los coches son los peores productos que existen en cuanto a lo que se refiere a nuestra privacidad según un reciente estudio de la fundación mozilla Microsoft concluye que la clave criptográfica utilizada por el grupo chino storm0558 quedó expuesta en un volcado de memoria en un entorno de depuración al que los cibercriminales pudieron Acceder al comprometer la cuenta de uno de sus ingenieros nueva ocasión para seguir aprendiendo e informándose sobre temas de ciberseguridad en esta nueva entrega de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 21 de septiembre de 2023 episodio número 106 yo soy Martin vigo no está conmigo Alexis porros que bueno sigue de viaje pero aún así ha buscado el hueco para grabar y seguir adelante de manera conjunta con nuestra misión Pues de manteneros informados Así que no estamos grabando a la vez pero él aún así preparó su noticia Hola Alexis qué tal Muy buenas Martín pues aquí estamos de nuevo de vuelta con muchas ganas aunque estamos un poquito aquí entre el one off de vacaciones extendidas estoy así que con el horario de aquí para allá que voy que vengo Pues nada no nos fue posible conectar en directo esta semana pero Igualmente no os preocupéis queridos oyentes tenemos un episodio de lo más calentito Vais a ver así que quedaos hasta el final para escucharlo Y para no enrollarme mucho como siempre al principio comentaros que nos podéis seguir en todas las redes sociales más populares donde nos podéis encontrar como tierra de hackers o @tierra de hackers os invitamos a suscribiros a tierra de hackers en cualquiera que sea vuestra plataforma de podcast favorita Ahí estamos y también sois más que Bienvenidos a nuestro canal de discord al que podéis acceder vía tierra de hackers.com barra discord Muy bien pues yo de Novedades contaros algo que tenía muchas ganas de contaros Y es que voy a he preparado un curso de ciberseguridad para desarrolladores web está centrado sobre todo para gente que todavía no tiene conocimientos profundos sobre ciberseguridad especialmente en el ambiente web Así que si eres un desarrollador Y estás interesado voy a estar dando un curso presencial en Barcelona Eso sí en inglés para que también gente internacional pueda asistir el 7 y el 8 de noviembre de 5 de la tarde a 9 de la noche por trabajas que así también sea compatible insisto curso de ciberseguridad para desarrolladores web he hecho un partners con Barcelona code School y itrane sec Y la verdad tengo mucha mucha ilusión de empezar a dar este curso que le estoy metiendo muchas horas y además ya os digo que es un curso presencial que es como realmente a mí me gusta hacer estas cosas Si queréis más información podéis ir a tierra de hackers.com barra web Security en inglés tierra hackers.com barra web Security y ya nos vamos a dar las gracias como siempre a nuestros mecenas de patreon Por cierto antes de nada os dejo también el enlace en las notas del episodio que sé que así es mucho más cómodo gracias jsbp que se ha unido a nuestra familia de patreon te lo agradecemos un montón y a nuestro sponsor monatura empresa que comparte los mismos valores que tierra de hackers hacer la seguridad Max accesible y transparente nosotros a través de un podcast inmórate con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y que está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web monat.com y mandarles vuestro currículum a tierra de hackers @monat.com vamos ya para adelante con la noticia hablemos de coches hablemos de privacidad probablemente no vaya a ser una sorpresa para nadie esta noticia pero a la vez conviene que profundicemos en el tema para ser conscientes de Hasta qué punto llega esto un reciente más artículos estudio de mochila la fundación detrás de proyectos como el navegador firefox lleva como título lo siguiente es oficial los coches son la peor categoría de producto que hemos revisado en cuanto a privacidad dicho de otra manera en el mundo de los smartthings que vivimos los coches es lo que más invade nuestra privacidad cuando me topé con este

artículo sabía que os lo quería traer porque es uno de esos temas que llevan rondándome la cabeza hace un par de años ya yo nunca he tenido un coche en propiedad la verdad siempre he usado el de los demás pero en algún momento sé que me tocará comprarme uno por un lado ya digamos tengo El dilema de si ir a por uno un coche puramente eléctrico o si todavía es pronto para ello sobre todo hablando que ahora vivo en España y que la infraestructura de cargadores y todo esto pues no está tan desarrollada Como por ejemplo en San Francisco donde vivía antes pero sin duda lo que más me preocupa con diferencia es mi privacidad quiero decir pensemos en un coche eléctrico en el coche eléctrico por excelencia el tesla no cámaras por todos lados coordenadas GPS que no solo te indican a dónde ir sino que se suben a la nube información sobre cómo cuándo y dónde conduces para entrenar y mejorar sus algoritmos necesitas una cuenta online con todos tus datos personales se conecta tu móvil y bueno un largo etcétera de Preocupaciones en torno a la privacidad hemos pasado de coches tontos o a demasiado listos En mi opinión y ojo entiendo que en parte esto es necesario para tener los coches avanzados que tenemos hoy en día es inevitable no para obtener coches autónomos que se graben miles y miles de horas conduciendo necesitamos métricas de Cuantos más conductores mejor para hacer nuestros mapas mejores Queremos saber dónde hay tráfico y cuánto tardo en llegar a un destino y eso requiere saber cuántos automóviles están parados en cierto punto es decir los móviles una vez más No sé quiero decir que yo quiero esos avances pero no quiero ser parte de los datos agregados no quiero que pase lo que ha pasado con las televisiones por ejemplo producto en el que ya es prácticamente imposible encontrar un televisor que no sea inteligente y esté conectado a internet no quiero eso Quiero un televisor con 4k sin tener que tener una cuenta de Samsung vale en Netflix Pero bueno que sea opción mía si quiero Netflix o no pero es que ahora una tele de estas de 4k inteligentes ya requiere que tenga cuentas tienes que estar aceptando las cookies todo el rato en la televisión o sea Quiero poder ver series sin que tenga que estar conectado a internet Me gustaría que la televisión por cable no fuese la única opción sino que analógicamente todavía por antenas hubiese emisoras suficientes para poder ver la tele si no quieres conectarlo a internet quiero básicamente que siga viendo alternativas para los que no queremos renunciar a nuestra privacidad para usar objetos indispensables en el día a día Pero bueno volvamos al artículo de mochila o como decía más bien su investigación y veamos que nos cuentan han revisado 25 marcas de coches o fabricantes que no es poco y han hecho una tabla con varios red Flags o cosas que causan preocupación y han categorizado de esta manera a todos los fabricantes de coches son estas Cómo se utilizan los datos personales que están recolectando por ejemplo si recolectan más de lo estrictamente necesario si venden esos datos a terceros etcétera ya me entendéis luego qué capacidad tienen los usuarios como me refiero a clientes evidentemente para controlar esos datos es decir tienen la posibilidad los clientes de pedir que no se recolecten la posibilidad de la posibilidad de que se borren Por ejemplo si se han recolectado yo que sé pues vendes el coche ya a otra persona Pues deberías poder pedir la fabricante Oye todos mis datos que habéis recolectado elimina los también si la política dice que se almacenan demasiado tiempo o más del necesario que a veces Pues la política de privacidad te pone que se va a almacenar de manera infinita no pero sabes no hay en plan dos tres años y luego lo borramos luego también evalúan la marca por reputación y aquí se evalúa Cuál es el historial de ese fabricante en cuanto a incidentes de seguridad y protección de datos por ejemplo pues si ese fabricante ha sufrido alguna brecha de seguridad o fuga de datos un cuarto punto en el que evalúan es la seguridad aquí mochila desarrolló una lista de requerimientos mínimos de seguridad que todo fabricante debería cumplir y ojo eh requerimientos mínimos hablamos de lo basiquísimo para poder tomarse la empresa en serio Por así decirlo si El fabricante ni cumple con los mínimos estipulados entonces recibe este red flag y luego por

último Inteligencia artificial el uso de esta tecnología pero digamos de tecnologías cuestionables si bien mochila no usa este esto para digamos poner el a la mala reputación este factor no no entra para puntuar digamos negativamente pero si lo ponen porque es aún así una preocupación sobre todo insisto cuando se trata de el uso de algoritmos de Inteligencia artificial cuestionables ok pues ya tenemos Nuestro objetivo evaluar fabricantes de coches entornos a la protección de la privacidad de sus clientes tenemos un muestreo 25 marcas de coches Y tenemos el baremo con el que vamos a medirlos uso de nuestros datos control sobre nuestros datos reputación seguridad e Inteligencia artificial prácticamente todos los fabricantes puntuaron entre mal y muy mal siendo tesla el peor conme temía hay que aquí incidir o para ser justos que tesla es el peor si tenemos en cuenta el factor de la Inteligencia artificial que en realidad no puntúa para Nuestro objetivo si no tuviéramos en cuenta Eso tesla está entre los peores fabricantes pero junto con a Hyundai Kia Honda Mercedes Ford Volkswagen Toyota y muchos otros pero más que quedarnos en la lista profundicemos un poco en los hallazgos de mochila por ejemplo tesla ha puntuado muy mal como decía dado que el uso de su Inteligencia artificial para conducción Autónoma es usado por muchos conductores ya y su uso está relacionado con 17 muertes y 736 accidentes por tanto mochila lo evalúa como una Inteligencia artificial poco fiable y peligrosa luego ningún fabricante cumple con las expectativas mínimas insisto del lenguaje legal que mochila espera ver en los términos del servicio pero comenta que Hyundai se lleva la palma ya que su política de privacidad dice no solo que cumplirán con cualquier requisito legal por parte de un juez que pida por ejemplo que se le entreguen los se le entreguen los datos de un cliente sino que añaden que también cumplirán con las peticiones informales por parte de fuerzas y cuerpos de seguridad del estado Qué quiere decir esto que básicamente evidentemente en un estado de derecho como puede ser por ejemplo España o cualquier país en el que vivas querido oyente porque entiendo que no tenemos oyentes en Corea del Norte si un juez exige Pues yo que sé en una investigación me pongo lo más duro Pues sospecha de terrorismo las fuerzas y cuerpos de seguridad pues van a un juez a pedir una una orden judicial que les permita obtener datos de esa persona y entonces pueden ir al fabricante porque saben que tiene ese coche y pedirle toda su información pues por donde se mueve a qué horas Pues todos los datos que se recolecten no pero con una orden judicial pues Hyundai dice que también lo va a entregar sin orden judicial es decir no quiero decir que voy yo y pido tus datos y me lo den pero no hace falta una orden judicial con que un cuerpo policial le diga Oye pásame información de de Manolo va y se lo manda sin más pero claro esto es un problema porque no hay ni que justificarlo otro punto a tener en cuenta que o conclusión a la que llegó mochila es que todos los fabricantes a excepción de tesla Renault y dacia han firmado el documento lista de principios para la protección de los consumidores que fue creado por el Grupo Industrial automovilístico americano Alliance Ford automotive innovation bueno Esto es básicamente una lista de principios que incluye de hecho muy buenos requisitos en torno a la privacidad pero que según mochila y a pesar de que lo firmaron todos los cumplen exactamente 0 fabricantes 0 de los que lo han firmado O sea yo flipo ya no es que abusen de la privacidad de sus clientes sino que aún por encima les engañan directamente con marketing fraudulento O sea no Nosotros hemos firmado Esto bueno otra cosa le he dado aquí un golpe al micrófono otra cosa es que es que lo cumplamos sabes pero firmar lo hemos firmado Y si creéis que esto que os estoy contando no es para tanto dejadme dejadme que os lea lo que recolecta un fabricante como Nissan por ejemplo según su política de privacidad que os dejo las notas del episodio para que lo podáis ver con vuestros propios ojos a ver si soy capaz de decirlo de una sola vez cojo aire nombre dirección de correo electrónico números de teléfono dirección postal geolocalización código postal edad fecha de nacimiento número de carnet de conducir número de identificación

nacional estado de ciudadanía en el país estado migratorio raza país de nacimiento creencias religiosas o filosóficas orientación sexual actividad sexual geolocalización precisa datos de diagnóstico de salud e información genética número de seguridad social como empleado información de servicio o garantía de vehículos empleo de información relacionada como el número de identificación del empleado números de identificación nacional o Estatal e información de dependientes por la administración de ciertos beneficios o programas de empleados inferencias derivadas de cualquier dato personal recopilado para crear un perfil sobre el consumidor que refleje las preferencias características tendencias psicológicas predisposición predisposiciones comportamientos actitudes inteligencia habilidades y actitudes del consumidor número de identificación del vehículo información de geolocalización y navegación información de velocidad y distancia hábitos y estilo de conducción información de gestión de uso de la batería historial de carga de la batería información del deterioro de la batería funciones del sistema eléctrico códigos de problema de diagnóstico condiciones de mantenimiento información de versión del Software uso del vehículo y cualquier servicio correspondiente sitios web aplicaciones móviles inteligentes información del Estado del vehículo información sobre cerraduras de puertas puertas abiertas estado del motor datos sobre accidentes que involucran el vehículo de la dirección desde la cual fue impactado el vehículo y cuál es airbag se desplegaron orientación sexual actividad sexual e información genética de todo esto que os he contado insisto os dejo las notas del episodio el enlace a la política de privacidad de Nissan orientación sexual actividad sexual e información genética Pero esto quiero esto Qué es o sea cómo que están recolectando eso por Cómo que por lo menos se dan el derecho No la libertad te invitan a que aceptes eso cuando compras un coche de ellos a ver todos Cuando éramos jóvenes y no teníamos para pagar un alquiler de un piso y vivíamos con nuestros padres pues a veces utilizábamos los coches para para esto no pero es que no sé yo flipo la verdad pero dijimos que habría que habría tres de los 25 fabricantes de coches que ni siquiera firmaron esto tesla Renault y dacia aquí sucede algo muy interesante bueno que no lo haya firmado tesla no me sorprende porque evidentemente es el que más recolecta de todo en cierto modo no quiero ser un tesla hater o ir a lo fácil Pues si están intentando hacer un algoritmo para que el coche se conduzca solo yo entiendo que haya que recolectar información por eso digo que en parte no me sorprende que no hayan formado Pero qué pasa con Renault y dacia Y esto es muy muy interesante dacia realmente es parte de Renault probablemente mucho sobre todo oyentes en Latinoamérica por no conocían la marca dacia pero Renault Sí y Renault es un fabricante de coches que solo venden Europa por tanto no solo no ha firmado este acuerdo porque evidentemente es un acuerdo de Estados Unidos pero lo destaco porque Renault y dacia según mochila son los no digo los mejores sino los menos malos en cuanto a invasión de privacidad Y sabéis por qué queridos oyentes por el gdpr y yo llego aquí me siento orgulloso de Europa no quiero decir que un Renault y un dacia no recolecta información pero tenemos la Clara prueba aquí de que la legislación en temas de protección de datos funciona de que en Europa somos los que leyes más robustas y severas tenemos a nivel mundial y es precisamente por eso que Renault y dacia son los fabricantes que mejor puntuaron entre los 25 que analizó mochila porque no venden fuera de Europa y por tanto tienen que estar a Merced de la legislación europea en términos de privacidad o la Europa si bien las consecuencias no de estos abusos de a nuestra privacidad porque recolectan información como se Comenta hoy Nissan pueden ser obvios me ha gustado otro post que me encontré de mochila indagando un poquito más que se centraba Precisamente en esto no en vale sabemos que se recolecta de todo pero Qué puede pasar Pues mira un número de cosas según ellos una es que se recolecta demasiado una cosa es recolectar demasiado información otra peor es información que no necesitas para nada como la el material genético o actividad sexual pero

otra ya es llegar a nivel creepy no como la que la que os estaba diciendo ahora y que sepáis que lo de información genética y material genético que son ambos no porque materiales ir a coger muestras pero información Pues si tú mandas a yo que sé tú en mí tu información genética pues ellos se la pueden comprar si es que se vendiese que bueno eso es tema médico y dental pero es lo que digo no solo Nissan General Motors Chevrolet Kia también son fabricantes que en su política de privacidad tienen esto Además yo me pregunto porque una cosa es el porqué recolectan esto pero sería interesante también saber el Cómo no como decía bueno otro punto al que llega mochila es que abrimos una nueva era de cibercrimen tenemos que fabricantes de coches recolectan información a nivel de llevarse las manos a la cabeza Pero por otro lado tenemos que ninguno cumple con las mínimas expectativas de seguridad Entonces todos los conductores corremos peligros de que toda esa información caiga en manos de ciberdelincuentes y Se use para fraude y extorsión es que es un cóctel explosivo por un lado recolectas absolutamente de todo y por otro no me lo proteges ya no hablamos de que El fabricante vaya a usarlo venderlo sino que si no tiene una mínima seguridad entonces cualquier otro puede venir a robárselo por otro lado también el problema del espionaje masivo no solo el coche al igual que un móvil no geolocaliza en todo momento donde estamos yendo y a dónde vamos sino que también hemos visto que varios fabricantes están dispuestos a ceder esa información a fuerzas y cuerpos de seguridad del estado sin orden judicial O al menos un motivo justificado con que lo pida a alguien que lo puede pedir ya les vale Y ese es el baremo que hay por parte de varios fabricantes para entregar nuestra información lo cual pues abre las puertas a espionaje masivo luego También tenemos el problema de los hackeos como dice la famosa ley del Gran mico gipponen y es el título de su libro si es inteligente es vulnerable me encanta no podría estar más de acuerdo y es lo que sucede con el automóvil hoy en día estos coches los controlas desde una aplicación móvil abrir las puertas encenderlo poner el aire acondicionado subir el volumen de la radio luego Tenemos también cosas como las llaves digitales digitales de BMW que puedes pues por ejemplo compartir con gente para que por ejemplo un amigo tuyo que quiere usar tu coche no le tengas que ir a entregar las llaves físicamente sino que con que se instale la app tú le das acceso y ya puede usar tu coche luego funcionalidades como g-ofends que alertan pues cuando el coche sale de una zona específica y bueno teóricamente sirven para digamos controlar Pues que hacen tus hijos con tu coche no pero que puede ser usado también por personas celosas para tener controladas a sus parejas o peor aún personas con órdenes de alejamiento que quieren estar vigilando y monitorizando a sus parejas Tenemos también el control de los fabricantes sobre tus pertenencias porque hace unos meses Ford mandó una patente para ser aprobada en la que podrían bloquear tu coche remotamente si no pagas a tiempo un coche que hayas comprado a plazos podrían directamente dejarte sin coche a su gusto y preferencia con que por ejemplo te retrases un solo día en el pago pum coche bloqueado a distancia Pero esto va más allá la patente habla de que el coche podría no solo bloquearse sino flipa en colores conducirse automáticamente y de manera Autónoma a un almacén de Ford o si no tiene suficiente valor de Mercado el coche ya directamente a un desguace Pero qué me estás contando O sea me retraso un día en el pago del coche y el coche se me pira el desguace a suicidarse me quedo loco esto en la patente de Ford pero es que no no para aquí esto señores que la patente dice también que podrá grabarte continuamente mientras conduces para detectar y cito textualmente comportamientos inadecuados que el propietario del vehículo puede hacer contra del vehículo si se retrasen los pagos o sea ya en el momento que te retrases empiezo a grabarte en todo momento en tu coche pero la patente también habla de lo que yo denominaría directamente extorsión como controlar el sistema de audio para emitir una grabación constante recordándote que pagues en plan vas escuchando música y cada dos por tres paga paga cabrón es que es el cobrador del

frac llega tu vehículo a través de la radio chavales esto ya es que es increíble yo de verdad que os doy las gracias por ser oyentes de este podcast y que tenga sentido dedicarle tantas horas que le dedicamos a Alexis y yo porque es por momentos como estos que vale la pena todo la de cosas que he llegado a ver preparando semana a semana al episodio es que es increíble de verdad que no somos conscientes al mundo que nos dirigimos en fin Como puse Hace unos días en redes sociales esta semana Pues fui invitado por parte de europol y de fuerzas y cuerpos de seguridad del Estado españolas a una mesa redonda para debatir sobre la Inteligencia artificial y Cómo afecta a nuestros datos Y eso a nuestros datos personales y a nuestra privacidad tuve la ocasión de preguntarle al Gran micona en que estaba allí de hecho me firmó me firmó un libro y de hecho me llegó a prometer que para el año cuando hagamos visa Barcelona vendría como King of speaker lo digo aquí y me lo firmó que aparte puse una fotito por ahí Yo le hice una pregunta y le pregunté específicamente porque había preparado esta noticia porque él hablaba de bueno los peligros de los dispositivos inteligentes no como decía antes por su famosa ley de si es inteligente es vulnerable y yo me centré un poco más en la privacidad ya que la conferencia iba de eso y le preguntaba que qué cómo podíamos hacer porque el problema que yo tengo es yo soy una persona que valora muchísimo mi privacidad y hago muchísimas cosas como ya os he contado muchas veces para preservar mi privacidad pues utilizo datos falsos emails únicos tengo diferentes números de teléfono hago muchas cosas más que no no quiero ni comentar aquí pero claro yo por otro lado yo quiero tener un coche que sea capaz de conducirse solo yo quiero poder ver Netflix entonces hay me encuentro en que hay tecnologías que quiero pero que es inevitable que para que funcionen o para que se desarrollen incluso tengamos que previamente ceder nuestra privacidad para que llegue a eso Por ejemplo el claro ejemplo los coches autónomos es que tenemos que cederles la información de cuando conducimos la visión de las cámaras para mejorar los mapas y que los coches puedan realmente algún día llegar a ser autónomos entonces Cómo podemos hacer eso Cómo podemos estar en un mundo donde la tecnología avanza pero no a coste de nuestra privacidad no como moneda de pago nuestros datos personales y Su respuesta fue bastante desoladora tampoco me lo esperaba diferente Pero me dijo pues no tengo una buena respuesta para ti me dijo una frase que me gustó mucho que dijo nuestra generación pasará la historia como los primeros en los que renegamos de nuestra privacidad para avanzar tecnológicamente y con esto con esa reflexión doy paso a mi querida Alexis Alexis adelante me has dejado los pelos de punta Martín Así que los coches modernos son los que peor tratan nuestra privacidad como consumidores quién lo hubiera dicho uno pudiera haber pensado que bueno los teléfonos móviles son los peores en este aspecto básicamente Porque casi cada persona en el planeta Tiene un teléfono móvil y es un gran abanico de usuarios que es muy jugoso para las empresas de telefonía móvil y ya hemos visto más de una noticia como desarrolladores de aplicaciones móviles como sobre todo las aplicaciones del tiempo y similares y de algunos juegos en concreto recopilar información de usuarios móviles y bueno venden toda esta información a otras empresas por mucho dinero y a nosotros y nada no nos dan nada ni un rábano inicialmente conformidades mencionando la noticia tenía en mente que no solo tenemos a los fabricantes de vehículos que pueden recopilar esta información cuyo caso más obvio como del tesla pero también hay aplicaciones de terceros como todo el tema de entretenimiento y aplicaciones instaladas en los vehículos no que no necesariamente tiene que ser tesla muchos otros vehículos permiten instalar aplicaciones de terceros entretenimiento y similares pero en otros casos un poco menos directos que se me está ocurriendo el tema está en las empresas de alquiler como zipcar o similares que incluyen un dispositivo para controlar el coche de forma remota es decir abrir y cerrar puertas Apagar y encender el motor detalles de diagnóstico ubicación del vehículo y que pueden recopilar

información del usuario no también y por comentar otro caso que me parece también muy interesante y que también puede pasar un poquito desapercibido y que hemos comentado en algún otro episodio pero ya llevamos tantos que ya no me acuerdo pero bueno el tema era de las empresas de seguros de coches que comentamos que te dan un descuento si instalas uno de sus dispositivos en tu coche estos dispositivos normalmente van conectados al puerto vd2 que es de diagnóstico del vehículo y también incorporan una conexión a internet para enviar los datos recopilados de la conducción y Bueno de nuevo abuso a nuestra privacidad como usuarios de vehículos en este caso como usuarios o clientes de este seguro de automóvil pero después de saber todos los detalles sobre los datos que los automóviles recopilan Me he quedado sin palabras como digo es increíble no sabía que los fabricantes de coches recopilarán tantos datos distintos de cada usuario Incluso el ADN Pero para qué necesitan eso a ver en el futuro igual se me ocurre un escenario tipo guerra en el que los soldados van conectados a vehículos como en la película Matrix no ahí por por detrás por el cogote y igual ahí tendría algo sentido no que El fabricante supiera el grupo sanguíneo por si necesita proporcionar sangre perdida al soldado por el tema de estar conectado de forma No sé metálica pero en conexión con tu cuerpo con tu interior Con tu sangre y tal Y bueno Y si se pierde sangre el soldado Pues que te proporcionen la que sea correcta en función de tu tipo de sangre y esto es una idea un poco estratosférica podríamos decirlo pero de ahí a los a nosotros a los usuarios civiles que necesiten saber nuestro ADN la verdad es que nos lo expliquen No pues nada en cualquier caso lo que sí que necesitamos es que más organizaciones indaguen en estos aspectos porque como consumidores nosotros yo creo que todos damos por sentado muchos temas de privacidad y confiamos demasiado en la buena fe de las empresas y hemos visto más de una vez que las empresas no siempre buscan hacer lo mejor para nosotros para los usuarios sino normalmente lo que beneficie más a su negocio Incluso si eso requiere sacrificar la privacidad de sus usuarios no estoy diciendo que todas las empresas sean malas con Malas intenciones pero sí que miran por sus intereses y no por interés de un bienestar común digamos no por el bienestar de sus clientes que es lo que debería hacer si quieren seguir teniendo esa reincidencia de un cliente contento y satisfecho Pero bueno aquí no hablamos de negocios hablamos de ciberseguridad y Nada igual un poquito relacionado con eso sería también igual que hubieran más leyes pero bueno a mí hecha la ley hecha la trampa no y gente curiosa como digo como los de la fundación mozilla esta organización que acaba de hacer este análisis de privacidad de los datos que recopilan los vehículos un aplauso a ellos por hacer este estudio la verdad muchas gracias mozilla y nada ya sin más seguimos pasamos a la siguiente noticia que es un follow up o una continuación de una noticia que no sé si os acordáis pero en el episodio 103 cubrimos el incidente de seguridad en el que Microsoft publicó el 11 de Julio que el grupo apt chino storm0558 había robado una clave criptográfica de firmado digital de tokens de autenticación de usuario consumidor una clave llamada MS aquí del inglés Microsoft account key y que la habían utilizado para forjar tokens de autenticación contra usuarios empresariales en Outlook web Access y outlook.com y así poder acceder a los correos electrónicos de 25 organizaciones incluidas múltiples agencias gubernamentales de Estados Unidos cuando la noticia se hizo pública Microsoft todavía no sabía cómo los cibercriminales comprometieron dicha clave criptográfica la clave msa ni cómo pudieron utilizar esta clave de usuario consumidor para acceder a sistemas de usuarios empresariales Pues el miércoles de la semana pasada Microsoft publicó los detalles del Análisis forense que han llevado a cabo y es lo que os voy a comentar en este episodio como seguimiento follow up de la noticia que cubrimos en el 103 voy a comentar un poquito el tema de las claves criptográficas que Microsoft ha dado algunos detalles que me parecen interesantes mencionarlos para que tengamos un poco de contexto sobre lo que son ya comenté cuando surgieron los detalles iniciales de la noticia que el grupo

de cibercriminales comprometió una clave criptográfica de firmado digital de tokens y autenticación conocida como MS aquí no pues bien son muy importantes y se mantienen en un entorno de producción seguro y aislado del resto de la red corporativa de Microsoft aislado con esto me refiero Air Gap no como se le conoce en temas de redes networking y ciberseguridad no el acceso a este entorno y Por ende a estas claves criptográficas solo se proporciona a empleados que han superado un análisis exhaustivo de su pasado lo que en inglés se llama un background check en el que investigan el historial criminal hacen un perfil psicológico investigan relaciones con vecinos familiares y amigos entre otros temas vamos que te intentan averiguar si vas a ser una buena persona trabajando para ellos o no O sea eso es lo primero que se necesita pasar este análisis exhaustivo no sólo esto sino que solo se puede acceder a través de cuentas dedicadas con eso Microsoft se refiere a cuentas diferentes a las de su entorno corporativo y solo se puede acceder a este entorno de ese sistemas dedicados protegidos Y utilizando tokens Hardware para autenticación de doble factor vamos con estos cuatro requisitos la seguridad parece bastante elevada para acceder a este entorno de producción donde se mantienen esas claves criptográficas incluso para securizar más este entorno sistemas de correo electrónico videoconferencia acceso a web y otras herramientas colaborativas no están disponibles están baneadas para de esta forma evitar vectores de ataque típicos no como vemos siempre en casi todas las noticias que cubrimos como malware de Drive by Download o ataques de phishing y no esto sino que también limitan el acceso a sistemas y datos en base a políticas que ellos denominan que se conoce comúnmente como Justin Time y jazz Enough Access básicamente esto significa dar acceso solo de forma temporal cuando se necesite y solo A quién lo necesite además según Microsoft este entorno está segmentado el del resto de su red empresarial donde sus trabajadores tienen acceso a email y otras herramientas corporativas como digo en resumen este entorno de producción que tienen las claves criptográficas está muy aislado no tiene herramientas que no sean necesarias y luego Microsoft tiene su entorno corporativo como todas las empresas en el que bueno se puede utilizar de todo no Microsoft considera la red corporativa como una red de mayor riesgo que la de producción obviamente no porque ahí sus empleados pueden utilizar herramientas empresariales como en el videoconferencia web y aplicaciones de colaboración y por tanto tienen una política en la que definen que las claves criptográficas utilizadas en tokens de autenticación como las que el grupo cibercriminal chino comprometió recientemente no deberían salir del entorno aislado de producción Entonces nos viene la pregunta cómo es que la clave criptográfica pudo ser comprometida significa esto que los chinos se metieron hasta en la cocina y llegaron al entorno de producción donde están estas claves se va poniendo interesante el tema Pues según Microsoft en abril de 2021 un fallo en el sistema de firma digital de tokens de autenticación de usuario consumidor provocó un volcado de memoria automatizado lo que se conoce como un Crash damp Ok hasta aquí dices Bueno esto es normal los volcados de memoria los utilizan los administradores de sistemas desarrolladores de software y analistas de seguridad para determinar Cuál fue el fallo asociado con este Crash el fallo que creó este volcado de memoria y así poderlo arreglar y así es como lo hace normalmente Microsoft por eso necesita estos volcados de memoria para ver Oye qué ha pasado aquí Necesito un poco mirar las trazas el stack Trade sin debudar depurar y arreglar el fallo Aunque siendo una empresa tan grande Microsoft aplica medidas de seguridad adicional para limitar y proteger la información confidencial que los Crash damp contienen bueno Y esto cómo lo hace Microsoft Pues según ellos dicen que por una parte sus sistemas están diseñados de tal forma que cuando se produce un volcado de memoria debido a un fallo en el sistema estos no contienen claves criptográficas es decir al igual que tenemos rutinas de sanitización de datos de usuario de entrada y salida en aplicaciones web para evitar temas de inyección como

sql injection Crossing scripting y similares Microsoft implementa rutinas de sanitización de datos de entrada y salida creados por sistemas o programas no por usuarios como es en el caso de la web y del psicoanyección scripting Y en este caso estos datos de entrada y salida son los Crash damps volcados de memoria y también otros blogs de sistemas y aplicaciones según Comenta Microsoft la clave criptográfica se coló en el volcado de memoria debido a una condición de carrera o reis condition en inglés ya hemos comentado en otros episodios lo que esto significa pero para refrescar un poquito la memoria un ejemplo es el escenario en el que se asigna un valor a una variable que pudiera ser el volcado de memoria y también se comprueba su contenido que sería la búsqueda de datos como claves criptográficas Ok tenemos estas dos acciones asignación de datos a una variable y comprobación de los datos de esta variable pues qué es lo que pasa en una condición de carrera en este caso probablemente el caso concreto de Microsoft se hizo la comprobación antes de que el contenido de volcado de memoria se asignará a la variable que se analizaba en busca de información confidencial y por lo tanto obviamente la clave criptográfica no se encontró en el contenido de la variable cuando la rutina de sanitización analizó dicha variable y así Entonces es como se coló Ok Vale entonces me está diciendo Alexis que los chinos se colaron en ese entorno de producción y pudieron hacerse con este volcado de memoria que tenía la clave criptográfica pues por ahí va el tema pero os sigo explicando posteriormente y como suele hacer Microsoft en el análisis y resolución de problemas este damp se trasladó del entorno aislado de producción súper seguro nivel súper militar extremo a un entorno de depuración corporativo con conexión a internet Microsoft tiene otro sistema que escanea todos los volcados de memoria que se mueven a este entorno de depuración en busca de datos confidenciales como claves criptográficas entonces tienen una medida adicional de que Oye si se mueve algún tipo de dato como volcados de memoria o logs a este entorno de depuración que tiene menos seguridad que el entorno de producción y que además está conectado a internet Oye vamos a implementar algo una rutina de escaneo para para asegurarnos de que no están estos datos confidenciales aquí en este entorno un poco menos seguro que se puedan comprometer Pues en este caso tachán una vez más los sistemas de Microsoft fallaron en identificar esta clave criptográfica ok entonces me estás diciendo Alexis que no entraron hasta el entorno de producción que es mucho más difícil meterse por todos esos requisitos no que se necesitan y que se colaron en este entorno de depuración y consiguieron el volcado de memoria Sí señor algo así pero os voy a contar más porque como es que se colaron en ese entorno de depuración Pues según Microsoft estos cibercriminales comprometieron la cuenta de uno de sus ingenieros y esta cuenta atención que os imagináis se escucha redoble de tambores bingo esta cuenta tenía acceso al entorno de depuración donde se encontraba el volcado de memoria de abril de 2021 que contenía la clave de firmado o MS aquí de usuario consumidor que permitió a Storm 0558 forjar sus propios tokens de autenticación para acceder a sistemas de usuarios empresariales de sistemas de Microsoft en la nube así que ya tenemos resuelto aquí el misterio de cómo estos cibercriminales pudieron comprometer esta clave criptográfica lo curioso es que Microsoft No indica Cómo estos cibercriminales comprometieron la cuenta de este ingeniero de Microsoft y por qué bueno pues porque realmente no lo saben debido a políticas de retención de logs Microsoft dice que no sabe a ciencia cierta si este fue realmente el caso de como Storm 0558 ex filtró la clave criptográfica o si lo hizo de otra forma pero comentan que este es el caso más probable bueno bueno aquí como dice el dicho en casa del herrero cuchara de palo Microsoft no tiene los blogs sobre el compromiso de ingeniero que irónico y esto de los blogs está en línea con el problema que identificaron muchos usuarios de sistemas en la nube de Microsoft a raíz de este incidente cuando se dieron cuenta de que si no pagaban extra para el nivel Premium no tenía acceso a logs cruciales para determinar si se les

ha comprometido según leían la noticia y un poco intentaba atar Cabos me surgió una contradicción en la política de retención del oxx que Comenta Microsoft Por una parte tenemos que Microsoft dice que no tienen lo suficientes para determinar a cómo fue exactamente la forma en la que Storm 0558 comprometió la cuenta de uno de sus ingenieros ni ve cómo pudieron infiltrar la clave criptográfica si la primera actividad de compromiso Data del 15 de mayo de este año y la fecha de publicación del incidente de seguridad es del 11 de Julio podemos deducir que micro no guarda logs relacionados con su entorno de depuración por más de dos meses y por otra parte tenemos que el volcado de memoria que se creó en abril de 2021 ha estado en el entorno de depuración por más de dos años Así que estoy un poco confuso en qué quedamos Microsoft tienes logs o no los tienes o quieres hacerte el loco y escurrirte de publicar Cómo fue realmente el compromiso entiendo que igual se tienen políticas diferentes en función del tipo de información que se registra que se guarda de esta forma se pueden tener que datos de logs de acceso y otro tipo de actividad de usuario se pueden retener por ejemplo por dos meses como en este caso que más o menos se puede deducir y temas como volcado de memoria por más tiempo en este caso por incluso más de dos años algo que es casi decir como de manera indefinida una No muy buena práctica Por cierto uno esperaría que después de la investigación e identificación de la causa raíz del problema el damp se eliminará pero aún estaba ahí más de dos años más tarde podríamos pensar que aún no habían resuelto el problema y por eso estaba todavía el damp en el sistema en el entorno de depuración pero no creo que una empresa de tal calibre como Microsoft tardé más de dos años en determinar la causa de ese problema asociado con ese Crash damp en concreto Así que esto es algo que Microsoft se tendría que replantear bueno pues esta es una pieza del puzzle que ya tenemos resuelta el Cómo han podido comprometer la clave criptográfica pero el otro misterio por aclarar un poco más es por qué exactamente Es que pudieron acceder a sistemas empresariales con un token de autenticación de usuario consumidor Como ya comenté en el episodio 103 los cibercriminales pudieron utilizar una clave de firmado de usuario consumidor para forjar tokens de acceso a entornos tutoriales de audio web Access y outlook.com como los de agencias gubernamentales de Estados Unidos el suceso fue que para poder seguir ofreciendo servicios a escala Microsoft decidió lanzar un servicio de metadatos de claves criptográficas a finales de 2018 además de ofrecer acceso a esta nueva funcionalidad también actualizó la documentación asociada clarificando los requisitos para la validación de las firmas digitales es decir qué se necesita para validar una firma de usuario consumidor y también que se necesita para hacer lo mismo con una clave de usuario empresarial esto significa que la documentación incluía la sintaxis de la función específica como llamarla que variables o qué contenido de datos se le tenía que pasar para poder validar esta firma sin embargo por otro descuido Microsoft no implementó de forma correcta unas librerías preexistentes antes de publicar este servicio y utilizó como parte del mismo por lo tanto las firmas de claves de usuarios consumidores podían resultar en una validación correcta y ofrecer acceso a sistemas de usuarios empresariales y viceversa pues es debido a este fallo en la Api llamada get Access que los cibercriminales pudieron acceder a entornos empresariales con tokens de autenticación de entorno consumidor lo curioso es que Microsoft dice que sus ingenieros actualizaron sus sistemas de correo electrónico esto me refiero a Outlook web Access outlook.com y exchange online en 2022 para que utilizaran este nuevo servicio publicado en 2018 quienes asumieron que las librerías utilizadas por la Api realizaban de forma apropiada la validación de firmas y no aplicaron ninguna modificación por lo tanto los sistemas de email de Microsoft permitían el acceso a sistemas de correo empresarial un tokens de seguridad firmados con claves de usuario consumidor ya incluso desde 2022 a modo de Marco Temporal y de fanfat de tema interesante comentar que la clave

de firmado había caducado el 4 de abril de 2021 muy cerca de la época en la que se creó el volcado de memoria por lo que otro fallo es que sus sistemas no deberían haber aceptado un token de autenticación firmado con una clave criptográfica caducada ahí quedan identificados todos los fallos de Microsoft Pero bueno al menos han venido con todo este análisis de cara al público y también han mencionado en su comunicado reciente que han arreglado todos los fallos descubiertos en primer lugar mencionan que han identificado y resuelto la condición de carrera que permitía que la clave de firmado estuviera en volcados de memoria en segundo lugar comentan que han mejorado la prevención detección y respuesta a la inclusión de material criptográfico en volcados de memoria también comentan que han mejorado los escaneos de credenciales para una identificación más eficiente de material criptográfico en entornos de depuración y finalmente han publicado actualizaciones a librerías de autenticación utilizadas en la validación de claves criptográficas y la documentación asociada además de todo esto Microsoft ha revocado la clave de firmado msa comprometida para evitar que se puedan forjar otros tokens y autenticación y comprometer otras cuentas y mencionan que han investigado y no han encontrado evidencia adicional que indique acceso no autorizado a otras cuentas de usuario utilizando la misma técnica de forjado de tokens de autenticación de entornos cruzados Es decir de entorno consumidor a entorno empresarial Cuál es el impacto de todo esto además de poder acceder a correos electrónicos de 25 organizaciones relacionadas con el gobierno de Estados Unidos que es por sí bastante grave pues e investigadores de wish una empresa creada por exempleados de Microsoft y una de las más famosillas en el mundillo de ciberseguridad en la nube hoy en día y que utiliza Inteligencia artificial Según dicen ellos para identificar incidentes de seguridad en la nube con más eficiencia previsión y más rapidez pues comentan que la clave de firmado msa comprometida podría haber permitido a los atacantes forjar tokens de autenticación e impersonal a cualquier cuenta de aplicaciones de la nube de Microsoft o en los entornos de las empresas afectadas incluidas cuentas privilegiadas como administradores de plataformas en la nube estilo Outlook sharepoint One drive y teams así como aplicaciones basadas en autenticación con asher active directury lo que incluye la funcionalidad de hacer login Con Microsoft o login with Microsoft que seguro que lo habéis visto esta funcionalidad que se muestra se puede utilizar en muchas páginas web para hacer login con otros proveedores de identificación y autenticación como Microsoft Google y similares En definitiva Storm 0558 podría haber utilizado la clave de firmado que comprometieron para obtener acceso a cualquier aplicación como cualquier usuario con el mayor nivel de privilegios en base a todo esto tenemos que tomar tiempo para reflexionar y aprender de este incidente y hacernos preguntas autocríticas como mi sistema se exponen material criptográfico o tokens de autenticación en volcados de memoria cuando se produce un fallo guarda los volcados de memoria en segmentos de red expuestos a internet o a zonas no seguras como de empresas de terceros recopilo lo suficientes con información adecuada para determinar incidentes de seguridad protejo las claves criptográficas en un entorno aislado y solo las uso en sistemas online cuando las necesito Y de forma temporal mi compañía o negocio ha facilitado demasiado el acceso cruzado de entornos de distintos niveles como consumidores y empresas bueno estas son unas cuantas se me Podrían haber ocurrido más pero ahí tenéis un poquito la idea de este ejercicio que deberíais hacer y de aquí de este estudio de este análisis autocrítico podríamos definir mejores prácticas de seguridad Como por ejemplo la primera es los volcados de memoria no deberían contener datos como clave criptográficas y deberían utilizarse solo en sistemas de depuración y por un periodo limitado no dos años lease en segundo lugar podríamos decir que los blogs de actividad de usuario de entornos críticos como producción o depuración deberían contener información que permita la identificación de incidentes de seguridad en tercer lugar las claves criptográficas de firma no

deben estar accesibles online cuando no estén en uso es decir que deberían estar siempre en un sistema el Gap aislado seguro y cuando se tenga que utilizar moverlas de forma temporal al sistema online que lo necesite y en último lugar podríamos decir que la autenticación sólida es esencial para todos los usuarios y no debería tener fallos el tema de que se puedan utilizar tokens de autenticación para acceder a entornos cruzados es un riesgo de seguridad que se debería haber identificado con anterioridad quiero cerrar un poquito también con contexto político de este ataque según Microsoft el grupo de Ciber criminales al que nombró storm0558 tuvo acceso a los sistemas de correo electrónico de múltiples empresas desde el 15 de mayo de este año dos de los objetivos comprometidos fueron Gina raimondo que es la secretaria de comercio de Estados Unidos y también Nicolás bornes que es el embajador de Estados Unidos para relaciones con china Esto fue algo muy oportunista o digámoslo que coincidencia ya que ocurrió escasas semanas antes de que el secretario de estado Anthony blinken viajara a Pekín para conversar sobre restricciones de exportación de tecnología de Estados Unidos a China y una de las tácticas de negociación del gobierno chino es espiar a su oponente e intentar conocer sus intenciones en la negociación para ir un paso por delante y obviamente tener la ventaja en las negociaciones en este aspecto en relación a estas limitaciones de exportación de tecnología biden prohibió a nvidia que pueda vender sus gpus más potentes las a100 y H100 tanto en China como en Rusia para de esta forma poder entorpecer el desarrollo de Inteligencia artificial en ambos países Pues ahora a principios de este mes de septiembre el gobierno de biden ha vuelto a imponer otra restricción ha ido un paso más allá y no permite ahora en evidia vender tampoco estos modelos de gpu en Oriente medio Porque sabe que algunos de estos países los revenden a China y Rusia en su lugar ahora en evidia vende allí tanto en China Rusia como en Oriente medio unos modelos de gpu similares los a800 y H 800 pero con menos poder de computación esto es muy interesante porque normalmente lo que vemos en las noticias es que los chinos y enemigos de Estados Unidos normalmente espían a departamentos del gobierno y otras organizaciones relacionadas con armamento militar o agencias de seguridad sin embargo Ahora parece que el departamento de comercio es uno de sus objetivos predilectos y como digo todo esto viene motivado por el tema del entorpecimiento del desarrollo de la Inteligencia artificial en China lo que confirma que los chinos están muy metidos en la carrera de esta Inteligencia artificial algo destacar de este incidente es que los chinos no han ido directamente a comprometer de forma quirúrgica los sistemas de su objetivo como digo estas personas involucradas en las negociaciones de exportación tecnológica de Estados Unidos a China sino que en este caso fueron un paso más allá y a una escala mayor y se han centrado en atacar a uno de los entornos en la nube más grandes del mundo Microsoft asier y esta capacidad ofensiva junto con las fallas defensivas y de seguridad Microsoft un tanto obvias hay que decirlo dan escalofríos y con esto queridos oyentes llegamos a la pregunta del episodio que es la siguiente para aquellos que seáis clientes de servicios de Microsoft en la nube y para los que no seáis bueno os lo podéis imaginar podéis poneros en ese caso en base al reciente incidente de seguridad sobre el compromiso de la clave msa por parte de este grupo chino apt storm0558 os iríais de Microsoft a otros proveedores en la nube Y como siempre os damos cuatro respuestas la primera es no no merece el esfuerzo tengo descuento total estoy bien la segunda es no da igual esto le va a pasar a otros proveedores en la nube tarde o temprano la tercera es si lo estamos planificando y la última es Sí ya lo hice inmediatamente después de escuchar el episodio 10 3 así que ya sabéis lo de siempre en votad en Twitter y comentamos los resultados en el próximo episodio me gusta que tengamos estas noticias de follow up de seguimiento de noticias anteriores que siempre siempre es importante mantener el ojo porque ahí hay cosas que al final Al fin y al cabo cuando os las traemos Pues todavía como Queremos cubrir la actualidad Pues siempre

puede pasar que se desarrolla la noticia Así que muy bien traída está Alexis por mi parte ya como nos vamos a la hora dejaros aquí Muchas gracias como siempre no hay mucho más que decir acordados que si os interesa aprender sobre seguridad web tenéis el curso os dejo el enlace en las notas del episodio y espero que nos escuchéis para la próxima semana con nuevas noticias que os traeremos un gusto una alegría muy grande un placer que nos sigáis escuchando episodio 3 episodio queridos oyentes Y que nos apoyéis online en el ciberespacio en las redes sociales en las plataformas de podcast y en discord así que de nuevo toda vuestra colaboración es muy comida y seguir así Muchas gracias por vuestro apoyo Adiós adiós chao chao nos escuchamos 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