78. Google Home y WebCarHacking

un investigador consigue convertir los altavoces inteligentes de Google en el espía perfecto y además se lleva más de 100 mil dólares por este hallazgo marcas de automóviles de lujo como Ferrari Porsche o BMW y otras marcas como Ford Honda y Toyota corrigen múltiples vulnerabilidades que Podrían haber permitido la toma de control total de los vehículos e incluso ataques de tipo ranson Wii damos la bienvenida al nuevo año como se merece dentro nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 8 de enero de 2023 estamos en el episodio número 78 yo soy Martín vigo y está conmigo de resaca pero listo para darlo todo Alexis porros Hola Alexis qué tal pues Buenos días Martín pues aquí muy bien aquí con con mucho ha aprendido una palabra gallega gracias a Martín recientemente que digamos sería con con mucho amor con muchas ganas de que estoy Gozando de estar aquí contigo en un nuevo episodio lo que te dije no tiene traducción la palabra es muy difícil de traducir al Castellano ahí aprendiendo idiomas ya que nos gusta aprender todo Pues nada aquí vengo con razones de peso además Bueno digo con unos cuantos kilitos de más de lo que de todo lo que he comido durante navidades fin de año sabes otras fiestas supongo que no soy el único que alguno de nuestros oyentes están en el mismo yo como digo siempre las comidas estas de familia o de Navidad deberían venir o los regalos deberían ser una suscripción de un mes a un gimnasio o una consulta gratis a un nutricionista para poner a Tono la dieta de primeros de año no Para volver a estar en forma sí Yo empiezo el lunes yo empiezo el lunes el lunes el lunes el lunes de no sé de qué semana ni de qué mes no Pero algún lunes vas a empezar Pues eso pero bueno también vengo con energía porque los Reyes Magos me han traído una batería del litio súper de esta supercargada no y vengo aquí con las pilas puestas Así que contigo como si fuéramos los Reyes Magos Martín trayendo otro episodio de regalo a nuestros oyentes y lo primero es lo primero como siempre Muchas gracias a todos vosotros queridos oyentes por el seguimiento que nos hacéis en redes sociales donde nos comentáis nos enviáis vuestras sugerencias preguntas de mejora no decir lo que os gusta más y lo que os gusta menos y lo que que mejoremos Y eso nos encanta porque nosotros estamos aquí para compartir y mejorar con vosotros os recordamos que si no lo estáis debería estar suscritos a nuestro podcast en vuestra plataforma escucha favorita la que quiera que uséis si aún no lo estáis por favor suscribíos Y nos podéis seguir en redes sociales en Twitter Instagram y Facebook con el handle @tierra de hackers También estamos en mastodon ahora como arroba tierra de hackers por aquellos por si hay alguno sí que nos preguntaban en discord si estábamos por allí linkedin YouTube y Twitch como tierra de hackers correos electrónicos tenemos el email podcast arroba tierra de hackers.com Y como dice Martín podéis acceder a nuestro servidor de discord a través de tierra de hackers.com barra discord y finalmente como siempre agradecemos vuestro apoyo a la pregunta del episodio Gracias por votar en Twitter que la del episodio anterior fue lo siguiente Cuál de las siguientes tendencias en ciberamenazas creéis que va a ser la más popular en 2023 este año que acaba de empezar tenemos cuatro respuestas la más votada con un 35% fue ataques destructivos la sigue hackeo con drones con un 25% seguida de El próximo wana Cry con 22% y la última fue malware distribuido vía signing con un 18% Muy bien pues pues como tú bien dices aquí con los Reyes Magos con Santa Claus Papá Noel todo lleno de regalos yo me he hecho un auto regalo que anuncio aquí a mis queridos oyentes que me he mudado en San Francisco de vuelta a España Así que ahora vamos a seguir todavía en

diferentes horarios pero por lo menos ya no del lado de San Francisco sino de aquí Así que ahora me he mudado a Barcelona y voy a estar aquí unos a que tenía muchas ganas he dejado también mi empleo O sea que ahora tendré más tiempo para dedicar al podcast mucho más así que estar pendientes porque tierra de hackers va a ir tú de Next Level eso más me vale porque ahora los ingresos están a cero O sea que al no trabajar pero bueno tenía muchas ganas de hacer varios proyectos personales Y tal Así que nada eso también me va a facilitar mucho más si la conferencias aquí en España y conocer como como estuve haciendo las últimas conferencias en albacete y tal a muchos de nuestros oyentes que es una como ya había dicho es una pasada Así que ya sabéis ahora dando por España y súper contento la verdad yo yo encantado así Mira así tenemos todavía más conexión con España porque a veces nos decían Oye que a veces salen noticias en España alguno había comentado que no os habéis enterado o no habéis cubierto tal ahora con Martín en España vamos no vamos a enterar de todo y conexión Estados Unidos España y nada Yo también espero que Martina aprenda alguna palabra en catalán como yo he aprendido el Gallego yo parlo una una mica catálogo poquito a poco gracioso que estoy siendo Barcelona al final acabo yo aquí pero es que me encanta me encanta tu ciudad Barcelona es una pasada Así que aquí aquí andamos Y bueno necesitaremos a alguien también en Latinoamérica porque también tenemos un montonazo de oyentes en países por allí a ver si vamos incrementando lo que es tierra de hackers y acabamos con gente por allí también y si no si nos van invitando pues vamos nosotros por ahí no latinoamérica pues destino latinoamérica Pues nada dicho esto también quiero menciono esto también porque me estaréis escuchando con un poco de eco o mucho eco O sea que mis disculpas pero estoy en mi piso vacío Sentado en una silla que me he pillado exclusivamente para poder el episodio de hoy pero es que literalmente estoy en un piso vacío al que me acabo de mudar Así que disculpa si en este episodio tenéis un poco de eco de fondo de mi lado pero bueno es por una buena razón estoy más cerca de nuestros oyentes en España ahora y bueno ya sin más dilación que empezábamos aquí con tal como siempre dar las gracias a nuestros mecenas a la gente que nos apoya económicamente en patrón especialmente a José torrico que justo se acaba de incluir Añadir meter en nuestro grupo de oyentes preferidos que son los que nos apoyan a través de patreon Así que bienvenido Muchísimas gracias por tu aporte económico que ayuda muchísimo y también a nuestros sponsors que en este caso es mona tú una empresa que comparte los mismos valores que tierra 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 y que está buscando ya sabéis muchos ingenieros a pesar de que todo el mundo parece que está en crisis y están contratando en remoto así que ya sabéis si queréis echarle un vistazo a su web mona.com y le podéis contactar en tierra de hackers @monat.com y ya ahora sí nos vamos con la noticia hablemos de altavoces inteligentes en tierra de hackers os hemos contado numerosas historias no a través de noticias de técnicas de espionaje y lo valioso que sería para alguien que quiere espiarte tener un micrófono oculto en tu casa si bien en los 80 90 y principios de 2000 eso era el caso lo cierto Es que la mayoría de la gente ya tiene un micrófono siempre consigo ya sea en tu móvil que está todas horas contigo tu ordenador cuando lo estás usando los mandos a distancia de las televisiones inteligentes que te facilitan la búsqueda de tu show favorito o bueno como no los altavoces inteligentes que te permiten hacer preguntas a sirio Google preguntarles el tiempo o pedir que reproduzca tu canción favorita con esto lo que digo es que a diferencia del pasado el que te quiere espiar ya no tiene que conseguir una manera para introducir un micrófono en tu casa sino simplemente controlar uno de

los muchos que ya tienes en casa y esa fue en parte la motivación del investigador que recientemente encontró una manera de controlar el altavoz inteligente de Google remotamente y entre otros Acceder al audio que captura en tiempo real en su web ha publicado un detalladísimo right up con todos los detalles técnicos que os recomiendo leer si estáis interesados y que por supuesto os dejo enlazado como siempre las noticias del episodio Perdón en las notas del episodio yo Mientras tanto os lo voy a contar por encima parandome en lo más interesante el investigador comenzó a jugar con Google home bueno Esto de jugar en el ámbito del husking viene siendo toquetear todo y ver si algo rompe pues empezó a juguetear con Google home Google home es la solución de Google en cuanto a domótica un sistema centralizado para controlar todos los dispositivos inteligentes en tu hogar pues bueno como luces enchufes cerraduras cámaras etc básicamente todo está conectado a través de sus protocolos y lo puedes controlar fácilmente desde la aplicación móvil Google home el equivalente en Apple sería el famoso homekit para que os hagáis una idea pues lo dicho estaba el tío ahí toqueteando todo y se fijó que era muy fácil Añadir usuarios nuevos a Google home desde la aplicación móvil como os podéis imaginar interesa que varias personas puedan controlar los dispositivos de una misma casa porque por lo general son varias las personas que habitan en ella Pues él empezó a analizar Cómo funcionaba a bajo nivel esto de Añadir usuarios nuevos a un hogar Por así decirlo se fijó también que en cuanto a privilegios un usuario lincado a un hogar y a un dispositivo tiene muchos privilegios aunque no sea el administrador puede por ejemplo crear rutinas nuevas esto de las rutinas te permite configurar una serie de acciones hacer en base a un comando el investigador mismo da el ejemplo de crear por ejemplo una rutina que al decir buenos días Google apague las luces y te diga el tiempo que hace fuera no así tú te despiertas en cama y dices OK Google Buenos días y va apaga la luz y te dice Fuera fuera hace frío tal ponte un paraguas coge un paraguas por tanto un usuario puede mandar comandos a los dispositivos remotamente a través de la creación de rutinas y estas rutinas además pueden ser configuradas para que se ejecuten automáticamente a unas horas o días preestablecidos no teniendo que ser iniciados por un comando de voz Es decir para un atacante es más interesante que en vez de tener que decir OK Google Buenos días porque si no tendría que el atacante estar ya en la casa Y entonces ya no sirve para nada es preprogramar Oye a las 9 de la mañana inicia esta rutina con esta serie de comandos pero un usuario que forma parte de una cuenta de Google home puede también instalar acciones las acciones son como pequeñas aplicaciones que extienden la funcionalidad de los dispositivos inteligentes en el hogar yo creo que ya sabéis ya ya vais viendo por dónde voy si un atacante encuentra una manera de añadirse a la cuenta de Google home de un hogar puede controlar completamente todos los dispositivos inteligentes y con unas capacidades que le permitiría invadir seriamente la privacidad de los que viven en esa casa Solo una pregunta No sé A mí igual que no soy experto en esto no sea los oyentes tampoco no me ha quedado claro Cuál es la diferencia has mencionado rutinas y acciones hay alguna una rutina es múltiples acciones combinadas juntas o cuáles como la diferencia muy buena pregunta Alexis básicamente las rutinas te permite combinar una serie de comandos bajo un para ejecutarse bajo un solo comando de voz por ejemplo activa el modo fiesta y entonces eso creas una rutina activa el modo fiesta que lo que hace es subir el volumen encender la radio subir el volumen y encender una luz roja por ejemplo y desactivar la alarma de la casa para que no salte Por así decirlo mientras que las acciones lo que te permite es extender los comandos que tú puedes hacer No solo los que ya te vienen preestablecidos es como no entiendo yo eh que no tengo un Google un Google home y puedes hacer nuevos comandos como yo que sé Oye Siri Dame

el tiempo del antes de ayer no sé no sé es un mal ejemplo pero te permite extender la funcionalidad eso vendrían siendo las las diferencias Ok Muchas gracias Total que la motivación del investigador está más que justificada para empezar este proyecto y con un claro objetivo en mente que era averiguar Cómo poder Añadir un usuario a un altavoz el investigador pues se puso manos a la obra comenta el investigador que para ver cómo funciona el hincado de nuevos usuarios una cuenta de Google home tenía cuatro opciones la primera obtener el firmware de algún dispositivo no de su altavoz y reversarlo la segunda sería un análisis estático de la aplicación móvil de Google home que se usa para Añadir usuarios nuevos el análisis estático viene siendo mirar el código fuente o cómo está programado para entender cómo funciona una tercera opción para el investigador era el análisis Dinámico con Tools por ejemplo como Frida para jukearse o engancharse las funciones relevantes esto es en vez de mirar el propio código fuente de la aplicación móvil miras cómo se comporta mientras se está ejecutando y detienes la ejecución la pausas donde te interesa para ver qué está haciendo y la cuarta opción era pues interceptar las comunicaciones entre la aplicación móvil y el dispositivo inteligente mediante el típico Man in the middle Man in the middle ya sabemos que básicamente es que tú que puedas observar las comunicaciones entre dos dispositivos y pues Sabiendo lo que las comunicaciones y los datos que se están enviando pues sacar tus conclusiones se decidió a empezar analizando el tráfico mediante un Man in the middle Pero antes comenzó a probar una serie de aprobar una serie de peticiones para ver si podía comunicarse con el dispositivo inteligente en su caso como decía el Google home mini que es un altavoz inteligente que fabrica y vende el propio Google después de escanear los puertos y ver que podía utilizar el protocolo http para lanzar peticiones se dio cuenta que podía obtener respuesta para comandos básicos Cómo obtener detalles del dispositivo pero si mandaba un comando más sensible Como por ejemplo apagar el altavoz necesitaba un token de autorización un secreto Por así decirlo que solo obtienes si ya tienes un enlace establecido con ese dispositivo es decir el atacante estando en la misma red que el altavoz podía enviarle peticiones comandos y decirle Oye Dame información sobre ti Y eso se lo daba pero si era una acción un poquito más sensible como apágate o enciéndete o empieza a grabar entonces necesitaba estar autorizado vale esto tiene sentido porque si no cualquier atacante que está conectado a la misma red que el dispositivo no imaginaros que yo quiero espiar a mi hermana que tiene un altavoz en su habitación estamos en la misma casa en la misma red Pues claro podría hacer eso pues cualquiera de esto podría enviar comandos sin ningún tipo de sin ningún problema ni autenticación por tanto volvemos al objetivo inicial de comprender cómo se añade un nuevo usuario a un dispositivo para ello montó su laboratorio con un Man in the middle que le permitía ver el tráfico entre la aplicación móvil y el dispositivo en la red local sino también el tráfico enviado entre la aplicación móvil y los servidores de Google esto pensarlo es esencial porque en toda creación de usuarios nuevos Google tendrá que formar parte de ese workflow de ese proceso Y puede que se esté enviando información valiosa a Google que les sirva al investigador para encontrar una vulnerabilidad no entraré en Como hizo este laboratorio de Man in the middle porque es más técnico y no quiero aburriros pero como os comento de nuevo tenéis el link a su blog post de las notas si queréis indagar más con este Setup lo primero que hizo fue abrir la aplicación móvil de Google home y añadió un nuevo usuario al altavoz previamente había configurado el altavoz con su propia cuenta de Google para simular el escenario de un atacante añadiéndose al altavoz de otra persona no es decir Añadir un usuario a mayores a un altavoz que ya está configurado con su dueño observó que la petición enviada a Google para Añadir un usuario nuevo al altavoz contenía un certificado el

nombre del dispositivo y otro parámetro llamado Cloud ID si bien Esto puede no sonar muy interesante inmediatamente a él le recordó que precisamente estos tres parámetros fueron los que pudo obtener previamente mandando una petición en la red local sin autenticación recordáis que os conté hace un minuto que al principio hizo pruebas mandando peticiones directamente al altavoz en su propia red y que algunas peticiones básicas como obtener la configuración del altavoz funcionaban pero apagarlo no requería autenticación no pues la petición que funcionaba sin autenticación le daba exactamente los parámetros que tenía que enviar a Google para añadirse como usuario al altavoz es decir el ataque propuesto en este punto sería el siguiente paso 1 en la misma red es decir el atacante que está en la misma red que el altavoz obtiene los tres parámetros del dispositivo haciendo una petición en la red local nombre y obtiene el nombre del dispositivo Cloud ID y el certificado y el paso 2 sería usar estos parámetros para crear una petición que envías a Google para Añadir tu usuario de Google a ese altavoz Tan sencillo como eso pero claro tiene varios requerimientos principalmente que el atacante tiene que estar en la misma red que el objetivo para obtener los parámetros del paso 1 que cuando lo pensamos así si vas a estar en la misma casa por ejemplo pues claro ya puedes escuchar quizá la conversación de otras maneras no pero bueno para verificar que efectivamente este ataque a nivel teórico funcionaría implementó este ataque en python de manera que tenía un programita Por así decirlo que dada una IP local del dispositivo y los de la cuenta de Google del atacante iba y obtenía los parámetros de configuración del dispositivo y añadía tu usuario a ese dispositivo de manera automática es decir a este programa que él creó tú le dabas la IP local del altavoz y tus credenciales de Google y pum automáticamente ya te añadía esto ya es un ataque muy significativo y el investigador plantea el escenario de un atacante que programa una aplicación de móvil maliciosa y la sube a la Google Play Store cuando los usuarios se la van descargando esta aplicación Busca en la red local dispositivos inteligentes conectados a Google home lo cual encontrará escuchando peticiones de dns según recolecta ips internas de dispositivos inteligentes obtendrá los parámetros de configuración para luego mandar la petición famosa Google para Añadir el usuario de Google del atacante ha dicho altavoz dándole acceso a dicho dispositivo remotamente me parece un vector de ataque muy guapo factible y sobre todo escalable ya que una vez tú tienes una maliciosa en la Play Store pueden ser miles los que se la descarguen e instalen y cuando lleguen a casa estarán conectados a la misma red que están conectados los altavoces y la aplicación empezará a hacer el ataque pero ahora cabe contestar la pregunta de qué es lo más peligroso que el atacante en este escenario podría hacer cómo puede el atacante llegar a abusar la posición de control sobre el dispositivo que tiene para crear un escenario de peligro real para la privacidad de Los afectados pues este investigador se puso a mirar cómo podía Acceder al audio capturado por el micrófono del altavoz ya que eso en altavoces inteligentes es claramente el ataque que peores consecuencias tiene no poder escuchar remotamente las conversaciones de las víctimas en sus propias casas si bien inicialmente pensaba que tan fácil como enviar algún tipo de comando que activase el micrófono Google diseñó los altavoces y apis de manera que eso no fuera posible como mucho podrías acceder a la transcripción del audio a través de Google ya que se ya que Google puedes configurarlo para que haga eso la transcripción de audio que se va capturando esto ya es muy significativo Aunque no es lo mismo que acceder directamente y en tiempo real al audio en sí de la gente hablando no por tanto el investigador no desistió y siguió investigando y leyendo documentación de Google hasta que encontró una Api digamos una funcionalidad que permite indicar al altavoz que haga una llamada telefónica esto es muy interesante si yo le puedo decir a un

altavoz inteligente que llame a Manolo también podría indicarle que llame a un número de teléfono específico el mío como atacante y lo cual ya me permitiría escuchar a la víctima no solo eso sino que recordemos que estas rutinas podían ser programadas para horas y días específicos por lo que podías con antelación preprogramar altavoces inteligentes para que te llamen por teléfono y escuchar todo lo que está pasando en la habitación Así que llegados a este punto ya tenemos que el investigador encontró una manera en la que teniendo acceso a la red local en la que está el altavoz conectado puede añadirse como usuario y luego escuchar el audio en tiempo real a través de una llamada telefónica recibida directamente desde el altavoz ahí es nada pero aún con estas el investigador no se detuvo aquí y quiso ir más allá para mejorar el vector de ataque podía de alguna manera llevar a cabo este ataque sin tener que estar en la red local pensamos que estar en la red local indica que tienes que tener previamente la contraseña de la WiFi o hacer que la víctima instale una maliciosa no como explicábamos hay alguna manera de llevar a cabo este ataque sin que requiera ningún tipo de interacción por parte de la víctima como instalar una maliciosa Pues sí señoras y señores sí la hay el investigador se puso a mirar qué investigaciones anteriores se habían publicado sobre ataques tanto a Google home como Chromecast que está íntimamente relacionado etcétera y encontró dos muy interesantes y sobre todo relevantes para para este proyecto cast hack presentado en defcon en 2019 que demostraba como miles de dispositivos inteligentes de Google están accesibles abiertamente desde internet no solo en Red local y rickmode que es un artículo publicado por bishop Fox en 2014 en el que un investigador es capaz de ganar acceso a Chromecast que están cerca suya y hacer que empiecen a hacer streaming del vídeo de Never Gonna Give You Up vamos unricron Y cómo Pues resulta que Chromecast cuando pierde conexión a la WiFi lo que hace es ponerse automáticamente en modo Setup creando el propio dispositivo una red abierta WiFi para que sea más fácil conectarse a ella y reconfigurar el dispositivo es decir si un atacante consigue de alguna manera desconectar digamos un altavoz este abre sus puertas a través de una red WiFi automáticamente que se genera y a la que te puedes conectar hacer que un dispositivo conectado a una red WiFi se desconecte Es realmente muy sencillo solo hay que enviarle muchos paquetes conocidos Como diaothentication packets que básicamente indican al dispositivo que se desconecte lo más interesante es que este tipo de paquetes no requiere de ningún tipo de autenticación previa ni nada por el estilo por tanto cualquiera que esté en la vecindad de un dispositivo puede enviar al aire este tipo de paquetes dirigidos específicamente al dispositivo a desconectar y este se desconectará Pues que hizo el investigador eso mismo mandó muchos paquetes de autenticación a su altavoz y efectivamente este se desconectó y creó inmediatamente una WiFi a la que lactante se pudo conectar y una vez conectado al altavoz es el mismo escenario que estar conectado a la red local Ya podía correr su Script que extraía la configuración del altavoz que contiene los parámetros para enviar a Google y añadirse como usuario por tanto el atacante para Acceder al audio en tiempo real del altavoz de altavoces inteligentes ya no requiere instalar Apps maliciosas o estar en la misma WiFi solo requiere al atacante estar en la proximidad física de tu dispositivo para llevar a cabo el ataque vives en un edificio Cuántas redes wi-fi ves desde tu ordenador cuando vas a conectarte a la tuya decenas verdad todas las de tus vecinos Pues eso tu vecino perfectamente puede desde su casa hacer que tu altavoz inteligente se desconecte añadirse como usuario y decirle a tu altavoz que le llame por teléfono a una hora preprogramada para escuchar a ver qué estás diciendo y aquí lo dejo porque me da Que varios Vais a parar el podcast para no Escuchar más otra noticia de espías de James Bond de nuevo los guionistas de películas de Hollywood nos pueden contratar podemos dar

ideas Esto me recuerda por ejemplo las tantas noticias que hemos comentado en episodios anteriores como el episodio 6 en la que comentamos un poquito el lanfon ese que era el ataque con láser contra la bombilla para escuchar la conversación dentro de la casa o ese esa otra noticia sobre que llamaron un ataque light commands no que con un láser desde fuera de la casa apuntaban al micrófono de dispositivos inteligentes que tenían micrófono valga la redundancia como homes Google home Smart y similares para escuchar Pero esto ya es otro nivel como dices Martín esto se puede hacer de forma remota bueno la primera aproximación sería te tienes que acercar físicamente no en proximidad para realizar el tema de autenticación que se cree la nueva WiFi esta asociarte y añadirte como usuario pero una vez hecho eso no ya se te puedes retirar pero también se podría hacer creo que has mencionado distribuyendo una aplicación maliciosa que eso no tienes ni que estar en proximidad de la aplicación del hogar del usuario Así que podría ser totalmente remoto es que ese es el tema o sea por ejemplo los otros atacan los otros ataques que mencionabas que son así como más de ciencia ficción eran más como de laboratorio que se podían llevar a cabo pero un poquito más complicados Pero es que este es uno más uno dos y yo me imagino incluso que puedas o sea lo primero lo que dices tú lo importante en proximidad Sólo tienes que estar una vez una vez que es para añadirte como usuario a partir de ahí tú ya tienes control total puedes crear tus rutinas remotamente y todo pero incluso y está remotamente quiere decir que puedes estar fuera de la casa enfrente de la puerta o incluso en el piso de arriba o sea que tampoco es que tengas que estar en proximidad pero en el interior del hogar no por no hablar de que incluso hasta podrías implantarle yo que sé quieres espiar a uno del curro te haces una pequeña raspberry Pay que te puedes comprar de estos días automáticos porque lo único que tiene que hacer tiene que hacer dos peticiones dos peticiones y un deut que eso vamos tiene son tres líneas de python te metes un dispositivo pequeñito que cuando vaya a su casa lo está haciendo automáticamente todo el rato cuando vuelva se lo quitas de la mochila al día siguiente y ya está no has ni tenido que estar en la proximidad pero yo sobre todo lo veo porque los lanforms y todo esto pues podemos pensar a nivel gubernamental Y tal Pero es que aquí esto a nivel gubernamental no de espionaje de altas figuras o ver important people o cosas así pues esto es súper factible vamos súper factible sí o le envías un paquete de estos que se queda en la puerta también lo pone y luego lo abre pero ya es tu late ound le puedes poner la foto del Bueno le envías ahí yo que sé le puedes enviar un puzzle de estos que hay ahora no sé se me ocurre algo así porque en una operación anterior de retina hicimos algo similar hay puzzles que tienen un USB porque es parte de resolver el puzle y no sé qué y era un poco con la idea de que lo enchufasen en el ordenador Pero tú puedes sabes montar en un dispositivo algo que está dentro esa persona Nunca lo va a ver acabará tirando lo dejándolo por ahí ya está se lo envías por correo ideal Bueno tal me ha tocado esto lo que sea sí pero sí muy interesante Por cierto que no que no lo mencioné este investigador hizo lo correcto lo reportó de manera responsable a Google y se llevó 107.500 más de 100.000 pavos por esta investigación que se lo merece y aparte el artículo está súper bien escrito Qué poco dirían algunos si lo hubiera vendido en el mercado negro Pero bueno ya yo es que ya te digo como no una una vez hecho todo el resets toda la investigación lo que es el vector de ataque no tiene nada de sofisticado esto sería súper valioso para la gente pero el tema ese o sea pero a mí una una un vector de ataque sería el que hemos dicho está en proximidad enviar esos dos paquetes tal pero el otro como mencionamos sería crear una aplicación maliciosa que es que se la descargara claro de alguna forma y ya hemos visto muchas veces no no es que la seguridad de una plataforma u otra sea mejor que la otra Google versus Apple pero parece que no sé es más fácil

colar aplicaciones maliciosas en el Google Play Store que en el Apple Store Así que igual habrían más posibilidades incluso aunque no sea que parece ser que es así como tú dices que hay menos Control pero a mayores Android te permite instalar Apps de otros sitios no como dispositivos de Apple que solo puedes hacer desde la Apple Store por tanto es mucho más propenso que tú puedas decirle eso hacerte como hemos visto muchos ejemplos que no estamos dando un ejemplo en plan Sería posible aplicaciones maliciosas que hacen cosas malas en tu dispositivo ha habido apartadas y sobre todo en Android por tanto esto tampoco es nada del otro mundo en este ataque menciona el investigador si puede hacer las modificaciones digamos permanentes en el firmware o reflexionar el firmware o solo son crear estos comandos rutinas acciones temporalmente y si se hace un refrán se regeneran o no se menciona Bueno yo no creo que ni que tengas que hacer un refresh de hecho es buena pregunta porque a lo mejor el usuario si va y mira las rutinas que se han creado a lo mejor las ve pero a lo mejor las rutinas es por usuario claro No lo sé si las rutinas son por usuario en plan somos varios no en la casa los que tenemos acceso al altavoz con nuestros usuarios personales de Google si yo creo una rutina es una rutina solo para mí y por tanto los otros no la ven o es una rutina para todos claro No sé pero vamos Esto no es a nivel de de firmware esto es a nivel de aplicación Por así decirlo no no y aparte no sé bien Por dónde Ibas con el tema de firmware de sí o Supongo que puedes Chávez parchear el firmware y meterte pero yo creo que ahí ya te metes en otros problemas temas de que está firmado y todo esto que esto es más de sí no ahora te vengo con el tema la idea era si se puede hacer de forma permanente o no era yo con ideas de negocio y temas financieros pues ataque de ransomware venga vamos a hacer un poquito de malicioso aquí contra los las víctimas podría uno podría hacer una rutina una acción mencionando el nombre de la víctima junto con palabras son antes que se que se pusieran a toda pastilla a todo volumen sabes en plan señor Pepito eres un bla bla bla y págame tanto o voy a emitir este sonido cada tres o cuatro o mencionar su cuenta de banco o yo que sé sus contraseñas sabes y hasta que no pagara Pues eso no se no se apaga no se apagaría el tema del anuncio sabes no el típico el típico audio Este que se llevaba mucho ahora no tanto pero que se enviaba mucho por mensajería como WhatsApp el típico vídeo este que parecía interesante y luego a todo volumen se escuchaba la tía hacer Pues imagínate programarlo para que el altavoz tienes invitados y cada dos por tres se escucha gemir a a una mujer o sea algo así ransomware a través de de los huevos pero pero tú dices Bueno esto porque esto podría ser se podría dar y a ver tú mencionas que hay usuarios que podrían mirar las acciones está pero cuántos usuarios son técnicamente aptos para revisar eso seguro que dirá No sé cómo hacer esto voy a pagarlo aunque sea y le y les cobras aunque sea 5 eurillos que es menos que que llamar a Google no no no no le creas una rutina le creas una rutina que sea haz una transferencia a y solo tienes que decir tu cuenta bancaria ya el resto ya está programado en el altavoz Ya está si es es Es justo hacer temillas estos así que bueno a Google que se ponga las pilas con esto pero bueno ya he dicho que sea se ha arreglado no y los últimos firmwares pues Supongo que ya tienen esto arreglado verdad sí Supongo que sí de hecho en principio yo aquí donde veo el problema es más en la parte de las apis hacia Google porque recuerda que tú añades un usuario con datos que puedes obtener del altavoz sin autenticación entonces o hay que arreglarlo del lado del servidor de Google Esa llamada o del lado del altavoz que eso sí ya sería firmware que no te dé esa información sin estar previamente autenticado claro se podría solucionar en dos puntos diferentes Claro a mí el tema de que por de autenticación se cree una nueva WiFi Yo estaba pensando Pues que solo se permita Pues si aprietas un botón físico en el cacharro que significa que estás ahí sí pero bueno tenga en cuenta Sí sí eso es verdad Pero

eso solo solucionaría el que sea explotable con acceso físico pero a través de una aplicación No porque si tú instalas una aplicación sabes Todavía sería por eso lo que hay que solucionar es o que el altavoz en Red local no te dé la información que necesitas para un usuario poder añadirse o que un usuario pueda añadirse requiera algo más que lo que te da el altavoz entonces claro no sé dónde lo van a solucionar Supongo que lo solucionará la solución harán del lado del altavoz que no debería darte nada utilizar o por lo menos el todo requerido para Añadir a un usuario o sea es a lo mejor el clout ID ese o un identificador único del altavoz que tienes que tener acceso físico al altavoz para saberlo algo así sí si no tiene sentido que dé nada información si no estás autenticado totalmente Ok pues muy buena Martín para que tengáis Google homes a ver esto Google ha parchado seguro porque si no la investigación sería pública Así que ir a parchear vuestro sistemas inmediatamente y nada pasamos con la siguiente noticia pero antes queremos hacer un breve inciso para darle las gracias a nuestro patrocinador brawler que nos apoya en el podcast y que hace unos meses ha lanzado un servicio en la nube para proteger tu infraestructura en aws hablamos de brawler pro y sus sass el servicio gratuito más completo de seguridad para aws brawler Pro está construido sobre la Popular herramienta Open source brawler y además por el mismo equipo de ingenieros si ya conoces prowler que está disponible en github seguro que vas a aprovechar las bondades que ofrece brawler Pro en cuestión de minutos tendrás resultados del estado de seguridad de tu cuenta de aws y podrás mejorar tu postura de seguridad a través de múltiples dashboards que te permitirán ahorrar tiempo y tener una visión completa del estado de tu infraestructura puedes empezar a usar brawler pro de forma totalmente gratuita en prauer.proprow l e r.prro desde ya mismo y bueno una vez dicho esto dentro noticia lo que traigo ahora queridos oyentes va de marcas de automóviles de lujo de no lujo otras empresas relacionadas con automóviles que bueno se han visto colores se han visto sus cachetes sonrojados porque se han publicado vulnerabilidades que permitían tomar el control total de cuentas que afectaban a todos estos vehículos y dispositivos y sistemas incluso las empresas enteras un equipo de investigadores de seguridad ha informado de que algunas de las marcas de automóviles más grandes del mundo han corregido decenas de vulnerabilidades algunas de las cuales Podrían haber permitido como Digo toma control total de vehículos de forma remota sin tener que estar cerca de ellos y hemos visto esto hemos cubierto en otros episodios ataques físicos de proximidad por ejemplo vehículos de tesla en los que hacía falta estar cerca del vehículo como digo para abrirlos abrir las puertas desbloquearlos encender el motor y para llevárselos no para conducirlos haciendo el tema ese de hacer un Replay de la llave vía radio pero en este caso todo esto se podría hacer de forma remota lo de conducirlo de forma remota Bueno solo si el vehículo es autónomo no los fallos se encontraron en vehículos de marcas de lujo como ese número Ferrari Porsche Mercedes Benz Jaguar Genesis BMW o bien rolls-royce otras marcas de vehículos que no son tan de lujo como Kia Honda Infiniti Nissan Acura Ford Toyota Hyundai Land Rover en la marca de matrículas digitales reviver no sé si os acordáis queridos oyentes pero ahora entre un poquito más en detalle en la empresa de seguimiento y gestión de flotas vía GPS spyron y en la compañía estadounidense de radio por satélite con programas en vivo y grabados Sirius xm estos fallos son una extensión del trabajo inicial de Sam curry y su y un grupo suyo que trabajan juntos de investigadores de ciberseguridad una empresa yugalabs que publicó estas vulnerabilidades en vehículos de todas estas marcas y las empresas adicionales como digo de matrículas digitales gestión de flotas vía GPS y radio por satélite algunas de estas modalidades fueron publicadas ya en noviembre del año pasado esto queda interesante no decir año pasado

2022 ya estamos en el 2023 pero sí sí de hecho en noviembre encontraron algunas y han ido tirando del hilo y han ido encontrando muchas más y ha publicado Sam curry un blog post bastante largo en el que menciona bastantes detalles técnicos de todas estas vulnerabilidades que van desde las que permitían acceso amplio a sistemas internos de la empresa e incluso datos de clientes hasta otras que permitían a un atacante enviar comandos a un vehículo Sam curry confirmó que todas las empresas mencionadas en el corrigieron las vulnerabilidades en una semana y fueron muy receptivas esto de unas semanas increíble que hayan arreglado todo esto tan rápido pero bueno voy a mencionar primeramente lo que quiero mencionar es el impacto que estas volaridades podría haber permitido a un atacante en este caso Los investigadores no de buena fe pero voy a ir más o menos empresa por empresa o grupo de empresa por grupo de empresa empezamos con Kia Honda Infinity Nissan y Acura estas vulgaridades fueron publicadas como digo en noviembre del año pasado lo primero que les permitió fue bloquear y desbloquear puertas arrancar y parar el motor obtener la ubicación precisa del vehículo activar y Desactivar luces delanteras activar el digamos lo pito claxon bocina o corneta depende del país de los vehículos de forma totalmente remota usando solo el número de bastidor o chasis Bin como se le conoce en Estados Unidos beagle identification number que además es esta expuesto No ese se puede ver desde no está dentro del capó sino por lo menos en Estados Unidos muchos coches lo tienen fuera que lo puedes ver a través del cristal no sé si es pues ahora yo creo que sí que en algunos sí lo que sí que lo que sí que recuerdo es que en España también por ejemplo están expuestos no sé si también por ley pero es muy fácil de ver así que es es un riesgo porque este Bing es bastante público digamos y otro impacto otra acción que les permitía hacer a los investigadores fue tomar control total o digámoslo robo no de cuentas de forma remota y obtención de datos personales como nombre número de teléfono dirección de correo electrónico y dirección física de nuevos solo usando el número de bastidor o Bin también les permitieron Espérate que me acabo de acordar que carls o car owners.net ahí puedes buscar por nombres y portal y te da el Bin del dueño del coche que me parece una locura porque esto ya lo había mencionado alguna vez de que si vas por la calle ves un coche aparcado por lo menos en Estados Unidos y ves el Bing size a quien le pertenece pero también puedes buscar por nombre o sea que puedes encontrar bings y empezar a que le quite el coche a un tío en Virginia y tú desde San Francisco Sí pues pues sí creo que no las tengo identificadas pero hay varias de austint que te dan esta información Así que aunque uno cubra el Bin del vehículo no se puede escapar a esto porque esa información se comparte aunque no lo sepamos Así que estamos expuestos en higüey y también el otro impacto la otra digamos maldad que podían hacer era bloquear a los usuarios para que no pudieran administrar su vehículo de forma remota incluso podían cambiar el propietario del vehículo además específicamente solo para Kia pudieron también obtener acceso de forma remota a la cámara de visión completa de 360 grados y Ver imágenes en vivo desde la cámara de automóvil que esto es bastante increíble sobre el tema de Mercedes Benz pudieron acceder a cientos de aplicaciones críticas internas abusando de una incorrecta configuración en una solución de inicio de sesión único single Sign que esto le permitió acceso a múltiples instancias de github herramientas de chat interno de toda la empresa que lo llaman Mercedes Benz matter most que es básicamente un slack personalizado Y capacidad de unirse a casi cualquier canal con lo que comentan los investigadores que un cibercriminal pudiera haber buscado y encontrado información confidencial que se comentan esos canales no sobre los sistemas de Mercedes vehículos o incluso clientes y también pues podían haber hecho preguntas técnicas haciéndose pasar como empleados en plan soy un nuevo

empleado y porque la cuenta es nueva no O bueno comprometiendo alguna cuenta específica y hacer preguntas para obtener respuestas y de esta forma obtener información crítica para lanzar ataques adicionales también podría acceder a sistemas de desarrollo de aplicaciones como sonar cube que es bueno es para desarrollo aplicaciones análisis de código y similares jenkins también para un poco de lo que se le llama si hay CD bueno es como para un poco analizar empaquetar compilar todo esto las aplicaciones y otros servidores no también servicios internos para administrar instancias de la nube de aws y apis relacionadas con sistemas internos de los vehículos también con en Mercedes Benz esto les permitió ejecutar código de forma remota en múltiples sistemas aunque no mencionan cuales y también encontrar un fugas de memoria en los ecosistemas en estas digamoslo en points Api que les permitieron filtrar información personal de empleados y clientes y acceso a dichas cuentas en el caso de Hyundai y Génesis muy similar al primer caso de Kia Honda Infinity Nissan yakura lo único que en este caso sólo utilizando la dirección de correo electrónico de la víctima con esto en lugar del Bing que la dirección de correo electrónico es incluso más pública no que un Bin Pues lo mismo bloquear desbloquear puertas arrancar y para el motor Localizar el vehículo activar y Desactivar luces delanteras el claxon y todo esto de forma remota obtener información adicional nombre teléfono dirección física y bloquear a los usuarios incluso cambio de propietario pasamos con BMW o rolls-royce abusando de nuevo con navidades en sistemas de inicio de sesión único de single Sign también los investigadores pudieron acceder a cualquier aplicación de empleado como cualquier empleado lo que les permitió acceder a Portales de distribuidores internos donde se podía consultar cualquier número de bastidor o bim para recuperar documentos de ventas de BMW que bueno esto tiene mucha información no de los clientes también acceso a cualquier aplicación protegida mediante este single Sign en nombre de cualquier empleado incluidas aplicaciones utilizadas por trabajadores remotos y concesionarios en el caso de Ferrari pues adquisición total de cuentas sin interacción del usuario para cualquier cuenta de cliente de Ferrari acceso a todos los registros de clientes de Ferrari debido a una falta de control de acceso en su sistema de content management System tipo no Cuál es pero tipo wordpress magento jumpla o drupal no pues esto les permitió o le permitirá un atacante crear modificar y eliminar cuentas de usuario administrador en estos sistemas y modificar todas las páginas web de la empresa y también pudieron agregar rutas digamos Así es decir manipular un poquito hacer hombre en el medio en en points específicos de Ferrari en Api punto ferrari.com y obtener secretos o digámoslo credenciales tokens de acceso a estos servicios o sea hay muchos que se exponen en Api punto ferrari.com y todos esos encontraron un archivo que expone cada uno de ellos barra login barra customer barra lo que sea y además no sólo eso sino que también incluían las credenciales para acceder a ellos de forma exitosa no luego tenemos esta empresa spireón que es básicamente un conglomerado de empresas de seguimiento digestión de vehículos GPS que bueno fueron creadas en los años 90 y 2000 como onstar goldstar flip locate que permiten gestionar flotas de automóviles a través de dispositivos GPS que se colocan en los vehículos que tienen capacidad de ser rastreados y recibir comandos arbitrarios por ejemplo bloquea el motor para el vehículo para que el vehículo no pueda arrancar No pues spireón las compró todas las adquirió y bueno y se dedica a gestionar flotas de vehículos y lo que pudieran hacer contra esta empresa después de identificar las volaridades fue acceder de forma completa como usuario administrador al panel de administrador y según menciona expireón en su web esto permitiría acceder o permitiría afectar a unos 15,5 millones de vehículos en todo el mundo y enviar comandos arbitrarios para desbloquear el automóvil encender el motor o desactivar el motor de

arranque o leer la ubicación de cualquier dispositivo Es decir de cualquier vehículo no y también flashear o actualizar el firmware del dispositivo todo esto de forma remota también permitiría ejecución remota de código en sistemas que administran las cuentas de usuario y dispositivos de flotas capacidad para acceder y administrar todos los datos en todo expeding es como una toma de control completa de la empresa básicamente capacidad para hacerse cargo por completo de cualquier flota esto de hecho hubiera permitido rastrear y Apagar los motores de arranque de atención la policía ambulancias vehículos de otras fuerzas del orden para varias grandes ciudades y enviar comandos a esos vehículos del tipo dirígete a esta ubicación también pudieron acceder de forma administrativa a todos los productos de expireón de todas las empresas que han ido adquiriendo Como he mencionado goldstar low Jack flight locate en spire tráiler en asset y bueno como he dicho esto afecta a 15,5 millones de dispositivos principalmente vehículos y a 1,2 millones de cuentas de usuario para la prueba de concepto Los investigadores dijeron vamos nos vamos a invitar a nosotros mismos o sea usaron su email para gestionar una flota aleatoria Bueno más que aleatoria la eligieron porque luego recibieron una invitación y tachan podían ser podían administrar la flota de un departamento de policía de Estados Unidos para rastrear la flota entera esto como digo hubiera permitido rastrear Apagar motores de arranque de la policía y enviarle comandos para en plan dirígete a esta ubicación no un caso de abuso muy interesante para cibercriminales pudiera haber sido saber si le están persiguiendo los policías o distraerlos en plan dirígete a esta ubicación o evitarlos bueno bloquearle el motor de arranque estilo un poquito películas así no sé de italian Job no O luego tenemos el caso de Ford filtración de contenidos de memoria de nuevo de las apis telemáticas de vehículos esto lo que reveló fue información personal de cliente y tokens de acceso para rastrear la ubicación y ejecutar comandos en vehículos revelar credenciales de configuración para servicios internos de la empresa de servicios telemáticos es decir dónde está el coche todo el tema de consumo de coche y similares capacidad para autenticarse en la cuenta del cliente y acceder a toda su información personal y realizar acciones contra los vehículos y pudieron tomar posesión de la cuenta del cliente lo que le permitió a un atacante lo hubiera permitido un atacante acceder completamente a la cuenta de la víctima incluido el portal del vehículo pasamos al caso interesante de reviver en octubre de 2022 California anunció que había legalizado las placas de matrículas digitales Y actualmente casi todas por no decir todas las emite la empresa reviver si alguien quiere una placa de matrícula digital compraría la placa de matrícula virtual de reviver que incluye una tarjeta SIM para el seguimiento y la actualización de la matrícula de forma remota los clientes que usan reviver podrían actualizar de forma remota el eslogan o texto el fondo la imagen y además informar si el coche había sido robado pues marcando la etiqueta de la matrícula como robada en el episodio 69 cubrimos el ataque de not my Plate y mencionamos el tema de las matrículas digitales de reviver y de hecho comentamos que era raro que no se hubiera publicado una investigación de volaridades asociadas con con esto con River Pues mira Bola ya ha llegado no es que seamos visionarios Es que esto era de cajón era cuestión de tiempo y de que alguien se interesara por identificar buenavidades en reviver los investigadores se interesaron de hecho en esta empresa porque la matrícula digital se podía utilizar para rastrear vehículos y comenzaron a auditar la aplicación móvil de forma muy similar a la que ha comentado Martín en la popularidad anterior contra el Google Smart home no interceptaron ataque de maní in the middle inspeccionar el tráfico de la aplicación móvil que iba a en points de apis de un sistema un Host específico pr-api punto rplay.com e intentaron abusar de esas apis Y funcionalidades aunque no consiguieron nada interesante luego pasaron a la URL para

restablecer la contraseña que esta ofrecía muchas más funcionalidades y con ella sí que pudieron causar impacto que fue el siguiente pudieron acceder de forma administrativa para gestionar todas las cuentas de usuario y vehículos de todos los dispositivos conectados arriba y ver un atacante entonces podría haber realizado lo siguiente rastrear la ubicación física del GPS y administrar la matrícula para todos los clientes de reviver por ejemplo cambiando el texto en la parte inferior de la matrícula actualizar el estado de cualquier vehículo a robado lo que actualizará la matrícula e informaría a las autoridades o sea en plan irías conduciendo un vehículo robado y te perseguiría la policía Supongo pueden acceder a todos los registros de usuario incluidos los vehículos que poseían las personas su dirección física número de teléfono y dirección de correo electrónico y acceso a funcionalidad de gestión de flotas para cualquier empresa con la capacidad de localizar y gestionar todos sus vehículos Los investigadores pudieron acceder a cualquier concesionario también por otras volaridades y lo interesante es por ejemplo los concesionarios de Mercedes ahora ofrecen matrículas digitales de reviver y Podrían haber cambiado la imagen por defecto de matrículas de vehículos recién comprados en este caso Mercedes Benz con las matrículas que estuvieran en modo concesionario ese sería una una bromilla que Podrían haber hecho la otra bromilla que se me ocurre es en plan Swatch no hemos mencionado algunos ataques de mal gusto anteriores de Swat que envían gente a casa policía digamos gente Envíame la policía a tu casa No pues en este caso si marcas un vehículo de alguien que te cae mal como robado pues la policía les va a perseguir Y bueno Yo estaría asustado de si me persigue la policía Bueno aunque no haya hecho nada No pero depende En qué país la policía a veces Bueno no es que sea súper cariñosa Pero bueno también serían otra bromilla digamos así que sería de mal gusto pasamos al tema de Porsche por ejemplo en este caso con esta marca pudieron obtener ubicación del vehículo enviar comandos al vehículo la información del cliente a través de vulnerabilidades que afectan el servicio de telemático del vehículo en el caso de Toyota pudieron acceder de forma no autorizada obviamente al portal financiero Toyota financial y pudiera obtener nombre número de teléfono dirección de correo electrónico y el estado del préstamo de cualquier cliente financiero de Toyota esto es muy interesante también Jaguar y Land Rover de nuevo acceso no autorizado a cuentas de usuario que revelan el Hash de la contraseña aunque no mencionan De qué tipo que Hash es pero bueno probablemente igual un caso de uso aquí para cibercriminal sería crackearlo intentar ver si se puede utilizar en otras plataformas Porque también se podría identificar el email que está asociado también se conseguía el nombre número de teléfono dirección física e información del vehículo y finalmente tenemos a Sirius xm estas Navidades fueron publicadas también en noviembre del año pasado y lo que pudieron acceder fue a claves de aws que permitían acceso a buckets de sc S3 de organizaciones enteras con permisos de lectura escritura capacidad para recuperar todos los archivos que algunos de ellos mencionan parecen ser bases de datos de usuarios código fuente y archivos de configuración para esta empresa Sirius xm vamos que han hecho un aun completo a todas estas empresas voy a mencionar dos casos interesantes porque son bastantes y los vamos a poner en las notas del episodio para que os leáis si queréis en detalle el informe Y también todos los tweets es interesante seguir a este investigador Sam curry porque va poniendo las las que va encontrando las va poniendo también en hilos en Twitter que vamos a Añadir unos cuantos para en las notas del episodio para que lo veáis pero por ejemplo en el caso de BMW lo primero que hicieron fue analizar sistemas web de BMW con herramientas de osint mencionan dos no gau y ffu después de algunas horas de fashing digámoslo de dejarlas corriendo identificaron un archivo wadl que es web application description Language que expone

información de los enpoints de las Apps de un sistema específico de BMW que era x Pita punto BMW group.com y lo que pudiera hacer es enumerar los entpoints de esta de este sistema los en points y ver Qué funcionalidad ofrecen uno de ellos una de las eps una de las funcionalidades que podían acceder podían consultar fue obtener todas las cuentas de usuario de BMW mediante el envío de consultas que incluían el símbolo de asterisco al final del nombre de usuario en en la Epi Por ejemplo si enviabas algo como test y un asterisco pues podías obtener información de usuarios por ejemplo testing o test 1 2 3 o similares sin tener que adivinar el nombre de usuario real Así que ahí puedes empezar con la todas las letras del abecedario en asterisco y te sacas todas las nombres de usuario todas las cuentas no sé si con el asterisco solo sacarían todas igual no igual necesita alguna letra pero bueno que se podían Descargar todas los nombres de usuario una vez que encontraron esta volaridad continuaron probando otros Eso me suena me suena un poquito a squaling Jackson eso se puede poner ahí un asterisco y tal Me pregunto si probaron a cerrar la comilla y todo esto en otro caso sí que lo mencionan Así que en el caso de Mercedes Benz mencionan que estuvieron haciendo pruebas manuales digamos sql y que no obtenían buen resultado luego empeza con una comilla comilla dos comillas y luego de empezar avanzando y sacaron también temas perdón no era Mercedes era un portal creo que era el de spirium un portal que tenía mucha pinta de esto me parece interesante porque por la forma de ver solo un portal de cómo está diseñado los colores las tablas de html dices esto tiene pinta de ser vulnerable así que el injection y efectivamente lo era Sí cuando es cuando es en plan súper cutre de estas de es muy bueno porque mira te pones a hacer capturas de pantalla digamos de páginas web por ahí con un poco de computer Vision dices esto esto parece feo esto parece retro dijo que es vulnerable inyección te da una puntuación de cutrismo y las que están por cinco o más de nivel cutrismo ya empiezas ahí el ataque automatizado Sí sí pues Total que en este caso fueron probando más Apps no encontrar una que Oye curiosamente se llama teotp Oye esto significa o bueno intuían que pudiera ser Time One time password o sea un código que se envía de esos que se envían típicos cuando creas una nueva cuenta no O al restablecer tu contraseña un código temporal normalmente de 67 dígitos que te envían a tu email a tu a tu bueno por sms a tu móvil o incluso te llaman y te lo dicen por voz no efectivamente confirmaron que este Api en Point estaba asociado al servicio de restablecimiento de contraseñas de usuarios de BMW así que a la obra hicieron lo siguiente primero con la primera volaridad de enumerar usuarios la del asterisco enumeraron usuarios arbitrarios eligieron uno segundo fueron la función de restablecer la contraseña para ese usuario lo que sea bmw.com/h reset password le salió la pantalla de en plan introduce el código que tenemos enviado Ok Voy a la Epi hay en esta de teotp y para este usuario me pide un código pum ya tengo el código Lo pongo aquí en la web que tengo de restablecer la contraseña pum ahora me permite cambiar la contraseña pongo la que quiera y ya está tomado control de esta cuenta Qué te parece Pues a ese punto decían que era posible hacerse cargo por completo de cualquier cuenta de empleado de BMW o rolls-royce y acceder a herramientas utilizadas por esos empleados para demostrar el impacto de la vulnerabilidad simplemente buscaron en Google portal de concesionarios de BMW y usaron la cuenta comprometida para Acceder al portal de concesionarios que utilizan los asociados de ventas que trabajan en los concesionarios físicos de BMW y Rolls después de Iniciar sesión observaron que la cuenta que habían comprometido estaba vinculada a un concesionario real y podían acceder a todas las funciones a las que tenían acceso los propios concesionarios esto incluía la capacidad de consultar el número de bastidor o bim específico y recuperar los documentos de venta del vehículo muchas de las vulnerabilidades

publicadas en esta investigación han sido posibles gracias a un único punto de fallo digámoslo principalmente uno de estos dos o explotación de credenciales de usuario que han podido conseguir de alguna forma u otra o claves de apis para gestionar estas estos automóviles estas plataformas web muchas veces el primer paso en estos ataques contra vehículos es la obtención de los secretos como digo credenciales de usuario o claves Api que se encuentran en aplicaciones móviles tanto iOS y Android y luego ya con esta información Se pueden abusar las interfaces de la plataforma como las apis el owash el open web application Security project tiene una digamos un subgrupo que se llama owas Mobile que publica una lista que la llaman owas Mobile top ten que es la lista de los 10 riesgos más importantes en aplicaciones móviles según owasp y ha puesto en el número 2 al riesgo de almacenamiento de datos de forma insegura en las dos versiones que tiene de esta lista top ten publicadas tanto en 2014 como en 2016 se ha mantenido en el o sea esto significa que es algo Bastante problemático que se han encontrado muchas veces tanto los de uvas como bueno las noticias no esto es interesante ya que se identificó como riesgo número 2 El segundo más crítico hace Casi más de 9 años y aún las empresas de aplicaciones móviles no han podido reducir este riesgo de forma similar owas Mobile top ten lista la autenticación insegura como el riesgo número 4 una categoría que incluye temas como autenticación y autorización incorrecta acceso a las apis y temas similares como los abusados en esta investigación que afecta a estas aplicaciones móviles de los vehículos de forma similar a los riesgos de aplicaciones móviles o webs también publica una lista con las diez volaridades más críticas en apis la owas apis Security top ten que fue publicada en 2019 las vamos a poner en la notas en las notas del episodio para que le echéis un ojo también son interesantes últimamente comentar que a ver tradicionalmente ha habido mucho interés y muchas vulnerabilidades identificadas en temas web no pero hoy en día más y más con el tema de containers dockers kubernetes se están haciendo más microservicios micro servicios son estilo apis que es básicamente una URL a la que se le envían parámetros y lo único que te hace es devolverte una respuesta Ya está no es como una aplicación web completa como digamos lo sería una una aplicación web para un banco online en el que te autenticas haces clic en tu cuenta de crédito miras el balance haces una transferencia tiene diferentes pasos está el hacer clic aquí te lleva otro paso te envía un token tienes que autenticarte hoy en día hay muchos estos micro servicios que son básicamente una vez te has autenticado has obtenido un token para la Api lo envías como una cabecera como parte de la petición y ya está es digamos sin estado completamente sin estado en vías petición recibe respuesta Así que se están encontrando muchas vulnerabilidades en este campo de las apis owas ha sacado esta lista top ten también han salido libros últimamente también no Stars tiene un libro también de apis hacking apis no sé si se llama así pero algo parecido Así que es un campo que está un poquito también verde las apis también últimamente utilizan Este lenguaje de consulta graffield no que es un poco así también estilo sql que también se pueden ser inyecciones así que bueno es un campo interesante que se podría indagar más si queréis Ahí os dejamos como como sugerencia queridos oyentes comentar que tradicionalmente las empresas de automóviles se han apoyado más en la ofuscación digamos lo de alguna forma como medida de seguridad para sus aplicaciones móviles aunque esta investigación ya demuestra que no previene ataques con impacto crítico para los productos de dichas marcas y que estas tienen que inverti más en una en seguridad en profundidad o en más temas de seguridad Y a medida que más marcas ofrezcan la opción de desbloqueo gestión de vehículos a través de dispositivos móviles y vehículos también conectados a internet probablemente haya un aumento en volaridades similares a las publicadas

en esta investigación o ataques reales como el daño o robo de vehículos Así que preparados para que bueno vayamos comentando más más noticias de este tipo y voy a extender un poquito más los ataques potenciales porque dándole vueltas a esta noticia en una de las vulnerabilidades Los investigadores listan el hecho de que el fallonalidad permitiría desactivar el motor de arranque Entonces yo me puse a pensar desde el punto de vista de Cyber criminales Cómo se podrían beneficiar de esto no pues se me ocurre de nuevo el punto de vista de ransomware que yo creo que es uno de los riesgos más evidentes y más críticos Porque da sobre todo también ventaja financiera un cibercriminal sería lanzar un ataque de ransomware contra el vehículo dejándolo inservible habiendo desactivado el motor de arranque y pidiendo un rescate Para activarlo de nuevo la nota de rescate del ransomware la podrían mostrar en las pantallas de los sistemas de infotainment con un código QR no para facilitar el código vía móvil además de reproducir una grabación desagradable Como he mencionado anteriormente en el caso que del ataque cubierto Martín por los altavoces del vehículo como con el nombre del usuario junto con palabras malsonantes o bueno o como decíamos gemidos de alguna forma desagradables no motivando a la víctima a pagarlo cuanto antes para que ese sonido se apague y que pueda utilizar el coche para ir a su trabajo porque Oye Son son las 8 de la mañana entra a las 9 y ahora el coche no me arranca Y encima me empieza a gritar ahí dice mi nombre y dice que no he pagado que soy moroso o lo que sea no en este aspecto hace poco leía que las empresas lo están teniendo más difícil para conseguir seguros que les cubran contra ciberataques Y es que cada vez son más frecuentes los ataques de ranso muere contra grandes empresas con cantidades de rescate y daños multimillonarios y más grandes las pérdidas de las empresas de seguros Porque se están dando cuenta de que su negocio ya no le está saliendo rentable y Por tanto se están negando a ofrecer seguros de este tipo Por una parte o si la hacen si te ofrecen seguro te van a requerir unas franquicias o Premium mucho más elevados me pregunto si los seguros de automóviles van a hacerse eco de esto y van a hacerse más caros para los consumidores debido al incremento de la superficie de ataque de vehículos inteligentes o vehículos conectados al irse descubriendo más vulnerabilidades como las de esta investigación y ataques impactantes tipo ransomware al que atención a mí se me ha ocurrido el gracioso nombre de bautizarlo como ranson Will con el sufijo Will por lo de lanzar ataques de ram sawer contra vehículos con ruedas en inglés y también En referencia a que el volante en inglés quedaría bloqueado Qué te parece Martín esta palabra me gusta me gusta tienes que hacer el Trade marking ya eh Y esta palabra no sale de ningún sitio Así que si querías oyentes si la escucháis a partir de ahora viene de tierra de hackers la he creado yo así que así que bueno Esperamos que no sea muy pronto y que no salgan muchos pero en cuanto haya algún ataque de ranson Will no os preocupéis que lo vamos a cubrir en el podcast el equipo de investigadores sugiere que los propietarios de automóviles deben asumir la responsabilidad comentan limitando la entrada de información de identificación personal en estos sistemas web de vehículos no O sea no proporcione mucha información pero bueno de alguna forma el concesionario me pide mis datos de forma legal tengo que como lo como lo limito o es un poquito difícil esto no también mencionan utilizar la configuración de privacidad más alta en los en los sistemas telemáticos Ok Esto sí igual se puede activar Aunque podría venir por defecto ya no no que fuera a optim sino que fuera up no y implementar la autenticación de dos factores de doble factor pero otros especialistas en este campo dicen que son los fabricantes de automóviles los que tienen que asumir la responsabilidad y configurar de forma segura y probar periódicamente sus apis o sistemas web desde el punto de vista de un atacante y bueno y aquí está un poquito el

debate no y con esto llegamos a la pregunta del episodio queridos oyentes que es la siguiente quién Debería ser responsable de los daños ocasionados por vulnerabilidades explotadas por potenciales ataques de seguridad como ranson Wild contra vehículos conectados tenemos cuatro opciones la primera es empresas de automóviles la segunda empresas de ciberseguros la tercera los consumidores es decir nosotros y la última gobierno con esto queremos decir que hay falta de regulaciones el gobierno debería poner un poquito más presión a empresas de automóviles o bueno incluso igual a empresas de móviles porque de alguna forma las aplicaciones móviles también contienen vulnerabilidades que los investigadores han podido abusar para tomar control de los vehículos y ahí lo dejo un poco como en Aviación No que los gobiernos en Aviación pues obligan a las a todos los fabricantes de aviones aeropuertos aerolíneas a tener un mínimo de seguridad en Aviación y en otra que es en otra industria que es también muy mucha presión es en la médica por ejemplo en Estados Unidos la fda desde siempre les ha puesto las pilas a muchas empresas que hacen dispositivos como marca pasos que bueno que son críticos y los medicamentos no así que sí sí O sea Tendría que haber algo en este en este en esta Industria Del automovilismo interesantísima la pregunta a ver qué comentan nuestros oyentes en nuestro Twitter @tierra de hackers como siempre También interesantísima la noticia me encanta cuando Hacemos como toda una recopilación para en plan Bueno no es un caso aislado de un fabricante de un coche chino en plan no no has hablado de rolls-royce de porsches de de marcas tan comunes como un Mercedes y además con diferentes consecuencias no estos ataques con diferente impacto siempre está el tema de la privacidad es una de las cosas que a mí me encantaría a pesar de que no es santo de mi devoción Don elon musk Pero me encantaría tener un tesla lo que lo que me tira para atrás Es toda la información que tienen sobre mí cuando ya cuando compro el coche pero es que luego todas las que están apuntando todo lo que se sube a la nube donde estoy como voy Qué velocidad qué tal claro es el problema de los coches cada vez más modernos que vienen con sistemas de pilotaje automático de asistencia al conductor y tal que al fin al cabo tiene un impacto brutal en tu privacidad es un poco como como lo que pasó con las Smart tvs no antes era una televisión y está conectada a internet y tal Y ahora todas las televisiones están conectadas a internet hubo la época donde incluso tenían cámaras la mayoría de ellas Entonces vamos perdiendo privacidad cada vez que hacemos los dispositivos más inteligentes que tiene sus pros pero también tiene tiene sus cons y con los coches la verdad es que van a quedar pocos ya donde el único dato que das es efectivamente cuando compras el coche pero es que ahora es por dónde vas en todo momento grabándote tal Sí me tira bastante para atrás la verdad poco a poco el gran hermano se va metiendo en nuestras casas Así que con esto no quiero meter el miedo pero no pero es que es verdad es verdad y además O sea me parece personalmente No no quiero hacer un vayas aquí a o inclinar la balanza como nuestros queridos oyentes contestan a la pregunta que les has planteado pero me parece bastante de chiste que los fabricantes digan no no la culpa es vuestra por no hacer las cosas bien Vamos a ver si soy yo el que Configura el escenario donde te obligo a meterte es decir si yo construyo una casa y te metes en la casa Cómo joder tendré que Construir la casa primero de manera segura y luego pues sí si tú te tiras por una ventana Oye pues no te tires por la ventana pero si yo me meto en la casa y se derrumba el edificio no no te puedo echar la culpa a ti decirte bueno no entres en la casa no Por así decirlo como un ejemplo tonto flipo que los fabricantes digan no la culpa es vuestra no pongáis datos todos los datos personales pero si me los estás pidiendo Ah no poner en la política de privacidad que que activar que queréis privacidad bueno pónmelo perfecto lo que decías tú no es me parece bastante

absurdo y ahora la estaba intentando Buscar pero es que no la encuentro pero he leído hace poco que en España al menos hay una iniciativa nueva también de bueno de mucho más rastreo y obtención de datos telemáticos de vehículos no sé si para bueno para ofrecer mejor mantenimiento o para bueno para pagar un poquito más de forma más más fácil pero ahora no la encuentro Pero bueno ha salido algo algo al respecto hace poco que lo he visto y me pareció interesante también y lo que se me olvidó mencionar era cubrimos también en otras noticias anterior en el episodio 62 cubrimos el tema de mikodus GPS esos habían fallos en 1.5 millones de dispositivos GPS que se utilizaban en vehículos desplegados en 169 países que es muy similar al caso de esta de esta empresa que se llama spireón no que es una empresa de gestión de flotas GPS Así que como decimos se van dando cada vez más casos y cuando investigadores se pongan me voy a poner a investigar esta empresa porque me gusta esto del GPS tal van a ir saliendo muchas más así que bueno como digo vamos a irlas cubriendo Y a ver cuándo salen los ransomwills me ha encantado eso de ranson Will desde luego está claro que hacen falta expertos en ciberseguridad en todos los campos en todos los ámbitos en todo tipo de industria pero el automovilística está has dejado muy claro que desde luego ahí tiene que haber demandas esperemos que haya demanda Y la verdad también es un es un espacio por lo menos para mí bastante atractivo no dedicarte a hacer los coches seguros a intentar hackearlos y todo eso a mí el tema del Carl hacking siempre me ha parecido muy sexy no por el tema de que une el tema ciber con el físico pero en este caso estos investigadores han hecho hacking que podría estar a la misma altura a la misma talla de hacer hacking físico Hardware de vehículos pero macho lo han hecho todavía web y Api hay y tiene un impacto incluso o casi mayor que haber hecho haber descubierto una vulnerabilidad en la Easy you en el en el computador este que lleva interno como han hecho como publicaron la primera vez no el Charly Miller y Chris balasec eso fue eso fue un antes y un después no en tema de cara hacking pero es que esto no sé también es un antes y un después en tema Carl hacking pero lo vamos a llamar web Carl hacking que es como lo vamos a titular un poquito esta noticia tal cual tal cual una especie de site Channel Attack no que en vez de ir a por el coche en Sí pues pasa por los sistemas que lo controlan y todo esto a nivel de web la nube todo esto Pues bueno nuestros queridísimos oyentes Hemos llegado al final del episodio un poquito largo Pero esperemos que como siempre os haya gustado si así lo creéis que lo merecemos por favor por favor dejarnos una review cinco estrellitas lo que sea en la plataforma que nos estáis escuchando que nos ayuda un montonazo y os cuesta 5 o 10 segundos como mucho recordad que tenéis en nuestra web en tierra de hackers.com todas las notas del episodio todos los enlaces no Solo lo hacemos para dar crédito a las personas que escribe los artículos a los investigadores que hacen estos proyectos tan interesantes o a simplemente a todas las fuentes de donde sacamos la información queremos desde luego dejarles un enlace para que lo podáis visitar pero si no también para que vosotros podáis indagar todavía mucho más Muchas gracias por quedaros hasta el final empiezo un nuevo año van a venir muchas más cosas con tierra de hackers gracias Gracias por apoyar Muchas gracias Feliz año nuevo 2023 y nos vemos en el próximo episodio con más noticias interesantes Adiós adiós hasta luego chao chao si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers