nueva campaña de espionaje detectada que afecta países latinoamericanos a cargo de un grupo de ciberdelincuentes conocido como Dark caracal un estudio analiza los datos de sesiones del juego bitsaver de meta Quest 2 y consigue desanonimizar a usuarios en el metaverso gracias a sus movimientos de cabeza y manos otro episodio más para los anales de la historia de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 20 de marzo de 2023 este es el episodio número 87 yo soy Martín vigo y está conmigo el Cyborg mitad humano mitad máquina Alexis porros Hola Alexis qué tal Muy bien Martín aquí más me gustaría pensar más humano que máquina Aunque como dices después de ayer la verdad que estoy un poco sorprendido porque como te comentaba un poquito antes lo que hacemos no antes de cada episodio nos charlamos aquí Martín y yo qué cómo te va y tal pues le comentaba que ayer fui a un evento en Connecticut Aquí el estado norte de Nueva York una competición de robots en la que dos robots luchaban durante tres minutos para destruir al otro y en algunos casos alguno de estos robots tenían incluso típico jet de combate de estos de motor de estos de jets de combate a escala pero sacando fuego fue bastante interesante Qué guapo de hecho el tema habían como 200 robots y el tema iba desde las 9 de la mañana hasta las 2 de la noche no me quedé hasta tan tarde pero fue fue interesante Cómo le Mola Los Americanos todo lo que tiene que ver así eso en plan también los los Monster trucks estos los coches enormes todos los el door Este lo de los coches estos que están como medios cacharrados y se tienen que reventar unos a otros aquí los robots con fuego tal Sí sí los Mola mucho eso usa baby muy espectacular pues vamos a temas más importantes como siempre Gracias queridos oyentes por apoyarnos en todas las redes sociales online en discord ya sabéis dónde nos podéis encontrar en redes sociales nos podéis Buscar como @tierra de hackers o simplemente tierra de hackers linkedin YouTube Twitch todos esos ya lo sabéis en discord igual no muy difícil pero algo más de requisito es que tenéis que ir a tierra de hackers barra discord y bueno lo de las plataformas de podcast ya sabéis estamos en todas y si no estáis suscritos todavía Ya y ahora mismo a suscribiros y finalmente agradecer como siempre el apoyo a la pregunta del episodio que publicamos en Twitter después de publicar cada episodio y la anterior la última pregunta fue la siguiente siguiendo la línea de mentalidad hacker de los soldados ucranianos con la modificación de los drones Dj eye para su uso en combate en la guerra que otros dispositivos electrónicos comerciales crees que podrían ser los siguientes que se pudieran reutilizar para convertirlos en armas os dimos cuatro opciones la más votada son los coches autónomos como decíamos puede ser tesla o utilizando el coma de jojot con un 48%, la sigue robots móviles con un 24% seguida En tercer lugar por globos aerostáticos con un 20% y finalmente los submarinos teledirigidos con un 8% que yo creo que serían mis favoritos son son muy divertidos desde luego que sí yo como siempre agradecer a nuestros amigos de patreon que nos apoyan y a nuestro 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 focalizada en dar respuesta tres Pilares principales prevención detección y respuesta cubren servicios ofensivos como retín pentesting auditoría de código y mucho más también dando servicios gestionados de monitorización Avanzada respuesta ante 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 vistetes web en a3sek.com y rápidamente también darle las gracias a brawler Pro por apoyarnos el podcast la herramienta más completa de seguridad de la WS empresas de todos los tamaños se apoyan diariamente en prawler pro para que sus equipos puedan confiar en su modelo de seguridad de aws 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 también visión completa de tu infraestructura en todas las regiones de WS y tendrás todos los resultados en apenas unos minutos empieza a usar plau y beneficiarte de sus resultados visitando tierra de hackers.com/pruer proprowllrpro muy bien y justo antes de empezar mi noticia solo comentar que así como tierra de hackers estuvo ayudando a montar la Barcelona Cyber Security ahora Estamos ayudando a montar visates Barcelona tierra de hacker sigue ahí a divulgando y apoyando en todos los eventos y cosas que podamos apoyar Así que visage Barcelona va a ser el 8 y 9 de junio aquí en Barcelona en el campus de La Salle tenemos el Cold papers abiertos y también Estamos buscando sponsors para ayudar a montar la mejor conferencia del mundo mundial así que ya sabéis ir a la web Barcelona punto Perdón visage punto Barcelona vsides punto Barcelona que tenéis el Cold for papers abierto y pronto pondremos las entradas a la venta entramos con la noticia hoy os traigo algo que también nos comentasteis cuándo os pedíamos feedback cubrir más apts ya sabéis grupos de ciberdelincuentes con capacidades muy avanzadas y que en ocasiones operan bajo las órdenes de los gobiernos de sus países correspondientes pues me he encontrado un informe muy interesante que hace un par de semanas de hace un par de semanas de la organización sin ánimo de lucro electronic Frontier foundation esta que nos gusta tanto y va sobre un apt apodado Dark caracal Y por qué os traigo a este apt Bueno pues porque su última campaña y sobre la que va el informe del ff O sea la electrónica Frontier foundation Es sobre ciberespionaje una cosa que nos encanta aquí cubrir pero es que además centrado en países latinoamericanos tenemos miles miles de oyentes en prácticamente todos los países latinoamericanos y no nos olvidamos de vosotros hermanos Así que aquí vamos con el tema y estar muy atentos dar caracal es un grupo de ciberdelincuentes que lleva ya bastantes años operando me encontré de hecho un informe de la empresa lockout de 2018 y que os dejo por supuesto las notas del episodio donde desgrana n muy bien las actividades y tácticas y técnicas y procedimientos de este apt y ya apuntan de aquella a que se dedicaban a ciberespionaje a escala no solo look out documentó los detalles y crímenes de este grupo sino que ese set también tiene un extenso reporte este de 2021 más actual que detalla las herramientas y malware que utiliza este grupo este informe también lo tenéis en las notas del episodio y ya se habla aquí de una campaña de ciberespionaje masivo que afecta a Venezuela mayormente ya sabéis Cómo es esto de nombrar a grupos de ciberdelincuentes que cada empresa pues le pone su nombre no así que no sorprendáis de que en el informe concreto de sset hablen de bandidos que es el nombre que ellos le pusieron pero vamos que es el mismo que dark caracal en esta campaña de espionaje contra Venezuela este grupo utilizó un antiguo malware que Data ya de 2005 llamado banduck has oído hablar de ese Alexis de bandook pues no no me suena pero vaya nombres que se utilizan sí no y yo tampoco lo conocía pero me sorprende que sea ya de 2005 pues parece ser que el malware no fue desarrollado por ellos sino que por desarrolladores contratados específicamente para este propósito ese set en 2021 cuando empezó a seguir el rastro de strego grupo encontró que unas 200 máquinas habían sido infectadas mayormente en Venezuela como decía estas máquinas eran parte de la infraestructura de empresas de construcción hospitales empresas de venta al por mayor y servicios de desarrollo de software el objetivo principal era el espionaje a estas objetivos y víctimas en concreto 200 máquinas infectadas no parece mucho pero recordemos que esta es una campaña de espionaje a medida diseñada específicamente con un propósito en mente No es simplemente digamos infectar ordenadores a tutiplén no Cuantos más mejor para crear una botnet y bueno sí a lo mejor te centras en un país pero bueno no no no esto Aunque parezca poco 200 máquinas es porque son 200 máquinas específicas que querían infectar y por eso no es coincidencia que todas las máquinas infectadas eran parte de una empresa u organización y no de ordenadores personales de gente Pues como tú y como yo querido oyente la técnica de

infección eran emails falsos específicamente diseñados para el objetivo para así maximizar digamos la posibilidades de que ejecutasen el malware que venía incluido los emails el spier fishing de manual el email era un PDF que venía diseñado de tal manera que se veía la contraseña 123456 y se indicaba que había que hacer clic para verlo al hacer clic esto hacía que se descargase un archivo comprimido de internet que contenía un ejecutable para Windows el cual era lo que se conoce como el dropper en el mundo del malware que una vez ejecutado instalaba el famoso malware baduo Es decir para los menos técnicos te llega un mail que te cuenta la película de que tienes que poner una contraseña que es 123456 que el PDF está cifrado y que tienes que hacer clic y al hacer clic se descarga un malware de internet baduc se inyecta se inyecta en el proceso de Internet Explorer por tanto Aquí vemos que el objetivo específicamente las máquinas de Windows no funcionaban un Linux o un mac y contactaba con el command en control los que son los servidores de los atacantes para notificar que la máquina ha sido infectada y se queda a la espera de instrucciones me fijé en el tipo de direcciones o urls que usaban y desde luego se puede ver que estaba orientado a infectar negocios y de hecho también está en castellano insisto porque se centrarán en países latinoamericanos por ejemplo uno de los dominios era beatly barra lista de precios 2 bitly ya sabemos que es uno de esos acortadores de direcciones para que parezca menos sospechoso O también por ejemplo re brandt.li barra información bonos productividad o rebrand.ly barra Perdón file dn.com/h lista de precios punto rar o adn.com/facturas ya vemos aquí que las urls siempre hacen como referencia que hay un contenido interesante Pues de facturas de listas de precios de informes de bonos de productividad todo esto un poco para no solo dar credibilidad sino despertar la curiosidad de la persona que acaba de recibir el email una vez infectado este malware permite recibir hasta 132 instrucciones diferentes entre las cuales incluye leer cambiar borrar o renombrar archivos hacer capturas de pantalla controlar el ratón Cerrar aplicaciones por ejemplo muy útil pues para desactivar el antivirus si lo tiene instalado el objetivo desinstalar el malware esto sería pues autodestrucción no si tú ya roba auto lo que querías pues quieres eliminar pruebas y aquí así nunca ha pasado nada ejecutar todo tipo de archivos incluso los puntos har o punto pyc que es para archivos programas escritos en Java o en python obtener información de redes wi-fi esto quizá era para geolocalizar a la víctima controlar la webcam esto es uno grande grabar el sonido a través del micrófono y por supuesto ejecutar programas maliciosos todo esto era parte de los 132 comandos que soportaba este malware que podían enviar los atacantes para ejecutarse en la máquina víctima evidentemente os dejo el informe de ST en las notas del episodio para que podáis leer todos los datos técnicos especialmente Los indicadores de compromiso curiosamente buscando más sobre este grupo me encontré una charla de Black hat de 2016 titulada whenberg States sponsor malware attacks Again activist loyers en journals viene de hacer algo así como cuando quien ataca es el gobierno ataques ataques basados en malware exponsorizados por gobiernos contra abogados y periodistas activistas Pues esta charla de hecho fue dada por los mismos miembros del ff y resulta que en su día atribuyeron esta campaña de espionaje a abogados y periodistas disidentes de kazajistán y Líbano a un grupo desconocido de ciberdelincuentes pero resulta que ahora se han dado cuenta Gracias se acusaban las mismas tácticas técnicas y procedimientos que dar caracal eran realidad quien estaba detrás de esto ese grupo desconocido en 2016 para estos investigadores a día de hoy en 2023 se dieron cuenta que es el mismo que están Mirando por tanto entre los informes de ese set los informes de lucaut la investigación del ff en 2016 y la actividad reciente contra países latinoamericanos llegan a la conclusión de que Dark caracal es un grupo de ciberdelincuentes a las órdenes de quien más les pague es decir el famoso hacker no parece tanto que trabajen para una nación específica debido a sus objetivos en países tan diferentes Durante los años sino que es un grupo que se

puede digamos contratar para que espían y hackeen infraestructura de países o personas consideradas enemigos de quienes quiere que sean sus clientes no os dejo un link a la charla de Black hat porque a mí la verdad me resultó súper interesante y llegados a este punto Qué hay de novedoso en todo esto Al fin y al cabo en tierra de hackers nos centramos en traeros la actualidad pues como decía al principio ff ha vuelto a toparse con este grupo operando en países latinoamericanos a día de hoy hay 700 ordenadores infectados repartidos por países de Centroamérica y Sudamérica y mencionan que la mayoría de infecciones están presentes una vez más en Venezuela pero más aún en República Dominicana Y por qué tienen información tan precisa sobre la actividad de este grupo pues es uno de hecho de los detalles curiosos de esta noticia consiguieron una nueva muestra del malware que están utilizando y se dieron cuenta de que desde el informe de ese de 2021 que os contaba antes el malware que usan baduc ha sido actualizado y ahora soporta 148 comandos en vez de los 132 que mencionaba el set en 2021 esto quiere decir No solo que el software malicioso está siendo actualizado a día de hoy sino que el grupo sigue muy activo su coman en control se halla bajo El dominio de a proof puntoru de Rusia pero lo curioso viene de que tienen un dominio secundario por si el primero falla que es Aunque el sol punto com y es aquí donde viene los datos curiosos ya que los investigadores del ff hallaron este dominio Aunque el show.com al hacerle ingeniería inversa a la muestra del malware que les había llegado y cuando fueron a verificar que había detrás de este dominio se dieron cuenta que nadie lo había registrado Aún es decir un dominio que el malware estaba enviando información todavía los malhechores no lo habían registrado pues Qué hizo el ff en esta situación pues evidentemente registrarlo inmediatamente empezaron a ver cómo ordenadores infectados por todo latinoamérica empezaban a contactar con su servidor después de asignarle al dominio inexistente y o sea después de asignarle a sus servidores El dominio inexistente y gracias a esto supieron que actualmente hay una campaña de espionaje en estos países que es de lo que va esta noticia otra curiosidad es que el mismo día que asignaron los dns para apuntar a sus servidores otros seis dominios desconocidos inmediatamente asignaron el mismo dns por lo que también empezaron a ver ese tráfico y esos dominios eran sets con doses punto com Second save.com scan Lost con dos test.com sanes City email secure link.com y godaddy punto com con varias aps aquí por ejemplo vemos godaddy es probablemente el Hosting Provider más popular de Estados Unidos el tema este de email secure link está claro que es el típico que te mandan en un email y es en plan no vete a este link para que puedas verlo de manera segura lo que sea y en realidad es malware total a los tres días varios de los dominios se cambiaron de nuevo a otra pero varios de ellos siguieron apuntando a la ff es decir solo va solo digamos que los ciberdelincuentes solo corrigieron varios de estos dominios para que el ff no pudiera seguir viendo el tráfico la verdad es que muy raro todo y ellos mismos reconocen que no entienden bien la utilidad de estos nuevos dominios adicionales porque no tenían nada que ver con esa campaña Ah Martín esto esto de los dominios me recuerda al tema del ransomware wanna Cry que igual algunos de nuestros oyentes lo han luchado de este personaje llamado malware Tech online su nombre real Marcus hatchings creo que lo estoy pronunciando bien que en su época cuando salió wanna Cry se dedicaba bueno en sus orígenes este este esta persona se dedicaba a crear malware luego se vino al lado del bien y se dedicaba a analizar malware Y en este caso se puso a mirar ranso muere de wanna Cry y encontró algo parecido a lo que tú comentas creo si no algo muy similar y que él lo llamó Kill switch no que había también se comunicaba con un dominio en especial en específico y no estaba registrado a nadie entonces en lo que hizo fue registrarlo Y de alguna forma desactivar el malware enviándole un comando para que digamos se desinstale o se desactive o se destruya Sí muy buen apunte aquí sabes cuál es la diferencia interesante A ver que en el caso de en el caso de wanna Cry no estaba registrado a propósito porque como tú

bien explicas era un Kill switch Si alguien lo registraba automáticamente la campaña de ransomware se paralizaba en este caso era un dominio secundario que cuando el primero fallaba pues tenían ese entonces fue como que lo desarrollaron registraron el primero como que medio Se olvidaron que tenían unos segundos por si acaso y nunca lo llegaron a registrar sabes es ahí yo creo que fue más un despiste que otra cosa faily obsek no lo que siempre decimos sí Y además Fíjate que en cuanto lo hicieron otros seis nuevos dominios como decía empezaron a apuntar a ese también que parece como el malware estaba o el Cómo en control de manera que si se registraba un secundario automáticamente se ponían nuevos nuevos secundarios no por eso esos otros empezaron a apuntar a este Entonces a lo mejor por eso no lo registran en plan Oye si algún día nos paralizan El dominio principal registramos unos segundos que ya está jarcodeado en el malware y automáticamente tenemos un sistema que ya registra nuevos y empieza a apuntar a lo mismo algo así no sé pero desde luego le salió el turbo por la culata total que a los tres no sé dónde me había quedado vamos lo que venía a decir es eso que es que me quedé volado no muy buen apunte por lo de lo de wanna Cry Pues a eso que decía que le bebe el eff no vio que estos nuevos dominios tuviese nada que ver con esta campaña de espionaje en Latinoamérica en concreto Así que es posible ellos especulan que pertenecía a una campaña de espionaje diferente que este grupo estaba llevando a cabo en otros países Este no es el único cambio que hicieron los delincuentes tras El ff hacerse con El dominio Aunque el show punto cambiaron el command en control a otros dominios específicamente cadden power.com y gómez.rum pero recordad que El dominio que tiene ff es usado como secundario por lo que a pesar de que estos de estos cambios a día de hoy a día de hoy siguen viendo toda la actividad de los ordenadores infectados Parece ser que los deber delincuentes no se han dado cuenta de este detalle o a lo mejor pues como está jarcodeado o digamos está ya puesta esa dirección en el propio malware de los ordenadores infectados pues no lo pueden cambiar Aunque sí por lo que vimos en los comandos a lo mejor no quieren no sabemos otro dato curioso es que gracias a que el malware hace que los ordenadores infectados se conecten a los servidores de los ciberdelincuentes cada tres horas para ver si hay instrucciones nuevas Efe se dio cuenta que la actividad de los ordenadores infectados disminuye drásticamente los fines de semana y Durante los días de vacaciones en los países correspondientes esto qué quiere decir pues una vez más que han infectado ordenadores de empresas ya que los ordenadores están encendidos durante las jornadas laborales y durante las horas laborales así que ya sabéis un apt a sueldo que está contratado para campañas de espionaje a empresas y entidades que de un país concretas de un país y que actualmente está operativo en varios países latinoamericanos Así que mucho cuidado queridos oyentes sobre todo si trabajáis en infraestructura crítica o empresas muy potentes muy interesante Martín Y supongo que en las notas del episodio vas a poner los enlaces de esto sobre todo los indicadores de compromiso para que nuestros oyentes puedan mirar si si tienen algo de ello por ahí en su red o qué pasa muy bien tú siempre Alexis Alba guardando que no solo nos dediquemos a educar a la gente y entretenerla sino también que haya y action items al final y efectivamente ponemos Los indicadores de compromiso os dejo cuatro enlaces en concreto varios a varios reportes el del actual de 2018 también el a la charla de Black hat pero si tenéis también todos estos reportes Los indicadores de compromiso y los ttps Y luego dices que el ff está viendo un poco todavía a día de hoy está viendo las comunicaciones con algunos de esos dominios no del malware está infectado me pregunto si si trabaja en plan vigilante y les ha comunicado algo a las empresas infectadas o un poquito muy buen apunte lo que dicen en el informe de ellos es que lo caparon o sea dejaron de recolectar información a partir del 800 de los 800 ordenadores para preservar la privacidad de la gente infectada es decir cuando llegaron a 800 ordenadores ellos consideraron que tenían suficiente información para investigar a este

grupo entonces dejaron de recolectar esa información creo que lo que hacían era mandarlo a de null o algo así que esto quiere decir que básicamente la información que entraba se borraba automáticamente que eso Pues mira Está muy bien solo recolectar un lo mínimo que les permitió pues averiguar quién está detrás Cuáles eran los ttps los indicadores de compromiso Dónde está centrada la campaña y me imagino que están trabajando pues con las autoridades Ah o sea que creemos que que están trabajando intentando notificar a las empresas bueno han puesto este reporte público quiero pensar que no solo se han dedicado a esto en general el sí que intenta presionar y bueno Esto se trata de ciberdelincuentes quiero pensar que que sí no que han puesto esta información también en manos de de pues las entidades competentes no sé quiénes serán pero sí sí no está bien está bien pues nada ya sabes queridos oyentes leer los artículos que he puesto Martín en la web y Esperamos que ninguno estéis afectados esperemos que no pues continuamos para bingo después de haber cantado línea con la noticia de Martín y antes de pasar al premio quería comentar y dar las gracias a monat otro de nuestros patrocinadores 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.commond.com y le podéis mandar vuestro currículum a la dirección tierra de hackers@monat.com y nada Ahora sí ya vamos al premio que es la siguiente noticia del episodio y lo que traigo Es una nueva investigación del centro de inteligencia descentralizado responsable de la Universidad de Berkeley en California que revela que por defecto los usuarios del metaverso no van a disfrutar de privacidad a no ser que se apliquen nuevas medidas de seguridad innovadoras el estudio involucró el mayor conjunto de datos de interacciones de usuarios en realidad virtual que jamás se haya analizado en busca de riesgos de privacidad en breve momento De dónde sacaron toda esta información lo que hace que los resultados sean tan sorprendentes es la poca cantidad de datos que se necesitan para identificar de forma única un usuario en el metaverso eliminando potencialmente cualquier posibilidad de anonimato Real en los mundos virtuales en este estudio Los investigadores demostraron que un gran conjunto de usuarios de realidad virtual en concreto 55.541 pueden identificarse con alta precisión de manera única y confiable utilizando solo atención el movimiento de su cabeza y manos según Los investigadores este trabajo es el primero en demostrar verdaderamente Hasta qué punto la biomecánica puede servir como un identificador único en la realidad virtual es decir tu huella dactilar en el metaverso vamos que ya no hay donde esconderse en el mundo virtual ya desde la década de los 70 Los investigadores han demostrado que las personas revelan información de identificación sobre sí mismos a través de sus movimientos un estudio un poquito más reciente de la década de los 2000 pero en 2005 utilizó técnicas estadísticas de movimiento para lograr identificar el género varón hembra masculino femenino con una precisión del 79%. en 2016 un estudio de 8 participantes concluyó que el movimiento de los niños se puede diferenciar del de los adultos con un 66% de precisión dos estudios uno de 2000 del año 2000 y otro de 2015 demostraron que es posible inferir la estructura esquelética de una persona a partir de datos de movimiento obtenidos de sensores de movimiento y si recordáis queridos oyentes En el episodio 12 cubrimos la noticia de una aplicación móvil que a partir de tus movimientos puede determinar si estás bajo la influencia del alcohol o no sobre todo para usarlo como alternativa a los alcoholímetros para determinar si puedes conducir en la mayoría de los estudios anteriores se han utilizado entre 8 y 40 sensores de movimiento cada uno de estos se puede pensar como un dispositivo enganchado a la ropa o al cuerpo del usuario o incluso podrían ser gorros gafas o

mandos como videoconsola estilo como la meta Quest 2 en el caso de la realidad virtual esto se reduce mucho ya que solo se tienen tres sensores de movimiento pensemos de nuevo en la meta Quest 2 Qué tiene de qué se compone Pues de las gafas que el usuario lleva en la cabeza y luego de dos mandos cada uno en una de las manos o sea en total son tres y uno podría pensar que esto no es suficiente para desanonizarte online en el metaverso porque son tres puntos tres dispositivos esto no no pueden saber si soy yo quien quien está jugando quién está utilizando este dispositivo pues Vais a ver ahora cuando os cuente más que tres dispositivos tres sensores de movimiento es más que suficiente para conseguir este objetivo Por qué se han centrado en la realidad virtual Pues bueno sobre todo porque se ha puesto mucho de moda y Bueno hasta no hace mucho digamos ahora en el 2022 no se ha puesto tan de moda sobre todo porque meta ha empezado a vender los meta Quest antes llamados oculus Quest y los hechos super populares ahora porque los ha bajado mucho de precio y el Quest 2 de hecho en el año pasado se vendió muchísimo se vendieron casi 10 millones de dispositivos a principios de 2023 el 91% de las aplicaciones más populares de realidad virtual son los videojuegos y es en un videojuego en el que se han centrado Los investigadores en este estudio y uno puede pensar que los videojuegos en sí pueden ser bastante inofensivos cuando hablamos de privacidad No no es un navegador no es ahí una aplicación que estás introduciendo tus datos verdad pero en este caso Vais a ver de nuevo que especialmente en el metaverso es más el caso contrario este análisis también viene motivado por una parte como he dicho por el interés y la vamos a decirlo así Martín proliferación profiteroles tío mira que en la ruta hubo varias eh No solo uno voy hubo varios que me lo recordaron que no se me da bien decir proliferar que ahora estuve ensayando delante del espejo tío después de esa noticia Qué gracioso si gusta me ha venido la he venido a la memoria ese episodio qué risas Bueno pues una de las motivos que de la elección de realidad virtual de este estudio es primero por eso por la proliferación de la realidad virtual sobre todo por el meta Quest 2 que es más barato y el otro es por un estudio anterior realizado incluso por el mismo centro de inteligencia descentralizado responsable de la Universidad de Berkeley de California publicado en julio del año pasado en el que los investigadores crearon un juego de realidad virtual en el metaverso como una sala de escape virtual en inglés las típicas Scape room antes de entrar en detalle quiero comentar algo interesante puntual es que uno de los investigadores de este estudio se llama Gonzalo munilla Garrido y es curiosamente una académico de la Universidad Técnica de Munich que estuvo visitando la universidad de Berkeley y junto con los investigadores de Berkeley pues publicó este estudio según lo que indica en su linking Gonzalo es original de Zaragoza Así que es interesante que tengamos un español en este estudio lo que comentaba sobre este esta investigación participaron 30 personas que se metieron este videojuego en este escape room virtual para resolver los acertijos moviéndose de una habitación a otra si no habéis jugado nunca no habéis estado en un escape room es digamos una especie de puzzle normalmente cuando lo haces en persona pues tienes ahí objetos que tienes que analizar e intentar sacar de alguna forma un código para abrir un cerrojo o bueno una contraseña que igual tienes que introducir en un ordenador o algo así no pues en este caso era muy similar cada una de las habitaciones tenía su propio reto tenías que buscar la palabra que te dejaba avanzar a la siguiente sala durante el juego Los investigadores analizaban las acciones y reacciones del jugador y a través de esto pudieron inferir información sobre el usuario como parámetros físicos la altura del jugador la longitud de sus brazos y su destreza manual moviendo los mandos esto lo hicieron con una prueba que le hacían al usuario alargar los brazos agudeza visual y distancia entre pupilas con una prueba interesante que es como cuando vas al oculista determinarán si el usuario también era daltónico no con imágenes basadas en estas cartas típicas de ishihara que son este círculo con diferentes puntitos de dos colores tu nivel de

condición física también lo pueden saber haciéndote hacer sentadillas para pasar a la siguiente sala también determinaron la reacción a estímulos Pues cuando emitían un sonido o hacían que saliera algo en la pantalla te hacían apretar un botón y también determinaban tu preferencia de mano diestro o Zurdo también podrían terminar tus parámetros demográficos es decir tu edad cómo lo hacían a través de Machine learning utilizando tu agudeza visual tu altura y tu nivel de condición física para determinar tu género si eres hombre o mujer Pues a través de de nuevo Machine learning utilizaban tu voz y analizaban un poquito Supongo el tono y la cadencia y tal Y también podían saber tu origen étnico porque había unas salas algunos retos por ejemplo que te mostraban diferentes palabras la misma palabra en diferentes idiomas y tenías que elegir una entonces la que eligieras en el idioma que eligieras Pues un poco te delataba eres eres de esa zona digamos también pudieron determinar los alrededores el tamaño del espacio en el que el usuario se encuentra por como mueves la cabeza bueno Y sobre todo las manos yo me quedo con un detalle me ha encantado lo de lo de que podían mirar las pupilas no el tal y cual me recuerda cuando si pueden detectar si has consumido drogas esa llegar a no lo digo por mí que yo no consumo drogas pero ese llegar a las 3 de la mañana con 17 años y tu madre decirte Déjame ver las pupilas deja de ver a ver si si has fumado o si has hecho esto pues cuidado que se puede ser otro dato eh Quién quién consume drogas Sí muy acertado el comentario en este caso era la distancia entre pupilas como cuando te vas a hacer unas gafas Bueno yo he visto a mí que me gusta la música electrónica he visto con alguno al ojo virulé en algún en alguna raíz tío O sea que ahí hubiese sido un indicador tú he visto a marujita Díaz tío bailando no te digo más que era esta que ponía los ojos a los Camaleón pero no sé si lo que comentas se puede hacer porque por ejemplo los Quest 2 ahora llevan rastreadores de movimiento de tus ojos Así que podrían hacer una foto analizar digamos obviamente como dices el tamaño de la pupila pero lo curioso de este estudio es que no utilizaron esos sensores y solo en el metaverso poniéndote una imagen más cerca o más lejos y es increíble determinaban la distancia entre tus dos pupilas Qué bueno tío así voy a poner un vídeo el enlace a un vídeo de Youtube de digamos el escape room y Vais a ver que es bastante interesante cada una cómo lo han pensado para sacar es un poco obvio no como lo han hecho porque te dicen Haz sentadillas y tú claro ahí sabes que que te mide un poco la condición física y luego hay una sala que es como una como cuando vas al oftalmólogo al doctor de los ojos No pues al oculista pues ahí también te ponen unas de esas Dime la letra que es y te la pone más cerca más lejos y Aparentemente a través de eso pueden determinar también la distancia entre tus pupilas y tal Y también parámetros cognitivos en plan la agudeza de razonamiento tuya también puede terminar discapacidades mentales que tengas con pruebas de bueno discapacidad físicas con pruebas de ejercicio físico o también discapacidades mentales con pruebas digamos de memoria y bueno lo que quería decir que toda esta información la podría haber obtenido cualquier jugador de este videojuego ya que cuando se juega en modo multijugador que es en sí el concepto de metaverso estos datos se envían al servidor vale pero de ahí también se envían a todos los usuarios porque estás en el metaverso y como en cualquier otro juego para reproducir el mismo el mismo escenario pues se tienen que enviar los datos de movimiento a todos los jugadores Porque por ejemplo si estoy jugando con tiene que ver lo que yo estoy haciendo y yo veo lo que le está haciendo en contra de esto y antes del estudio no había forma de defenderse no había un modo incógnito Digamos como en los navegadores un modo privado en el metaverso que oculte esta información y nos proteja a los usuarios contra este tipo de evaluación pero a partir de este estudio Los investigadores de la Universidad de Berkeley comenzaron a construir una herramienta llamada meta gard del metaverso protección al metaverso no metaverse gard que se puede instalar en sistemas de realidad virtual estándar la herramienta puede enmascarar muchos de los parámetros que se

usaron en esta investigación para perfilar las características físicas y cognitivas del usuario en el metaverso es tiene una configuración que puedes elegir quiero enmascarar mi altura quiero enmascarar mi longitud de brazos quiero enmascarar mi movimiento algo así Depende para que lo estoy usando Por ejemplo si es un juego de destreza Pues el tema de movimiento de manos igual no te interesa pero la altura y el tamaño de la sala pues eso sí que lo querrías ocultar y esto cómo lo hacen pues funciona inyectando compensaciones aleatorias en el flujo de datos es decir si mueves la mano arriba abajo pues le añade un poquito más de movimiento hacia arriba y hacia abajo para que no sepa Exactamente no se asocie contigo vamos y esto lo hacen para ocultar parámetros físicos como digo altura envergadura movilidad física que se podrían utilizar para predecir características de edad sexo salud e identificarte online esta herramienta Es de software gratuito y también permite a los usuarios enmascarar su habilidad manual como digo y también el rango de frecuencia de su voz y su nivel de condición física Aunque el problema de privacidad no se queda aquí como decía Martín los últimos dispositivos Quest de meta incluyen seguimiento facial y ocular que aunque es probable que estas nuevas capacidades desbloqueen características muy útiles en el metaverso por ejemplo permitir que los avatares expresen sentimientos a través de la cara y el movimiento y bueno todo lo que lo que hacemos con la cara no las arrugas y movimiento de ojos boca y nariz y tal para hacer el tema todo más realista pues estos datos también podrían usarse para rastrear y perfilar las emociones de los usuarios pero nos ponemos como siempre el sombrero del atacante no esto se podría abusar para proporcionar a los usuarios digamos anuncios adaptables que estén optimizados para la persuasión Es decir para que los usuarios actúen de la forma que quiera el autor del anuncio o el cibercriminar este caso es decir persuadiendo al usuario para que haga clic en algún link o yendo algún lugar en el metaverso en concreto o comprando algún artículo en particular imaginaos que vais caminando por el metaverso y te enseñan dos anuncios uno de Google y otro de Bin el de Microsoft midiendo el tiempo que pasas viendo uno u otro pues pueden determinar tu interés si te estás más rato mirando el de Google Pues a este a esta persona le gusta más Google o utiliza más Google entonces pues a partir de ahí te pueden bombardear más con anuncios específicos de esa marca o incluso pueden ir todavía refinando más el tus intereses no saber si vale le gusta Google ahora le voy a poner un anuncio de Gmail o Google Drive Pues si se para más tiempo mirando Gmail pues seguro que usa más Gmail que G drive y Bueno ahí Supongo que cogéis la idea Google y Pink se pueden reemplazar por cualquier marca no voy a comentar un poquito Cómo son los dispositivos de realidad virtual para aquellos que no tengan ninguno que no les han usado y que no sepan Qué es pues estos dispositivos el más común sería como digo el de meta el Quest 2 y se compone normalmente de unas gafas llamémoslo así con una pantalla micrófono y auriculares o altavoces que se adaptan a la cara y cabeza del usuario y también Vienen con mandos de control remoto para las manos normalmente dos uno para cada mano algunos dispositivos bueno en concreto este el Quest 2 pero otros también incluyen normalmente los más modernos incluyen sensores adicionales como cámaras y dispositivos de seguimiento ocular o incluso de cuerpo completo el sistema utiliza sensores internos o externos para medir la posición y la orientación de estos dispositivos en el espacio en tres dimensiones proporcionando 6 grados de libertad por objeto rastreado esto significa que de cada uno de estos tres dispositivos se tienen tres medidas de cómo se mueve el dispositivo y estas seis medidas por objetos se toman para la cabeza y las manos del usuario como digo teniendo un total de 18 dimensiones rastreadas estos datos se Capturan a velocidad de entre 60 y 144 veces por segundo lo que da un resultado de muchos datos que se le llama flujo de telemetría que es utilizado primero por una aplicación del lado del cliente que se ejecuta en un ordenador integrado en las gafas o conectado por algunos necesitan conectarse a un portátil a un ordenador y así genera una serie separada de estímulos

visuales bueno genera todo el tema de los gráficos que se ve en la pantalla estímulos auditivos incluso fácticos eso que son de sensación de sensaciones táctiles digamos en los mandos creando un mundo virtual 3D más inmersivo tú crees que el metaverso tío o sea estamos hablando de un de algo que podía ser una pregunta el episodio Esto del metaverso va a pasar o no va a pasar porque a lo mejor o sea este estos dos vectores de ataque al final se quedan nada porque no triunfa es un poco como si estuviéramos dando una noticia de en su día de peligros en google+, tío que al final murió y da igual tío tú qué opinas Alexis me interesa Esto del metaverso va a algún lado o no A ver ahora cuando acabe la noticia vas a ver que que sí que ya hay formas de que se puede hacer y bueno lo han demostrado con un videojuego en concreto que es que es de los más utilizados Pero yo lo veo en el tema de videojuegos pero más allá tema en plan comercial para negocios empresas todavía está creo bastante verde y para comunicarse ahí sobre todo por el tema de que mucha gente se marea cuando lo utiliza por más de media hora y bueno no sé cómo van a resolver eso porque eso es una limitación física de todo humano Así que no sé vamos a ver cómo sí no O sea que estoy convencido que este vector de ataques posible era más el si el escenario en el que se produce que es esto todo del metaverso en realidad virtual no va a desaparecer no pero sí Yo quiero pensar al revés o sea en videojuegos Sí pero qué pasa que ahora ya no estamos en una pandemia Pero yo lo usaba para alguna reunión Y sí que hay una diferencia brutal entre estar en zoom tío que es imposible estar en dos reuniones seguidas sin distraerte y no querer morirte y estar ahí en el metaverso es decir en realidad virtual porque es mucho más inversivo tío pero sí evidentemente falta adopción y aparte ahora como estamos volviendo un poco al trabajo desde en empresas y todo esto a ver yo lo veía también para temas de que nos estamos yendo un poco del tema pero para temas de clases universitarias tío que me gustaba mucho el concepto ese sí si lo has usado y te parece bien Mira es un punto A ver no conozco a mucha gente que la he usado para reuniones solo a gente que ha trabajado en meta antes pero ya el tema también que me hace mucha gracia es que los personajes los avatares no tienen piernas que creo que están trabajando en ponerle piernas no pero es que era un poco flotan bueno anunciaron anunciaron las piernas pero ahí se le metió mucha caña y decir que joder Oye por lo menos fueron transparentes explicaron que el tema de que no tuviera piernas era porque era al llevar el casco era muy difícil con las camaritas saber dónde tienen las piernas En qué posición y todo esto entonces claro parece un poco absurdo no que una de las grandes novedades el año pasado era y ahora tienes piernas pero es un problema un problema no menor si lo quieres hacer real real Oye no tengo piernas para eso hay un Jean de estos un genio de la lámpara que voy flotando aquí el sitio sitio Pero bueno el tema es que decíamos que hay cierta forma en que estos datos que te pudieran identificar pudieran acabar en manos primero del servidor del videojuego o de la aplicación que estés utilizando el metaverso y también de todos los otros usuarios conectados al mismo a la misma plataforma al mismo videojuego o al mismo mundo real de aplicación a lo que fuera porque como digo de nuevo se tiene que Reproducir te tienen que Reproducir a ti en el metaverso de los demás o sea el metaverso tiene que ser uno el mismo para todos Así que los datos se tienen que enviar entre todos los usuarios en el pasado se han realizado investigaciones sobre la identificación de usuarios a partir de datos de realidad virtual similares a este estudio Pero en esos casos previos se utilizaron datos de pequeñas muestras de usuarios entre 16 a 511 participantes un tamaño 100 veces menor que el estudio actual en esos casos como éstas tan pequeñas lo que hacían era identificar a usuarios a través de atributos simples y estáticos como la altura En cambio cuando el objetivo es identificar a una persona entre miles millones o miles de millones no se pueden usar estos atributos estáticos porque hay mucha gente que va a tener la misma altura que otra persona así que la única forma es mediante las diferencias de comportamiento reales en los patrones de

movimiento que es lo que este estudio analizado además esta investigación es mucho más realista que las anteriores Porque además de contener datos de muchos más usuarios 55.000 como digo 541 estos usuarios son de más de 40 países diferentes y además estos usuarios utilizan más de 20 tipos diferentes de dispositivos de realidad virtual Ok y en qué se han centrado en la realidad virtual en concreto pues se han centrado en el videojuego beatsaver que es el juego de realidad virtual más popular y con mayor recaudación de todos los tiempos con 6,2 millones de copias vendidas probablemente muchos de nuestros oyentes sepan de que de juego E incluso lo tengan en casa pero vamos a ver vamos a hacer una encuesta aquí a Martín tú sabes de qué va este juego el Beat saver hombre Alexis tú me has visto en la Discotec bailar tío Por supuesto que sí O sea nada es Coño pero sí sí que lo sé porque al tener un Quest 2 y de hecho está súper logrado es esto de bailar a la vez que tienes ahí dos espadas y al ritmo de la música vas cortando movidas es una mezcla entre el ninja fruitter o cómo se llamaba no me acuerdo y uno quitar giro Este pero me parece muy bien salían las sí lo que tocaba es un instrumento y aquí es más bien quedas espadazos para mí es como Fruit Ninja con pues el que sea de baile pero sí estaba está muy logrado pues pues ahí ahí la descrito Martín mejor que yo fruitinya y uno de baile dense Revolution alguna de estas Pues eso que tienes dos sables Láser Un poco han pillado el tema este así atractivo de Star Wars uno rojo y otro azul y te van saliendo cubos de también del mismo color rojo y azul y entonces los tienes que cortar cuando lleguen cerca de ti al ritmo de la música La verdad que es muy interesante Yo creo que es bastante ejercicio de manos aunque poco más del resto del cuerpo pero bueno Y luego también pues bueno se han centrado en este en este videojuego no como digo del metaverso y luego también tenemos por otra parte otro ingrediente de este estudio es el Beat líder que es una extensión de bitsaver de código abierto que lo que hace es mantener tablas de clasificación no oficiales para más de 100.000 mapas de bitsaver estos mapas le llaman mapas a las canciones y no lo llaman canciones porque aparte de tener canciones pues tienen los objetos no que que salen que a veces son como me los tienes que esquivar y similares por eso los llaman mapas en lugar de canciones Pero bueno son canciones en sí los jugadores de beatsaver pueden instalar la extensión Beat líder para competir con otros jugadores Y lograr una posición más alta en las clasificaciones de Beat líder después de jugar a un mapa de bitsaver con la extensión Beat líder instalada las puntuaciones se cargan automáticamente en una tabla de clasificación visible a nivel mundial desde mayo de 2022 más de 50.000 usuarios han publicado más de 2,5 millones de puntuaciones en la plataforma Beat líder lo que incluye las sesiones de juego con movimientos de cabeza y manos es decir que estas 50.000 personas han jugado han hecho a 2,5 millones de canciones y todo esos movimientos de estas 2,5 millones de canciones se han subido a los servidores de bit leader en una asociación con los administradores de Beat líder y para el objetivo de este estudio Los investigadores obtuvieron un conjunto de datos de 3,96 terabytes que consta de bueno 2,6 millones de repeticiones de los 55.000 usuarios en 713.000 sesiones de juego separadas el conjunto de datos tiene entre 1 y 4.500 reproducciones por usuario y las reproducciones varían de duración desde dos segundos hasta más de una hora y a través de estos datos pues realizaron un análisis utilizando técnicas de Machine learning y después de hacer un entrenamiento a su modelo de clasificación con 5 minutos tan solo 5 minutos de datos por jugador analizando sus movimientos de cabeza y manos que obtuvieron todo esto de Beat líder pudieron identificar a un usuario de forma única del grupo completo de más de 55.000 usuarios con una precisión del 94% si luego capturan 100 segundos de movimiento es decir un minuto de 40 segundos o con una precisión del 73% capturando solo 10 segundos de movimiento en este estudio a pesar de trabajar con 100 veces más datos que estudios pasados se han conseguido se ha conseguido una precisión de identificación de usuarios comparable a los trabajos anteriores hay una

limitación principal en este estudio es que el modelo de Machine learning utilizado para analizar los datos no tiene tanta precisión como otros modelos que son más complejos y requieren mayor poder de computación pero el modelo elegido es suficiente para Resaltar el problema de privacidad que supone usar el metaverso esto de hecho para mí a mí me dice que no es tanto una limitación sino un una oportunidad de mejora porque esto me dice que incluso esta identificación se pudiera hacer de forma más rápida y con menos datos si se utilizan modelos de Machine learning mejores que el que utilizaron en este caso y uno se puede preguntar Oye estos datos que obtuvieron de Beat leader los puede obtener cualquier persona pues según comentan para evitar exponer a los usuarios de Beat líder Los investigadores no han hecho público el conjunto de datos sin procesar que no utilizaban su estudio Pero bueno uno puede pensar y Beat líder la empresa el servidor que corre este esta aplicación Pues bueno La respuesta es que sí si ellos tienen todos los datos no y solo tienen que desarrollar un análisis y herramientas similares a las creadas por los investigadores Así que el tema es si confías en digamos en el videojuego en la aplicación que estás utilizando y el servidor Pues entonces te puedes quedar tranquilo pero si crees que tienen algún tipo de agenda oscura y van a utilizar tus datos para identificarte pues no utilices esa aplicación ese videojuego y ahora voy a entrar un poquito y acabar la noticia con escenarios de ataque os voy a comentar un par de ellos no primero por una parte tenemos obviamente que se puede identificar al dueño del dispositivo es decir te compras la Quest 2 con el bidsaver e instalas Beat líder la extensión está para subir tus mapas como bailas como mueves las manos con con cada canción luego te creas una cuenta en Quest 2 en meta en Quest 2 con tu información email similares y añades tu info altura lo que sea esto no es esencial no es que se utilice en este estudio pero podría ayudar a identificarte con mayor precisión e incluso sacar la identidad de tu persona porque si son capaces de asociar un tipo de movimiento específico contigo y tú además tienes el email especificado en la cuenta de Quest 2 pues Oye ya saben quién está detrás no luego con que solo juegues cinco minutos a este videojuego al bidsaver Ya está ya te tienen fichado porque es lo que dicen con solo 5 minutos de videojuego pueden crear una huella dactilar tuya en el metaverso y luego a partir de ahí Eso es la leche porque aparte es que yo tenía bueno tenía ahí un tema que podía testear videojuegos gratis por la empresa donde trabajaba antes y tío o sea yo jugaba muchísimos juegos que jugaba cinco minutos y ahora va como los tenía todos gratis pero me sorprende porque hubiese pensado que me dirías no Esto es lo típico que ya eres megamaster llevas 50.000 horas jugando al juego cinco minutos tío Sí sí con cinco minutos Solo que lo típico que vas a casa del colega juegas Ah qué Guay tal no has tenido una encuesta en tu vida se lo pones a tu padre tío para la coña y ya está justo Así es que lo que voy a comentar ahora a continuación que cinco minutos es cuando vas a casa de un amigo y tienes la novedad dice Ah lo voy a probar lo voy a probar y juegas y luego te aburres o lo que sea y lo dejas y ya han invadido tu privacidad Tu colega esto eslabón más débil justo Mira hay que tenemos que apoyarnos los unos a los otros si algún colega te viene a casa y tiene la quesos No le dejes jugar sería una buena excusa no pero bueno como decíamos si has jugado cinco minutos ya te tienen fichado cualquier otra vez que juegues bueno Comencemos una clarificación con tan solo 10 segundos te pueden identificar como he dicho con una precisión del 73% Y si juegas ya un minuto 40 segundos Pues con una precisión del 94% y esto entre 1 entre 55.000 personas así que es bastante preciso pero el impacto va más allá y voy a continuar con o sea continuo con el escenario anterior en el que eres un usuario de Quest 2 y has jugado a bitsaver al menos 5 minutos luego vas a casa de un amigo y quieres echarte un vicio como decía Martín y le pides a tu amigo que te deje la quesos que quieres echarte una partidilla los que estén monitorizando el flujo de telemetría que envía bitsaver a los servidores de bit leader van a saber que el jugador eres tú y no tu amigo Aunque el dispositivo esté registrado con la info de tu amigo de

nuevo esto es posible porque la identificación se basa en los movimientos del jugador no en la información estática del usuario como email y registro en la cuenta de esta forma los abusadores de la privacidad podrían saber que estás en casa de tu amigo y ahora un escenario de guión de serie de csi Black mirror o alguna película de Hollywood en este escenario empezamos desde cero digamos nunca habéis jugado a ningún juego de realidad virtual ni usado la Quest 2 No sabéis ni lo que es ni creado ninguna cuenta en el metaverso pero Vais a casa de un amigo de nuevo el típico amigo que se ha comprado la Quest 2 hace poco y tiene el juego beatsaver y Beat líder como es la novedad de nuevo todo el mundo juega Bueno pues parece curioso ponéis a jugar y lo de antes lo típico después de 5 minutos os parece difícil perdéis el interés nunca habéis jugado esto os mareáis empezáis a sudar os Llama a alguien al teléfono o distraís y dejáis el juego como he dicho antes con estos 5 minutos ya os han fichado luego vais y por algún motivo Este es el escenario el plot este digamos de esta historia cometéis un crimen digamos en la casa de vuestro amigo la policía acude y obviamente ya no estás porque no quieres que te pillen pero encuentran pelos vuestros o ADN en la Quest 2 y sabe entonces que la habéis usado esto Solo lo digo para que de alguna forma sepan han sabido que que has usado la Quest 2 pueden enterarse de cualquier otra forma pero este sería el caso no un poco para atar Los Cabos del guión los policías han escuchado sobre Esta técnica también que estoy justo ahora comentando en este episodio que es de sirve para desvirtualizar a los usuarios en el metaverso obtienen una orden judicial para los datos de jugadores de Beat líder y de esta forma identificar pueden identificar vuestro patrón de movimiento o huella digital como digo en el metaverso en base a los datos de Beat líder del día y el momento en el que jugasteis en casa de vuestro amigo además de esto les piden a bill líder que les continúen proporcionando todos los datos hasta que os encuentren en forma en tiempo real Esta es la policía está recibiendo todos los datos de Beat líder por su parte la policía crea un programa de monitorización continua de estos datos de Beat líder en busca de vuestro patrón de movimiento que ya han podido identificar ya han podido hacer la huella dactilar digamos de vuestro patrón de movimiento con los cinco minutos anteriores Y que les alerte la próxima vez que encuentre dicho patrón os olvidéis de esto obviamente no sabéis de este de este de este análisis de esta investigación a no ser que escuchéis tierra de hackers y cinco meses más tarde Vais a casa de otro amigo que tiene bitsaver y Beat líder instalado jugáis por 5 minutos y 5 minutos más tarde badabun la policía tumba la puerta de casa y os arresta en este escenario ficticio la policía obtuvo los datos a partir de una orden judicial como digo pero Se podrían obtener estos datos a través de compromiso de los servidores y sistemas de Bill leader o a través de la interceptación de datos en algún punto de la red o de la plataforma e incluso comentan los investigadores que los usuarios también podrían de alguna forma obtener alguno de estos datos Porque como digo están disponibles un usuario puede ir a bit líder y ver un poco Cómo se ha movido la persona que ha subido la puntuación el score pero está un poco más de forma agregada según comentan Así que es un poco más difícil pero yo creo que no imposible Wow episodio de csi Las Vegas Cuál era el Cyber csi este da para a lo mejor no para película de Hollywood pero para un episodio Sí yo de hecho quitaría lo incluso Porque si quiero decir si tú te has dejado pelos ya saben que eres tú por el ADN Ya está no tienen que esperar a que vuelvas a jugar a bitsaver O sea no no haría falta No ya ya está ya tienen el ADN Pero yo lo pongo así tú vas a jugar a casa de Tu colega resumiendo mucho yo voy a jugar a tu casa Alexis me tocas los pies y te pego un cuchillazo y te asesino y ahora viene la policía y no hay ningún indicio saben que se ha cometido un asesinato porque tú estás muerto en el suelo pero no hay nada más Pero ven que se ha jugado a este juego y saben de esta investigación Entonces se ponen a mirar y detectan que hay dos patrones diferentes de que dos personas han jugado tú y otra más entonces ya saben que hay una segunda persona solo por los patrones que se que se

tiene de esto y ahora lo que hacen es monitorizar cuando la persona con ese mismo patrón vuelve a jugar en algún sitio y tú Pues dentro de medio año al final te compras la Quest te pones a jugar a registrar la cuenta con tu con tu nombre esta vez salta el patrón la firma el finger printing de cómo juegas pum la policía ya tiene asociado ese fingerprinting a tu cuenta medio año después ya saben que eres tú zas y te pescan tío Sí sí episodio eh No no vamos a ver si alguien nos está escuchando que no que nos escriba que podemos tenemos ideas que la Industria del cine tío venga y nos exponsorice por lo menos que se meta en patreon tío si tenemos a gente como platanito canario y el zolomeo Paredes tío nos puede venir alguien de la Industria del cine o artistas con un hombre curioso también ha exponsorizado creo que no os lo merecemos Sí nosotros lo del ADN lo hacía para que se hiciera más rápido el episodio y que no durará 40 minutos Pero y para que vieran Oh ha usado Quest porque si no se podían tirar ahí los hombres los policías mirando en rincones Claro pero yo a lo que iba a lo que iba era que si ya sabían que usaste la Quest que qué novedad tiene el que sepan a través del patrón que has jugado a la juez o sea cuál es la diferencia a la hora de que tú hayas cometido el crimen una una serie que aunque sepan quién eres cómo te van a encontrar si Imagínate que eres un tío de estos que no voy a usar ninguna tarjeta de crédito ni tengo teléfono Ah bueno entonces el crimen desaparece joder busca y captura Y saben dónde soy vale si en ese sentido sí de que luego me pongo a jugar desde desde no sé una playa en Brasil ahí a tomar esa es una esa buenista también Brasil Pues sí Bueno sí sí así que ya sabéis tenemos ideas la verdad que es un poco terrorífica un poquito el tema o sea eso es un tema un poco más de historia de mal pero como he dicho anteriormente está igual se puede abusar estilizar en contra de cualquier persona y cualquier civil que no haya cometido ningún crimen Así que pueden rastrearnos pueden saber dónde estamos en todo momento Y bueno eso da un poco escalofríos no y con esto queridos oyentes llegamos a la pregunta del episodio 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 y respuestas tenemos sí y no pedazo pregunta tío pedazo pregunta desanonimizarte en el metaverso en el metaverso Vete a contarles a tu padre a ver qué te a ver qué te dice papá tengo miedo que me desanonimicen en el metaverso tío te saca de aquí chaval que va mucho y llevas está yendo muchas veces al museo eso de suena desatomizarte o algo así o ha visto muchas películas de superhéroes Pues sí ahí lo dejamos y a ver si nos comentáis si tenéis alguna otra respuesta pero no la respuesta será sí o no sí era sí o no lo que pasa que lo he dicho igual estamos estamos hablando el uno con el otro y nos hemos excitado ahí y nada sí y no nos hemos excitado ahí te ha salido un anglicismo un poco porno tío no nos vemos yo no me excitado nada contigo hacer el podcast contigo Alexis me lo paso bien de situación tampoco eres tan colegas tampoco eres tan Esa es la palabra bueno excitados o no Alexis Cálmate tomate y gracias esperemos que estéis excitados también queridos oyentes Y si lo estáis Pues sí O sea no es una review hombre todo excitados darles al like que compartir esto con con amigos que a lo mejor pues tienen yo que sé carencias sexuales y necesitan excitación Pues que se pongan a escuchar tierra de hackers que a lo mejor funciona y nada Muchísimas gracias por estar siempre hasta ahí y recordar eso compartirnos y hablar de nosotros Muchas gracias a todos por escucharnos y nada Gracias por estar siempre ahí y nos escuchamos en la próxima Adiós adiós chao chao si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers