69. NotMyPlate e Intellexa

[Música] tenemos un nuevo identificador único a nivel global que puede ser abusado para usarlo en tu contra la matrícula de tu coche ya creías conocer a todos los actores supervillanos cuando se añade uno más damos la bienvenida a intelexa un conglomerado de empresas de ciberespionaje que se está haciendo con los negocios y clientes que sus competidores están perdiendo debido a la legislación israelí de vuelta con el tipo de episodio habitual os traemos novedades en torno a tu privacidad y seguridad como un nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 8 de octubre de 2022 este es el episodio número 69 yo soy Martín vigo y está conmigo listo para ilustrarnos con su profundo conocimiento de las artes del hacking y pirateos varios Alexis porros Hola Alexis qué tal Muy bien Martín muy bien muy bien y voy a hacer un hincapié usemos bien la palabra hacking yo yo no soy un ciber criminal pero sí estamos aquí para documentar a los cibercriminales porque como ellos no paran nosotros menos estamos aquí para destaparlos a diestro y siniestro las artes del hacking y pirateo como dos cosas independientes es decir lo bueno y lo malo o acaso no hablamos aquí de cosas malas que me estabas acusando no es broma es broma era para hacer un comentario No no tú tienes o no tienes un profundo conocimiento en las artes del algo algo algo sabemos algo algo sé sí sí hombre Sí yo que sí lo tienes pues ya está no he dicho ninguna mujer para para dar un poco de bromilla aquí pues nada Muchas gracias Martín aquí estamos como tú dices trabajando duro destapando piedra tras piedra y sacar las noticias de donde nos vengan sobre todo nos vienen a veces de vosotros nuestro queridos oyentes Así que os agradecemos eso y no solo eso os agradecemos que nos sigáis episodio tras episodio y que estéis ahí como dicen engage no comprometidos con nosotros a facilitarnos un poquito Pues eso lo que digo para pasar una noticias a darnos comentarios que nos pueden ayudar a las siguientes los siguientes episodios y para los que no estéis os recordamos que deberíais estar suscritos a nuestro podcast en vuestra plataforma de escucha favorita la que sea estamos en creo que casi todas Así que elegir la vuestra y dadle al Play También estamos en redes sociales en Twitter Instagram y Facebook con el handel@tierra de hackers linking YouTube y Twitch como tierra de hackers nos podéis enviar vuestros emails a podcast@ tierra de hackers.com y os podéis unir a nuestro servidor de discord que es muy Majo y lo tenemos en tierra de hackers.com barra discord a través de ahí podéis conectaros y este episodio no tenemos pregunta del episodio ya lo comentamos En el anterior Así que damos paso directamente al podcast en Sí muy bien pues yo recordar que bueno recordar no lo habíamos mencionado solo en Twitter Pero somos candidatos a los premios de ivoox Y si os gusta lo que hacemos y nos queréis echar una mano pues podéis votar por nosotros como uno de los podcast que escucháis y que más os gusta lo tenéis la información en Twitter pondremos el enlace también en las notas del episodio y Bueno yo creo que haremos un enlace también que sea tierra de hackers.com algo para que sea más fácil para el próximo episodio pero si podéis y os apetece y creéis sobre todo que lo merecemos darnos un voto para los premios ebox a los mejores podcast estamos en la sección de empresa y tecnología y con esto todavía hay que agradecer a nuestros mecenas todo su apoyo económico que nos ayuda a seguir adelante y especialmente mencionar a Kevin o que justo se acaba de transformar en uno de nuestros patrios con el nivel más alto y también Dark helly Así que muchísimas gracias a estos dos nuevos patrios que les gusta desde luego lo que hacemos y lo muestran apoyándonos chicos Muchísimas gracias

si vosotros queréis hacer lo mismo Pues patreon.com/tierra de hackers que ayuda mucho y también como siempre recordar nuestro partnership con Mónaco una empresa que comparte los mismos valores de tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y mónate a través de una herramienta de gestión de datos y telemetría de seguridad una empresa de silicon Valley que busca ingenieros como tú así que si estás buscando trabajo especialmente en tiempos de crisis como esta no dudes en contactarles en mónaco.com m o n.ad.com y específicamente su el email que han creado tierra de hackers@monat.com y también este episodio lo apoya a un branding Siempre os contamos que es mucha la gente que nos contacta en torno a cuentas robadas y acoso online pues son branden es una empresa formada por especialistas en varios ámbitos que se enfocan la reputación todo esto online han ayudado desde personas como tú y como yo hasta famosos a recuperar cuentas comprometidas en redes sociales llevar a juicio casos de ciberacoso ayudar a empresas en situaciones donde su reputación estaba siendo mala intencionadamente dañada e incluso borrar la huella digital que dejamos online no Solo han decidido Apoyar el podcast sino que se le contáis que venís de parte de tierra de hackers tendréis un descuento especial en sus servicios si necesitáis recuperando vuestras cuentas o reputación online ya sabéis un branding.es onb ra n d ing.es y no te olvides mencionar a tierra de hackers y yo creo que con esto ya comenzamos vamos a hablar de matrículas de coche y su potencial para construir un sistema de seguimiento de personas a nivel Global en muchas ocasiones cuando hablamos de privacidad mencionamos distintos tipos de identificadores únicos No que en manos de una empresa o entidad pues pueden servir para identificarnos y seguirnos a través de internet ips advertir ids correlación de nombres de wifis cookies son muchos esos tipos de etiquetas que cada uno llevamos colgadas no cuando nos paseamos por internet y que le dicen a los demás quienes somos digamos que nos da una identidad digital esto por supuesto en ciertos escenarios es necesario para el correcto funcionamiento de internet por ejemplo necesitamos una IP para identificar nuestro ordenador y conectarnos con otro ordenador usando su IP como llamar por teléfono un amigo no ambos necesitamos números de teléfonos únicos globalmente para que la red de telefonía funcione pero también sabemos a la vez que tanto ips como números de teléfono son usados para invadir nuestra privacidad tenernos monitorizados y monetizarlo en la industria de la publicidad online pues uno de estos identificadores a nivel mundial que de manera única nos identifica O al menos nuestro coche son las matrículas y existe tecnología desplegada por todo el mundo capaz de leer estas matrículas en tiempo real esto lo vemos en autopistas cuando nos cobran automáticamente por ejemplo en San Francisco donde yo vivo Pues cuando cruzas la El peaje pues ya no hay nadie allí cobrandote ni siquiera máquinas para trabajar para cobrar con tarjeta de crédito porque tienes que frenarte todo el mundo todas las puertas están abiertas Y te mandan la factura en base a tu matrícula o cuando alquilamos un coche y al salir del garaje la Barrera se abre automáticamente porque sabe que es un coche de alquiler y que no debe cobrarte el parking de hecho una tecnología muy curiosa es en San Francisco también los autobuses llevan ahora cámaras que ponen multas automáticamente si detectan coches mal aparcados muchas veces lo típico que vas en coche y poner los cuatro intermitentes y paras un momento en la parada donde el autobús tiene que recoger a los pasajeros pues estos autobuses ahora en San Francisco llevan matrículas que llevan Perdón cámaras que leen las matrículas y automáticamente te envían la multa a casa sin que tenga que venir nadie a ponértela bastante curioso esto y una vez más se basa en tecnología que lee automáticamente un identificador único que identifica tu coche que a su vez está registrado de manera única a un individuo que eres tú en

fin resumiendo las matrículas sirven para identificarnos y la tecnología para hacerlo existe y es barata además Pues con esto aumente a unos investigadores se les ocurrió la manera de implementar un sistema de seguimiento global usando esta tecnología y aplicaciones móviles para encontrar parking tal cual como suena me pareció súper interesante así que me leí el paper el otro día ya que lo publicaron hace solo un par de semanas y aquí os traigo los detalles de hecho no es que ellos hayan creado el sistema de seguimiento a través de matrículas de hecho ya estaba ahí solo que en el más puro estilo del significado de la palabra hacking y hacker han usado tecnología existente para llevarla un pasito más allá y utilizarla para un propósito que los diseñadores no habían contemplado y han escrito un Piper al respecto hacking en su pura esencia como mencionan Los investigadores la pandemia de Kobe 19 ha hecho explotar los sistemas contacless en todo tipo de infraestructuras incluyendo parkings y peajes de autopista son cada vez más las aplicaciones que te permiten registrar una matrícula la de tu coche y asociar una tarjeta de crédito Así la próxima vez que vayas a entrar en el parking no hace falta que saques el ticket ni pagues en la máquina sino que se te cobrará directamente porque la cámara instalada en la entrada del parking le era tu matrícula y te facturará de manera automática Lo mismo sucede en los peajes de las autopistas que te permitirá utilizar el carril rápido sin tener que detenerte a pagar para que suba la Barrera y puedas continuar todo ventajas hasta que alguien es capaz de abusar estas tecnologías todas estas aplicaciones de móvil te permiten registrar una matrícula sin ningún tipo de autenticación o verificación de que la matrícula que está registrando es tu matrícula es decir no hay nada que me impida registrarme en una aplicación de parking metiendo tu matrícula en vez de la mía y cada vez que ocurre un automático porque una de estas cámaras ve la matrícula llegará una notificación al móvil de que te acaban de cobrar por Entrar en este parque en específicamente o cruzar aquel peaje específicamente ya vais viendo por dónde voy no a través de Twitter Los investigadores pidieron voluntarios que diezen sus matrículas para un experimento de espionaje no dieron más detalles para que los voluntarios pues no cambiasen sus patrones de movimiento y su vida al conocer los detalles de la investigación no consiguieron 120 voluntarios que entregaron sus matrículas y el primer día Ya consiguieron geolocalizar a uno de ellos a través de una notificación que les llegó dándoles la bienvenida al parking de un hospital concreto fácilmente identificable en la ciudad después de 100 días recibiendo notificaciones consiguieron geolocalizar al 26.5% de los coches en algún instante es decir más más o menos uno de cada cuatro voluntarios consiguieron identificar dónde estaban mencionan que después de la primera notificación recibida para cada voluntario desactivaban la cuenta en la aplicación para no levantar sospechas Al fin y al cabo al levantarse la Barrera del parking o no tener que pagar en la autopista de manera continuada podría hacer que la persona empezase a sospechar Pues que algo raro ocurre No recordemos que los investigadores son los que están pagando el parking ya que han registrado la matrícula de la víctima que quieren monitorizar mencionan también los investigadores que con suficientes datos de la actividad sería incluso posible de anonimizar a una persona si lo único que tienes es una matrícula por ejemplo vieron actividad de Pues de estos voluntarios que tenían Pues en casinos hospitales conciertos oficinas los patrones de movimiento en el tiempo no podrían indicar dónde trabaja esta persona como pasa su tiempo libre grupos musicales que le gustan etcétera de hecho con ustedes de grupos musicales hasta lo mejor puede es una de las respuestas a las preguntas de cuando reseteas la contraseña como mencionaba Los investigadores pagaban los tickets ya que los requiere este tipo de vector de ataque Pero cuánto Les costó no es factible hacer esto pues lo es porque Les costó toda la investigación de seguir a 120 personas pues 276 euros que me parece

bastante poco para trackear a 120 individuos Bueno en realidad tuvieron información de uno de cada cuatro como decía mencionan que muchas ocasiones no les cobraban porque la víctima pues entraba y salía del parking inmediatamente lo típico que a lo mejor entras por error y te da 10 minutos sin cobrarte para salir o a veces incluso había algún error en la aplicación y no les cobraba perdonad pero es que estoy un poco resfriado mencionaban que un escenario real en que agencias de espionaje o delincuentes usen este vector de ataque se puede abaratar costes cerrando la sesión anticipadamente o utilizando tarjetas de crédito robadas que esto pues esto es muy común para mí más que el uso de Esta técnica para espionaje masivo lo veo más factible para un individuo en concreto plantearos el caso de una pareja que abusa o acosa a su expareja y tiene una orden de alejamiento algo Lamentablemente bastante común Pues podría utilizar Esta técnica para saber dónde se encuentra la víctima en todo momento también ladrones se me ocurre sabemos que hay muchos monitorizando redes sociales para averiguar cuando los dueños de una casa normalmente de lujo se va de vacaciones observan directamente la casa Si las persianas están bajadas todo el día o el consumo de Electricidad que suele estar accesible desde el total del edificio pues no no está no está registrando actividad eléctrica cualquier indicativo de que pueda acceder a la casa porque los dueños están ausentes se han ido de vacaciones o lo que sea pues podrían utilizar Esta técnica para localizar que se han ido a un aeropuerto o simplemente cuando han dejado la casa esto es especialmente relevante si uno vive solo ya que indicaría sin error que no hay nadie en la casa En ese momento porque si tú vives solo y tu coche de repente se detecta pues estás en un parking que está a 100 kilómetros pues es bastante posible que la casa vaya a estar vacía o simplemente para robar coches de lujo pensadlo identificar cuando el coche entra en un parking y en qué parking en concreto un ladrón puede ir por la calle apuntando matrículas de coches de lujos aparcado en la calle y luego los va registrando y luego en un momento se habrá dónde está ese coche sobre todo cuando entra en un parking o imaginaros ya en el parking de un aeropuerto que sabes que probablemente vaya a estar el coche ahí todo el día y por supuesto Pues como siempre agencias gubernamentales estoy convencido de que las agencias de espionaje ya tienen acceso a los datos de todas estas cámaras sin tener que hacer triquiñuelas y lo hacen cuando seguramente cuando quieren encontrar un vehículo de un sospechoso de un terrorista y quieren saber Pues dónde está o en concreto la actividad No de hecho lo hemos cubierto ya en episodios anteriores software de este tipo que utilizan los gobiernos Pero bueno esto sería otra técnica Y seguramente pues más baratas que las licencias de este tipo de software no también mencionan otra técnica por ejemplo hay ahora con la con las ciudades cada vez más saturadas Pues están implementando medidas para evitar tráfico en el centro de las ciudades por temas de contaminación por temas de ruido y entonces hay en muchas ciudades donde se leen las matrículas automáticamente y te permite pues aparcar una vez al día durante 30 minutos de manera gratuita pero luego ya no puedes O si el tipo de coche es eléctrico pues entonces puedes más porque te da unos beneficios porque contaminas menos pues estos investigadores encontraron páginas web puestas por los diferentes gobiernos y y ayuntamientos para ciertas ciudades donde tú puedes ir a registrar que que te has aparcado O puedes ver pues simplemente tu actividad porque solo puedes aparcar una vez al día y ellos lo que hicieron fue automatizar el digamos el registro de sesiones de parking con duración de un segundo de manera masiva es decir empezaron a poner a través de la web que habían aparcado pues 5.000 coches de 5.000 matrículas diferentes y la web si tú ya has aparcado ese día en la ciudad te da un error te dicen no puedes volver a aparcar por tanto utilizaban esto para saber que ese coche había aparcado en la ciudad

que estaba presente en la ciudad en ese momento y por ejemplo esto lo hacían pues al final del día no para saber si el coche seguía allí aparcado esto ya es una técnica un poco más difícil realmente de hacer un ataque real y factible Pero bueno es una manera más de a través del error de una página web poder averiguar que hay un coche aparcado en la ciudad y eso te está dando información sensible que en manos de la persona equivocada pues pues se puede abusar y puede tener sus consecuencias la verdad es que si bien Esto es una investigación académica por ahora han hecho una muy buena prueba de concepto y el ataque es técnicamente sencillo Al fin y al cabo se trata de registrarte en una aplicación y poner una tarjeta de crédito no tiene más pero las consecuencias como decía son serias y el problema es que la situación es difícil de solucionar las cámaras que leen matrículas están instaladas por todos lados y tú no puedes hacer nada para evitar que alguien registre tu matrícula en una aplicación como hemos visto los investigadores a través de su web not my plate.com que os dejo en las notas del episodio tienen un formulario que al rellenarlo te da una solicitud básicamente te da una solicitud gdpr que puedes enviar para evitar que tu matrícula acaba en estos sistemas Esto del gdpr Ya lo hemos mencionado varias veces es una ley de protección de datos a nivel europeo donde pues esto es especialmente relevante Pues cuando cierras una cuenta en un servicio online y le dices pues que quieres que borren todos tus datos de sus bases de datos y todo esto Pues teóricamente tú puedes enviar una solicitud a diferentes empresas para que cuando vean tu matrícula pues la ignoren Y entonces esta web te ayuda digamos a redactar esa petición de manera formal no sé cómo de efectivo será esto Pero quizás no es mala idea por otro lado estás ahora asociando tu nombre a tu matrícula mandándolo pues a una empresa o una agencia Es cierto que el estado de tu país ya tendrá esa información porque todos los coches están registrados a sus dueños Pero bueno vale la pena mencionarlo para tomar las medidas oportunas para proteger tu privacidad con toda la información no Los investigadores mencionan otras medidas para paliar este ataque por ejemplo implementar sistemas de verificación que revisen si la matrícula que está registrando en la aplicación es realmente tuya porque a día de hoy ya digo que yo puedo registrarme en la aplicación con la matrícula que yo quiera no hay ningún tipo de verificación que esas Efectivamente mi matrícula otra cosa que recomiendan es evitar el registro doble o múltiple de matrículas resulta que las aplicaciones y esto esto lo deberían hacer las aplicaciones permiten registrar la misma matrícula con varias cuentas varias veces es decir aunque tú seas ya usuario de este tipo de aplicaciones y tengas registrada tu matrícula la mayoría de las aplicaciones me permiten crear una nueva cuenta a mí y registrar tu matrícula otra vez por tanto el hecho de que se podría decir Oye registra tu coche en todas estas Apps y así ya nadie puede puede de hacerlo un poco ya Esta técnica la hemos es lo que se conoce como Plant your flag no como plantar Tu bandera entonces registras tú las cuentas antes de que las registre alguien malicioso y esto en muchos ámbitos ayuda y de hecho tanto Alexis como yo lo hacemos tres estamos registrados en muchos servicios que no utilizamos para evitar que otra persona pueda registrarse por nosotros porque normalmente el proceso de registrarte es más sencillo que el proceso de averiguar tu contraseña otra técnica que recomiendan es permitir un output un octach digo Perdón o el decidir que no quieres formar parte de esto Esto es una medida digamos activa no pero tú podrías decirle a la aplicación Oye esta matrícula yo no quiero formar parte de este sistema Por tanto si alguien va y la intenta registrar como está la has puesto como que no quiere ser parte del sistema pues lo ignoraría en principio no una especie de lista Robinson en España tenemos pues una lista que teóricamente las empresas respetan a las que tú puedes poner tu número teléfono en una lista de no me llames entonces en

principio por las empresas de marketing si hacen lo que deberían hacer todos los teléfonos que estén ahí registrados no lo utilizan pues para mandarte spam o hacerte llamadas para venderte algo y la última medida que comentan es que los parkings muestren en pantalla que ha sido cobrado el parking a través de una app comentan que los las víctimas en este caso no las voluntarios no sospechaban nada ninguno de ellos reportó que había sospechado nada cuando llegaba un parking y se le abría la Barrera de hecho a mí eso me ha pasado en alguna ocasión Pues porque a lo mejor justo era gratis ese día o lo que sea sobre todo cuando viajas a otras ciudades pues no sabes no y no tiene por qué levantar sospechas otra cosa es que Durante un mes todos los parkings se te abran gratis entonces Claro si en la pantalla por lo menos mostrase Oye te acaban de colgar a través de esta aplicación en vez de no Mostrar nada que es lo que sucede ahora pues podría ser un indicativo de que algo raro está pasando a ver Esto es una medida que seguramente no vaya a ser muy eficiente Pero bueno Los investigadores querían mencionar muchas digamos alternativas no para intentar paliar un poco estos problemas pero bueno ya para terminar ya veis tenemos un nuevo identificador único del que preocuparnos muy interesante como siempre Martín esta noticia yo sobre el contexto que has mencionado de todo esto no de que ya está implementado no garajes que se abren automáticamente me ha gustado lo de los autobuses que ponen cámaras para para reconocer la matrículas y poner multicas esto no lo sabía pero me ha recordado en el 2018 en algunos cuerpos de policía local en España tenían algo similar tenían montada una cámara también que iba patrullando y va a ir circulando por la ciudad y se había un coche mal estacionado tipo carril bus o taxi pues le ponía una multica también y lo de los peajes yo creo que lo he visto por primera vez en Estados Unidos pero bueno aquí en España también han incorporado reconocimiento de matrículas para el pago Además del tema este del transpondedor este remoto que tienes que sería adicional si no te puede leer la matrícula pero se me estaba ocurriendo mientras ibas diciendo las recomendaciones un adicional que como vamos leyendo tantas noticias se van apuntando y nunca se pueden comentar pero iba a mencionar el tema de no sé si conoces que hay el concepto y Es legal una matrícula digital es decir te puedes poner una matrículita donde tienes la matrícula y esto completamente digital y la puedes controlar Oh en vez de Y sí la puedes controlar desde la aplicación móvil Es legal no sé hasta qué punto se puede cambiar o no pero obviamente si es digital es una pantallita y y Es legal que instalártelas pues ahí si puedes modificar la aplicación móvil si no te deja que yo creo que te deja cambiar Pues nada el tema Me imagino un escenario Pero esto esto el tema este de que es legal Yo sé que en Estados Unidos Pues eso puedes pagar por tener una matrícula customizada y todo esto entiendo que hablas de esta Yo pensaba que tenía que tener la forma y todo el color y todo esto todo igual no sabía que lo único que tienes que tener Es que se vea el número o sea que lo puedas hacer con una pantallita LCD ahí me parece la leche eso eso eso en Estados Unidos la empresa se llama reviver.com Reve r.com de sponsor nos tendrían que ayudar pero está muy está muy bien el tema yo lo vi pero creo que lo tengo apuntado aquí lo tenía que mirar a ver lleva batería lo empleado hablar pero creo que cada mes hay que pagar unos 20 dólares al mes y es un mínimo de 48 una suscripción de 48 meses lo interesante eso se me ocurre lo que tú decías no el escenario en el que para evitar ser traqueado no Pues sabiendo los lugares en los que hay lectores de matrículas de alguna forma esto no sé si se debería saber eso asumo de que se tiene información pues cuando te acercas no con una aplicación complementaria o incluso si se si se añade a esta aplicación cambias la matrícula y pones otra totalmente aleatoria que no exista o que exista no sé si si estás reconocimientos de matrícula miran a ver que las matrículas existan o no Para evitar el tracking o si

no Si usas la de tu vecino Pues mira que no no te cae muy bien pues que le cobren a él y tal si la tiene dada de alta pero hostia pero estoy viendo la web y tienes toda la razón y el tema es que se ve Exactamente igual que la matrícula común o sea que lo que yo decía de pero coño No no puedes cambiar el formal es que no se cambia utilizan y in o sea las pantallas estas de igual que que el kinder Y entonces es que se ve igual que la matrícula o sea Estoy flipado esto esto hay que mirarlo Y que aparte te pones viene con app para Bluetooth Mira pone un poco te lo venden un poco como servicio de que puedes cambiar las matrículas donde Fly Supongo que habrá empresas que lo tienen que hacer o cosas así pero pero estoy grabando a ver el tema incluso es que te permite temas telemáticos en plan lo pueden utilizar también empresas que tienen muchos vehículos para controlar su flota no y saber dónde están O sea aparte del tema de que puedes poner más bonita o más fea la matrícula pues que controlaron están los vehículos y tal otro tema que me parecía similar era de hace años no Yo creo que he visto en alguna película o incluso alguno implementado en la vida real ese más mecánico no que tienen dos matrículas y con un botón desde dentro la apretadas si se cambiaba sí No no De hecho yo me acuerdo de ver eso en el Bueno aquí se reirán nuestros queridos oyentes de latinoamérica seguramente porque sé que el nombre diferente Pero en España el coche fantástico de Knight Rider ahí tenía como cambiaba de lado la matrícula y de hecho yo había visto en alibaba venden venden rollitos cambiar la matrícula o cubrirla Pero bueno aquí estamos hablando de algo muy ilegal recto pero estoy flipando con esto de porque es que no tiene ningún sentido porque es como tener una una matrícula aparte de la vende no para individuos y familias pero que Qué ventaja tiene tener tener una matrícula digital si realmente no la puedes cambiar o sea es como comprarte un kinder y dejarlo en la misma página del libro para siempre no yo creo que hay gente que le gusta eso personalizar la matrícula y ponerle el estado de verde el estado no sé que salir un solo un árbol entonces un poquito lo de alrededor pero el número no creo que se pueda cambiar pero Oye tú haces un jailbreak a la aplicación y la modificas y tal Y quién te dice claro esto es un buen proyecto para hacer risas yo imagínate que que yo que sé que puedas cambiar la de otros tío y le metes un problema legal o yo que se lo vas detrás de una mente claro las vas detrás detrás de uno y justo cuando vas a pasar El peaje te cambia matrícula pim Pam le cobra al del tío que tienes enfrente o lo que sea sí estoy flipando yo no sabía que tengan también y meterte en el temilla del Remote localización y a través de esta plataforma saber también dónde están no los que tengan estos pero sí aún así sí sí es otro Bueno claro Sí porque tienes la aplicación pero bueno yo creo que eso ya es más avanzado que no tiene porque estar conectada a internet o sea sí que pone que está conectada al móvil Supongo que por Bluetooth pero ostras tía matrículas por Bluetooth ya estoy flipando tío pues revival.com Les estamos haciendo publicidad pero todo por nuestros oyentes para que investiguen y lo vean lo podremos en las notas del episodio porque me acabas de dejar flipando tío y lo interesante es que los los investigadores parece que no lo mencionan Así que igual le podemos dar un gint Oye una pistita te has dejado este este tipo es verdad muy buena Alexis muy buena como digo vamos leyendo tanto tú como llevamos leyendo y se quedan en el tintero Y me acordé de esta la he rescatado de los archivos y digo la voy a mencionar que me parece interesante Pues nada acaba de la noticia queremos hacer un breve inciso para darle las gracias a nuestro patrocinador brawler que nos apoya en el podcast y que hace unos días acaba de lanzar un servicio en la nube para proteger tu infraestructura en aws hablamos de prowler pro y sus sass el servicio gratuito más completo de seguridad para aws browler Pro está construido sobre la Popular herramienta opensores frawler y además por el mismo equipo de ingenieros si ya conoces frawler que está disponible en github

seguro que vas a aprovechar las bondades que ofrece prowler Pro en cuestión de minutos tendrás resultados del estado de seguridad de tu cuenta de la WS podrás mejorar tu postura de seguridad a través de múltiples dashboards que te permitirán ahorrar tiempo y tener una visión completa del estado de tu infraestructura puedes empezar a usar brawler pro de forma totalmente gratuita en frawler punto desde ya mismo y bueno una vez dicho esto dentro noticia y la siguiente noticia va de parecemos unos pesados pero es que no paran de salir semillas de spyware y empresas que están detrás vendiendo estos servicios Bueno Las mil y una noticias de compromisos de Los Pesados son ellos nosotros solo informamos tío Los Pesados dejar de salir dejar de salir dejar de abusar a los ciudadanos de este planeta dejarnos tranquilos pero sí y podríamos comentar las miles que casi cada semana creo que sale alguna noticia de este periodista ha sido comprometido este funcionario de ese comprometido este político tal pero bueno voy a comentar el tema de una empresa en concreto que todavía no voy a revelar su nombre pero voy a hacer una mini intro del contexto no porque viene todo esto en recientemente hemos visto como el gobierno de Israel ha puesto trabas a empresas de spyware y de armas cibernéticas que se han creado en su país y venden sus productos a países de todo el mundo también desde los propios países de los países en los que hay clientes de estas empresas que venden spyware se han impuestos duras medidas económicas a los fabricantes de spyware por ejemplo en Estados Unidos se ha puesto una Lista negra en ese grupo nuestro querido en ese grupo que desarrolla el spyware pegasus y el que no le permite vender su software espía a empresas americanas ya ha puesto muchas trabas muchos temas financieros y de hecho hemos visto como algunas empresas se han querido mantener a flote o reinventar siendo compradas por otras empresas como es el caso de nuevo de en ese grupo que estuvo a punto de ser adquirida por esta empresa norteamericana que hace trabajos para el gobierno americano norteamericano llamada l3 Harris Y aunque vemos más y más obstáculos en este campo no paran de surgir empresas y confirmarse públicamente sobre todo sus existencias y sus modelos de negocio y esta noticia viene motivada por esto por dar a conocer un poco más a todo el mundo a todos nuestros oyentes este tipo de empresas que aunque no sean tan famosas como en ese grupo o candiru también candiru es una buena son igual de potentes y peligrosas en el tema del ciberespionaje Y en este caso voy a cubrir a intelexa un grupo o consorcio de empresas deciden inteligencia creadas Y dirigidas por un exmilitar de la inteligencia israelí actualmente con sede en Grecia desde 2020 y muy tema muy relacionado por eso también la traemos al podcast que recientemente ha habido polémica en Grecia por temas de ciberespionaje Y es que en agosto de este año el jefe del servicio de inteligencia de Grecia panaggiotis contoleon renunció a su cargo como líder de este servicio de este grupo de edición inteligencia debido a la polémica de las prácticas de vigilancia de su agencia ya que se descubrió que se estaba vigilando a zanasis coucaquis un periodista financiero conocido por su investigación de poderosas figuras bancarias esto se supo porque el mismo zonassis declaró haber recibido un mensaje de texto con un enlace un poco así en plan ingeniería social y Bueno luego ya sabemos todos su móvil fue infectado con en este caso Según dicen con el spyware Predator de la empresa citrox el caso de zanasis de hecho es el segundo de este tipo en Grecia Ya que en septiembre del año pasado hubo un incidente similar contra nikos androlaquis un miembro del parlamento europeo Y entonces el principal candidato para vencer al partido de Centro izquierda de Grecia y un rival histórico del partido de michotaquis El Primer Ministro griego vamos que el gobierno en ese momento estaba un poco bueno tenía sospechas de esta persona y no quería digamos que se metiera en contra del poder en principal en ese momento no y esto se descubrió gracias a una investigación

parlamentaria europea que bueno está bien que se definan se establezcan estas investigaciones que vienen directamente desde parlamento europeo para un poco aclarar el tema del ciberespionaje no las autoridades griegas admitieron haber realizado vigilancia pero enfatizaron que lo habían hecho legalmente y denegaban haber usado software espía y mucho menos Predator de citrox que justo esta empresa pertenece al consorcio de empresas de Ciber inteligencia de intelexa que es la empresa que voy a comentar incluso con estas declaraciones se ha descubierto una serie de conexiones entre los funcionarios griegos y las empresas vinculadas a intelexa O sea que aunque los el gobierno denegara haber utilizado este software espía igual no lo he utilizado en ese específico en ese caso de espionaje Pero hay hay lazos y hay evidencia de que el gobierno griego está de alguna forma relacionada con este consorcio de empresas de ciberespionaje llamado interexa y es que tres empresas que forman parte de intelexa fueron creadas en Grecia por un hombre de negocios vinculado altos funcionarios del gobierno griego cuando se trasladaron sus operaciones al país después de los problemas que tuvieron en chipre en el episodio 42 Ya hicimos Ya hicimos un guiño a intelexa y un tal tal Indian como decía Martín te acuerdas Martín y producto estrella de ciberespionaje la famosísima furgoneta Guay Spear que era aquella furgoneta aparcada en el aeropuerto de la arnaca en chipre que permitía interceptar comunicaciones de cualquier teléfono móvil ya sea Android o iOS en un radio de 500 metros Sí sí que me acuerdo tanto del tal tal como de la furgoneta esa que es una manera de empacar toda esa tecnología en un vehículo que puedes mover de lado a lado esa noticia fue súper interesante lo curioso Martín sí era que había un vídeo hecho de ahí cubierto por Forbes o sea el hombre es el tal tal Indian este no sé no se escondía era como como él dice dice soy un secreto público y esto vino se descubrió Bueno un poquito también por ese vídeo pero se pusieron a investigar y le metieron una multa por violación de la gdpr por estar ahí en chipre y por eso un poco salió más a la luz pero no no se ha hecho tan famosa como en ese grupo y kandiru sí que recuerdo que la multa probablemente sea una licencia de las que de las miles que habrá vendido a los propios gobiernos que le metieron la licencia esto es especulación mía pero bueno que si tiene es de risa eso de hecho el desparpajo ese de salir así un poco indica que yo estoy aquí en un paraíso hay hay paraísos Fiscales hay para ahora tenemos que hablar ya de paraísos de aplicaciones de espionaje no un poco sí un poco lo que dices es venga el gobierno Te vendo 10 licencias Pero para que no se vea así muy mal el tema hazme una multa de una y así es como el descuento no tal cual Te vendo una extra en plan el IVA no te vendo una licencia extra Y esa ya te quedas tú el dinero ya ni me lo pagues Pues sí pues se volviendo al tema de intelexa que como digo whisper es una de las empresas que forman intelexa pues tiene oficinas en A las afueras de Atenas cinco pisos O sea que no es pequeña la empresa incluye dormitorios un centro de formación Incluso un área con alfombras de oración para que puedan orar las personas que de hecho vienen de países musulmanes porque Aparentemente por ejemplo tiene clientes en bangladesh esta empresa intelexa hace negocios con personas de bangladesh Y aunque la empresa esté en Atenas se ha confirmado que algunos de los empleados que trabajan en persona desde el edificio en Atenas son de origen israelí obviamente también como el fundador o los fundadores que son de como digo ex militares de la inteligencia militar de Israel hacia finales de Julio la empresa dio instrucciones a su personal para que trabajara desde casa incluso desde Israel y reubicó sus actividades en otra parte de la capital griega sobre tal Indian mencionar que es un empresario del ciberespionaje y como he dicho él decía yo soy un secreto público no se esconde pero tampoco lo va publicando a gran escala es un ex jefe del departamento de inteligencia militar israelí conocido como unidad 81 que se encarga el desarrollo tecnológico en

2002 decidió dejar el ejército Según dicen con honores después de un escándalo menor relacionado con irregularidades financieras en la unidad 81 que hizo que su ascenso se detuviera tallín es un israelí que también tiene ciudadanía maltesa Aparentemente en Malta hay muchas ventajas financieras de impuestos Así que eso le interesó sin embargo las diferentes empresas en las que está involucrado y que juntas forman intelexa están registradas en muchos países del Mundo formando una compleja red corporativa que es bastante difícil de desenredar su primera empresa fue Circus de la que ya hablamos Incluso en el episodio 18 de tierra de hackers que ofrecía servicios de seguimiento y afirmaba poder identificar la ubicación de cualquier dispositivo móvil en el mundo con solo un número de teléfono a partir de 2019 Dylan operaba desde chipre donde su paraguas de firmas intelexa se autodenominó la alianza estelar este nombre así muy top muy Pro en plan parece algo tipo Star trek Star Wars bueno la eso la alianza estelar de la cibera inteligencia Y el mundo digital como digo las firmas dentro de la alianza incluyen wispear está esta compañía esta furgoneta que permite comprometer teléfonos y geolocalizar objetivos a través de sistemas wi-fi y móvil re celular citrox esta empresa cuyo producto estrella es Predator un software espía similar y competencia directa a pegasus en ese grupo y no solo eso sino que intelexa también tiene otros aliados que no fueron creados directamente por ellos pero por ejemplo hay una empresa que se llama nexa technologies antiguamente conocida como amesis que es una empresa francesa de cibera inteligencia asociada aliada con intelexa y también otra que se llama senpay technologies una empresa de la India de ciberespionaje que ayudó por ejemplo al líder corrupto de Malasia a espiar a la oposición según documentos presentados a un tribunal israelí los servicios de intelexa son muy completos incluyen inteligencia de red bueno todo esto basado en soluciones de recopilación y producción de inteligencia remota utilizando un producto que tienes senpai que es de osint y también geolocalización basada en la red ss7 que es una red celular que permite identificación de números de teléfono en todo el mundo también tiene una línea de productos lo llaman Field intelligents inteligencia de campo que permite la interceptación de tráfico a través WiFi y red de celulares línea de productos de inteligencia para infección exploits compromiso y extracción de datos otros temas tienen de sistemas de análisis y fusión de datos llaman tiene una plataforma llamada inside y tienen otra plataforma que se llama overside que permite a los equipos de la sede de intelexa proporcionar servicios y monitorizar todas las actividades de recopilación y análisis de inteligencia definir prioridades globales y controlar la asignación de recursos un tema diferenciante o diferenciador entre intelexa y en ese grupo por ejemplo es que en ese grupo normalmente o se ha visto o en sus contratos lo hice te dan la plataforma te dan el software y tú como cliente tienes que infectar decidir qué vas a hacer con esos exploits en cambio intelexa te ofrece un servicio completo es decir tú le dices exactamente estos móviles y saca información ellos te lo hacen para ti te hacen todo así que no te tienes ni que preocupar de hacerlo tú mismo y tener esa persona con ese conocimiento de hacerlo los orígenes de intelexa son un poco lentos diría yo y con pasos algo torpes Dylan se apoyó en un par de compañeros de la unidad 81 para crear intelexa uno de ellos había creado hacía poco sitrucks la empresa del spyware Predator que curiosamente se registró en macedonia del Norte y luego se incorporó en lugares como Hungría de nuevo el creador de psychocks es otro ex militar de inteligencia israelí pero eligió macedonia del Norte obviamente para escaparse de temas legales que voy a comentar en breve en 2020 Dylan y sus socios Fueron demandados por uno de sus primeros inversores la demanda detalla los primeros pasos de la empresa y describe intentos un tanto inútiles dicen de comprar exploits en la red oscura en la Dark web algo que es muy

interesante Esto indica que no todas empresas de spyware tienen su propio departamento de desarrollo de exploits como en eso Group que hemos visto que tienen un departamento muy top cubrimos en una noticia que a veces no dormían que tenían comportamientos raros y bizarros Pero bueno que vamos que hay empresas que no no invierten todo su dinero en eso porque a veces es muy caro desarrollar exploits y lo que hacen es yo lo compro esta terceros y hago un desarrollo de una plataforma Software que esto más o menos lo puede hacer y no es muy caro y incorporo los exploits y listo esto lo ofrezco a mis clientes el tema de la legalidad en Israel respecto a la tecnología clasificada hay una ley de exportación de defensa de Israel que requiere que cualquier ciudadano israelí que venda tecnología o conocimientos clasificados cuyos orígenes se encuentren en Israel es decir empresas registradas en Israel se registre la empresa es esta esta tecnología y bajo la superficie el supervisión de la agencia de control de exportaciones de defensa en el acrónimo sería dk en inglés deca se ha negado a confirmar o negar qué empresas están Bajo su supervisión Y sí intelexa está operando con su aprobación o no sin embargo durante el año pasado fuentes de alto nivel en la industria de las armas cibernéticas de Israel Que también es supervisada por dk se han quejado de que las nuevas y estrictas regulaciones impuestas por dca las están asfixiando un ejemplo es que a raíz de la presión de Estados Unidos en noviembre del año pasado cuando se descubrió que funcionarios del departamento de estado de Estados Unidos fueron espiados en África por un cliente de nso Group y que puso en ese grupo en una Lista negra de relaciones de negocio con empresas y gobiernos de Estados Unidos la cantidad de países a los que la década permite que las empresas y realiz vendan su ciber fireware se redujo drásticamente a solo 37 países en todo el mundo para no recuerdo pero creo que hay un poquito más de 200 países en el mundo no pues solo pueden vender ahora a 37 países que son principalmente naciones occidentales y democráticas con antecedentes limpios de Derechos Humanos Aunque bueno todo eso queda Aunque una nación sea limpia de en temas de Derechos Humanos ya hemos visto que que en ese grupo que pegasus se ha usado en muchos países de Europa así que bueno parece que igual todavía tiene negocio No pero claro quieren vendérselo a muchas más empresas las más interesadas serían las de poderes abusivos pero el auge de intelexa Aparentemente está directamente relacionado con el intento de Israel de controlar su industria de armas cibernéticas es como un poco contradictorio no que Israel lanza se pone más duro en plan vamos a evitar que haya más a casos de estos de abuso de uso de spyware y intelexa pues se está lucrando de en este suceso Y por qué sucede esto Pues el tema es que la legalidad es la principal diferencia entre intelexa y en ese grupo algo que intelexa está aprovechando mientras que empresas como en ese grupo han perdido tratos y se han visto obligadas a despedir incluso a trabajadores recientemente se ha visto no sé si fueron unos 500 trabajadores que se fueron amablemente digámoslo de la empresa otras también han cerrado debido a problemas de cumplimiento y las operaciones de Dylan han prosperado y su imperio ha crecido incluso ha abierto nuevas oficinas nuevos equipos y incluso nuevas capacidades según altos ejecutivos como digo de la Industria Del ciberespionaje mencionaban intelexa está operando de manera pirata al margen de la ley israelí para todos los efectos y propósitos se niega a someterse a la regulaciones como resultado puede sellar grandes acuerdos en partes del mundo donde los israelíes ya no pueden obtener autorización para hacer negocios por ejemplo los estados del Golfo o incluso en lugares en los que los israelíes nunca se les permitió trabajar incluso algunos comentaban algo que me pareció interesante dicen se puede decir que en ese Group es un actor con una ética problemática no dudosa que se puede debatir Pero al menos todo lo que hizo lo hizo desde la

legalidad siguiendo un poco las leyes que habían en Israel y en otros países y autorizado por el estado de Israel Esto es algo diferente y mucho más grave porque como digo se quieren saltar todo el tema de exportación de tecnología de decir espionaje en que está definido en Israel a pesar de que sus fundadores y algunos de sus trabajadores sean israelíes y que muchos de sus ejecutivos y miembros clave del personal vivan en Israel intelexa no se considera una empresa israelí las empresas dentro del paraguas de intelexa están registradas en países como y empiezo Irlanda Francia Hungría macedonia del Norte Grecia y las Islas Vírgenes británicas fuentes de la industria dicen que la empresa ha tenido representantes de ventas en Indonesia Dubai París y bueno obviamente tel aviv no parece que Atenas ha sido el centro de sus actividades en los últimos años Mientras que el propio Dylan vive principalmente en chipre esta compleja red de empresas hace que La regulación de la actividad de la empresa sea casi imposible y plantea un desafío nuevo y único para los reguladores tanto en Israel como en Europa parece que este este dital dillion es bastante inteligente cuando se refiere al tema de negocios y crear empresas para saltarse un poco como decimos no los loophones los agujeros legales y parece que le está funcionando hasta que bueno los abogados y los legisladores se pongan un poquito las pilas para ver cómo pueden evitar esto otro ejemplo he dicho que hay muchas empresas que han cerrado No pues hay una empresa también bueno otra empresa no es que van surgiendo te pones a rascar otra empresa que se llama Némesis que también es otra empresa dedicada ciberespionaje una empresa israelí cerró después de que dos acuerdos que estaba autorizado a negociar con clientes potenciales en África y Asia finalmente no obtuviera la aprobación de la década Y a quién fueron estos contratos finalmente Pues a intelexa O sea que Némesis no está sola ya que otras dos empresas de la industria cerraron en los últimos meses Mientras tanto las empresas vinculadas a intelexa han designado nuevos funcionarios de funcionarios incluido un ex jefe de ventas senior de Némesis y otro competidor de nso Así que incluso las empresas la cierran intelexa está acaparando a todos los empleados que se quedan sin trabajo claro y recientemente también hace unos meses Esto fue interesante la cuenta de Twitter de vx - underground Bueno una cuenta y un sitio web que tienen detrás en el que comparten muchos temas de malware de spyware e informes muy interesantes que recomendamos que que le echéis un vistazo filtró unas imágenes capturadas de unos mensajes publicados en el foro cibercriminal xss.i.s el 14 de Julio estas imágenes mostraron un documento en el que se especificaba el coste de una plataforma de ciberespionaje llamada Nova o también helios y sus funcionalidades ofrecida por una tal empresa llamada intelexa ya la conocéis no el producto spyware lo vendían por unos 8 millones de euros algo que indica que este documento estaba ofrecido por estar en euros algún gobierno que opera con la divisa del euro los documentos etiquetados como privados y confidenciales así que esto fue un buen una buena fuga describen servicios para la extracción remota de datos desde dispositivos Android e iOS específicamente la oferta es para explotaciones remotas basadas en navegador con un solo clic es decir la víctima tiene que hacer clic que permiten a los usuarios inyectar un exploit o carga útil en dispositivos móviles Android o iOS la breve descripción sugiere que la víctima tiene que hacer clic en el enlace para que se entregue el exploit la oferta incluye 10 infecciones por el módico precio como digo de 8 millones de euros concurrentes al mismo tiempo para dispositivos iOS y Android así como un paquete de 100 infecciones exitosas es decir se pueden infectar a 100 dispositivos pero tener conexiones abiertas solo a 10 al mismo tiempo los documentos filtrados también muestran una lista parcial de dispositivos Android iOS contra los que supuestamente funcionaría un ataque los documentos dicen que los exploits deberían funcionar en iOS 15.4.1 esto es interesante porque

Apple lanzó a ellos esta versión en marzo de este año lo que sugiere que la oferta es bastante reciente y también los exploits funcionan en la versión Android 12 hay que aclarar que por 8 millones de euros se obtiene mucho más que un exploit para iOS o Android ya que por esta cantidad también se obtiene una plataforma completa que incluye capacidades para analizar los datos extraídos por los exploits así como una garantía de 12 meses me arreglo de la garantía para poner en perspectiva en 2016 se publicó que en ese grupo había cobrado a sus clientes 500 mil dólares por instalar su plataforma de control y 650 mil dólares por comprometer 10 dispositivos aquí como digo son 10 dispositivos en concurrentes y 100 en total infectados por 8 millones de euros Aunque en 2019 se de una licencia de pegasus que costó algún cliente aproximadamente entre 7 y 8 millones de dólares al año Así que ya vemos un incremento considerable de 2016 a 2019 Y supongo que intelexa pues ha estado al tanto de estos precios que se cobraban y bueno lo cobra en comparativa con en ese grupo en relación a la multa vuelvo un poquito al tema del whisper antes de cerrar la noticia que me pareció interesante fueron unos 900.000 euros que se le impusieron como multa a whisper en 2019 por el gobierno de chipre según investigadores que conocen el mundo de la venta de datos de usuarios publicaron que los bloques israelíes han estado ofreciendo conjuntos de datos supuestamente capturados desde las redes inalámbricas en los aeropuertos la policía de chipre investigó y descubrió que otra empresa vinculada a dilian llamada Go networks o gonet systems había estado en contacto con el aeropuerto de larnaca en chipre donde tenía aparcada la furgoneta whisper esta empresa que cerró este año brindaba servicios de infraestructura WiFi los informes de 2019 muestran que wissperger afirmó que los sistemas wi-fi se instalaron como parte de un acuerdo en el aeropuerto de la arnaca para mejorar la red wifi no para recopilación de datos es decir No solo tenían la furgoneta sino que habían instalado sistemas wi-fi en el aeropuerto para mejorar la red wifi no para capturar datos y hay que creerlos el tema de los aeropuertos es curioso porque la gente no se para pensar Pero hay sitios donde sucede mucho espionaje porque pensarlo es como un embudo de entrada al país tú si quieres espiar a alguien en el país tienes que encontrarlo Pero es que cómo acceden al país no sobre todo cuando estás intentando espiar a gente extranjera políticos o lo que sea los aeropuertos es el nodo de entrada entonces poner ahí todos tus dispositivos o tecnología desplegarla en aeropuertos tiene todo el sentido del mundo porque es como el embudo no por donde va a entrar Sí o sí entonces por eso los aeropuertos es un caso curioso sí Y en este caso según la demanda de 2020 presentada contra dillion y sus socios Go networks también estaba vinculada intelexa tachán no a través de la propiedad corporativa compartida en Irlanda Es que esto habría que un poco mapear todas las empresas que tiene este hombre y ver que yo me he puesto a investigar un poquito y salían este como digo esta esta empresa de India que se llama sempai luego sale esta otra que se llama anexa technologies de Francia bueno deben haber incluso más que todavía no han salido a la luz pero bueno el tema es que esta empresa con networks está vinculada intelexa y las fuentes dicen que uno de los exaltos funcionarios de gonet systems Ahora tiene un puesto importante en intelexa y para cerrar este suceso que esto es bastante nuevo en febrero de este mismo año el tribunal de lo penal de larnaca publicó el fallo final del caso que pareció curioso según dijo el tribunal señaló y matizó que la infracción atribuida a la empresa gonetworks y Por ende intelexa nunca involucró ninguna intención de piratería o escuchas telefónicas afirmando que nunca hubo ningún intento o propósito de personalizar ningún dato el tribunal enfatizó que no se cau ningún daño a ninguna persona individual Así que lo creemos lo hicieron todos por el bien de nuestras conexiones a internet conclusión con esto vemos que intelexa es uno de los mayores

rivales podríamos decir de en ese grupo o incluso de candiru o todas estas top que siempre hemos mencionado aquí allá Aquí allá dándole bombo y platillo Pero es que yo quería queríamos traerles esta empresa intelexa que no es nueva que ya hemos mencionado digamos en el episodio 18 con su primera empresa circles del talin Dylan en el episodio 42 como digo Martín mencionó el tema del whisper que es de intelexa pero ese nombre intelexa está un poco en las sombras No pues eso se está quedando con la mayoría del mercado como digo está haciendo que empresas competidoras de ella estén cerrando está llevándose a los empleados de las otras empresas que cierran y bueno vamos a ver lo que surge en el futuro a través de esta empresa Pero mucho con ellos igual un tema Bueno de esto es que como todas están cerrando los investigadores de seguridad se pueden centrar más en una única empresa Y en lugar de tener que preocuparse por empresas nuevas que vayan saliendo no pero como digo cuando parecía que ya conocíamos a todos los jugadores del mundillo del ciberespinaje tachán surgen más participantes en este caso intelexa y todas sus empresas y en relación a esto traemos la pregunta del episodio que es la siguiente Qué medidas crees que podrían implantarse para limitar la proliferación y la creación de nuevas empresas de software espía la primera opción de respuesta es más legislación en torno a ciber armas la segunda es leyes internacionales o sea el tema de yo creo que Israel lo está haciendo un poquito bien el tema de controlar la exportación pero se seque la jurisdicción se queda un poquito solo aplica a Israel no no sale de ahí entonces tendrían que hablar un poco más con a nivel europeo o a nivel global aplicar todo esto y seguir a todas las empresas que se de origen Israel israelí que se crean fuera de Israel o se registran fuera de Israel la tercera opción sería más transparencia el tema de que la deca está la agencia de control de exportaciones de defensa se ha negado a confirmar o negar que empresas están Bajo su supervisión y sin intelexa está operando con su aprobación o no pues Oye podrían hacer una lista No sé qué tal legal o no sería esto pero bueno al menos mencionar las que hay y un poco la gente saber a qué se dedica En qué mundillo está metida a cada empresa y la última también un poco relacionada con temas de legislación pero podríamos decir más legislación en torno al ocultar empresas a través de estos fallos o estos agujeros de legalidad que creas una empresa madre y luego creas una empresa hija esto Esto es fácil de trazar se deberían empezar no sé que tener alguna automatización o de vez en cuando mirar que hayan todas como se han creado y un poquito poner orden desvincular crearlas digamos a nivel único que no hayan relaciones madre e hija en el caso del cibelespionaje para que un poco se hagan responsables directamente los los dueños de cada empresa porque un poco lo que hace el dilian es vaya Crea una empresa madre luego cree otras desde las que opero y un poco así me lavo las manos porque hay tantos niveles que que sea un poco se licúa las multas o las imposiciones que se hacen sobre cada empresa no le llegan muy impactantes a él digamos pues esto de las empresas de espionaje por un lado están hackeando la legislación O sea ya son expertos en temas de hacking y estaba pensando son como los nuevos youtubers mencionado que se van a andorra que se van a un país con leyes ventajosas para lo que están haciendo y pues esto es lo mismo No Ah pues en Israel me banean Pues venga me voy a otro lado Entonces es muy buena la pregunta muy buena las opciones porque es lo que dices tú no no es suficiente con que el propio país establezca limitaciones Porque si se van a otro sitio y ya está y de hecho chipre creo que también es un paraíso fiscal de estos tengo escuchado que puedes solo te exige estar dos meses allí como residencia fiscal y tal Por tanto a lo mejor muchos de estos países que si las Islas Caimán y todo esto a lo mejor hay lo que decía el nuevo concepto de paraíso fiscal pero paraíso de leyes tenemos un ejemplo en de la web no que todas las empresas están registradas en de la web

también y todo esto Oye pues vete tú vete tú a saber la verdad es un es un problema todas estas empresas por supuesto ofrecen servicios que son útiles para las fuerzas de del Estado no porque seguramente pues muchos de esos datos y herramientas utilizan para combatir terrorismo pero claro tierra de hackers está plagado de episodios donde estas tecnologías se han abusado para para espiar a ciudadanos Sí el tema de esta empresa también es interesante porque es como un amalgamo un consorcio de empresas incluso asociaciones con otras empresas de otros países como he dicho en la India Francia y tal así que no se da como un poco más miedo y además que operaba entre las sombras nadie se había puesto Aunque hay un hay un citizenlab ya tiene alguna investigación sobre el software espía por ejemplo de Predator de sitex a finales del año pasado Pero bueno no parece ser tan popular no sé si el nombre es difícil de recordar intelexa más que en ese grupo Bueno sí ahí es el concepto de estas metaempresas no yo un documental sobre una en concreto que era me acuerdo de un punto en concreto que era muy bueno que era una empresa que tiene que tiene axe que es el desodorante este que cuando ves la publicidad no es un desodorante para hombres y suele tener así ese componente de uvas a traer a chicas y tal como un componente digamos hay un poco casposo sexual pero a la vez es también la empresa que está detrás de Dove de Dove el jabón este que se suele el marketing ese entorno a que todas las mujeres Pues todo tipo de cuerpos y todo tal y un poco pues leía esta noticia y veían este documental un poco la crítica no de cómo nos venden en marketing dos componentes diferentes pero la misma empresa está detrás estas meta empresas que tiene que nunca hemos oído hablar de ellas y que están dentro detrás de todas esas marcas que nosotros creemos que son empresas independientes Sí sí estas que lo quieren controlar todo vamos que quedan miedo es como los malos de las películas de superhéroes lo mismo Pues bueno Yo creo que hasta aquí Hemos llegado Muchísimas gracias por quedaros hasta el final escucharnos recordad que os dejamos un enlace para que nos deis vuestro voto si así creéis que lo merecemos para los premios ebooks os lo agradeceríamos un montón el formulario es un pelín largo pero estamos en la categoría de creo que era empresa y tecnología y nos podéis Buscar ahí agradeceríamos muchísimo ese voto como siempre también nos podéis apoyar en patrón patrón.com/hackers y por supuesto pues simplemente compartiendo el podcast en redes sociales con amigos con compañeros para ayudarnos a seguir creciendo sí como dice Martín Yo creo que el voto muy importante y vamos a estar muy muy agradecidos va a ser probablemente cinco o diez segundos de vuestro tiempo Así que si podéis Bueno un minutillo que es un formulario un pelín largo Pero bueno un minutillo Mientras nos escucháis mientras escucháis esto Es que a mí el concepto del tiempo se me va Espero Ok si nos podéis ayudar pues lo dicho estaremos muy agradecidos Y como siempre gracias a los patrones sponsors y todos nuestros oyentes sin vosotros no seríamos lo que somos eso mismo Pues nos vemos y nos escuchamos la próxima semana 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