Avalanche es la nueva herramienta de espionaje que según su Creador está a medio camino entre palantir y Cambridge analítica hiddenc nadie se puede escapar investigadores alemanes compran dispositivos militares de captura biométrica en Ebay y exponen los datos personales no cifrados que estos contienen sobre ciudadanos de Afganistán y Oriente medio y también de soldados estadounidenses Ya llegó la primavera a tierra de hackers con un nuevo episodio disponible Comencemos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 28 de marzo de 2023 este es el episodio número 88 yo soy Martín vigo y está conmigo Alexis qué tal Pues aquí como dices con las bolas de 8 haciendo carambolas y nada aquí siguiendo para adelante para bingo Ah no que yo me estoy confundiendo ya deportes y jueguitos de mesa pero nada Pues aquí contigo otro episodio más así que para Dante mis valientes pero como siempre vamos a dar gracias a nuestros oyentes que es lo importante sobre todo en la intro Muchas gracias como siempre por apoyarnos online en redes sociales discord plataformas de podcast si no estáis suscritos en nuestra plataforma de podcast por favor ir ahora mismo a suscribiros y os invitamos a entrar en discord podéis entrar vía tierra de hackers.com/discore tenemos muchas conversaciones interesantes ahí y luego Bueno lo típico tierra de hackers en todas las redes sociales y en las que usen estilo handle pues es arroba tierra de hackers todo junto una palabra o tierra de hackers y bueno dicho esto voy a pasar a la pregunta a cubrir la pregunta del episodio que cada después de cada episodio publicamos en Twitter y que para el anterior fue la siguiente te preocupa que se puedan utilizar tus movimientos de cabeza y manos en dispositivos de realidad virtual como la Quest 2 para obtener tu huella digital y desanonizarte en el metaverso tenemos dos respuestas en esta ocasión la más votada fue un Sí con un 81% y seguida obviamente de un no con un 19% muy bien perfecto y yo pues darle las gracias a nuestros mecenas de patreon Gracias por siempre estar ahí y a nuestro primer sponsor que es A3 una empresa española de ciberseguridad con presencia en España México y Colombia que lleva más de 10 años en el sector foca dar respuestas a los tres Pilares principales prevención detección y respuesta cubren servicios ofensivos como red Team pen testing auditoría de código y mucho más también dando servicios gestionados de monitorización Avanzada respuesta incidentes con un enfoque diferenciador en el mercado siempre están buscando profesionales para incorporar a su equipo ofensivo y de seguridad y vigilancia digital para trabajar en un ambiente colaborativo y con enfoque muy técnico visita su web en a3sek.com y cuéntales que viniste nuestra parte también darle las gracias a brawler Pro por apoyarnos en el podcast Y ser uno de los 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 brawler 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 visión completa de tu 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 barra brawler proprowl e rpro muy bien y yo antes de dar paso a mi noticia comentar que tenemos un sorteo nuevo para una conferencia en Jaén la hack en Y tenemos dos entradas una la vamos a sortear entre todos nuestros oyentes favoritos que son bueno todos son nuestros favoritos Pero entre nuestros oyentes que nos apoyan en patreon una entrada en exclusiva solo para sortear entre ellos y luego una segunda entrada entre todos que lo vamos a anunciar en Twitter esta semana Así que estar pendientes ya se nos ocurrirá una pregunta para sortearlo y luego también recordaros que tierra de hacker se está apoyando visa Barcelona el Cold papers está abierto ya podéis comprar las entradas hay que ir ahora mismo a visates punto Barcelona bsi DS punto Barcelona y comprar vuestras entradas mandar

Core papers si sois un sponsor esponsorizar y también Estamos buscando voluntarios aquí con todo nos vamos a la primera noticia Cyber Grandpa es el sobrenombre de un influencer de hecho en YouTube que su pasado fue un agente del kgb la agencia de espionaje rusa la verdad no esperaba yo traeros en una noticia un abuelete youtuber que en el pasado era espía ruso pero aquí estamos Forbes le dedica una columna la semana pasada le dedicaba a este personaje que se ha hecho famosillo en parte por una herramienta que vende a través de sus múltiples empresas llamada avalanch o Avalanche pero empezamos primero por el personaje andrei massalovich akeyey abuelete como decía se dedica a crear contenido online donde habla de su vida pasada trabajando para el gobierno ruso O al menos es lo que dice porque hay mucha gente que le critica diciendo que las cosas que dice pues son exageradas desde donde dice que ha cooperado con el gobierno de Vietnam pasando por sus lazos con agencias de inteligencia hasta incluso las capacidades de su herramienta estrella Avalanche la verdad es que hay mucha gente que lo pone en duda Pero lo cierto Es que Estados Unidos acaba de incluirlo en su lista de enemigos y meta la empresa detrás de Facebook e Instagram ha declarado que sus empresas constantemente infringen las políticas de uso al hacer scrapping esto es interesante para recordaros para los oyentes que scraping es la técnica en la que uno recolecta de manera automatizada toda la información pública que existe en internet Bueno toda mucha por ejemplo pues todo lo que publicamos en este caso en Facebook y en instagram los post los comentarios todo eso se puede acceder de manera pública pues se escriben digamos programas lo que se conoce como screapers para recolectar toda esa información meterlas en bases de datos Y luego pues lo que tienes es muchísima información con la que puedes pues empezar a hacer cosas no el departamento del tesoro como decía hace apenas Pues unas semanas declaraba que incluía a andrey en su famosa lista of fax es DM que para los que no conocéis esta lista bueno el off son las siglas del office of Rain assets con troll que viene siendo la oficina de de la oficina del control de cosas extranjeras no O por así una entidad no me sale ahora la traducción de assets pero es una es una entidad estadounidense a cargo entre otras cosas de gestionar la lista sdn cuyas siglas vienen a ser special y designated nationals en block persons list nacional es especialmente designados y personas bloqueadas Qué es esta Lista pues viene siendo una lista que te declara como enemigo Oficialmente de los Estados Unidos O sea que no te interesa estar en esta lista yo creo Alexis tú en el pasado has hablado de lix en listas de estas no pero era más la notefly list correcto Sí sí correcto que era una sublista de la lista de del FBI de gente mala Claro porque tenemos los Moss Wanted no los más buscados que la míticalista del FBI la notefly list que es los que no pueden volar pues aquí os añadimos una nueva lista de United States of America en la que no quieres estar que es esta sdn no el special y designate National Pues bueno la razón que ha dado el departamento del tesoro que por cierto os dejo un link que las notas del episodio al anuncio oficial en la web pues la razón que ha dado para incluirlo en esta lista ha sido por atacar la democracia de los Estados Unidos Ucrania y otros países alrededor del mundo no solo eso me lo he leído y también comentan que es una manera de responder ante los que buscan exportar la marca de la autoritarismo del gobierno ruso Mostrar palabras palabras duras os dejo la web como decía por si queréis ver también a la web de los fac por si queréis ver a personas en vuestro propio país las que han sido declaradas enemigos de Estados Unidos que a lo mejor Oye tenéis un colega que es enemigo de Estados Unidos cuando lo habéis dicho Oye cuándo te vienes a burriman tío cuándo te vienes al coche le dice nada no me apetece tal vez tú vas a ver Claro porque eso es como la lista esa que decías de que no te dicen Si estás en la lista tú tienes que tener ahí un poco de scrapping no en este caso que es un poco sí sí yo tengo yo me puse una alerta en Google Para ver ahí si me añaden alguna vez no no No hombre no espero no estar ahí De hecho estoy grabando esto desde San Francisco ahora mismo o sea que que ya ves que te

han dejado no sé que de momento no estoy de momento no estoy bueno tiene 95.000 seguidores este tío en YouTube y teóricamente su canal cyberded pero no de Padre sino de YouTube ha eliminado este canal porque me puse a buscarlo y luego buscando información pues lo eliminó por la inclusión Hace unos días de andrei en la lista esta oficial de enemigos de Estados Unidos que por tanto como están esta lista es una persona sancionada como por ejemplo pues cuando se habla de que es más común de sancionar países no como Sudán Corea del Norte pues entonces YouTube siendo una empresa americana tiene que cumplir no con eso y por eso le han quitado el canal de YouTube La verdad es que hay frases suyas muy curiosas como lo que Contesta los que bueno no se creen mucho de lo que dice no como os mencionaba antes él dice para conquistar y capturar nuevos mercados en la era de la colonización digital uno tiene que ser un científico un investigador un aventurero e incluso un pirata pero uno no puede ser un estafador mucha gente esto no lo entiende y por eso hay tantos vende humos en la industria del big Data me pareció bastante curioso estas declaraciones y con esto En parte está contestando a críticas del famoso Bruce snyder un experto criptógrafo que decía que hay muchísimas empresas vendiendo la capacidad de influencia en base a datos recolectados con técnicas de scrating como os contaba antes que dice que en realidad es todo mentira esto esto la verdad me me resultó muy interesante Pero por qué pushback contra este hombre hablemos ahora de su empresa y su producto estrella Avalanche según él según andrei y cuando hace campañas de marketing de hecho su manera de venderlo es decir que Avalanche está a medio camino entre atención palantir y Cambridge analítica joder ahí es nada si recordamos tenemos un episodio específico hablando de palantir que es una empresa norteamericana que se dedica en parte a recolectar información de todo el mundo pero es una empresa que o sea seria y que se ha utilizado y está ha estado muchas polémicas yo os repito volver a escucharlo en ese episodio por temas de ciberespionaje en masa y a nivel global o sea os podéis imaginar el típico creo que eran magnolity report que estás ahí cogiendo información de aquí de allí sacas conclusiones pones una matrícula te puede decir en tiempo real donde está ese coche porque tiene acceso a las cámaras de policía cosas así pues ese rollo es palantero y luego Cambridge analítica pues os sonará por el escándalo de durante las elecciones de 2016 de la presidencia de las elecciones a presidente de Estados Unidos cuando hubo esa campaña famosa de Rusia de influencia para para inclinar la balanza hacia Donald Trump que acabó ganando y en parte pues había recolectado información de productos como Facebook a través de encuestas falsas para adivinar la personalidad de la gente y como influenciarles y detrás estaba esta empresa de Cambridge analítica Pues según este tío a balance está a medio camino entre palantir y Cambridge analítica Avalanche recolecta información pública de internet y utiliza granjas de Bots Para recolectar más información todavía lo que os decía del scrapping por ejemplo de grupos privados de aplicaciones de mensajería como Telegram redes sociales tiktok y foros online teóricamente con esta información Avalanche puede alertar a los clientes y detecta actividad de empleados filtrando información o vigilar a individuos a través de su actividad online no te lo vende así un poquito como del buen rollo no en plan no son empleados malos necesitas este servicio pero lo cierto Es que se puede utilizar para espionaje esto insisto es lo que públicamente se conoce que hace la herramienta pero Forbes tuvo acceso a una entrevistarse con gente que trabajaba en la empresa y que desarrollaba Avalanche y la empresa que desarrollaba esta que desarrolla de hecho esta herramienta se llama la vina pools y confirma esta gente que en realidad hay otra línea de negocio más secreta la utilización de una cantidad enorme de Bots para amplificar o disminuir contenido a través de redes sociales que viene a ser influenciar a la opinión de la gente de dos de los empleados que hablaron dijeron que los clientes eran secretos es decir no sabían Quiénes eran pero que estaban a cargo ellos de lanzar y gestionar servidores que

controlaban miles de Bots estos empleados creando los ellos mismos con miles de números de teléfono y emails falsos luego evidentemente programaban los Bots para atacar alguna comunidad en concreto Esto es lo que decían estos ex empleados y algunos de ellos hacían referencia a que a veces incluso podían intuir Quiénes eran los clientes secretos en base a lo que le pedían que se hiciera Y muchos de hecho dejaron la empresa por conflicto contra su propia ética y moral un par de clientes de andrey que sí se confirmaron son empresas petroleras que contrataron los servicios para luchar contra el mensaje de la gravedad del cambio climático esto la verdad es que es grave y demuestra la poca ética de esta empresa que está dispuesta a luchar contra los avisos de la comunidad científica sobre los efectos del cambio climático Y la verdad es que esto nos afecta a todo ya no es aquello de Bueno pues vas a espiar a este individuo y bueno yo que vivo en otro país pues bueno Está mal pero ni me va ni me viene o sea aquí estamos hablando de manipulación para que la evidencia científica y el consenso científico pues se vea disminuido no como como dicen ellos y así manipular a la gente de hecho en Rusia varios activistas y organizaciones sin ánimo de lucro centradas en el cambio climático precisamente han sido designados oficialmente como enemigas del Estado tócate los pies otro cliente que sabemos gracias a las sanciones interpuestas por Estados Unidos es el Gro en la famosa agencia de inteligencia rusa que ellos también usan Avalanche para sus misiones el propio andrei reconoce que Avalanche usó para disminuir el alcance de las protestas ucranianas en contra de la invasión rusa pues pues ahí ya tenéis un impacto que muy reciente y que está ahí con las claras consecuencias que todos podemos ver el tío la verdad que no se corta aunque claro es marketing también le da igual la imagen que proyecta porque está claro que bueno a diferencia de otras empresas que hacen algo parecido como os decíamos palantir o otras de las que os hemos hablado esta trabaja directamente solo con los clientes con objetivos muy cuestionables por no decir directamente que trabaja solo ya con los malos no es como su su Nicho son los países opresores los dictadores y básicamente quienes tienen Pues un objetivo bastante cuestionable no necesita hacer un esfuerzo por parecer una empresa bien no digamos entre comillas Es que le da igual si uno se va a la web propia de andrey la propia personal puede ver fotos en birmania país muy afectado por la brutalidad de sus fuerzas militares actuando contra disidentes y que se ha convertido en un Aliado de Rusia pues ese también es uno de sus clientes pero también tenemos clientes hispanohablantes señores según meta o sea la empresa Facebook Nicaragua ha contratado los servicios de andrei y su herramienta avalance Esto es algo que en la entrevista que le hizo Forbes andrey en esto en concreto no lo confirma pero tampoco lo niega así que bueno ahí queda con todo esto quiero destacar de nuevo la gente que le resta importancia de algún modo no como decía antes mencionaba las declaraciones de Bruce snyder pero por ejemplo las de un ex analista de la nsa y que de hecho estuvo involucrado directamente en la lucha contra las actividades de campañas de influencia durante las elecciones de Estados Unidos de 2016 que decía lo siguiente la gente se cree ese mito de que empresas como Cambridge analítica pueden escapear vamos a decirlo así suficientes puntos de información sobre una población en concreto y que con un algoritmo ya pueden moldear la información Global en masa esto es palabras textuales Y la verdad es que para terminar la noticia se me ocurre una pregunta muy buena no porque por un lado tenemos pues todas estas empresas que tanto os contamos y ahora tenemos también gente diciendo que bueno que eso está un poco exagerado entonces Os preguntamos queridos oyentes vamos a la voz de los sabios crees que la efectividad de empresas como Avalanche bueno de servicios como Avalanche o empresas como Cambridge analítica a la hora de manipular a la gente es exagerada y os damos directamente dos opciones sí es exagerada o no no lo es porque ahí están las pruebas no digamos así que ya sabéis como siempre Twitter arroba tierra de hackers Sí eso cuando decías lo de avalanch me bueno dos

temas venían a la mente uno es una forma un como decirlo un seudónimo de Attack surface management no era la parte bonita pero sí te voy a hacer un poco de monitor in the tu de tu external Food print tu tu huella digital externa pero es una tapadera para un servicio más oscuro Sí aparte si si lo piensas como que ya te da un poco de indicios no Ah No mira yo monitorizó esto monitorizó aquello pero solo tienes que darle un pequeño vuelta de tuerca y ya sabes que cosas una vez con esta infraestructura también podemos hacer otras cosas no es como si un carnicero que tiene ya las herramientas y la infraestructura en vez de cortar solo públicamente corta carne de animales para consumo y por otro lado pues contratar para acuchillar a gente Pues sería algo parecido y lo otro también sí creo que hemos mencionado otras empresas similares a estas como tú dices Cambridge analítica la cubrimos la otra más reciente es habíamos hablado de ella también Sí otra también hace poco en el 85 episodio hablamos de ese 2t que es otra empresa muy similar cierto cierto la de auror que era un poco más reconocimiento facial pero de Nueva Zelanda que hasta un oyente nos escribió y no es confirmaba que sí que él conocía de esa Así que las hay efectivamente la próxima noticia que deberíamos traer es cuando algunos de estos cibervillanos conecten su sus datos que han hecho scripping a gpt 4 o alguna Inteligencia artificial para mejorar su efectividad en los mensajes No si Dentro de poco o sin ti todo esto ya o sea yo le he puesto Quién es Martín vigo y joder de una descripción bastante guapa a ver nada que no puedas encontrar porque tengo públicos Twitter Y tal Pero oye esto es solo el comienzo dentro de poco ya puedes hacer o sin directamente preguntándole a Chad gpt yo que sé subes una foto Oye dónde se tomó esta foto o le preguntas Tengo este email quién está detrás Eso sí por ejemplo ostras pues no lo he probado Pero eso Si tira de Data Brokers y cosas así que a veces tiene información pública te puede decir cosillas tengo que poner mi email a ver si si sabe de quién es sí no solo el reconocimiento sino también está pensando en el impacto de escribir el texto más persuasivo en plan mi audiencia tiene de entre 18 y 35 años que son los que igual van a ir a votar tú dices para generar campañas para generar las campañas de influencia Sí sí tal cual tío De hecho yo estoy viendo ahora mucho muchos shorts y tiktoks y todo esto de Oye Cómo montar tu negocio pues chat gpt le puedes pedir que te escriba artículos sobre un tema con se optimizado para tal la web la creas aquí que tele con un clic ya tienes una tienda y esto aquí pim pamín con tres servicios que hay gastándote nada o prácticamente nada ya tienes ahí una web con contenido indexado pim Pam es la leche tío lo de chat ya tenemos miles de bolas de humo hay que es verdad no lo había pensado mira ahora obtén tu propia bola de humo en tres sencillos pasos y montas tú tu web que es súper súper tarde y ya cuando te vaya entrando dinero ya y un figuere out Ya verás muy silicon Valley empieza con chat gpt vamos a empezar por el fake ya luego el Maker ya vamos viendo si eso justo ahí Bueno vas creando nuevas bolas de humo y ya está listo de bola en bola y tiro porque hago carambola como a lo Ninja el 88 Pues nada pasamos a la siguiente noticia pero antes queremos hacer una breve parada para dar las gracias a 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.commod.com y mandarles vuestro currículum a tierra de hackers arroba-monat.com y nada habiendo dicho esto pasamos a la siguiente noticia que va de riesgos de privacidad relacionados con dispositivos desechados o reciclados y vendidos a través de tiendas online como eBay un investigador de seguridad de Hamburgo Alemania compró unos dispositivos de captura biométrica muy usados entre las fuerzas armadas de Estados Unidos desde 2010 en Afganistán principalmente Aunque en todo Oriente medio

también y pudo acceder a los datos que estos contenían lo que incluía información biométrica de personas contra las que se utilizaron los dispositivos para identificarlos para hacerle un screening un filtrado y bueno este estas personas no solo eran civiles sino que también eran soldados y ahora os explico el caso de uso de cada uno de ellos un poco de contexto para comentar Por qué se empezaron a utilizar estos dispositivos en Afganistán Pues en el momento en el que el dispositivo se usó por primera vez en Afganistán porque lo pudieron ver gracias a la información que contenía el investigador que compró este dispositivo en Ebay pues la actividad de guerra estadounidense allí en Afganistán estaba disminuyendo Osama Green Laden había sido asesinado en Pakistán un año antes y según los informes su identidad fue confirmada mediante tecnología de reconocimiento facial y entonces ahora es por qué se empezaron a utilizar estos dispositivos en Afganistán si parece que todo la actividad de guerra estaba disminuyendo pues una de las principales preocupaciones de los líderes militares en ese momento era una serie de tiroteos en los que los soldados y policías afganos apuntaron con sus armas a las tropas estadounidenses esperaban que el programa de registro biométrico biométrico pudiera ayudar a identificar a cualquier posible agente talibán dentro de sus propias bases de esta forma los datos biométricos de estos dispositivos se recopilaron en los centros de detención en las patrullas que iban haciendo las fuerzas estadounidenses durante Las evaluaciones de los empleados locales e incluso después de explosiones de bombas improvisadas ya desde 2016 hay informes de dispositivos biométricos de este tipo en manos de los talibanes luego haciendo Fast Forward yendo hacia el futuro llegamos a 2021 Pues en abril de 2021 biden anuncia su retiro de Afganistán en agosto de 2021 se completa el retiro de tropas pero Estados Unidos Deja atrás aproximadamente 7 mil millones en equipo militar que ahora está obviamente en tierra de talibanes que podríamos decirlo en tierra de hackers y es esta la principal motivación de esta investigación el hecho de que los talibanes ahora hipotéticamente que probablemente sea más realística la connotación que hipotética se pueden haber apoderado de estos dispositivos después de la evocación de Estados Unidos de Afganistán el grupo de investigadores quería saber si los talibanes podían identificar a las personas que han ayudado a Estados Unidos gracias a estos dispositivos y los datos biométricos que contienen obviamente esto es de Gran preocupación y podría poner en riesgo la vida de muchas personas y por eso pues se decidieron comprar estos dispositivos online y hacer un análisis de seguridad los dispositivos tienen nombres muy curiosos relacionados con el tema de la privacidad no sé Martín si te atreves a hacer alguna sugerencia sobre el nombre de los dispositivos que hay dos De hecho está está intentado acordarme de aquellos que te escaneaban el Iris Cómo se llamaban no sé tío Igual igual estos o sea como digo esto se empezó a usar en el 2011 pero igual lo hemos mencionado alguna otra noticia Aunque yo ahora mismo no me acuerdo pero uno se llama hide y el otro se llama sick sí hite creo que hyde sí fue fue si lo mencionamos pero ya hace tiempo el de hyde pero High en sí que es como el pilla pilla no el escondite no correcto lo dejáis en plan esconderte y sí que es lo de Buscar no Aunque Highland puesto una y adicional pero bueno sí significa decir en inglés y luego en español handel inter agency identity Direction equitment equipo de detección de identidad interinstitucional o inteligencia portátil y el sic se llama secure electronic en rolman kit kit de inscripción electrónica segura episodio 38 hablamos de height fíjate como como se va cerrando el círculo siempre en tierra de hacker solo que ahora has añadido el sic y ahí que te acuerdas cuál era la conclusión esa iba sobre Si recuerdo bien la noticia porque aparte la di yo esa lo que recuerdo fue cuando hablábamos de que cómo Ah vale Ya me acuerdo instrucciones que daban organizaciones sin ánimo de lucro porque usaban utilizando estos dispositivos para encontrar a gente y sospechosos pero en realidad lo utilizaban contra disidentes Y entonces te decían que movieses cuando te lo ponían en los ojos moviese las pupilas muy rápido luego para que no te

reconociese O sea que presionases como la cara contra el dispositivo luego había otras técnicas para evitar que te detectasen con cámaras como hinchar los mofletes para evitar el reconocimiento facial Si recuerdo sobre eso sobre eran pautas para evitar la vigilancia en países que pues que tenían un régimo un régimen opresor Ok Pues sí pues esa Mira pues ya tenemos un poco yo he venido un poco a comentar los peligros de privacidad y la que cubrirse tú Martín era un poco como escaparse de estar en riesgo que está está muy buena Por eso digo que es que es cojonudo O sea primero tenemos una noticia hace el 38 ya tiene que ser hace años de de ostras la gente está intentando evitar esto y ahora tú estás hablando de qué pasa cuando no lo pudiste evitar Esto es lo que pasa Sí la verdad que un poco preocúpate si no lo pudiste evitar pero bueno ahora te digo igual a ver cómo está el tema Pues el height este es como dice Martín captura el Iris también la huella dactilar y tu cara tiene también flas infrarrojos por si no hay mucha luz digamos tiene una pantalla táctil y registra una persona de forma completa en 15 minutos y almacena un máximo de 500.000 personas vigiladas porque luego a partir de eso una vez ha creado la huella digamos de la persona si la vuelve a ver pues Oye le dice Esta persona es tal persona le dice el nombre y todos los datos de personales de la persona en sí parece si lo veis vamos a poner un enlace en las notas del episodio a los documentos donde hay imágenes del dispositivo parece como el cuerpo de una cámara de fotos tipo Canon 6d de estas dslr pero sin el objetivo sin la lentes sin eso el precio en Ebay está por unos 400 dólares y luego tenemos el sic que este dispositivo parece más como un terminal de punto de venta de esos que se usan en los comercios para pagar con tarjeta del mismo tamaño también también captura el Iris la voy a activar y la cara y parece un poquito más completito porque tiene una pantalla LCD de estas pequeñas un teclado físico en miniatura que tienes que tener las uñas muy afiladas o los dedos muy finos porque si no aprietas dos o tres teclas a la vez y un touchpad o alfombrilla de estas de ratón diminuta la cámara es digamos estilo polaroide Esta es que se despliega un poquito se abre de un extremo del dispositivo para permitir el escaneo del Iris y además tomar fotos y este dispositivo la memoria un poquito más limitada tiene capacidades de 60.000 personas vigiladas a ambos tienen conexión celular y WiFi y el sí que además tiene posicionamiento GPS Este es en concreto el dispositivo el sic el que los investigadores analizaron inicialmente luego a partir de lo que los resultados que obtuvieron se decidieron a comprar el height también y los analizaron algo curioso del sic es que el investigador la usó en sí mismo la se hizo un poco un análisis de Iris voy a dactilar y cara para ver cómo funcionaba lo típico no cuando obtienes un cacharro lo que quieres hacer un poquito a ver cómo funciona a ver cómo lo puedo atacar No pues es lo que hizo un poquito vio algo interesante en el mensaje que le salía en la pantallita le pedía conectarse a un servidor del Comando de operaciones especiales de Estados Unidos para cargar los nuevos datos biométricos recopilados lo interesante es que el mensaje en pantalla proporciona la URL a la que se va a conectar a ver si adivinas un poquito Cómo es la url Martín por el tema que era una url como Cómo empieza la URL esta haydensic.com no pero antes de eso cómo empieza la url http bingo sabía yo si fuera preguntas o sea sin cifrar se enviaba todo vaya tela eh aquí es que madre mía los datos más sensibles biométricos y todo sin cifrar se enviaba justo y no comentan a ver dices igual el dispositivo tiene el software VPN no y automáticamente se conecta cuando tiene conexión WiFi o 3g o 4G o lo que sea pero probablemente No la verdad que bastante fallo fallo operacional fallo fallo de todo madre mía De hecho no sé si os acordáis pero en el episodio 81 comentaba un estudio que pude identificar sitios web de comunicación encubierta utilizados por los informantes de la Cia y resaltaba el problema de seguridad operacional debido a que no utilizaban cifrado tampoco utilizaban http para enviar mensajitos entre los informantes de la y los servidores de la Cia pues Este es otro caso de fallo de este tipo de seguridad de datos en tránsito no cifrados utilizando http el precio en Ebay de estos

dispositivos sic oscila entre 124 y 184 dólares americanos Los investigadores aparte de utilizarlo un poquito tocándolo y tal en persona pues luego hicieron lo típico no hacer un poco de osin online y Buscar a ver que encontraron instrucciones material de entrenamiento y vídeos de cómo usar los dispositivos también obtuvieron una guía interesante que es un PDF la voy a la voy a Añadir las notas del episodio es la guía del comandante sobre biometría en Afganistán y luego Tenemos también informes anuales del grupo de trabajo de biometría del departamento de defensa de Estados Unidos el investigador de seguridad alemán su nombre en concreto es Macías March compró un dispositivo sic por unos 125 dólares en lo más barato que lo encontró y con otros investigadores del que os computer club de Berlín analizaron El cacharro para los que no lo sepáis el que os compite Club es es un grupo digamos de hackers bastante importante en Alemania y además tiene conferencias que cada año hacen una la que os con Peter Clap Conference normalmente en diciembre y a veces cada dos o cuatro años creo la hacen en verano también en un hangar yo estuve en verano en una de esas Y la verdad fue muy interesante Así que si podéis ir si estáis cerca os la recomiendo en total lo que hicieron es acceder a los datos de la tarjeta de memoria del dispositivo que contenía datos de 2.632 personas los datos estaban se estaban dentro de un conjunto que lo habían llamado una lista de vigilancia en base a parámetros biométricos y no todo era parámetros biométricos como obviamente una foto de la cara el scan de huellas dactilares y del Iris pero también tenían otros indicadores como el primer nombre segundo nombre o nombre del medio no como le llaman en Estados Unidos apellido sexo raza altura peso color de ojos color de cabello fecha de nacimiento lugar de nacimiento estado de ciudadanía nacionalidad fecha cuando se agregó a la lista y el ID de lista de vigilancia estoy interesante porque la lista de vigilancia algunas decían si eran si se tenían que capturar si eran personas inofensivas bueno de ahí decía un poco el riesgo que tú a los a las tropas a norteamericanas contenía como digo 2.632 personas de estas tenían 2.300 rostros 2.946 escaneos de Iris un poco más que las personas Supongo que repetidos o de los dos ojos para algunas no sé eso no lo confirman Pero bueno Y luego 24.000 78 huellas dactilares bueno son casi el 10 veces más pero bueno y de estas 2.632 personas 1405 que es casi Bueno un poquito más de la mitad eran afganos y 125 son iraquíes y luego el tema descendiendo en otras nacionalidades no muchos según comentan los investigadores eran terroristas conocidos y personas buscadas pero otros parecían ser personas que habían trabajado con el gobierno de Estados Unidos o simplemente habían sido detenidos en los puntos de control los metadatos del dispositivo revelaron que se había utilizado por última vez en el verano de 2012 cerca de kandahajar en Afganistán Así que desde el 2012 hasta el 2022 que lo compraron diez años no se había estado en un almacén o había estado por ahí en casa de alguien sin haberse analizado Así que incluso a veces dices Ah este dispositivo han pasado cinco años ya seguro que no no se encuentra pues mucho cuidado con con dónde ponéis vuestros dispositivos que desecháis o que recicáis después de obtener los resultados del Análisis del primer dispositivo sic los investigadores compraron otros adicionales en eBay en total consiguieron seis dispositivos dos height y cuatro sick pues dos de los dispositivos sic tenían datos confidenciales de las personas que habían analizado y habían obtenido su Iris sus huellas dactilares y sus las fotografías de sus caras el segundo dispositivo sic en concreto contenía metadatos de ubicación que muestran que se usó por última vez en Jordania en 2013 y y parecía contener las huellas dactilares y los escaneos de Iris de un pequeño grupo de miembros del servicio estadounidense curioso verdad pues cuando el New York Times que estuvo involucrado en esta investigación al menos contactó a los investigadores luego contactó a uno de estos miembros del servicio estadounidense de los que se habían capturado estos datos biométricos y la persona confirmó que los datos probablemente apuntaban a que eran suyos dijo que en el pasado trabajó como especialista en inteligencia de la Marina y que sus

datos y los de cualquier otro estadounidense encontrado en esos dispositivos probablemente se recopilaron durante un curso de entrenamiento militar el hombre que habló bajo condición de anonimato Porque todavía trabaja en el campo de la inteligencia Y no está autorizado a hablar en público pidió que se elimine su archivo biométrico los oficiales militares confirmaron que esto era una práctica común utilizar estos dispositivos contra los propios soldados para para enseñarles a usarlos en el campo de batalla después de analizar todos los dispositivos Los investigadores sacaron varias conclusiones que os la comento a continuación la primera es que los dispositivos contienen datos reales que no están encriptados bastante fallo verdad la segunda conclusión fue que tienen acceso completo a todos los archivos programas y bases de datos locales en los dispositivos es decir no estaban protegidas estas bases de datos ni estos datos la tercera conclusión es que hay amplia documentación online luego también concluyeron que estos dispositivos tienen credenciales débiles y bien documentadas en documentos que se pueden encontrar online a través de osin también concluyeron que el software se puede utilizar de forma intuitiva es muy fácil de utilizar las consecuencias pueden ser graves como hemos visto si se identifican a las personas que estuvieron en Afganistán colaborando con los estadounidenses pues Y todavía se encuentran en ahora en territorio talibán pueden sus vidas pueden estar en peligro y lo último es que encontraron otro dispositivo similares que se pueden comprar online ya hemos visto que sick haydensic pudieron comprarlos online Pero también dicen que hay dispositivos militares estadounidenses similares que se pueden obtener en Ebay recuerdo de nuevo que los militares estadounidenses cuando se fueron de Afganistán a finales de A mediados del 2021 dejaron 7.000 millones de dólares en dispositivos detrás de ellos sin sin llevárselos con ellos no está claro exactamente como estos dispositivos fueron de los campos de batalla en Oriente medio a un sitio de subastas online como eBay según la agencia de logística de defensa que se encarga del reciclado de millones de dólares en exceso de material del pentágono cada año dispositivos como el hyde y sick nunca deberían haber llegado al mercado abierto y mucho menos a un sitio de subastas online como eBay en cambio se supone que todo el equipo de recopilación biométrica se destruye en el sitio donde se utiliza cuando el personal militar ya no lo necesita al igual que otros dispositivos electrónicos que alguna vez Tuvieron información operativa confidencial los datos confidenciales de los dispositivos se almacenaron en tarjetas de memoria Como he mencionado anteriormente Los investigadores es lo que se dedicaron a analizar porque realmente Ahí es donde estaban los datos almacenados si las tarjetas hubieran sido retiradas y destruidas algo tan sencillo como este gesto de clic sacar y pisotear o igual darle un martillazo estos datos no habrían quedado expuestos no está claro cómo los vendedores de eBay obtuvieron estos dispositivos pero el dispositivo con los 2.632 perfiles fue vendido por Rain of Trade una empresa de equipos reciclados de Texas en Estados Unidos el tesorero de la compañía David Méndez dijo que había comprado el sic en una subasta de equipos gubernamentales y no se dio cuenta de que un dispositivo militar dado de baja tendría datos confidenciales el sic con la información de las tropas estadounidenses es decir el segundo sic que analizaron con datos biométricos provino de techmart un vendedor de eBay de Ohio el propietario de techmart aiman arafa se negó a decir cómo había adquirido este y otros dos dispositivos que vendió a Los investigadores un portavoz de eBay dijo que la política de la compañía prohibía la lista de dispositivos electrónicos que contenían información de identificación personal literalmente dijeron se eliminarán los listados que violen esta política y los usuarios pueden enfrentar acciones que pueden incluir la suspensión permanente de su cuenta dicho esto a 12 de diciembre de 2022 según los investigadores días después de notificar a los responsables e incluso a eBay Aún se pueden encontrar se podían encontrar dispositivos hyde a la venta en Ebay por 270 dólares americanos Los investigadores también alertaron al

departamento de defensa de Estados Unidos sobre los datos desprotegidos quien contestó debido a que no hemos revisado la información contenida en los dispositivos el departamento no puede confirmar la autenticidad de los supuestos datos ni comentarlos de otra manera y también añadieron que el departamento solicita que cualquier dispositivo que se crea que contiene información de identificación personal sea devuelto para un análisis más detallado y acababan sus declaraciones diciendo dado que la vulnerabilidad real reside en el propio Hardware nuestras opciones están limitadas H ID global siendo El fabricante proveedor de estos dispositivos Hardware Debería ser el principal punto de contacto en este momento para la verificación y validación de sus hallazgos continuaremos monitoreando la situación a medida que se desarrolle los investigadores también contactaron al proveedor h y de global que dijo que no podía compartir detalles sobre sus clientes o implementaciones de productos específicos y que la configuración gestión protección almacenamiento y eliminación regular de datos es responsabilidad de la organización que utiliza dispositivos fabricados por h y d El problema es que esto ha puesto en riesgo la vida de muchas personas como he dicho incluidos soldados americanos y personas locales afganos que han trabajado con las fuerzas militares estadounidenses Y que ahora pueden estar en busca de captura si se encuentran en países totalitarios que disponen de la información de estos dispositivos como como digo el propio país Afganistán donde se utilizaron estos dispositivos el european digital rates que es un grupo de defensa de la privacidad dijo que el ejército debería informar a todas las personas cuyos datos han sido expuestos atribuyen y justifican que no importa que sea de hace una década y que uno de los puntos clave sobre los datos biométricos y por qué son tan confidenciales es porque pueden identificar a cualquier persona para siempre y es que las bases de datos biométricos son bombas de relojería Porque primero no puedes cambiar tus datos biométricos o si se puede es muy difícil y costoso por ejemplo una operación de cambio de huellas dactilares no es algo que sea bastante fácil ni barato por tanto no te puedes ocultar y finalmente la biometría que te da acceso En algunos momentos se vuelve en tu contra eventualmente el investigador Marx presentó su investigación en un evento en el caos computer club de Berlín hace unas semanas este mes de marzo Pero obviamente no se ha publicado la información obtenida de los dispositivos para proteger a todas las personas que están involucradas y que estos dispositivos tienen sus datos biométricos Y esto podría parecer un incidente aislado único que sucede poco pero desgraciadamente no es así hace tres años se publicaba que un portátil del boom de sware el ejército alemán que se vendió en Ebay Por 90 euros contenía información secreta sobre un sistema de defensa que utiliza misiles y que aún estaba en uso a la fecha de la publicación de la noticia en marzo de 2020 el portátil era del fabricante Alemán roda con Windows 2000 un procesador pentium 3 bastante antiguo 128 megas de ram y bastante pesado unos 5 kilos Los investigadores de seguridad de la empresa G Data con sede en bohum Alemania analizaron el portátil y vieron que se iniciaba sin necesidad de solicitar credenciales el software principal tenía una contraseña por defecto guest de invitado en inglés y contenía datos interesantes no encriptados como instrucciones para destruir el sistema de defensa aérea leflasis ocelot en caso de emergencia que es un sistema de misiles que se monta encima de un tanque de guerra para derrumbar a objetos voladores lo curioso es que aunque el procedimiento dice que hay que retirar el disco duro o borrarlo con métodos fiables antes de vender o reciclar el ordenador los militares no hicieron lo especificado en las instrucciones de reciclado o desechado con este portátil y de hecho no es la primera vez que le ocurre algo así a la bundestware en julio de 2019 un guardabosques de la alta baviera compró un ordenador portátil junto con las instrucciones de funcionamiento clasificadas de un lanzacohetes de llamado Mars y compró este ordenador en una subasta de la sociedad de recaudación Federal que tiene entre otras funciones la misión de gestionar los

objetos que desecha el ejército alemán desde teléfonos y vehículos hasta helicópteros y ordenadores viejos así que ya vemos que una organización cuya responsabilidad principal es la de asegurarse de que se desechan o se reciclan dispositivos del ejército alemán de forma segura pues falla mucho en sus funciones yo incluso una vez tuve que hacer un análisis de seguridad de una bomba de infusión de estas grandes que se pueden encontrar en hospitales que se usan para proporcionar a los pacientes pues medicinas suero fisiológico y similar y conseguí una inhibe me conecté vía Puerto ethernet credenciales por defecto del manual del fabricante online y tuve acceso a los datos no cifrados que obtenían contenían información sobre pacientes medicaciones y dosis concluyendo Este es un caso de mala práctica de protección de datos y De hecho no es un incidente aislado se han encontrado múltiples dispositivos militares médicos y similares que contienen información personal que podría suponer graves riesgos para las personas relacionadas Este es un gran ejemplo para aquellos que se oponen al cifrar los datos Porque no tengo nada que esconder podría decirse no pero siempre hay algo en tus datos que de alguna forma u otra se puede utilizar en tu contra sobre todo por Mentes malvadas no es el caso igual de familia y amigos pero si el de enemigos y cibercriminales así que acabo recordando queridos oyentes de que tengáis cuidado cuando recicléis o desechéis vuestro dispositivo es electrónicos os comento algunas de las formas más efectivas para proteger vuestros datos en dispositivos reciclados o desechados una forma sería a través de métodos software podría hacerse restableciendo los datos de fábrica o incluso utilizando herramientas de borrado especializadas estas que dicen de grado militar en lo que hacen es escribir muchas veces en el disco duro datos para que realmente los discos los datos que habían originalmente que queréis borrar realmente se borren se sobreescriban con datos totalmente aleatorios sobre métodos Hardware pues tenemos que para dispositivos de almacenamiento magnéticos como discos duros los antiguos los tradicionales se pueden utilizar dispositivos de desmagnetización en inglés se conocen como the gausers por la relación del científico gauss y el con el campo magnético Aunque Esta técnica no afecta a dispositivos de almacenamiento ssd de solid State drives discos de estado sólido o incluso tampoco afecta a nand flash como los que podemos obtener o podemos usar en samdrives o esos spence USB no en este caso para dispositivos lo mejor es utilizar herramientas software de borrado especializadas o métodos físicos básicamente destruirlos y pasando a estos métodos físicos de destrucción pues lo que se podría hacer es si vuestros dispositivos tiene tarjetas de memoria discos duros o incluso la memoria RAM que a veces puede contener datos que no sean vaporizados sean todavía se están guardando porque están en la memoria durante algún tiempo no años pero igual algunos días y si lo vendéis justo después de haberlo apagado pueden contener incluso vuestras vuestros datos sensibles Así que tener cuidado también con la memoria RAM Pues nada le podéis dar algunos buenos martillazos o algún buen golpetazo con contra la pared contra el suelo como queráis luego podéis vender el resto del dispositivo como la placa base monitor ratón teclado etc siempre y cuando no sean inteligentes y tengan dispositivos de almacenamiento en bebidos porque en muchos casos últimamente en las televisiones son inteligentes y tienen incluso almacenamiento pueden grabar vídeo y similares Así que cuidado en estos casos y si fuera necesario de vuelta al martillo y para evitar dañar más al planeta lo ideal es reciclar los dispositivos y venderlos a empresas de reciclado o donarlos a personas que lo necesitan pero si no hay forma de asegurarse de la protección de los datos Pues en algunos casos es mejor darles unos buenos golpes y a la basura Bueno cuando digo basura me refiero a estos sitios donde llevas los dispositivos que ellos en principio los tratan de forma responsable e intentan reciclarlos lo más posibles separar los diferentes materiales y bueno hacer un buen uso lo mejor que puedan para para evitar dañar más al planeta todo lo que comento son medidas reactivas y quería comentar una medida proactiva para proteger los

datos en reposo que es la de cifrar todo el disco idealmente y si no se puede al menos cifrar un volumen o parte del sistema de ficheros o incluso la tarjeta de memoria completa de esta forma es menos probable que se consigan estos datos protegidos Aunque no es imposible las claves pueden estar en algún lugar no cifrado del sistema de ficheros o en documentos online incluso o como digo podrían estar en la ram así que ya sabéis queridos oyentes tener cuidado con los dispositivos que desecháis recicáis le dais a alguien vendéis online y sobre todo tener cuidado con los datos que estos llevan y intentar hacer algo para protegerlos eliminarlos o hacer algo al respecto pues ya sabéis queridos oyentes mucho cuidado porque Aunque parezca que que nuestra información al cabo del tiempo está segura en dispositivos en cosas así de Hardware Es que esto no es la primera vez que hablamos de Hardware que se consigue a través de eBay o los wallapop por lo que sea MercadoLibre y luego la gente se pone a hacer reversa enging o bueno no reverse ingeniering sino más bien ay que no me sale ahora hombre forense análisis forense porque he visto he visto charlas en Def con donde compran servidores servidores que han sido utilizados por gobiernos y cosas así todavía mantenía información de hecho Ahí si vosotros os vais a borrar el disco duro veis que se puede elegir Incluso en vuestros macbook pros nivel de grado con el que se borra el disco duro porque recordemos que borrar un disco duro no elimina la información sobre solo la marca como que se puede sobreescribir entonces hace falta hacer varias pasadas Por así decirlo y Hay ciertos niveles que son digamos grado militar no un poco lo que escuchamos aquello Cuando te quieren vender criptografía y todo esto Pues es lo mismo para eliminación de información y lo mejor de todo sería que estuvieras cifrado porque entonces te deshaces de la llave de cifrado y ya está pero bueno muy muy muy interesante Alexis Sí sí justo lo que te dice es Martín como como acabo de comentar también pensado un poquito en las opciones que os hemos dado para un poquito tratar bien a esos dispositivos que desecháis o recicláis pero sí tener cuidado y pensad que aunque lo desechéis todavía su vida continúa y si no lo tratáis bien su vida se puede volver en contra vuestra claro Aquí no hay un End of Life No como la obsolescencia programada eso no quiere decir nada para nuestros actos solo si los de machacas y lo destruyas con un martillo como digo ya hay físicamente exactamente de hecho hay de desmagnetizadores de discos duros que creo que hemos mencionado alguna vez bueno queridos oyentes hasta aquí Hemos llegado no nos liamos más Muchísimas gracias por quedaros hasta el final recordad visage Barcelona si queréis atender que tenemos el sorteo para la hack aquí en tierra hacker siempre colaborando con todo el mundo Así que ya sabes déjanos un like Bueno una review estrellitas lo que sea que nos puedas dejar que nos echas una mano y nos ayudó un montón Eso es en muchas estrellitas que nos gustan las estrellitas y nada Muchas gracias por apoyarnos siempre y hasta la próxima venga Adiós adiós 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