investigadores se encuentran varias vulnerabilidades críticas E incluso lo que parece ser una puerta trasera en un estándar descifrado de comunicaciones utilizado por fuerzas y cuerpos del Estado servicios de emergencias y el personal de infraestructuras críticas el sol aprieta con el comienzo de agosto y ya puede refrescarte con 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 7 de agosto de 2023 este es el episodio número 102 yo soy Martín vigo y sigue sin estar conmigo Alexis porros Pero bueno lo estará en el siguiente Así que no temáis bienvenidos deciros que este episodio que como veis he estado dos semanas sin grabar porque me ha pillado de vacaciones y de verdad que hago lo posible para poder grabar semanalmente Pero esta vez no ha podido ser Ya lo sé el sonido Es malo cada vez que digo una papi escucháis ruido en vuestros oídos y es que me he ido corriendo a comprar un micrófono y solo encontré uno que era de 10 euros Entonces era una opción o la otra era o grabar con un micrófono barato y que el sonido no sea tan bueno o no grabar y ya eran dos semanas sin grabar que no puede ser no os puedo tener sin que estéis al día así que aquí me tenéis grabando en una esquina de un hotel con un micrófono malísimo Pero bueno espero que me sepáis disculpar esta vez Pero creo que era es más valioso que os traiga la información a que esta vez con un micrófono un poquito más malo que me lo dejé antes de salir de viaje el que suelo utilizar y que sepáis que volveremos con la calidad que siempre tenemos de sonido Bueno antes de nada darle las gracias a nuestros mecenas de patrón como siempre empezamos así y en concreto esta semana Ricky Aguilera que se ha unido a nuestra gran familia de personas que nos apoyan en patreon Y si tú crees que nos puedes ayudar económicamente si te gusta lo que hacemos puedes ir a tierra de hackers.com y unirte también con todas las ventajas que yo conlleva Y por supuesto como siempre También a nuestros sponsor esta semana Cómo no mona una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast timonas monat con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y que está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan a todo el mundo y en remoto así que ya sabéis echar un vistazo a su web la que os digo siempre monat.commod.com y les podéis mandar vuestro currículum a tierra de hackers@monat.com recordar siempre decirles que venís de parte de tierra de hackers y no me lío más vamos directamente a la noticia y lo dicho hoy es de tú a tú querido oyente tú y yo solos Así que relájate si nos escuchas en la playa si ya estás en cama para dormirte si estás en el gimnasio vas a aprender un montón porque yo aprendí un montón con esta noticia de hecho nos salimos un poco de los sistemas habituales de los que solemos hablar solemos centrarnos aquí en tierra de hackers pues bueno en lo que dictamina la actualidad en torno a ciberseguridad que suele ser pues vulnerabilidades o hackeos a teléfonos servidores ordenadores personales dispositivos iot Bueno pues hoy no va de nada de eso hoy os vengo a hablar de radios y no no la radio de tu despertador para escuchar música sino las radios utilizadas por fuerzas y cuerpos del Estado militares agencias de inteligencia personal de infraestructura crítica Pues todos estos lo que utilizan para comunicarse entre ellos de manera segura destacar además que estas radios o más bien su protocolo no es solo utilizado por humanos para comunicarse el mismo digamos mecanismo de transmisión usado para la voz también se usa para comunicaciones entre sistemas de infraestructura ferroviaria El tendido eléctrico barcos de transporte de mercancías Y bueno ya ya os hacéis a la idea Por tanto vamos a hablar de un sistema de transmisión crítico utilizado en infraestructura crítica el estándar europeo de radio comunicaciones etcétera o las siglas de terrestre radio tetra es un protocolo de comunicación es mediante radiofrecuencia estandarizado por la Unión Europea en 1995 y usado en más de

100 países tetra está diseñado para comunicaciones confidenciales como comentaba antes por Pues por el uso en el ámbito militar en infraestructuras críticas por lo que es utilizado como un sistema y además es utilizado con un sistema de cifrado pero propio y hago énfasis en el sistema de radio propietario para proteger las comunicaciones y que no puedan ser leídas y escuchadas por adversarios Pues gracias a varios investigadores holandeses que recibieron una pequeña inversión para llevar a cabo una investigación sobre este protocolo tetra sabemos no solo que contiene varias vulnerabilidades críticas sino también una puerta trasera insertada a propósito y que ha estado presente desde el inicio recordemos 1995 en otras palabras las comunicaciones protegidas por tetra en realidad pueden ser capturadas y descifradas mediante una puerta trasera supuestamente vamos a decir de momento entremos en fondo en la conspiración lo que se conoce como el axioma de kerchhoff en el mundo de la criptografía dictamina que un sistema de cifrado ha de ser seguro aun cuando todo sobre el sistema es conocido con la única excepción de la clave de cifrado esto quiere decir que usando una analogía yo no debería de ser capaz de poder abrir la puerta de tu casa sin la llave correspondiente Aunque conociese perfectamente el diseño de tu cerradura tuviese una en casa que pudiera examinar al detalle conociese El fabricante incluso me dieras una copia exacta de tu misma cerradura pues eso es lo que dice este principio fundamental de la criptografía pero también nos dice otra cosa Y es que los sistemas de cifrados nunca deben ser secretos o su inspección pues restringida solo algunos como es el caso de tetra Y esto es lo primero que cherrría Precisamente en este protocolo el uso de un sistema de cifrado Secreto al que solo tienen acceso personal muy contado desde que se creó un sistema descifrado que no ha podido ser examinado verificado y testeado adecuadamente por expertos en el campo para comprobar que no hay fallos de diseño o como decía directamente puertas traseras es por eso también que este equipo de investigadores recibió fondos para intentar encontrar estos fallos ya que usándose como se usa este protocolo en sistemas críticos es importante asegurarse que un adversario no puede acceder al contenido pero en vez de creerme A mí en palabras del representante del centro de seguridad Nacional de Holanda miráis sheffer tetra es un sistema de comunicación crucial en Holanda y en el resto del mundo y tiene que ser robusto y seguro especialmente en situaciones de crisis estas vulnerabilidades demuestran que un atacante podría interceptar manipular e interrumpir las comunicaciones bueno esos son eso es lo que ha dicho este tío buscando rápidamente a ver si las fuerzas y cuerpos de seguridad del estado en España usaban tetra me encontré que la guardia civil usa uno diferente llamado tetrapol pero por ejemplo las chancha que es la policía del país Vasco sí usa tetra así como el departamento de seguridad del gobierno Vasco para emergencias pero buscando un poco más que siempre me gusta Pues indagar en las noticias Como ya sabéis me encontré con sirve s&r Dee que son las siglas correspondientes al sistema de radiocomunicaciones digitales de emergencia del estado este sistema según lo que vi en España es utilizado por atención Guardia civil la ume que es la unidad militar de emergencias la guardia costera el Ministerio de defensa y la casa real curiosamente una de las webs que consulte resaltaba la importancia de sirve durante la coordinación de la coronación del rey de España esto lo comento simplemente para Resaltar la importancia de la confidencialidad de las comunicaciones que se lleven a cabo mediante estos protocolos si bien por lo que Leo sirve se basa en tetrapol y no en tetra que es el protocolo del que realmente nos estamos centrando he visto que tetrapol en realidad es un protocolo más antiguo que tetra no solo eso los sistemas que trabajan con tetra pueden comunicarse con sistemas que trabajan con tetrapol son interoperables mediante el framework y ST resulta que en Europa existen mayormente dos sistemas para estas radios no tetra y tetrapol y la necesidad de que las comunicaciones entre fuerzas y cuerpos de seguridad de diferentes países sean fluidas hace de esto un problema si Francia utiliza tetrapoling y nosotros

en España utilizamos tetra Pues claro no se va a poder comunicar unos con otros por ello y según me encontré investigando una vez más en 2016 la Unión Europea propuso el framework isstep o intercester operatible lo vuelvo a decir intersystem intero interoperability for tetra tetrapole networks para que independientemente de si un país usa tetra y otro tetrapol puedan comunicarse de manera transparente Igualmente sin que insisto todo Europa tenga que llegar a un estándar y los que usan el otro pues tengan que tirar sus radios y comprar nuevas os dejo de hecho referencias en las notas del episodio Pero con esto decir que si bien puede ser que te trapol usado en España básicamente para todo no esté afectado por la Sub vulnerabilidades y bueno y la puerta trasera si lo está tetra sistema con el que puede comunicarse también y si no puedes descifrar las comunicaciones del lado de España pues quizás la puedes descifrar del otro lado del país que si usa tetra y digo quizás porque Lamentablemente Los investigadores todavía no han ofrecido todos los detalles técnicos de su investigación ya que la van a presentar la semana que viene en Las Vegas en Las conferencias de Black Cat y defton han creado una web específica para sus hallazgos que es un poco de donde yo me alimenté y se puede ver información preliminar y un par de vídeos de demostración de cómo pueden llevar a cabo estos ataques interceptando mensajes pero vamos que no me sorprendería nada que te trapol se viera afectado de manera indirecta en comunicaciones con sistemas tetra Y por supuesto os dejo la web en las notas del episodio para que podáis ir a leerla Pero bueno sigo palante que yo me pongo a investigar y no salgo del pozo y me voy por las ramas ahora que sabemos lo crítico que es que estos protocolos de comunicación sean seguros Qué es eso de que alguien metió una puerta trasera Ok lo primero que tenemos que saber es que tetra utiliza una serie de cifrados simétricos dependiendo de quién lo utilice llamado tetra en cription algoritmo o tea existen cuatro de a1 ta2 de A3 y te A4 y todos son cifrados basados en claves de 80 bits lo cual no es mucho pero todavía a día de hoy es resistente ataques de Fuerza bruta 1 y Teatro están destinados a uso comercial es decir no deberían ser utilizados por fuerzas y cuerpos de seguridad cuerpos de emergencia y cosas así de a2 está restringido a su uso en la Unión Europea y a su uso por parte de cuerpos y fuerzas de seguridad servicios de emergencia etcétera vale tea3 se usa del mismo modo que ta2 pero Se reserva su uso para cuando hay problemas de comunicación mediante ta-2 A lo mejor pues porque justo la frecuencia que utiliza ta2 Pues hay ruido así pues se puede utilizar te A3 digamos que es como un backup por otro lado tenemos el Air en creption interface o ie que es otra capa de cifrado usada en tetra para en este caso en vez de cifrar las comunicaciones autenticar los dispositivos en la red esta fase es crítica pues es también donde se negocian las claves privadas de cifrado que recordemos son de 80 bits Ok esto de los 80 bits es importante entenderlo digamos que representa lo compleja que es la llave de tu casa no volviendo a esa analogía si la cerradura de tu casa tiene una llave súper simple digamos de Solo dos o tres dientes no con dientes ya me entendéis pues la digamos la sierra que tiene la cerradura que son los piquitos no que en realidad Pues es lo que como está en codeada tú tu llave de tu casa pues eso lo tiene dos o tres da igual los robusta que sea la cerradura en Sí yo puedo crear todas las llaves con todos los piquitos de dos o tres dientes y probarlas hasta que abra no digamos que la Fuerza bruta no sería tan compleja pero si en vez de tres dientes tiene siete que es lo normal 7 8 la cosa se complica mucho lo de crear todas las llaves posibles y probarlas una a una No pues a eso nos referimos al con lo de que el cifrado es suficientemente robusto porque es una llave de 80 bi con nuestra analogía de 80 dientes no pero resulta que el cifrado tipo de a1 tiene un mecanismo secreto que permite reducir la clave de cifrado a usar solo 32 bits 32 bits no es suficiente y con un ordenador como el tuyo como el mío se podría hacer un ataque de Fuerza bruta en cuestión de segundos sería como si cuando vas a comprar tu cerradura tú esperas que sea súper segura la llave Pero hay un mecanismo secreto que haría que la llave

fuese súper simple sin que tú lo supieras y con ello permitiese a cualquiera generar suficientes llaves como para entrar en tu casa Por qué existe un ese mecanismo para reducir la seguridad del cifrado y además es algo que solo conocen Algunos porque está protegido bajo nondis closer agreements recordemos los algoritmos de tetra Pues vete tú a saber cuando se le preguntó esto a uno de los responsables del desarrollo de este protocolo Brian murgatroit este dijo que no se trata de una puerta trasera sino que debido a los tratados de exportación vigentes en su día necesitaban una opción que pudiera reducir la robustez del sistema de cifrado en uso comercial a sólo 32 bits y añade que en 1995 cuando se desarrolló este este estándar 32 bits era suficiente complejidad para evitar ataques de Fuerza bruta con la tecnología en de esos años Bueno sí que es cierto que no solo Europa sino también Estados Unidos en su día también incluía sistemas cifrados los sistemas de cifrado como parte de la legislación referente a la exportación de armamento y que ello conllevaba debilitar los sistemas de cifrado de tecnología americana que iba a exportarse a otros países y os doy un ejemplo muy curioso de esto y es el caso de los primeros navegadores netscape cuando empezó a desplegar ssl que al principio internet iba todo sin cifrar pues lo hizo solo para proteger los pagos online Pues resulta que tuvieron que hacer dos versiones de netscape la versión estadounidense que utilizaba cifrados rsa de hasta 1024 bits y la versión internacional que usaban la mitad solo 512 bits haciendo literalmente y por imposición del tratado de exportaciones norteamericano a todo el mundo más inseguro en cualquier caso y en palabras de un experto criptógrafo de la Universidad de Jones Hopkins dice lo siguiente no diría que el uso de 32 bits en el cifrado tea 1 se activa y equivalente a no usar ningún cifrado pero desde luego está muy muy mal otra de las vulnerabilidades críticas que encontraron no afecta solo al modo de cifrado de a uno sino a todos resulta que de la manera como funcionan las radios cuando las enciendes y se conectan a una de las torres igual que haría por ejemplo tu móvil Es que la torre envía la hora actual a la radio y a es y es ahora la que solemos llamar en el argot pues Time stamps no que incluye la hora hasta el milisegundo es utilizado para calcular la clave privada usada para cifrar las comunicaciones si ya no deberías utilizar semillas predecibles para calcular claves criptográficas la situación con tetra es aún peor resulta que los paquetes que envían las Torres en modo broadcast es decir a todo el mundo van sin cifrar los paquetes que contienen la hora y pueden ser interceptados por cualquiera que esté escuchando en esa frecuencia te lo digo de otra manera cualquiera puede capturar los paquetes que contienen la semilla para calcular las claves criptográficas de los dispositivos que se acaban de Conectar a esa Torre cuál sería el vector de ataque Pues un atacante va y recolecta la información cifrada que se está enviando desde una radio usada por el objetivo mientras mantiene pues una conversión privada no el objetivo tú estás ahí capturando en la red en el aire no con Pues con tu con tu Hardware todos los paquetes de momento están cifrados Así que no pasa nada ahora el atacante anota la hora de conexión de esa radio a la torre es decir pues cuando acaba de conectarse o lo que sea con esta que recordemos que ese paquete va sin cifrar Pues con esta información el atacante Crea una torre falsa algo que se puede hacer con Hardware súper barato y hace que una radio suya se conecte a la torre falsa haciendo que la torre falsa envíe la misma hora que anotó cuando su objetivo se conectó la torre está Vale Según los investigadores pues unos 5000 dólares que eso es básicamente nada pues este tipo de radios confían ciegamente en la hora que les envía la torre es decir no tienen la hora de por sí sino que lo que le envía la torre es lo que cuenta por lo que aunque no sea realmente la hora que la torre está diciendo lo acepta igualmente y genera la clave de cifrado en base a esa hora con la clave de cifrado generada en la radio en base a la hora enviada por la torre falsa que es justo la que tú has capturado cuando estabas capturando el tráfico de tu objetivo todo lo que tiene que hacer el atacante ahora es extraer de la radio la clave de cifrado generada y ya puede

descifrar todo el tráfico que ha capturado de las comunicaciones del objetivo que estuviste recolectando la verdad me parece brillante Pero hay otro vector de ataque que me pareció muy curioso que sugieren también los investigadores en este caso los atacantes quieren poder inyectar información en la transmisión de datos por ejemplo pues para hacerse pasar por el objetivo y enviar información falsa o manipulada sin que el recipiente sepa que realmente vieron de un atacante en este caso utilizarían la torre falsa para hacer broadcasting de una hora en el futuro por ejemplo yo cojo pongo mi Torre falsa cerca del objetivo y digo que empieza a enviar que son las 12 del mediodía de mañana en vez de hoy Ok de esta manera y insisto estando cerca del objetivo para que su radio se conecte a mi Torre falsa la radio generará una clave de cifrado que sincronizará con la antena que se que será válida a partir de mañana mediodía es decir como la clave de cifrado se genera en base a la hora pues esa clave de cifrado va a ser válida no hoy pero mañana que es justo la hora que yo le estoy enviando ahora el atacante tiene en su poder una clave de cifrado válida para el día siguiente para la radio de un objetivo por lo que todo lo que tiene que hacer es ahora usar esa clave de cifrado para cifrar las comunicaciones falsas que inyectará al día siguiente Entonces ahora el atacante Ya solo le queda esperar a mañana al mediodía para inyectar los mensajes los paquetes en la red reenviándolos que cifró el día anterior con la clave de cifrado que iba a ser válida al día siguiente me parece la verdad una vez más un ataque brillante Pero bueno Cómo pudieron los investigadores analizar los algoritmos de cifrado para encontrar Estos tipos este tipo de fallos si dijimos que eran secretos y nadie tiene acceso más que unos pocos privilegiados pues haciéndolo de la manera difícil la verdad Hardware hacking e ingeniería inversa trabajo muy laborioso y que requiere muchísimo conocimiento técnico los tíos son unos cracks la verdad empezaron comprando una de las radios que usa tetra por eBay concretamente una radio del fabricante Motorola que es uno de los principales fabricantes de radios que utilizan este estándar con la radio en su laboratorio la desmontaron y se conectaron directamente a los diferentes chips de la placa para intentar extraer el firmware y sobre todo encontrar Dónde se almacenaba la lógica del sistema de cifrado Pero esto no es tan fácil como soldar cuatro cables a la placa y ya los fabricantes para precisamente proteger el secretismo del protocolo tetra ponen medidas antiingeniería inversa y protegen el código con chips especializados como un clave que tenía la radio y almacenaba precisamente el código del sistema criptográfico Pues los investigadores tuvieron que encontrar y explotar varias vulnerabilidades en los chips para conseguir finalmente extraer el código relevante para empezar a analizarlo lo dicho unos cracks O sea no solo encontrar un luego las vulnerabilidades críticas en el sistema de cifrado sino que para poder empezar a analizarlo o sea para poder empezar a trabajar tuvieron que encontrar vulnerabilidades en los chips de las radios brutal cabría ahora preguntarnos han sido estas vulnerabilidades y directamente bueno puertas traseras explotadas por algún adversario ya opuestas a propósito pues es difícil de saber por un lado llevan más de 20 años presentes pero es difícil saberlo porque no queda evidencia de ellos si alguien inyecta ese mensajes falsos y descifra información que recolecta de manera pasiva como estaban los ejemplos pero sí podemos irnos al archivo histórico y sobre todo apoyarnos en las famosas filtraciones de gente como Edward snowden o Wikileaks en el caso de Edward snowden entre los cientos de miles de documentos que filtró se encuentran referencias algunos en a la interceptación de comunicaciones transmitidas mediante tetra concretamente la nsa y GTA hq Según uno de los documentos top Secret que filtró snowden interceptó y descifró comunicaciones tetra de la policía de Malasia durante una conferencia que tuvo lugar en el país sobre el cambio climático en 2007 ese mismo documento menciona también la interceptación de comunicaciones mediante etcétera de los cuerpos de seguridad de Indonesia otro documento filtrado por snowden habla una vez más de la nsa y GC hq colaborando juntos para espiar comunicaciones

protegidas por tetra en Argentina concretamente en 2010 cuando Argentina y Gran Bretaña tensaron sus relaciones diplomáticas debido a la exploración y recolección de petróleo en unas Islas si esto nos parece suficiente os añado también uno de los cables filtrados por Wikileaks en su día correspondiente a las comunicaciones entre la Embajada de Estados Unidos en Roma y un fabricante italiano en el que Estados Unidos parece poner resistencia a la venta de radios tetra por parte del fabricante italiano a la policía iraní en ese cable se ve como El fabricante italiano le contesta la embajada estadounidense que Recuerda que el cifrado utilizado por la radios que se venderán a la policía de Irán a iraní será de menos de 40 bits en fin queridos oyentes es difícil pensar que esta puerta trasera o bueno digamos que esta manera deliberada de debilitar El cifrado estaba ahí puesto no solo a propósito sino con conocimiento No solo de los fabricantes sino de las agencias de inteligencia como os acabo de contar que la nsa lo sabía no sabemos si habrá sido explotado pero lo que sabemos es que son comunicaciones críticas y que esto es muy serio ya os digo que esta semana Será la blajatidez con Y estos investigadores van a presentar todo lo que saben y yo voy a estar pendiente de si de alguna manera afecta al estándar tetrapol que es que el que utilizamos por ejemplo en España para para temas críticos hasta aquí ha llegado la noticia querido oyente como siempre os dejo un montón de enlaces de las notas del episodio mis disculpas de nuevo de verdad por estar grabando con este micrófono que no vale para nada pero después de dos semanas sin grabar porque me resultó imposible porque ser agosto yo no quiero dejar abandonados quiero seguir ofreciendo el podcast en todo momento Así que preferido usar el primer micrófono que me encontré a dejarme una semana sin grabar Muchas gracias por estar ahí Muchas gracias por todos vuestros comentarios por todo vuestro apoyo mención especial a los de patreon y los que no estáis en patreon si nos queréis ayudar Igualmente cosa que os agradezco muchísimo dejarnos comentarios compartirlo con amigos por redes sociales dejarnos 5 estrellitas donde nos estéis escuchando que eso lo que hace es que gane más interés los sponsors y por tanto podemos costear todo lo que supone tener este podcast funcionando durante ya más de tres años se os quiere nos vemos y nos escuchamos en el siguiente episodio Adiós adiós si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers