agencias gubernamentales internacionales están pero conseguimos encajar un episodio más de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 21 de diciembre de 2023 es el episodio número 114 yo soy Martín vigo y no está esta vez en directo conmigo Alexis porros pero aún así dará su noticia Alexis qué tal estás pues muy buenas Martín aquí estamos otro episodio más episodio tras episodio con nuestros queridos oyentes ya muy cerquita de las navidades espero que todos los que nos estén escuchando estén cerrando los últimos detallitos para poder pasar unos buenos días con sus seres queridos durante esta Navidad y nada mejor que prepararse que escuchando este episodio para saber qué software actualizar En qué dispositivos aplicar parches Y cómo mitigarlos riesgos más recientes que os vamos a contar y sentirse un poquito más ciberseguro durante la navidad sin más os cuento que os podéis integrar más en la comunidad de Tierra de hackers primero siguiéndonos en redes sociales donde nos encontráis como tierr deeh hackers o @ tirad hackers segundo suscribiendo a tierrade hackers en cualquier plataforma de podcast la que sea vuestra favorita y tercero participando en nuestro canal de discord donde podéis entrar vía tierrade hakers.com brd discord y yo antes de comenzar la noticia como siempre darle las gracias a nuestros mecenas de patreon y en concreto esta semana a la persona que se acaba de unir a la familia de patreon overc Muchas gracias por aportar a este proyecto que nos dedicamos en tiempo y forma Alexis y yo incluso trabajando en época estival Muchas gracias por estar ahí y si te interesa formar parte apoyarnos ya sabes patreon.com bartierra de hackers o tierrade hackers.com barpo como lo prefieras la cuestión es que podamos seguir adelante haciendo este proyecto trayéndolo gratis a todo el mundo y seguir informando a toda la gente sobre este mundillo de la ciberseguridad también por supuesto No Sería posible este podcast sin nuestros sponsors y esta semana tenemos a 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 dañada e incluso a borrar la huella digital que dejamos online no Solo han decidido Apoyar el podcast sino que si le contáis que venís de parte de tierra de hackers tendréis un descuento especial en sus servicios si necesitas algún tipo de ayuda con vuestra identidad digital on branding es lo que estás buscando visita on brandings on nbr andi on brandings queremos 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 monat 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 echadle un vistazo a su web monat.com y mandad vuestro currículum a tirad hackers @mon at.com mad.com y ya damos paso a la primera noticia hoy os voy a comentar sobre una nueva manera que de espiarnos que tienen los gobiernos y agencias y que acaba de salir a la luz y que conocemos también gracias una vez más he de decir a una filtración anónima hecha nuestro querido senador estadounidense ron weiden son Ya varias las noticias que os hemos reportado aquí en tierra de hackers y que tienen su origen en el hecho de de que alguien observa algo que no está bien y tira de este mecanismo de comunicación anónima del que dispone este senador que está tan centrado en mantener no en control el alcance de la monitorización masiva por parte del gobierno y agencias estadounidenses la semana pasada el senador enviaba una carta pública al ministro de Justicia de los Estados Unidos merrick Garland donde describía como como agencias eh extranjeras estaban pidiendo acceso a las notificaciones Push tanto a apple como a Google las notificaciones Push como ya sabéis son

esos mensajes de alerta que nos envían las aplicaciones al móvil y que suele incluir información breve sobre la naturaleza de la alerta cuando te llega el u recibes una de estas notificaciones cuando te llega un WhatsApp puedes ver pues parte del mensaje que te llegó en esa notificación cuando pides comida y está a punto de llegar ya sabéis pues según la carta de ron weiden a este le preocupa no solo que las agencias internacionales estén haciendo peticiones a apple y Google para obtener información de las notificaciones enviadas a personas específicas sino también destaca el secretismo detrás de esta práctica comenta que al ser Apple y Google los únicos que pueden transmitir estas notificaciones se convierte en un cuello de botella muy jugoso por donde pasan millones de alertas diariamente dirigidas a las personas con información que puede llegar a ser sensible cualquier aplicación de iOS por ejemplo tiene que usar el servicio de Apple Push notification para integrar notificaciones y tres cuartos de lo mismo con Google mediante su propio sistema de notificaciones firebase Cloud messaging y aquí viene lo peliagudo según la carta de ron wien el equipo de este senador contactó a apple y Google para saber más sobre Qué es exactamente lo que están entregando estas empresas a los gobiernos sin ningún tipo de orden judicial y la respuesta fue la siguiente y cito textualmente la información respecto a esta práctica está fuera del alcance del conocimiento público según exigencia del gobierno toma ya Estados Unidos ha prohibido a apple y Google hablar o dar a conocer que las agencias están haciendo peticiones y obteniendo información de usuarios a través de los datos que se recolectan al procesar las notificaciones Push esto es especialmente importante porque tanto Apple como Google tienen un reporte anual de transparencia donde donde publican abiertamente todas las peticiones hechas por gobiernos en todo el mundo con respecto a datos de sus clientes es decir nosotros por supuesto en la mayoría de los casos Si no todos esto viene dado y justificado por investigaciones policiales para resolver o investigar algún tipo de crimen pero está Genial que las empresas publiquen reportes con estadísticas y detalles de ello para que sepamos por ejemplo Pues si está habiendo un incremento de peticiones si se está abusando este mecanismo Y bueno pues siempre está bien tener esta información de manera pública por ejemplo según la web de transparencia de Apple que os dejo un enlace en las notas del episodio y que por cierto Está muy muy bien pues me voy a España y entre enero y Julio de 2022 que son ahora mismo los datos más actuales que aparecen en la web de Apple Apple le han hecho esto en España eh 1206 peticiones en base al identificador del dispositivo es decir el el email no 890 peticiones en base a información financiera esto es pues por ejemplo que la policía tendría pues la información de una tarjeta de regalo de iTunes que a lo mejor se utilizó para temas de fraude eh que y que llevan identificadores únicos También tenemos 79 relacionadas a cuentas de iCloud esto se hace pues entregando un email no por ejemplo Entonces ese email le preguntan Apple se ha registrado alguna cuenta de iCloud y con iCloud pues ya tiene mucho más métricas de información que ya pues puede servir para una investigación y otro dato muy relevante es que se han hecho tres peticiones de emergencia y Apple lo describe así las peticiones de emergencia son casos en los que hay una vida en peligro inminente o una catástrofe a punto de ocurrir y se requiere que Apple entregue información con la mayor brevedad posible Pues en en la primera mitad del año de 2022 en España hubo tres peticiones de este tipo pues aparte de lo curioso de estos datos que además arrojan más luz sobre los potentes que son nuestros dispositivos móviles para averiguar información sobre nosotros volviendo al tema que nos concierne en esta noticia lo que sucedía es que Apple no se le está permitiendo tampoco incluir en sus reportes de transparencia las peticiones de gobierno solicitando información de notificaciones Push enviadas a los usuarios Apple y Google dan información sobre Cuándo se envió una notificación Push en particular Qué aplicación la envió a quién se la envió y la información de la cuenta de iCloud o de Google del usuario la carta menciona también que hay

instancias en las que las notificaciones no están cifradas y por tanto los gobiernos y agencias podrían llegar a obtener Incluso el contenido de la notificación que realmente es lo más sensible aún así para tampoco alarmar demasiado esto lo dejan más como un hipotético esto de de acceder a lo que es el contenido la norma es que lo que obtienen son los metadatos no el contenido en sí y con esto en mente por qué debería preocuparnos esto dejando a un lado por un segundo que quizás podrían Acceder al contenido de la notificación Push Cuál es el drama de que gobiernos y agencias de inteligencia puedan acceder a los metadatos de las notificaciones que recibimos recordemos hora de cuando la recibimos nuestro identificador de iCloud o Google qué app está enviando la notificación ese tipo de información Bueno pues este es un ejercicio de threat modeling no de modelado de finanzas pensemos en aplicaciones que podría la gente tener instaladas cuyas notificaciones serían especialmente sensibles y por tanto con los metadatos específicamente pues podrías llegar a ser muy revelador no se me ocurre por ejemplo aplicaciones de alarmas inteligentes en hogares normalmente pues recibes una notificación cuando armas y desarmas la alarma alguien con acceso a esto podría saber en tiempo real Cuando está en casa y cuando no estás en casa otra que se me ocurre según preparaba la noticia son las notificaciones de los relojes inteligentes como Apple watch que monitorizan y te alertan si te sube el ritmo cardíaco de manera que podría tratarse de un problema de corazón que requiere atención médica recordemos parte de los metadatos es Qué tipo de notificación te llega entonces pues aquí ya pues se podría saber el pues idades de la salud de su usuario no esto en cuanto digamos a saber la hora de Cuándo se mandan notificaciones y de qué aplicación se trata pero solo con el hecho de saber qué aplicaciones te mandan notificaciones sin ni siquiera el tema de la hora se sabe qué aplicaciones utilizas y cuáles tienes instaladas Qué pasa si tienes aplicaciones instaladas Pues de temas de salud muy específicos no sé yo no soy usuario de de dichas Apps Así que dejo volar mi imaginación aquí Pero supongo que hay aplicaciones que te ayudan Pues a dejar los malos hábitos como drogas o no sé otro tipo de aplicaciones como problemas de Salud Mental o notificaciones para mujeres que alertan sobre sus ciclos de menstruación ya me entendéis temas pues sensibles relacionados con la salud o otras aplicaciones que pueden ser reveladoras como pues una para saber dónde está la Meca y así rezar en dicha dirección como requiere las costumbres de de esta religión o aplicaciones para leer El Corán de otras noticias que cubrimos en el podcast sabemos que este tipo de aplicaciones existen pues imaginaros esto podría ser muy interesante para agencias de inteligencia saber qué usuarios tienen instaladas este tipo de aplicaciones Yo es que como no tengo instaladas muchas aplicaciones porque tiendo a utilizar la versión web de los servicios que por temas de privacidad hago eso ya que recolecta menos métricas pues la verdad me falta un poco aquí de sabiduría pero vamos que hoy en día hay aplicaciones para absolutamente todo así que os dejo a vosotros el ejercicio de pensar en aplicaciones peligrosas Por así decirlo en cuanto a tener instaladas en el contexto de que el conocimiento de metadatos sobre las notificaciones para esa aplicación podría llegar a ser un riesgo contra la privacidad o incluso seguridad donde yo veo el máximo valor para para agencias de inteligencia y fuerzas y cuerpos de seguridad es en poder utilizar este mecanismo de vigilancia para de anonimizar a usuarios de aplicaciones específicas me explico cojamos el ejemplo de un usuario anónimo que bajo un pseudónimo está publicando en alguna red social pues me pongo en el extremo propaganda Pro terrorista lo único que tiene la agencia o las fuerzas y el cuerpos de seguridad es el nombre de usuario de esa cuenta que está haciendo dichas publicaciones la agencia se va a apple o Google y pide información de las notificaciones enviadas por esta aplicación a ese usuario y ahora Apple y Google pueden ver qué cuenta de iCloud o Google está asociada al teléfono que está recibiendo las notificaciones y por tanto ahora ya tienen más información de la que tenían antes en el mejor de los casos el objetivo utilizó pues su nombre

real para crear la cuenta de iCloud o Google y Bueno pues en el peor de los casos tien un correo electrónico para seguir investigando o sea de un seudónimo han llegado un correo electrónico que fue el utilizado para registrar la cuenta de iCloud y ya nos queda la última parte de lo que planteaba es realmente un riesgo esto tiene algún valor real para el espionaje bueno como sabéis siempre que puedo me gusta daros prácticos después de explicaros digamos un poco la parte teórica me gusta daros ejemplos prácticos y reales y no dejar las cosas solo en en el lo hipotético y esta vez encontré como ejemplo una orden de registro metida por el FBI de 2021 donde explícitamente se pide acceso a los detalles de las notificaciones Push de dos cuentas relacionadas con Facebook y que por supuesto os dejo las notas del episodio para que le echéis un vistazo a a esta petición del vibi yo os Leo la parte relevante de la orden de registro porque es bastante larga concretamente la sección 1h respecto que que es respecto a todo el material al que se pida acceder dice así todos los registros pertenecientes a los dispositivos asociados con la cuenta y Software utilizados para crear y acceder a la cuenta incluyendo números de serie números de instrumentos tipos números de modelo identidades internacionales de equipos móviles lo que viene siendo el emeil identificadores de equipos móviles el mate identificadores únicos globales lo que se conoce como guit números de serie electrónicos el sn identificadores de dispositivos Android números de teléfono direcciones Mac información del sistema operativo información del navegador información de la red móvil información sobre cookies y tecnologías similares y atención y cualquier otro identificador único que ayuda a identificar cualquier dispositivo de este este tipo incluyendo números de aplicación únicos y tokens de notificación Push asociados con la cuenta incluyendo notificaciones Push de Apple mensajería en la nube de Google servicios de notificación Push de Microsoft servicios de notificación Push de Windows mensajería en dispositivos Amazon mensajería en la nube de firebase lo que es el fcm y mensajería en la nube de baidu vamos el paquete completo de todas las tecnologías de notificaciones Push para que todos los para todos los fabricantes que existen O sea no no se dejan ni uno yo ni sabía que que baidu también tenía tecnología Push os dejo también en las notas del episodio el blog de un desarrollador francés que habla de sus frustraciones con las notificaciones Push pero más importante Cómo se da el caso que incluso pueden estar violando la ley vigente en Europa en términos de protección de datos el gdpr Me parece que vale la pena leer su perspectiva Y además sugiere que al igual que pasa con las cookies hay que alertar a los usuarios con un mensaje como bueno como el que pone el que como ejemplo si tú si desarrollas una aplicación y mandas notificaciones ya que recordad tienen que pasar por Google o Apple forzosamente y él sugiere Pues digamos igual que con las cookies avisar de esta manera las aplicaciones Push utilizan servidores de terceros proporcionados por tu teléfono inteligente no podemos garantizar que los datos personales no puedan ser transferidos transferidos fuera de la Unión Europea y no podemos proporcionar garantías adecuadas al activar esta función comprendes los riesgos y das tu consentimiento para esta transferencia internacional de tus datos personales de acuerdo al artículo 491 del reglamento general de protección de datos O sea que imaginaos si hay información relevante en las notificaciones Push que este desarrollador está alertando que incluso puede llegar a incumplir la ley Europea de protección de datos Bueno ya para terminar la noticia hay algo positivo en todo esto Gracias a la carta de ron weiden apel ha declarado lo siguiente y y esto lo cito textualmente el Gobierno Federal nos prohibió compartir cualquier información y ahora que este método se ha vuelto público estamos actualizando nuestros informes de transparencia para detallar este tipo de solicitudes y yo Por supuesto me fui a ver si era cierto y efectivamente han añadido un párrafo que especifica Qué información referente a los Push notifications puede ser obtenida mediante una orden judicial y Google ha hecho lo mismo así Que supongo que tenemos que agradecer a a Don wien que a pesar de que

que todavía se puede tener acceso a esta información por lo menos ya no es un secreto y además aparecerán los reportes de transparencia de ambas empresas algo que podéis hacer para defender no entre comillas de esto es simplemente pues no habilitar las notificaciones de aplicaciones que consideráis más críticas o como os comentaba que hago yo optar por la versión web en vez de descargarte la aplicación a veces la funcionalidad bueno puede ser un poquito más reducida pero hay servicios que van muy bien usándolos desde el navegador web de todas formas ya os digo que esto es un caso muy concreto y y dudo que ninguno de nuestros oyentes tenga que temer o meter en su en su modelo de riesgos que un gobierno vaya por sus notificaciones Push pero nunca está demás saber que toda de todas las maneras en las que nos espían y podéis estar seguros de que en tierra de hackers os Seguiremos informando por muy rocambolescas que sean estas estas maneras de espiarnos fascinante la noticia Martín como ya comentado muy interesante y nada seguimos con la siguiente noticia y os traigo algo una vulnerabilidad un ataque de tipo cero click que un investigador ha publicado recientemente la semana pasada que permite inyectar pulsaciones de teclado a través de bluetooth contra dispositivos Android iOS macos y Linux Android ya sabéis que corre teléfonos móviles y tablets al igual que iOS en móviles iPad os también en tablets macos Bueno lo tenemos en macbooks y Linux en donde lo queráis correr No pues esta vulnerabilidad es Me parece muy importante porque como digo es de cero clic no hace falta que la víctima haga nada Solo contener Bluetooth activado eh es posible lanzar este ataque Aunque en algunos sistemas operativos Hay algún otro requisito y hay varias formas de protegerse también de este ataque dependiendo de como digo el sistema operativo una es parche aplicando la última versión haciendo vuestro dispositivo Bluetooth invisible o desactivando el bluetooth completamente en algunos casos Esto no es viable porque si estás utilizando tus airpods por ejemplo para escuchar y conectarte a una a una reunión eh A través del teléfono pues no te va a ser fiable a no ser que tengas unos auriculares con cable Así que iríamos un poquito hacia el pasado así que bueno os lo dejo aquí la intro seguid escuchando y os cuento en detalle pero antes de entrar de lleno en esta noticia os quiero contar sobre otro ataque muy similar que surgió en 2016 llamado Mouse Jack y que está muy relacionado con esta noticia sobre eh ataques de inyección de pulsaciones de teclado en dispositivos vía Bluetooth y que me parece interesante comentarla primero para que sea más fácil de entender la noticia nueva sobre Bluetooth que os traigo ahora algunos igual os acordáis de de este ataque que surgió como digo en 2016 pero para los que no os refresco Mouse Jack es una colección de vulnerabilidades que afecta a ratones y teclados ambos inalámbricos de al menos siete fabricantes y que puede permitir a un atacante tomar el control de forma remota de los dos tipos de dispositivos el ratón y o teclado inalámbrico vulnerable es uno de esos que viene con un dongle USB Wireless o También conocido como receptor USB inalámbrico este receptor USB está conectado físicamente a un sistema como un portátil oon o un ordenador de sobremesa y a su vez se comunica con el ratón y o el teclado de forma inalámbrica como digo y así si se mueve el ratón o haces clic con sus botones las coordenadas de movimiento y las acciones con los botones son enviadas vía radio al receptor USB que a su vez las comunica al sistema Al que está conectado y lo mismo sucede si presionas teclas en el teclado se se envían vía radio y el dongle USB las recibe y las comunica al sistema Al que está conectado este ataque funciona enviando señales de radio especialmente diseñadas a dicho receptor USB inalámbrico lo que permite como digo inyectar pulsaciones de teclado en el sistema Pero cómo funciona realmente este ataque voy a comentarlo brevemente y alto nivel pero el tema es que este ataque se nutre de tres vulnerabilidades distintas la primera es el emparejado forzado los dongles USB permiten emparejar a ratones y teclados inalámbricos a través del proceso de emparejamiento en el que el usuario tiene que apretar algún botón en el dispositivo y esperar a que el dongle reconozca

dicho dispositivo y establezca la comunicación Supongo que lo habréis hecho alguna vez le dais la vuelta al ratón o al teclado y hay un botoncito y hay una Lucecita un led no que se enciende parpadea y ahí se establece se empareja el ratón o teclado con el dongle USB pues este proceso es posible del tipo de dispositivo el problema con estos dongles USB es que algunos de ellos no distinguen entre paquetes radio enviados por un ratón o por un teclado Así que si de alguna forma un atacante puede crear paquetes de teclado y enviarlos a un dle USB de ratón este dongle USB los va a aceptar y la última vulnerabilidad es un fallo en el requisito decifrado en paquetes o comunicaciones enviadas por un teclado normalmente durante su fabricación se instala una clave de cifrado en los teclados inalámbricos que está asociada con la clave decifrado que está dentro del dongle USB para que de esta forma se puedan enviar pulsaciones de teclado de forma cifrada en este caso El problema es que muchos de estos dongles USB no requieren que los paquetes enviados por teclados estén cifrados Así que se pueden enviar pulsa de teclado sin cifrar Total que se puede suplantar a un teclado inalámbrico emparejarlo con un dongle USB de forma forzada y enviar pulsaciones de teclado a cualquier tipo de dongle USB ya sea de un teclado o de un ratón inalámbrico con un ataque como este teniendo el control de forma remota del teclado e incluso del Ratón de un dispositivo Es como estar físicamente delante del mismo y Por tanto se podría a realizar cualquier acción maliciosa que pudieras hacer si estás delante de dicho dispositivo Como por ejemplo desplegar técnicas de persistencia digamos Bueno voy a crear un usuario malicioso y así eh más adelante puedo conectarme de forma remota con este usuario podría también instalar una puerta trasera tipo troyano O spyware podría instalar pegasus o temas más eh Open source no Digamos como yo que sé un meterpreter un situ eh que los hay muchos también Podría buscar y ex filtrar documentos confidenciales también podría desplegar ransomware no O Eliminar todos los datos del sistema dejar el sistema Incluso inutilizable si voy más allá y borro un poquito el tema del Master Boot record bueno creatividad al poder vamos ya Supongo que ya veis un poco el impacto de este ataque Los investigadores de seguridad de la empresa basti networks entre ellos newlin que publicaron los detalles de este ataque demostraron que podía funcionar a una distancia de hasta 100 m usando un dispositivo malicioso inalámbrico bastante barato de unos 15 que ellos mismos prepararon y que podían llegar hasta 200 m con un equipo algo más caro que incluía una antena direccional lo interesante es que se puede llegar a una velocidad de inyección de pulsaciones de teclado de hasta 7000 15 por minuto o una pulsación cada 8 milisegundos esto es una velocidad suficiente para escribir de forma remota una línea en powershell o en el lenguaje específico del sistema operativo atacado para lanzar una una conexión inversa o una revers shell una conexión a un command and control o crear como dicho un usuario malicioso las otras ideas de de impacto para aquellos que quieran revisar los detalles de mouse Jack os pongo varios enlaces el primero es a la página web Mouse jack.com ahí hay varios enlaces del White paper en formato pdf y también os voy a poner el vídeo en YouTube de la presentación de mouse Jack de la defcon 24 brevemente para aquellos más curiosos os comento que los fabricantes afectados son del HP Lenovo gigabyte Microsoft y en su web mj.com tienen un enlace a la lista completa de dispositivos afectados cuando escribía sobre este ataque mous Ja me vinieron a la mente otros dispositivos que permiten ataques muy similares a maus y aquí os los quería comentar también para que estuvierais al tanto probablemente muchos de vosotros conozcáis el dispositivo rubber ducky lo hemos comentado en episodios anteriores pero os lo refresco el rubber ducky es un dispositivo USB que parece uno de esos pens usbs o memoria USB pequeña que está cargado con un Script específicamente creado para hacer impacto para ser malicioso que inyecta pulsaciones de teclado al sistema al que se conecta vía USB y luego igual conozcáis el dispositivo omg cable que es un cable que a simple vista parece un cable normal un cable de estos tipo usba a o usbc

micro USB o incluso cable lining de esos como los cables que se utiliza para cargar los iphones o ipads los antigüos no pero Eh no lo es no es realmente un cable para cargar este tipo de dispositivos porque al igual que el rubber ducky está cargado con un Script malicioso que inyecta pulsaciones de teclado al sistema al que se conecta lo interesante es que tanto del rubber ducky como del omg cable hay versiones Wireless que incluyen un módulo radio al que se puede conectar el atacante de forma remota e inyectar comando de forma inalámbrica siempre y cuando esté dentro del alcance radio pues este ataque Mouse Jack combina ambas capacidades la de inyectar pulsaciones de teclado contra el sistema atacado en este caso al que esté conectado el rubber daky el omg cable y la de ser inalámbrico porque no se tiene que desplegar ningún dispositivo malicioso contra el sistema objetivo lo que se hace lo que aprovecha este ataque Mouse Ja es el el USB que está directamente conectado al sistema Así que muchas veces igual e cuando viajamos nos ponemos el portátil en la mochila y dejamos el dongle USB conectado al dispositivo eh Si en algunos casos el ordenador no se apaga completamente y está todavía en standby porque hay algunas veces que estás instalando algo y y no se cierra no se digamos suspende de forma completa pues eh No lo estáis mirando y un atacante podría estar haciendo de las suyas Mientras tu portátil está en la mochila así que sería algo en lo que tendríamos que pensar cuando estemos viajando y pongamos el portátil en la mochila quitemos el dle USB o asegurémonos de que el portátil esté suspendido o esté al menos cerrado digamos bloqueado para protegerse del ataque Mouse Jack se puede hacer lo siguiente lo primero es que si se tiene un dispositivo de los incluidos en la lista de afectados y se quieres seguir utilizando habría que actualizar el firmware de dichos dispositivos si es que se puede lo segundo y algo mejor incluso es no utilizar Ninguno de los dispositivos inalámbricos afectados como digo tenéis la lista en la página web de mous ja.com y lo mejor es utilizar ratones y teclados Bluetooth ya que no son vulnerables al ataque Mouse Jack O al menos Esto es lo que sugería el investigador de seguridad que publicó Mouse Jack en su momento en 2016 y eso es lo que pensaba hasta que se publicó este nuevo ataque de inyección de pulsaciones contra dispositivos Bluetooth porque esto ahora cambia entonces Os estaréis preguntando qué podemos utilizar ahora no pues un poquito esperad hasta el final de la noticia que os comento este nuevo ataque como digo contra dispositivos Bluetooth se publicó la semana pasada el 6 de diciembre y lo publicó el mismo investigador de seguridad que publicó el ataque Mouse Jack que se llama Mark newlin pero ahora trabajando para otra empresa en este caso skysafe Cuál es la vulnerabilidad en Sí pues la esencia del problema es el emparejamiento forzado de nuevo una de las vulnerabilidades que el ataque Mouse Jack utilizaba y que os recuerdo que es el proceso mediante el que se puede obligar a un sistema vulnerable a conectarse en este caso a un teclado Bluetooth malicioso sin necesidad de confirmación del usuario de la víctima en este caso evitando las comprobaciones del protocolo Bluetooth del sistema operativo os habréis fijado que en vuestros sistemas modernos para conectar o emparejar un teclado Bluetooth tenéis que iniciar dicha conexión de forma activa primero poniendo en modo emparejado el dispositivo luego yendo al menú o aplicación de Bluetooth de vuestro sistema dejar que dicha aplicación escanee el aire en busca de dispositivos Bluetooth en modo emparejado y elegir dicho dispositivo para que se complete el emparejado bien pues el protocolo Bluetooth especifica una función de conexión no autenticada que ciertos sistemas operativos no implementan de forma correcta y es lo que un atacante puede abusar para inyectar las pulsaciones de teclado en este caso vía Bluetooth y que se han publicado en esta vulnerabilidad no se necesita ningún equipo especial para lanzar este tipo de ataque el investigador comenta que simplemente un un sistema Linux y un adaptador Bluetooth estándar es lo único que se necesita esto es bastante alucinante porque no necesitas el típico dispositivo Bluetooth medio avanzado que te permite indar paquetes bluetooth al más bajo

nivel del protocolo como podría ser el ubertooth one y o el otro Crazy radio que se utilizó en su día en el ataque Mouse Jack sino que cualquier adaptador Bluetooth sirve esto se traduce en que cualquier de nosotros con cualquier equipo que tengamos en casa porque instalar Linux lo podemos instalar en casi todos los sistemas y Bluetooth los sistemas modernos prácticamente todos vienen con Bluetooth Así que todos podríamos ser sospechosos no de de poder lanzar este ataque básicamente o digamos que podríamos tener la capacidad el equipo necesario para lanzar este ataque con equipo normal Este ataque puede funcionar a una distancia de hasta 10 10 m por el tema de que es Bluetooth si se utilizan antenas mejores un poquito más caras pues se podría extender un poco más el alcance esta vulnerabilidad os voy a comentar afecta a las implementaciones del protocolo bluetooth en Android macos iOS y Linux os voy a comentar cada una de ellas en detalle el investigador probó siete teléfonos Android con diferentes versiones del sistema operativo de Google probó en un Pixel 7 con Android 14 Pixel 6 con Android 13 Pixel 4a con Android 13 Pixel 2 con Android 11 Pixel 2 con Android 10 Nexus 5 con Android 6.0.1 y Blue Dash 3.5 con Android 4.2.2 este sistema operativo Android está disponible desde 2012 Así que desde entonces es increíble esta vulnerabilidad existe desde hace prácticamente 12 años lo que os quería decir es que todos estos dispositivos y versiones de Android son vulnerables a este ataque Bluetooth además en este caso para Android todo lo que se necesita para materializar este ataque es que Bluetooth esté habilitado en el dispositivo Android objetivo sin importar si está en modo visible o no eso es cuando desde otro dispositivo Bluetooth puedes identificar tu dispositivo si está en modo visible o no Porque lo tienes en modo invisible digamos pues no importa en qué modo esté visible o invisible es vulnerable mientras tenga Bluetooth activado Lo bueno es que el investigador informó a Google sobre esta vulnerabilidad a principios de agosto quien ya lanzó parches para las versiones de Android desde la 11 hasta la 14 el parche está disponible desde el 5 de diciembre un día antes de que se publicara la vulnerabilidad y Google comenta que comunicó estos parches a fabricantes de teléfonos y tablets El problema es que no hay parche disponible para la versión de Android 4 2.2 esa de hace 12 años Así que tenéis dicha versión Pues pensadlo si queréis seguir utilizando dicho dispositivo sobre sistemas de Apple el investigador pudo confirmar que la vulnerabilidad se puede explotar en iphones se con iOS 16.6 así como en dos versiones de macos corriendo en macbooks una la probó en macbook pro del 2022 que corría macos Ventura 3 1.3.3 en un procesador Arm m2 de Apple y el otro caso fue un macbook Air de 2017 con macos Monterrey 12.6.7 que corría en un procesador Intel el investigador comenta que no tenía tantos dispositivos Apple a mano como Android Así que no pudo determinar si la vulnerabilidad afecta a dispositivos que corren iPad os TV os y o watch os ipads Apple tvs y los Apple watches lo interesante del ecosistema de Apple Es que la funcionalidad de lockdown Mode o modo de bloqueo en la que muchos usuarios confían que hemos comentado en algún otro episodio anteriormente que protege en principio sobre ataques spyware pegasus candiru todos estos no protege contra ataques que explotan esta vulnerabilidad de bluetooth esto aplica a iOS y ipads obviamente pero también a co es ya que a pesar de que el lockdown Mode fue creado para dispositivos móviles como iphones y ipads y fue introducido en iOS 16 el 12 de septiembre del año pasado y en Ipad os 16 el 24 de octubre ahora también está disponible para macos desde Ventura Es decir desde el 24 de octubre del año pasado la misma fecha de la Release de iPad os 16 lo digo porque yo no me había enterado de esto y no sé si alguno de vosotros osotros queridos oyentes lo sabíais así que bueno si también tenéis dudas de si os están intentando atacar vuestro macos ventura en adelante podéis activar el lockdown Mode en vuestros macbooks pero que sepáis que no os va a poder proteger contra este ataque Bluetooth afortunadamente para que este ataque sea exitoso se requiere de una condición adicional además de tener el bluetooth habilitado Y es que el dispositivo objetivo debe haber estado

emparejado previamente con un Apple Magic Keyboard esto significa que los ataques de bluetooth contra dispositivos Apple representan una amenaza contra sistemas que se utilizan con un teclado inalámbrico en este caso Apple Magic Keyboard que es algo que se da más a menudo en sistemas que corren macos lo digo porque normalmente un Apple Magic Keyboard se utiliza en dispositivos un poquito más grandes no eh normalmente no utilizas un Apple Magic Keyboard en un iPad o un iPhone porque directamente escribes en la pantalla Por tanto la probabilidad de que un iPhone sea comprometido a través de esta vulnerabilidad parece un poquito remota ya que normalmente usuarios de iPhone como digo no utilizan teclados Apple Magic Keyboard con sus iphones directamente escriben en la pantalla Así que en resumen si no habéis emparejado anteriormente un Apple Magic Keyboard a vuestros dispositivos Apple estáis a salvo de este ataque el investigador no lo firma pero se podría pensar que si se elimina el Apple Magic Keyboard de la lista de dispositivos Bluetooth emparejados Oye igual el dispositivo Apple objetivo deja de ser vulnerable pero esta es una hipótesis y como digo no está confirmado lo que sí que es cierto es que Apple dijo que arregló esta vulnerabilidad en las versiones de iOS 17.2 iPad os 17.2 y macos Sonoma 14.2 esto confirma de forma silenciosa que los ipads corriendo iPad os antes de la versión 17.2 también son vulnerables a este ataque Gracias Apple por dejarnos lo saber de forma sigilosa como lo has hecho en el entorno Linux el investigador determinó que este ataque también afecta a Blue en concreto que es la pila Bluetooth incluida en el kernel oficial de Linux es el componente del kernel de Linux que gestiona todo el tema comunicaciones conexiones emparejamiento de dispositivos Bluetooth en concreto bluth es vulnerable en las versiones 18.04 20.04 22.04 y 23.10 de ubuntu Linux el investigador Comenta que la vulnerabilidad que descubrió en Linux fue parcheada el año 2020 pero la solución estaba deshabilitada de forma predeterminada en las distribuciones de Linux más populares como ubuntu devian fedora hentu arch y alpine es decir que esto se había arreglado pero estaba desactivado estaba deshabilitado según Google Chrome os fue la única distribución que habilitó por defecto esta solución a esta vulnerabilidad contra Blue el investigador comenta que no pudo probar su ataque en un Chrome os pero dice que la configuración de Blu en Chrome os parece mitigar la vulnerabilidad Supongo que revisó un poquito el código fuente y la configuración y dijo Oye en Chrome os Okay está está mitigado el tema en este caso en Linux para explotar con exito esta vulnerabilidad es necesario que Bluetooth esté en modo visible Así que se podría decir que si el dispositivo Bluetooth está en modo invisible Pues esta vulnerabilidad no te afecta en cualquier caso ya está disponible un parche para esta vulnerabilidad en Linux y recomendamos instalarlo lo antes posible el investigador comenta que los detalles completos de la vulnerabilidad y los scripts de prueba de concepto se publicarán en una próxima conferencia y añade que realmente no está seguro sobre Qué tipo de teclado inalámbrico recomendar después de publicar esta vulnerabilidad ya recordáis como he dicho que este mismo investigador publicó la vulnerabilidad de mouse Jack en 2016 y dijo Oye mejor no uséis los dispositivos teclados y ratones inalámbricos que vienen con el USB dongle inalámbrico mejor utilizar teclados y ratones Bluetooth pero ahora se está un poco retractado y dice Oye y es que ya no sé qué recomendar a nadie porque los dispositivos Bluetooth teclados eh y ratones en este caso ahora He descubierto que también están afectados por esta vulnerabilidad similar de inyección de pulsaciones de teclado a través de bluetooth ahora el investigador acaba poniéndole la guinda al pastel diciendo que Oye estad atentos viene una parte dos con más vulnerabilidades Así que vamos a ver qué publica en breve este investigador y os ponemos más detalles en discord en Twitter cuando sepamos más tal y como ha demostrado el investigador estas vulnerabilidades se encuentran en versiones de dispositivos comercializadas desde 2012 Android 4.2.2 sin embargo por qué no fueron encontradas Antes nos podríamos preguntar según Comenta por su parte cuando publicó

Mouse Jack en 2016 no tenía suficiente conocimiento de bluetooth y de hecho le asustaba lo veía muy complejo de entender y asumía que Bluetooth era un protocolo seguro el típico modelo de seguridad por oscuridad y ya os he dicho que él mismo recomendó ratones y teclados bluetooth en respuesta a su ataque Mouse Jack de 201 para las vulnerabilidades que acaba de publicar dice que todo empezó cuando se puso a investigar teclados inalámbricos para usuarios de videojuegos o Gamers pero se desanimó porque vio que eran muy complejos de entender Supongo que por toda la complejidad que tienen para ofrecer esta poca latencia y todas las miles de funcionalidades extra que ofrecen para tener una experiencia más avanzada no en en videojuegos entonces buscó un desafío nuevo en el Magic Keyboard de Apple porque tocaba dos temas de los que no sabía mucho Bluetooth y Apple Y bueno ya veis que de ahí fue tirando del hilo y encontró vulnerabilidades similares no solo en dispositivos de Apple sino en Android y también en sistemas Linux Cierro la noticia diciendo que ya veis que el aire el medio radio El entorno inalámbrico esconde muchas amenazas y riesgos y cada uno tiene que conocer su modelo de amenazas como siempre comento su superficie de ataque y gestionarla apropiadamente dependiendo de cada situación es decir que tengo un sistema que no puedo actualizar Bueno pues deshabilito el bluetooth en escenarios de alto riesgo como en lugares públicos tipo cafeterías hoteles y aeropuertos igual relacionado con esto recordatorio de que si queréis Desactivar bien el bluetooth en dispositivos iPhone y iPad hacedlo a través del menú Bluetooth de configuración y no a través del centro de control ese menú que se obtiene al deslizar el dedo desde la esquina superior derecha hacia abajo porque ese menú no Desactiva el bluetooth completamente y esto ya lo mencionamos en un episodio anterior así que espero que lo tengáis en vuestra mente Y bueno si quis actualizar vuestros sistemas vulnerables por este ataque pues actualizad losos y usad lo Igualmente con cuidado en entornos públicos porque ya sabéis que y lo último ya acordaos de esos ratones y teclados con dongles usbs inalámbricos vulnerables al ataque Mouse Jack y a mirar las notas del episodio y espero que no estéis usando ninguno de ellos y si no ya sabéis a cambiarlos a parchear losos a pasaros a bluetooth en un sistema que tenga los últimos parches o versiones o Bueno a teclear en la pantalla Gracias Alexis por haber preparado una noticia también para este podcast a pesar de que no pudiste grabar conmigo Pero bueno espero que nuestros oyentes lo entiendan yo con un resfriado época de vacaciones pero nosotros Seguimos aquí ya sea los dos juntos a la vez separados en diferido lo importante es que hagamos llegar este episodio este audio esta información a todos vosotros porque como siempre os decimos la actualidad no descansa y tenemos que conseguir siempre ya sea contra enfermedad o contra las diferencias horarias poder publicar nos vemos con suerte y nos escuchamos para la próxima semana si conseguimos encajar un episodio más nos despedimos ya y si no felices fiestas buena entrada al próximo año y no os olvidéis de nosotros Adiós adiós si te ha gustado esteis 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