a lo mejor estoy convencido de que hay alguien alguien que sabe de física que que se está arrancando los pelos con esta conversación siempre electromagnetismo que es como es una onda como la luz pero quería matizar eso que como estamos en la semana de pi del número pi seguro que igual hay algún matemático que está lo que tú dices está tirando de lo espejo no no yo lo que creo Es que estamos vomitando aquí conceptos que he leído en el Piper O sea que se nos da bien el tema de ciberseguridad pero claro me pongo a ver ecuaciones y me da así un jamacuco sabes entonces estoy intentando aparentar aquí que sé de lo que hablo pero vamos ya no hay ninguna vergüenza en reconocer Lo importante es eso nuestras limitaciones no por lo menos hablo por mi caso tenemos que empezar a invitar a expertos en la materia en materia que no sea de ciberseguridad para darle saborcillo abogados científicos físicos matemáticos a noticias que lo requieren todos esos todos esos que he mencionado los podemos ya con el chat gpt 4 que salió hoy los podemos ya reemplazar olvidaos ya no hace falta justo otro tema que me venía me ha venido ahora es el tema de que has dicho que se pueden identificar a la gente dentro del edificio lo curioso es que no lo han mencionado Los investigadores pero podían Añadir haber añadido una funcionalidad que hubiera sido la de aparte identificar dispositivos saber qué persona es porque normalmente tenemos los teléfonos móviles que están ahí

emitiendo el nombre del dispositivo móvil y muchas veces la gente se lo compra y se pone se lo registra no en iCloud o lo que sea o en Android en Google Play con su nombre entonces aparte de saber dónde está el dispositivo sabes quién de quién pertenece el dispositivo que es incluso me parece todavía más impresionante se podría hacer una versión 2.0 de de ataque igual lo han pensado no pero y de hecho hay hay ya frameworks de esto que han salido en el 2012 o así que lo hemos cubierto también lo hemos mencionado en otros episodios ese se llama Snoopy o uno que se llama pinotes que están en github de esta empresa sense post de Sudáfrica que lo que hacen es eso bueno Y también De hecho salió creo una charla el año pasado en la defón o Hace dos años que también era algo parecido que también podía traquear dispositivos móviles por vía Bluetooth y vía WiFi que también es una punta interesante Sí yo creo que tratándose de un paper académico ellos un paper académico Normalmente se centra en lo que no no se ha descubierto aún o un pasito más adelante en una en un campo en concreto no por eso yo creo lo podían haber mencionado con un poco como el comentario no de que puedes reutilizar tecnología existente o vectores ataque existentes para poder Añadir el nombre pero claro el se centra en la parte novedosa no pero desde luego lo que dices tú Es un complemento fantástico ahora ese que Manolo El guardia de seguridad está aquí no solo que hay un guardia de seguridad que está aquí esa es buena y el otro tema estaba pensando los últimos modelos de teléfonos cuando los apagas siguen emitiendo verdad al menos en plan celular no sé si la WiFi el chip WiFi sigue emitiendo pero por ejemplo los iphones sobre todo para el final iPhone y todo este tema de acoso y tal Creo que todavía cuando están apagados siguen emitiendo pero no sé la parte WiFi No sé si si sabes tú algo Martín Pero bueno sería algo también a investigar esa es muy buena lo que pasa es que aquí explotan fallos WiFi Pero sería interesante claro Alexis tú hablas de ahora las funcionalidades estas nuevas de si pierdes el móvil o te lo apagan que lo típico sigue emitiendo algo mínimo De hecho no solo eso sino incluso cuando se te queda sin batería realmente se apaga un poquito antes o sea que dices tú se ha quedado sin batería no no le das y te sale ahí el mensajito de que sigue emitiendo no sé si ahí hay algo a través de WiFi se podría se podría hacer algo porque eso va a estar bajo mínimos mínimos Entonces no sé sería sería interesante porque sería la leche que no no tengo el móvil apagado y aún así alguien puede saber dónde estás físicamente y luego a mí siempre me hace gracia un poquito no sé si lo han comentado pero ahora es contramedidas no un poquito quería mencionar cómo nos podemos proteger Es que mira me fui ya casi a los 35 minutos muy importante y no nos gusta hacer el podcast demasiado largo pero tienes toda la razón y no lo incluyen las notas pero evidentemente lo leí y básicamente Cómo me puedo proteger Pues mira tienes que moverte muy rápido O sea tienes 10 nanosegundos para estar en un sitio y luego en el otro porque así para cuando le llegue para cuando le llegue la respuesta ya ya te has movido no pero básicamente lo que sugieren son cambios al protocolo no recuerdo mal es que no tomé notas pues era hacer ciertos ciertos tiempos aleatorios luego hablan de cambiar Pues el cómo se comporta estos paquetes que a ver yo empezaría por ahí que tú te puedas comunicar con un dispositivo al que no estás asociado a la misma red me parece bastante curioso simplemente lanzando paquetes al aire y ya está Entonces yo creo que si quitas eso pues ya ya has destrozado todo este protocolo no sé si hay alguna razón de ser sobre todo la parte esta del Cómo era el WiFi Nobel wi-fi o bueno el paquete este que si tienes una dirección Mac te va a contestar porque lo del ahorro de batería lo puedo entender pero pero ese paquete de Contéstame con solo tener tu Mac no entiendo por qué existe que a lo mejor hay alguna razón de ser pero bueno a mí se me ocurrían sin ser experto y sin haberme leído el paper por ejemplo el iPhone tiene le puedes pedir le puedes dar un setting una configuración que utilice diferentes Mac que las aleatorice no sé cada Cuándo cambia pero creo que cada vez que se conectan a WiFi Pues sería diferente

Pues no sé si si desconectarte el problema y volverte a conectar efectivamente Si recuerdo bien en el paper mencionaban que la lectoriedad que se produce los teléfonos de la dirección Mac precisamente por temas de privacidad no ayuda porque como lo están utilizando como parte del protocolo capa 2 Aunque tú tengas una es tu manera de comunicarte con el dispositivo entonces va a funcionar igual a lo mejor no te funciona para mañana tienes que volver a averiguar una nueva Mac no básicamente sí queridos oyentes esto sería lo mismo que si Alexis en vez como se llama Alexis me dices que se llama Álex y mañana se llama Manolo se pone nicknames no pero pero claro yo a la hora de hablar con él si él se me presenta como Álex puedo tener una conversación con él A lo mejor mañana se ha cambiado el nickname y ya no me haces caso pero claro en este caso no funciona como mitigación a esto otra idea que se me ocurría que todavía el protocolo es wifi no lo implementan pero protocolos cable así como el macec es que se puede cifrar la dirección Mac o sea mi nombre como decíamos que si habláramos chino pues realmente no me entendieras o hablar a un idioma klingon Claro pero volvemos al tema de que esto es específico del protocolo WiFi Por eso yo creo que que Claro tú hablas incluso sabes como ha salido el wpa3 que todavía ni muchos dispositivos lo soportan en router sobre todo los móviles y eso sí ya pero digo que Podrían haber incluido esta funcionalidad que ya llevan con el WPA muchos años y todavía no han añadido ese tema de vamos a cifrar un poquito como tú dices la capa 2 los nombres que se mencionan así a todo el mundo claro lo que pasa es que yo creo que el concepto de wpa3 entra a una capa diferente Es que aquí donde está el fallo en el estándar del 802 no en Cómo estás cifrando las comunicaciones no entonces entra antes el fallo sino de hecho creo que el wpa3 no sé si tiene puede modificar la capa 2 porque para poder si fuera adicional por encima del bpa2 igual no habría que cambiar el firmware Bueno no sé habría que mirar solo era solo una idea porque esto en ethernet en redes cableadas sí que existe claro se puede cifrar las direcciones Mac y en WiFi no Y la otra bueno era pues caja de faraday eso esos esas bolsillos que bolsillos que puedes meter el teléfono cuando no quieres que no tienes que utilizarlo pues lo metes ahí mira aquí es incluso desactivar la WiFi tío un caso más de utilidad Oye si no te hace falta el teléfono cierto cierto Ah y lo último me ha hecho gracia lo de lo de el retraso de la respuesta que por el protocolo que sea 10 Nano segundo me preguntaba si si eso se pudiera Claro si esos protocolo no puedes hacer un poco ahí de Añadir un poco de variación porque entonces tus paquetes no llegarían y tal Así que esa contra medida no Sí de hecho ellos mencionan que no todos los dispositivos los cumplen se han encontrado con protocolos que pues que lo hacen en 8 Nano segundo Y tal Pero uno mediante la dirección incluso a veces por la dirección más puedes saber por los primeros bytes Qué tipo de dispositivo es Entonces si lo tienes pre estudiado pues ya lo sabes y luego pues eso con sus modelos y tal pues corrigen esos errores menores que efectivamente los hay no es 100% preciso y decían que desde el tron fueron capaces de localizar dispositivos con centímetros de margen de error espectacular increíble centímetro centímetro muy bueno Pues sí y antes de pasar a tu noticia Alexis Qué te parece si le damos las gracias a otro nuestro sponsors 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 mona con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley que está buscando ingenieros con experiencia 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 mona.com y mandarles vuestro currículum concretamente a tierra de hackers @monat.com También queremos dar las gracias A On branding que es otro de nuestros patrocinadores una empresa formada por especialistas en varios ámbitos profesionales que se enfoca en la reputación online a múltiples niveles han ayudado desde personas como tú y como yo hasta famosos a llevar a juicio casos de ciberacoso

mitigar situaciones donde la reputación de empresas estaba siendo mal intencionadamente dañada e incluso a borrar la huella digital que dejamos online no Solo han decidido Apoyar el podcast sino que si le contáis que venís de parte de tierra de hackers tendréis un descuento especial en sus servicios si necesitas algún tipo de ayuda con vuestra identidad digital on branding es lo que estás buscando visita o branding punto es y sin más dilación pasamos a la siguiente noticia voy a hablar un poco de la guerra en Ucrania y de los drones bombarderos durante la Guerra en Ucrania los soldados ucranianos han estado utilizando armas improvisadas armas caseras utilizando dispositivos electrónicos que cualquiera puede comprar comerciales baratos no nada así a nivel militar sofisticado de millones de dólares como por ejemplo los drones de DJ hay de uso civil esos que podemos comprar como digo en cualquier tienda online en cualquier tienda física en concreto el modelo Dj eye mavic 3 y lo que han hecho es engancharles bombas digámoslo así son unas granadas con un mecanismo de liberación casero para bombardear bases enemigas rusas y tanques para los siguientes que sigáis el podcast Esto no es nada nuevo ya que lo hemos comentado en otros episodios anteriores Y para aquellos oyentes que escuchen esto por primera vez os recomiendo que escuchéis los episodios 48 y 49 sobre la ciberguerra la bbc publicó en 2016 que Isis utilizaba drones comerciales para bombardear a sus enemigos y a principios de enero del año pasado se publicó un vídeo que mostraba al Cartel de Jalisco Nueva Generación o los matacetas usando drones comerciales para bombardear cárteles enemigos también se han publicado vídeos de los soldados ucranianos utilizando los drones dji mavic para bombardear los vehículos rusos los tanques rusos usuarios de Twitter que vieron algunos de estos vídeos publicados en noviembre del año pasado especulaban que la bomba descargada por el dron podría ser una granada Box 17 modificada que aunque parece que digamos que es porque tiene un tamaño pequeño como el de un puño es bastante efectiva como se puede ver en algunos vídeos en los que se muestra tanques rusos que se incendian después de dejar caer una de estas granadas desde un dron dji el dron está obviamente teledirigido a distancia y se ve tiene una cámara como todos estos drones y se ve en el vídeo justo como el dron se acerca y el tanque tiene esta abertura que tiene en la parte superior del tanque que es una abertura redonda y ahí justo se acerca y descarga la bomba y pum la granada y hace explotar y incendiar el tanque ruso estas granadas fueron modificadas y les añadieron unas aletas impresas en 3D para que siguiera la trayectoria cuando se lanza desde el dron Bueno lo curioso es que estas granadas Box 17 Normalmente se lanzan desde lanzagranadas automáticos a GS 17 que son rusos así que están utilizando grana lanzadas desde lanzagranadas rusos contra los rusos un poco irónico pero es interesante a todo esto comentar que dji esta empresa China de origen chino se opuso a que los ucranianos se utilizaran sus drones comerciales para fines bélicos y de hecho Dj mencionó a principios de noviembre del año pasado que iba a suspender las ventas de sus drones a los ucranianos y rusos debido a esto Estados Unidos proporcionó drones fantasma a Ucrania para poderlos utilizar en la guerra estos drones fueron desarrollados por las fuerzas aéreas estadounidenses dos meses después del inicio de la invasión rusa en Ucrania y apodas fantasmas Phoenix la empresa californiana avx aerospace también ayudó en la producción de estos drones así que estos drones no son drones caseros que se pueden comprar en cualquier tienda son drones de nivel militar desarrollados por el gobierno y una empresa privada quería mencionar brevemente otros drones que se han utilizado también para poner en contexto un poquito la diferencia del Dj mavic 3 el DJ mavic 3 por ejemplo puede llegar a una altura de 6 km puede llegar a una distancia a un Rango de 30 km que es bastante recorrer esa distancia puede alcanzar una velocidad de 68 kilómetros por hora tiene una batería de 46 minutos algo que la hace un poquito Pues eso un poquito tiene que volver a cambiarle la batería para poder usar de nuevo la carga Útil es entre medio y un kilo para los más grandes y el precio son 1700

dólares Por otra parte tenemos los drones militares fabricados por Irán y usados por Rusia justo en este conflicto bélico uno que se llama shajet 136 o También conocido como geranium 2 que tiene un Rango puede volar una distancia de 2500 kilómetros Comparado con los 30 del Dj mavic o con los 300 del dron va a ir tb2 que fue fabricado por Turquía y son los que usa Ucrania Así que vemos que los drones rusos fabricados por Irán son los que pueden volar una distancia más larga incluso la velocidad que pueden alcanzar es de 185 km/h aunque los drones ucranianos pueden alcanzar 220 kilómetros por hora y la carga útil pueden llevar hasta 30 o 50 kilos los drones rusos mientras que los drones es algo menor es también del del nivel de la unidad de kilos pero no llegan a tanto lo curioso es que los drones de Irán utilizados por Rusia valen 20 mil dólares que dices Bueno es un precio bastante asequible para ser un drone militar en cambio los drones fabricados por Turquía usados por Ucrania valen 2 millones de dólares cada uno hay que decir que las armas que llevan son bombas guiadas por láser que son mucho más precisas y claro requieren más tecnología pero ahí vemos que el DJ mavic por 1700 dólares está compite bastante bien con los otros drones militares tanto los ucranianos como rusos han estado usando drones militares en la guerra pero posiblemente solo los ucranianos han usado los drones comerciales que menciono como el DJ mavic 3 y de hecho los soldados rusos han estado atacando los drones comerciales de distintas formas y cuál es el objetivo de los ataques de los soldados rusos contra los drones comerciales pues varios el primero es hacer que el dron deje de funcionar mecánicamente y se estrelle es decir que pierda el norte y no sepa dónde está y Bueno ahí se queda y como se queda y se para pues se cae obviamente y se estrella contra el suelo el segundo objetivo también hacer que el dron deje de comunicarse con su operador y obviamente si pierde el control remoto pues una de dos o sigue volando hasta que se le acabe la batería o también lo mismo se separa en ese momento y cae hacia el suelo o aterriza también de forma sin dañarse o incluso a veces están programados Para volver hacia su origen que esto último podría utilizarse para seguir al dron a la base a donde está el operador a donde está el soldado ucraniano y dejarlo fuera de combate de alguna forma y cómo hicieron esto los rusos una forma es utilizando El rifle Support así se le ha dado este nombre que dispara pulsos electromagnéticos lo que deja los drones perdidos y desorientados ya que bloquea las comunicaciones GPS y el dron se queda sin poder Navegar otra forma es utilizando aerospace que es un sistema online que permite detectar e interrumpir las comunicaciones entre drones comerciales y sus operadores Esta es la tecnología que los rusos utilizaron ya desde los primeros días de la guerra para encontrar rápidamente la ubicación del dron y su piloto ucraniano el soldado ucraniano y bombardearlo y dejarlo fuera de combate según la bbc un soldado ucraniano dijo que ahora ya son capaces de evitar que los rusos sepan dónde se encuentran los operadores de los drones no se comenta si realmente supieron cómo lo hacían los rusos Pero me imagino que supieron que lo hacían a través de la interceptación y el análisis de las comunicaciones Radio Entre dron y controlador el controlador remoto y que harían algo al respecto Aunque tampoco dicen que hicieron los ucranianos pero me podría imaginar que igual falsificarían de alguna forma su ubicación igual a través modificando el firmware del dron o el controlador en cualquier caso aquí estamos desde tierra de hackers investigando para resolver este misterio bueno no lo resolvemos nosotros pero lo resolvieron los académicos de la universidad alemana de Ruth pues estos investigadores identificaron vulnerabilidades en varios drones fabricados por dji estos fallos permiten que cualquier usuario pueda cambiar el número de serie del dron y anular los mecanismos que permiten a las autoridades de seguridad rastrear los drones y sus pilotos inicialmente Los investigadores probaron tres drones Dj de diferentes categorías en busca de vulnerabilidades El DJ mini 2 que es bastante pequeñito el Air 2 que es digamos mediano y el mavic 2 que es un poquito más grande más tarde los investigadores reprodujeron los resultados en el modelo mavic 3 que es

el más nuevo y el más grande que es de hecho el que han estado utilizando principalmente los soldados ucranianos para bombardear a los rusos Supongo que primero se enfocaron en los tres anteriores porque son más baratos y validaron las vulnerabilidades en el mavic 3 que es un poco más caro para encontrar las modalidades Los investigadores atacaron directamente los drones reales a veces temas de este tipo de análisis de sistemas embebidos sistemas Hardware iot podríamos decirlo firmware se hace a veces offline no se consigue el firmware y se realiza pues análisis de seguridad pero en este caso el dron es un sistema tan complejo Que a día de hoy no hay incluso para otros dispositivos Hardware a veces no hay no hay emulación no hay plataformas de emulación que puedan digamos pretender ser el Hardware el rotor por ejemplo del dron para que tú lo puedas conectar digamos a tu ordenador como una máquina virtual en vmware y analizar eso Entonces tuvieron que hacer el análisis de seguridad directamente contra los drones y para eso lo que hicieron fue conectar los drones a sus ordenadores vía WiFi vía radio y lanzaron ataques de fashing una característica de Esta técnica es que los investigadores no necesitan saber cómo funciona exactamente el dron es decir no tienen que hacer ingeniería inversa del firmware los protocolos o las comunicaciones lo que hacen Entonces es tomar el drone como una caja negra y le envían grandes cantidades de datos inválidos inesperados o aleatorios mientras analizan en tiempo real el comportamiento del dron y buscan desviaciones o diferencias en su comportamiento comparándolo Con cómo se comporta en una operación normal es decir si normalmente le envían un tipo específico de paquetes o Comunicaciones y el dron vuela normalmente Pues si se le envía algún tipo de paquete especial y deja de moverse o se mueve para una dirección en concreto Pues hay algo en esos paquetes que acaban de enviar que son totalmente accesorios que hace que el drone cambie su comportamiento entonces esa sería una un digamos una venida de ataque interesante para investigaciones futuras una analogía en la vida real para poner en contexto el fassing Esta técnica que han utilizado para encontrar estas vulnerabilidades podría pensarse como un edificio con acceso restringido al que solo se puede entrar si se presenta una carta que contenga digamos el sello de la organización dueña del edificio y tenga las palabras acceso permitido sin saber nada de esto Esto es digamos lo sabemos entre entre tú y yo querido oyente pero el investigador o el atacante no lo sabe no un investigador podría pensar en diferentes formas de entrar en el edificio Porque al fin y al cabo no hay infinitas hay se puede un poco asumir y se puede un poco limitar el alcance las posibilidades no y luego indagar y hacer un poco de voy a probar esta funciona no sigo con las siguientes una de ellas sería por ejemplo proporcionar algún tipo de autorización verbal cuando se presente en persona en el edificio es decir diciendo por ejemplo Hola soy Alexis Déjame entrar la contraseña es un dos tres cuatro no funciona Ok Vengo mañana y voy a probar otra me pongo yo que sé me pongo una máscara me pongo para que no me reconozcan la siguiente sería Déjame entrar el presidente me envía y me ha permitido el acceso si no funciona pues puedo venir y decir Déjame entrar soy el dueño del edificio si no puedo probar Déjame entrar y yo trabajo aquí Bueno ya poco veis la idea no que es digamos el protocolo de comunicación entre el control remoto y el dron es el radio el medio aire en este caso un poquito sería también el medio aire Porque sería mi voz que le llega la oreja de la otra persona que está protegiendo el edificio y Bueno un poco Son noticias muy similares con ejemplos similares te iba a decir también que te faltaba el clásico tú no sabes quién soy yo Yo muevo Peña yo conozco gente Tú sabes con quién estás hablando Déjame entrar Sí sí saque con las películas típicas eso funciona siempre pues sí no es también similar a lo que tú mencionabas antes Martín para saber un poquito Cómo Cuál era la dirección Mac en este caso es con el intento más de ver si se puede encontrar alguna vulnerabilidad que en este caso lo identificaban viendo diferencias en el comportamiento Pero bueno espera espero que entendáis la idea y Supongo que sí con lo que he mencionado Martín

en la noticia anterior un poco creo que sea tan Cabos el tema es que sin saber nada un investigador probaría formas convincentes de entrar los protocolos o canales no se limitan solo a la autorización verbal en persona en este caso como he dicho el investigador podría también explorar otros canales otros protocolos como el teléfono el email la mensajería instantánea redes sociales correo postal no Pues digamos que una combinación de todo lo anterior es lo que los investigadores lanzaron contra el dron para esto tuvieron que desarrollar su propio algoritmo su propio framework de fashing para al menos poder comunicarse y hablar con el protocolo que habla el dron que en el caso de la analogía sería al menos saber que el grupo de seguridad que protege el acceso al edificio habla español y por tanto habría que intentar hacer el ataque de fashing en español para poder Acceder al edificio porque si te pones a hablar chino a los que están protegiendo el edificio pues no iban a entender nada y tu ataque no iba a funcionar vamos de ninguna de las maneras de esta forma pudieran determinar ciertos paquetes de datos que al enviarlos al dron causaron que uno estos fallaran y se estrellaran o que dos realizaran cambios en los datos del dron como el número de serie esto último lo pudieron verificar emparejando el dron con un teléfono móvil que ejecutaba la aplicación de DJ Y revisando periódicamente la aplicación para ver si el fashing Estaba cambiando la información del dron se encontró que los cuatro modelos probados tenían vulnerabilidades de seguridad en total Los investigadores documentaron 16 vulnerabilidades cuatro de ellas eran muy graves Por una parte estos errores permitieron que los investigadores pudieran modificar los datos de Registro o el número de serie y falsificar su identidad esto podría hacerse para que no les pillaran O también para incriminar a alguien que no es vamos un ataque que podríamos llamarle dron swatting por otra parte esta es unidades también pueden permitir la desactivación de los mecanismos de los drones dji que no les permiten Volar Sobre aeropuertos u otras áreas restringidas como prisiones y bueno sitios restringidos Como mar halago y similares finalmente Los investigadores examinaron el protocolo utilizado por los drones dge para transmitir la ubicación del dron y su piloto mediante la ingeniería inversa en este caso del firmware de DJ y las señales de radio emitidas por los drones pudieron documentar por primera vez el protocolo de seguimiento de DJ llamado drone ID y demostraron que los datos transmitidos no están cifrados y que cualquier persona puede leer la ubicación del piloto y del dron con métodos relativamente simples esta investigación demuestra que dji estaba mintiendo Cuando decía que no no estas comunicaciones entre drones y controladores el control remoto están cifradas y nadie puede ver lo que se intercambia pues no los investigadores mostraron que es digamos en formato Jason no un formato Así que se utiliza sobre todo en comunicaciones web y que ahí se enviaba la ubicación GPS latitud y longitud en cualquier caso porque querría Dj no cifrar estas comunicaciones se dice que es porque Dj permite a las fuerzas del orden identificar información relevante de cualquier drone Dj para actuar en caso de que se esté infringiendo algún tipo de ley con el dron es decir si un dron se está volando por una zona no autorizada digamos una ciudad como Nueva York en la que es casi el 99% de Nueva York no se puede volar drones pues las fuerzas del orden quieren saber quién es el dueño que opera el dron para multarlo o incluso si tienen que hacer algo de forma inminente identificar la posición exacta del operador y actuar y cómo pueden conseguir las fuerzas del orden esta información pues de varias formas no una sería que Dj las proporciones hay formación Porque al fin y al cabo estos drones también están Dj está recatando la información de todos los usuarios de dji la segunda sino sería que las fuerzas del orden intercepten las comunicaciones radio y extraigan esta información del protocolo entre el dron y el controlador remoto y por eso las comunicaciones deberían mantenerse sin cifrado Total que con todo esto os traigo un escenario de ataque interesante imaginaos tenéis un vecino que grita y hace mucho ruido por las noches y no deja dormir sabéis que tiene un

dron DJ un día lo seguís A dónde está volando y gracias a esta investigación de estos investigadores de la universidad alemana sabéis que podéis interceptar las comunicaciones entre el dron y el controlador y capturas el número de serie de su dron y su ID de cuenta de DJ luego os compráis un drone DJ y gracias a esta investigación desactiváis los mecanismos que no le permiten Volar Sobre áreas restringidas a tu dron paso siguiente y Gracias también a esta investigación cambiáis el número de serie de tu dron por el dron del de vuestro vecino finalmente vuestro drone en algún sitio no autorizado y listo multa o denuncias mayores para vuestro vecino ya podéis dormir tranquilo porque ya podéis dormir tranquilos se lo metéis en las gracias pero no si por ejemplo lo vuelas por un aeropuerto que eso es hiper restringido madre mía le puede caer el pelo porque es lo que dices tú es un ataque de falsa bandera no de falsa bandera eso es justo muy buena palabra que no me acordaba Sí porque es que este este os traigo esta noticia que ahora voy a acabar de comentarla por el tema de que los rusos podían identificar dónde estaban los soldados ucranianos pero también se puede utilizar ahora que está publicada para fines más swatting no de falsa bandera y para marear la perdición con Estos tipos de drones cuando tú te registras porque hay muchos tendrán una aplicación una app no para el móvil o así cuando tú te registras utilizas estaría Guay poder A ver es que se me acaba se me acaba de ir pero estaba pensando en en poder acceder a la cuenta de otra persona utilizando para registrarte el número de usuario o sea el número de serie del dron de esa persona que puedes obtener como tú explicaste pero claro no sé si va así la vaina un Idol no de esos sí un Idol o yo que sé a la hora de registrarte en la app de la manera que en la que te asocias con el dron es a través del número de serie eso no lo han comentado Pero oye investigación para tierra de hackers Pues a ver Esto es un caso de humor no como lo he presentado aquí un poquito para que podáis dormir bien dormir bien pero un caso más real y drástico como decía sería aplicarlo al campo de batalla como los ucranianos ahora saben que los rusos saben interceptar las comunicaciones entre los drones y sus controladores los controles remotos y que estas comunicaciones incluyen la ubicación de ambos podría modificar estas comunicaciones para falsificar la localización del piloto ucraniano y hacerlo aparecer en el mapa ubicarlo en una base rusa y de esta forma cuando los rusos intercepten la ubicación del piloto ucraniano y el dron y lo vayan a bombardear estarían atacando a sus propios soldados esto es como lo del doble agente no en Los espías Aunque bueno Supongo que ahora que esta investigación es pública los rusos no van a confiar más en las comunicaciones de los drones dji con sus controladores remotos para determinar la ubicación de los pilotos no pero bueno Los investigadores dicen que no se van a quedar aquí y que tienen la intención de probar también la seguridad de otros modelos de drones los investigadores informaron a Dj de las 16 vulnerabilidades detectadas antes de divulgar la información al público y Dj dijo que ya ha solucionado todos los problemas y bueno Supongo que ha publicado nuevas versiones de firmware para cada uno de los cuatro modelos afectados esta investigación fue presentada en la conferencia de seguridad en redes y sistemas distribuidos en edss que tuvo lugar hace muy poco entre el 27 de febrero y el 3 de marzo en San Diego en Estados Unidos vamos a Añadir un enlace al paper que publicaron en las notas del episodio por si lo queréis leer antes de ir a dormir y también el enlace a su repositorio de github con las herramientas que desarrollaron y otras herramientas que utilizaron en esta investigación solo un inciso de esta conferencia decir que está llena de papers cuando cuando lo vi este paper vi que habían un montón más y son algunos son muy interesantes también excelentes hay otro por ejemplo relacionado con drones en el que los investigadores publicaron una técnica que paraliza instantáneamente drones Dj emitiendo Una señal electromagnética desde una raspberry Pay la novedad de Esta técnica comparada con un ataque de pulso electromagnético ya conocido es que el pulso afecta a una gran cantidad de frecuencias no y te pueden afectar a

tu móvil a tu portátil a tu coche incluso tu vehículo a tu tesla que si lo estás conduciendo o bueno no hace falta que sea un tesla cualquier cualquier vehículo últimamente tiene está lleno de electrónica y el pulso electromagnético necesita mucha potencia en cambio este ataque se enfoca solo en las frecuencias específicas utilizadas por los chips o el sistema de posicionamiento que lleva dentro del dron lo cual permite emitir una señal con mucho con mucha menos potencia y evitar daños colaterales y por eso es una técnica muy precisa Así que os animo a que echéis un ojo a todos estos papers ya que igual algunos interesan no sé en el campo en el que estáis trabajando voy a Añadir un enlace a la página de los papers de la conferencia en las notas del episodio y bueno como mínimo 50 papers así que bueno tenéis un buen rato para entretenernos quería un poquito cerrar ya la noticia con Cómo consiguieron los rusos esta capacidad de interceptación de comunicaciones Pues de alguna forma han sabido esto desde los inicios de la guerra y podría ser pues por varios motivos no Uno es que tengan analistas que puedan identificar las mismas vulnerabilidades que descubrieron los académicos alemanes Rusia tiene mucha experiencia en el campo de las comunicaciones radio y señales electromagnéticas y siempre he tenido fama de tener muchos muchos científicos inteligentes no así que bueno en es que muchas veces se les colecciona para trabajar a favor del gobierno Pero bueno tienen tienen talento y la segunda es que Dj a él les haya dicho cómo hacer esto ya que las relaciones entre Rusia y China son un poco más favorables que desfavorables no y bueno cerrando quiero Resaltar un poco la mentalidad hacker esta de los soldados ucranianos de cómo han podido utilizar algo digamos barato como un dron dji que está al alcance de cualquier persona para convertirlo en un arma que se ha podido utilizar durante la Guerra eso es bastante creatividad que han tenido estos soldados y relacionado con esto queridos oyentes llegamos a la pregunta del episodio siguiendo esta línea de mentalidad hacker de estos soldados ucranianos de lo que han hecho con los drones dji Qué otros dispositivos electrónicos comerciales creéis que podrían ser los siguientes que se pudieran reutilizar para convertirlos en armas y os damos cuatro opciones la primera son los coches autónomos tipo tesla o bueno hay muchos Incluso se podría hacer algo como esta persona el geohoot no sé si lo conocéis el primero que hizo un and lock del iPhone y que luego hackeó la PlayStation 3 tiene ahora una empresa que se llama coma y que vende el digamos el cerebro que hace que un coche se pueda conducir solo así que no hace falta comprarse un vehículo de 30.000 dólares geohood vende este cerebro por unos 1200 dólares y luego una lo tienes que instalar en tu vehículo y Oye podrías tener un tanque podrías meterle armas ahí bombas y teledirigido y autónomo luego tendríamos los Globos aerostáticos como el chino que como te prometo Martín en la noticia anterior también os queríamos traer porque estamos comentando tierra también tendríamos los submarinos teledirigidos submarinos lanchas Pero hay hay yo de por ejemplo de pequeño tuve submarinos teledirigidos a poca distancia no pero seguro que se pueden comprar baratos y que lleguen a bastante distancia para que no se puedan ver y luego suban a la superficie y disparen algo o que justo se detona la bomba cuando llegue a su destino y lo último son robots móviles un poco se me con Martín antes hablando la noticia esta que los dispositivos que podíamos mencionar se me ocurre últimamente no si lo habéis visto pero sobre todo por ejemplo en Barcelona he visto bastantes que bueno como soy de ahí voy visitando la familia de tanto en cuando no y también a Martín y en algunos restaurantes asiáticos tienen estos robots nuevos que son que te traen la comida y tal No pues bueno se nos podría ocurrir la idea de que reutilizaran estos robots para en lugar de traerte la sopa de fideos te traiga una bomba que explota en la cara no bueno Incluso en conferencias no un montón que te vienen a decir hola sobre todas las conferencias había varios o si no el propio de porque tú hacías énfasis en lo de comerciales No él aún no está pero el de tesla este bueno el de tesla El de elon más que el que anunció el robot este humanoide no me sale ahora el nombre que

tiene el nombre de un robot de peli de este se me ha escapado megatrón o bueno no me acuerdo pues sí creo que se llama así sí creo que sí sí pues Pues ese es un robot eh humanoide En el sentido que tiene dos patas y van dando así también te podría traer de regalito una una historia Pues sí muy interesante yo quería completar completar no complementar tu noticia Pues precisamente la roote fue una charla súper guapa de David Meléndez sobre sobre drones y en ese que va muy acorde con esta noticia él mostraba un sistema antillaming para drones implementando sus propios protocolos a través de software radio de radiofrecuencia pero metiéndole un dispositivo sdr al dron y manejando la Sí la verdad la chala súper guapa aparte es súper simpático a él os la recomiendo se llama Supongo que era la ruta cara publicando las charlas Pues tú no tienes poder aquí sáltate los sistemas anti drone con sdr me gustó mucho porque el tío mostraba como iba en el espectro en diferentes frecuencias mostrando que la señal se transmitía igualmente entonces los sistemas antillamin Pues bueno intentan sabes una parte del espectro intentar meter ruido en la señal pero claro Aquí estaba por todos lados entonces la verdad estaba estaba muy guapo como sistema anti drone antijamin de drones digo en el paper ahora no recuerdo si mencionan una noticia si lo encuentro también algunas medidas de cómo evitar el que están utilizando de hecho activamente la guerra los los ucranianos pero ahora no recuerdo como no era exactamente el meollo de esta noticia pero es no sé no sé cómo me la he apuntado porque me muy interesante Martín lo de la de la charla de David Meléndez has dicho No yo me me preguntaba si es porque sabes cuando incluso has mencionado antes la tuya que se trata de un poquito de propagación de señal porque eso es 10 nanosegundos que te devuelve la señal las señales no van en una dirección única porque las señales electromagnéticas rebotan entonces en algunos casos cuando es como bueno es como una función si no soy de algo Si no cuando puedes tener varias señales que cuando se superponen pues tienen más potencia en ese en ese sitio pero cuando se superponen pero de manera que se contrarrestan una otra pues se anulan no sé si está utilizando un poquito esta tecnología en plan si emito a 10 10 hercios en una señal 1 y yo emito a 10 hercios la señal cero pues se queda en el medio y no afecta nada No sé si podría ser para cancelación desde este tipo pero de hecho es un poco similar a Cómo funcionan los cascos que lleva Opuestos Los cascos estos que son cómo se llaman que no me sale ahora los auriculares Bosé como se llama no No hombre Sonic anti ruido joder ostras macho estoy yo tío nois cancelling No sé eso los Vale pues los auriculares no Descansen en lo que hacen es cuadrar la señal que va entrando para para anularla precisamente un poco Como dices tú es cómo funcionan realmente pues muy interesante A ver si a ver si la vemos Que apliquen igual se la podrían enviar a los ucranianos para un poquito tengan un backup cierto pues bueno queridos oyentes Gracias como siempre por quedaros hasta el final no olvidéis seguirnos en redes sociales como decía Alexis si nos buscáis como tierra de hackers darle darle a esas reviews dejarnos comentarios que nos ayuda un montón y nada recordad que estamos aquí semanalmente aunque esta semana ha sido con un poco de retraso y que apreciamos un montón que estáis aquí con nosotros que cada día somos más Muchas gracias a todos por escucharnos y nada que sigan las buenas vibraciones de esas ondas electromagnéticas y Sonoras que se puede que sigáis propagando vuestro karma a través de a través del éter del buen rollito nos vemos y nos escuchamos en el siguiente Adiós adiós 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 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