un grupo de ex agentes de agencias de inteligencia israelís comandados por una persona que se hace Llamar Jorge ofrecen servicios de manipulación a ciudadanos para interferir en elecciones democráticas documentos filtrados por el grupo jardista guacamaya resultan contener presentaciones sobre una empresa llamada s2t & locking Cyber space que ha estado ofreciendo servicios de inteligencia web espionaje y desinformación a países como Colombia India y bangladesh para atentar contra periodistas u opositores del gobierno vota así al conocimiento vota así a un nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 6 de enero de marzo de 2023 este es el episodio número 85 yo soy Martín vigo el primer paso que estoy equivocando en lo que siempre repito y está conmigo pues Alexis porros así sin más ya para no equivocar qué tal Alexis sí sin más y más a ver vamos a vamos a un poco de vamos a ver dónde estamos sé que esto que es tierra de hackers o el noticiario de Bueno de hecho es un noticiario Así que bienvenido noticiero noticias me equivoco yo también macho noticiero el noticiero de la hora en la que lo estés escuchando querido oyente Pues nada sí estamos en marzo ya pasa el tiempo volando Así que nada le damos caña para para no seguir entreteniendo los más y como siempre queremos dar comentar lo importante y lo primero es daros como siempre las gracias queridos oyentes por seguirnos apoyarnos enviarnos comentarios mensajes sugerencias que hacer en los siguientes pasos para llevar tierra de hackers al más allá o como diría Buzz Lightyear hasta el infinito y más allá Pues de nuevo Muchas gracias por seguirnos ahí online apreciamos mucho a vuestros comentarios y sugerencias y también os queremos recordar que nos podéis apoyar suscribiendoos a nuestro podcast en vuestra plataforma de escucha favorita estamos en todas creo que las que más populares que se usan así que por favor ir a suscribiros para sobre todo para que recibáis las nuevas noticias de ciberseguridad que comentamos y estéis ciberseguros luego voy a pasar al tema de redes sociales quiero comentar que estamos en Twitter infoset.exchange Instagram y Facebook con el handle@tierra de hackers linkedin YouTube y Twitch estamos ahí como tierra de hackers los correos electrónicos no los podéis enviar a podcast arroba tierra de hackers y también estamos en discord podéis entrar a nuestro servidor de discord a partir de tierra de hackers.com/di discord y finalmente como siempre agradecemos vuestro apoyo a la pregunta del episodio que publicamos en Twitter y que fue la siguiente qué fuente adicional de información podría ser la siguiente que empresas Como auror pudiera Añadir a sus plataformas de vigilancia os dimos en este caso dos respuestas y la más votada fue datos de salud con un 56% muy seguida de datos de emociones con un 44% Así que vemos que no nos decidimos de cuál va a ser la siguiente que van a incorporar pero ambas probablemente puedan dar mucho juego a este tipo de empresas para rastrearnos y abusar de nuestra privacidad de rastreo de rastreo vamos a hablar de largo y tendido hoy yo como siempre y muy rápidamente para no enrollarnos darle las gracias a nuestros mecenas de patreo que son los mejores del mundo mundial acabo de venir ahora de dar unas charlas de dar unas charlas madre mía como estoy de ir a ver unas charlas al Microsoft Security day y me encontré allí con uno de nuestros mecenas Jordi que encantado de saludarle y con otro oyente en el mapa de World Congress Sí bueno había era un evento Así que estaba parte del Mobile satelital estaba orbitando en torno al fira de Barcelona pero como siempre genial y luego también otro oyente que vino vino a saludar y hacerse una foto y nada yo encantado como siempre evidentemente faltaría más sí quiero que sepan los oyentes que tanto Alexis como yo tenemos más de una camiseta porque como siempre aprovecho a ir a todos los eventos con la camiseta de tierra hackers Porque es que me he dado cuenta claro a ver es un podcast no a pesar de que hacemos algo de Twitch y tal la gente no me reconoce por la cara me reconoce por la camiseta Y como me hace mucha ilusión que la gente venga a hablar con conmigo y tal y cual Pues claro me veo forzado a llevar

la camiseta de tierra de hackers constantemente pero tengo más de una eh va nada valada Sí sí Yo también yo también así que pero siempre lo que te decía estamos preparando un poquito este episodio antes y le decía Martín que sabes en esas en esas ocasiones que no puedes llevar la camiseta así visible que vas con traje o algo así pues la llevas debajo estilo Clean Y si alguien no sé por ahí tienes que enseñar su identidad les sacas la barriguilla y me enseñas el logo fuiste a hacer daño cabrón Cómo que la barriguilla que tienes toda la razón lo dije con cariño lo dices por mí lo dices y con razón estamos trabajando para verano ya no hay ya no hay barriguilla bueno que he dicho que no me iba a ligar Gracias mona Muchas gracias una empresa que comparte los mismos valores que tiene hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y mona con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y buscando ingenieros con experiencia en ciberseguridad para ayudarles y construir y hacer realidad su misión ya sabéis contratan en todo el mundo y les podéis contactar en tierra de hackers arroba monat.com que así saben que vinisteis de nuestra parte y también queremos darle las gracias a brawler Pro por apoyarnos en el podcast es la herramienta más completa de seguridad en aws empresas de todos los tamaños se apoyan diariamente en brawler pro para que sus equipos puedan confiar en su modelo de seguridad de 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 visión holística de tu infraestructura aws en cualquier región y tendrás todos los resultados en apenas unos minutos empieza a usar brawler pro y descubre los resultados de tu primer escaneo gratuito visitando tierra de hackers.com barra para oler Pro PR o w l e r p r o y brevemente mencionar nuestro sorteo que seguimos con las entradas para la ruta que es para la semana que viene Gracias por ir contestando os preguntábamos os pedíamos no tanto os preguntábamos que recomendáis el podcast a alguien que genuinamente creíais que debería estar escuchando el podcast Muchísimas gracias por todas esas respuestas todavía no tenemos al ganador pero lo anunciaremos como hemos estado haciendo en redes sociales así que de Tú tranquilo que si has ganado te vas a enterar y para sortear la última entrada que tenemos que yo creo que la pondremos antes de que publiquemos este podcast porque lo tendría que hacer ya porque la conferencia es para la semana pues se me ocurrió preguntaros que contestéis cuál fue vuestro episodio favorito del podcast Cuál ha sido ese episodio que habéis dicho me ha flipado de lo que has hablado ha sido la leche o me ha sorprendido Así que contarnos porque así también un poco sabemos no Alex la temática que le suele gustar a la gente si es más cuando cubrimos papers cuando Alexis te cuenta una vulnerabilidad nueva cuando te hablamos de El espionaje de turno de la nación de turno Pues cuéntanos cuál es tu episodio favorito contestando al post que hagamos en redes sociales y con eso ya participas en la en la última entrada para la router y no podemos al lío no Alexis Sí sí iba a decir que es esa es una muy buena un buen dato para nosotros Claro para validar realmente De hecho también si las plataformas de podcast nos están dando los números bien o no en plan el episodio más escuchado fue el número x y luego la gente viene y me dice no si el que más me ha gustado es el y Ok pues algo algo aquí correcto correcto sería buen dato siempre es bueno telemetría Vale pues yo vuelvo a la carga con otra investigación de forbidden Stories bueno en conjunto en este caso con el diario de Guardian pero la semana pasada todo lo que os conté esta esta Crazy Story de eliminalia ya venía de esta serie de investigaciones por parte de esta organización sin ánimo de lucro francesa forbidden Stories que se está centrando en destapar escándalos de desinformación que empezó a raíz del asesinato de un periodista llamado gabrielantes a causa de sus investigaciones precisamente respecto a campañas de desinformación Pues bien os vengo a hablar de desinformación otra vez pero desde otro ángulo elecciones presidenciales votaciones y democracia os acordáis del

escándalo de Cambridge analítica es importante porque esta investigación de la que os voy a hablar se nutre del reminiscente que quedó del caso de Cambridge analítica las partes no que aún tras la investigación quedaron ocultas si os acordáis Cambridge analítica era una empresa británica donde utilizaron información de millones de ciudadanos que extraían a través de encuestas no falsas reales de que las ponían en redes sociales pero que no tenían el propósito que se supone que tenían en ese sentido me refiero a que eran falsas para extraer información digamos personal sobre la personalidad Mejor dicho de las diferentes ciudadanos para así poder ayudar a su cliente para poder digamos diseñar una campaña en torno a eso es decir Cambridge analítica fue contratada para averiguar y alterar la intención de Voto hacia un candidato específico a través de la extracción de información de ellos con encuestas falsas y hay un documental muy bueno en Netflix donde lo explica todo Pues bien gracias al ex director de Cambridge analítica y que se convirtió de hecho en uno de los weezer bloggers que denunció las malas prácticas sabemos que Cambridge analítica colaboraba con y digo entre comillas porque es así como lo dijeron ciertos hackers israelíes estos hackers entre comillas estaban a cargo de lo que llamaban ellos oposition research o Dicho de otro modo investigaciones de los oponentes esto qué quiere decir pues Cambridge analítica subcontrataba los servicios de extracción de información de los oponentes políticos de sus clientes para como veremos más adelante empezar campañas de desprestigio y presión contra ellos ya en 2018 se publicaba en la prensa que estos hackers entre comillas insisto israelíes misteriosos llegaban a la oficina de Cambridge analítica con pinchos USB llenos de emails privados de políticos que claramente habían sido hackeados de alguna manera en aquel caso mencionaban que habían llegado con información personal del futuro presidente de Nigeria como uno de los ejemplos que daban por tanto Cambridge analítica no solo expuso el mundo al hecho de que unas elecciones pueden ser perfectamente manipuladas mediante la distribución de información falsa para influenciar la intención de voto en la población sino también nos dejó El pequeño dato de la existencia de un grupo de individuos israelí desconocido de hecho en uno de los emails filtrados de Cambridge analítica el propio fundador Alexander knix hablaba de israelí Black Ops o operaciones negras israelí y o grupo de operaciones negras israelí Mejor dicho en este contexto y no se refiere a ello con una persona como a una persona o una empresa sino en el email se refería a él como atención Tim Jorge Sí sí el equipo Jorge Jorge como el nombre español no George es como el fundador de Cambridge analítica se refería a este a este grupo israelí no Así que ahora tenemos un pelín más de información no solo conocemos la existencia de un grupo de israelís que se dedicaban a la manipulación de la gente para alterar resultados de elecciones sino que sabemos que al líder le llamaban Jorge Y quién es este Jorge Pues eso es lo que se pusieron a investigar la gente de forbidden Stories concretamente durante cinco años que tardaron pero que fueron capaces de dar con la identidad de este Jorge que es un entre comillas consultor sobre el papel Claro que todavía sigue usando como apodo Jorge a día de hoy pero que en realidad se dedica a vender sus servicios de influencia y manipulación a quien más le pague evidentemente hace uso de herramientas propias como la generación de post virales de manera automática utilizando Inteligencia artificial o el hackeo a cuentas de Telegram algo que la verdad me sorprendió bastante porque no sé exactamente cómo lo llevan a cabo pero como veréis más adelante fue una de las demostraciones que hicieron yo me imagino que quizá va por el tema de quizás hackeo de buzones de voz que yo en su día Pues de una charla sobre eso Aunque es verdad que en un vídeo que os dejo en las notas del episodio donde salen las reuniones ocultas de las que os voy a hablar a continuación se menciona el famoso ss7 que cuando os cuente quién forma parte de este grupo de israelís veréis que tiene sentido que tengan acceso al sistema ss7 que es un protocolo de telefonía que quien tiene acceso a eso Pues digamos que puede ver el contenido de mensajes puede podría incluso

llegar a Escuchar llamadas y cosas que os hemos hablado en el pasado y que ya existen charlas en conferencias como la ccc y Black hat sobre esto y cómo hizo forbidden Stories para dar con esta persona que os mencionaba Y averiguar detalles sobre los servicios que ofrece Pues la verdad es que hicieron algo muy guapo ingeniería social llegar a Jorge no es sencillo pero haciéndose pasar por potenciales clientes en concreto se hicieron pasar por un representante de un país africano buscando que unas elecciones se retrasasen o incluso se llegasen a cancelar pidieron a gerge una demostración de sus servicios para esto como decía tuvieron que pasar por muchos intermediarios hasta llegar a poder hablar con él directamente porque evidentemente no tienen una web donde puedas ir y contratar los servicios de manipulación de elecciones democráticas No tuvieron que hablar antes con los oficiales de agencia de inteligencia expertos en comunicaciones e incluso empresarios en el sector de la ciberseguridad todo esto para llegar a poder hablar con Jorge pero una vez lo consiguieron y le pidieron que que lo que necesitaban era retrasar unas elecciones en un país africano incluso llegar a cancelarlas el precio que les dio fue 6 millones de euros que yo no sé qué opinas tú Alexis pero 6 millones de euros por Cancelar unas elecciones en un país me parece regalado Sí sí Comparado con con el dinero que te deberías gastar en policía y similares es bastante barato Es que para el presupuesto de un país Aunque quizás se trate de un país subdesarrollado africano 6 millones de euros no es mucho dinero cuando puedes hacer que cuando el resultado puede ser que te elijan a ti en vez de a tu contrincante político y convertirte tú en el en el presidente del país los periodistas no solo consiguieron tres reuniones online con Jorge y su equipo sino una cuarta persona en sus oficinas de Israel donde además les hizo varias demos Y es ahí donde tenéis que ir a ver el vídeo que os dejo las notas del episodio y de hecho es de aquí de donde los periodistas sacaron toda la chicha Jorge les comentó que sus servicios Se basaban básicamente en la inteligencia Y la influencia Y que aparte de las capacidades técnicas de las que disponía era un maestro en crear una narrativa y distribuirla masivamente mediante sus servicios que incluyen atención vodnets distribución a escala de información falsa y hacking a oponentes ahí lo tenéis chavales el full equip no el servicio completo necesario para alterar las elecciones de un país pero lo mejor viene cuando como buen vendedor Jorge se puso a alardear de proyectos anteriores Y de clientes anteriores para los que había sido contratado Como por ejemplo un escándalo que hubo en Francia que terminó con el despido de un presentador muy famoso de las noticias del Canal bfm TV el cual distribuyó noticias falsas en televisión que habían sido planeadas por Jorge en concreto que Europa había lanzado un nuevo paquete de sanciones contra Rusia y que en Mónaco las empresas dedicadas a las construcciones de yates estaban muy preocupadas por el impacto financiero entiendo que esto era para un poco dar la sensación de que las medidas que están tomando en Europa estaban perjudicando no solo amónicos sino en general Pues a Francia no por la cercanía esto era mentira y el presentador de hecho fue despedido y aquí tenemos a Jorge diciéndole a estos periodistas encubiertos que él tenía la capacidad de implantar noticias falsas en medios de comunicación franceses y poniendo este caso como ejemplo O sea que ya no hablamos de simples blogs falsos en internet no que esta empresa pues se dedica a postear automáticamente hablamos de que esta gente manipula y tiene a sueldo Así es como lo dice forbidden Stories No yo Ha presentadores de noticias en televisión y a periodistas a sueldo con retener Stories menciona que un servicio así puede costar 3.000 euros o sea poniendo el ejemplo de la manipulación del por parte del presentador de noticias insisto es que están de rebajas o sea por 3000 euros de verdad puedes tener a un tío en prime Time en las noticias diciendo una noticia falsa que tú quieras o sea me parece regalado o sea 3000 euros por la posibilidad capacidad de dinamitar tu carrera como presentador en vivo y en directo yo flipo pero esta no es la única manera en la que Jorge puede influenciar a la población de un país

Jorge le comentó a los periodistas encubiertos que tenía herramientas propias que generaban miles de avatares e interactuaban en varias redes sociales para distribuir historias falsas y generar interacciones falsas para incrementar la visibilidad a esta herramienta que evidentemente no es pública le llaman Advance Impact media Solutions o Ice Jorge menciona que tenía 30.000 cuentas falsas en Facebook Twitter Instagram ciertas tiendas online y bueno y bitcoin que esto de bitcoin Pues no sé bien A qué se refiere con cuentas falsas quizás se refiere a que tenía bitcoin en ciertas cuentas para poder hacer pagos Pero bueno ya se hace ya os hacéis la idea de la magnitud del problema 30.000 cuentas que son operadas automáticamente para hacer likes retweets reseñas falsas y todo lo que haga falta con tal de ponerte una historia falsa delante de los ojos por ejemplo una de las historias que contó Jorge en esa reunión es que con una cuenta falsa cuyo Avatar era la imagen de una mujer rubia y muy atractiva compraron juguetes sexuales y los enviaron a la casa de un oponente político de su cliente esto causó que la mujer del oponente pensase que le estaba siendo infiel la historia saló a la luz y acabó perdiendo las elecciones flipa o sea todo lo que hace falta es una cuenta falsa en una tienda online enviarle un dildo con un avatar que me imagino que habría referencia en el paquete a la persona que lo compró por lo que la mujer fue a ver quién era y vio el avatar de Pues de otra mujer que muy atractiva y sugerente Y eso sale a la luz sale el escándalo pierde esa credibilidad de tus votantes y pum se acabó ese es un nuevo una nueva categoría de ataque llamada dildo swatting Igual yo vendí dos por todos lados Oye qué buena eso dildos watting ya te habías inventado aquel término Cuál era el Carl Will no sé qué razón Will y ahora tenemos el dedo de nayalo service of service describete dildo the Night ahí está Pues bueno Jorge quería sus 6 millones y para convencer a los periodistas de la afectividad de sus servicios les propuso hacer viral una historia falsa que ellos quisieran atención y los periodistas aquí con un poco de toque de cachondeo repito los periodistas recordemos que en realidad estaban allí en capacidad haciéndose pasar por clientes le pidieron hacer virar el hashtag RIP Emmanuel con la foto de un emú que un emú Bueno es un animal parecido a un avestruz que esto lo tuve que buscar la verdad la Wikipedia pero para que os hagáis una idea y esto realmente estaba basada en un emmu llamado Emmanuel cuya foto se hizo viral el verano pasado y la idea es que Jorge distribuyese la noticia falsa de que había muerto mediante el hashtag RIP que es resting Peace en inglés Emmanuel pero aquí viene lo mejor de todo y es que los periodistas usaron este hashtag después de que el equipo de Jorge amenazase a la campaña empezase la campaña de desinformación de demostración para encontrar todas las cuentas falsas controladas por el equipo de Jorge esto es buenísimo y gracias a eso pudieron ver que esas mismas cuentas que estaban tuiteando con el hashtag RIP Emmanuel habían estado posteando en el pasado otras noticias falsas en concreto parte de 20 campañas de desinformación por todo el mundo pero la herramienta eins no solo tiene la capacidad de distribuir masivamente exactamente lo que le digas sino que puede hacer mucho más una demo que hicieron mostraba como le podías decir a la herramienta palabras clave keywords y un sentimiento en plan positivo negativo neutro y la herramienta se encargaba de crear post falsos en torno a esos parámetros es decir tú no tienes que idear 300 tweets diferentes sino que le puedes decir Martín vigo podcast tierra de hackers sentimiento negativo y la herramienta automáticamente empezará a tuitear frases coherentes como si fuera una persona normal tuiteando pero negativas sobre mí y el podcast ahí están usando chachi o alguna historia de estas Claro hoy en día estoy seguro que están tirando de apis ya no no han reinventado su historia Claro claro os doy el ejemplo Exacto que usaron de hecho en la demostración le dieron a la herramienta las siguientes palabras clave chat President brother y debbie chat era el presidente de un país y el hermano se llama débil No pues Chad President brother Devil y configuraron la herramienta para que mi teoría 10 tweets negativos Comenta los periodistas que en esta demo en 12

segundos había 10 tweets publicados por 10 cuentas diferentes en Twitter que decían cosas como inaz y naf Winnie to put and Twin competencial of President of chat brother Dave esto viene a ser ya es suficiente tenemos que poner un final a la incompetencia y nepotismo del presidente del hermano del presidente débil o otro era recordemos que esto Se generó automáticamente no lo escribió nadie otro tweet que salió de esta petición a la herramienta era de chat people have software Under the rule of President brother Devil que por cierto me doy cuenta que chat no era el presidente sino que chat es un sitio porque este tweet decía la gente de chat ya ha sufrido lo suficiente bajo la bajo las normas del hermano del presidente devi pues esto ya os digo mientras se hacía este demo de hecho uno de los miembros del equipo soltó la siguiente frase cada operador puede manejar 300 perfiles por lo que en dos horas tenemos a todo el país repitiendo nuestro mensaje o la narrativa que nosotros queramos os voy a repetir esto dicho por uno de los del equipo de Jorge cada operador puede manejar 300 perfiles por lo que en dos horas hago énfasis tenemos a todo el país repitiendo nuestro mensaje o la narrativa que nosotros queramos a todo eso A qué se si estamos diciendo que la herramienta emite esos mensajes de forma automática que haya un humano detrás de tantas cuentas es un poco para echarle un ojo para controlar que haya interacción que todo vaya bien muy buena pregunta lo que yo entendí Es que tú emites todos esos tweets hay gente que interactúa y luego tú pues a eso vas contestando me imagino que ya un humano si quiere si quiere reforzar el mensaje o no pero qué pasa que tiene 300 perfiles a la vez en un dashboard Y es capaz de ir contestando pim Pam un poco como los jugadores de póker que juegan en cuatro partidas a la vez pero tío evidentemente aquí hay un tío de ventas de fondo en una frase así pero en dos horas podemos tener al país repitiendo nuestro mensaje la narrativa que nosotros queramos es una frase muy fuerte tío muy fuerte mucho impacto y porque has comentado un poquito Twitter lo que me hace gracia es que nos quejamos un poco que Twitter está de capa caída Pero sigue estando entre las plataformas top de desinformación Sí bueno si atendemos a lo que dice lo más realmente no creo que esté tan de capa caída en términos de Daily active users no sino más bien de que es un desastre correcto opinión personal que tendremos muchos admiradores de él y Yo admiro a elon en muchísimas cosas no en su gestión de Twitter pero creo que va más por ahí los tiros porque estoy estoy contigo o sea Twitter de hecho yo es la Prácticamente la única red social que utilizo y no quiero que desaparezca y Ojalá funcione y lo haga bien en un Mask si no que me parece súper útil decíamos que no hay nadie perfecto pero que ha tenido un poquito de tema Solo que parecía mucha gente no me voy de Twitter La cierro mi cuenta me voy a más todo un poquito lo que venía pero sí sí sí sí sí a ver más todo tiene sus limitaciones nosotros mismos tenemos cuenta pero pecamos tenemos que integrar ahí sabes seguimos activos en Twitter porque no por preferencia ya nos gustaría pero es que al fin al cabo tenemos que tuitear y que alguien lo vea no Y si estamos era un poco como la historia de google+ cuando salió en competencia Facebook todo muy bonito pero si estás posteando si le estás gritando a una nube No como Los Simpson no sirve de mucho pero bueno sí ojalá ojalá crezca Oye qué Guay que crees que más que crezca más todo Pues mira buen reminder para para que le meta ahí la Api para por lo menos cuando tú tenemos en Twitter también lo hagamos allí total yo te pregunto Quién es este Jorge cuyo nombre evidentemente no es Jorge adivina Alexis si tú le tuvieras que poner un nombre no te quiero dar demasiadas pistas si tú le tuvieras que poner un nombre a un malhechor israelí cuál sería Y ya te he dado demasiadas pistas irland Trust no tío o sea tal tal tío tal cual tal cual se llama tal Jara tío y es que me río porque hace un mes y medio hablamos de Tales dalín o algo así que también era un tío que estaba en esto que de hecho cuando lo leí dije ostras a ver si estoy preparado una noticia que hayamos cubierto pero no Y si te acuerdas hace mucho mes Incluso el año pasado también Había otro tal que era de digo joder si alguien en Israel se llama tal

Empezamos mal Empezamos mal porque ya vamos por el tercero pues ya rima con lo de contar Bueno pues tal de hecho está rodeado de personas Bueno muy curiosas que estaban presentes durante las reuniones con los periodistas trabajando en cubierto o sea por eso por eso sabemos que formaban parte de esto Como por ejemplo Maxi maidan fundador de una consultora de ciberseguridad en Panamá pero que en el pasado fue miembro de los servicios de inteligencia domésticos de Israel que también se conocen como shinbet que yo esto no lo sabía ozuki friedman también exoficial del servicio de inteligencia israelí Y supervisor en Palestina durante muchos años que fue capaz de captar como espía a uno de los hijos de uno de los líderes de jamás o Jacob sedec cabeza de sedec media Group empresa de marketing digital y que él mismo se presenta como experto en publicidad digital muy acorde a todo lo que lo que estaban haciendo aquí osoar hanal el propio hermano de tal hanan que fundó una empresa de seguridad y se anuncia como experto en pruebas de polígrafos que bueno evidentemente aquí tiene que tener está relacionado una vez más con agencias de inteligencia eso es lo que los bolígrafos para escribir en papel dices esos esos como veis un equipo con un pasado y unas capacidades muy interesantes quiero terminar la noticia con una supuesta voy a decir campaña a cargo de esta empresa porque nos toca muy de cerca y una vez más nosotros no entramos en debates políticos Sólo nos hacemos Eco De lo que aparece en las noticias y es el ciberataque a la generalitat de Cataluña sucedida en 2014 esto lo nombró talán específicamente durante la reunión con los periodistas durante tres días la web de la generalitat fue atacada con con ataques de the Night of service sin dildos esta vez junto con la web de la asamblea de la nación catalana Pues según talán ellos estaban detrás de ese ataque de hecho mencionaban concretamente que no habían hecho el ataque más elegante que habían hecho hasta O sea que no había sido el ataque más elegante que que al que estaban acostumbrados a hacer yo dejo ese dato ese dato ahí que me sorprendió bastante la verdad pues porque aquí estamos viendo que a veces hablamos de que si Estados Unidos agencias de inteligencia que si en Países Árabes que si no sé qué pero aquí tenemos una empresa israelí que según ellos y según esta investigación ha afectado de una manera u otra un proceso que ha sucedido en España por tanto nos toca nos toca de cerca esto muy fascinante esta noticia Martín sobre todo por por el poder que empresas privadas no solo ya países y gobiernos que pueden influenciar elecciones pero en este caso es una empresa privada que ofrece estos servicios a cualquier al mejor postor o como digo a cualquier persona porque en este caso un poco vamos en plata digamos que Qué malos son analizando sus potenciales clientes si no pudieron ver que eran periodistas aquí el tema de hackback no de contraataque de estos periodistas para intentar destapar a esta empresa oscura pero no sé tú cómo lo ves Martín que que no hicieran sus deberes e identificaran que ese potencial cliente fuera un periodista tanto que se dedican a la Intel y luego no saben ver que sus potenciales clientes son periodistas me parece un fallo que dice que es que su que sus capacidades no son muy buenas a ver yo creo que yo creo que que hay un par de cosas aquí una 6 millones de pavos que se facturan tienes toda la razón al decir si yo llevo un negocio que es bastante shady bastante oscuro voy a hacer el Duty Legends no voy a revisar pero claro recordemos lo que mencioné no fue les mando un mail los periodistas y ya tuvieron que pasar para llegar hasta hasta el equipo de Jorge tuvieron que hablar con ex agentes de inteligencia políticos empresarios por tanto no llegaba llegaba de primera mano digamos es como si Alexis un cliente me viene porque me lo recomendaste tú entonces ya hay como digamos ahí esa confianza no porque me lo estás dando tú que eres mi amigo entonces yo creo que ahí es donde probablemente bajaron sus defensas aún así lo que dices tú claramente me da igual que venga por ti Que te puedan a ti pero sí y de hecho de hecho ya digo eh está el vídeo ahí tienes que vértelo Alexis los tíos ahí reunidos haciéndole de demos los pagos haciendo bromas hay un momento que hace una broma al tío Porque cuando

le está enseñando la herramienta de einds se ve como un montón de fotos de perfil y el uno de los periodistas le pregunta Ah de dónde sacas esas fotos de perfil porque no están hechas con esto de dispersos no existo tal son perfil fotos de perfiles reales de gente real y el tío le contesta eso no te lo puedo decir tendría que matarte y luego tengo que lidiar con enterrarte le dice con enterarte en medio del desierto no sé qué esto evidentemente en torno jocoso pero ostras yo no sé si estoy si soy un empresario y estoy con clientes no no me no me dedicaría hacer ese tipo de bromas pero sí sí sale en el vídeo Eso sí porque como dices creo que hicieron tres entrevistas virtuales y luego una ya en persona O sea que no sé es en plan correcto Esa es la que está en el vídeo hasta la cocina esto a mí me recuerda un poquito este concepto un poco que está de moda No ahora que se llama Zero Trust en plan Trust pues aquí aquí verificación cero Pero pero bueno es verdad es verdad aquí hubo Trust Mira qué ejemplo más bueno porque de esto de haber estado en el Mobile World Congress de haber estado en Barcelona Cyber Security Congress y todo esto siempre hay charlas ahora deciros topic y tío yo me he dado cuenta que mucha gente no sabe explicarlo yo el primero eh yo el primero que conste y me encanta Este ejemplo tío sé lo que quiere es lo que es cero atrás pues este caso sí básicamente Es lo que siempre se ha estado haciendo para ser más seguro pero llevándolo a un nivel de paranoico digamos así en plan Sí igual confío en ti pero voy a verificar antes de continuar pero anyway lo que también el otro tema que quería comentar de hecho Leí algo leí por Twitter de hecho un post que redireccionaba a mastodon sobre un investigador que mencionaba algo que creo que no sé si había confirmado o no que el tema de cómo comprometían las cuentas de Telegram era por eso que tenían relaciones con empresas de telecomunicaciones en los países que fuera y de esa forma podían redireccionar obtener número de teléfono hacer tema de Sims shopping digámoslo así para registra las cuentas de Telegram con el mismo teléfono y obtener los datos así de hecho creo que en ese set se Comenta también que hicieron un fallo de seguridad de operacional y que los mensajes porque interactuaron con esas cuentas verdad con sus víctimas pues borraron los que ellos enviaron pero no los que la otra parte envió o sea que así se dieron cuenta un poco pero bueno pues nada muy buena noticia y pasamos a la siguiente si te parece dale Candela y de hecho la que traigo Yo también es deformiden Stories porque tienen como dice Martín tienen una serie muy buena que se llama llamado el proyecto Story Killers asesinos de historias que es una investigación global sobre lo llaman así Los mercenarios de la información la de Martín fue enfocada más yo creo que más nivel de estado nivel de gobierno nivel de como él ha dicho influenciar las elecciones en la mía va un poquito más digámoslo así más bajo nivel Pero no por eso menos preocupante porque a bajo nivel me refiero a que nos implica a todos a ciudadanos de a pie a civiles no a tanto a gobiernos sino más a personas como nosotros y en ese en este caso voy a hablar de una empresa de desinformación llamada s2t and Looking service y este reportaje fue publicado hace menos de dos semanas Ese es una empresa de desinformación Y qué necesita para sembrar dicha desinformación pues necesita víctimas y cómo consigue estas víctimas Pues bueno una forma sería aprovechando la audiencia de plataformas organizaciones de éxito como Twitter en New York Times periódicos similares comprometiéndolas y pues ahí dejando un poquito las noticias pero bueno esto sería bastante sospechoso y se vería y estas empresas Supongo o no ya hemos visto en varias ocasiones que noticias desinformación sobre todo en redes sociales pasan desapercibidas y no se borran hasta que pasan años o mucho tiempo pero más fácil sería como ha dicho Martín creando usuarios falsos cuentas falsas a veces la llaman cuentas marioneta avatares bueno que no corresponden con ninguna persona en sí sino en Muchas cuentas corresponden a una persona como las controla Y utilizando estas cuentas para publicar mensajes de desinformación y la forma en este caso que utiliza s2t es la ingeniería social en redes sociales haciendo conexiones o amigos de forma digamos orgánica

primero establecen la conexión por ejemplo te envían una solicitud de amistad en una red social al recibirla revisas el perfil de la persona que te quiera Añadir como amigo Y ves que tenéis algunos amigos en común y además que tenéis temas en común intereses similares y bueno que vamos que compartís algo y que sería bueno que estuvierais conectados También aparte de eso ves que tu nuevo amigo comparte contenido interesante relacionado con tu trabajo o pasión Bueno pues entonces Decides aceptar a esta persona Total que me va a pasar no esto de las redes sociales no tiene peligro verdad pues como vemos en este caso otro caso más de sirotras pero verifica tienes que hacer un poquito más el ejercicio de indagar a ver quién es esta persona a partir de aquí una vez ya se ha establecido la conexión está amistad ficticia online viene la intrusión unos días más tarde Te envío un mensaje para compartir algo o una petición para que les permitas acceder a un grupo que tú administras de esta forma Pues expanden un poco más su círculo de acción y de impacto también te pueden pedir tu número de WhatsApp para compartir un enlace sobre una causa en la que estás involucrado y como estás interesado en el tema y tienes curiosidad pues haces clic en el enlace y de aquí de repente Sin tu consentimiento Sin tu conocimiento tu dispositivo se ha convertido en una máquina de espionaje detrás de la cuenta falsa altamente realista hay un agente de inteligencia o incluso los clientes de esta empresa que pudieran ser gobiernos fuerzas del orden o cualquier persona privada que ahora tiene acceso a tu información personal e incluso puede Activar cámara micrófono capturar lo que se ve en la pantalla del dispositivo para espiarte en tiempo real y ver dónde estás en cada momento esto ya lo hemos hablado más de una nave más de una vez en episodios anteriores Y hay empresas como en eso Group con pegasus e Intel Alexa con Predator y otras que proporcionan este tipo de software espía las fuerzas del orden suelen utilizar este procedimiento en una operación encubierta para rastrear bandas criminales cibercriminales y grupos terroristas pero en esta noticia según un documento de una presentación confidencial a la que pudo acceder forbidden Stories se ha determinado que estas herramientas se comercializan para su uso potencial contra periodistas y activistas personas civiles que no están relacionadas que no son criminales directamente a no ser que se demuestre lo contrario y que no están relacionadas digamos con el gobierno de un país por vida en Stories encontró la presentación en un conjunto de más de 500.000 documentos pertenecientes a las fuerzas militares de Colombia la presentación en concreto mencionaba una oscura y poco conocida empresa de ciberseguridad como he dicho antes llamada s2t &locking service estos documentos no sé si Cómo pudieron llegar a las manos de forbidden Stories Martín a ver si sabes No sé si lo escuchaste tienes alguna idea de cómo vino esto Pues a ver tenemos el caso de ingeniería social de esta semana y el de la semana pasada que era por la filtración de 50.000 documentos de eliminar Y entonces filtración check ingeniería social check no sé abofetadas siguieron amenazas no en este caso también fue tipo filtración pero de hecho curioso porque Cuántos cuánto o sea Cuántas veces hemos adivinado de fechorías muy serias gracias a la filtración de documentos a periodistas desde desde tema de lo de snow de papeles de Panamá ahora casos como los de eliminalia este Qué curioso Y en este caso es que te lo comentaba porque igual había escuchado porque esto fue estos datos fueron obtenidos y filtrados por este colectivo de activistas conocido como guacamaya que esto sucedió en agosto del año pasado no si te sonaba que bueno yo leí la noticia pero no la comentamos no nos hicimos eco en el podcast de esta noticia porque sacaron tantos datos que no hubo como los papers de Panamá que dijiste seguro que la noticia de que se filtraron salió o igual no pero como todo en este caso se comentó que esta empresa Bueno en ese caso era la fiscalía del gobierno de Colombia había tenido una brecha se habían exfiltrado 500.000 documentos y ahí estaba se quedó el tema ahí porque claro quedaba analizar todos estos documentos Entonces ya ha pasado medio año y ahora justo han sacado los colores digamos a los documentos Pero

me pareció interesante unir un poquito los esos puntos con la noticia de agosto Qué bueno Insisto que es necesario este tipo de no pensaba que ibas a decir porque sí que hemos cubierto varias veces está intentando recordar ahora Quiénes eran estos tíos que tenían Cloud document.com o algo así te acuerdas que los hemos cubierto varias veces y subían ahí toda la documentación es como digamos una especie del nuevo del nuevo Wikileaks secrets o algo así justo pensaba que ibas a decir esos Sí sí pues mira se parece hay dos por cierto referencia el chiste el chiste son given Kids Pues nada esto como digo han estado analizando todos estos documentos y han sacado esto la luz no sólo eso comentar también que en aquel entonces en agosto del año pasado guacamaya también pudo extraer datos de cinco empresas mineras públicas y privadas y varias agencias ambientales en Colombia y Guatemala en marzo incluso del año pasado un poco antes se Fil otros cuatro terabytes de datos de una empresa minera suiza que operaba en Guatemala Así que un montón de documentos y que probablemente vayan a ir saliendo más historias y cuando nos enteremos de más pues no os preocupéis que vamos a traer todo esto a tierra de hackers una una pregunta Porque aquí sí que cabe matizar cuando te refieres a filtración no te refieres entiendo filtración te refieres a que no salió los detalles se filtró a la prensa sigue en tal pero también podría ser filtración de se dejaron la base de datos abierta públicamente y la encontró alguien que también hemos cubierto mucho O sea qué tipo de filtración o no lo especifican estas directamente las empresas esta lo que involucra es primero una intromisión o una sí un compromiso vamos de sus redes y que es este grupo guacamaya recopiló estos documentos y se los llevó y luego no los han puesto creo yo de forma pública accesible que se los han dado de forma digamos los responsables a personalidades como forbidden Stories y otros periodistas que van a hacer buen uso de esta información es lo que entiendo yo he entendido vale vale o sea que fue una filtración proactiva en plan las traigo Yo no es que me la encuentre por ahí Eso sí sí sí sí fue este grupo vigilante como que está por el bien de los civiles está ahí un poco sacando los documentos no O sacándole los colores a la vez también o sea sí ciberactivismo pero a la vez También hay que ser justos cometiendo delitos correcto más que nada para No claro lo del cuando nos quedamos solo con el resultado pues pues Guay pero claro también hay que hay que exigir que se cumpla la ley no se incumple es la si te queja si cumples la ley para demostrar que otros incumple la ley también también es un caso curioso no da para debate interesante apuntado sería sería justificable incumplir la ley para demostrar que alguien está incumpliendo la ley claro el caso más interesante aquí Martínez el tema de cómo combaten sobre todo el gobierno australiano ahora con ese equipo de 100 personas full time el ransomware que tiene Carta blanca para contraatacar muchos que igual lo ven mal a esto se oponen a eso pero Oye si tienes el permiso del gobierno Pues claro de todo depende A dónde vayas a atacar si vas a atacar a otro país en ese país No Es legal eso porque no tienes jurisdicción pero sí me recuerda cuando hablamos de Ucrania que Rusia dijo podéis piratear todo todo el Hardware todo perdón todo el Software que no sea de Bielorrusia O Nuestro venga palante vía libre pues nada nos ponemos tierra de hackers hecho en Rusia algo así para evitar que seamos objetivos tenía que haber aprovechado a bajarme el Windows 11 con una VPN en Rusia tío incumpliría la ley otra pregunta abierta tengo muchas preguntas existenciales en discord creo alguna vez el usuario Comentó uno de nuestros oyentes comentó que que para evitar en malware que se detonara digamos en tu máquina y te infectara que lo pusieras en ruso o algo así no el teclado que evitaba así que te vas de Windows en ruso y luego usas la cámara del móvil que para traducir y ya está fácil creo que era el sistema operativo que lo tengas ahí y el teclado también o sea eso también lo miraban pero claro para no infectar a compatriotas Pues es de la manera que puedes saber si esa persona rusa o no Claro claro ni antivirus ni nada pues nada volviendo a ese 2t decir que fue fundada en 2002 por el empresario Ori sasón es una empresa con oficinas en Singapur sri

lanka el Reino Unido e Israel los investigadores identificaron estas ubicaciones al correlacionar los gráficos y las inscripciones tecnológicas de su sitio web con los del folleto informativo que se filtró Así que no han podido confirmar exactamente dónde tiene actualmente oficinas esta empresa porque a diferencia de los investigadores y periodistas de la noticia de Martín que ellos fueron en persona en este caso el análisis de esta noticia se ha basado en documentos digitales Así que igual algunas de estas ubicaciones y oficinas en esos lugares pues puede que hayan cerrado o no pero en todo caso esta empresa Afirma tener docenas de clientes en los cinco continentes y emplea personas de agencias de inteligencia en el Reino Unido Estados Unidos Rusia e Israel así como a las fuerzas del orden local en el medio oriente América del Sur y central y Asia Los investigadores identificaron clientes en Singapur e Israel y posibles clientes en bangladesh Turquía sri lanka India y Malasia según el sitio web de s2t otros clientes incluyen un grupo de medios en América Central y una nación Sudamericana donde sus herramientas se utilizaron para encontrar información relevante sobre el autor intelectual de un secuestro esta presentación también analiza las demostraciones quizás realizadas en 2020 incluidas las de la marina de la India y un hombre de negocios en Malasia llamado dato Mohamed loft no la empresa se anuncia a sí misma como una empresa de inteligencia de código abierto osint este concepto Ya lo hemos hablado en otros episodios anteriormente pero la presentación muestra herramientas Más allá del típico gossint entre ellas incluye una herramienta de phishing automatizada para instalar malware de forma remota como he dicho este malware probablemente sea pegasus o Predator o similares también ofrece bases de datos de publicidad masiva para rastrear objetivos otro concepto que hemos mencionado más de una vez el tema de los anuncios que se utilizan mucho para rastrearnos online y también operaciones de influencia automatizadas utilizando cuentas falsas para engañar a objetivos desprevenidos es lo que ha comentado Martín en su caso más tema a nivel gubernamental influenciar elecciones en este caso un poco más bueno pues para engañar a la gente sobre algún concepto específico pero no a tan alto nivel Stories investigó como ese 2t y otras empresas de ozin se han beneficiado de Este mercado no regulado que esto es bastante importante y habría que hacer algo al respecto lanzando y vendiendo herramientas de vigilancia digital cada vez más sofisticadas a clientes con un historial de espionaje periodistas y disidentes Y esto es muy preocupante amnistía internacional decía lo siguiente esta presentación y otras publicaciones de este año sobre empresas de inteligencia web realmente exponen una nueva industria de vigilancia que no conocíamos y que parece estar creciendo realmente debemos prestar atención a este a esto Porque existe un alto riesgo de que se abuse en todo el mundo la noticia también contiene imágenes de los documentos relacionados con esta empresa una de las imágenes contiene digamos un flujo de trabajo centrado en el objetivo con varios puntos no empiezan con el número de teléfono Pues cuando tienen esto intentan pivotar de este punto de datos a obtener el nombre del nombre intenta sacar el perfil de la red social de ahí intentan conectar con la víctima a través del Avatar o cuenta falsa y hacerse amigos de esta forma cuando son amigos y pueden ver más datos sobre esa víctima Pues enriquecen el perfil de dicha víctima y luego ya pues a partir de ahí envían el payload fishing pegasus pre editor lo que sea para obtener información de forma más activa también hay otra imagen en la que muestran un flujo de trabajo centrado en temas en plan empezamos desde un tema de interés a partir de ahí pivotamos y creamos un proyecto y encontramos buscamos contenido luego identificamos influencers clave o comentaristas importantes de este aspecto de este tema conectamos con la víctima encontramos grupos identificamos más objetivos Para futuras investigaciones todo esto pues compartiendo este estos documentos de desinformación con las víctimas no he tenido no han publicado como he dicho estos documentos online así que pues tenemos que confiar con el análisis de forbidden Stories Pero

me quedo con un comentario que han hecho que dicen que el folleto este informativo de s2t tiene 93 páginas y que se lee como una novela de espías o un episodio de la serie Black mirror con gráficos detallados que ilustran Cómo funciona la herramienta Así que para los que hayáis visto Black mirror pues puede ir por ahí el tema temas así distópicos de un futuro un poco incierto de opresión y control a ver cuánto sale la próxima temporada que aparte una de las cosas que ha sucedido es que siempre tenemos ejemplos en tierra de hackers de noticias que son un maldito episodio de Black mirror tío pero qué bien los guionistas de esa serie Y por supuesto oyente de tierra hackers que no haya visto Black mirror en cuanto acabe este episodio que se ponga a verla Sí muy buena serie como dice Martín Así que ahí si tenéis un fin de libre o cuando podáis también quería comentar expertos en privacidad estaba muy preocupados y decían lo siguiente nunca antes había visto un mapa tan completo que vincule todo el proceso y tantas técnicas con tanta claridad especialmente si no se dirige explícitamente a los activistas la plataforma en Sí pues una de las imágenes de la presentación muestra una captura de pantalla de esta plataforma de inteligencia web de s2t y muestra el nombre de Deep Fusion no sé si probablemente sea el nombre no se indica en la noticia pero se podría extraer que ese igual sería el nombre de la plataforma Deep Fusion y además de esto la captura de pantalla muestra un menú arriba del de la pantalla con varios varias secciones digamos la primera pone documentos y pone un número tal que 13,4 millones Así que esta plataforma debe nutrirse de muchas fuentes de información entre ellas documentos y tienen tantos luego tienen una sección de perfiles que tienen 851 Así que esos podrían ser potencialmente los que han estado atacando casos o entidades tienen 17,3 millones Así que son Probablemente sean temas o algo no sé son muchos casos igual pueden ser incluso también las víctimas a las que quieren utilizar como forma intermediaria para llegar a la víctima final tienen una sección de ingeniería social que menciona 325 herramientas menciona el número 52 y fuentes de información 2.385 en estas fuentes de información Se incluye el tema de bueno permiso de conducir identificador nacional como puede ser el dni También incluye tema que pone cdr que me imagino que deben ser registros de datos de llamadas y un par más que no conseguí descifrar porque tienen acrónimos y igual es algo de referencia interna de la empresa el usuario demuestra se llama Optimus user Así que no no es muy significativo pero tiene 28.631 notificaciones sin leer Así que bueno no sé tiene mucho mucho trabajo por hacer digamos el usuario de demo la herramienta también muestra opciones de menú para ver documentos analizar enlaces datos multimedia ubicación geoespacial línea de tiempos o cronológica y luego ideas o descubrimientos un poco más para el tema de crear desinformación de un tema en específico esta plataforma de osin también integra el reconocimiento facial e Inteligencia artificial de nuevo como mencionaba Martín anteriormente para crear esos mensajes de forma automatizada con un par de palabras y procesamiento de lenguaje natural en inglés natural Language processing también de nuevo para crear mensajes más humanos más realistas la herramienta puede por ejemplo usar Inteligencia artificial para identificar una cara de un vídeo como imágenes de cámaras de circuito cerrado de televisión o vídeos que se postean en redes sociales o imágenes y mapear las opiniones o sentimientos en torno a un término o persona en una ubicación geográfica específica en un tiempo en determinado y obviamente como decía al principio la herramienta no sólo ofrece capacidades pasivas de recopilación de información y creación de perfiles a partir de inteligencia web sino que también ofrece funcionalidades activas para influir en el público que más que influir yo diría manipular en un gráfico por ejemplo se muestra que los operadores de la herramienta parten de un problema político local identifican puntos de conversación y sentimientos clave de un grupo objetivo luego unas cuantas de las cuentas falsas compartirían los puntos de conversación en redes sociales Mientras que otras cuantas

cuentas hacen clic en me gusta comparten y comentan en las publicaciones de las cuentas falsas originales estás copiando mi noticia esa frase la tenía yo verbatim en mi noticia cuenta tanto justo es que la verdad es que es interesante que hayan tantas empresas de este tipo distintos niveles como decía la tuya más enfocada no sea a nivel de impacto global elecciones está un poco más enfocándose a los activistas que también son importantes pero utilizando técnicas muy similares las cuentas estas a mí me gusta lo de cuenta marioneta me hace mucha gracia y que unas interactúen con las otras en este caso parece lo que decíamos antes no que tú comentabas que tienen personas que interactúan con con ellas en este caso igual parece que al menos la interacción está de hacerle like compartir y me gusta lo tienen automatizado pero probablemente necesiten de un humano para para comentar a respuestas a comentarios de usuarios reales y lo que comentan es que detrás de estas cuentas falsas que hay una red compleja de proxys y que las hace muy difíciles de detectar por parte de las plataformas de redes sociales Supongo que por eso en algunos casos en algunas plataformas de redes sociales hemos visto que han habido tantos casos de desinformación y que fueron tan difíciles de encontrar y de borrar Supongo que porque aunque borren los mensajes estas cuentas siguen estando ahí y si no se corta de raíz del problema eliminando o bloqueando estas cuentas que según dice la noticia hay formas de ocultar si realmente es una cuenta verdadera o falsa o marioneta pues se hace más difícil el tema la herramienta también facilita el seguimiento de ubicación de un objetivo los datos incluidos en las aplicaciones de teléfonos móviles se pueden combinar con otras fuentes de datos como un mente en poder de las agencias de defensa e inteligencia como registros de vivienda o registros de geolocalización telefónica para obtener una imagen más precisa de los movimientos del objetivo la presentación muestra un comentario que dice Tal cual podemos llegar a casi todos los usuarios de teléfonos inteligentes eso nos tendría que dar escalofríos a todos qué tenemos un teléfono inteligente a no ser que vivas en una cueva querido oyente que entonces no sé cómo nos puedes escuchar pero bueno otra imagen de la presentación muestra un ejemplo de una campaña de fishing exitosa que desencadenó la activación remota de la cámara del dispositivo móvil de un objetivo de una víctima la imagen que se muestra la foto que se muestra en esta imagen esta captura de pantalla es de muy mala calidad lo podéis ver en las notas del episodio vamos a poner enlace al artículo pero se puede apreciar una captura de pantalla tipo selfie de una persona con la cara redactada cubierta con un círculo blanco artificial añadido de forma digital para Supongo lo han hecho los periodistas para proteger la identidad de esta persona de esta víctima y luego dos mapas debajo de la selfie que entiendo muestran la ubicación del objetivo voy a pasar un poquito a comentar la clientela de esta empresa porque ya vemos ya sabemos un poquito de qué va las capacidades y la funcionalidades de esta plataforma pues la presentación se adjuntó a un correo electrónico enviado entre analistas de inteligencia colombianos en marzo de 2022 los documentos filtrados muestran que fuerzas militares de Colombia Se reunieron con representantes de siete empresas de osin a principios de 2022 incluido un revendedor de s2t como parte de un proceso de licitación para obtener una nueva herramienta osin para sus intereses de hecho una fuente con conocimiento de los asuntos militares internos colombianos confirmó la existencia de un proyecto para obtener una nueva herramienta de osin pero no sabía cuál se compró finalmente con esto Quiero concluir un poquito que por si no fuera poco aparte de ese 2t hay otras seis empresas sino más que ofrecen el mismo tipo de servicio y que en algún momento Si pasan por tierra de hackers tranquilos que es la vamos a traer una de estas firmas competidores de s2t se llama Delta Haití Solutions esta empresa de hecho confirmó a forbidden Stories que había enviado una propuesta para un sistema osin en septiembre de 2021 a través de un intermediario llamado anhiruda sharma va midi Paty cuyo nombre aparece en los metadatos del documento s2t en una carta representantes de esta

empresa Delta it Solutions confirmaron que eran aliados estratégicos de ese 2t y Tenían un acuerdo de distribución abierto para el mercado colombiano pero dijeron que no fueron contratados por el ejército otro dato interesante aquí es que no solo hay empresas de este tipo que dices normalmente cuando hay una empresas diferentes tienen intereses distintos O al menos intentan competir pero es que en este caso una dice que es una aliada estratégica de la otra esto da más miedo porque puede ser una empiezan a compartir información de víctimas que han comprometido Unas con otras pues pueden hacer una red global muy interesante y muy potente en una carta de presentación dirigida a inteligencia militar colombiana s2t promueve sus herramientas para ayudar a combatir grupos maliciosos lo dicen entre comillas incluidos terroristas ciberdelincuentes y activistas antigubernamentales más adelante el folleto muestra cómo los operadores pueden identificar objetivos para una mayor investigación a partir de una base de datos de activistas conocidos entre 2018 y 2019 decenas de periodistas fueron blanco de la inteligencia militar colombiana utilizando una herramienta de monitoreo de código abierto llamada voicester analytics vendida por Boyer labs entonces con sede en Israel de nuevo con el país de Israel tiene mucha trayectoria de Ciber inteligencia esta empresa se reunió nuevamente con funcionarios de inteligencia colombianos en la primaria de 2022 según muestran los documentos Pero no solo en Colombia hay interés por estas herramientas en concreto sino que una captura de pantalla muestra que un cliente indio podría haber estado interesado en adquirir esta herramienta para monitorear los movimientos de protesta en redes sociales en un ejemplo de caso de uso de la herramienta con fecha de febrero de 2020 se muestra como se usó la herramienta para analizar palabras clave dinámicas relacionadas con las protestas estudiantiles en 2020 contra la ley de enmienda de ciudadanía de India de 2019 y lo que probablemente sea una referencia a los cierres de internet de dos ciudades colindantes en 2019 llamo y cachemira también bangladesh fue identificado como un cliente confirmado de s2t entre forbidden Stories y sus socios identificaron a la dirección general de inteligencia de las fuerzas de bangladesh una subsidiaria de s2t parece haber realizado un envío a esta entidad en diciembre de 2021 o enero 2022 y que forbidden Stories confirmó a través de datos comerciales no se Comenta Cómo pero debe ser algo como un albarán o recibo o datos de transacciones comerciales públicas o que alguien les ha filtrado la revelación sigue a otra investigación del periódico israelí jareds que descubrió que los servicios de inteligencia de bangladesh compraron otra inteligencia otra tecnología vinculada a Israel en 2022 incluidos vehículos de espionaje que podrían interceptar el tráfico móvil y de internet esto Martín ya sabes a lo que se refiere no no lo mencionan Pero estos vehículos de espionaje te acuerdas de cuáles eran te refieres a drones y así no vehículos de espionaje la furgoneta que ella Ah la wisp interesante que después de tantas noticias sabes es como cuando por ejemplo ves una película de no sé de Nueva York si has estado en Nueva York y te resuena más no y pues esta noticia que mira tanto Cabos justo para mí como que se cierra el círculo sí dices y sí te sientes más identificado bueno no identificado porque usemos esto sino porque el tema más identificadas patinado ahí eh pero me caí de culo pero me he vuelto a levantar me he patinado estos hechos se alinean con las declaraciones públicas del gobierno de bangladesh en enero según el periódico bangladesí de business standard el ministro de interior del país anunció que introduciría un sistema de interceptación legal según literalmente decía en un intento de monitorear las plataformas de redes sociales y frustrar diversas actividades antiestatales y antigubernamentales bueno Y cuál es la consecuencia podría seguir con estos casos porque hay miles pero estoy cortando la noticia porque ya llevamos bastante rato quiero comentar un poquito las consecuencias de la presión pues periodistas colombianos ilustran el efecto escalofriante de estas herramientas de austint algunos se han visto obligados a adaptar sus prácticas de información para responder a las nuevas amenazas digitales es decir ser más

precavidos online utilizar como decimos siempre cuentas de un solo uso barner teléfonos bost sobre IP que solo das a una persona y todo esto se han ido incorporando estas prácticas para ser más seguros online en las semanas posteriores a que supieron que habían sido perfilados los periodistas de rutas del conflicto que es un periódico que se dedica a atraer a la luz todos estos temas de opresión contra activistas y similares pues comenzaron sesiones de terapia grupal por los años psicológicos muchos dejaron de incluir sus firmas y publicaciones en redes sociales y algunos incluso abandonaron la profesión así que ya vemos que estas empresas que atacaban a estos periodistas ganaron en este caso bueno y quería cerrar la noticia un poco comentando cómo protegerse de este tipo de abusos tenemos tengo una lista un poco larga pero como ya vamos un poco cortos de tiempo solo quería mencionar y esto lo hemos mencionado más de una vez en otros episodios y que tampoco es cuestión de repetirme pero tema de sobre todo proteger vuestras cuentas con una buena contraseña gestionada con de forma correcta en un gestor de contraseña es activar el doble factor y no utilizar dispositivos compartidos que pudieran estar comprometidos un tema quería recalcar es el tema de que no hay un botón de borrar Así que sé consciente que lo que posteas online puede ir no lo puedes borrar Sí pero alguien algún Bot de estas empresas lo ha captado y si se ha filtrado está de forma pública algún alguna motor de estos de búsqueda también lo ha consumido y está ahí para la posteridad que si luego puedes ir a que lo borren directamente Pero estos Bots de inteligencia web a esos no se lo puedes decir también el la ubicación puede ser consciente de que estas plataformas algunas por defecto incluyen tu Ubicación pero si no también se puede incluir en imágenes en documentos los metadatos No pues un poquito ser consciente de eso los enlaces también vigilar que haces clic o no lo de los amigos pues también hacer un poco más Duty Legends como decíamos antes y investigar realmente a quién estás aceptando también revisar tu lista de amigos de vez en cuando y borrar aquellos con los que no hayas hablado o mirado sufrir en un año Digamos que ya no son tus amigos no bueno fuera broma Si quieres hablar con ellos en algún momento pues volver a añadirlos así que puedes reducir un poquito tu superficie de ataque de esta forma eliminando las conexiones con las que no has interactuado en un año una alternativa es no borrarlos pero hacer que todos tus mensajes sólo sean visibles por los demás tu círculo cercano de amigos y familia aunque esto a veces es difícil de gestionar normalmente requiere establecer opciones individuales cada vez que posteas algo que se hace poco user friendly complejo para el usuario quien se va a olvidar de hacerlo también no olvidar esas aplicaciones externas que conectamos relacionadas con juegos o aplicaciones del tiempo y luego el tema de la configuración de privacidad es decir quién puede ver qué tipo de información y mensajes y fotos quién te puede encontrar por número de teléfono o email quién te puede agregar como amigo y similares y luego el tema de Finalmente la información sensible no posteis información sensible como tus números de tarjetas de crédito o fotos de las mismas número de seguridad social identificador nacional esto dni un poquito sentido común verdad la recomendación También incluye que se evite publicar tu nombre completo dirección fecha y lugar de nacimiento número de teléfono en parte estoy de acuerdo con esto pero en la realidad la práctica Es que la mayoría de la gente la mayoría de nosotros los usuarios estamos acostumbrados a publicar toda esta información cuando que te creas una cuenta te pide normalmente esta información no y es algo en lo que las plataformas de redes sociales podrían ayudar Es decir cuando vas a crear una cuenta en una red social que esta misma te aconseje utilizar un alias por ejemplo o nombre de pila o solo tu nombre sin apellidos Sin nombre completo y después de eso Listo ya tienes acceso a la cuenta directamente no que tienes que te piden luego no no hemos acabado de crear tu cuenta además de toda la información que me has dado tienes que darme tu fecha de nacimiento de dónde eres y más información y por ejemplo tus intereses o los grupos de música que te

gustan temas así Todo depende del tipo de red social no Y esto por qué obviamente porque les beneficia estas redes sociales su justificación es para hacerte contenido específico en el que estés interesado a través de la información que les has proporcionado y sus algoritmos Pero la realidad es para vender nuestra información hace dinero de ella y que empresas que compran estos datos pueden rastrearnos espiarnos crear perfiles de nuestra persona y promover la desinformación para manipularnos como es el caso de s2t esta empresa que estoy comentando Sé que suena muy George orwelliano de gran hermano pero es la realidad y cierro con una noticia que he visto hace poco que me parece interesante al caso que estoy comentando recientemente en un discurso en la universidad de carne gemelon la directora de ciza Jane eastery ha planteado la idea de que las empresas de tecnología deberían ser consideradas responsables por las fallas de seguridad en su software history pidió una nueva legislación que impida que las empresas renuncien a su responsabilidad a través de contratos y términos de servicio y sean consideradas responsables por productos de mala calidad los ejecutivos de ciza apoyan esta y creen que esto produciría mejores productos y mejores prácticas de seguridad con esto lo que se refiere gent eastery es entiendo que hacerlo responsables no solo de que no funcione el software en sí Sino de temas de seguridad y privacidad es decir que nuestros datos se vendan se haga mal uso de ellos y que también puedan ser comprometidos y filtrados a empresas de terceros Como por ejemplo podría ser ese 2t y relacionado con esto último queridos oyentes traigo la pregunta del episodio que es la siguiente De qué forma crees que se podría evitar que empresas de vigilancia puedan recopilar información de usuarios online y os damos cuatro respuestas la primera es medidas antibot es decir que estas plataformas de redes sociales tengan capacidad de identificar si el extremo que está pidiendo los datos visitando las páginas de los perfiles de sus usuarios son bots o no y si son bots pues no dejarles obtener esta información porque todas estas plataformas de vigilancia como s2t se basan en automatización es decir en Bots La segunda opción sería redes sin perfiles a esto me refiero a que bueno pueda ser un usuario en esa red pero realmente no muestres nada de tu información personal a los demás y en ese caso pues sólo sería digámoslo por ejemplo un Twitter sin nada en tu Bio sin nada todo vacío que puedas ir leyendo los mensajes de otras personas que tengan un alias y listo la tercera opción serían leyes proactivas al estilo de Jane eastery delcisa pues un poquito hace responsables a estas empresas sobre todo redes sociales que es de donde se saca principalmente esta información de usuarios online puedes hacerla responsables de proteger esta información mucho más de lo que hacen actualmente porque a día de hoy lo que hacen es de hecho todo lo contrario no desprotegerla pero sí venderla sin pensar mucho en el impacto que nos causa a los usuarios y la última respuesta es educar al usuario es decir todo estos consejos que he mencionado anteriormente pues hacer No lo sé Se podría hacer que una plataforma de red social pida una digamos certificación pida que los usuarios que se quieren crear una cuenta pasen completen un mini cuestionario de educación de privacidad y seguridad online antes de poderse puedes una cuenta Ya sé que es algo Bastante utópico Pero bueno Oye sería como idea igual se pudiera hacer si se implementa si se si se requiere a nivel legal pues Oye sería algo que estaría bastante bien para que los usuarios estuvieran más concienciados sobre este tipo de riesgos el impacto de la información que ponen estas redes sociales y también lo que implica en temas de privacidad y seguridad online pues esto es de forbid stores la verdad nos han dado para para ya varias noticias entre la semana pasada y esta y la verdad es que su serie está muy bien Hay varias más por si estáis interesados tenéis los enlaces en las notas del episodio y ya sólo nos queda Pues agradeceros que os hayáis quedado hasta el final esperemos que os haya gustado este episodio recordar que estamos sorteando la última entrada de la router y espero veros por allí porque yo voy a estar desde los tres días desde el jueves Así que si me veis por ahí con

la con la famosa camiseta venir a saludar y a lo mejor voy con alguna pegatinilla por si la por si la queréis Muchas gracias por estar hasta el final por favor no olvidéis dejarnos comentarios y estrellitas en donde nos estéis escuchando que eso ayuda un montonazo a ganar visibilidad y nos vamos a escuchar y nos vemos y nos escuchamos en el siguiente episodio Muchas gracias a todos como siempre Muchas gracias por vuestro apoyo online en redes sociales en las plataformas de podcast todos esos comentarios en discord y nada seguimos reportando desde primera línea e intentando hacer el trabajo lo mejor posible para traeros episodios chulos Así que muchas gracias 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