sabes esa captura de pantalla que has hecho con tu móvil y has editado antes de compartirla para eliminar una parte sensible como parte de tu pasaporte o algo comprometedor que se ve en la imagen pues una vulnerabilidad permite recuperar la original can injection una nueva técnica de robo de automóviles similar a hacer el puente que criminales están utilizando para llevarse coches modernos y que requiere conectar un dispositivo ilegal a los cables de los faros del vehículo entramos en la cuenta atrás para llegar a los 100 con este nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast de publicamos este episodio en 10 de eso estaba mirando 10 de Abril de 2023 este es el episodio número 90 yo soy Martín vigo y está conmigo ni siquiera puesto la bromilla de turnos Alexis porros Fíjate si voy con prisa qué tal Alexis hoy así sin titubeos sin sin cosillas directamente qué tal Alexis como dicen los los buenos no en plan Do it Life Do it Life estamos haciendo una demo y esperemos que no salga bien la hacemos este episodio Aquí bien contigo otro episodio más así que ya vértigo estos números el 90 Pronto pronto el 100 3 dígitos Así que nada muy contentos de estar aquí con todos vosotros queridos oyentes Y también muy contento por siempre por apoyarnos online en redes sociales ya sabéis no hace falta que las nombre ya las he repetido 90 veces así que nada lo que sí que me gusta a repetir porque es algo más nuevo es el tema que estamos en discord que podéis acceder a ello a través de tierra de hackers.com barra discord y también el tema de que estamos en mastodon a como infoset punto exchange en el servidor Aunque bueno Twitter de momento se está comportando Aunque hay cierta polémica pero no vamos a entrar en ello y también el tema del podcast debería estar suscrito si no lo estáis Así que hacerle click a suscribirse para que recibe los últimos episodios y listo con todo esto también quería cubrir como siempre la noticia del episodio que para el episodio anterior la pregunta la pregunta Perdón no sé qué he dicho Es que voy tan rápido ya la noticia Dale dale como cura la noticia del anterior que es la siguiente Estás de acuerdo que deberíamos de tener el desarrollo de tecnologías de Inteligencia artificial durante seis meses como piden muchos expertos os dimos dos respuestas posibles sí y no y la del no obtuvo un 60,8% es un poquito más aplastante que él en la pregunta anterior que está muy reñido el tema y la del sí es un 39,2% así que bueno vemos Que hay gente que no no seguir avanzando que quiero Supongo que están interesados en el tema de la Ai Pero bueno hay gente que todavía tiene algún alguna preocupación al respecto muy bien y yo pues lo de siempre darle las gracias a la peñita que está ahí en patreon apoyándonos Muchísimas gracias que cada día sois más y nos ayuda un montonazo y también por supuesto nuestros sponsors que en este episodio tenemos a de vuelta un branding una empresa formada de por especialistas en varios ámbitos profesionales que se enfocan en la reputación online a múltiples niveles han ayudado desde personas como tú y como yo hasta famosos a llevar a juicios casos de ciberacoso mitigar situaciones donde la reputación de estas empresas estaba siendo mal intencionadamente dañada incluso 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 en su servicio si necesitáis algún tipo de ayuda con vuestra identidad digital ya sabéis o branding es lo que estáis buscando visita ombranding.es o nbrandi ng.es y también queremos darle las gracias a brawler Pro por apoyarnos en el podcast otro de nuestros patrocinadores brawler pro es la herramienta más completa de seguridad en aws empresas de todos los tamaños se apoyan diariamente en brawler pro para que sus equipos puedan confiar en su modelo de seguridad de WS puedes probar prauer Pro hoy mismo y de manera totalmente gratuita obtendrás paneles y gráficas con información concisa y accionable con todo lujo de detalles sobre la madurez de tu modelo de seguridad y una visión completa de infraestructura en todas las regiones de aws y además tendrás todos los resultados en apenas unos minutos empieza a usar brawler pro y beneficiarte de sus resultados

visitando tierra de hackers.com/uler proprowlrpro pues perfecto pues ya voy yo con la primera noticia no sin antes recordaros lo de visa Barcelona que tenemos Cold papers llamadas para voluntarios tickets a la venta o sea que no os olvidéis de eso os Traigo una vulnerabilidad que se encontró hace unas semanas muy curiosa la verdad curiosa y no demasiado compleja pero con un impacto Oye pues potencialmente muy alto como Vais a ver especialmente si tu teléfono es un Google Pixel ya sabéis el teléfono de con sistema operativo Android pero que además el propio Google hace que creo que van por El séptimo alguna vez te pregunto querido oyente has enviado fotos con información confidencial que querías no Mostrar Como por ejemplo no sé al enviar un pasaporte o documentación de como una tarjeta de identificación con marcas de agua para que así pues Si alguna vez se filtra pues estar más seguro o quizás eres de esos que luce su nueva tarjeta de crédito en redes sociales Pero por supuesto no sin antes editar la foto desde el teléfono cubriendo los números de la tarjeta o voy más allá alguna foto subidita de tono que en confianza bueno compartes con tu pareja pero donde quizás pues te has cubierto la cara editando la foto bueno por si acaso no pues tengo malas noticias querido oyente si esto lo has hecho desde tu teléfono Google Pixel esas fotos que has subido a internet de manera de una manera u otra y que te aseguraste antes de enviarla de cubrir zonas sensibles con la herramienta de edición de tu teléfono puede ser desenmascarado una nueva vulnerabilidad que afecta a todos los Google Pixel y que su autor Simon Arms ha denominado acropalipsis permite revertir las imágenes editadas para editar para cubrir zonas sensibles y restaurar la imagen original Bueno a decir que acropalips pues hombre es un juego de palabras entre cropping que es como recortar lo de recortar una foto y apocalíptico no pues pues de ahí viene el nombre en otras palabras si has usado un teléfono Google Pixel para subir a internet fotos de tus hijos cubriéndoles la cara como hacen Pues muchas familias no cuando tienen un bebé ahora cualquiera puede ver la cara de tus hijos la foto de la llave de la primera casa que te has que te acabas de comprar y orgullosamente luces en instagram Eso sí previa adición para cubrir las muescas los dientes de la llave y que nadie te la puede clonar pues ahora cualquiera puede clonar tu llave tan fácil como irse a la web que ha publicado el mismo autor de la vulnerabilidad como prueba de concepto Sólo tienes que subir una foto editada que está cubriendo o está recortada y te la muestra inmediatamente sin los filtros o sin los recortes es decir la foto original parados a pensar unos segundos en alguna foto que hayáis subido cubriendo alguna zona estoy convencido que el 99% de nuestros oyentes alguna vez lo han hecho yo por lo menos lo he hecho pues no sé Mientras preparar la noticia pensaba no cuando quise Compartir por ejemplo que me dieron la Green Card en Estados Unidos no eso fue un día muy feliz para mí la greencard pues es el visado por excelencia Por así decirlo que Estados Unidos lo que pasa es que por supuesto como cualquier tarjeta de identificación contiene mucha información confidencial pues yo la compartí entre entre amigos y familiares una fotillo como sujetando la Green Card No y cubrí esa información es decir estaba subiendo un documento muy sensible pero a la vez cubriéndolo la ventaja que yo tuve Es que yo normalmente lo que hago es cubrirlo físicamente es decir yo lo que precisamente porque no me fío de estas cosas y mira que me ha salido pero en vez de hacerlo por software no editando la foto y quitando pues números de identificación y cosas así pues yo lo cubrí con mis propios dedos entonces yo te pregunto Alexis a ti se te ocurra porque ya te digo yo mientras preparaba esta noticia se te ocurre alguna foto que hayas subido de esto pues ya te digo que con el típico rotulador digital este no pues cubres A lo mejor una dirección de un tag de yo que sé de cuando te envían un paquete o documentación que tienes que subir y que como buena recomendación la subes como una marca de agua cosas así y yo y como tú como también soy paranoico y no me fío de estas aplicaciones no no usos y si lo uso para realmente lo que hago mi modus operandi es no sé si estoy revelando aquí una vulnerabilidad de cómo me pueden

atacar Pero creo que es bastante seguro tú me puedes decir después de esta noticia que ahora sabes más si si lo que hago es con una software de modificación de imagen es tapo con en negro lo que quiero y luego hago una captura de pantalla que eso espero que no hago Exactamente lo mismo y de hecho es una de las recomendaciones que tenemos Cuando entiendas la y la otra también que hago es si no imprimir a PDF directamente que creo que eso también elimina posibilidad de recuperar los datos redactados pero sí ahora entro un poquito más en los detalles pero muy buena recomendación esa el tema es que no solo hablamos de fotos en las que digamos ocultamos información mediante el editor no que trae el propio teléfono pues ya digo quizá pasándole como dices tú Alexis el típico la típica rayita negra no para cubrir algo también se puede recuperar en su totalidad las imágenes que hemos recortado como decía que Entonces ahí es donde yo eso sí ya lo hago bastante más a ver en general A veces es por quitar algo trivial pero sí que a veces es Ah Pues he recor todo esto y por tanto no me no me he molestado en cubrir la zona o sea no he cubierto la zona y recortado si lo recorto de eso sabes no he sido tan cuidadoso digamos al si podía recortar una foto porque entonces ya consideraba que lo había eliminado mientras que cuando no podía recortarlo sino que tenía que cubrirlo ahí sí que era más cuidadoso y lo cubría físicamente pues las fotos recortadas también se pueden recuperar en su totalidad esa foto tuya saltando en el mar en el pelotas no que recortaste de cintura para abajo para pasársela a tus amigos de WhatsApp pues tus amigos pueden verte como tu madre te trajo al mundo tú Alexis me imagino que también no O sea no lo de saltar en pelotas que sé que tienes una vida una segunda vida oculta en la noche pero nada estoy de coña Pero has hecho eso también me imagino a la hora de digamos filtrar fotosensibles no recortar directamente sí Bueno sobre como tú y como yo cuando tenemos que la parte más divertida de hacer retti mini seguridad ofensiva es como todos sabemos hacer informes Y entonces en esa parte muchas veces he tenido que poner imágenes de evidencia no de lo que he conseguido y en esa pues a veces redacto temas o a veces como tú dices recorto porque he conseguido una imagen de algún sitio o hecho una captura de pantalla y solo quiero que la gente se Centre en lo que quiero que vean y además porque lo de alrededor No no me es confidencial Y entonces lo recorto pero si en ese caso por ejemplo lo he hecho sí Bueno en general como las fotos hay ya van parte del PDF pero sí por si alguien no había pillado el Sarcasmo los reportes es lo peor de cualquier cosa Bueno qué es lo que ha pasado no porque Hemos llegado hasta aquí porque ahora cualquiera puede recuperar las fotos originales de las ediciones que nosotros hemos hecho y que hemos subido a internet recordemos Pues resulta que parece ser un fallo en como Android las fotos png de esta digamos formato cuando las recortas o modificas no quiero entrar en los detalles super técnicos porque hablan de algoritmos de compresión de imágenes y yo creo que aburriríamos aquí un poco al personal pero aún así os dejo el blog post donde explican el fallo y también pues el enlace al Tracker de Google donde Bueno se puede un poco ver dónde dónde se cometió el fallo y cómo lo están solucionando pero básicamente y de manera simple cuando tú modificas una imagen o la recortas el teléfono no se deshace de la foto original sino que digamos como que la deja ahí dicho mal y pronto almacenada junto con la foto editada es como si la foto editada tuviera dentro aún la imagen original de manera que estos investigadores consiguieron una manera de recuperarla Esta es evidentemente una vulnerabilidad que se ha dado una evaluación no de crítica pero sí de impacto elevado y ya las enaron un CV para identificarla que es el sube 20-23 21 036 esto de que la imagen contiene la imagen me recuerda también que creo que todavía se sigue utilizando Es que hace tiempo que no uso mucho Windows de cerca del tema de esto de los neil.dv este archivo no que tiene la miniatura de todas las imágenes o incluso no solo imágenes sino los documentos de PDF también en la primera página por ejemplo pues también creo que de eso se hace una mini

capturilla de pantalla digamos y también se contiene creo que en el porque cuando usas la vista de creo que se llama iconos en el explorador de Windows pues ahí se ve es de donde saca la imagen eso lo hace una vez cada vez que se añade un archivo nuevo No Y ahí se guarda pero igual Es algo similar si no no tal cual porque de hecho preparando un curso de Office que estoy preparando para para dar muy pronto pues me he encontrado un caso en el que una famosa subió una foto suya a su blog recortando la foto y no sé si la recortaba o editaba los pechos no porque aparecía pues pues bueno pues en la playa de manera normal y pues un poco se tapó no y ya empezó a correr por internet su foto sin cubrirse los pechos y era precisamente porque dices tú porque la foto que subió contenía el original dentro como la preview esta y por tanto fue lo que encontró la gente que eso en sí no es una vulnerabilidad porque eso Realmente es como es la funcionalidad no pero un afiche pero digo sobre todo porque aquí hay una diferencia Porque aquí sí que explotaron digamos debilidades en Cómo Android implementó el Cómo funcionaba la compresión de imágenes en que cuando hacemos capturas de pantalla en teléfonos Google Pixel sé que muchos de vosotros queridos oyentes estáis pensando esta semana me he Librado no los de tierra de hackers me han vuelto a hablar de una nueva vulnerabilidad pero en este caso a mí no me afecta porque ni tengo ni uso un Google Pixel como teléfono Okay querido oyente Qué sería de tierra de hacker sin su ya clásico plot twist ese giro dramático de los acontecimientos que cuando crees que te ibas a ir de rositas va Martín y te dice quieto parado quieto para resulta que el investigador que encontró esta vulnerabilidad lo publicó en Twitter y otros investigadores empezaron a fijar en las características de la vulnerabilidad entender el fondo de Por qué sucedió esto lo que os decía antes del tema de los algoritmos de compresión de imágenes y todo esto Y entonces uno de los investigadores se dio cuenta que la herramienta por defecto para hacer capturas de pantalla de Windows 11 también es vulnerable O sea que este problema ya no solo afecta capturas de pantalla hechas en tu teléfono sino también en tu ordenador Esto fue comprobado por David bucanam y os dejo su tweet de cuando lo descubrió pero básicamente el problema de fondo es el mismo y de hecho haciendo unas pocas modificaciones a la herramienta publicada por el investigador de acropalipsis las imágenes editadas en píxeles y todo esto pues pues simplemente lo que podía hacer era con esas pocas modificaciones hacer lo mismo en sistemas Windows 11 Es decir de Las capturas de pantalla que se editaban o se recortaban Pues con esa misma herramienta a recuperarlas ya sabéis queridos oyentes la edición de imágenes no es suficiente a veces para ocultar detalles sensibles en tus fotos debemos tomar otras medidas yo por ejemplo algo que hago siempre cuando no puedo poner una barrera física Digamos como un trocito de papel o mis dedos para tapar algo es lo que o sea después de editar la foto hago exactamente lo que decía Alexis una captura de pantalla de la captura de pantalla por tanto esa captura de pantalla es una nueva imagen que no contiene ninguna información del anterior porque esto es el equivalente aquello que se que tú le hagas una foto a tu teléfono prácticamente mostrando una imagen no del todo pero pero básicamente por tanto al ser dos imágenes diferentes eso evita este problema Así que quedaros con esta recomendación siempre barreras físicas en vez de edición de imágenes y cuando no se pueda editáis la imagen y luego le hacéis una captura de pantalla a esa imagen Y así por lo menos pues está la cosa un poquito mejor y como ya os digo os dejo todos los detalles en las notas y enlaces del episodio a todo esto has dicho que la aplicación la vulnerabilidad está en Google Pixel y en Windows 11 esto en la aplicación de captura de pantalla y edición de imágenes que viene por defecto en ambos dispositivos efectivamente efectivamente si alguien usa otra Hay muchas pero una que la gente usa mucho en Windows por ejemplo Green Shot se llama Bueno hay varias no pero es snack o cualquiera que sea otra es en principio no debería tener la vulnerabilidad no esa en principio no bien bien pues esa sería otra idea como como Bueno sí lo que pasa es que lo

importante aquí es no no es cambiar la herramienta sino cambiar el hábito no porque quien te dice a ti que no volverá a pasar esto el hábito Es el monje correcto y el tema también que quería comentar es que otra forma de que también Creo que he leído online es para evitar esto es convertir formatos no haces una captura de pantalla en png como tú dices Martín que creo que estás aplicaciones que decimos que tienen esta vulnerabilidad creo que por defecto hacen png pues se podría luego convertir a jpg y ahí se pierde también todo el tema de la compresión o el tema ese de la vulnerabilidad que se ve de la imagen original dentro de la imagen modificada incluso puedes liar más la troca si no te fías de jpg a despeje a jpg a png ative a png a yo que sé te lo puede montar como quieras Sí un poco como el tema de criptomonedas que usamos a veces no pasa lo de bitcoin a monero de monero a ethereum y otra vez a monero y luego a bitcoin ahí se pierde se pierde rastro Pero bueno casi más fácil casi más fácil hacer captura de pantalla de captura de pantalla o incluso Oye mira se me ocurre un poco en plan desinformación como está la vulnerabilidad y la gente la conoce ahora van a ir a mirar la foto original Pues realmente en la foto original pones algo que sea de desinformación en un documento Así que se ha publicado así legal yo que sé del gobierno de algún país o sea esto vale sabes a qué me recuerda las fotos estas míticas de WhatsApp que te llegan por teléfono y luego te sale el negro de WhatsApp se podía hacer en plan troleo tío una foto que cuando recuperas Pues yo que sé sales tú Sale sale el negro de WhatsApp y otra hay una vulnerabilidad también que me ha venido a la mente a partir de lo que decías el tema que de que hubo no me acuerdo cuando y creo que lo son tantos episodios que ya no recuerdo cuál pero creo que en un episodio comentamos el tema de a una vulnerabilidad nada no totalmente la misma pero era aquella en la que la gente estaba redactando imágenes sobre todo texto aplicaba más a texto que realmente una parte del cuerpo no y era que utilizaban este este filtro o este esta forma de redactar que no es un color único y opaco sino que era el tema de hacer pixelar un poco el texto y alguien descubrió una forma de cómo no recuperar totalmente nítido el texto original Pero oye lo lo digamos que lo de no descifraba no pero como cuando ves el canal Plus no que está todo así como gris y tal y cierra los ojos así lo pones y se ve algo pues algo si se veía un poquito mejor entonces de ahí sacaron que oye eso es una vulnerabilidad se puede recuperar un poquito el texto original en base a si utilizas este tipo de forma de redacción de texto en imágenes Sí sí de hecho me recuerda a que algunos investigadores tío No sé si fue europoldo así publicaron una imagen de un de un sospechoso Bueno me imagino que no fuera no sería solo sospechoso si publicas en la imagen pero de alguien que estaba acusado de delitos de abuso sexual infantil y en la imagen esa persona evidentemente recortaron la parte del menor no pero para que no se lo reconociese o había utilizado un algoritmo de Photoshop un poco que salía como su cara en espiral no había aplicado un filtro en espiral pues qué bueno tío que unos investigadores no sé si eran de Canadá sabes en plan lo que has hecho es horrible así que vamos a ayudar y consiguieron reversar el algoritmo que deformaba la cara en forma de espiral un poco y gracias a eso no recuerdo si lo llegaron a pillar o no pero vamos recuperaron la imagen del tío prácticamente perfecta una pasada tío no hay nada mejor para unos investigadores que una buena motivación de poder meter a alguien así sabes en la cárcel de por vida esa no la había escuchado pero sí sí me encanta sí a ver si lo encuentro y lo pongo en las notas del episodio luego me gusta esa es buena y yo De hecho no he hecho lo de la espiral pero el tema de redactar como digo de nuevo en informes sí que he utilizado el tema del pixelado y como también algo dentro de mí me decía que no eficiara mucho lo que hacía era hacer el filtrado pixelado más de una vez porque si lo haces una vez si haces la espiral una vez es más o menos fácil pero haces una haces otra haces otra y eso ya no te lo recuperan al menos es muy difícil que te recuperen Sí sí sí porque aparte yo recuerdo creo que la cubriste tú se basaba también en que previamente sabías Cómo eran las letras porque si tú no sabías

Cómo eran la forma de las letras que se habían pixelado esa información es esencial porque entonces puedes hacer Pues un poco intentar adivinar correlar y cosas así pero claro lo que dices tú si embadurnas lo embadurnado ya es más complicado pues muy bueno Martín Bueno pues antes de que pases tú a tu noticia Alexis lanzó la pregunta del episodio que yo creo que puede puede estar muy bien en este caso y la pregunta es la siguiente Cómo ocultas las partes de las fotos que contienen algo que no quieres enseñar antes de subirlas a internet y se me ocurrieron tres opciones una edito la foto con la aplicación como muchísima gente hace la segunda es tapo físicamente al sacar la foto y la tercera no subo fotos confidenciales así que ya sabéis como siempre Twitter arroba tierra de hackers Mientras nos lo permita lo Mask allí pondremos la votación ir a votar gracias gracias Y sí Y si os ocurre alguna que ser agradecido me lo enseño mi madre Hay que ser agradecido siempre eso siempre Muchas gracias Y si se os ocurre alguna más yo diría incluso Añadir algún comentario que estamos aquí para aprender porque esto nos puede pasar a todos a Martín y a mí así que igual hay alguna técnica que más que agradecidos pues nada antes vamos a pasar con la siguiente noticia pero antes de eso queremos dar las gracias a otro de nuestros patrocinadores en este caso 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 con 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 enviarles vuestro currículum a tierra de hackers arroba monat.commod.com y ahora sí pasamos con la siguiente noticia que me ha hecho gracia lo que ha dicho Martín que en esta noticia no hay nada motivar un poquito a los investigadores para que identifiquen realmente la vulnerabilidad y o formas de saltarse la más como por ejemplo el tema de la espiral esta esta también viene motivado por algo que le pasó a un a un investigador de seguridad y ahora Vais a ver la historia para hacer un breve resumen para dejaros ahí un poquito con el aperitivo esta noticia va de robo de coches en este caso un Toyota Rav4 mediante el uso de un dispositivo comprado en lardar web que vale unos 5.000 Dólares pero realmente contiene solo Hardware valorado en 10 dólares y también es requisito indispensable acceso físico externo al vehículo ya en episodios anteriores hemos comentado noticias relacionadas con vulnerabilidades en vehículos en el episodio 13 cubríamos el tema de Black and pound esos dongles de 2 que eran vulnerables por temas de radio comunicaciones radio comunicaciones Bluetooth y permitía permitían detener un automóvil en movimiento en el episodio 78 comentamos el tema del web Carl hacking esto ya era a través de la web no necesitaba acceso físico al automóvil pero se demostró que marcas de automóviles de lujo Incluso como Ferrari Porsche o BMW y otras marcas como Ford ondas y Toyota también en este caso corrigieron múltiples vulnerabilidades que Podrían haber permitido la toma de control total de estos vehículos e incluso ataques de tipo ranson Wii o donde si os acordáis de aquel concepto interesante de ataque y luego en el episodio 53 también cubrimos dos noticias una sobre como un investigador descubrió una forma de abrir las puertas y maletero de un tesla remotamente a través de bluetooth Slow Energy y sin interacción por parte de la víctima y varios modelos de coches de la marca Honda yakura vulnerables a ataques de Replay que permiten a un atacante Acceder al coche y arrancarlo remotamente en el pasado los ladrones robaban coches utilizando ataques como los que he mencionado o incluso también Relay o retransmisión en los que se amplifica la señal entre el automóvil y mando o control remoto que se usa para desbloquearlo y encenderlo los sistemas de apertura y encendidos sin llave Generalmente solo se comunican a distancias de unos pocos metros normalmente unos 20 metros al colocar un dispositivo radio cerca del vehículo los ladrones amplifican el mensaje

normalmente débil que envían los automóviles y con suficiente amplificación los mensajes llegan a la casa u oficina donde se encuentra el mando de distancia del vehículo y cuando este responde con el mensaje criptográfico que Desbloquea y enciende el vehículo el repetidor del ladrón lo transmite al automóvil con esto El ladrón entra al vehículo con el motor encendido y se lo lleva ahora que la gente es más consciente de esto Supongo que Esperamos que en parte gracias a los episodios de tierra de hackers Pero supongo obviamente por tema de concienciación global No pues ahora que la gente sabe más cómo funciona este tipo de ataque de Relay o retransmisión los propietarios de los automóviles guardan O al menos deberían guardar si han aprendido la lección sus llaves en una caja de metal o una caja de estas tipo faraday que bloquea la señal de radio del automóvil y algunos fabricantes de automóviles ahora incluso proporcionan llaves que se duermen o desactivan si no se mueven durante unos minutos y así no recibirían el mensaje radio del automóvil y no responderían Esto fue una derrota para los criminales que utilizaban Esta técnica para robar coches pero no dispuestos a renunciar a una actividad tan lucrativa adoptaron una nueva forma de robar vehículos y es eludir todo el sistema de llave inteligente y lo hacen con un nuevo ataque que lo han llamado Can injection o inyección a la red cambus del vehículo que ahora voy a comentar un poquito más de qué se trata este ataque se puede ver como una versión moderna de hacerle el puente o Hot writing desde fuera del vehículo Martín tú esto te acuerdas sabes en su época no sé si sabes que es hacer el puente a un vehículo cómo funciona hombre claro sabes cuando tenía 15 años iba yo robando coches por ahí Para ganarme la vida no pero es muy de hecho es de esas cosas de pocas cosas de Hollywood que en realidad son ciertas que se puede pasear de hecho Mira veía el otro día que se hizo viral en tiktok sabes que a veces dice pues el juego de no sé qué el juego no sé cuánto y muchos casos de hecho es bastante peligroso pues había uno que era el juego del Hyundai o algo así que con un cable cargador del iPhone podían arrancar el coche y por tanto los chavales se ponían no solo a arrancar coches ajenos sino a conducirlos y grabarse en tiktok después de haber robado el coche una locura Pues con un cable de iPhone y un destornillador creo algo así eso cuando estaban dentro del vehículo Supongo sí cuando estaban ya dentro cuando se habían roto el cristal o algo estaban dentro y metí en el cable que debe tener alguna lógica o algo sí a lo mejor o mira no recuerdo los detalles porque fue hace bastantes meses pero no sé si si la coña se trataba solo de poder arrancarlo y por tanto el Cómo accediese internamente al vehículo pues da lo mismo o había una manera también de abrir la puerta pero yo me acuerdo que la coña era que le quitan el típico plástico embellecedor a donde está la llave y por dentro pues con la forma del USB del cargador o sea el típico cargador de Iphone que por un lado tiene el Lightning no y por el otro el USB pues ese era justo la forma que encajaba ahí y encendían el coche tío Mira añádolo a las notas del episodio luego te lo para que lo vea la gente los vídeos y ya te digo chavales de 16 años robando coches y grabándose por ahí aparte la coña del juego de tiktok era que ibas tenías que ir haciendo eses por la con el coche robado o sea flipa de hecho Igual hasta tiene si se conectan a un cable de estos del vehículo digamos de forma externa iguales incluso algo muy similar a lo que estoy comentando y es no precursor no no no no De hecho de hecho es verdad que me he ido un poco por las ramas en el sentido de no tiene nada que ver con hacer un puente que tú me preguntaste exclusivamente lo de hacer un puente No En ningún momento hay ningún cable ni nada básicamente el USB tiene una forma que entra justo en la ranura que normalmente entraría la llave pero no hace falta la llave porque le has quitado la parte esa de la cerradura Solo tienes que físicamente girar el cilindro Y entonces justo el USB del cargador del iPhone bueno o de cualquier cargador cabe entonces no tiene nada que ver con con el puenteo de esto Ah vale tendría que que usaban alguna conectaban el cable algún cable Ok Ok es que justo Mira se dio ahí la casualidad que puente cable cargador pero sin podían usar

perfectamente un pincho USB algo creo que incluso he escuchado porque he visto alguna noticia de tiktok que últimamente está también polémico no un poco como Twitter por otros temas no pero sí también he visto que había en plan la gente se quejaba de que adolescentes estaban compitiendo en este tipo de juego de robar vehículos Y dices Se podrían dedicar a temas más interesantes pero bueno sí como dice Martín ha explicado lo que es hacer el puente de forma excepcional Así que no lo voy a comentar yo pero lo que quería comentar a raíz de eso es que hoy en día los ladrones con este nuevo ataque pueden robar coches sin tener que meterse dentro de ellos porque el tema de hacer el puente a un vehículo requería en su momento que tenías que estar dentro del vehículo de alguna forma has abierto la puerta o roto el cristal y estás dentro mira lo he encontrado mientras hablaba el reto era con el hashtag Kia Boys que Kia pues es en los coches Kia y voices pues una manera de decir chicos no y eran los guías y en Chicago se aumentó los robos estaba buscando el porcentaje aquí pero no lo veo para aumentar los robos de los Kia un montón porque ya te digo por el por el rollo este o sea que los coches que ya lo robaban con con cargadores de teléfono tío casi a Mira casi un 800% se incrementaron los robos en Chicago de coches cuando salió el este Así que si quieres añadirlo a las notas del episodio Sí sí claro lo vamos a Añadir eso es un dato muy interesante para que estemos todos al tanto porque sí sí muy buena pues hoy en día como digo lo que hacen los ladrones es no necesitan entrar dentro del vehículo para hacer el tema este de hacer el puente lo que hacen es utilizar dispositivos especialmente diseñados para el robo del vehículo para interactuar con la electrónica y las redes internas del vehículo que se conectan a los cables conectados a los faros del automóvil de la víctima una vez enchufado este dispositivo a estos cables que tiran de las luces del automóvil los ladrones pueden desbloquear encender y llevarse el vehículo antes de que el propietario se dé cuenta de lo que está sucediendo Cómo se ha descubierto Cómo se ha llegado a identificar este tipo de ataques Pues esta fue una investigación un poco desgraciadamente reactiva digamos así tipo análisis forense dos investigadores de ciberseguridad de automóviles y antagor que trabaja en el grupo edak que se dedica a temas de ciberseguridad y otros temas tecnológicos y que además es organizador del Carl hacking Village de Reino Unido y kentindle el sitio de canis automotive labs comenzaron a analizar estos ataques después de que a tavor le robaran su Toyota Rav4 2000 de 2021 el año pasado todo empezó en abril de 2022 tabor publicó unos mensajes en Twitter compartiendo su frustración malestar enojo por encontrarse su Toyota Rav4 con el guardabarros frontal colgando como muestras de marcas muescas de destornillador y el cableado de las luces delanteras estando fuera de lugar estaba enfadado pero lo calificó como vandalismo no sé no le dio más no sospechó más sobre este incidente y dijo Bueno esto debe ser algún graciosillo que me ha querido desencajar el frontal las luces luego tres meses después en julio le volvió a pasar lo mismo guardabarros frontal colgando y cableado en luces delanteras tocado aunque esta vez la foto de su coche que puso en Twitter no se veía tan destrozado no se ve tanto destrozo como en la primera ocasión Los vándalos digámoslo entre comillas habían hecho su actividad con más elegancia y luego dos días después Boom su coche desapareció lo habían robado gracias a la aplicación móvil de Toyota pudo ver dónde estaba el coche y de hecho vio que en ese momento en lo que estaba mirando la aplicación estaba en circulación no solo el suyo sino que el Toyota Rav4 de su vecino también fue robado momentos después tabor comenzó estudiando detenidamente el sistema telemático que se llama my t la aplicación móvil que utiliza Toyota para rastrear las anomalías del vehículo conocidas como códigos de diagnóstico de problemas o diagnostic Travel coach algo interesante de estos códigos es que algunos de ellos incluyen una recopilación de datos del sensor alrededor del momento del fallo es decir un poco antes y un poco después esto para qué para ayudar a un mecánico de taller a tratar de diagnosticar el error y de esta forma determinar si fue debido no sé a la velocidad del

vehículo a la temperatura exterior o interior de aceite lo que fuera el voltaje de la batería temas similares esto es muy interesante y es algo que también se utiliza en sistemas de captura de paquetes de red para temas de optimización de rendimiento por ejemplo pero también para análisis forense después de un ciberataque en este caso resultó que su vehículo había registrado muchos códigos de problemas en el momento del robo algo Que apuntaba obviamente algo sospechoso no y que se pudiera haber utilizado para alertar al dueño del vehículo con las apropiadas reglas de detección de problemas Martín y queridos oyentes con lo que he contado hasta ahora a ver si adivinas cuál fue uno de estos códigos de problemas que el investigador vio en la aplicación telemática mighty código de problema en plan un número no Bueno un poco ok No número sino código de problema relacionado a Qué componente del vehículo el campus vale Sí pero de qué parte del vehículo sin darte pista Supongo el eco no el fv Este vale vamos bien pero un poco más abstracto no sé no sé estoy un poco pillado a ver ok Te doy te doy una pistas te dan unas opciones no pistas estos códigos están relacionados con las ventanas están relacionados Espera espera Espera Ya sé por dónde vas vale los códigos del protocolo digamos y tal No sé Claro si lo pregunto es así seguro que va a ser gracioso con no sé con el acelerar por ejemplo con lo que controla las agujas de revoluciones acelerar digamos el dashboard este cerca porque está cerca de esa zona pero no era esta o sea cerca Físicamente pero no cerca de que tenga sentido los códigos estaban relacionados con el ordenador de abordo está Easy you como has dicho tú la ecu que controla la iluminación exterior del automóvil porque específicamente los ladrones arrancaron el parachoques y desconectaron los cables de los faros de los focos de las luces para alcanzar los cables conectados como muy bien has dicho a la unidad de control electrónico o Easy you o ecu responsable de la llave inteligente del vehículo claro este es el típico fallo de diseño que cosas esto es como tener una caja fuerte no pero que por detrás está hecha de plástico o algo así o digamos que la cerradura Mejor dicho mejor dicho porque esto es sobre todo un caso real típico tú te vas a la caja fuerte de los típicos hoteles y es toda de hierro ahí muy duro pero donde tú pones el pin esos plástico barato y ahí ese plástico barato es lo que guarda la plaquita electrónica que es lo que activa y Desactiva la cerradura por tanto no están protegiendo una parte vital de todo el sistema de las cajas fuertes y esto pasa mucho también en los cajeros automáticos que normalmente protegen Dónde se guarda el dinero pero no protegen el ordenador que controla viajero automático que de esto yo creo que en algún episodio hemos hablado sí sí hemos hablado de cajeros automáticos largo y tendido Pues el tema de la Easy u Esta es que la mayoría de los vehículos modernos tienen múltiples y siyus que son dispositivos electrónicos que se encargan de distintas funciones del vehículo como el motor desbloqueo encendido la transmisión los faros el control del clima la telemática como la presión de los neumáticos el nivel de aceite y gasolina las cámaras la llave inteligente el control remoto las ventanas los asientos los sistemas de seguridad vamos hoy en día nuestros vehículos son como naves espaciales tienen un montón de electrónica un montón de componentes que controlan motores y sensores y bueno eso añade complejidad y incrementa la superficie de ataque las distintas Easy you Se podrían ver como neuronas distribuidas en el vehículo que reciben información de varios sensores para coordinarse tomar decisiones y ajustar el rendimiento en tiempo real como lo haría el cerebro de un ser vivo en pocas palabras la Easy you las Easy use en este caso porque hay varias como digo Son dispositivos importantes que ayudan a controlar el funcionamiento del automóvil luego como he dicho hay varias Easy Us en cada vehículo y cómo se comunican Pues igual que las neuronas de un cerebro utilizan una red de sinapsis las Easy use están conectadas entre sí a través de buses de red de área de controlador o controller Network o can que es como me voy a referir a ella de ahora en adelante el hecho de que sea un bus de comunicaciones significa que es una línea de comunicación en la que todos los dispositivos para hablar entre ellos se

conectan a este bus y a través de este bus de comunicaciones pueden hablar entre todos ellos os lo podéis imaginar como un cable de cobre típico de teléfono en el que vas y pinchas tu teléfono como lo haría la Cia por ejemplo o no como lo harías para comunicarte con una persona de forma normal y puedes hablar con los que estén pinchados en el cable la alternativa a este diseño de comunicación de Canvas que es digamos un cable único un sistema de mensajería de comunicación único sería la comunicación en Estrella en la que cada dispositivo tiene un cable conectado desde el propio dispositivo un nodo central podríamos decir el cerebro Pero esto implica mucho más cableado y un punto único de fallo que sería el cerebro el nodo central y es una desventaja este diseño de Canvas es similar al de un Hub para aquellos que saben algo de redes saben que el utilizar un Hub conlleva bastantes riesgos el primero es que cualquiera puede pincharse al cable o conectarse al Hub o al Canvas en este caso y escuchar lo que otros usuarios dicen porque los mensajes se envían en el bus y es un medio físico en el que todos pueden escuchar y recibir dicho mensaje el segundo riesgo es que cualquiera puede intera o inyectar mensajes e impresionar a otros usuarios del cable en el caso de la analogía del teléfono o dispositivos en el Canvas las Easy use ya que los mensajes enviados en el cam bass no están protegidos no están cifrados no están autenticados no están ni digitados nif firmados digitalmente y se Confía en todos los dispositivos conectados actualmente casi todos los vehículos fabricados a partir del año 2000 utilizan el sistema Canvas en mayor o menor medida el atacante no necesita conectarse directamente a la ecu de la llave inteligente en lugar de esto puede llegar a comunicarse con la Easy u de la llave inteligente desde cables que estén conectados a otros dispositivos pero en el mismo Canvas Como he mencionado anteriormente por qué todos los dispositivos que estén conectados a ese bus a ese bus de comunicaciones pues pueden hablar entre todos ellos en este caso en el mismo bus en el que está conectado el laicidio de la llave inteligente también está conectado conectada a la Easy you de los faros y por eso es el dispositivo en el que se han centrado para abusar este ataque Y no es que sea un ataque sencillo Porque hay que desmontar y sacar los faros para llegar hasta los cables que a veces requiere como digo descuadrar el parachoques pero es un esfuerzo bien recompensado el robo del coche y posible posteriormente o reventa Esta es la forma más fácil Porque además de los faros se podría Acceder al Canvas haciendo un agujero en un panel por donde pasa el cable es que es un par trenzado de cobre de cables de este canvas cortando los dos cables y empalmando este dispositivo el inyector de mensajes can Pero esto haría que el valor de reventa del vehículo robado disminuyera porque tiene un agujero ahora el vehículo que tienes que arreglar antes de poderlo vender o si no tienes que descontarle el precio del arreglo al que a tu comprador no Y esto es algo que los ladrones van a tender a evitar si pueden evitar destrozar el coche que quieren vender pues mejor que mejor Los investigadores descubrieron además que la mayoría de estos autos que se están robando se están destinados a exportarlos enviados en contenedores marítimos a ciudades en África os preguntaréis Cómo es que yo pensaba que las luces de un vehículo son bastante sencillas porque se necesita una Easy you que es como un algo inteligente no pues como digo en nuestros vehículos son bastante inteligentes modernos casi como naves espaciales y hoy en día no sé si os habéis fijado pero aparte de lo típico que realizaban hasta digamos antes del 2000 que era encender Apagar las luces y parpadeo de los intermitentes ahora las luces realizan mucha más muchas más funciones como por ejemplo incluyen motores y estos tienen que ser controlados para nivelar los faros de forma que cuando el automóvil esté cargado con equipaje pesado o incluso pasa de algún tamaño las luces se giren se ajusten para compensar el desnivel luego también hay que dirigir los motores de los faros para iluminar las esquinas cuando se va girando también hay que controlar los sensores que pueden detectar automáticamente si las luces han fallado y te lo comunican O también para encender las bombas el de agua para que

se limpien también los focos no algunos incluso También tienen un mini parabrisas Así que esto también tiene que ser controlado de alguna forma y también incluso temas de lógica porque en el Toyota Rav4 también se permite elegir qué leds se van a encender en una cuadrícula específica para no deslumbrar a otros conductores que se aproximan pero aún así iluminar el resto del camino así que vemos que los faros hoy en día son bastante avanzados bastante y por eso necesitan estar conectados a una Easy you que es un mini ordenador digamos así podría verse como una mini raspberry pay que controla todo esto no motores sensores incluso la lógica de cómo se tienen que comportar los mensajes de diagnóstico que los investigadores identificaron en la aplicación myt en relacionados con los fallos los problemas de las luces los llevaron a sospechar que los ladrones probablemente conectaron un dispositivo especial que les permitió desbloquear el vehículo y enfocaron su investigación principalmente en el vector de ataque que incluye la inyección de comandos en el Canvas Los investigadores descubrieron que este tipo de dispositivos se pueden comprar en sitios de la web oscura o Dark web por hasta 5.000 euros o unos 5.500 dólares y a menudo se anuncian como dispositivos de arranque de emergencia que pueden ser usados por los propietarios de vehículos que han perdido sus llaves y se ofrecen para automóviles de muchas marcas como BMW Cadillac Chrysler Fiat for General Motors Honda Jeep jaure Lexus maserati Nissan Toyota Volkswagen Bueno hay muchos esto esto hay que pensar Porque si el mismo dispositivo se puede utilizar en muchos vehículos es que el problema es de diseño en los vehículos en la electrónica interna de los vehículos Los investigadores decidieron comprar uno de estos dispositivos para desmontarlo hacer la ingeniería inversa y entender realmente cómo funciona y qué vulnerabilidad estaban abusando los criminales que estaban robando los vehículos el dispositivo que recibieron después de comprarlo online dicen y de hecho hay fotos que voy a incluir un enlace al análisis de estos investigadores y en ese análisis hay varias fotos de este dispositivo se ve como un altavoz portátil normal de hecho el dispositivo en sí es igual es idéntico la carcasa es la de un altavoz Bluetooth de la marca jbl que se ha modificado y Dentro de este altavoz se tiene todo el Hardware necesario para llevar a cabo el ataque de inyección de mensajes can resulta que este dispositivo que venden por tanto dinero por unos 5000 euros Está compuesto por solo 10 dólares en componentes Hardware tiene un chip que contiene Hardware para hablar el protocolo Canvas obviamente software pre programado en el chip para hacer esta tarea Luego tiene un transceptor que es bueno un dispositivo que envía a ajusta el tema digital a señales analógicas en los voltajes necesarios para comunicarse con el Canvas Y luego tiene otro circuito adicional que es un poco para saltarse la mínima seguridad que tiene el Canvas el dispositivo se alimenta de la batería del altavoz y se conecta como digo al Canvas que es una conexión mediante un par de cables trenzados de cobre la verdadera magia del dispositivo está en la programación Porque estos estos componentes por 10 dólares lo podría comprar cualquiera pero claro si no se conoce Cómo funciona un Canvas aunque tengas estos componentes Hardware por 10 dólares pues no vas a conseguir inyectar los mensajes que han falsos en la red cambus del automóvil y robar el vehículo que es ahí donde entiendo que el criminal que vende estos dispositivos pues está ofreciendo su valor añadido no digámoslo de alguna forma básicamente los mensajes inyectados en el Canvas engañaron al automóvil para que pensara que se estaba utilizando una llave confiable lo que convenció al sistema interno del Canvas que hay un componente que se llama Gateway que se puede pensar como un componente que filtra mensajes can en varias redes Kan De hecho se puede ver como un enrutador que todos conocemos en redes tcp o incluso como un cortafuegos o firewall no en plan dejo pasar esto o no en función De dónde viene a dónde va del de la información que contiene el mensaje can y de esta forma lo que hicieron es como digo convencer a este dispositivo can Gateway para que transmita mensajes que instruyen al automóvil a Desactivar su inmovilizador para que

desbloquee las puertas y esencialmente que encienda el motor y que les permita a los ladrones conducir el vehículo fuera de ahí llevárselo a donde quieran el tema de que parezca un altavoz está muy bien pensado si os lo paráis a reflexionar por un momento porque si eres un ladrón y estás ahí en la calle intentando robar un vehículo y bueno Obviamente si todavía no has desencajado el foco no y te para la policía y te ve con un altavoz jbl no va a sospechar o decir este Bueno le gusta la música está un poco Ahí se va a poner a escuchar algo de música en cambio Si te ve con un dispositivo que se podía pensar tipo raspberry Pay o similar con electrónica y cables expuestos Pues eso huele un poco no Y ya puedes tener una buena justificación para lo que estás haciendo o vete llamando a tu abogado y bueno en este caso para acabar con cómo funciona este dispositivo es que cuando una vez lo tienes conectado que es la parte más difícil a los cables del Canvas cuando he sacado el foco del vehículo luego lo único que tienes que es de hecho lo han preparado de tal forma que solo Tienes que apretar los botones del altavoz el Play alguno de estos botones y listo en unos segundos el vehículo se enciende ves cómo se enciende las luces las puertas se abren y el motor se enciende y Listo ya te lo puedes llevar quiero comentar que hacer hincapié en que este es un problema que afecta a muchas marcas de automóviles Aunque en este caso el robo se centra en un Toyota Rav4 como he dicho el dispositivo que venden en la Dark web Se ofrece para muchas marcas Así que no es algo aislado solo a dispositivos Toyota ni a Rav4 afecta a más modelos de Toyota y más vehículos de otras marcas dato interesante es que pude encontrar un vídeo de un robo real de un Toyota Rav4 de 2021 y de hecho esto fue captado por cámaras de circuito cerrado de televisión de alguna casa en Londres y os voy a poner el link en las notas del episodio para que lo veáis en el vídeo se ve bueno una calle de Londres así bastante oscura pero se puede ver que hay coches aparcados y está enfocado en un coche y se ve como a mitad del vídeo llegan dos personas vestidas así con ropa oscura y bueno se ve ahí como se agachan y se ponen a un poco a manipular la luz el foco delantero de la parte del piloto del conductor y en menos de dos minutos lo de se ve como los desmontan se ve se ve bastante mal no pero se ve que algo hacen conectan algo que su dispositivo se ve como las luces de freno de atrás del vehículo se encienden y luego vuelven a poner la luz encajada en su lugar se cada uno se va a la puerta de piloto conductor y copiloto se monta en el coche y se lo llevan es escalofriante ver que en menos de dos minutos tu coche Bye bye Los investigadores informaron de sus resultados a Toyota pero sin mucho éxito Ya que to no ha contestado De todas formas me parece interesante que a esta vulnerabilidad contra el Toyota Rav4 se le ha asignado un cve que bueno son los se utilizan para eso para identificar y registrar en vulnerabilidades en componentes software pero también temas de Hardware el informe de la investigación contiene algunas recomendaciones enfocadas en los fabricantes de vehículos sobre todo para prevenir este tipo de ataques pero también nos vamos a dar alguna opción para vosotros queridos oyentes porque me parece interesante que nosotros los que no tenemos Tanto poder como para modificar la electrónica y las redes internas de los vehículos podamos hacer algo al respecto medidas proactivas para fabricantes Los investigadores mencionan que se podría Modificar el firmware del Canvas Gateway ese componente que he dicho que se comporta como un router para que envíe los mensajes solo si no ha habido errores recientes no he mencionado porque no he querido entrar en detalles técnicos de cómo funciona realmente el ataque pero lo que hacen es como una especie de denegación de servicio envían un montón de mensajes que cuando se envía muchos mensajes en un en un Canvas esto se ve como un error un fallo Entonces digamos que se resetea un poquito toda la comunicación Pero esto esto en este caso no importa mucho y finalmente el Canvas Gateway lo que hace es reenviar de forma exitosa el mensaje de desbloquea el vehículo enciende el motor a donde tiene que ir y entonces Bueno lo que dicen los investigadores Oye añádele funciones al firmware del Canvas Gateway para

que sólo permita reenviar mensajes Si no ha habido regiones errores recientes Ok Esta es una la otra es la de Añadir cifrado en los mensajes del Canvas o incluso firma digital o autenticación y ha dicho antes que el Canvas es una red de comunicación interna de los dispositivos las Easy Us estas de vehículos modernos que realmente no tiene temas de protección de este tipo de cifrado ni firma digital ni autenticación la forma más segura de implementar esto es a través de componentes de Hardware criptográfico lo que requeriría modificar los vehículos actuales y incrementaría su coste algo que no pasaría en vehículos y ya en el mercado porque requeriría vamos a destriparlos y volverlos a montar con los hardwares requeridos para esto pero igual en nuevos sí que se podría implementar pero como digo esto encarecería el tema de comprar el vehículo e incluso Bueno un poco la complejidad de cómo arreglarlos mantenerlos cambiarle las piezas y todo esto hay una alternativa que de hecho uno de los investigadores es muy es un dato muy interesante dice que él estuvo involucrado en el diseño del Canvas de los vehículos de Volvo Así que tiene bastante experiencia en este campo y la alternativa que Comenta es emular criptografía en lugar de Hardware en software lo que solo requeriría Modificar el firmware Aunque en cualquier caso a todo esto tenemos el problema de la gestión de claves criptográficas que aquellos que nos sigan y que estén involucrados en este tema deben de saber que es un mundo bastante complejo otro dato interesante es que esta persona este investigador que Comenta esta alternativa de hacer la criptografía en software en lugar de Hardware dice que este mismo sistema está en proceso está ayudando al gobierno de Estados Unidos a mejorar sus vehículos militares para incluir este tipo de protección emulando criptografía en software así que es algo que está sugiriendo que no es algo teórico académico sino que es algo que el gobierno de Estados Unidos está implementando o está queriendo implementar en sus vehículos militares y ahora medidas proactivas para usuarios se me ocurre el tema del bloqueo del volante con uno de esos candados metálicos realmente no sé cómo se llama Pero bueno Supongo que entendéis la descripción no sé Martín si tú sabes cómo se llama exactamente esto pero sabes eso que es como un candado metálico que conectas al volante para que no se pueda no se pueda girar para derecha o izquierda Entonces si aunque te roban y te encienda el motor pues no van a poder girarlo y ahí se queda Entonces esta sería una medida proactiva que que antes se utilizaba bastante pero hoy en día Supongo que la gente confía mucho en el tema de seguridad interna del vehículo no me lo van a robar no va a poner encender porque necesitan mi llave y todo es muy electrónico y tal Y solo hackers así muy avanzados van a poder hacerlo pero pone esto que funcionaba antes y sigue funcionando Ahora no Y chavales en tiktok con cables cargadores o sea justo Sí sí tú te refieres un poco es el equivalente de las motos de cuando no te permite girar el manillar pero solo que tú lo pones como candado Esa sí sí y luego tenemos algunas a mí se me han ocurrido también medidas reactivas Ok vale No es no sería lo ideal porque reactivo significa que es después de que repartir ahí a todo lo que se Menea si no pero se me ocurre temas como utilizar aplicaciones de telemetría es decir estas aplicaciones que ha mencionado el investigador mighty de Toyota tesla tiene una Porque todo lo que la electrónica de tesla pasa por sus servidores Sí o sí Bueno y otros vehículos modernos tienen también pues el tema de es configurar estas aplicaciones de telemetría para que te avise si tu vehículo se ha si el motor se ha encendido cuando tú estás en casa Y dices pero si yo estoy en casa y mi llave está conmigo de alguna forma No sé si la llave algunas tienen algo de bluetooth y se puede comunicar con tu con tu teléfono pero bueno en cualquier caso que sea que te notifique cuando se arranque no pasa nada si estás tú conduciendo que arrancas tú pues Ok si soy yo no hace falta ni que conteste al menos que te notifique o es incluso sale de una zona geográfica determinada sería una buena forma para saber Oye algo está pasando el vehículo vamos a investigar no he jugado con estas aplicaciones pero se me ocurre que también si permiten la configuración de alertas en base a lo que

mencionaba códigos de diagnóstico de problemas Se podrían configurar alertas para que te avisen si se identifican fallos en el Canvas de control al que están conectadas las luces porque este es el vector de ataque utilizado en estos robos y los códigos que el investigador pudo identificar en la aplicación de telemetría My tee de su Toyota Rav4 esto es como gente que trabaja en los shocks operation Center que recibe muchos logs de red de en points de Windows macos s Linux y pues en función de no sé si muchos logins fallidos en un tiempo de un minuto más de 100 pues Oye alértame pues sería algo similar no que que tuviera esta funcionalidad de que te alertaras Y hay muchos errores códigos de problemas de este tipo relacionados con las luces en concreto luego también se me ocurre esos dispositivos obd2 que como digo en un episodio anterior comentamos que tenían vulnerabilidades a nivel radio y se podían abusar para para bueno para robar el vehículo también bueno los habría que Investigar cuáles son seguros Pero uno de estos que fuera seguro y estuviera conectado al vehículo con conexión a internet pues configurarlo para que te avise de si tu vehículo se arranca o si sale de geográfica determinada Esto lo digo porque no todos los vehículos disponen de esta telemetría en bebida en el vehículo no lo ofrecen de serie e incluso algunos te cobran más por hacer esto y Oye un dispositivo obd2 de estos conectada a internet el dispositivo no vale mucho la conexión a internet igual te sale a pocos no sé 10 dólares al mes y podría ser otra alternativa y el último truco que bastante barato y simple de implementar es por ejemplo el simple erttack ponerle si tu dispositivo no tiene aplicación de telemetría y no te quiere gastar dinero en ponerle como digo ni añadirle el pack de telemetría ni comprarte el dispositivo obd2 que lo tienes que conectar incluso cogerte comprarte la conexión mensual a internet pues puedes utilizar un dispositivo de este tipo de rastreo como alertack que te puede alertar de cuando sale de una zona geográfica específica yo creo que en otro episodio lo hemos mencionado pero si no lo menciono a mí me ha pasado esto alguna vez que mi vehículo en algún momento no estaba donde tenía que estar y esto era porque estaban rodando una serie y no no la habían comunicado bien de que esto iba a pasar entonces está bastante preocupado y llamé a la policía y todo me dijeron repórtalo como robado y yo pero como os he robado si si faltan aquí 10 coches seguidos Cómo se van a llevar llevado 10 coches tiene que pasar algo no sabía la policía que había pasado no sabía dónde estaba y luego me enteré de que era esto estaban grabando una serie entonces lo que hice fue comprarme un airtag lo puse en el vehículo Así que ahora sé en todo momento donde está y si se va de cerca de donde lo tengo digamos donde debería estar pues me alerta Total que cerrando la noticia ya quiero hacer un par de comentarios que el crimen organizado tiene suficiente dinero tiempo oportunidades e incentivos para comprar automóviles porque a todo esto los ladrones en sí de los vehículos probablemente no pero la persona esta que ha creado este dispositivo que vale 5 que lo vende por 5000 euros en la Dark web ha tenido que o entiende trabaja para una empresa de automóviles o ha comprado algún automóvil lo desmantelado se ha conectado al Canvas ha hecho ingeniería inversa y bueno ha encontrado estas vulnerabilidades algo que me sorprende también de esta noticia Es que esto sucede en ciudades con tanta policía y tanta vigilancia como Londres donde hay medio millón la última vez que lo miré hace años ahora deben haber no sé millones y millones de cámaras en todos sitios y que esto no se no se notifica un poquito más rápido se hace algo al respecto y lo último es que tanto si tenéis un Toyota Rav4 como si tenéis otro vehículo cualquiera que sea fabricado después del año 2000 tener cuidado vigilarlo a través de la cámara o sistemas de telemetría como digo y ponerle este bloqueo de volante que esto os va os va a ahorrar algún susto que otro las noticias de coches de robo de coches como es algo muy peliculero siempre siempre está muy Guay yo creo que que hemos cubierto probablemente casi todas las técnicas que salían a la famosa peli esta de 60 Segundos de cómo se llamaba Nicolas Cage en Nicolás Cage Nicolas Cage Angelina Sí ya Bueno de hecho hemos

cubierto más porque como es una peli ya un poco antigua no hay no hay tanta cosa telemática Villa más aquello del clonado de llaves que nos llamen para la segunda parte no Claro es verdad 120 segundos que le van cambiando así el nombre en esta serie en esta sería robado en 30 segundos no vamos a mejorarla menos Sí claro es verdad lo que pasa que si vas a menos estás limitado si vas a más pues estar haciendo pelis hasta que quieras justo bueno queridos oyentes Muchas gracias como siempre por estar ahí hasta el final no nos liamos mucho más así que seguir compartiendo el podcast que seguimos creciendo todos los días y eso nos ayuda un montón atrae más sponsors podemos dedicarle más horas hacemos más contenido de calidad y sobre todo hacemos cosas nuevas que Alexis y yo andamos muy ocupados y por eso esta semana empezamos Así un poco tal y vamos a toda leche porque la verdad es que los que yo los Pillo a los dos en todo pero aquí estamos eh aquí estamos como siempre Todas las semanas ponen dos al día sí ya que hemos acabado ya podemos respirar tomarnos lo que queda de fin de semana y nada nos escuchamos en el siguiente episodio eso mismo Adiós adiós Muchas gracias 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