uno de los apetes más avanzados chinos desarrolla un nuevo malware para infectar routers y esta vez a pesar de tratarse de un apt nos afecta a todos por igual welcoin empresa fundada por Sam altman ceo de opening se quiere posicionar como moneda mundial además de ofrecer su servicio walld de identificación global utilizando el Iris de las personas Cuántas cuchara el podcast que te interesa lo que te vamos a contar comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 8 de junio de 2023 este es el episodio número 96 yo soy Martín vigo y está conmigo una parte esencial de este nuestro podcast Alexis porros Hola Alexis qué tal Aquí andamos experimentando ya lo que es el cambio climático bueno Supongo que es debido a eso porque nos está llegando un humo desde Canadá por todos los incendios que están pasando ahora que el cielo está amarillo parece un episodio de esos The Walking Dead o similares yo siempre con las series ya sabes y pues nada aparte de eso estar muy agradecidos por vosotros nuestros queridos oyentes por estar siempre con nosotros episodio tras episodio y que sepáis que sin vosotros esto no sería lo mismo y también os Quiero recordar que estamos en todas las redes sociales más populares en las que nos podéis encontrar como tierra de hackers o arroba tierra de hackers También estamos en todas las plataformas decentes de podcast y si no lo estáis ahora mismo rápido ID a suscribiros para recibir notificaciones de nuestros episodios Y tenemos un servidor de discord al que podéis acceder vía tierra de hackers.com barra discord y finalmente como siempre cerrando la intro agradeciéndoos vuestro apoyo a la pregunta del episodio que publicamos en Twitter y que la del anterior fue la siguiente estás A favor o en contra de la postura de España de que se debería prohibir el cifrado extremo extremo Teníamos dos respuestas la más votada 96% en contra de que se prohíba y un 4% a favor de que se prohíba era un poco de esperar no muy interesante como siempre y yo darle las gracias a nuestros mecenas de patreon que decías antes esto no sería lo mismo sin sin los oyentes ni sería lo mismo si los mecenas de patreon ni sin nuestros esposos porque es que no habría pocas por tanto gracias por haberte una herramienta más compleja más compleja de seguridad en aws empresas de todos los tamaños se apoyan diariamente en brawler pro para que sus equipos puedan confiar en su modelo de seguridad de aws puedes probar brawler pro y mismo y de manera totalmente gratuita y vas a obtener dos cosas principales paneles y gráficas con información concisa y accionable con todo lujo de detalles sobre la madurez de tu modelo de seguridad y además visión completa de tu infraestructura en todas las regiones de aws y tendrás todos los resultados en apenas unos minutos empieza a usar brawler Pro y benefíciate de los resultados visitando tierra de hackers.com barra brawler Pro prw l e rpr y también queremos darle las gracias a otro de nuestros patrocinadores en este caso monat una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y monat a través de una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echadle un vistazo a su web monat.com y mandarles vuestro currículum a tierra de hackers @monat.commod.com perfecto Pues nos vamos al lío a toda leche y volvemos a hablar de apts algo que un tema que os gustaba mucho quizá a los oyentes un poquito menos técnico no tanto cuando nos metemos ahí al meollo técnico pero en general todos os resulta por lo que nos contáis muy interesante también volvemos a hablar de China algo también muy interesante y hoy volvemos a hablar también de malware apt China malware la receta de siempre pero hoy querido oyente viene con una particularidad que te interesa si bien cuando solemos hablar de estos grupos muy avanzados de hackers a la onda a la orden de gobiernos poco democráticos como china en este caso no suele ser una amenaza que nos suele afectar al Común de los mortales como tú

como yo como Alexis Pero esta vez sí en esta noticia veremos que china ha decidido comprometer los routers de nuestros Humildes hogares para utilizarlos como puentes en ataques objetivos más importantes como empresas y gobiernos rivales china quiere utilizar tu conexión a internet para conectarse a su vez a sus otras víctimas para así dificultar la tarea de los investigadores cuando suceda el ataque ya que las conexiones No van a llevar a los servidores chinos llevarán a tu humilde morada querido oyente Así que todos atentos que esto te incumbe nos llega de la mano de una investigación de checkpoint Security Aunque bueno Es cierto que otras empresas como sset y abast que he visto por ahí también detectaron esta campaña y empezaron sus propias investigaciones todo empezó cuando esta empresa empezó a fijarse en ataques atención contra oficiales de varios países europeos no especifican exactamente Cuáles sólo mencionan Bulgaria por ahí brevemente concretamente en la investigación de ese que también me leí pero dicen varios países europeos Lo que sí detallan es que se trata de personal relacionado con entidades de relaciones exteriores teniendo en cuenta que china está intentando posicionarse como el ente conciliador entre Rusia y Europa y Estados Unidos no me extrañaría en la digo en el conflicto de Ucrania no me extrañaría nada que esta campaña tuviera que ver con esto quiero decir china infectando oficiales europeos encargados de relaciones exteriores para espiarles Y obtener información confidencial sobre la postura europea frente a la guerra estrategias negociaciones etcétera ya lo que china bueno haga después con toda esta información pues es pura especulación Pero insisto no me sorprendería que le pasase toda esta información luego a Rusia también destacar que checkpoint al contrario que ese día vast que como decía también reportaron sobre esta actividad atribuyen este ataque a un apt desconocido que han llamado Camaro dragón ese sin embargo lo atribuye a la apt también chino por supuesto pero que es más conocido y que en la industria lo conocen como Mustang panda pero checkpoint argumenta que si bien tiene muchas similitudes hay diferencias en sus tácticas técnicas y procedimientos por lo que checkpoint piensa que son dos grupos de apts chinos Aunque están operando evidentemente ambos bajo el gobierno de ese país en qué consiste los vectores de ataque pues este grupo ha desarrollado un nuevo malware concretamente un implante incluyendo puerta trasera contra los routers tp link a muchos de vosotros os sonará tú Alexis tienes uno de estos routers tp-link Pues de estos no pero no lo vamos a decir en la audiencia no va a ser que me quieran aquí comprometer pero de momento parece que estoy a salvo O sea no nunca has tenido un router topperrín lo digo porque la mayoría de hogares tienen uno yo he tenido uno en su día ahora pues coincide que no pero sí creo que tenía uno de esos pequeñas pequeños de esos creo incluso que son como para de viaje no que te puedes llevar a un hotel y lo conectas al abierto al hotel vía WiFi o incluso vía cable y luego conectas tus cacharros pero en casa ahora mismo no pero sí pues pues bueno Esto es solo para decir que Alexis tuvo uno yo tuve uno o sea imaginaros es una marca muy muy común Y estoy convencido que la mayoría de los oyentes lo tienen también pues esto lo hallaron porque investigando los ataques a los oficiales europeos dieron con parte de la infraestructura de los atacantes y se encontraron con muchos de sus archivos y herramientas evidentemente lo primero que hicieron fue empezar a analizar todo y en este caso se trataba de miles y miles de archivos Así que empezaron a buscar cosas llamativas y es así como encontraron un fichero un archivo que se identificaba como el firmware de routers Inc claro encontrarte un firmware de un router muy común entre los archivos de un atacante tan potente como este apt chino Pues claro enseguida invita a ponerte a analizarlo no Y eso es precisamente lo que hicieron se descargaron de la web oficial de tp-link la misma versión de firmware y compararon las dos la oficial con el que encontraron entre los archivos chinos para ver si era Exactamente lo mismo os había modificado y enseguida se dieron cuenta que el chino era algo diferente había sido manipulado lo más curioso de todo es

que las modificaciones las cuales mencioné voy a mencionar ahora estaban hechas de tal manera que eran independientes del firmware al que se le inyectaban Dicho de otro modo el mismo malware esas mismas modificaciones se podían hacer perfectamente a otros firmware de otros routers de otras marcas un malware orientado a firmware de routers polivalente O sea me parece muy top y en qué consistían las modificaciones hechas por los chinos de tal manera de hecho que fuera independiente del firmware a infectar Pues mira modificaron el sistema de archivos agregando cuatro ficheros nuevos y modificando dos que ya existían en el firmware original añadieron estos cuatros barra user barrabín timer y barra user barrabín udhcp Y como decía estos son los que añadieron pero modificaron dos archivos barra tc barra rc punto de barra rcs y barra web barra user rpm barras software upgrade rpm.htm antes de entrar en los detalles como llegaron a infectar los routers para meter este implante no están seguros y lo estuve buscando en todos los reportes especulan que seguramente los chinos escanearon todo internet en busca de modelos de routers pues con la consola de gestión expuesta a internet y credenciales por defecto aquello de admin admin no o routers directamente con firmware Antiguo y vulnerable que permitiese la ejecución de código remoto hoy en día de hecho un par de consultas en servicios como shodan ya puedes tener una lista de millones de routers expuestos bajo tu criterio de búsqueda Así que es perfectamente factible que los chinos lo hayan hecho así pero parémonos un momento en los archivos añadidos y modificados y vamos a verlos con lupa empezamos por los modificados esos dos que ya existían en el firmware original y que como decía eran barra etc/rc de punto de barra rcs y el web usrpm software upgrade rpm.htm vamos primero con este último porque me pareció brutal y sencilla la modificación que hicieron software upgrade rpm punto htm es un archivo de una página web básicamente en vez de punto html es punto htm y como los oyentes un poco más técnicos sabréis cuando Vais a configurar vuestro router para modificar la contraseña de la WiFi o abrir algún Puerto porque quieres utilizar bittorrent accedéis a vuestro navegador verdad normalmente Vais a una IP del estilo 192 168.1.1 o algo similar básicamente estáis accediendo a una página web que es el portal de gestión o administración de vuestro router y como os podéis imaginar este archivo software upgrade rpm punto htm es concretamente la página de actualización de firmware del Sistema de Administración del router típica página que te muestra un pequeño formulario donde te permite pues o subir un archivo para actualizar el firmware por tu cuenta o directamente pues darle un botón no el típico actualizar ahora y que consulte en la web oficial si hay una actualización nueva no lo típico Pues bien y atento Alexis nuestros queridos chinos hicieron unas simple y pequeña modificación a este archivo display dos puntos Non qué te dice esa modificación No sé creo que me dice que están haciendo algo para ocultar en la Wii lo que están haciendo Y entonces toda su actividad todas las ventanas que saldrían de su actividad están escondidas no sé si es algo estás cerca Piénsalo hablamos de un archivo que es de una página web un archivo htm Y de qué te suena Yo sé que esto lo conoces de sobra solo que ahora no te viene a la cabeza display dos puntos no tú has escrito esto Alguna vez estoy seguro display dos puntos de ventanas de Linux Pero obviamente claro estaba no estaba prestando toda la atención Es que has dicho tantos archivos que me Estaba volviendo un poco pero sí sí para ocultar las capas DIF de las páginas html y temas similares o cualquier elemento htm efectivamente lo que hicieron los chinos fue el archivo de la página web de la página en concreto que te permite actualizar el firmware del router añadieron esta propiedad css que lo que hace es alterar la interfaz y ocultar el formulario de actualización es decir tú podías poner la página pero no te aparecían los botones para actualizarlo Por qué Pues porque los chinos no querían que tú aunque no supieras que estás infectado fueras actualizar en firmware y por tanto ellos perdi implante una sola línea que tiene una funcionalidad muy buena de hecho como siempre por supuesto os dejo el reporte técnico y largo y detallado de

checkpoint Security en las notas del episodio y ahí veis dos capturas de pantalla de cómo se ve con y sin esta modificación Y la verdad es que está muy bien seguimos el otro archivo modificado es el de barra de tcrc.d rcs este es parte del sistema de arranque del sistema operativo del propio router y añadieron tres líneas tres líneas a este archivo barra user barrabín udhcp/user barrabín/h para user Bin barra timer espacio 60 si recordáis estas tres líneas hacen referencia a los a tres de los cuatro archivos nuevos insertados por los chinos en el firmware analicemos los porque básicamente barra etc de punto de rcs lo que está haciendo con esta modificación es asegurarse de ejecutar esos tres archivos cada vez que se inicia o reinicia el router Así que vamos a ver esos tres archivos el barrayuser barra bim/shell es una puerta trasera que Sencillamente pues Abre una shell en el puerto 1444 y que también está protegido por una contraseña que bueno está directamente a jarcodeada en el implante hago una breve pausa aquí sé que hoy es un episodio un poquito más técnico para los oyentes que normalmente nos escuchan que no son tan técnicos si nos escuchas por primera vez y estás un poquito perdido No te preocupes no todos los episodios son así pero me veo en la aplicación de cubrir la actualidad e intento hacerlo lo más sencillo posible y hay veces que hay noticias de estas que es inevitable meterse un poquito en el fango no pero básicamente esto archivo lo que hace es abrir una puerta escondida de manera que tiene una contraseña que sólo los chinos conocen Y de esa manera pueden digamos introducirse en el router siempre que quieran y la ocultan detrás digamos un poquito de un puerto de acceso un poquito raro vale luego tenemos el barra user barrabín barra udhcp este archivo es el implante principal permite a los atacantes llevar a cabo tres acciones crear una shell para que se pueda conectar de esa manera el router es decir si la otra si la puerta trasera no funcionase esto te permitiría crear una nueva puerta trasera permite también transferir archivos a los servidores de los atacantes o del servidor de los atacantes al router y esto porque es útil Bueno lo que vemos normalmente en este tipo de atacantes es que suelen infectar máquinas en este caso routers pero luego quieren enviar actualizaciones de su firmware módulos o cuando si han sido parcheados pues quieren inmediatamente volver a reinfectarlos básicamente esta capacidad es muy importante para seguir expandiendo en el tiempo la infección de los de los routers en este caso pero la tercera es la más importante crear un túnel para actuar como un Proxy entre los servidores de los atacantes chinos y cualquier otro punto o servidor en internet y digo que este es el más importante porque es aquí donde nosotros como decía el común de los mortales Alexis yo tu querido oyente tenemos que preocuparnos esta funcionalidad de este implante permite a los chinos encadenar routers infectados sus conexiones entre routers hasta llegar al destino final de manera que si alguien en el destino final se da cuenta que ha sido infectado y mira Por quién va a haber tu router y cuando Investiga tu router si llega eso va a haber el mío y cuando Investiga el mío va a ver el de Alexis y el de Alexis es el que se han conectado los chinos esto lo que permite es precisamente eso ir encadenando añadiendo puentes a sus conexiones para dificultar la investigación por parte de expertos en seguridad cuando están investigando campañas de malware como en este caso contra oficiales relacionados con entidades de relaciones externas europeas muy muy inteligente y nos afecta como decía a todos nosotros no es a nosotros a quien quieren espiar es a nosotros a quienes quieren utilizar como como vehículo para llevar a cabo esas infecciones lo primero volviendo al implante que hace es decir una vez infectan tu router lo primero que sucede es enviar información a los chinos sobre tu router concretamente el nombre de usuario el nombre del sistema la versión del sistema operativo la hora que es la arquitectura Cuántos números de cpus tienes la Ram la dirección IP por supuesto la dirección Mac y bueno las típicas telemetrías de un sistema cualquiera las comunicaciones curiosamente mencionaba esto están cifradas para bueno ocultar un poquito esas filtración de datos no pero curiosamente utilizar un cifrado propio se inventaron uno

basado en bueno en sustituciones esto Imagínate con cifrado súper sencillo Y por supuesto inseguro sería pues cuando hay una a pongo una B cuando hay una B pongo una c cuando hay una c pongo una de algo así no pues este tipo de cifrado he de decir también que en checkpoint decían que si bien se reían un poco de utilizar un cifrado propio porque eso no suele ser lo más inteligente no fueran capaces de romper ese cifrado Bueno nos vamos al siguiente archivo modificado el barra user barrabín/shell pero escrito sh eel este archivo también es bastante curioso Perdón modificado no añadido a ver esto demuestra que los chinos saben lo que están haciendo porque la función de este archivo es escribir datos en digamos su forma más pura no lo que conocemos como rodeira o te puedes imaginar prácticamente como si fuera unos y ceros a una partición que tienen estos routers dedicada y dedicada exclusivamente para almacenar telemetría del chip WiFi insisto perdonar un poco técnico hoy pero tenemos también muchísimos oyentes técnicos vamos a ver los routers tienden a tener más de una partición y hay una que está dedicada a la telemetría Pues bien los chinos decidieron utilizar esta partición poco conocida en vez de la principal donde se encuentra Pues todos los archivos programas ejecutables relacionados con el funcionamiento natural del router para ocultar los dominios de los servidores de los atacantes que el implante consulta cuando se va a conectar básicamente los dominios del command de control así un administrador haciendo sus tareas de administración o incluso porque a lo mejor ve algo de actividad en el tráfico rara cuando va a mirar el router las tripas del router por así decir normalmente va a mirar la partición principal donde está todo el mejunje no Por así decirlo y se va a olvidar de que hay particiones adicionales por eso los chinos lo están metiendo ahí la verdad es que me quito el sombrero Y por último tenemos otro archivo añadido al que decía este barra user barrabín barra timer que concretamente el comando dentro del otro archivo era espacio 60 pues esto básicamente como ya os podéis imaginar es un temporizador que cada 60 Segundos intenta ejecutar el implante que os acabo de contar así básicamente si algo fallas y rompe el implante pues se aseguran de que se vuelve a intentar ejecutar pasado un minuto y así cada minuto conclusiones para terminar la noticia Bueno aquí pues en principio ninguna novedad en el sentido de que pues otro ataque más de otra campaña con otro malware de una Pt chino pero me gustó mucho de esta noticia y por eso se la traigo esta vez nos afecta bastante a nosotros Porque nos utilizan como vehículo como enlace como como cable de conexión para infectar finalmente a gente o a gobiernos o a entidades o a personal muy relevante y que a la hora de una investigación lo que van a dar es con nuestros routers y no con los servidores chinos O sea que los chinos están montando su propia red Thor digamos en paralela a internet Sí sí mira qué Qué buena analogía esto es como un Thor donde los nodos somos el común de los mortales somos nosotros y no nos pagan nada si nos dieron al menos unas criptomonedillas pero una propenilla que te dejen ahí ostras eso molaba van dejando cripto wallets en las particiones para sí son administradores en plan oye bien nos has encontrado toma una propinilla chaval Claro que sean buena gente Al menos que al menos por los servicios no ocasionados los gastos de energía y aunque sea para pagar la conexión a internet Ya que la están utilizando ya que vamos a pachas no sí con los chinos pues por lo menos que paguen su parte O sea que me quedo con que si yo tuviera un tp-link lo tendría que tirar a la basura y comprarme otro porque es los que están comprometiendo Pero has dicho que este implante puede afectar a otros modelos no claro Entonces no no se trata de tirar el tp link se trata de tirar todos los routers Entonces no sé no sé cómo lo vamos a hacer me vale porque claro ellos detectaron el de tp-link porque Pero insisto sobre un tesoro de miles y miles de archivos Lo que pasa que pues con el que dieron fue con el de tp-link y además de manera que veían que se podía infectar a otros O sea que ya ves porque es que si lo piensas es eso o sea por un lado con css te quitaban la opción de actualizar no era un tema de Modificar un

binario de actualización no no el css por otro lado te meto tres archivos nuevos en el sistema de ficheros por tanto eso te lo puedo hacer en cualquier otro lado y luego pues con el y como en general todos los routers están basados en bici Box o cualquier tipo de sistema unix o Linux Pues claro es que es luego el implante en sí es un archivo nuevo de ellos es que los que han modificado no han modificado Nada del otro mundo Entonces es que es muy inteligente a ver sí Este es el problema de dejar instalar tu propio firmware Porque si estos cacharros permitieran solo instalación de firmware firmado digitalmente por tp-link que sí que hay casos no que puedes sitelod cargar firmware no firmado pero metiendo el router en modo en modo digamos de ibagué o modo develo pero modo aparte que un usuario normal no lo haría Pues claro te metes en estos meollos en estos problemas no sé si en la noticia dicen Cuántos tp links hay expuestos en internet según shodan o sensis o algo de esto no eso no no lo mencionan pero vamos insisto por eso Oye si tú habías tenido uno yo había tenido uno que bueno que eso no quiere decir que estuvieran expuestos pero muchísimo lo están muchísimos en actualizar quiere decir preguntas a los siguientes Cuándo es la última vez que actualizaste tu router Pues eso y además que son son de estos baratillos no no son así en plan unos Cómo se llama la marca uniqua y unify esos que son un poco más y está este otro como es y el héroeste claro Una pasta y no no hacen falta Sabes Por eso digo que los hogares te va a estar el links el tp-link y pues alguno más que no me sale ahora pero vamos los tres de Thank you y algo así no sí Ese es el justo justo pues interesante la noticia Martín A ver no sé cómo podemos evitar esto pero bueno esperemos que igual Los isps Iguales estén al tanto algo y estén bloqueando estas estas estos problemas estos ataques no sé también cambiándole la contraseña por defecto sería una posible solución no Sí claro a ver lo primero no tener el Sistema de Administración expuesto y luego si lo tenemos después puesto que no deberíamos por lo menos con una contraseña potente y luego pues tener los sistemas actualizados O sea no tengas la administración expuesta y tenga el sistema actualizado en principio así pues ya vas bastante bien no ya Ok pues lección aprendida un poquito para que sepamos los problemas de las contraseñas por defecto Esta es una noticia que ilustra ese riesgo a todos los públicos aquí vendría muy bien la frase típica de nos comen los chinos Pues a través del routers los pandas porque según la noticia dicen que esto es el Panda Mustang no que la hemos combinado los animales o sea eso es lo que decía lo que decía el code name no que común para este apt Pero insisto según checkpoint es uno nuevo o sea tiene muchas similitudes pero pero ciertas ttp son diferentes Entonces ellos le dieron un nuevo nombre que es un poco el nombre que le voy a dar a la noticia que es Camaro dragón Ok pues si los dragones y los pandas bien de China obviamente Así que nos vamos para la siguiente noticia que Bueno él va de semillas de privacidad un futuro incierto e Inteligencia artificial y bueno me meto de lleno el tema es que una empresa que tiene hay una empresa ha salido en las noticias de hace poco que hay una empresa que tiene una moneda virtual llamada Walt Coin la moneda del mundo hasta aquí Cualquiera podría decir que es otro día más en el mundo de las criptomonedas no han habido cientos y cientos de criptomonedas que han salido y que se han hundido Pero bueno las más famosas Obviamente que se han quedado son bitcoin ethereum tester y todas estas no pero leyendo la noticia cuenta de que esta empresa llamada tools for humanity o herramientas para la humanidad en español y que recientemente ha salido en una noticia porque ha vuelto a recaudar más fondos en este caso 115 millones de dólares en la serie C de inversiones tiene pinta de tener planes de control global de la población y su plan en tres actos es el siguiente primer acto crear una moneda global con la intención de que valga más que el dólar americano y que de hecho sustituya a todas las demás monedas Fiat normales o virtuales criptomonedas y de ahí el nombre welcoin en el segundo acto tienen la intención de utilizar un identificador único y global para cada uno de los más de 8 billones de personas en el mundo llamado Wall ID

y acto III su objetivo es desplegar una plataforma online de aplicaciones web y aplicaciones móviles en la que se pueda utilizar la moneda Welcome para poder pagar por servicios y bienes es decir que quieren registrar a todo el mundo en su sistema para que su sistema valide autentique a todos los usuarios y que ofrezca una moneda que la van a poder utilizar en sus plataformas para comprar productos a través de ella así que todo el mundo va a tener que usar su plataforma para vender el objetivo de World Coin cuya empresa matriz como digo es tools for humanity es catalogar a cada individuo mayor de 18 años a través de un protocolo que según ellos respeta la privacidad vamos a ver si cuando os cuente lo que como lo hace estáis de acuerdo con este comentario o no el proyecto utiliza un dispositivo llamado orp en inglés una orbe digamos en español que escanea el Iris del ojo de una persona y convierte la imagen biométrica en un código que la empresa llama Iris code o código del Iris este código se asigna a cada persona y permite verificar su identidad la orbe es un objeto redondo con tres sensores dispuestos en forma de triángulo esta esfera se ve como una de esas bolas mágicas número 8 que se pusieron de moda hace ya un tiempo no si tú las has visto alguna vez Martín esas que agitabas y le decías bola bola me responder a esta pregunta o algo así como en plan el futuro y te mostrará un mensajito ahí en una mini ventana de cristal supuestamente en respuesta a tu pregunta no sé si sí sí eso o sea yo las he visto en series americanas que es una versión más cara y más coñazo de tirar la moneda No sí porque te decía sí o no sí sí o no poco más porque no no cabe más dentro de la bola Pues esta orbe tiene un aire también si veis la imagen que vamos a poner un enlace a la noticia que tiene tiene fotos de la orden incluso la hemos puesto en la imagen de del episodio también para que la veáis un poquito Aunque es bastante pequeña pero si la veis tiene un aire 9000 de la película 2001 uno dice en el espacio y cuando escanea un nuevo usuario parpadea con luces blancas y rojas un espectáculo así muy de ciencia ficción de película hollywoodiense yo creo que las lo de las luces blancas y rojas no no haría falta Supongo lo han hecho un poco para hacer más más espectacular pero igual le sirve a la operador de la bola para saber si se ha registrado bien o no pero pues nada a partir de aquí tiene la plataforma tienen el dispositivo para registrar esos usuarios Martín Cómo crees que convencieron a los usuarios para registrarse porque tú irías y te registrarías en esta plataforma a ver en principio para empezar Ya viene como bien tú dices infectado con el tema de las criptomonedas es que es y ya lleva el tufillo a estafa no o de alguna manera Hay algo esto soy yo que a lo mejor pero a mí hoy en día me hablas de criptomonedas de fiats de nfts y de tal Es que es muy difícil que me lo tome en serio Y esto es un vayas mío no quiere decir que sea correcto pero entonces no La respuesta es No y me imagino que el incentivo dado que estamos hablando de una moneda y la moneda se la crean por sus por sus a ver me sale por sus huevos morenos pero ya os que se lo sacan de la manga eso es lo que quería decir es pues lo que te incentivan es con eso que te dan parte de su moneda no un ico o algo así un inicial con offering o cualquier historia correcto correcto a la mayoría les ofrecían una recompensa de 25 Wolf coins pero como dices como dices actualmente no vale nada vamos a meternos tierra de hacker Coin y mira mandarnos fotocopias de vuestros pasaportes y os damos 500 de tierra hacker coins venga pa'lante sin fallo un certificado de ser oyente que apoya el podcast pues Bueno pues eso que pretenden que te registres en su plataforma que les des tu Iris sin darte un duro que al menos te den una tarjeta de regalo no con 50 dólares o algo sería algo mejor pero de hecho comenta la noticia que han hecho otras otras simulaciones de cómo captar a usuarios supongo que el tema de 25 welcoins no les fue muy bien y estaban dando también en bitcoins o incluso tester e incluso también airpods digo Bueno si si me das igual algo así un airpod igual te vale 200 dólares ya ya estamos hablando de cositas guapas ya luego ya te cambiarás el ojo no el Iris Te lo actualizas Claro claro bueno eso voy a entrar en breve a ver el cambio de Iris pero aún así también decían que no era suficiente porque porque Martín cuánto vale tu

privacidad la mía la mía es impagable tío es como como el arte de que te puedes encontrar de esto de valor incalculable Pues lo mismo como la de mastercard no para todo lo demás mastercard no tiene precio pues Welcome esta empresa se lanzó en 2021 porque no es nueva digamos a finales de 2022 su objetivo era haber registrado a entre 20 y 30 millones de personas utilizando 6000 orbes en todo el mundo suena pero si no hay tanto airpods como como si al final la culpa es de Apple tío que no consigue hacer justo justo Pero sabes lo que pasó que justo llegó el cripto invierno o el cripto Winter del 2022 no Y supongo que nadie ya quería ni un token que no valiera nada el World Coin obviamente ni otros tokens como bitcoin al tercer que estaban bajando ahí has dicho algo muy gracioso y gracioso porque es cierto como llegó el cripto invierno Ya nadie quería una moneda que no valía nada porque antes sí es que es verdad tío el que antes a ti te va moneda no sé qué moneda no sé cuánto ostras le veías un valor tangible ahí tío espectacular Y es que es tal cual tío es tal cual justo Pues la verdad que se han alineado unos cuantos temas aquí unas cuantas unos cuantos imprevistos y debido eso al cripto invierno y tal y la un poco la falta de interés hasta la fecha Welcome solo ha registrado a 1,4 millones de personas teniendo entre 100 y 200 orbes operacionales al mismo tiempo sí sí son bastantes pero no llegan a los 20-30 millones que esperaban pero sí 1,4 millones de personas han dado su Iris ahí por nada por una moneda que no vale nada porque o sea tú puedes hacer un trading en yo que sé en coinbase o o algo de esto de la worldcoin o ahora mismo no la puedes intercambiar por nada No yo creo que es que no ni lo han lanzado le han dado como un hay hoy uno de esos no en plan un tiquetito y cuando lancemos Sí cuando lo hacemos por el Iris te dan un papel de un pagaré de una moneda que no vale nada esto ya es el siguiente nivel tío lo siguiente ya sería no una promesa de que te doy un papel para que en algún momento te daré algo que no vale nada es que ya la desfachatez tío alcanza unos niveles que es espectacular Pues sí sí sí sí sí y a pesar de todo esto Ok se estima que cada semana unas 40.000 personas son escaneadas no por esta por el tiempo que lleva la empresa viva y la cantidad de personas que lleva hasta la fecha y haciendo cálculos a esta velocidad si no incrementa el para que su plan sea fructífera y exitoso y registran a todas las billones de personas del mundo necesitarían 4.000 años para que para conseguir a que todas las personas a esta a este ritmo actual Aunque la empresa dice que todavía no está operando A todo gas así que bueno y a principios de 2022 justo antes del cripto Winter Habría que ver ahora cuánto vale Supongo lo mismo porque su moneda no valía nada la empresa tenía una valoración de 3.000 millones de dólares Así que no es una empresa porque empecé diciendo que han recabado 115 millones de dólares que dice Oh es bastante pero es que tiene una valoración que es bastante increíble que a lo mejor es literal increíble o sea esa valoración porque yo recuerdo que ftx de la que hablamos aquí tenía una valoración del copón pero realmente luego se mirabas su libro de cuentas aquello no no había por donde cogerlo Sí la verdad inflado por dentro y por fuera se ve se ve se ve venir no se ve que va a explotar La burbuja Pues también como he dicho el otro servicio de verificación ofrecen aparte de la moneda ofrecen un servicio de verificación de identidad que lo llaman Walt ID Esto es para evitar el fraude que últimamente estamos viendo con tanta Inteligencia artificial no que se pueden suplantar y falsificar voces imágenes y vídeos Pues esta empresa walcoin va a ofrecer el Wall ID o identificador mundial un servicio de verificación de identidad basado en los datos biométricos captados durante el registro y escaneo de los usuarios en este caso el Iris de los ojos no del usuario pero quiero también hacer una breve mención a otras formas de verificación biométricas no por ejemplo tenemos el reconocimiento de voz que es probablemente la forma biométrica más fácil de falsificar ya que existen empresas de Inteligencia artificial como Eleven labs.io a las que les das unos segundos del audio de una persona y pueden recrear cualquier texto con la voz de esa persona efectivamente falsificando la voz y esto lo hemos comentado

en episodios anteriores de forma de rebote digamos no pero sobre cómo fibra delincuentes han llamado a padres o madres y suplantando de sus hijos les han pedido dinero o algún tipo de extorsión Sin que los padres se dieran cuenta de que la voz la llamada era de alguien falso de un ciber delincuente No pues nada más lejos y antes de su evento de World White developer Conference de este año de hecho fue ahora esta semana en junio Hace unos días Apple presentó un conjunto de funcionalidades de accesibilidad que llegarán en septiembre con el iOS 17 una nueva función llamada voz personal atención permitirá a los iphones y ipads generar reproducciones digitales de la voz de un usuario para conversaciones en persona y en llamadas telefónicas facetime y de audio la tecnología se llama Live speech y requiere que el usuario grabe 15 minutos de audio para generar su voz en el dispositivo a partir de cualquier cualquier texto que se le ofrezca así que ya está al alcance de cualquiera falsificar voces realistas porque es bastante probable que se puedan encontrar 15 minutos de audio de personas en redes sociales o si no te llevas el teléfono y le vas a charlar algún desconocido que quieras atacarle digamos y suplantar su voz y tienes el teléfono ahí y grabándolo y 15 minutos de hablando de cualquier tontería Random y ya tienes su voz y con el iPhone que cualquiera tiene un iPhone actualizas la última versión la 17 cuando salga en septiembre y Listo ya puedes suplantar voces luego tenemos el tema de las huellas dactilares que son bastante fáciles de evadir y hay películas hollywoodienses en las que se obtiene la huella dactilar de un vaso y luego la rehúsan en un plástico que se pone encima del dedo y son fáciles de cambiar con operaciones de cirugía pero no sé si has visto eso tú Martín que a mí se me ocurre alguna película de estas que tipo espía va a coger el vaso y del vaso saca ahí la huella dactilar y luego se la pone en un plástico ahí y luego ya funciona Te lo saltan luego tenemos el reconocimiento facial que es fácil de evadir con una cirugía bueno eso de fácil tienes que someterte a la cirugía igual primero no pero más fácil es con fotografías no han habido noticias como investigadores de seguridad han utilizado fotografías online de personas creo que fue incluso con la la Merkel a la presidenta de Alemania no en que cogieron su creo que fue su cara y con cogiéndola de internet pudieron saltarse o pudieron probarla digamos con contra un sistema de biometría de identificación biométrica de reconocimiento facial y luego tenemos el reconocimiento de Iris la forma de identificación biométrica probablemente más difícil de falsificar porque no te puedes cambiar el Iris y falsificarlo esto hasta el momento ha probado imposible Aunque todo depende de lo bien diseñado que esté el sistema porque en la conferencia de keos computer club de 2014 la número 31 un investigador mostró cómo pudo saltar selectores de verificación biométrica incluyendo lectores de Iris utilizando una imagen de alta resolución de los ojos de la víctima así que aunque no es posible cambiarse el Iris sí que es posible digamos falsificarlo con una imagen de nuevo todo depende de lo bien diseñado que esté el sistema volviendo a Wall ID la empresa Welcome que es la que ofrece el servicio walla ID se unirá o reemplazará a los nombres de usuario y contraseñas los usuarios que hagan login en distintas plataformas online utilizarán las World Apps de Wall ID probablemente unos proveedores de servicio de identidad Esto traduciéndolo me lo imagino como cuando vas a hacer cuando vas a entrar alguna página online que permite hacer login con otras otros proveedores otras páginas digamos Google o Facebook por ejemplo No pues van a Añadir una opción adicional que diga hacer login con Wall ID y luego de alguna forma se conecta con Wall ID y te autentica aunque esta parte de como tú te autenticas contra World desde tu propio ordenador o desde el ordenador que estés utilizando no me queda Clara a no ser que Wall ID de proporcione un escáner de Iris fabricado por ellos mismos para que lo conectes a tu ordenador sabes tipo como cuando usas una smartcard para autenticarte en algunas páginas web online como con el dni electrónico español pues bueno no sé está por ver esto no comentan realmente como lo hacen pero bueno y voy a entrar en temillas de problemas de privacidad obviamente porque walcoin ha recibido

críticas por preocupaciones de este tipo el proceso de escaneo del Iris y la creación del Iris code único han planteado preguntas sobre cómo se gestionan y protegen estos datos además la idea de tener un World ID que demuestre que no eres un Bot que no eres falso un producto de la Inteligencia artificial también ha generado preocupaciones sobre la privacidad online tools for humanity insiste que en el futuro el proceso será completamente de código abierto y dirigido por la organización sin fines de lucro World Coin foundation en dos investigaciones publicadas en abril de 2022 por basfit news y el mit Tech review los periodistas alegaron que las pruebas de World Coin en países en desarrollo estaban plagadas de promesas engañosas tanto para los operadores de la orbe que son los que atraían a los usuarios para que se registraran en la plataforma como para los mismos participantes o usuarios que se registraban otras acusaciones incluían violaciones de leyes de privacidad e incluso corrupción el ceo de World Coin calificó la cobertura periodística de injusta y agregó que los problemas surgieron debido a que la empresa todavía estaba en fase de pruebas beta y enfrentaba enfrentaba dificultades naturales en el proceso mi opinión es que con tal calibre de empresa y estos objetivos de grandeza no objetivos mundiales y además el tipo de datos sensibles que usan el Iris de las personas esta empresa walcoin no sé no puede justificar estar en fase Beta para escaparse de las críticas si eres una empresa de tan de tan de tanta importancia no puedes ponerte a diseñar el producto Y su seguridad sobre la marcha según walcoin el proceso sea perfeccionado para garantizar una privacidad total después de captar el Iris de una persona los datos biométricos nunca salen de la orbe y se convierten en el Iris code que sólo se utiliza para crear una verificación de la singularidad de una persona a través de un sistema complicado de pruebas matemáticas que si queréis igual lo podéis leer en su web son temas de cironolex y proton sharding que no vienen no lo vamos a explicar porque requieren tiempo los principales inversores insisten en que el aire scode no se puede revertir para reconstruir la imagen de un Iris al menos por el momento El problema es que leyendo los documentos del kit de prensa de la web de la web de worldcoin comentan que recopilan la siguiente información atención vídeo y fotografías de alta definición de tu cuerpo rostro y ojos incluyendo tu Iris visibles y con infrarrojos detección de radar de movimiento sin contacto de tu ritmo cardíaco respiración y otros signos vitales y además mapeo tridimensional de tu cuerpo y rostro qué opinas Martín de toda esta información para qué quieren un modelo 3D de tu cuerpo si si tu cuerpo además cambia Bueno te van a identificar cuando él tiene 24 que cuando tienes 40 Esto es para para Apple que anunciadora sus gafas y tal todos necesitamos un avatar no en el mundo virtual que es donde vamos a vivir todos Alexis es por eso hombre es por eso y justo Pues a ver Vamos a ponernos siempre a veces nos queremos poner de las dos partes no poniéndole un poco de la parte de Welcome digo Bueno no está mal recabar tanta información porque en caso de que digamos Dios no lo quiera pero un usuario pierda ambos ojos Cómo se autentica ahora Supongo que walla ID usaría los otros datos biométricos Porque ya no tiene Iris esa persona Aunque ninguno es tan único como el Iris y todos los que he mencionado la forma de tu cuerpo el ritmo cardíaco respiración y todo lo demás eso varía a lo largo de los años Así que no sé yo creo que el world para personas sin ojos no valdría y aparte yo algún sábado que he llegado de fiesta creo que mi ritmo cardíaco Iris mi temperatura o sea todos los factores todo todo el analytics tío fallaría o sea digan pero este pavo Quién es suelo suelo cambiar de noche eres otro otro animal pasas de Panda a Mustang a dragón Pues ahora una pregunta te voy a hacer Martín ahora como tú dices a veces hemos dicho plot twist a que no sabes quién está A ver si me puedes adivinar quién está detrás de tools for humanity y World Coin a no ser que ya lo hayas mirado antes pero si no lo has mirado que creo que No no lo he mirado quién está detrás a ver por un lado diría alguna agencia de inteligencia rollo nsa FBI Pero me imagino que será una empresa privada un holding o algo así no sé tío pero seguro que esta relación con china

alguna empresa china me voy a aventurar vale vale no hablo de la empresa privada que quedaba bien y de hecho es que tú Sur humanity tiene dos fundadores uno de ellos no tiene importancia y el otro es Sam Víctor el ceo de openi flipa el creador ostras Y es que claro ostras Ahora como si te queda el cuerpo temblando digo temblando a ver por un lado él tampoco tiene de momento toda esa mala fama pero es verdad que por ejemplo hpt en términos de privacidad Pues iba un poco corto y Pero bueno tampoco es aquello de yo dije Peter que ya entre el famoso creador de PayPal pero que tiene ahí en palantir ha creado otras acciones o otras empresas muy relacionadas con temas de espionaje claro ahí ya me saltarían todas las alarmas pero pero claro con el este tío de chat gpt pues dices tú joder Qué guapo pero claro por otro lado sigue siendo información súper confidencial confidencial Perdón súper sensible Sí es que este Sam altman ahora con chat gpt openea que es la empresa que ha conseguido el que ha tenido la tasa de suscripción la más rápida de la historia que no sé cuántos millones de usuarios tiene ahora con esta nueva empresa digamos que sería como el Google no una nueva de estas empresas que amasa información de todos los usuarios y a saber qué va a hacer con ella No pues quién se beneficia yo me he imaginado un escenario Así un poco rocambolesco no Pues altman podría obtener control total de la población no porque con opening lo que hace es crear el problema de que en el futuro va a haber una Inteligencia artificial o una inteligencia general artificial que cause desempleo y pérdidas económicas y todo eso no y con World Coin Mister altman pretende resolver el problema repartiendo beneficios de las ganancias extraordinarias de empresas de Inteligencia artificial algo que se conoce como la cláusula del beneficio extraordinario o windful Close que es un compromiso asumido por empresas éticas de Inteligencia artificial básicamente que como si la Inteligencia artificial va a causar daño a la economía y a las personas del mundo por quitarle sus trabajos Pues todo eso que ganen de beneficio extraordinario que no creo que esté muy bien definido pues ese dinero lo van a donar de vuelta a Supongo a personas en desempleo o empresas que han quebrado se podría ver como lo que sucede en la industria farmacéutica no como muchas otras pero en la farmacéutica hay empresas que comercializan medicamentos que son adictivos y luego también ofrecen la cura no que son otros medicamentos que ayudan a eliminar la adicción es un poco el tema así O sea voy a crear el problema todo el mundo todo el mundo sabe que Kaspersky que mcafee creaban los virus porque también te crean el antivirus ese iba a ser mi siguiente comentario no que ahí conspiranoias empresas de antivirus que hacen lo mismo Justo a mí mi dentista me recomienda comer dulce es todo el rato para que vaya allí a empastarme y el mecánico también no que le ponga las ruedas que él quiere y el aceite no no te da el cambio de aceite gratis la venta cambiar aceite gratis y sales de allí con la junta de la troca huele vinagre en lugar de aceite Total que en cualquier caso si todo necesitamos World coins porque si es la forma en la que opening va a obsequiarnos con o vas a darnos la recompensa por hacer el mundo Un poco peor debido a la Inteligencia artificial eso significa que la empresa va a tener que todo nuestros datos biométricos Porque nos tenemos que registrar en su World Coin en sus plataformas para obtener esos World coins de recompensa Sabes Así que es como el problema y la solución y al mismo tiempo un pez que se muerde la cola vamos en cualquier caso la empresa dice que debido a regulaciones de criptomonedas en Estados Unidos solo va a ofrecer el servicio de verificación de identidad para los estadounidenses sin ofrecer el token Virtual y esto se puede dar en otros países también comentan vamos que no tiene pinta que vaya a registrar a toda la población porque no creo yo que nadie quiera estar en un servicio de verificación sin beneficio alguno si no le dan unas criptomonedas o sea para todos los millones de americanos si yo Si yo fuera Digamos si estuviera en Estados Unidos y a mí me viene esta empresa y me dice sí Utiliza este sistema de verificación porque es mucho más seguro yo que sé que utilizar Google o Facebook el open ID

este y no me da nada en recompensa y tengo que darle mi Iris pues obviamente no me voy a registrar no no sé el resto de la población pero esa sería mi opinión y por el momento Welcome siguen fase beta y a pesar de que la empresa Espera que en el futuro otras empresas puedan crear sus propios métodos de verificación basados en Wall ID Welcome aún no ha hecho completamente de código abierto su protocolo aunque así lo dicen que va a ser en un futuro pero la mayoría de los esquemas de la orbe están disponibles en github según comentan algo interesante es que la empresa matriz aún no ha publicado la información sobre Se le comenta se le llama esto tokenomics no del proyecto es decir cómo se generarán se generarán y distribuirán las walcoins pero se especula que más del 70% de los tokens se destinarán a los usuarios que se han registrado en World Coin Mientras que el resto irá a tools for humanity y sus inversores el lanzamiento de los tokens Podría tener lugar en la primera mitad de 2023 pero la primera mitad estamos ahí ahí y todavía no ha salido nada así que los que se hayáis registrado si hay algún oyente que se ha registrado esto por favor nos interesa nos interesa nos interesaría saber vuestra experiencia así que enviarnos algún mensaje y sin Nos gustaría saber Cómo cómo fue el tema y que os han ofrecido Y qué opináis al respecto y con esto queridos oyentes llegamos a la pregunta del episodio que es la siguiente estarías dispuesto a registrar tus datos biométricos en la plataforma de World Coin para una identificación global a cambio de unas criptomonedas Welcome os damos cuatro opciones la primera es si quiero un identificador global la segunda es Sí porque quiero las walcoins la tercera es no de momento no me espero voy a ver que como sigue el tema y la última es no basta de gran hermano la mía creo que queda bastante después de haber dicho aquello de no me dan un pagaré de algo que no vale nada para que dé el Iris claro no había pensado que a lo mejor algún oyente si son 1.4 millones y que lo ha dado O sea mis disculpas no pretendo ofender a pero quiero pensar que no vamos a tener ningún oyente entre ellos ahora a la hora de darlo a ver que Estaría muy bien ya hubo intentos como rollo Open ID para hacer sistemas de autenticación globales lo que pasa es que no basados en datos biométricos ahí es donde está el gran error datos biométricos que insisto no podemos cambiar si te roban la información ya sabemos que no vas a poder cambiarte el ojo Entonces eso es un problema no es una contraseña que puedas cambiar a ver si si el sistema es lo que dice snowden decía Oye están utilizando nuestro cuerpo como si fuera un ticket como si fuera un password no es el cuerpo completo que no me lo puedo cambiar pero me si algún ciber criminal de estos tipo película No si el sistema de biométrico está súper bien diseñado y no te lo puedes saltar con una foto qué van a hacer o te secuestran y te llevan cerca para poner tu ojo ahí o te arranca en el ojo de cuajo no como en las películas hollywoodenses y similares sí había dónde era que con un boli creo que era una de silvester Stallone que la arrancaba el ojo con un bolígrafo y Lo ponía delante del lector sí está Wesley snipes en esa creo propicios no sí de Mauricio Man Sí sí esta que es en el futuro propicios días porque no podías decir palabrotas insultos y tal si no te llevas una un insulto pero eso es verdad pues bueno queridos oyentes yo creo que ha estado muy interesante hoy seguimos en el tema de la privacidad muy fuerte y en el tema chino por un tema bastante recurrente Y por eso es tan útil cuando ponemos tags a nuestros episodios así que ya sabéis siempre lo tenéis en nuestra página web si os queréis pegar un maratón de China o un maratón de todas las maneras en las que están utilizando nuestra información biométrica con usos como mínimo cuestionables sea como fuere recuerda darnos un like por ahí sobre todo compartir el podcast y por favor dejarnos esas estrellitas y comentarios en la plataforma de podcast que nos estés escuchando si no estás suscrito aún suscríbete y muchas gracias por seguir siendo fiel a tierra de hackers Muchas gracias lo mismo que ha dicho Martín dejarnos esas estrellitas como Mario Bros en el videojuego clin clin clin y nada no escuchamos en el próximo episodio 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 una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de tierras