hackean un dispositivo para mezclar las cartas usadas en los torneos de póker más importantes a nivel mundial después de que una investigación sobre una mano sospechosa concluyese que el dispositivo era en jaqueable no os fiéis del modo avión una nueva técnica de persistencia en iphones permite mantener canales de comunicación encubiertos vía datos móviles a pesar de haber activado esta funcionalidad Nueva Ola de calor y 9 episodio de tierra de hackers para sobrellevarlo comenzamos Hola hola y bienvenidos a tierra de hackers quiero decir seguridad hecho podcast publicamos este episodio el 25 de agosto de 2023 este es el episodio número 104 yo soy Martín vigo y está conmigo quizá un de resaca de Las Vegas a Alexis porros Hola Alexis qué tal muy bien Martín juntitos de nuevo echándote de menos en esas resacas pero bueno contento de estar aquí contigo con los oyentes porque estas últimas semanas fueron ajetreadas entre vacaciones conferencia y recuperarse del Jet lag que como te he comentado en la previa del que siempre hacemos un poquito de cancha antes de cada episodio Estoy escuchando un libro sobre el acto de dormir que dice que necesitamos un día para recuperarnos de cada hora de cambio horario Así que según esto yo he necesitado unas dos semanas para recuperarme de todo el Jet lag y Oye no está mal encaminada esta teoría porque sí que me he notado bastante bajo de energía hasta hace poco pero sobre todo Enhorabuena una buena siesta española gran costumbre que tenemos no vaya a solucionar una Power up no como dicen esto lo He descubierto hace poco también te tomas un café antes de dormirte y media hora dejas que haga efecto el café y te levantas café Pues nada también con las pilas cargadas por estar aquí de nuevo dando la tabarra a nuestros oyentes y nada pues viento en popa todavía no me enrollo más estamos como siempre ya sabéis en todas las redes sociales más populares dónde pues no la voy a mencionar pero no podéis Buscar como tierra de hackers o arroba tierra de hackers plataformas de podcasts enésima vez que lo comento no pero ahí estamos como tierra de hackers donde debería estar suscritos y si no Dale al pausa o Mira si sabes hacer multitareas como muchos procesadores ves y apúntate ahora mismo mientras sigues escuchando el episodio y también podéis uniros a nuestro canal de discord vía tierra de hackers.com barra discord perfecto y yo pues dar las gracias a nuestros mecenas de patreon algo que no puede faltar en todos los episodios y a nuestros sponsors en este caso on branding 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 como llevan haciéndolo durante años ahora sino que si le contáis que venís de parte de tierra de hackers tendréis un descuento especial en sus servicios si necesitáis algún tipo de ayuda con vuestra identidad digital om branding es lo que estáis buscando visita on branding.es o nbrang punto es También queremos hacer una pequeña pausa para dar las gracias a otro de nuestros patrocinadores monat una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y mona a través de una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web monat.com y mandarles vuestro currículum a tierra de hackers @monat.com m o n a d.com Ok pues ya vamos con la noticia y os pongo en escena torneo de póker entre algunos de los mejores jugadores del mundo y llega una mano que se disputan garrett all design que es conocido en todas las mesas de Texas Holden más top y Robbie Jade liu una chica que si bien habitual en los torneos no tiene digamos el caché no el reconocimiento de garrett la mano hablemos un poquito de poker la mano empieza con un 7 y 8 de tréboles para agarre y una jota

de tréboles y un 4 de corazones para Robbie ninguna de las manos son espectaculares y con el flop conteniendo un 10 de corazones un 10 de tréboles y un 9 de tréboles garrett decide subir la apuesta a 2500 dólares debido a que con sus 7 y 8 de tréboles pues tiene una posible escalera de color por las dos puntas además mientras que ese Flow para Robbie no es muy potente pero aún así ve la apuesta de 2500 dólares OK siguiente carta el turn trae un 3 de corazones carta la verdad irrelevante para esta situación pero garrett decide presionar apostando 10.000 dólares haciendo Pues básicamente un poco de un Black no con la posibilidad existo todavía de Aunque menor porque solo queda una carta de conseguir esa escalera de color aquí viene la primera sorpresa cuando Robbie no solo ve los 10.000 dólares que acaba de apostar Garret sino que sube la apuesta 20.000 dólares teniendo una mano bastante mala en este punto y aquí garrett siendo el experto que es y teniendo cierta posibilidad de sacar la escalera de color se decide por hacer un oling apostar todo 109 mil dólares para presionar a Robbie a que se salga de la mano en este punto la situación básicamente es que Robbie no tiene nada y su oponente que ha estado liderando las apuestas durante esta mano hace un hollín y aún con estas lo primero que hace Robbie es usar un Time chip en este torneo para que os hagáis una idea permiten pedir tiempo adicional para pensar si quieres jugar la mano o no es muy común que haya jugadores que se quedan pensando si apostar o no durante tres cuatro o cinco minutos y entonces pues hay la posibilidad de que los oponentes los demás jugadores pidan El reloj no clock que le dicen y así pues le da solo un minuto más para que no esté ahí cinco horas y jugar más manos Pues en este torneo tienen como un tiempo limitado pero tienen varios chips para poder usarlos Cuando necesitan pensar un poco más esto lo explico porque ya es un poco raro porque es que Robbie aquí debería simplemente abandonar porque no no debería seguir apostando ya que no tiene nada total con un jugador medianamente conocedor habría abandonado la mano frente a un olín sobre todo teniendo en cuenta que hablamos de más de 100 mil dólares pasa un minuto y Robbie sorprende a todo el mundo diciendo que ve la apuesta haciendo del bote un total de 269 mil dólares recordemos sin ella tener absolutamente nada en este punto se puede de hecho Escuchar al comentador decir que tuvo que haber un error de la lectura de las cartas de Robbie o algo porque eso no tiene ningún sentido me refiero con esto a que normalmente cuando ves televisado una un torneo de poker no tú puedes verla todas las cartas que tienen los jugadores en la televisión y eso es porque donde apoyan las cartas boca abajo pues hay una camarita que lee las cartas que tiene pero alguna vez Es raro ocasión pero Lee más la carta Pues porque el jugador no las bien A pesar de que el torneo les exige hacerlo pues para que se pueda retransmitir por televisión y pues coge la carta que no es no entonces aquí el comentador dice esto no tiene ningún sentido que haya visto el olín de este jugador si no tiene ella absolutamente nada por tanto tuvo que haber un fallo Pues bien no acaba aquí lo raro de esta mano sino que deciden jugar la carta que queda es decir el River a dos tandas lo que en Poker se conoce como running twice no esto básicamente quiere decir que en vez de enseñar la última carta el River una sola vez pues sacan Dos cartas y entonces se reparte el bote pues si yo gano la primera vez pues me llevo la mitad y si el otro gana con la otra carta pues se lleva en la mitad es una cosa especial que tiene este torneo no Pues bien la Dealer saca la carta del River por primera vez y sale un nuevo de rombos un 9 de rombos dando a Robbie la mano Gracias a que su J es la carta más alta pero es que en la segunda ronda del River vuelve a pasar lo mismo esta vez saliendo un as de picas y dando de nuevo la mano a Robbie con la con la J al ser la carta más alta de las que poseen ambos jugadores por tanto Robbie se lleva los 269 mil dólares lo curioso es que llegados a este punto garrett cuando muestran las cartas en el River recordemos que todavía los jugadores no han mostrado las suyas solo lo sabemos los telespectadores y el comentarista Garret aquí cuando ve el River empieza a sonreír asumiendo

que la mano estaba perdida por su cuenta porque recordemos que él iba con un Black no el tampoco tenía nada potente tenía un proyecto de escalera de color pero no llegó a materializarse entonces pensaba que Robbie tendría al menos un par o seguramente algo más Mucho mejor un trío o un póker porque si no nadie va a haber un olín todo sonrisas hasta que Robbie enseña las cartas que tiene y bueno los comentarios tanto en la mesa de póker como del comentador lo dejan claro s me equivoqué You look like you wanna Kill me alcanza a decir Robbie o algarret a ver yo sé que este es un comienzo una noticia para sobre todo para los que no saben de póker un poco liosa pero lo que acaba de suceder aquí es que Robbie apostó más de 100 mil dólares cuando todas las señales toda la lógica y todo manual de póker indica que lo que tienes que hacer es retirarte y no solo ganó la mano una vez sino dos os dejo el vídeo de Youtube con la mano para que lo podáis ver vosotros mismos y analizar porque vale la pena solo por ver las caras y reacciones de la gente y cuando os digo que esta mano es rara lo digo por algo es una mano inusual por no decir claramente sospechosa hasta el punto de que los organizadores del torneo tuvieron que hacer una investigación para ver si Robbie de alguna manera habría hecho trampas y sabía qué cartas habían la pareja con antelación para decidir apostar contra lolling de garrett que no tiene ningún sentido las redes sociales como se estaba transmitiendo en directo pues ardían y era tan tensa la situación que Robbie llegó al punto de devolverle el dinero a garrett después del torneo flipa O sea estás en un torneo donde se juega miles y miles de dólares ganas una mano y al final le devuelves el dinero o sea What the fuck Robbie realmente luego en declaraciones dijo que Gary la rinconó y se puso violento Es verdad que en que las imágenes del vídeo el tío está como una cara de póker nunca Mejor dicho en plan no me puedo creer esto aquí pasa algo raro pues ella dice que se puso violento aunque yo no encontraba ninguna prueba de ello buscando por y de hecho garrett por su lado dice que fue ella quien le vino directamente a ofrecer el dinero de vuelta desde luego lo que digo muy raro todo no Pero esto es tierra de hackers Por qué hago una introducción tan larga y detallada porque como os decía se hizo una investigación y se concluyó que no se encontraron pruebas de que había habido ningún tipo de trampa os dejo por supuesto la investigación con todos los detalles en las notas del episodio Y es ahí donde encontramos la famosa frase que ha hecho que hoy os estoy hablando de esto cito textualmente del párrafo sobre las conclusiones de la investigación punto número uno la máquina deckmate que se encarga de barajar las cartas Es segura y no puede ser comprometida toma ya esto hace Las Delicias de cualquier hacker que se tercie no hace falta más que leer que alguien dice que algo es injaqueable para motivar a un hacker a demostrar que no tiene ni idea de lo que está diciendo Y esto es exactamente lo que pasó aquí investigadores de la empresa de iOS active decidieron Investigar por su cuenta si esta afirmación tan tajante se sostiene y se pusieron a investigar el aparato que usan casi todos los casinos de Las Vegas para barajar las cartas y Es que además lo acaban de presentar en la conferencia de Blackjack en Las Vegas y os dejo las diapositivas de su charla en las notas del episodio para que lo podáis ver deckmate es un sofisticado aparato cuyo precio de hecho llega a alcanzar nada más y nada menos que 20.000 dólares Todo esto para barajar cartas pero bueno en principio de manera segura de hecho la versión más nueva es el deckmate 2 Y dispone hasta de una cámara que permite identificar la posición de todas las cartas en tiempo real una cámara apuntando a toda la Baraja Quién pudiera Acceder al Stream de esa cámara no otra de las funcionalidades es la de ordenar La baraja como te viene cuando la compras O sea que este aparato también puede colocar las cartas en sitios específicos de La baraja Okay muy interesante Pero dónde se encuentra físicamente este aparato Pues justo debajo de la mesa muy cerca Por cierto de las rodillas de los jugadores Esto va mejorando tenemos que el dispositivo oficial para los torneos de póker a nivel mundial no solo incorporó una cámara para ver la posición de todas las cartas de La baraja en tiempo real además de tener la capacidad de

ordenar las cartas sino que además está físicamente al alcance de los jugadores sentados a la mesa durante el torneo pero Cómo podemos hacer para hackear el dispositivo hay algo expuesto a lo que conectarse para interactuar con él pues Supongo que a estas alturas no sorprenderá que efectivamente Así es el aparato tiene perfectamente a la vista un puerto USB Así que perfecto ya tenemos todos los ingredientes para interactuar con una máquina que nos puede decir en todo momento las cartas que tienen todos los jugadores Así que los investigadores lo que hicieron fue comprar varias máquinas de segunda mano de deckmate la misma que se utilizó en el torneo de hecho la versión 2 a una empresa que la revende y se pusieron a analizarlas haciéndoles ingeniería inversa al firmware y Software y también pues un poco de Hardware hacking al comprarlos lo primero que le sorprendió es que El vendedor les dio la contraseña para poder Acceder al menú que utilizan los técnicos para hacer reparaciones o actualizar el software del dispositivo la contraseña no la han publicado y la razón es que no solo es una contraseña muy débil sino que según dijeron es prácticamente imposible cambiarla por lo que están seguros de que muchísimos aparatos deckmate que hoy en día se están utilizando los casinos de Las Vegas siguen teniendo la misma contraseña una de las primeras vulnerabilidades obvias que encontraron está precisamente uno de los mecanismos que se supone que previene que se pueda instalar firmware malicioso para hacer esto el dispositivo calcula el Hash del firmware a instalar y lo compara con uno que está ya almacenado y que por supuesto corresponde al Hash de un firmware benigno no sin ninguna alteración Pues bien los investigadores encontraron Cómo podían alterar la firma almacenada permitiendoles poner la que ellos quisieran es decir modifican el firmware calculan el Hash lo almacenan meten el firmware se compara con el Hash que acaban de almacenar y ya está el aparato interpreta que el firmware es bueno y no ha tenido ninguna alteración curiosamente Los investigadores mencionan que hay otras verificaciones para que el propio casino no haga trampas y altere el código para que le dé una ventaja Al fin y al cabo todas las máquinas que hay un casino tienen que estar preprogramadas en base a la ley y con las probabilidades de que el cliente gane pues estipuladas no pues por ejemplo máquinas Pues el 5% de las veces de cada 100 jugadas en 5 da premio y cosas eso está súper regulado de hecho pues bien los investigadores comentan que los casinos también pueden explotar esta vulnerabilidad para instalar su propio firmware pero que pensemos que al fin y al cabo Son ellos los que han comprado el aparato y podrían perfectamente alterar su funcionamiento ya no hablamos de un atacante externo de hecho en palabras de uno de los investigadores se le está pidiendo a una máquina comprometida que detecte si está comprometida ahora que se conocen la vulnerabilidades queda el último paso no explotarlas y es ahí donde entra en juego el puerto USB que os mencionaba Los investigadores utilizaron una raspberry mini un ordenador muy pequeñito del tamaño de una moneda para que os hagáis una idea para ejecutar su paylor es decir el código malicioso que explota estas vulnerabilidades y hicieron de hecho una demostración que les permitiría saber en tiempo real dónde estaba cada carta de La baraja Por cierto Sabiendo cada carta que le ha tocado a cada jugador toma ya y recordemos que el dispositivo se encuentra debajo de la mesa al alcance de los jugadores pero los investigadores van más allá y plantean eso sí de manera teórica cómo comprometer el dispositivo Desde la distancia es decir sin necesitar acceso físico resulta que estos dispositivos al ser tan caros y recordar 20.000 dólares pueden ser alquilados y se paga un precio por cada vez que baraja tus cartas imagínate Por ejemplo que quieres organizar una timba en casa no vas a pagar 20000 dólares por el aparato no pero pues lo alquilas y pagas por todas las veces que lo uses para barajar las cartas O quizá para una timba en casa no pero a lo mejor un torneo para yo que sé de una organización sin ánimo de lucro o algo así que quieres tener algo que es fidedigno no o digamos que baraja las cartas bien pero no te lo vas a comprar el aparato pues lo podrías hacer a eso y cómo cuánto quiere decir el

próximo torneo de tierra de hackers que hagamos en algo pues sí molaría eh torneo de póker tierra hackers lo que pasa es que claro nos van a venir todo hackers y a ver quién se fue ahí De nada nos van a venir esto los autores del research ya ya te digo Pues claro Cómo sabe el dispositivo pues Cuántas veces se ha utilizado Pues por conexión móvil Integra una tarjeta SIM y se comunica con el servidor de la empresa en tiempo real para poder facturar Los investigadores por tanto plantean que se puede hacer mediante una estación falsa de gsm una torre que la máquina se conecta a esa torre del atacante y así tener el punto de entrada para interactuar con deckmate y explotarla recordemos que muy probablemente usen la misma contraseña por defecto como explicaba antes por tanto ya puedes empezar por ahí como no podía ser de otra manera la empresa que desarrolla este dispositivo que se llama lighting Wonder salió rápidamente a desmentir lo anunciado por estos investigadores diciendo lo siguiente y cito textualmente ni al deckmate 2 ni ningún otro mezclador automático de cartas de Lite en Wonder ha sido comprometido un casino además las pruebas realizadas por io active no identificaron ningún defecto fallo de diseño en el mezclador de cartas deakmate 2 y estas pruebas de io active se llevaron a cabo un contorno de laboratorio bajo condiciones que no pueden replicarse en un entorno de casino regulado y monitoreado claro esto lo dijeron antes de la charla cuando se anunció la charla y no había detalles pero claro se quedaron tan anchos y pues menos mal que ahora sacaron literalmente una demostración Los investigadores donde se ve el ataque pero no solo eso resulta que a joactive mostró públicamente emails con la empresa lighten Wonder donde estos les felicitaban por los hallazgos y reconocían que desconocían estas vulnerabilidades Y qué intentarían arreglarlas en el futuro menudo Sinvergüenza los de lighting Wonder se han cubierto de gloria con estas declaraciones acabar la noticia mencionando que los propios investigadores avisan que en realidad y con todas sus vulnerabilidades el deckmate cumple con los estándares de seguridad referentes a maquinaria de casinos en el estado de Nevada esto la verdad me dejó flipando porque mencionan que los requisitos legales están muy anticuados y como ejemplo concreto ponen que la vulnerabilidad en la que puedes cambiar el Hash de verificación del firmware Realmente está cumpliendo con con la ley porque en vez de exigir la ley que se firme el código digitalmente con un certificado que sólo posee la empresa un poco pues como utilizan los teléfonos iOS y Android la ley sólo exige que se verifique su integridad y por tanto un Hash es suficiente pues para completar esta tarea no Pues con todo esto Solo deciros que os miréis el vídeo de la mano de póker que os comenté al principio que os la dejo las notas del episodio quizá estamos ante el primer caso televisado en donde se ha comprometido la máquina de barajar cartas y resultó en un bote de más de 200.000 dólares para el atacante a mí cuando has dicho que han empezado con lo de la mano me he venido a la mente algo así en plan película de terror una mano ahí no esto es que tienen como la mano postiza y por dentro de la chaqueta está la tercera mano o algo así podrías hacer algo así Total que la moraleja es siempre gana la casa queridos oyentes ya sea la casa del dueño del casino o la casa del cibercriminal que abusa este fallo no pero siempre cierto pero por ejemplo para esto de que puede parecer un poco difícil no que eso es lo que escribía un poco la empresa de joder Pero vale Ok Pero cómo conectas el USB por ejemplo Los investigadores decían que por ejemplo puedes conectarlo antes de que se empiece a jugar el torneo o incluso cuando se envía el aparato como hace la nsa lo intercepta y ya lo metes ahí claro no tienes que meterlo cuando se está televisando pero incluso televisando Yo vi un documental guapísimo a ver si lo encuentro lo pongo las notas del episodio sobre hackeos más que hackeos sobre estafadores a casinos no y distintas maneras que lo hacían y unos lo cubrían tío que eran capaces de a una máquina tragaperras instalarle un chip y alterarlo para que siempre tocase Premio no pero claro La Movida es cómo te pones a instalar un chip dentro de una placa cuando estás en un casino que hay cámaras por todos lados pues los tíos se hicieron

un dispositivo que por donde sale el dinero o sea tenían como un alambre por así por simplificarlo y lo metían por ahí o sea se acercaban como tres a la máquina tragaperras para hacer pantalla y los tíos ponían el chip al final del alambre lo metían por donde sale el dinero hacia arriba y tenían una en casa donde habían estado practicando horas y horas y eran capaces de en segundos poner el chip tío y de hecho están las imágenes en el documental O sea que perfectamente como dicen los investigadores teniendo en cuenta la de dinero que está en juego podrían perfectamente diseñar una manera en la que poder enchufar un USB que hoy en día son súper pequeños que contiene Pues eso una raspberry como hicieron ellos para alterar el juego pero si no pues cualquiera de las otras maneras que dijimos a mí me recuerda eso al truquito este de cuando éramos niños de las arcade no de meter el el de las chispas no de La chispa del mechero que hacía eso y contaba nueva moneda era un poquito pero te funcionaba sí me tienes ahí el cablecito Pero eso da mal rollo que de hecho eso envié este un que he mirado discord enviaste un link de un Twitter de un pibe que menciona muchos cacharreos de aliexpress y uno de ellos pero ya te ponía él por eso digo que qué mal rollo Que eso genera muchísimo voltaje no bueno Sí con cuidado lo usaba también con los colegas para hacerle la bromilla y no voy a controlar pero hackeo a casino también me recuerda te acuerdas la noticia esa que hubo hace un par de años de unos ciber criminales comprometieron un cajero a un cajero un casino a través de la pecera de una vulnerabilidad en una pecera que rebota tal cual pero para robar datos claro o para hacerle ransomware este Mola porque es de hecho ni atacas al casino esto le estás quitando el dinero a los contrincantes y el otro tema es esto también da que pensar no porque el casino si sabe hacer de esto que probablemente si lo sabe contrata a alguien podrían hacer trampas no ellos cargan su propio firmware y siempre va a ganar la casa siempre van a saber ellos claro no Claro claro ahí Bueno siempre hay que pensar que el cibercriminal va a ser una persona como tú como yo que no lo somos Pero puedes decir el criminal puede ser el mismo casino y nadie lo audita dijo claro No no por eso mismo comentaba eso precisamente que como el casino es el propio ellos mismos los que lo compran tiene la contraseña de acceso tienen todo lo pueden alterar Entonces porque recordemos que esto baraja cartas no solo se utilizan el póker lo puedes utilizar en el en el Black hat me sale en el Blackjack que eso sí que juegas directamente contra el casino o el póker 7 o todos estos juegos de cartas que también se barajan las cartas pero juegas contra el casino y ahí pues mejorar sus ganancias 100% sí Y otra pregunta que tenía es cuando es mencionado que la chica era la chica no la que pidió un Time out un poco de tiempo sí sí sí O sea a mí me gustaría saber si la cámara captó algún movimiento raro o alguna Ella miró a alguien o alguna historia que le enviaron una señal porque tío aparece que lo has visto porque claro para preparar la noticia me puse a buscar vídeos de gente que lo analizaba también porque yo no soy un experto en póker o sea se jugará el póker pero me encontré un blog donde explicaban bien el porqué y tal y cual pero me encontré dos vídeos uno de ellos ponían a cámara lenta justo cuando ella decide hacer el olín y como a ver lo que pasa que el vídeo joder No se ve tanto pero es como que cambia las O sea hay una cámara enfrente grabándola y como que ya de repente mira un segundo a la cámara el vídeo de Este de YouTube da a entender que el tío de la cámara que es el que va grabando alrededor de la mesa es el que de alguna manera le hace una señal de que debe ir olín uno porque claro el tío de la cámara puede estar compinchado con el realizador que sí está viendo las cartas no porque esto se publica por por la tele eso lo que me imagino digo yo que a lo mejor hay un retraso o algo así por seguridad estoy pensando seguramente No a lo mejor va con un minuto de retraso Porque si yo de alguna manera estoy viéndolo en casa y lo puedo enviar una señal a mi compañero que está jugando al póker yo que sé que le vibre Hay algo en el bolsillo Pero bueno eso uno y el otro que dices tú lo del movimiento pues también hay otro vídeo donde vi que cuando pide el Time out como a los 20 segundos empieza

como a vibrar la silla y ella no Pero lo típico como cuando estás nervioso y mueves una pierna no que la estás así moviendo para arriba y para abajo todo el rato pero como a ver en el vídeo lo ponen como usted sí que se ve vibrar la Silla pero no sé me parece un poco exagerado porque perfectamente no se le ven las piernas a ella y yo lo veo más como que está moviendo la pierna pero sí hay ahí esa especulación pero aquí tienes esto sirvió como motivación para estos tíos y han demostrado que perfectamente la máquina esta podía haber sido comprometido para saber cómo están las cartas falta la parte de cómo luego informar a la jugadora de si tiene que apostar o no claro y ahí Las mil y una creo que hemos comentado a veces que se pueden meter dispositivos en cualquier parte del cuerpo no incluso imagínate te acuerdas los cinturones de castidad que cubrimos en un episodio Pues que te vibre un poquito eso de hecho los tíos sugieren creo que lo hicieron en la demos que yo no estuve en Black de este pero seguro como la raspberry tiene Bluetooth por Bluetooth tú puedes enviar la señal a lo que tú quieras y luego pues alguno comentaba por Twitter que puedes tener un backplack no esto correcto dispositivo que te introduces analmente por la excitación sexual pero es que unas bolas chinas de estas que tengan Bluetooth que las hay y la tienes analmente insertada y tienes Estás explotando una vulnerabilidad en la máquina que baraja las cartas que te envía por bluetooth a tu culo la vibración para decirte de alguna manera encodeada si tienes que apostar o no cuánto tío la verdad es que si de verdad fue así se merece haberse llevado el dinero tío es como mucho mucho curro tío se lo merece da para otra otro episodio de alguna serie de estas apocalípticas lo que también me pregunto es si a partir de este esta investigación los del casino afectado van a hacer ahora un poquito de análisis forense para ver si realmente Esto fue lo que sucedió o no pero no desean puesto en cuarentena esa máquina y todavía la tiene no la tiraron o yo que sé sería interesante bueno es que tengamos en cuenta que es de las que se utilizan todos los torneos digamos que es como la que se utilizan todos lados Sabes porque me imagino que muchísimos torneos rollo pocker Stars y todo esto Pues siempre quieren tener el mismo en Bayern no quieres tener una mesa una máquina y en otra otra y tal para que en todo sea la las mismas circunstancias eso lo primero lo segundo es que claro con la respuesta está de la empresa que por un lado dice que aquí no pasa nada Pues pues no pasa nada sí que es verdad que la un representante de la comisión de juegos de Nevada de no sé qué que lo pone en uno de los artículos que leí dijo que iban a mirar de cerca la investigación y que iban a tomar cartas en el asunto en base a los resultados y todo esto por tanto sí que parece que algo vayan a hacer y en principio Pues los emails que publicó iOS active con la empresa donde ahí sí decía ostras esto lo tenemos que solucionar pues con suerte lo solucionan Ok pues a ver igual hacemos un fallo up cuando hagan en un análisis forense o algo así que digan Claro que ya se ha hecho no la investigación independiente teóricamente lo que hizo pero como decía no no esta máquina no se puede hackear pues ya ya vemos como de Cómo lo han mirado sabes con qué profundidad porque claro es eso yo lo que comentaba es que todo esto vino de que se hizo una investigación independiente y se dictaminó que no hubo trampas y una de las frases en las conclusiones era que deckmate era en jaqueable y así vinieron los tíos de dijeron sí sí vamos a verlo y lo has comentado que ya lo último que quería comentar el tema del supply Chain Attack o ataque implantar algún algún Hardware en el cacharro durante la cadena de suministro durante se envía y tal mientras envía claro lo pides por Amazon y te lo envían Pues ahí lo paras y ya está el caso más famoso fue ese de que sucedió en 2018 como un descubrieron que en algunos servidores que se enviaron a empresas Grandes como Apple y similares desde China de la empresa súper micro contenían implantes Hardware y a través de eso tenían digamos una especie de backdoor en estos servidores y de ahí Salió bueno muchas historias mucho muchos cursos muchos Hardware y mucho abrió los ojos un poquito a la gente de todo el mundillo de lo que se puede hacer pero en igual como tú dices Martín menudo sinvergüenzas no esto es

del casino me quedo con esa frase pues nada tiramos palante y vamos con la siguiente noticia voy a hablaros de iphones el modo avión y como falsificar dicho modo para crear canales de comunicación encubiertos Así que no os vayáis que esto os interesa aquellos que tengan iphones y aquellos que no lo tengan seguro que tenéis algún familiar amigo o conocido que tenga iphones y que también le interesa que le comentéis esto recientemente investigadores de ciberseguridad del jump Fred labs jump es una empresa que ofrece productos de gestión remota de dispositivos de Apple es casi como decir que ofrecen software espía y de seguimiento de productos de Apple pero de forma legítima Cuando digo de espía es productos que empresas pueden utilizar para mantener la seguridad de sus dispositivos Apple haciendo cumplir sus políticas de seguridad aplicando parches y jarding remotamente y obteniendo telemetría para identificar amenazas o compromisos de datos Pues esta empresa que se dedica a eso se dedica a gestionar flotas de dispositivos Apple de forma remota para que empresas grandes puedan mantener estos sistemas Apple seguros tiene un departamento que lo llaman streetlabs Pues un laboratorio que analiza Investiga amenazas de ciberseguridad pues este equipo ha documentado una nueva técnica de persistencia en iOS 16 que se podría usar para que las comunicaciones entre el malware de un iPhone infectado y su servidor de comer en control pasen desapercibidas y que así un atacante pueda mantener el acceso a un dispositivo Apple un iPhone incluso cuando la víctima cree que su teléfono está desconectado de internet Bueno y no solo de esto sino de toda red esta nueva técnica lo que hace es engañar a la víctima haciéndole creer que el modo avión de su dispositivo funciona es decir que después de activarlo su teléfono móvil se ha quedado sin conexión a redes inalámbricas que son WiFi Bluetooth y celular o bueno digámoslo así que incluye datos móviles llamadas y mensaje de texto no cuando en realidad el atacante después de haber conseguido comprometer el dispositivo de alguna forma en la que se ASUME que tiene digamos un forma de ejecutar código y que ha infectado el dispositivo de alguna forma pues ha colocado un modo avión artificial o falso que lo que hace es editar la interfaz gráfica de usuario del iPhone para mostrar el icono del modo avión ese avioncito pequeño que por defecto sale arriba a la derecha junto al icono de la batería y lo que hace es este modo avión falso es cortar la conexión a internet a todas las aplicaciones excepto obviamente a la aplicación spyware del atacante y os preguntaréis pero Alexis de qué magia negra se trata esto Como dirían algunos desarrolladores no es magia negra querido amigo es un no es un exploit es una ficher pero bueno la experiencia típica cuando el modo avión está activado es que aplicaciones Como por ejemplo Safari después de un tiempo de intento de conexión a la URL que queráis visitar muestra una ventana de notificación con el texto Safari no puede abrir la página porque tu iPhone no está conectado a internet aunque cuando vuelves a intentarlo de nuevo otras en otras ocasiones también la aplicación puede mostrar una ventana emergente o también que se conoce con el nombre de pop no con el texto desactivar el modo avión o utilizar Wireless Land la red WiFi para acceder a datos acompañado de dos botones uno que dice configuración no para acceder a la aplicación de configuración y bueno eso activar Desactivar modo avión utilizar la wirelesslam y otro que dice ok hasta aquí ya sabéis Cómo funciona el modo avión es un poco la mayoría lo ha usado y sabe cómo funciona pero quería dejarlo al menos dicho que para que sepáis el contexto de lo que voy a contar a continuación Cuál es el objetivo del modo avión falso pues por lo tanto después de habilitar el modo avión los usuarios esperan que la brisafari la aplicación no se pueda conectar a Internet obviamente de esta forma el objetivo del ataque es ideal el modo avión artificial que mantenga intactos los cambios de la interfaz de usuario O sea que muestre todo como si fuera un modo avión de verdad pero que conserve la conectividad celular para que un malware o programa espía pueda correr y utilizar la red de datos móviles de forma encubierta Los investigadores identificaron algo que les ayudó para

hacer esto y es que en el demonio digámoslo así o proceso com Center o centro de comunicaciones este este proceso usa una base de datos sql para registrar el estado de acceso a datos móviles de cada aplicación es decir hay una lista de todas las aplicaciones Safari aplicaciones no sé Gmail todas las aplicaciones de mensajería que tenéis y tienen un valor asociado si dicho valor es el número 8 Esto indica que la aplicación específica no se le permite el acceso a datos móviles entonces lo que haría un spyware o malware de estos móviles de iPhone sería bloquear el acceso a datos móviles de todas las aplicaciones Excepto a sí mismo o sea que se recorraría recorrería toda esta tabla en la base de datos Y pues pondría el valor 8 a todas las aplicaciones Excepto a sí mismo para llevar a cabo este digámoslo artimaña el código malicioso lo que haría es utilizar comunicarse con el Home Center para bloquear el acceso a datos móviles aplicaciones específicas y Mostrar lo que he dicho antes no el tema de cuando vas a una aplicación Safari de nuevo pues que salga mensaje de no se puede conectar a Internet o el popup que diga desactivar el modo avión utilizar Wireless para acceder a datos Ok esto lo hace para evitar sospechas podría no hacerlo pero queremos bueno el atacante Quiere pasar desapercibido el Center que es el que recibe la notificación que el modo avión se ha activado Y entonces lo que hace es desactivar la conexión a datos móviles notifica a otro componente en iPhone que se llama springboard que digamos sería la interfaz el programa que controla la interfaz visual del iPhone muestra es el encargado de mostrar la ventana emergente falsa que es bastante igual a las reales es se ve igual que la real y que de nuevo dice esto que he mencionado cuando se visita una aplicación que se le ha cortado el acceso a los datos móviles esto lo consiguen modificando o haciendo lo que se llama hooking a ciertas funciones específicas de springboard que se encarga de nuevo de mostrar estas ventanas emergentes Los investigadores de Jean han publicado un blog con detalles técnicos sobre Esta técnica y también un vídeo demostración y os los vamos a dejar ambos en las notas del episodio en el vídeo muestran un iPhone que puede capturar el vídeo de la cámara de otro iPhone infectado Y que cuando se activa el modo avión del iPhone infectado el iPhone el primer iPhone continúa recibiendo el Stream el Flow el vídeo en sí no sólo esto sino que también su malware algo interesante Desactiva el led esa luz que normalmente se enciende y sale verde arriba al lado de la cámara frontal selfie Así que no hay señal de que es este capturando vídeo a través de la cámara del iPhone y obviamente no hay no se puede determinar que se estén enviando datos a través de la red móvil algo me pareció curioso al ver este vídeo porque Los investigadores utilizan guantes de plástico tipo látex para hacer la demostración en este vídeo me pregunto si es por evitar que al ser vídeos de alta calidad alguien vaya a intentar obtener su huella dactilar de la pantalla de los iphones que salen en el vídeo y la utilicen en su contra pero es algo que me he ido encontrando recientemente en otros vídeos que investigadores de ciberseguridad utilizan guantes en vídeos de alta calidad de enfoque cercano como en vídeos de móviles no sé si vosotros queridos oyentes os habéis encontrado con lo mismo pero me ha parecido curioso cuanto menos mencionarlo voy a hablar sobre el impacto en unos tres escenarios distintos que se me ocurren tres o cuatro no el primero sería exfiltración de datos gracias a Esta técnica cibercriminales que hayan infectado vuestros teléfonos móviles podrían ex filtrar datos durante uno de vuestros sueños se dice de nuevo volviendo al mundo del dormir no de los sueños se dice que el adulto normal necesita unas 8 horas de sueño por lo que esto daría tiempo más que suficiente a un atacante para ex filtrar muchísimos datos de vuestros teléfonos y si tenéis vuestro teléfono con conexión 5g pues bueno ya ni os cuento muchísimos más datos en esas 8 horas que lo tenéis en modo avión porque Supongo que os vais a dormir y lo ponéis en modo avión el segundo escenario de impacto sería abuso como dispositivo espía el escenario es que vas tienes una reunión importante y vas a discutir temas confidenciales y pues si eres un poquito paranoico no pones tu teléfono en modo avión y con eso queda satisfecho porque

dices modo avión aunque tenga malware no me van a estar escuchando en tiempo real y Bueno pero si tu teléfono está infectado y los atacantes están utilizando Esta técnica te va a servir de poco porque como ya he dicho van a poder espiarte Igualmente a través de la red de datos móviles aunque tú pienses que esté en modo avión no te vas a enterar y el tercer escenario sería en seguimiento de personas no cuando una persona está en una relación Abusiva o tiene instalada una aplicación de seguimiento con consentimiento y quiere dejar de ser seguida o espiada por cierto tiempo algo que de todas formas seguro causa sospechas si lo determinas si se da cuenta la pareja espía digamos no conseguiría ser invisible activando el modo avión ya que los datos móviles seguirán funcionando Incluso si no se tiene una aplicación de seguimiento instalada con consentimiento y se tiene malware de seguimiento encubierto sucedería lo mismo un usuario podría Activar el modo avión y pensar que ya no se le puede rastrear pero nada más lejos te están siguiendo aunque tengas el modo avión activado y quieras un poquito hacerte invisible quiero recalcar de nuevo que Esta técnica es post explotación se le denomina así a técnicas que requieren que el atacante haya comprometido antes el teléfono móvil objetivo de alguna forma eso significa que te ha explotado el teléfono te ha instalado algún tipo de malware de alguna forma y luego utiliza Esta técnica para bueno para eso para hacerse pasar digamos para no levantar sospechas y conseguir seguir enviando ese datos y controlar tu teléfono a distancia en el pasado hemos hablado de exploits para teléfonos móviles y locaros que son por poder dar acceso a dispositivos que siempre llevamos con nosotros y que se pueden abusar como dispositivos espía Como he mencionado en los escenarios anteriores Y también hemos comentado que según empresas que trafican digámoslo así con exploits para móviles estos sobre todo los de acceso inicial son muy caros por ejemplo simperium ha mostrado web una tabla periódica de los exploits como digo yo en la que los exploits de día cero de cero clic para iPhone o Android están valorados en aproximadamente unos 2 millones de dólares y hemos explicado que el acceso inicial es algo que deberíamos dar por sentado la típica frase de cuando suceda el compromiso debería tomarse más en serio que la frase de si es posible El compromiso es decir no es el sí no es el si pueda ser posible porque posible es es el cuando te van a comprometer porque no hay nada 100% seguro de esta forma nos queda el partir de la base de que nuestro dispositivo se están siempre infectados y que para detectar la infección para detectar este caso en concreto Esta técnica de digamos de esconderse y no levantar sospechas y mantener el canal de comunicación abierto Incluso en modo avión lo que deberíamos hacer es prestar atención a las indicaciones muy sutiles de dicho compromiso y para ello como usuario final tenemos técnicas bastante poderosas y efectivas digámoslo así y esto lo hemos comentado en algún otro episodio cuando hemos hablado sobre todo de temas de pegasus y bueno y empresas similares no candiru y Intel Alexa y todas estas una técnica de detección sería Oye el teléfono se comporta de forma extraña algo algo le pasa ya podéis empezar a sospechar otro tema sería Oye aplicaciones nuevas instaladas que no tenía antes en mi dispositivo también se pueden esconder de alguna forma no así que esto bueno Son son ideas son técnicas que se pueden ir sumando una tras otra algunas pueden funcionar otras no pero yo os las voy mencionando también puedes decir Oye se me ha borrado alguna aplicación por algún motivo y igual no tiene espacio suficiente y el criminal ha tenido que borrar alguna de tus aplicaciones para instalar la suya tengo menos espacio de lo normal de mi móvil algo algo ha pasado aquí o la batería se descarga muy rápido estás un poco alto nivel genéricas de técnicas de detención como usuario normal que puedes puedes ponerte a mirar en tu teléfono móvil Pero en el caso particular de Esta técnica como digo de comunicaciones de datos móviles encubierta a través del modo avión falso algunas técnicas de detección específicas serían por ejemplo puedes hacer una captura de pantalla de la actividad y consumo de batería por aplicación en la sección

de configuración batería antes de Activar el modo avión y luego después de un rato o cuando te despiertes después de que ya no vayas a usar el modo avión y que vuelvas a utilizar tu teléfono de forma normal haces otra captura de pantalla de la misma de la misma sección y comparas actividad y consumo de batería y te fijas en diferencias ya que no debería haberlas o deberían ser minúsculas por ejemplo actividad en principio cuando tu teléfono no tiene conexión a internet no debería haber mucha digamoslo así por ejemplo en una como Safari o Gmail o similares no Y la otra técnica que me parece más interesante es monitorizar el consumo de datos móviles haciendo una captura de pantalla de la sección de configuración celular en inglés con si lo tienes en inglés o red celular si lo tienes configurado en español el iPhone antes de Activar el modo avión y otra después de desactivarlo habiendo dejado un periodo de tiempo entre ambos escenarios y comparar para de nuevo determinar si se ha incrementado el consumo de datos móviles porque esto te va a indicar que oye está en modo avión y estoy comparando El antes y el después con esta captura de pantalla y hay diferencias como puede ser esto también comentar que si el malware Es inteligente esto debería también ofuscarlo y no dejar que este este Contador se incremente que seguro que es algo que puede modificar pero en este caso la técnica de los de estos investigadores no no lo no lo consideran Por otra parte tenemos técnicas un poco digámoslo así más formales más profesionales o precisas como el proyecto Mobile verification tool kit del laboratorio de seguridad de amnistía internacional para el análisis forense de teléfonos móviles que ha ayudado a descubrir casos de infecciones de spyware como pegasus como ya hemos comentado en otros episodios Aunque Probablemente esta técnica sea utilizada por un grupo de usuarios más reducido no porque sea muy difícil de usar sino porque muchas veces el usuario final no tiene ganas de cacharrear Al fin y al cabo y bueno por eso quería comentarlas las otras anteriores que parecen técnicas más de a pie no Pero oye sobre todo la técnica de comparar el consumo de datos celulares antes y después de Activar el modo avión eso eso da si se ha modificado da que sospechar la moraleja de esta historia es que cuando estéis en una situación importante como una reunión en la que Vais a discutir temas confidenciales u os vayáis a dormir o no vayas a usar vuestros teléfonos móviles por tiempo extendido o queráis ser invisibles por un rato Es mejor que apaguéis vuestros iphones que ponerlos en modo avión o Mejor aún que los metáis dentro de una bolsa de faraday de esta forma os protegéis de este ataque bueno os protegéis hasta que salga la siguiente técnica que demuestre que aunque apagues tu iPhone este sigue encendido Y utilizando la red de datos móviles o incluso la WiFi o bluetooth y esto que digo está digamos última modificación o añadida a la técnica de encubierto no es del todo tan descabellado porque en otro episodio anterior hemos comentado que en las versiones de iOS más recientes que soportan la funcionalidad de localizar dispositivos mediante la aplicación encontrar dispositivos valga la redundancia los iphones que tienen esta funcionalidad habilitada sin siguen enviando su ubicación a iCloud durante las 24 horas siguientes después de su apagado y esto está en una página oficial de la web de Apple es decir que aunque apagues tu teléfono el teléfono todavía se guarda cierta parte tiene tiene cierta batería para o incluso cuando se apaga tu teléfono también que se le acaba la batería el iPhone es Está programado de tal forma de que se guarda un poquito de batería para seguir enviando tu ubicación hasta 24 horas siguientes a que lo hayas apagado o hasta que lo que le dure la batería que lo tenga o sea es decir que cuando está apagado todavía se sigue comunicando con la red celular bueno Y así os sigue traqueando así que es habría oportunidad de enviar datos incluso Aunque el teléfono esté apagado Sí de hecho Bueno A eso le sumas que no se puede quitar la batería del móvil y solo te queda lo de la jaula faraday que siempre hablamos da para usarlo de forma maliciosa pero también para usarlo de forma beneficiosa digamos para intentar encontrar el teléfono así que y como comentaba Esto está en la en la página oficial de Apple Así que eso es una

funcionalidad que está implementada de forma oficial Así que si el malware puede digamos aprovechar esto de alguna forma Pues también podría podría activarse podría seguir enviando datos incluso cuando lo apagues digamos de alguna forma y todavía haya batería obviamente De todas formas en la página que la vamos a poner también en las notas del episodio para los más paranoicos también menciona que esta funcionalidad se puede Deshabilitar obviamente de forma permanente yendo a configuración tu nombre encontrar Buscar mi iPhone y red de encontrar pero también se puede desactivar temporalmente para que no se envíe la ubicación del iPhone después de que se apague yo obviamente nunca me había fijado eso que va siempre rápido apagas el teléfono sin casi sin mirar no porque ya somos somos monos y sabemos hacerlo todo Sin mirar Pues cuando vas a pagar el iPhone que aprietas los dos botones no de arriba de los lados debajo de la línea que dice desliza para pagar en la que tienes que usar tu dedo no obviamente y hacer lo que dice deslizar de izquierda a derecha y así se apaga el teléfono se puede ver una pequeña línea de texto que dice iPhone localizable después de apagarse y al hacer clic ahí se muestra una ventana de popup con un texto que te explica que se puede desactivar el seguimiento temporalmente y un botón para activar esto que dice app encontrar desactivada temporalmente Y bueno pues eso si le das a esa a Ese botón pues se apaga tu teléfono y esto lo que hace es que tu ubicación nos envía Aunque tu teléfono esté apagado Pues nada espero que esto ayude a algunos a estar más protegidos sobre todo cuando cuando vayas a tener una una reunión con alguien importante en plan Putin o similares luego que no vaya a ser que os pase como el caso al líder de Wagner no y nada y que tengáis una una bolsita de faraday siempre a mano en el coche en la mochila del colegio en la mochila el trabajo y que pongáis el teléfono ahí para para estar protegidos Sí pues eso como no se puede sacar la batería al móvil es una fischer es una funcionalidad bastante guapa si te roban el móvil como a mí pero pero claro también tiene eso que sigue mandando datos no hay manera de sacar la batería ni nada Solo meterlo en el bolsillito Silent sea el enfoque de ese y como Martín lo que he comentado que se puede desactivar temporalmente tú te habías dado cuenta eso cuando apagas el móvil porque como yo digo yo nunca me había fijado no sé si tú te habías estado la verdad es que no porque sinceramente y a pesar de que no estaría mal ir apagando el móvil de vez en cuando por si te meto en un exploit o algo así es que yo apenas apago el teléfono entonces claro es rara vez veo yo ese mensaje porque en tu caso este de los que te robaron el móvil una de dos o les importaba un pimiento que le supiera donde estaban porque ya búscalos o o no saben de esta de esta función Porque si eres un ladrón vas y activa de eso y ahora sí que me busquen pero lo puedes Desactivar Sin poner el pin porque entonces es un poco absurdo es una medida de seguridad pero pues estoy bueno no lo pruebes ahora porque estamos en una llamada tuyo ahora pero luego y os invito a vosotros queridos oyentes hacerlo igual si lo apagas cuando acabe el episodio le das a los botones Cómo apagar y justo debajo del desplazar sale súper pequeño y en gris que casi no se ve y pone ahí lo que te digo pone exactamente iPhone localizable después de apagarse un texto totalmente no tiene sentido para para activar esta funcionalidad y luego le das y hay un botón un texto grande y un botón que pone app encontrar desactivada temporalmente que tampoco tiene sentido gramatical así la frase Pero bueno no tiene espacio y ahí le das ahí y en principio Pues no te envían no Envía tu ubicación del teléfono cuando se apaga para mí esto es que no tiene ningún sentido o sea meto una funcionalidad de seguridad que luego a la vez puedo Desactivar o puede desactivar cualquiera Qué raro sí no sé si debe ser para casos como digo más de tema de seguimiento o de relaciones abusivas estas en plan voy a desactivarlo por unos minutillos porque si lo desactivas de seguimiento en plan este en plan con tu familia no con un grupo de con quien sea creo que la otra persona debe recibir una notificación de que este iPhone la ubicación de este iPhone ya no se comparte pero si haces esto pues no están puedes decir Oh

se me quedó sin batería o algo así igual la otra persona no sabe que siempre se envía la ubicación sabes y igual es para eso me pregunto por siempre hay temas de estos de abuso de personas y tal Sí pero bueno entonces no lo vendas como un mecanismo de seguridad porque si no es absurdo Sí sí así que bueno igual hemos destapado aquí una una técnica que no deberíamos destapar Pero bueno hay que todo lo tiene que saber Bueno pues hasta aquí el episodio por hoy ya estamos los dos de vuelta esperemos que os haya gustado se va acabando el verano Aunque todavía le queda y más con el cambio climático que aquí no no para el calor disfrutarlo escuchando tierra de hackers una cervecita en la playa o un café con hielo si no bebéis lo importante es que os mantengáis informado y bueno si es con nosotros pues mejor que mejor y ya si nos dejáis una review cinco estrellitas donde nos escuchéis un comentario o se lo comentáis algún amigo mejor que mejor Muchísimas gracias por estar ahí con nosotros durante el verano muchísimas gracias y se lo dice Martín tomamos una nuestra salud y nos escuchamos en la siguiente Adiós adiós Chau 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