72. WiFi drones y SiriSpy

comprometen las redes de una empresa financiera utilizando drones modificados con Hardware especializado para hacking de redes inalámbricas una vulnerabilidad en sistemas operativos de Apple llamadas Siris Pipe permite Escuchar conversaciones capturadas por micrófonos de auriculares Bluetooth de forma legítima y sin levantar sospechas ni dejar rastro alguno celebramos Halloween contando las noticias más terroríficas en el episodio de esta semana de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 31 de octubre de 2022 este es el episodio número 72 yo soy Martín vigo y está conmigo el terrorífico zombie momificado de Alexis porros Hola Alexis qué tal nos falta música de esta de miedo porque me estaban entrando mira que con tanto tantos oyentes en países hispanohablantes A lo mejor lo de Halloween dice pero pero que están haciendo Halloween es Halloween Halloween Halloween como el vídeo ese que corre por WhatsApp Pues sí la verdad que con escalofríos no tanto por Halloween sino por las noticias que traemos Como cada episodio es verdad venimos a meteros miedo con las noticias que os traemos O sea no lo había pensado Claro claro que justo ahí te ha salido un pareado podría ser el próximo el el Cómo se dice el Moto este el eslogan de Spider episodios especiales como este de terror Yo es que tengo mucho Flow yo debería ser rapero si no fuera por la voz Pues nada aquí contigo Martín otro episodio más y nada como siempre dar las gracias a todos vosotros nuestros oyentes por el seguimiento que nos hacéis en redes sociales donde nos comentáis nos enviáis vuestras sugerencias preguntas respuestas bueno y nos estamos ahí con una comunicación abierta como se diría no os recordamos que deberías estar suscritos a nuestro podcast en vuestra plataforma de escucha favorita si aún no lo estáis estamos en todas las conocidas y por haber creo yo y en redes sociales Pues también estamos en la gran mayoría Twitter que está muy de moda últimamente verdad pero no voy a entrar en detalles Instagram Facebook no te vayas por las ramas que no nos va el episodio otra vez a dos horas Sí sí pues en esas tres con el handel arroba tierra de hackers linking YouTube y Twitch como tierra de hackers correos electrónicos no los podéis enviar a podcast@ tierra de hackers.com y tenemos un servidor de discord en tierra de hackers puntocom barra discord ahí podéis Acceder al servidor y a los canales que tenemos muy majos Y como siempre agradecer vuestro apoyo a la pregunta del episodio que publicamos en Twitter después cada episodio y la última fue la siguiente Qué medidas aplicas para protegerte de este tipo de ataques de bring you Driver O trae tu propio controlador vulnerable si no os acordáis de esta noticia pues ya ya sabéis ir al episodio anterior Pero tenemos teníamos cuatro respuestas la más votada con un 40% pues uso antivirus o en Point detection en response o bueno estos sistemas de seguridad para protegerme la segunda con 36% uso capas de seguridad con un 15% tenemos Pues nada me fío de Microsoft y un 9% la última es nada no me afecta Así que esas fueron las votaciones pues muy interesante como siempre yo en mi caso eh paso a agradecer a toda la gente que nos apoya en el podcast Empezando por nuestros queridos patreons Muchísimas gracias a todos y tenemos a uno nuevo Luis garijo que se ha unido a la gente que nos apoyan patreon patreon.com/tierra de hackers como decimos siempre es esencial Así que muchísimas gracias por por apoyarnos ahí y también a nuestros sponsor de este episodio monad 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 mónate a través de una herramienta de gestión y visualización de telemetría y datos de seguridad una empresa fundada en

silicon Valley que está buscando muchos ingenieros sobre todo con algo de experiencia y seguridad para ayudarles a construir y hacer realidad su misión lo mejor de todos que están contratando en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web monad.com y contactarles en tierra de hackers@monal.com para que sepan que venís de nuestra de nuestra parte y con esto ya pues estamos listos para empezar hoy os Traigo una de esas noticias fantasía no un hack Por así decirlo que suena a ciencia ficción pero que en ocasiones hemos comentado que sería muy posible y por eso me encanta cuando Tenemos la oportunidad de cubrir una noticia como esta que muestra un caso de uso real que esto realmente ha sucedido no es solo una historia o una posibilidad un estudio académico una demo no no no se ha utilizado para robar hace un par de semanas se publicó una noticia hablando del ataque sufrido por una entidad financiera ataque en que los delincuentes consiguieron acceder a las redes internas de dicha empresa remotamente y comprometer varios servicios expuestos solo internamente en la red interna La pregunta es y lo interesante es cómo lo hicieron pues utilizando drones modificados y equipados con Hardware especialmente diseñado para comprometer redes wi-fi A qué Mola el ataque lo sufrió como decía una empresa dedicada a las inversiones financieras en Estados Unidos y nos hemos enterado de ello gracias a Greg Linares un investigador que publicó recientemente un hilo un hilo en Twitter con los detalles de este ataque y que me encontré y me lo guardé para para estudiarlo y traeroslo aquí al podcast por temas de acuerdos de confidencialidad De hecho no pudo entrar en todos los detalles pero buscando también porque Bueno yo no conocía hasta este investigador en particular he visto que otros medios de comunicación cubrieron la noticia también y corroboraron lo que decía es decir la historia que contaba con otras fuentes por tanto Pues bueno digamos que un poco hice los deberes ahí y y por pintada a que pues efectivamente la historia real os dejo por supuesto los enlaces tanto al hilo de Twitter como a los artículos bueno todo empezó cuando el equipo de respuesta de incidentes de la empresa en cuestión detectó actividad inusual en una instancia interna de confluentes si os acordáis que complace lo sacamos aquí constantemente es un software muy parecido a la Wikipedia que las empresas utilizan pues para escribir y revisar documentación de proyectos manuales etcétera lo dicho como una Wikipedia de cosas de empresas Pues bien el equipo de respuesta de incidentes ante esta actividad sospechosa decidió aislar el servidor donde estaba alojado confluentes es decir donde lo tenían instalado para toda la empresa y empezar una investigación a ver que estaba pasando no una de las primeras cosas que se dieron cuenta y que confirmaba aún más sus sospechas Es que la dirección Mac desde la cual se accedió a la WiFi de la empresa correspondía a un empleado que estaba conectado desde su casa al mismo tiempo la dirección Mac para menos técnicos es un identificador único para la tarjeta de red que llevan todos los ordenadores por tanto esto quiere decir que este empleado estaba teóricamente conectado desde dos sitios a la vez con el mismo dispositivo lo cual evidentemente es imposible tú no puedes estar conectado desde tu casa con el ordenador y a la vez desde la oficina Así que con esto en mente el equipo de investigación utilizó dispositivos especializados para localizar desde dónde venía la señal WiFi del dispositivo conectado a la red de la oficina que era donde estaban evidentemente estos dispositivos permiten encontrar puntos de acceso y otro tipo de dispositivos emitiendo un sonido más agudo Según uno se va acercando al dispositivo ya que la potencia de la señal aumentará Y es un poco lo que utiliza como indicio no esto es parecido al típico detector de metales de esto que ves a varias veces gente por la playa utilizar no y Cuanto más te acercas al metal Pues se ve hace más agudo el sonido para ver exactamente dónde está Pues lo mismo Pues nada el equipo de

investigación siguiendo el pitido de la señal y van andando andando Y a dónde creéis que les llevó pues al tejado del edificio y fue ahí donde encontraron dos drones en el suelo una de la marca Dj modelo Matrix 600 y otro Dj también pero este del modelo Phantom por lo que comentan no es que se hubieran estrellados sino que los aterrizaron allí a propósitos o sea los granos los drones volaron hasta el tejado y aterrizaron uno de los drones sí que lo encontraron como medio metido en un conducto del aire y a pesar de que no estaba dañado como decía porque lo tercero sí que parecía que tenía como había tenido como un brusco aterrizaje algo y y luego voy a comentar el por qué pero bueno qué tenían de especial estos dos drones no porque hasta aquí pues bueno te has encontrado dos drones en el tejado hay unas señales wi-fi raras bueno Pues el Phantom cargaba un dispositivo muy conocido para todo hacker que es una WiFi pine Apple la WiFi Apple es un dispositivo especializado para comprometer redes wi-fi que la verdad lo puede comprar cualquiera online y Vale pues unos 200 euros para que te hagas una idea es un dispositivo que permite no solo comprometer este tipo de redes inalámbricas sino también automatizar los ataques yo De hecho tengo una WiFi Apple que me tocó este verano mientras Alexis y yo estábamos en defcock en un evento y la verdad es que está muy guapo te acuerdas no Alexis que fuimos ahí a un happy hour no solo nos tomamos nuestros copazos si lo compro encima me llevé una wifipainable puede llegar hackear coger las botellas y la WiFi pineapple y llevarnoslo así da gusto es lo guapo de ir a deff contigo 100% recomendado para el año para que todos nuestros oyentes se vayan También muchas piezas mucha oportunidad de ganar cosas Bueno pues ya digo que esto de la WiFi Apple es el Gadget por excelencia de los hackers no y se utiliza mucho en el ámbito profesional y sobre todo por parte de red teams que son los encargados Pues digamos de la parte del ataque todavía más curioso son las modificaciones que hicieron en el otro dron acordaos había dos en el Matrix 600 este llevaba como carga una raspberry Pay varias baterías un mini portátil modelo gpd un módem 4G y otra tarjeta WiFi vamos todo el equipo necesario para conectarse a la WiFi de la empresa y puentear la conexión a cualquier zona del planeta mediante la conexión del módem 4G a ver qué explico esto un poco más porque la verdad es la leche el raspberry este le habían colgado Por así decirlo al dron le habían pegado pues lo que decía una raspberry pike una raspberry pues es un ordenador muy muy muy muy muy muy pequeñito y muy barato por Bueno ahora está caro porque los problemas que hay en el mundo para para enviar cosas desde china pero en general te lo puedes comprar por 35 dólares imagínate Pues el ordenador que tú tienes en casa pues con menos potencia menos capacidad computacional pero que aún así puede hacer muchísimas cosas tamaño de un poco más de una tarjeta de crédito y evidentemente pues un poco más gordito pero pero para que os hagáis una idea varias baterías ya que este este ordenador que es un ordenador al fin al cabo se puede alimentar de baterías USB como con la que cargas tú teléfono móvil un mini portátil modelo gpd yo esto no lo conocía muchos de los oyentes se acordarán de los netbooks no que se hicieron tan populares a principios de los años 2000 Yo creo por ahí que era Cuando yo estudiaba y eran estos portátiles súper pequeñitos yo la verdad nunca lo entendí porque son muy incómodos pero yo tenía varios compañeros de clase que los tenían pues parece ser que como que medio se han vuelto a poner de moda y hay uno que está súper bien hecho y de hecho tiene una campaña en índigo que es así como como kickstarter que es este mismo yo no lo conocía Y la verdad las capacidades de este mini portátil son bastante sorprendentes porque me estuve viendo un vídeo de un Unboxing y explicaban todo y está muy Guay también os digo vale 2000 euros y ya os digo que es un mini portátil que es muy capaz pero evidentemente tú te compras también un portátil normal de 2.000 euros y es 10 veces mejor pues bueno habían metido

este portátil lo habían colgado del dron también evidentemente para hacer No solo necesitas el Hardware especializa para hackear wifis sino que luego también Pues necesitas digamos un portátil es esa parte del ordenador donde tú pues corres tus aplicaciones y haces digamos todo un poco la gestión la logística los programas se Ejecutan necesitas Digamos como esa pieza central no luego tenía un módem 4G como decía que esto lo que te da es conexión a internet mediante telefonía móvil y otra tarjeta wi-fi esto lo que está diciendo es que con una de las tarjetas WiFi se conectaba a la red de la empresa el mini portátil y la raspberry Pipe pues servía para hacer toda la gestión de puentear esa conexión y mandaba la conexión todo el tráfico a través de 4G al atacante o dicho desde el otro lado desde el punto de vista del atacante el atacante se conectaba al ordenador que estaba en el dron mediante 4G y luego a la empresa mediante la tarjeta WiFi vamos una pasada Espero no haberos liado más pero pero para que os hagáis una idea y la pregunta que tenemos ahora es por qué utilizaron dos drones con dos configuraciones tan diferentes por los investigadores llegaron a la conclusión de que días antes el dron equipado con la WiFi pine Apple había sido utilizado para robar los credenciales de acceso a la red wi-fi de la empresa de uno de los empleados es decir primero enviar un drone con el equipo necesario para robar la contraseña de acceso a la red interna es decir a la WiFi de la propia empresa utilizando los credenciales de uno de los empleados la WiFi Apple precisamente te permite hacer este tipo de ataques que pueden hacerse de varias maneras dependiendo de la seguridad y configuración de la red inalámbrica de la empresa por daros un ejemplo pues uno de los ataques que se puede hacer es simplemente crear un punto de acceso o una red WiFi igual a la de la empresa con el mismo nombre por ejemplo y esperar a que algún empleado se conecte a tu red en vez de la de la empresa de hecho esto lo que puedes hacer es también un ataque de de autenticación un día os Attack que lo que hace es hacer que desconecte a todo el mundo que está conectado a la red WiFi de la empresa para luego que tenga que volver a conectarse y con suerte alguno Escoge tu punto de acceso tu red WiFi que tiene el mismo nombre que el de la empresa y si es así pues claro acaba poniendo los credenciales y se lo puedes robar esto ya digo que es simplificando un poco el ataque y no dan detalles de cuál fue el ataque Exacto que se llevó a cabo pero es que es para que os hagáis más o menos una idea y por qué saben que primero se envió al dron con la WiFi pine Apple para robar los credenciales porque una cosa es que tendría lógica pero es quien lo sabían porque el segundo drone contenía los credenciales robados por la WiFi pine Apple harcodeado es decir escrito en las propias herramientas que llevaba instalada la raspberry del dron la verdad es que una pasada Primero te envío un drone para robar credenciales y luego te envío un segundo drone para conectarme con esos credenciales que he robado con el primer dron y crear un puente aéreo literal de esa conexión a través de la red 4G a cualquier punto del mundo me quito el sombrero comentan que el ataque no llegó a ser tan exitoso o exitoso del todo porque lo detectaron como decían cuando vieron actividad sospechosa en confluentes es decir si comprometieron la red inalámbrica pero una vez dentro de la red bueno tienes que hacer algo no intentar un ir a por esto de confluentes porque sospechan que en confluentes como ya digo es una wiki contenía muchísimas contraseñas entonces querían acceder a eso entonces yo estos especulación mía seguramente estaban intentando hacer scripting de todo confluenso analizar todas las páginas procesarlas lo cual un humano pues no podría estar mirando tantas páginas por segundo para así decirlo esto es especulación mía pero yo creo que es a lo que se refieren con actividad sospechosa de hecho comentan que la razón por la que el segundo lo encontraron tan cerca del conducto del aire medio estrellado había sido porque los atacantes intentaron huir es decir sacar el dron del tejado

demasiado rápido y lo estrellaron que por cierto Me parece muy guapo como concepto de eliminar pruebas chavas con tu dron a ver toda la movida ostras que me han pillado Wow Me piro y buena suerte encontrando el origen de la brecha de seguridad porque llegarían allí Oye alguien se está conectando desde el tejado pero aquí no hay nada bueno el investigador menciona que que el Hardware utilizado para este ataque todo lo que decía los dos drones el Hardware especializado y todo esto asciende a unos 15 mil dólares yo que la mayoría del precio evidentemente es en los drones porque a pesar de que hay drones muy baratos recordemos que todo este equipo que llevaba anclado pesa y por tanto necesitas drones más grandes y potentes y profesionales la verdad es que es bastante dinero aunque se podría realmente hacer más barato lo más interesante lo más interesante de este dato es que en mi opinión el atacan un atacante del montón Por así decirlo no se gasta 15.000 euros en atacar una empresa porque no los tiene para empezar y menos con un ataque en el que quizá ni puede recuperar el Hardware porque dices Bueno me gasto 15.000 euros pero luego recupero el dron y recupero todo además es bastante sofisticado y no está ni garantizado que pueda romper la seguridad de una WiFi ya que hoy en día pues es bastante más complicado no es como de aquella cuando todo el mundo le robaba la wifi al vecino porque estaba cifrada con web y ya está recordemos también que hablamos de una una red empresarial no corporativa no una red de una casa me da a mí que los responsables de este ataque no son unos cualquiera quizás espionaje Industrial entre empresas financieras o alguien que sabía que podía robar dinero Si accedía a la red interna esto ya son especulaciones mías de hecho el propio investigador especula que tal como se llevó a cabo el ataque Está seguro que los delincuentes tenían mucho conocimiento previo sabían cómo estaba configurada la red inalámbrica para saber cómo atacarla las debilidades la existencia de confluentes etcétera Así que quizá esté un empleado detrás de todo esto o los pagaron algún empleado para facilitar parte de la complejidad de esta instrucción intrusión no lo sabemos pero bueno sí que parece que había mucho conocimiento previo en cualquier caso tenemos un auténtico caso de uso real que a partir de ahora podemos referenciar Cuando hablemos de este tipo de ataques que suenan un tanto hollywoodienses de hecho en el propio íleo de Twitter que iba leyendo los debates pues hablaban de como había hace años algunos penetration testers y tal que trabajaban para empresas Pues sugerían que había que hacer también fases de reconocimiento en zonas que podía haber acceso de drones y cosas así y que Bueno un poco por las empresas le decían A dónde vas chaval y que y que estaba contento de que por fin había un caso que podía referenciar no evidentemente sigue siendo un ataque sofisticado un ataque que no va a ser común del todo incluso a veces pues desde puedes desde el parking hacer esto sin necesitar un drone Pero bueno está bien que tener un caso ahora para poder justificar un poco más medidas no de protección de hecho diré que esto no es nuevo este tipo de ataque como siempre primero viene la parte teórica académica en la que se Proponen estos ataques no luego son los investigadores los que muestran las pruebas de concepto en conferencias y luego suelen pasar años hasta que vemos casos de uso real no Y en este caso ya hubo charlas sobre estos mismos ataques en Black no con demos por ejemplo como de nuestro querido Sami campcar que hackeaba un dron utilizando otro drone es decir en uno de los drones también ponía el Hardware necesario se acercaba a otro drone que al fin y al cabo funciona por WiFi también y lo que hacía era interceptar las señales y obligarle a dar piruetas en el aire la verdad es que la demo está muy guapa y tenéis el vídeo en YouTube pero incluso hay vídeos de demos con ataques con drones con propuestas diferentes al de este caso uno que me encontréis de una famosa investigadora china sexy Cyborg que a lo mejor muchos la conocéis en

El que uso un dron para llevar un implante físico a un tejado de un edificio solo que en este caso el dron se utiliza solo como medio de transporte para dejarlo en el tejado no está atado al propio drone obligando al dron a quedarse en el tejado Así que esto es como si utilizas el dron sueltas allí tu raspberry con tu todo y te pidas y así por lo menos por recuperes el drone como siempre os dejo el vídeo a esta demo que me apareció súper chula en las notas del episodio y también de cómo lo construyo y para termina la noticia Pues yo creo que esto es perfecto para una pregunta para para nuestro episodio yo os pregunto temes ataques hollywoodienses con drones contra la red WiFi de tu casa o empresa y os damos cuatro opciones sí por el abaratamiento del Hardware cada vez los drones son más baratos la wi-fi en Apple raspberry Pines todo esto a pesar de que quise gastaron 15.000 euros se puede hacer más barato la segunda opción Sí porque es de fácil automatización es decir hoy en día existen muchas herramientas o Open source gratuitas que facilitan el automatizar este tipo de ataques por tanto pues no solo es un tema de Hardware barato sino que es fácil de implementar o a lo mejor como tercera opción no te preocupa porque todavía es caro Es verdad que a pesar de que sea barata el hardware no es algo tampoco que ahora vaya aquí todo el mundo con drones por todos lados a todas las wifis o a lo mejor pues no te preocupa porque sigue siendo un ataque pues sofisticado no estar alcance de cualquier vecino que quiere fastidiarte no así que ahí tenéis las cuatro opciones contestarlas en Twitter arroba tierra de hackers sí que me da escalofríos ves yo yo tenía razón al principio que nos iba a dar escalofríos este episodio yo me preguntaba cuando detectaron el ataque como decías enviaron un drone primero para intentar capturar las credenciales de la WiFi de alguien haciendo en plan tipo ingeniería social y luego enviaron el otro digo en tema de seguridad operacional Podrían haber enviado solo uno y hacerlo todo desde uno pero bueno decidieron hacerlo así pues también fue interesante lo que decía es que la verdad es que los cacharros Estos son son bastante caros pero siendo una empresa financiera igual el beneficio que iban a obtener al sacar credenciales o futuras de empresas e invertir en bolsa hubiera sido mucho el beneficio Entonces no sé igual dices 15.000 Comparado con dos millones de dólares Tampoco es tanto no Claro es que tú imagínate no sé Solo sé que era una empresa financiera porque no dieron el nombre por lo que insisto era temas de confidencialidad Pero tú Imagínate los algoritmos de inversión automática todos estos Bots de trading que hacen operaciones en milisegundos y que ya hemos cubierto aquí si tú puedes robar esa propiedad intelectual ya no son dos millones o sea te da para empezar una ventaja competitiva respecto a tus rivales o simplemente pues el acceso a utilizar tú esos algoritmos entonces claro el retorno de inversión es brutal no todo el mundo tiene 15.000 euros por eso no creo que aunque se te ocurriese a ti o a mí o a cualquier así no digamos lo puede llevar a cabo pero vamos el retorno de inversión es importante entonces es por donde yo creo eso lo que eso el empleado un empleado supiese que Oye si tú accedes a la red interna vas por aquí por allá y tienen las bases de datos de transacciones financieras aquí y allí y te puedes empezar a transferir dinero que aquí no se entera nadie Oye pues hazlo desde el tejado y tal y cual o a saber un insider Fred pero desde desde el tejado Está buena Sí luego también pensaba Digo tanto montaje igual se hubiera podido haber hecho con un dron solo y te ahorras ahí un poquito de dinero luego el tema de la no sé implementar todo en una raspberry pinet en lugar de tener que meter el ordenador ese de 2000 pavos ahí adicional y me pareció curioso el tema de la 3g porque ahí dejas rastros no digo igual si hay algún algún hotelito por ahí cerca con visión directa Pues nada Oye te quedas ahí y te recibes la conexión WiFi directamente desde desde el dron que has deja claro el tema el tema o sea sí sobre el papel se podría hacer de otras maneras pero yo diría por ejemplo lo de conectarte desde un hotel si estás

en un tejado y tiene temas elevados pues probablemente la cobertura no sea tan buena Yo ahí sí que entiendo el 4g aparte que te permite no tener que estar tan cerca de ahí no puedes una vez el drone porque ten en cuenta que por qué no no llevaron el dron y lo sacaron así porque a lo mejor no querían estar mucho cerca Porque para el dron para volar el dron Pues necesitas cierta cercanía Aunque Bueno tengo entendido que estos van kilómetros O sea que no hay ningún problema en llevarlo hasta el tejado Pero eso por un lado luego lo que dices de los dos drones vale Sí que podían ir robar la contraseña de del tal y Pero entonces tendrías que automatizar una vez la tienes meterla en las herramientas de tal es mucho más fácil el Oye En cuanto la tengas tranvías y ya configuramos con calma todo lo que tengamos que configurar y lo metemos en un nuevo en un nuevo drone no porque claro eso es más fácil aparte ten en cuenta que el dron tiene que estar allí aparcado a lo mejor Estuvo una semana es que no lo sabemos porque tiene que esperar claro hasta que alguien caiga en la trampa para darle los credenciales de hecho ahora que dices eso el Phantom este que lleva la pine Apple solo como como se enviaron las contraseñas las credenciales porque no tiene no dicen que tiene módulo de celular eso es verdad Pero creo que te permite igual Estaban cerca eso o a lo mejor pues venía para conectarse a la WiFi real y utilizó la propia WiFi solo para enviar los credenciales a casa es como lo haría yo no si quieres ahorrarte la parte de 4G y tú estás esperando a robar los credenciales de la propia WiFi una vez lo robas pues no es muy complicado automatizar El conectarte a la WiFi real cuando tienes los credenciales otra cosa es automatizar todos los ataques de que si de confluencia y todo esto no eso es complicado pero ostras yo sé que esta es la WiFi que voy a pretender ser y de la WiFi que voy a desconectar a la gente en cuanto consiga los credenciales Conéctate a esa WiFi real y los envías a eso no lo veo muy complicado o a lo mejor incluso No lo sé Pero puede que hubiese wifis allí abiertas y le utilizasen esas para enviar los credenciales de vuelta ya yo yo personalmente lo hubiera hecho con un dron solo porque todo el cacharreo que tienen ahí montado en dos drones para Pero bueno para ahorrarse o luego a lo mejor también también es un tema de peso porque meterle la WiFi pero yo insisto llevas la WiFi pine Apple que ya te viene out of the Box para hacer todo tipo de ataques no entonces tendrías que meterle todo lo demás Y de alguna manera pasar de la WiFi pine Apple a ver que sí que puedes montarte una ramsberry pi en la WiFi No te compliques cuando puedes comprar algo algo ya está no entonces tendrías que pasar de la WiFi en Apple y los credenciales pero aparte tener todas las herramientas configuradas de manera que coge esa variable de Los credenciales ahí y tal Por eso sí os parece sofisticado Pero al final acabo a nivel técnico o sea esto se podría implementar sin productos comerciales como como tú dices podríamos meter una raspberry está en el tema ahí de Claro claro conocimientos técnicos me parece Aunque tiene muchos conocimientos 100% 100% Porque al fin y al cabo esto es una WiFi pine Apple que ya te viene con todo el software y te automatiza todo y luego pues es una raspberry pital que eso es enchufar las cosas juntas y es que una vez tienes la conexión ya estás tú desde tu casa haciendo los sofisticado pero la conseguir esa conexión pues no tiene tanto me refiero a que sofisticado en el tema Pues de los drones de colocarlo siempre pues una WiFi Apple pues Siempre tienes que saber usarla automatizarla y todo eso Pero sí no hablamos de cero de eso es el nivel de complejidad ni muchísimo menos también Ahí está un poco lo bonito no sí y justo lo que he dicho de las redes abiertas WiFi enjustas hace poco vi también un vídeo de unos investigadores de hecho que publicaron en el Canal de esta empresa que vende los las WiFi apples que crearon un aparato similar un artac con un chip de estos sp8266 que vale 5 dólares y tenía bueno Tiene tiene incorpora una conexión WiFi una tarjeta WiFi y le pusieron un módulo de GPS iba capturando por dónde iba

pasando porque lo usaban como rastreador e iba enviando sin módulo celular ni nada eso lo iba enviando en la ubicación a través de dns cuando tenía una red de WiFi abierta cercana que me pareció muy cool la idea para para hacer un rastreador sin que sin que te enteres que te están rastreando Eso sí sí que Mola Sí señor pues y lo último que quería comentar era que dijiste ha salido también la WiFi No la Cómo se llama la WiFi Coconut que tiene 14 tarjetas inalámbricas y te hace todo el temilla de Porque si Solo tienes una WiFi Pues tienes que ir saltando no todos los 14 canales entonces puedes perder paquetes pero esa me pareció interesante de pillarse una así que y trastear con ella sí es como el tío este que va por Def con que tiene el WiFi cactus que se montó una mochila con 14 routers ahí y va esnifando todo lo que se puede descifrar en la conferencia un crack Sí pues está está igual vale 200 dólares y es pequeñita no sea el tamaño de un disco pequeño de esos de vinilo pero pues interesante pasamos a pasamos adelante y queremos hacer un breve inciso para darle las gracias a nuestro patrocinador brawler que nos apoya en el podcast y que hace unos días o unas semanas en este caso Ya acaba de lanzar un servicio en para proteger tu infraestructura en aws hablamos de prowler pro y sus ass el servicio gratuito más completo de seguridad para aws prover Pro está construido sobre la Popular herramienta opensores frawler y además por el mismo equipo de ingenieros si ya conoces frawler que está disponible en github seguro que vas a aprovechar las bondades que ofrece brawler Pro en cuestión de minutos tendrás resultados del estado de seguridad de tu cuenta de aws podrás mejorar tu postura de seguridad a través de múltiples dashboards que te permitirán ahorrar tiempo y tener una visión completa del estado de tu infraestructura puedes empezar a usar brawler pro de forma totalmente gratuita en brawler.pro PR owler.pro desde ya y bueno una vez dicho esto dentro noticia voy a hablar esta de esta noticia que va de un ataque que permite que aplicaciones potencialmente curiosas o no corriendo en sistemas Apple como iphones ipads o Max pueden obtener el audio capturado por micrófonos de auriculares Bluetooth como airpods y bits sin dejar ningún rastro alguno en los dispositivos en la interfaz gráfica es un buen caso creo yo de espionaje de conversaciones de usuarios de dispositivos de Apple siempre ha habido esa polémica no de si las aplicaciones móviles están usando los micrófonos que llevan incorporados en los teléfonos para escuchar lo que sus dueños y usuarios dicen no si este fuera el caso lo podrían utilizar para beneficiarse vendiendo y enseñando anuncios más personalizados o incluso para espiar y atentar contra la seguridad y la privacidad de las personas no sé si os ha pasado que estáis hablando de algo de algún tema con un amigo sacáis el teléfono del bolsillo entráis a una aplicación de una red social o cualquier aplicación que muestra anuncios y van justo un anuncio relacionado con la conversación que estabas teniendo sospechoso No a mí De hecho alguna vez me ha pasado no sé si es tanto por la conversación o por tema de geolocalización pero hasta la fecha no ha habido evidencia de que las aplicaciones abusen del micrófono Aunque sí que abusan de otros indicadores como con la ubicación del GPS la ubicación en base a la dirección IP o los dispositivos Bluetooth que tienes alrededor o incluso las redes wi-fi que tenemos alrededor como comentamos en episodios anteriores por ejemplo hay una base de datos pública que está en Google punto net W y gle.net y ahí Bueno pues la gente va subiendo cuando hacen War driving que es esta actividad de ir por ahí conduciendo o caminando que sería work working con sus tarjetas inalámbricas pues capturan los nombres de las redes inalámbricas que ven por ahí y sus sus direcciones Mac asociadas de los puntos de acceso y la suben a esta a esta base de datos Bueno pues se puede hacer triangulación en función de las direcciones Mac con el nombre de las redes inalámbricas y saber dónde te ubicas no potencialmente incluso aplicaciones podrían abusar de tu historial de

navegación ya que recientemente hemos visto como un investigador publicó que algunas aplicaciones móviles en inyectan código javascript en el navegador web embebido en estas aplicaciones Así que si un usuario si vosotros hacéis clic en enlaces que recibís en esas mismas aplicaciones y lo abrís en el navegador de la propia aplicación pues estas podrían estar capturando toda tu actividad web digo podrían porque algunas lo igual lo han hecho y otras no lo tenían ahí en plan para hacer depuración y bueno eso es lo que dicen que los motivos por lo que tenían todo este javascript inyectado no el desarrollador de aplicaciones para Apple plataformas iOS iPad o es inmacoes que se llama guillerm Rambo público esta semana que había descubierto que cualquier aplicación con acceso a Bluetooth podría grabar tus conversaciones con Siri y el audio de la función de dictado del teléfono de y iPad o es cuando se usan auriculares airpods o bits solo en este caso porque estos son los que tiene una funcionalidad un poquito más avanzada que permite este digamos este ataque o funcionalidad como se quiera ver esto sucede sin que la aplicación solicite permiso de acceso al micrófono y sin que la aplicación deje ningún rastro de que estaba escuchando el micrófono Es más en maco s no solo sucede esto sino que además se puede capturar el audio aunque no se esté utilizando Siri o el dictado y Boom algo que da muchos escalofríos pues quiero comentar brevemente el modelo de seguridad de Apple o en este caso el modelo de sandboxing que es como segmentan aplicaciones y previenen que unas aplicaciones accedan a componentes críticos del sistema o incluso a otras aplicaciones Pues los sistemas operativos de Apple tienen un componente llamado transparencia Con sentimiento y control que es responsable de todas las solicitudes de permiso que se ven cuando una aplicación requiere acceso a tu ubicación micrófono cámara red local calendario y similares estos permisos suelen estar muy estrictamente controlados en las plataformas de Apple a través de la firma digital de código y el uso de derechos por defecto los dispositivos modernos de Apple solo ejecutarán aplicaciones con una firma de código que haya sido aprobada por Apple esto es como tener un edificio con muchas habitaciones o salas y detrás de algunas puertas de estas habitaciones o salas se encuentran los datos del usuario de geolocalización audio del micrófono acceso a la cámara bueno Y también en otras puedes tener las propias aplicaciones no Pues digamos que tienes un policía que sería el componente transparencia Con sentimiento y control que de hecho controla todas las puertas de todas las salas del edificio el edificio sería en este caso el sistema operativo de Apple el símil del modelo de sandboxing que traducción literal es caja de arena no es decir una caja que contiene arena y que está hecha de tal forma de que no se salga nada de esa arena y que no entre nada tampoco en esa caja pues en este caso el símil sería que cada aplicación vive en una sala específica y no puede acceder a otras salas a no ser que el policía se lo permita dejándole salir de su sala y yendo a otras cuando una aplicación en modo sandboxing con bajos privilegios quiere acceder a datos del sistema operativo de Apple el edificio realiza una petición al policía acto seguido el policía primero le pide que se muestre la firma digital de la aplicación que se puede pensar como el equivalente de una identificación emitida por el gobierno donde el gobierno en este caso es Apple Y si el policía puede verificar la firma digital Entonces te pide acto seguido de derechos que tienes que son como se podría ver como licencias no que también han sido verificadas por Apple y pueden dar acceso a las aplicaciones o recursos del sistema a los que normalmente no se pueden acceder y que están protegidos es decir el policía te dejaría entrar a una sala o a varias incluso depende de tus permisos depende de tus derechos o te prohibirá El Paso completamente y de esta forma aplicaciones pueden acceder a datos del sistema operativo o incluso de otras aplicaciones de hecho en el episodio anterior en el que hablé

del ataque de trae tu propio controlador vulnerable o brindinger comenté que Microsoft protege el acceso al kernel de Windows y otros componentes privilegiados de una forma muy similar y solo permite Que corran con controladores o drivers que tengan firmas digitales creadas con certificados emitidos por Microsoft o por delegados en Microsoft y que además estas firmas fueran veri por Microsoft en el caso de trae tu propio controlador vulnerable los atacantes abusan de bueno en habilidades en controladores legítimos mientras que en este caso los atacantes abusaron de una vulnerabilidad en el sistema de transparencia Con sentimiento y control Bueno digo los atacantes en este caso fue el investigador pero se pudiera dar que si hubiera habido ataques relacionados con este ataque digamos lo valga la redundancia pues hubieran sido este caso como se produjeron el investigador que reportó la buena Navidad Guillén Rambo desarrolla la aplicación airbady que facilita la conexión de airpods bits y otros accesorios bluetooth a los Mac obviamente como desarrollador se pasa mucho tiempo trabajando con dispositivos Bluetooth como los airpods que son auriculares Bluetooth durante una de sus sesiones de desarrollo y mientras llevaba puestos los airpods descubrió que podía obtener audio de sus auriculares sin pedir permiso para usar el micrófono en macos esto lo dejo anonadado el investigador intentó Reproducir estos datos que obtenía directamente en una herramienta de audio como audacity Pero llegó a la conclusión de que los datos que recibía no eran datos de audio reproducibles tal cual es decir el vio que recibía un flujo de datos hexadecimales y los pasó digamos a binario y luego los intentó reproducir en herramientas como digo como audacity pero no se escuchaba nada no el audio no era inteligible Entonces se puso a buscar información sobre los componentes del sistema afectado el audio Este que viene vía Bluetooth y vio que el flujo de audio utilizaba una codificación llamada opus que es como decir No sé MP3 ugg que reproductores de audio como audacity no soportan por defecto entonces lo que hizo fue desarrollar una aplicación para capturar el flujo de audio decodificarlo en base al formato opus y de esta forma el audio y hacerlo inteligible y así es como se pudo escuchar a sí mismo hablando con Siri aquí llegó el momento en el que se quedó bastante petrificado por lo que pudo conseguir en este ataque pero no se queda ahí porque sospechaba que esto pudiera afectar a más dispositivos de Apple el siguiente paso entonces que siguió fue verificar las otras plataformas Así que escribió una aplicación que podía ejecutar en iPhone iPad Apple watch y Apple TV y la aprobó en dispositivos que ejecutaban tanto la versión de iOS 15 como la última Beta de iOS 16 en ese momento porque el investigador hizo estos descubrimientos en agosto de este año y es cuando de hecho lo reportó también a apple la aplicación que creó hacía lo siguiente primero pedía permiso para interactuar con el módulo Bluetooth segundo encontraba intentaba encontrar un dispositivo Bluetooth low Energy conectado que tenga el servicio que envía audio vía Bluetooth luego se suscribe a sus características para recibir notificaciones y saber cuándo se empieza y se para de transmitir audio y cuando llegan los datos de audio acto seguido cuando comienza la transmisión crea un nuevo archivo web luego decodifica los paquetes en formato opus provenientes de los airpods o bits y escribe el audio sin comprimir en este archivo web Una vez que se detiene la transmisión cierra el archivo web y luego Envía una notificación Push local para demostrar que la aplicación ha grabado con éxito al usuario en segundo plano una notificación que típica que sale desde arriba del teléfono o bueno en los macos donde se tenga configurado pero normalmente en la arriba a la derecha y sale el mensaje de la aplicación en un escenario de explotación del mundo real o un ataque de cibercriminales una aplicación que ya tiene permiso de bluetooth por algún motivo podría estar haciendo esto sin ninguna indicación para el usuario de que está sucediendo porque no hay una solicitud para

Acceder al micrófono y la indicación en el centro de control que algunos se preguntarán nada bueno pero igual sale ahí no ahí se ve el nombre de la aplicación que ha accedido al micrófono no no ahí solo muestra Siri y dictado Así que no sale por ningún lado que una aplicación pueda haber estado accediendo al audio de bluetooth de esta forma el investigador ha publicado unos vídeos en los que demuestra su ataque tanto en iPhone como en macos y bueno está en la página de en su propia página Así que la vamos a poner en las notas en las notas y referencias del episodio y podéis Ver los vídeos vosotros mismos quiero comentar que hay ciertas limitaciones primero indicar que este ataque solo permite acceso al audio del usuario en iPhone y ipads cuando se utiliza Siri o el dictado solo en estos casos y solo si se tienen conectados auriculares Bluetooth airpod o bits solo estos auriculares si utilizas otros auriculares Bluetooth este ataque no funcionaría porque como digo los airpod y los bits tienen funcionalidad adicional que permite este ataque de hecho y segundo a pesar de que este ataque se pase por alto el permiso del micrófono en estos dispositivos móviles aún necesita acceso a Bluetooth algo que las aplicaciones no se pueden saltar por alto Así que aplicaciones de este tipo que quisieran Acceder al audio vía Bluetooth obviamente tienen que tener el permiso de acceder a Bluetooth y esto con una aplicación se instala normalmente sale una ventanita un poco y te pide le pide al usuario que acepte o de nivel acceso Bluetooth sin embargo la mayoría de los usuarios no se esperan quedar acceso a bluetooth a una aplicación cualquiera también le podría permitir a esta aplicación acceso a las conversaciones con Siri y al audio del dictado verdad bueno esa es Esas son las limitaciones Aunque lo más escalofriante es que en maco es no hay limitaciones el proceso agente que permite acceso al bluetooth low Energy no tenía estas comprobaciones de derechos que decíamos que aplicaba este policía no en este edificio ni indicaciones de transparencia Con sentimiento y control para proteger el servicio del audio vía Bluetooth por lo que cualquier proceso en el sistema maco es podría conectarse enviar solicitudes y recibir datos de audio de auriculares airpods y bits de esta forma el maco es las aplicaciones pueden grabar las conversaciones con o el audio dictado sin ningún tipo de solicitud de permiso pero peor aún este ataque en particular también permite que cualquier aplicación en maco es solicite audio vía Bluetooth lo bueno allí sin tener que esperar a que el usuario hable con Siri o inicie un dictado en cualquier momento una aplicación se puede poner digamos engancharse al audio vía Bluetooth y grabar todas las conversaciones que suceden en ese caso Cuál es el impacto igual os estaréis preguntando pues en iPhone y iPad digamos que igual sería el menor de los impactos y este estaría en los comandos de Siri No ya que un usuario normalmente no proporciona mucha información sensible como contraseñas a través de Siri o números de seguridad social no O cuentas de banco Aunque sí que puede proporcionar temas que se pueden utilizar para abusar de la privacidad del usuario por ejemplo se me vienen a la mente direcciones de correo electrónico vas y le dices Siri Envía un email a podca arroba tierra de hackers.com o temas de nombres de amigos y familiares Siri Llama a Martín vigo o temas de ubicación Siri Qué temperatura hace en Nueva York cuando pasamos a temas de dictado ya pues rienda suelta la imaginación Supongo que usuarios igual alguna vez lo han utilizado para transcribir datos que tienen en la mente vas por la calle y no quieres pararte a escribir entonces usas el dictado No eso es bastante común Supongo pero igual También algunos datos que son difíciles de escribir pues usuarios utilizan el dictado Como por ejemplo un número de cuenta que te dan que es bastante largo entonces dices dictado el número de cuenta es 2.100 24 o 32 y lo va escribiendo no o una dirección física Oye tengo que ir a esta dirección que es yo que sé la calle Broadway número tal Y que lo escriba el dictado Entonces es esos datos en un iPad o

iPhone los podría capturar una aplicación que abusará de este de este ataque digamos al irnos yamaco es el impacto es muy elevado porque de nuevo no se tienen restricciones en cuanto a qué audio se puede capturar se me ocurre atención a mi a mi imaginación pero estás hablando de los vectores de ataque se me ocurre para obtener algo útil entre lo que dices de subir y dictados y tal alguien va por autopista tú ves en el coche al lado normalmente a veces va a llevar Los cascos puestos hay gente que conduce con unos al lado con un airpod y todo esto si sabes la el email de la persona no por eso le está siguiendo cerca del coche resetea su contraseña le llega un mensaje con el código esa persona va a decir Oye Léeme el mensaje que me acaba de llegar y pum y ya tienes los seis dígitos del código Qué te parece y ya le puedes robar el email me parece bueno Me parece buena lo único que este ataque voy a clarificar solo solo la aplicación solo puede capturar el audio que viene del micrófono del Bluetooth de los auriculares Bluetooth Así que si dices Léeme a no ser que estuviera en altavoz Entonces lo cogería el micrófono Ah no captura lo que dice Siri captura lo que tú le dices a Siri vale vale esa parte hay que prestar atención a la noticia porque también digo es el audio qué audio es el que es el audio realmente que capturan los auriculares brutos básicamente el micro que hablas en el micrófono pero no sé como tú has dicho vale está está bien está bien que especifiques eso porque como lo había entendido Yo era Claro porque Bluetooth uno se imagina de ambos lados no lo que va a través de bluetooth del sonido Pero oye Qué curioso vale Sí sí tiene valor si lo tienes digamos en altavoz en algo por algún motivo y tienes los auriculares la gente se lo ponen en el cuello No pues Oye igual en el investigador no ha mencionado Pero mira sería una una nueva vuelta de tuerca que se le puede dar al ataque a veces porque a veces lo pones ahí en altavoz no porque te llama alguien y tienes a alguien al lado que quieres unir a esta a esta conversación no y pones el móvil en altavoz mientras llevas los airpods y te los bajas a nivel del cuello bueno o los bits Y todavía están conectados vía Bluetooth e igual eso podría capturar lo que se dice por él por el teléfono así que no hay que descartar ese ataque muy bueno Martín bueno en las mitigaciones Apple ha arreglado esta vulnerabilidad de hecho en iOS 16.1 el 12 de septiembre y en iPad o es 16 el 24 de octubre al igual que en las actualizaciones de macoes Así que si no tenéis actualizarlo para que nos puedan porque como decimos no se puede saber qué aplicaciones que tengan Bluetooth están digamos ahora mismo escuchando de vuestros auriculares no para mitigar la vulnerabilidad en iOS en la que en el atacante podría suscribirse al servicio que permite recibir el audio que se envía del dispositivo es Bluetooth como digo Apple ha añadido este servicio a una lista restringida por lo que de ahora en adelante las aplicaciones de terceros no desarrolladas por Apple no van a poder acceder a este servicio esto de lista restringida me recuerda un poquito de nuevo el capítulo el episodio anterior en el que también decíamos lo mismo no Microsoft ha hecho una lista de drivers vulnerables que bloquea que no permite Que corran y no la actualizado en tres años así que bueno Yo supongo que el parche está ahí Y según dice el investigador funciona No pero en un futuro Si salen estos servicios que me parece interesante que solo lo pongan una Lista negra y ya no pero bueno lo que hace es que previene que aplicaciones de terceros no accedan a este servicio se lo ha puesto en una Lista negra obviamente los componentes y sistemas propios de Apple sí que pueden acceder porque serían digamos legítimos y confiables y para mitigar la buena vida en maco es que es la crítica la más grave porque se puede escuchar cualquier tipo de audio no solo el audio que se crea cuando se usa Siri o el dictado pues Apple ahora verifica que el proceso que intenta utilizar el servicio tenga el permiso de bluetooth y si no no permite la comunicación otra medida de mitigación que un usuario de a pie como nosotros puede aplicar es una bastante radical es desactivar el bluetooth

no aunque se entiende que esto no siempre es posible la otra es si no se puede desconectar los dispositivos Bluetooth como airpods o bits cuando se mantengan conversaciones importantes Se use Siri o se utiliza el dictado como hemos dicho antes como decía Martín en el caso este de que igual se pudiera recibir audio a través de que el micrófono de los auriculares Bluetooth reciben lo que sale del altavoz del teléfono en Sí pues Oye cuando vas a tener una conversación de este tipo y altavoz Desactiva apaga los los auriculares Bluetooth y también lo que se puede hacer es de vez en cuando esto ya lo hemos comentado creo alguna vez a mí me gusta de vez en cuando irme a los temas de permisos de iPhone iPad 2 y revocar permisos de cualquier tipo de aplicaciones en este caso pues Vais a la de bluetooth y miráis ahí Qué aplicaciones tienen acceso a Bluetooth eso está en configuración privacidad y seguridad Bluetooth y Oye decís Oye Esta aplicación no sé una aplicación que no tiene nada que ver con Bluetooth porque porque tiene que tener acceso a Bluetooth pues lo desactivo Y ya y con esto Pues un poco reducís un poco el riesgo no Aunque en este caso lo mejor es parchear la verdad es que hay que dar gracias a esta investigador por publicar esta vulnerabilidad porque claramente podría haberse callado y venderla a un broker de 0 days quien la hubiera vendido alguna agencia gubernamental o empresa de spyware leas en ese grupo o similares candiru intelexa o directamente a verla vendido a una empresa de espionaje no directamente a estas porque la verdad que este ataque está está bastante bien Apple De todas formas se lo agradeció con una recompensa de 7.000 dólares así que bueno está bastante interesante y quería cerrar la noticia con una funcionalidad que bueno He descubierto a raíz de investigar este esta noticia es que hay una funcionalidad en los no sé cuándo se introdujo igual es en iOS 15 o el 16 creo que es el 15 se llama funcionalidad Live Listen que te permite utilizar tu iPhone iPad o iPod Touch como micrófono remoto y escuchar audio vía bluetooth a través de los auriculares de nuevo airpods of bits eso que vas y te dejas olvidado no entre comillas el iPad o el iPhone en una sala de reuniones y Bueno ahí entra la siguiente reunión no los ejecutivos de alguna empresa o bueno lo que sea y lo ven Pero lo típico no Bueno se lo ha dejado alguien ya lo vuelve a recoger luego más tarde lo ponemos aquí en un lado porque somos buena gente y que luego que vuelva luego y lo no Y tú en una sala próxima porque creo que Bluetooth como máximo puede llegar a 100 metros Aunque si hay objetos como muros Entonces menos no se atenúa la señal Y entonces menos distancia Pero bueno digamos que en una en una sala colindante pues puedes estar escuchando todo lo que se habla en esa sala en tus auriculares Bluetooth así que bueno Esa esa me parecía interesante comentar esta funcionalidad que se ha diseñado un poco más para gente O sea tiene un caso de uso bueno digamos inicial que es el que hay gente que no tiene buena audición y entonces pone su teléfono cerca de la persona que le está hablando y con los auriculares Bluetooth pues recibe ese audio de forma más clara y concisa y se puede hacer una mejor comunicación Esto me recuerda a los anuncios de sonotone ahí ponte ponte justo ahí bueno nuestros oyentes más jovenzuelos no lo recordarán Pero esto hablamos de la teletienda el anuncio de el pinganillo para la gente mayor con sordera y que te lo anunciaban como que era algo cojonudo hasta para para espiar al vecino ampliadas ahí el sonido y ya está digamos que una versión mejorada de aquella de poner el vaso contra la pared y el oído que eso no no funciona Pero bueno no que lo haya probado yo pero el típico vaso sí que pones contra las Sí sí Bueno eso ya está la otra que era mitiquísima que ese no sé si habéis visto la imagen esta de es como una pequeña Antena parabólica pero que tiene una mirilla y miras atrás de ella y tienes Los cascos puestos es como una Antena parabólica que había ya en alguna peli lo he visto pero y creo que en alibaba vendían uno pero yo vamos yo creo que eso tiene que ser un timo es que a ver no soy no soy físico

yo aquí como para para saber cómo funciona todo pero no sé una pequeña Antena parabólica No sé exactamente cómo funcionaría para pillar mejor el audio O sí no sé Bueno nos estamos es cuestión de probarlo si igual iguales es más como un vaso más grande lo pones contra la pared y ya si alguien nos quiere enviar Sí a ver una Antena parabólica Así va a captar mejor la señal acústica y lo que sea no pero va vamos un poco un poco full además si estás hablando hacia el otro lado las ondas van hacia el otro lado quiero decir tiene que estar la persona mirando hacia ti en tal caso Pero bueno que está fuera del scope de tierra de hackers o no sabes ostras a lo mejor podíamos hacer en Twitch que hace mucho por cierto queridos oyentes que no hacemos directos en Twitch o que no grabamos en Twitch porque bueno hemos estado viajando un montón y entonces es un poco más complicado pero volveremos pronto a hacerlos en directo que era súper divertido pero estaba pensando que podíamos hacer pruebas ahí en directo de gadgets textos no solo Deja aquí de que funciona pero de cosillas de estas y ver cómo funcionan ver si son inseguras estaría Guay Sí sí totalmente cacharreando es como se aprende y animamos a todos los oyentes que hagan eso todo por el bien de la ciencia en la educación y el aprender juntos bueno queridos oyentes que nos íbamos alargado ya sabéis muchísimas Muchísimas gracias por quedaros hasta el final nos agradecemos un montón cuando nos escribís y nos decís lo mucho que os gusta el podcast este nos sube la moral qué queréis que os diga y cada día somos más es exponencial como está creciendo la audiencia en todos los sentidos Así que estamos encantadísimos llevamos dos añitos y pico con el podcast Y la verdad es que es una gozada Muchísimas gracias por estar ahí por escucharnos por apoyarnos Gracias por todo de verdad muchas gracias a todos y bueno Esperamos que se os hayan ido ya los escalofríos que igual estuvierais tiritando durante la hora que os hemos dado terror pero ahora ya todo bien y podéis volver a vuestras vidas y todo todo bien Todo tranquilo no no hay que tener a la ciberseguridad y recordad como siempre que nos podéis contactar en por email redes sociales que os podéis patria con uniros a discord y nos vemos en nos escuchamos en el próximo episodio Adiós adiós 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