ftx la plataforma de inversión en criptomonedas más grande del mundo se declara en bancarrota y su fundadora acaba en la cárcel después de que salga la luz una historia de rivalidades estafas engaños hackeos favores políticos y romances digna de Hollywood una investigadora accede a un servidor expuesto en internet de la aerolínea commute Air parte de United Airlines y consigue obtener la lista de exclusión aérea estadounidense o no Playlist list que contiene detalles de personas a las que no se les permite Volar por ser sospechosas de terrorismo sin prisa pero sin pausa Seguimos con nuestra edición semanal de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast Toy es el 22 de enero de 2023 este es el episodio número 80 yo soy Martín vigo y está conmigo un cacho de Alexis porros Hola Alexis qué tal te falta un trozo dice buenas Martín sí un pequeño incidente con tareas domésticas lavando algún que otro vaso Pero bueno todo bien Todo bien algunas puntillos pero todavía puedo teclear y hacer y hacer daño con el con el piano digo con el teclado bien bien me alegro Pues nada ya episodio 80 madre mía prontito episodio 100 La verdad es que el tiempo vuela Así que nada muy muy muy contentos de estar con todos vosotros queridos oyentes En todos estos episodios Así que aquí vamos a por una más vamos a dar gracias como siempre a nuestros queridos oyentes Gracias por estar ahí apoyándonos en redes sociales en discord en todos las plataformas online donde nos escribís nos dais sugerencias nos enviéis noticias y nos respondéis a las preguntas del episodio incluso no solo votáis sino que añadís también vuestros comentarios muy interesante también os recordamos que si no lo estáis deberíais estar suscritos a nuestro podcast en vuestra plataforma de escucha favorita la que sea estamos en todas Así que pida suscribiros también nos podéis seguir en redes sociales Twitter infoset.exchains el servidor de Instagram Facebook todo estos nos podéis encontrar con el handle @tigradehackers linkedin Twitch estamos como tierra de hackers los correos electrónicos no los podéis enviar a podcast arroba tierra de hackers.com y podéis entrar al servidor de discord que tenemos a través de tierra de hackers.com barra discord finalmente como siempre en la intro queremos agradecer vuestro apoyo a la pregunta del episodio que publicamos en Twitter y que para el episodio anterior fue la siguiente qué creéis que era el objetivo de Cold River apt ruso a las órdenes del kremlin al intentar acceder a laboratorios estadounidenses dedicados a la investigación nuclear y será la pregunta y teníamos cuatro respuestas la más votada fue la de Sabotaje con un 30% muy seguida de robo de secretos con un 28% de los votos también muy seguida de célula Durmiente con un 24% y finalmente tenemos un 18% que corresponde a conocer al enemigo Así que la mayoría de la gente bueno se ha dividido bastante equitativamente entre un poquito de Sabotaje robo de secretos célula durmiente vamos que no están seguros o obviamente podría ser todos esos casos porque un apt muchas veces tiene más de una motivación detrás suya Pues yo continúo dando las gracias a todos nuestros oyentes que deciden apoyarnos en patreon muchísimas gracias de verdad que marcáis la diferencia y a nuestro sponsor que en este caso es 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 inmonada a través de una herramienta de gestión y visualización de telemetría de datos de seguridad fundada en Valley y buscando ingenieros sobre todo con algo de experiencia en seguridad para ayudarles a construir y hacer realidad su misión lo mejor de todo es que están contratando en todo el mundo y en remoto así que ya sabéis echar un vistazo a su web monat.com monad.com y les podéis mandar vuestro currículum a tierra de hackers @monas.com también mencionar que como íbamos ya poniendo en Twitter y en discord vamos a comenzar con un sorteo de entradas para la para varias conferencias para dos de ellas que ya podemos anunciar una de ellas es la ruted tenemos cinco entradas que vamos a sortear que una entrada a la ruta y Son 180 pavos ahora mismo Así que como veis tiene tiene bastante valor una de esas Ya ves esto

Esto es lo bueno que tiene escucharnos Escuchar tierra de hackers este tu podcast favorito una solo aprendes un montón con nosotros no solo esperemos que te lo pases bien sino que de vez en cuando pues conseguimos pues este tipo de cosas para poder repartirlas con vosotros o sea cada día es navidad en tierra de hackers queridos oyentes es el nuevo es el nuevo eslogan pues la router es una conferencia una de las mayores sino la mayor de España que se celebrará en Madrid en creo que en marzo sería haberlo escrito pero bueno ya lo iré anunciando Así que si creéis que podéis asistir pues no dudéis en participar lo anunciaremos en Twitter en la próxima semana probablemente haremos algo en plan que para participar pues contestes al tweet total para tener referencia de quién se está apuntando al sorteo y nada muchísima suerte como decía una de las entradas las sortearemos en exclusiva entre nuestros mecenas de patreon Pues un poco para agradecer y hacer ahí un retorno of investment de la aportación económica que ellos nos hacen pues es una manera de devolvérselo a ellos y las otras cuatro pues ya entre todos incluyendo por supuesto también a nuestros mecenas de patrón pero también queremos anunciar Por cierto mencionar que además esto viene en parte por una colaboración con uno de los tracks en la router que es cripto red que en concreto Pues creo que el día jueves es cuando van a estar dando una serie de charlas muy buenas que yo desde luego voy a asistir estaré allí y os recomiendo a vosotros pues hacer lo mismo luego mencionar por otro lado otra conferencia la Barcelona Cyber Security Congress como veis de momento vamos dominando España a ver como decíamos en el episodio anterior ya iremos dentro de poco expandiéndonos a latinoamérica Pero bueno Tenemos aquí esta otra conferencia Barcelona Cyber Security Congress que sucederá entre el 31 de enero fin de semana que viene o sea el lunes que viene digo y el 2 O sea que son tres días de conferencias y en concreto dentro de esa conferencia está el hacking Village que es donde va a haber ctfs donde Vais a tener temas de abrir cerraduras con ganzúas cursos charlas buenísimas pues tierra de hackers no solo es un media Partner del Barcelona Cyber Security Congress no solo estamos ahí como unos de los miembros que apoyan este congreso sino que además en concreto yo ya una Lamentablemente Alexis ya que se encuentra en Nueva York no podrá estar pero yo estaré ahí haciendo de como me dicen maestro de ceremonias de MC Durante los dos días enteros anunciando las charlas anunciando a nuestros speakers colaborando en varios foros y conversaciones y debates que vamos a tener muy interesantes Así que no faltéis y os vamos a dejar una vez más en Twitter y en discord unos códigos de descuento para las entradas pero también sortearemos entradas para que podáis entrar de manera totalmente gratuita así que ya sabéis por un lado entradas para la router por otro lado entradas para la Barcelona Cyber Security Congress el primer sorteo lo haremos sobre esta ya que sucede dentro de una semana Así que lo pondremos estar atentos a nuestro Twitter durante esta semana que ahí pondremos tanto los códigos de descuento como el sorteo joder Martín me quedo con las ganas con los dientes largos ahí de estar contigo y ver a toda la gente Todo todo el meollo claro un cacho de tierra de hackers que estaba estudiando es que te faltaba te faltaba un cacho tío Pues claro va todo esto vas a llevar pegatinas no lo más preciado de que nuestros oyentes quieren por supuestísimo voy a llevar me he comprado 500 pegatinas Para repartir entre entre la gente que viene siempre a saludarnos que viene a hacerse fotos con nosotros A preguntarnos qué tal qué tal estamos a decirnos lo mucho que le gusta el podcast nos hace una ilusión tremenda Y por supuesto todo lo que podamos hacer por la comunidad y por nuestros oyentes de sobra es sabido que lo haremos Pero bueno no quiero liarlo más Ya sabéis que ahí estamos siempre intentando colaborar con la comunidad encontrando oportunidades para llevaros no solo a través del podcast sino conferencias colaboraciones todo lo que podamos pues medios para que podáis acudir a seguir formando si crear todavía más pasión en torno a la ciberseguridad y con eso me callo o no pero empiezo por lo menos con la noticia vale si bien en tierra de hackers nos caracterizamos por traeros la

más absoluta actualidad en temas de ciberseguridad ya que como dice nuestro eslogan Este podcast es un noticiero no he de confesar que llevo monitorizando esta noticia que os traigo pues varios meses ya y la razón es que cada semana ha estado desarrollándose los acontecimientos Y en vez de hablar de esto nada más sucedió prefería traeros la historia completa hablemos de ftx me consta que muchísimos de vosotros ya habréis oído hablar del escándalo financiero que provocó la bancarrota de esta empresa Pero quizás no conocéis todos los detalles y como es de esas que da para película de Hollywood como siempre os decimos yo os la traigo aquí con todos los detalles os presento a Sam backman fright el personaje principal de esta historia tan loca hijo de dos abogados y profesores de Stanford fundó Alameda research unos años después de finalizar sus estudios en Stanford quedaros con el concepto de Alameda research Porque será una pieza fundamental en esta historia Alameda research fue fundada en 2017 como decía por Sam y otra persona llamada tara Mac aulai y empezaron a hacer mucha mucha pasta dedicándose exclusivamente al arbitraje de bitcoin y qué es esto del arbitraje de criptomonedas pues la compraventa de por ejemplo bitcoin entre diferentes exchanges o plataformas de intercambio de criptomonedas resulta que diferentes plataformas tienen diferentes precios para una misma moneda Y aunque la diferencia sea mínima de céntimos dado que la compraventa de bitcoin no solo se puede automatizar sino también es escalable si Vas sacando céntimos o satoshis en este caso y haces miles de transferencias al día pues al final haces mucho dinero básicamente Por decirlo de alguna manera veo que en Kraken o coinbase una plataforma de intercambio de monedas puedo comprar bitcoin a 10.000 euros un bitcoin y que en vainas lo puedo vender a 10.000 euros con 10 céntimos pum ya tengo una ganancia de 10 céntimos por bitcoin se entiende No pues ahora esto lo haces miles y miles de transacciones según monitorizar los precios y ya está Y así te vas ganando mucho dinero y esto es precisamente Cómo empezó esta empresa a la meda resorts pues es así como hizo la fortuna inicial también Sam y viendo que iba bien a la meda research se abrió a nuevas formas de inversión como la compra de criptomoneda como solana que está íntimamente ligada al mundo de los nfts Pues bien solo unos meses después de fundarse Alameda research tara la recordad la persona que había fundado a la meda reasons junto con Sam tuiteaba públicamente que abandonaba junto con un grupo de ingenieros la empresa debido a y bueno cito textualmente preocupaciones con la gestión de riesgo y la ética a la hora de hacer negocios aquí ya vemos que solo meses después de la trayectoria emprendedora de Sam sus compañeros ya empiezan a sembrar dudas nos vamos a abril de 2019 cuando nuestro amigo Sam decide fundar otra empresa ftx tirando de la reputación ganada gracias a la meda research porque a la me da risa en ese momento seguía haciendo dinero uno de los primeros inversores de ftx empresa que se centraría en ser una de las mayores plataformas de inversión en criptomonedas fue el fundador de binance chapen Saw También conocido como Sisi que es como le voy a llamar yo a partir de ahora y aquí llegamos a otra de las variables de esta historia muy importante binance y Sisi binance al igual que ftx es una plataforma la mayor del mundo de hecho para comprar vender invertir en criptomonedas ftx de hecho creó dos plataformas ftx y ftx Us la segunda centrada en regular en el mercado de criptomonedas específicamente en Estados Unidos Vale pues nos movemos ahora al año 2021 Solo dos años después de que Sam fundase ftx y esta empresa ya se había transformado en el segundo exchange más potente del mundo con un valor estimado de 30 billones de dólares billones con b solo por detrás de binance que sigue siendo la número uno dado que ftx creció tanto Sam decidió hacer ceo de Alameda research la primera empresa que había fundado a Caroline ellison Caroline es otra pieza fundamental en esta historia y ambos se conocieron en 2018 mientras estaban en una empresa de inversión llamada jamestre se cuenta que Caroline es superdotada y tiene unos conocimientos muy elevados de matemáticas de hecho leía por ahí en la Wikipedia que

teóricamente le hizo un trabajo de matemáticas a su padre Cuando solo tenía 8 años pero Cabe destacar también que al igual que Sam es muy joven 26 años cuando la hicieron ceo de Alameda research recordemos una empresa millonaria dedicada a la inversión de criptomonedas y no tenía ninguna experiencia laboral Pues bien esta decisión de Sam de hacer ceo de una empresa tan importante no viene tanto por lo inteligente que era Caroline sino Parece ser que es más bien porque ambos estaban en una relación romántica Caroline y Sam eran novios cuando se tomó esa decisión por tanto ahora tenemos a Sam al mando de ftx empresa valorada en 30 billones de dólares sino también que tenemos a la novia de Sam promocionada a ceo de alamada research de la nada empresa donde San por cierto aún tenía el 90% de las acciones por eso pudo hacerla feo Pues ftx en este punto estaba por todos lados con anuncios constantes en televisión protagonizados por estrellas de cine Como Larry Davis y deportistas de élite como Steve curry shaquille o'neal o Tom Brady y Sam por su cuenta Se convertían una estrella él mismo con presencia constante en los medios transformándose en la cara amable por ejemplo del movimiento efective altruismo movimiento cuya filosofía es generar las máximas ganancias de dinero durante tu vida para donarlo todo cuando te vayas a morir y también siendo un ejemplo de buen millonario ya que es vegano y con todo el dinero que tenía pues decía que conducía un Toyota Corolla no San también se convierte en una de las personas más ricas del mundo ocupando el puesto 60 en el ranking con un patrimonio estimado en los 26 billones de dólares que son cirífugas astronómicas La vida es bella para Sam que opera ftx y supervisa la media reachers desde su mansión en Las Bahamas pues ha llegado la hora queridos oyentes de plantarnos al comienzo del debacle estamos a 2 de noviembre de 2022 haces casos dos meses y medio ese día condesk uno de los medios informativos más conocidos sobre criptomonedas publica un artículo explosivo que marcará el inicio del fin de ftx y lo que algunos consideran el lehman Brothers de las criptomonedas coindesk consigue acceso a un documento interno de Alameda research que muestra que esta empresa Tiene un total de 14.6 billones en reservas hasta aquí todo podría parecer normal el detalle está en que la mayoría de ese patrimonio es en forma de la criptomoneda ftp una moneda creada por ftx por si no lo acabáis de pillar las reservas financieras de Alameda research son básicamente una moneda inventada por su propio fundador una moneda que en principio tiene la función de darte descuentos si haces trading en ftx pero que como digo fue creada de la nada para ese propósito esto es como si yo monto una empresa y esa empresa crece hasta tener un valor de billones de dólares en activos activos entre comillas pero se descubre que los activos de mi empresa son mi colección de calzoncillos usados que yo mismo he valorado en un billón de euros cada calzoncillo usado Sé que es difícil de creer pero tan cierto como la magnitud de este escándalo en palabras del ceo de una famosa plataforma de inversión financiera y cito textualmente es fascinante ver que la mayoría de los bienes netos de Alameda research es en realidad la moneda creada de la nada y controlada exclusivamente por ftx esto como digo no lo digo yo sino este ceo esto por supuesto puso a toda la comunidad en torno a las criptomonedas en alerta pero no solo a la comunidad sino también a reguladores porque recordemos que estamos hablando de millones de dólares de dinero real invertidos tanto por inversores y gente como tú y como yo bueno como yo no y es porque como tú tampoco porque si no significa que te habrás quedado sin ese dinero pero ya me entiendes Como gente normal Sam inmediatamente reaccionó a este artículo intentando calmar a inversores a través de Twitter diciendo que las reservas de ftx estaban a salvo y que no había nada de que preocuparse eso es lo que decía su tweet recordemos que por ley el dinero que ponen los clientes una entidad financiera para sus propios ahorros no puede ser utilizado sin su consentimiento para otras inversiones es decir tu banco donde tienes tu dinero no puede coger ese dinero e invertirlo para ganar más dinero o ellos necesita tu consentimiento y esto por

cierto también lo decían los términos de servicio la propia web de ftx hace que si las reservas de dinero estaban a salvo Pues en principio bueno no habría mucho de qué preocuparse no pues solo cuatro días más tarde 6 de noviembre de 2022 Sí sí recordar el ceo de binance e inversor inicial de ftx da la estocada final a ftx tuiteando lo siguiente como parte del plan de salida de vainas de su inversión en ftx vainas recibió el equivalente a unos 2.1 billones de dólares en moneda ftp dadas las revelaciones recientes hemos decidido vender todas nuestras monedas ftp pensar lo que estaba diciendo en este tweet de un día para otro el mayor inversor de tu empresa decide transformar la moneda que tú te has inventado en dinero real por el equivalente de billones de dólares y por supuesto tienes que pagarlo estos catastrófico para una entidad financiera sobre todo porque este tweet arrastró a toda la gente a hacer lo mismo y liquidar sus ftps por dinero real o bueno otras criptomonedas no es decir vender sus ftps para que les den bitcoin o pasta real nuestros oyentes de hecho argentinos recordarán una versión de esto en el pasado cuando sucedió el tema del corralito en el que los bancos como se estaba todo el mundo quería sacar dinero y hubo un momento que no había liquidez pues decidieron bloquear la capacidad de retirar el dinero de cajeros para evitar el colapso de los bancos lo que pasa es que en el caso de las criptomonedas tiene consecuencias aún peores que en el caso del corralito Por así decirlo Por supuesto que lo del corralito fue fatal pero es que la gente al vender de manera masiva monedas ftp estas a su vez bajan de valor porque la baja la demanda Y al bajar el valor de ftp hacía que más gente aún quisiera deshacerse de ellas y lo peor de todo es que según bajaba el valor debido a que la mayoría de activos de Alameda research y de ftx eran ftp esto se quedaban sin fondos y ftx siendo ftp como decía su manera principal de hacer dinero y Quienes más tienen les pasaba pues tres cuartos de lo mismo o sea que vamos que tenemos una reacción en cadena totalmente catastrófica para Sam y sus empresas para que os hagáis una idea en 72 horas 72 horas ftx liquidó 6 billones de dólares en ftp quedándose sin dinero real para satisfacer la lista enorme de transferencias pendientes de otros clientes que también querían vender sus ftps pero hay algo que nos dejamos en el tintero Por qué el ceo de binance Sí sí teniendo en cuenta que era uno de los mayores inversores de ftx y amigo de Sam iba a interesarle hacer pública su decisión sabiendo que es un diría la empresa Pues resulta que meses antes Sam y Sisi pasaron de ser amigos a enemigos y aparte públicamente sus tiranteces y ataques se podían ver públicamente en Twitter mientras se tiraban dardos envenenados mutuamente todo ello porque cuando Sam creció de la nada a ser el segundo exchange más grande del mundo solo por detrás de vainas empezó a establecer relaciones con políticos y legisladores en Estados Unidos para hacerles Loving y beneficiar a su empresa de hecho salió a la luz donaciones por parte de Sam directas al partido tanto demócrata como republicano que incluso creo que para el demócrata fue el mayor donante de 2021 o 2020 hablamos de millones de dólares Pues bien Sí sí se enteró de que Sam fue a sus espaldas a pedir a hacer todo este lobbing a los políticos y que parte de los cambios legislativos que Sam estaba intentando impulsar perjudicarían gravemente a vainas lo cual por supuesto cabreó mucho a Sisi declarándole la guerra abiertamente por tanto sí sí no solo quiso deshacerse de su Gran Reserva de ftp sino que vio la oportunidad perfecta para aplastar públicamente a su enemigo en el campo de batalla donde estaban librando la guerra hace meses Twitter y todo esto además con un solo tuit Pues solo dos días más tarde Estamos a 8 de noviembre de 2022 viene la guinda del pastel que se cocinó Este sí sí este anuncio en Twitter que va a comprar ftx para salvar la empresa y a sus inversores toma ya primero usas Twitter para hundir financieramente a Tu rival y cuando ya no vale nada anuncias que la compras o sea una jugada maestra pero esperad queridos oyentes que viene ahora el plot twist solo 24 horas más tarde 9 de noviembre de 2022 una vez más en Twitter binance anuncia que se retira del plan de la compra de f3 de ftx tras estudiar su contabilidad noticias de supuesto uso fraudulento de fondos de

clientes y una posible investigación por parte del gobierno de los Estados Unidos O sea imaginaros el panorama y el pánico entre la gente uno de los exchanges más importantes del mundo capitaneado por el chaval altruista al que todos admiraban es acusado de tener todo su capital basado en su propia moneda luego toda la gente se deshace de esa moneda tras un tuit de su mayor rival para que luego se ofrezca rescatarles y al día siguiente dice que no que pasa que hay mucho follón en su contabilidad y pinta muy mal pues si bien durante toda esta semana que transcurrió Sam seguía tuiteando que no había nada de que preocuparse dos días más tarde el 11 de noviembre ftx se declara en quiebra junto con todas sus subsidiarias además que incluye por supuesta a la meda research pasando a ser el nuevo ceo de ftx John Jay ya que no solo se declara un bancarrota sino que abandonó el puesto de ceo Pues solo horas más tarde de anunciar ftx la bancarrota de ftx ftx anuncia que ha sido hackeado y 300 millones de dólares han desaparecido toma ya qué conveniente alegan de hecho que fue un empleado que tenía instalado malware en su ordenador Solo dos días más tarde el 13 de noviembre la agencia de noticias reuters publica que al menos un billón billón con b de dólares de los fondos de dinero de clientes han desaparecido o sea 300 millones me los han hackeado por aquí un billón ha desaparecido por allá espectacular o sea es que estoy intentando hacer las matemáticas decíamos que estaba valorada en 30 billones que tenía solo 14,6 Claro pero tenga en cuenta lo que dije estaba valorada en 30 billones pero claro muchos de sus ases era su moneda inventada porque claro era 30 billones de dólares era en assets que tienen un valor que fluctúa brutal no era un Fiat o una moneda fija sabes con un curso legal bueno curso legal sí que tienes Supongo pero mi pregunta era Pero espera que viene cuánto le quedaba después de haberle robado los 300 millones y el billón cuánto le queda ya bueno no sabemos si lo robos aquí a ver si nos va a denunciar el Sam tío siempre añade el supuestamente pero bueno decía que Que bueno que aquí después de eso de que 300 millones hayan dicho que no están porque les han hackeado y que un billón de dólares pues no aparece por ningún lado aquí ya es cuando se arma la marimonera en los siguientes días porque sucede las siguientes cosas ya resumiendo se crea una demanda colectiva contra todas las estrellas que salían los anuncios de ftx por publicidad engañosa esto incluye al everyday Tom Brady Giselle Kevin este que sale en lo de shark Tank Naomi osaka shaquille o'neal Steve curry vamos toda esta gente famosa que ha salido en publicidad les denuncian por otro lado el gobierno de los Estados Unidos Llama a declarar ante el congreso a Sam luego tenemos que John Jair Ray recordemos el nuevo ceo de ftx que lleva solo tres días en el puesto hace las siguientes declaraciones jamás en toda mi carrera había visto tal completa falta de controles y absoluta ausencia de información financiera fiable como he visto aquí desde la integridad comprometida de los sistemas falta de regulación por parte de gobiernos a la concentración de control absoluto en manos de un pequeño grupo de individuos sin experiencia y potencialmente comprometidos esta situación no tiene precedentes esto el ceo el nuevo ceo de ftx que llegó ahí me imagino que a los 72 horas sin dormir dijo que qué es esto tío Qué es esta vaina bueno por supuesto No faltaron tenemos que Añadir esto aquí los estafadores añadiéndole leña a esta estafa haciendo su estafas sobre la estafa que os acabo de escribir oportunistas empezaron a salir empezaron esto es inception tío un sueño en un sueño empiezan a salir cuentas de Twitter publicando un vídeo Deep fake de Sam diciendo que iba a devolver el doble de dinero que habían invertido los clientes de ftx y que para ellos solo tenían que ir a una web y rellenar sus datos os dejo el vídeo Deep fake en los enlaces del episodio junto con más información donde me he documentado porque la verdad está bastante logrado y podría haber como alguien desesperado que acaba de ver como toda su inversión ha desaparecido podría intentar creérselo porque se lo quiere creer evidentemente cuando lo veáis ya lo veis con ojos de esto es un Deep fake pero no está nada mal Así que Aquí vemos que los estafadores se aprovechan de otras estafas para hacer su

propia estafa sobre sobre esa estafa que me encanta este concepto pues Bueno estamos en el 22 de noviembre los primeros detalles con cifras reales empiezan a emerger donde se hablaba que ftx debía unos 3 billones de dólares a instituciones financieras en forma de créditos que habían pedido También salió a la luz que antes incluso de que todo esto sucediera que os acabo de contar entre 2019 y 2021 ftx y a la meda research perdieron entre los dos cuatro billones de dólares destacando como en realidad nada era lo que parecía y lo bien que iban las empresas eran solo apariencias y llega el 12 de diciembre cuando inevitablemente las autoridades de Bahamas detienen a Sam después de darse supuestamente a la fuga para extraditarlo a los Estados Unidos el 22 de diciembre de manera la verdad un poco inexplicable para mí el juez decide ponerle una fianza Sam que si la paga Puede irse a su casa si bien es la más alta de la historia 250 millones de dólares joder un tipo que valía 26 billones de dólares no va a tener problemas que desaparecen 300 millones por aquí de dinero real no de ftp de dinero real y un millón por allá y de repente puede pagar 250 millones así a tocateja pues ya me dirás tío No sé que a lo mejor soy un desconfiado No lo sé pero bueno las condiciones de poder salir es que tiene vivir en casa de sus padres que esto me parece la leche El chaval tiene que volver a vivir con sus padres y llevar en el tobillo un brazalete electrónico para monitorizar donde está en todo momento un poco lo que le dicen al houser rust no el tiene que estar en casa y no puede salir de ahí Pero oye por lo menos no está en la cárcel de manera preventiva y aquí es a donde estamos a día de hoy con el juicio previsto para octubre de 2023 en principio decidí traeros la noticia esta semana precisamente porque no he visto mucho más movimiento no Bueno uno sí pasó que le da el giro de hacking que tanto nos gusta a esta historia recordáis Cuando os comentaba que horas más tarde de anunciar la quiebra de ftx anunciaron que había desaparecido cientos de millones de dólares porque habían sido hackeados Pues toma ya el miércoles pasado hace apenas unos días el tribunal de Delaware donde se juzga el caso de ftx declaraba que le habían llegado informaciones de que Sam indicó al cofundador de ftx Gary One a crear una puerta trasera para desviar fondos de clientes de ftx Alameda research de manera encubierta sin el consentimiento ni el conocimiento ni de reguladores ni de clientes esto lo hizo insertando una sola línea de código en los sistemas de ftx y la cantidad transferida de manera encubierta fue de cuánto Alexis para terminar la noticia un billón al más más frío frío pero si no tenían tanto pues vamos a poner 20 billones 65 billones de dólares y es que flipo me imagino que que será una vez más entre criptomonedas y todo esto no será de pero claro como aquí están yo me hago mi moneda yo me hago mi historia yo me hago tal yo me hago Cuál es una locura sería entre eso entre criptomonedas entre dinero real entre todos 65 billones de dólares una sola una sola línea de código de puerta trasera zas para mandar su dinero entre empresas acojonante madre mía y esa línea de código dan detalles sobre qué hacía exactamente que era o sea parte de enviar el dinero pero más detalles técnicos o Yo supongo que diría si fondos mayor que 65 billones transfiere 65 millones y ya está justo tampoco joder No puede ser mucho más a no ser de que sea una lambda de estas de que es medio programa y ahí metido tío Pues sí interesante y el un sistema que se me ha quedado aquí un poco me queda pensando es como como a ver Eres un ceo que te ofrecen el cargo En esta empresa que no es que tenga muy buena reputación no y vas y lo aceptas sin analizar un poquito la empresa y un poquito cómo está estado interno a ver yo entiendo que cuando te ofrecen un trabajo te dan un disclosure agreming de estos no y puedes un poquito analizar un poco hacer un poco de Inquisición no a la empresa Pero este tío eso eso te puede contestar el ceo que tomó el mando Era un era un tío famoso ya por tomar los mandos de no me acuerdo de la empresa tío pero hubo otra quiebra muy muy grande y este tío era famoso porque tomó los mandos de esa empresa también entonces me imagino que un poco lo eligieron a él me imagino porque es un tío que no sé pues que esa va a hacer las cosas bien o levantarse que no

me acuerdo ahora cuál es estos típicos como la MTV no que salen Pink my house que compran una casa está destrozada y nacen nueva te viene el pavo digamos es el chicote el chicote del Hostal te viene ahí el restaurante mira aquí tiene grasa No sabes limpiar tú no tienes ni pajolera idea de lo que has puesto tú de aquí te cambio el menú pim Pam Pam Ya está ya la empresa funcionando ahora el chicote de las finanzas tía Okay okay muy interesante Sí no sé si queda todavía alguna o sea dijiste que el tema que le habían hackeado es presuntamente eso al final Cómo cómo fue era lo de la puerta trasera o realmente lo habían hackeado o era mentira O es que es que aparece como como noticias diferentes de hecho reuters fue el publicó las dos lo que lo que encontré respecto al hackeo por lo que yo Considero que eran cosas diferentes es que en el hackeo se vio que durante semanas se estuvo sacando dinero y luego lo de la puerta trasera eso parece ser que fue un incidente separado Es que aquí sobraba la pasta tío o sea billón por aquí 60 por allá de 300 millones por aquí increíble O sea que yo creo como yo lo he entendido porque me tuve que documentar de varios artículos es que fueron incidentes separados O sea que es que al fin al cabo esto eran 10 chavales en que vivían juntos en esta mansión de Bahamas claro tío tú montar todo esto O sea todo un exchange ya tiene tela tío Porque tú hacerlo seguro ahora sabes y es lo que decía el ceo este que que o sea no había ninguna regulación ni supervisión ni nada o sea claro tío Si tú puedes o sea no sé cómo lo tendrán implementados Pues exchanges digamos hasta día de hoy porque voy a ser precavido hasta día de hoy serios como un crack en un binance joder Supongo que tendrá que ser público el código tendrá que estar auditado por ser parte porque porque es verdad que si tú controlas los exchanges todo lo que te sale ahí de Aunque Bueno teóricamente un banco también lo podría hacer no por eso existe regulaciones Y supongo que cuando están certificados y tal y cual pero claro como con las criptomonedas todavía está muy muy verde todo pues claro Okay y aparecen más están en Bahamas que no se fueron a Bahamas de casualidad Pues para eso para eso dónde tienen los cerditos que están nadando en la playa el tema de Sí sí este también no te pregunta dice Bueno tal Voy a intentar comprarla para salvarla y salvar sus inversores y luego dice que no la compra esto porque eso fue una jugarreta que le hizo un poco para hundirlos más o porque realmente se puso a analizar los documentos y dijo que nada o que se retiraba por eso es una pregunta muy buena que yo mismo me hice sobre el papel Por lo que el tuiteó fue porque vio que aquello era un pifostio y prefirió no meterse ahora perfectamente puede ser el restregarle por la cara el venga sabes como uno se está ahogando le vas a dar la mano y luego te peinas sabes algo así perfectamente me lo creo Oye y para que luego digan con toda la polémica de Twitter pero el poder de un solo tweet nuestras y tanto tío el poder de un solo tuit bueno y yo lo último ya para cuando podemos comprar tus calzoncillos enmarcados Martín tengo que hacer un nft joder me salió así El ejemplo pero a lo mejor tenía que joder la gente va a pensar que es un poco cringe tío le espero unos resultados desagradables queridos oyentes quería hacer un ejemplo y a veces así improvisando pues no me sale los mejores digamos que es lo que lo que pude pensar que menos valor tiene en mí Unos calzoncillos usados está bien está bien se entiende se entiende pues nada muy interesante vamos a ver vamos a ver qué pasa hasta octubre también es otro tema que se van a esperar tanto yo no sé si están esperando hay que analizar todos esos documentos hay tantos documentos si es que no tiene nada no no tiene ningún documento que tienen que tracear un poco las transacciones a ver dónde se fue el dinero y tal o qué pero no sé por qué hasta bueno la casa los temas de palacio van despacio no pero tanto está hasta octubre no sé porque sí a ver bueno los juicios siempre suelen tardar también porque hay que recabar pruebas no para llegar al juicio tienes un tiempo por encima justo lo que dices tú Aquí se han dado pasos de gigante para dificultar cualquier tipo de auditoría de rastreo de chequeo y de regular de exigir regulaciones sabes se ha puesto todas las trabas que se han podido poner

entonces claro me imagino que por eso también lo ponían estaba previsto para octubre Pues ahora Esperamos que ningún oyente esté afectado por esta noticia y nada si si cuando surja algo os lo vamos a comentar de primera línea en tierra de hackers Así que nada muy buena Martín y seguimos para adelante Traigo una noticia que va de la noufly list es una lista que te excluye de vuelos una investigadora de seguridad descubrió a principios de este mes de enero un servidor no protegido que contenía las identidades de cientos de miles de personas de la lista de exclusión aérea que en Estados Unidos se la conoce como no Fly list y es propia del gobierno de Estados Unidos y que es esta lista os preguntaréis queridos oyentes pues tengo que hacer un poquito retroceder y comentar quién la creó Y de dónde viene el centro de detección de terroristas fue establecido por el FBI en 2003 comparte información sobre presuntos terroristas con las diferentes agencias federales departamento de estado departamento de defensa autoridad de seguridad del transporte la que se denomina tsa que si habéis volado a Estados Unidos Pues ahí lo veis en todos los aeropuertos de Estados Unidos en la aduana aduanas y protección fronteriza cbp que también los agentes los veis ahí los que os piden el pasaporte así como algunos socios internacionales Supongo que igual está lista también la comparten con no sé los cinco ojos no en Australia Inglaterra y similares Pues bien la base de datos de detección de terrorismo según el FBI es una lista de personas que está compartida entre departamentos gubernamentales los que he mencionado para evitar el tipo de fallas de inteligencia que ocurrieron sobre todo a raíz del 11 de septiembre del 2001 No ese evento que marcó tanto El antes y el después de Estados Unidos sobre todo de la seguridad nacional Pues dentro de esta base de datos Está la lista de exclusión aérea o no Fly list que es más pequeña y más estrictamente controlada bueno estrictamente controlada un juez decían porque como vemos en esta noticia no es tanto el caso las personas en esta base de datos pueden estar sujetas a ciertas restricciones y recibir una evaluación de seguridad adicional en puntos de control de seguridad como en aeropuertos al volar pero también en otros lugares como al acceder a edificios gubernamentales las personas que se encuentran explícitamente en la lista de exclusión aérea tienen prohibido abordar aviones que despeguen desde Estados Unidos hace tiempo que se realizan estimaciones tanto de la base de datos de detección de terrorismo como de la lista de exclusión aérea y se estimó que la base de datos contenía hasta un millón de entradas y Se informa que la lista de no Fly list es mucho más pequeña en 2014 el grupo de noticias de intercept informó que la lista de exclusión aérea contenía más de 47.000 nombres en un documento oficial publicado el 17 de junio de 2016 el FBI declaró que la nove list contiene 81.000 personas el 1% de las cuales o menos del 1000 personas son personas norteamericanas Así que esas son todas las personas 81.000 personas potenciales que podrían ser terroristas en el mundo me parecen unos cuantos Pero bueno la notoria lista está lista de exclusión aérea es un subconjunto decir que esos son los conocidos porque luego están los que no son conocidos justo también el justo justo Pues esta lista es un subconjunto de la base de datos como digo tiene una base de datos que es para detección de terrorismo pero luego además tienen una que es en plan esta los nombres de esta lista es más pequeña a estos no les dejo volar la de terror y la base de terrorismo en los monitorizó los vigilo online donde sea pero en esta exclusivamente estos no vuelan al menos en Estados Unidos pues se supone que la lista de vigilancias clasificada y solo se otorga acceso a agencias y funcionarios que están autorizados para realizar investigaciones terroristas en el ejercicio de sus funciones inicialmente antes del 2015 esta lista no Playlist era clasificada y solo se otorgaba acceso a agencias y funcionarios que tenían que utilizarla no luego en 2015 Estados Unidos cambió su política y comenzó a informar en privado a las personas que se agregaban a esta lista cualquiera cualquier ciudadano que fuera agregado pues se le notificaba Oye estás en esta lista y con todo el trauma esto que te puede llevar no Aunque las personas de fuera de Estados

Unidos normalmente no saben si están en la lista hasta que intentan abordar un vuelo en Estados Unidos solo se notificaban las personas ciudadanos o residentes en Estados Unidos y esto por qué pues esto fue gracias a la unión de libertades civiles americanas la aclu que es una organización sin ánimos de lucro fundada en 1920 para defender los derechos y libertades individuales de cada persona en Estados Unidos ofrecidos por la Constitución y por las leyes del país Vamos pues este organismo sin ánimo de lucro a favor de los ciudadanos causó presión legal contra el gobierno de Estados Unidos ya desde junio de 2010 cuando pues como digo puso una denuncia legal en nombre de 10 ciudadanos estadounidenses y residentes permanentes que no podían volar hacia o desde Estados Unidos o sobre el espacio aéreo estadounidense porque estaban en esta lista secreta de exclusión aérea del gobierno a estos demandantes nunca se les dijo por qué estaban en la lista ni se les dio una oportunidad razonable para excluirse para justificarse y para salir de ella su incapacidad para volar afectó gravemente sus vidas incluida su capacidad para estar con sus familias ir a la escuela Por ejemplo si ha venido de vacaciones no sea otro país y volvían a Estados Unidos para ir a la escuela o viceversa y también viajar por trabajo a otros países lo que la hace Lu estaba y está combatiendo es el uso de dicha lista secreta de exclusión aérea del gobierno sin el debido proceso ya que las personas son nominadas Y añadidas a esta lista de vigilancia A discreción del gobierno por tanto es se preguntan y están un poco demandando Cuál es el proceso podéis ser transparentes en cómo lo hacéis En qué os basáis Cuál es el criterio que utilizáis para Añadir a estas personas de esta forma actualmente ya no se considera un documento clasificado debido a la cantidad de agencias individuos que necesitan acceder a ella en una declaración a la aclu está organización sin ánimo de lucro G Clayton grig en ese momento director adjunto de operaciones del centro de detección de terroristas dijo que si bien la lista contiene información clasificada de seguridad nacional mantener la base de datos de detección de terrorismo como un sistema sensible pero no clasificado permite agentes de control de la aplicación de la ley utilizar la información de identificación de esta base de datos aunque no posean autorizaciones de seguridad secreta o Ultra secreta que en Estados Unidos se le denomina top Secret que es una categorización que se otorga a personas de muy alto nivel que tienen acceso a secretos muy importantes No pues esta lista Aparentemente se demobionos Se le bajó un poco la prioridad y la importancia y muchos funcionarios podían tener acceso a ella no se Comenta cuantos cuales Pero bueno miles y miles de personas en el gobierno de Estados Unidos claro durante el gobierno de Obama surgió una noticia en 2014 relacionada con el análisis de esta base de datos que se había proporcionado a unos periodistas de de intercept este organismo de noticias ellos concluyeron que de las 680.000 personas en esa base de datos el 40% llegando casi a la mitad de ellas no estaban conectadas con ningún tipo con ningún grupo terrorista conocido y esta cantidad de hecho era superior al número de personas sospechosas de tener vínculos con al-qaeda jamás Y gesbola juntos O sea que el 40% de las personas de esta base de datos no tenían ninguna ningún motivo de estar en esta lista porque no estaban asociadas a ninguna a ningún ningún grupo formalmente declarado como terrorista de nuevo igual habían hecho algo ilícito pero igual no era terrorismo un comentario interesante de un ex Agente Especial senior del FBI es que según comentó literalmente si todo es terrorismo Entonces nada es terrorismo queriendo decir que al ser una lista tan grande pueden haber muchos terroristas O al menos muchos considerados terroristas y esto podría causar problemas en plan identificaciones incorrectas ya sea porque la persona no es realmente un terrorista o porque o por el cansancio causado por las alertas o también se le conoce en inglés como alert fatic cuando tienes a tantos casos de terroristas que los analistas bajan su sensibilidad en la detección y respuesta y dejan pasar pasan desapercibido digamos al terrorista sin darse cuenta este concepto de cansancio causado por las alertas lo traducía así

Un poco yo libremente o alert fatic nos puede pasar o igual nos ha pasado algunos de nosotros y un caso cercano de todo esto es cuando los cibercriminales quieren acceder a nuestras cuentas protegidas por doble factor y envían peticiones de aprobación de login al dispositivo asociado al mecanismo de doble factor Hasta que el usuario cansado de recibir tantas peticiones tantas de la mañana acepta la petición para evitar seguir recibiendo las alertas pues es un poquito lo que Comenta este ex Agente Especial senior del FBI que la lista es tan grande que tiene mucho ruido que es es bastante difícil que sea útil Pero bueno volviendo a la noticia actual ahora que ya sabéis sois expertos en esta base de datos y la no Fly list Pues el descubrimiento actual este fallo fue identificado por una investigadora de seguridad conocida como maya arsón crimeo la investigadora dice que estaba analizando los resultados de zoom hay que es el clon digámoslo así chino de shoudan que shoudan y Por ende sum hay es un Buscador de información de sistemas expuestos en internet como un Google para sistemas o dispositivos iot Ya lo hemos mencionado en otros episodios Así que no voy a entrar en mucho más detalle pero básicamente es puedes buscar en este buscador en plan Quiero buscar los sistemas expuestos a internet que corren Windows y que además tienen expuestos el remote de stop protocol para poderme conectar de forma remota Pues justo estaba revisando los 860.000 resultados que suma y le devolvió a su consulta de servidores jenkins porque era lo que estaba buscando Estos tipos de servidores que son unos una es una plataforma jenkins que ayuda en el proceso de integración continua y desarrollo o despliegue continuo lo que se conoce como si hay CD no en inglés continuos integration continuos Delivery o development y es una plataforma como digo de automatización que ayuda en la creación prueba e implementación de software pues su búsqueda específica fue x-genkins que es una cabecera http que todos los servidores jenkins devuelven por defecto cuando un cliente se conecta a ellos en este caso los clientes eran los servidores de reconocimiento de internet de zoom hay después de solo clicar en 20 servidores en 20 resultados que le devolvió su Mai buscando hay 20 servidores de jenkins interesantes siguientes siguiente pues Aparentemente el servidor número 20 encontró uno administrado por una aerolínea estadounidense llamada commute Air que le permitía acceso anónimo o no protegido o no autorizado digámoslo así básicamente que el acceso no requería credenciales commute Air es una aerolínea Regional de vuelos cortos con sede en Ohio que en junio de 2020 se unió a United Airlines Que supongo que ya está la conoceréis para servir los vuelos United Express banner Así que es una empresa es una aerolínea pequeña pero que está adscrita a una de las mayores empresas de vuelos de Estados Unidos el servidor jenkins de commute Air permitía acceso anónimo o no autenticado a crear espacios de trabajo y a través del abuso de esta funcionalidad la investigadora pudo acceder a los diferentes repositorios a los que jenkins tiene acceso uno de estos espacios de trabajo se llamaba ackars incoming que son las siglas del inglés de aircraft communication Audrey sing en reporting System un sistema de comunicaciones entre las aeronaves y la estación terrestre para conocer el estado de las mismas y permite ofrecer servicios de mantenimiento Sabiendo el momento de la llegada de la aeronave su estado sus averías Y por consiguiente planificar un poquito mejor y optimizar el tiempo en Tierra y las intervenciones a efectuar Pues dentro de este espacio de trabajo se encontraban varios archivos de datos del estado de las aeronaves obviamente y otros de configuración y sobre estos últimos había archivos para entorno de producción entorno de desarrollo y también el entorno este uit user acceptance testing o pruebas de aceptación de usuarios en uno de estos archivos de configuración se encontraban las credenciales para acceder a un servidor sftp de naftech que es una plataforma de agregación y análisis de datos comercializada por airbas que es utilizada por las aerolíneas de nuevo para enviar todos los datos del estado de sus aeronaves a la nube y poder hacer análisis de datos combinarlo con Machine learning y todo eso y un poco predecir si el mantenimiento

que requieren las aeronaves más concretamente los datos expuestos fueron los siguientes el servidor contenía datos de 900 empleados de la empresa esta empresa commute Air que está adscrita a United y esto lo que contenía era números de pasaporte direcciones postales números de teléfono números de las licencias de los pilotos y la fecha de renovación también de la prueba de habilidad de los pilotos que es la que les permite que puedan volar o no de forma legal También aparte de eso contenía credenciales de usuario de más de 40 buckets S3 y servidores de Amazon administrados por commute air no sólo eso sino que además también encontró credenciales y las apis específicas que le podían haber permitido Modificar el repostaje es decir le voy a meter menos gasolina menos queroseno a este a este vuelo y entonces pues no sé Supongo que los pilotos lo verían no antes de despegar Pero sería una buena bromilla anular y actualizar vuelos que eso también podría causar bastante estragos y caos y también intercambiar miembros de la tripulación aparte de esto y el meollo de esta noticia es que estos datos también contenían la base de datos o esta lista relacionada con personas sospechosas de ser terroristas y por lo tanto la novela list el análisis del servidor resultó en el descubrimiento de un archivo de texto llamado nofly.csv una referencia al subconjunto de personas de la base de datos de detección de terrorismo a quienes se les ha prohibido volar porque bueno el estado el gobierno de Estados Unidos piensa que tienen vínculos sospechosos o conocidos con organizaciones terroristas la lista según la investigadora parecía tener más de 1,5 millones de entradas o personas en total los datos incluían nombres y fechas de nacimiento también incluía múltiples alias de las personas es decir otro nombre Pues digamos que pudiera ser Martín pues martinico o yo que sé que Alexis Alex lo que sea no y nombres también o apellidos mal escritos porque Aparentemente a veces cuando se registran en algunos servicios pues ponen su apellido mal a conciencia o sin querer así que el número de personas únicas era mucho menor a los 1,5 millones en la lista había varias figuras notables incluido el traficante de armas ruso recientemente liberado Víctor void junto con más de 16 alias potenciales para él los alias comprendían errores ortográficos como digo antes anteriormente diferentes y comunes de su apellido y otras versiones de su nombre así como diferentes cumpleaños y de hecho gracias a su fecha de nacimiento se pudieron asociar estos 16 diferentes alias con la persona de Víctor void los presuntos miembros del ira la organización paramilitar irlandesa también estaban en la lista otra persona en la lista según la investigadora figuraba como una persona de 8 años de edad según su fecha de nacimiento esto es bastante interesante porque no sé cuántos terroristas declarados hay de 8 años de edad pero bueno es interesante que estuviera una persona de 8 años de edad en esa lista muchas entradas de la lista eran también nombres que parecían ser descendientes de árabes o del medio oriente aunque también estaban en la lista nombres que suenan a hispanos y anglicanos o ingleses el análisis demostró que la gran mayoría de la lista contenía personas con nombres asociados bueno con árabes o rusos commute Air la empresa afectada dijo que la infraestructura expuesta que describió como un servidor de desarrollo se usaba con fines de prueba y también dijo que el servidor que se desconectó antes de la publicación de la noticia no expuso ninguna información de clientes según una investigación interna que estaban lanzando en ese momento commuter también confirmó la legitimidad de los datos afirmando que realmente sí era una novelist y pero que era una versión de aproximadamente Hace cuatro años del 2019 que incluía nombres y apellidos y fechas de nacimiento y también que habían enviado una notificación a de seguridad de infraestructura y ciberseguridad la cisa y que continuaban con una investigación completa Así que realmente la investigadora se había apoderado de la atmósferalist Aunque está un poco desactualizada desde 2019 no 4 años para atrás pero bueno Yo supongo que si eres un terrorista el tema es que la lista está normalmente y voy a mencionarlo en otro caso en el pasado más adelante pero en la lista también tiene atributos

adicionales digámoslo y uno de ellos es un flac que te dice que si puedes volar o no Así que si ya te han pillado alguna vez como terrorista estás en la base de datos Y si no te dejan volar pues Incluso te añaden en esta lista pero si no te dejan volar o si te dejan volar si Cambia tu estado de puede volar o no igualmente te siguen manteniendo en esta lista Así que no sé cuándo la lista disminuye es una lista que supuestamente solo se dedica a hacerse grande lo interesante es que cuando este esta investigadora descubrió los datos expuestos fue justo no sé si lo habéis visto en las noticias queridos oyentes pero hubo una noticia hubo un pequeño caos que afectaba bueno pequeño digo igual porque no me afectó pero si hubiera estado en el meollo hubiera estado un poquito hubiera dicho que era un caos mayor hubo un incidente que afectaba aerolíneas en Estados Unidos con 11.000 vuelos retrasados y 1300 anulaciones aunque como comenta la investigadora no se debe a sus acciones y de hecho según noticias publicadas más tarde el impacto aerolíneas estadounidenses se produjo cuando un empleado externo borró de forma No intencionada pues eso dice archivos de la base de datos que gestionan los vuelos que se llama nothies to Air missions de los servidores de la administración de Aviación Federal estadounidense la a de hecho la investigadora descubrió los datos expuestos el 6 de enero y el impacto a las aerolíneas tuvo lugar el 11 del mismo mes cinco días después así que en principio no están relacionados la tsa dijo que estaba al tanto de un posible incidente de seguridad cibernética con commute Air y que estaban investigando en coordinación con sus socios federales el FBI se negó en rotundo a responder a preguntas específicas sobre la fuga de información de la noufly list y como he dicho no es la primera vez que se publica un incidente relacionado con la fuga de información de esta lista de hecho en el 19 de julio de 2021 el investigador de seguridad voló demir díachenko También conocido como Bob para los amigos encontró una copia detallada de la lista de vigilancia del terrorismo esta novelis con 1,9 millones de entradas y de forma similar a la investigadora encontró el cluster de distintos servidores de Plastic Search expuesto a través de búsquedas de sensis y zoom eye O sea que de nuevo de la misma forma buscando en buscadores de sistemas encontró este esta base de datos expuesta también elastic Search digamos lo que es un servidor que agrega y permite analizar datos el investigador en este caso informó al departamento de seguridad nacional el mismo día que lo descubrió y el servidor expuesto se eliminó unas tres semanas después el investigador un poco se quedó preguntando por qué se tardó tanto tiempo en eliminar tres semanas Cuánto tarda en desconectar a un servidor de internet de este tipo con esta información tan crítica Pero bueno y tampoco pudieron confirmar si algún otro usuario con Malas intenciones pudo acceder a esta información cada registro en esta lista contenía más información que la que la investigadora actual pudo obtener en la lista que este investigador obtuvo en 2021 los datos contenían nombre completo El identificador de la lista de seguimiento de terrorista la ciudadanía el sexo fecha de nacimiento número pasaporte país de emisión del pasaporte y como he dicho antes un indicador de prohibición de vuelo en plan estás en la lista o qué Pero puedes volar o no Porque se podría permitir que pudieras volar Aunque fueras un terrorista por algún motivo algo muy interesante es que la base de datos se encontró en una dirección IP de barraine no en una dirección IP que estuviera ubicada en Estados Unidos eso sí que flipo porque esto es información muy confidencial que al fin y al cabo tienes listas de terroristas ahí con nombres y datos Sí la verdad es que no comentan exactamente qué hacía en esa y esta noticia es de 2021 Así que no no encontré mucha más pero si eso parece muy interesante no sé si es que igual había algún grupo de Estados Unidos FBI que estaba desplegado en barrain y tenía un servidor ahí en plan Shadow Haití que habían desplegado ahí lo habían expuesto a internet sin querer o el servidor en la nube era el más barato y ya está Pues un mini análisis que hizo este investigador de los ciudadanos la ciudadanía de de estas de esta lista comentaba que habían muy curioso sólo cinco ciudadanos

americanos estados estadounidenses en esta lista 19 de Inglaterra 778 de Brasil 1871 de Holanda 11.019 de Bélgica y unos 16.000 de Francia Así que Aparentemente hay muchos terroristas en Francia y muy pocos en Estados Unidos Bueno no sé De todas formas hasta el 1,9 millones de entradas Ahí hay muchas más así que de nuevo probablemente en esto es 1,9 millones de entradas habían muchos alias en el caso anterior este este esta persona que vendía armas esta persona rusa pues tenía 16 diferentes alias así que bueno puede ser que sea un tema similar Pero bueno no menciona todas las otras nacionalidades pero también habría muchas quiero comentar un poquito Cómo afecta esta la fuga de información de esta no Fly list a ciudadanos a cualquier persona como tú o como yo querido oyente pues la lista de vigilancia de terroristas está formada como digo por personas sospechosas de terrorismo pero que no necesariamente han sido acusadas de ningún delito en las manos equivocadas está lista podría utilizarse para oprimir hostigar o perseguir a personas de esta lista y a sus familias extorsionar y similar no ha habido varios informes de autoridades estadounidenses que reclutan informantes a cambio de mantener sus nombres fuera de la lista de exclusión aérea las identidades de algunos informantes pasados o presentes podrían haberse filtrado y esto obviamente podría hacer que su vida ahora mismo fuera mucho más difícil también podría causar una serie de problemas personales y profesionales a personas inocentes cuyos nombres están incluidos en la lista como he dicho anteriormente por algún motivo u otro la forma en que añaden personas de esta lista no es muy transparente así que no se sabe a ciencia cierta cómo lo hace no y en qué criterio se basan el director del proyecto de seguridad Nacional de está la aclu la organización sinónimo de lucro a favor de los ciudadanos no de Estados Unidos estadounidenses mencionaba que Estados Unidos tiene un sistema de listas de vigilancia masivo e inflado que puede estigmatizar a las personas incluido los estadounidenses como terroristas conocidos o sospechosos en función de estándares secretos y evidencia secreta sin un proceso significativo para desafiar el error del gobierno y limpiar sus nombres las categorías de personas en la lista de vigilancia parecen expandirse y nunca restringirse las consecuencias son significativas y tienen daños reales para la vida de las personas existe el estigma la vergüenza y las dificultades de no poder volar en nuestra era moderna de ser señalados de ser buscados y han tenido casos de esas pobres madres y padres estigmatizados y avergonzados frente de sus hijos en los aeropuertos cuando los han tenido que mover a un lado para decirles Oye estás en una lista terrorista tenemos que hacerte unas preguntas tenemos que tocarte más no analizar todo lo que llevas y bueno algunos miembros del Congreso de Estados Unidos han propuesto prohibir la venta de armas de fuego a personas en la lista de exclusión aérea Así que si estás en esta lista y te interesa comprar algún tipo de arma y vas a un establecimiento que las vende de forma legal Pues tampoco podrías por estar en esta lista tiene pinta de que esta lista al ser antigua y no actualizada y me refiero a la identificada este mes por esta investigadora no se está utilizando sin embargo en el hipotético caso de que la investigadora no lo comenta Pero y si la lista se estuviera utilizando y hubiera podido modificarla pues esto hubiera podido permitir a guasones hacer bromas de mal gusto a cualquier persona añadiéndolas y denegando las el acceso a volar aunque esto se lo hubiera me parece bastante amable por tu parte llevarle guasones yo les llamaría hijos de mala madre Sí es que digo a ver qué palabra puedo usar que no he usado antes sí guasones básicamente meto en la lista que te identifica como un terrorista el gobierno de los Estados Unidos jijiji Jajaja tengo risas es una es una muy mala broma y esa persona debería también ir a prisión un ratito pero bueno sí sí aunque Bueno si Hubieran hecho eso el impacto hubiera sido no tan malo porque esto sólo hubiera afectado abuelos operados por commute Air los de United Express banner y potencialmente igual a cualquiera de United Airlines si esta lista el notefly.csv también lo estuvieron utilizando a nivel de empresa madre y United Airlines no sin embargo lo que los

guasones o digamos cibercriminales no hubieran podido hacer es modificar dicha lista la que está controlada a nivel del FBI y saltarse las comprobaciones de aduanas ya que como digo esta Lista pues en el caso de commute Air le viene dada desde el FBI no es algo que commute propague de vuelta al FBI O sea la lista madre la tiene de FBI y en este caso no se dio al menos no sabemos que alguien haya podido comprometer esta lista en los servidores del FBI y con todo esto ahí queda la noticia el riesgo y bueno los problemas para los que estén en esa lista y llegamos queridos oyentes a la pregunta del episodio es un hueso Estás de acuerdo Sí sí Qué palabra te parece más apropiada para denominar a estas personas no la pregunta realmente queridos oyentes fuera Guasa es estás de acuerdo con que el gobierno de Estados Unidos comunique a las personas de que se ha añadido su nombre a la nove list recordemos que al menos se comenta la noticia que para los las personas ciudadanas o residentes en Estados Unidos se les notifica pero no a las que están fuera así que estarías de acuerdo con que el gobierno de Estados Unidos comunique a estas personas que se les ha añadido a la novelalist tenemos cuatro opciones la primera es no confío en el gobierno no hace falta que se comunique a nadie con esto me refiero a que Confío en su criterio y si dicen que una persona es terrorista pues me lo creo no porque avisaría terroristas le estás diciendo que que es un terrorista Entonces aunque seamos honestos los que son terroristas y ya lo saben así que bueno pero claro voy a pillar un avión a Estados Unidos y estoy en el Note list me entero cuando ya llego a Estados Unidos y por tanto me puedo meter en la cárcel o me entero antes de coger el avión entonces da igual no lo comentan pero directamente comentaban que no te permitían abordar vuelos en Estados Unidos pero el caso ese que se ha mencionado de la aclu estaban luchando porque esas diez personas que están representando no pudieron ni despegar ni aterrizar ni Volar Sobre espacio estadounidense Así que no he conseguido saber exactamente Cuál de esos tres casos podría ser pero asumamos que son todos Así que si cuando vas a despegar de de tu país de origen dirección Estados Unidos probablemente te avisen igual como tú dices Martín te puedes escapar porque estás ahí no Y aunque no lo sé si te vendrían a restar tipo caso Sam de ftx y para extraditarte a Estados Unidos la tercera respuesta sería sí para evitar el trauma y por favor avisa a estas personas que están en offline Así que cuando van Ya están preparados no de que no les van a dejar volar o no van a volar o yo que sé O al menos puede intentar luchar contra esto con la esta organización sin ánimos de lucro y finalmente tenemos la respuesta sí queremos total transparencia pues súper interesante Esto del Note flyst yo lo recuerdo que la primera vez que lo escuché fue porque Obama se quejaba había hecho unas declaraciones que lo único que podía hacer en contra de terroristas era añadirles a no Flights y iba un poco en torno a el tema de las revelaciones de snowden y de tal que poco para justificarse pero sí desde luego es un mecanismo interesante Pues en relaciones Así estuve me estuve documentando y justo decían que la lista creció un montón gracias al gobierno de Obama y que se añadían 900 personas o al menos bueno 900 900 entradas recordemos que hay alias no pero 900 entradas cada día durante el gobierno de Obama Así que son bastantes personas ostras llegaría a lo mejor llega el día en que las aerolíneas empiezan a quejarse en playa Oye párate que al final perdón sabes de un plan de que opera en Aunque Bueno claro sería solo para Estados Unidos pero bueno sí que aún así sabes hay muchas aerolíneas árabes que vuelan a territorio estadounidense a decir Oye Pancho que medio país me lo tienes en la lista Sí sí habría Que supongo que tienen ahí un gol de logs no un un Rango en en plan vamos a como mucho esta lista puede tener dos millones de personas porque si no luego como tú dices luego es lo que dices tú no que además esa opción quiero pensar que el gobierno sabe decide bien a quién está poniendo ahí quiero pensar Pero bueno a saber queremos pensar claro sabemos Cuál es el baremo no a lo mejor el baremos que has hecho una búsqueda en Google de algo un poco cuestionable pum te meto ya porque

claro meterte en el Note realmente no es algo tan agresivo no es que te metan en guantánamo o te vas a ir a juicio te detengan o tal Entonces a lo mejor precisamente el problema de esto es como que en principio es una medida bastante suave a pesar de que tiene un impacto importante y estás en una lista compartida con terroristas de verdad O sea pues claro Habría que ver cuál es el baremo Sí y el tema es no comentan Y supongo que no se hace pero en Estados Unidos no que te hacen un background check cuando un análisis de tu pasado no y pasado criminal también cuando vas a buscar trabajo Yo creo que esto Esto no sé no se expone no a los a los empleadores que te van a contratar Pero al menos el trauma de cuando vas y no te dejan volar y que no te dicen porque no te lo dicen por qué no te dejan volar te dicen que estás en la lista y que no te dejan volar OK Por qué no no te lo podemos decir pues Vaya pues claro entiendo que si te lo dicen y no he encontrado todavía Las pistas que te incumben Pues claro te están acusando de algo vas a borrarlas no te va a decir porque eres un terrorista bueno perdone sido juzgado ni condenado ni nada O sea me habéis añadido claro no me dejáis volar ahí que el equivalente puede ser perfectamente no te doy el visado para venir a Estados Unidos que eso es lo curioso también no porque joder cuando tú para entrar en Estados Unidos todo el mundo necesita un visado aunque sea temporal bueno de Canadá y tal Quizá no pero bueno que se me entiende Entonces ya está Sí la verdad que sí Igual no te dan el visado como dices o no sé igual quieren arrestarte cuando llegues aquí y sí que te dan el visado te dejan volar No sé no en principio no te dejan volar pero Claro porque si no ya no sería no no vente vente eso es como cuando quieres extraditar a alguien pasaje gratis lista de señuelo Sí sí luz listo Sí sí muy buena pues queridos oyentes hasta aquí Hemos llegado recordad que vamos de estar pendientes en Twitter que vamos a lanzar ese ese primer sorteo para entradas para el Barcelona Cyborg Security Kong donde voy a estar ahí de anunciando todas las charlas y todo esto para que os pueda conocer venís a saludar va a estar muy guapo no faltéis si estáis por aquí por Barcelona o tenéis ocasión de venir hasta aquí y nada Muchísimas gracias por quedaros hasta el final esperemos que os haya gustado Y sobre todo también gracias por seguir compartiendo el podcast con toda la gente que que podéis y que queréis y que queréis ayudar a apasionarse por la ciberseguridad como nosotros recordad también dejarnos esas reviews en donde nos estés escuchando cinco estrellitas y así crees que lo merecemos que nos ayuda un montón Sí muchas gracias a todos como siempre por escucharnos por seguirnos por darnos like comentarios y por seguirnos en estos 80 episodios ya señores y señoras nos vemos en el 81 Adiós adiós hasta luego chao si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers