74. MDM y Medibank

información filtrada periodistas muestran como el departamento de homeland Security estadounidense planea monitorizar y actuar contra lo que ellos llaman mdm mis information mis information y mal information licencia para hackear el último ataque de ransomware contra medibank ha convencido Australia a crear un grupo de contraataque ofensivo contra cibercriminales proponer la ilegalización de los pagos de rescate de ransoware e incrementar las multas de brechas de privacidad continuando con nuestra auto impuesto obligación de concienciar sobre los peligros en internet ya tenéis un nuevo episodio del tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast que hoy es el 19 de noviembre de 2022 este es el episodio número 74 yo soy Martín vigo y está conmigo estático en Nueva York mientras yo sigo móvil esta vez en Madrid Alexis porros Hola Alexis qué tal Pues muy bien por aquí como tú dices con bastante frío ya Hemos llegado algún día bajo cero así que bueno de momento la nieve no ha llegado pero pronto así que nada un poco con chaqueta por vivir en Nueva York claro lo que ando es con la chaqueta y el micrófono así para ver cuando hay que grabar el siguiente episodio Sí pero estoy dispuesto Pues nada agradeceros a todos vosotros como siempre queridos oyentes el seguimiento que nos hacéis en redes sociales y por escribirnos enviarnos sugerencias comentarios emails de dudas que algún oyente nos ha enviado Oye tengo este este problemilla me podéis lanzar algunas ideas nosotros encantados de compartir nuestros conocimientos pedazos respuesta te marcaste hay que hay que darte ahí el crédito que vi la respuesta que le enviaste a este a este oyente y juego Eh sí no sí Bueno los dos intentamos proporcionar la mayor cantidad posible de punteros digámoslo así para que Bueno luego vosotros hagáis lo que queráis Pero bueno así tipo consultorio digamos no consultorio de tierra de hackers pero lo dicho estamos muy agradecidos de que contéis con nosotros para todo eso y como digo Muchas gracias por estar suscritos a nuestro podcast y si no lo estáis ya sabéis ir a vuestra plataforma de escucha favorita y suscribíos así estaréis al tanto de cuando sale un nuevo episodio de tierra de hackers estamos en todas las redes sociales Twitter Instagram y Facebook con el handel arroba tierra de hackers linkedin YouTube Twitch como tierra de hackers correos electrónicos ya sabéis podcast@ tierra de hackers.com y os podéis meter en nuestros servidores de discord en tierra de hackers.com/discord Finalmente y como siempre Muchas gracias de nuevo a por responder a la pregunta de episodio que pusimos en Twitter y la relacionada con el anterior episodio fue la siguiente crees que estas herramientas como urlscan de análisis de indicadores de compromiso deberían estar disponibles para todo el mundo tenemos cuatro respuestas y la más dotada con un 92% fue un Sí y gratis seguida de un 5% para no nunca seguida de un 3% para no solo empresas gobiernos y nadie votó a la de no solo de pago Así que vemos Que sí que estas herramientas ayudan mucho a la respuesta a incidentes y a encontrar y echar de nuestras redes a los malhechores perfecto Pues yo como siempre continuo dando las gracias a la gente que nos apoya en patreo muchísimas gracias patreon.com/tierra de hackers por si tú queridoyente te gusta lo que hacemos y nos quieres apoyar ya que directamente utilizamos esos ingresos para reinvertirlo en el podcast y poder seguir creando contenido y parte de este apoyo viene de nuestros sponsors que esta vez es como siempre mona una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y mónate a través de una herramienta de gestión y visualización de telemetría y datos de seguridad

una empresa fundada en vale que está buscando gente para contratar remotamente Incluso en este clima tan tan duro que están viviendo las empresas tecnológicas así que ya sabéis monad.com tierra de hackers @monal.com m o n.ad.com le escribís ahí y lo mandáis vuestro currículum también en este episodio nos esponsoriza on branding Siempre os contamos que en tierra de hackers nos llegan muchos emails de oyentes que Necesitan ayuda porque han perdido acceso a sus cuentas o redes sociales un branding.es es una empresa formada por especialistas en varios ámbitos que se enfocan la reputación 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 está siendo malintencionadamente dañada incluso a borrar la huella digital que dejamos online no Solo han decidido Apoyar el podcast sino que si le contáis que venís de nuestra parte de tierra de hackers tendréis un descuento en servicios si necesitáis ayuda recuperando vuestras cuentas o reputación online Is A On branding.es onb Randy ing.es y no olvidéis mencionarnos y nos lanzamos de lleno a la noticia y para ello hablemos de desinformación y hablemos de ello porque hace un par de semanas el medio de intercept obtuvo años de documentación interna emails y notas confidenciales del departamento de homeland Security de los Estados Unidos que demuestran su empeño creciente de influenciar a las corporaciones tecnológicas para controlar la información que se publica y que ellos consideran desinformación repito filtraciones de información secreta de una agencia gubernamental estadounidense muestra como el gobierno quiere decidir que información publicada en redes sociales es aceptable y cuál no lo es esto dicho así suena muy mal Así que vamos a entrar al detalle vamos a matizar esto y ver lo bueno y lo malo todo esto empezó cuando a principios de este año el departamento de homeland Security Que bueno lo voy a llamar dhs a partir de ahora anunció un nuevo desinformation governance Board un comité encargado de controlar la desinformación online que puede suponer una amenaza para los intereses de los Estados Unidos que bueno Esto de una amenaza para los intereses de Estados Unidos pues es una manera bastante genérica decirlos No porque si hablamos de pues desinformación dañina para la población o algo así pero los intereses de Estados Unidos no tienen por qué ser los intereses de los estadounidenses ya no decir los intereses del resto de las Naciones del mundo entonces solo Resaltar que me pareció bastante orgulloso esto de los intereses de Estados Unidos porque el interés de Estados Unidos puede ser asesinar a un líder político de un país en Latinoamérica por ejemplo Pero bueno de hecho hablan algo que me pareció muy interesante hablan de tres tipos de información falsa lo cual me parece muy muy interesante que debemos repasar por un lado tenemos this information que viene siendo información falsa publicada sin mala intención por ejemplo lo de una copa del vino al día es buena para la salud algo que que no es cierto ya está más que revocado eso o esperar dos horas después de comer para bañarse no es información incorrecta falsa pero que no había mala intención a la hora de publicarlo luego tenemos mis information información falsa publicada con mala intención Como por ejemplo las elecciones durante las elecciones de Estados Unidos de 2016 perdón de 2020 donde salió elegido yoeidón Pues que se hicieron trampas no a la hora de contar votos que es un poco la narrativa de Donald Trump pues esto es información falsa más que he probado que es falso y además Pues evidentemente iba con mala intención o por ejemplo que el cambio climático no existe eso pues si nos basamos en lo que dicen los científicos es completamente falso Por supuesto que existe pero claro Hay intereses corporativos y políticos detrás por tanto es información falsa con mala intención Pero tenemos un tercer tipo mal information información real pero específicamente

parcial o fuera de contexto con Malas intenciones por ejemplo las declaraciones de un político donde solo se publica por ejemplo 5 segundos diciendo una frase en concreto sin el resto del contexto vale Sí que dijo Esa frase pero es que si solo pones esa frase Sin poner todo el contexto Pues claro se puede interpretar de otra manera o por ejemplo lo típico esto lo veo mucho fotos de mítines políticos o protestas y esas fotos están enfocadas con el ángulo perfecto para que parezca que hay más asistentes de los que realmente hay no Bueno pues esto esto de mis information dice information y mal information lo llaman o lo abrevian como mm Lo cierto es que la opinión pública Fue bastante negativa y de hecho la gente llegó a ridiculizar esta iniciativa hasta el punto que al cabo de unos meses se desmanteló Pero también es cierto que el dhs tiene otras iniciativas con las que entre otras cosas monitoriza redes sociales recopilando información esto lo sabemos gracias a juicios por parte de un abogado de Missouri Pues gracias a eso existe un documentos públicos que muestran que el gobierno de los Estados Unidos está presionando a empresas privadas para controlar la narrativa online sobre diferentes temas por ejemplo un mensaje filtrado por parte de un director del dhs a un ejecutivo de Microsoft decía lo siguiente las plataformas tienen que empezar a sentirse cómodas con el gobierno me resulta llamativo que sean tan reticentes a colaborar otro documento que se filtró eran las notas de una reunión entre un oficial del FBI y ejecutivos tanto de Twitter como de JP Morgan el banco este tan grande de Estados Unidos estas notas muestran que el FBI dijo tenemos que exigir responsabilidades a las empresas y medios Twitter cuando fue preguntado por esto por parte de periodistas hizo un comunicado diciendo que ellos no coordinaban con otras entidades la moderación de contenido en su plataforma pero lo cierto Es que gracias a esta documentación y reuniones vemos que parece lo indicar lo contrario que las fuerzas de seguridad del estado que los gobiernos que ciertas agencias Pues sí que sí que tienen algo que decir tanto es así que los gobiernos Y como decía las fuerzas y cuerpos de seguridad del Estado tienen habilitados portales especiales en las distintas redes sociales para reportar contenido que quieren que se elimine llegados a este punto conviene mencionar la parte buena coherente innecesario no de lidiar con la desinformación ejemplos claros como decía antes son las elecciones de Estados Unidos de 2016 donde Rusia hizo campaña brutal de desinformación para inclinar los votos hacia el candidato Donald Trump esa misma desinformación que llevó a la gente hasta el punto de seguir el movimiento cubanon y cuyos seguidores estaban entre los asaltantes al Capitolio movimiento que por cierto bases de información en mensajes anónimos posteados en foros online Como forchan así que es así de fácil poder llegar a manipular a ciertas personas con consecuencias gravísimas como vimos otro ejemplo sería la desinformación durante la pandemia del Kobe 19 desde por ejemplo el origen del virus hasta cuestionar su existencia fue temática de campañas de desinformación masivas creo que todos podríamos entender que no hacer nada en contra del altavoz que probé internet para decir cada uno lo que se quiera y con ellos llegar a miles de personas pues no es ideal sí que hace falta hacer algo al respecto de hecho el tema covity y las elecciones son ejemplos que pone el propio dhs para justificar La regulación del contenido por su parte y lo que ellos consideran mdm no mencionan que ven las campañas de desinformación especialmente enfocadas en zonas y gente marginada de bajos recursos gente que es más fácilmente manipulable y que vive ya en condiciones duras y Busca aferrarse a cualquier mensaje que bueno pues prometa uno ha habido mejor no lo que también conocemos como populismo por parte de políticos pero la cosa empieza a tomar a tornarse cuando también vemos Cómo mencionan por ejemplo o justifican estos programas como los casos de la controlar la información de La retirada de Afganistán porque esto ya es un tema más político y es uno de los

peligros de todo esto el dhs no especifica exactamente qué es lo que considera desinformación o bueno mdm y que una entidad gubernamental pueda meter mano en las decisiones de empresas para eliminar lo que considera dañino pues evidentemente puede ser aprovechado políticamente hay un peligro de que se convierta en una nueva forma de censura Qué pasa si el gobierno considera desinformación la causa de una huelga general Podría empezar a eliminar mensajes en redes sociales que llaman alzarse contra injusticias por ejemplo miremos al pasado y pensemos que en todas las injusticias cometidas por gobiernos de dictadores que fueron derrocados por la o por organización en masa de las personas pues a través de redes sociales no esto ha ocurrido Pues si ahora les damos una manera de poder eliminar todo ese contenido de comunicaciones Pues podría ser un problema pero lo cierto Es que tampoco Tenemos que irnos a un ejemplo tan radical podría ser todo mucho más sutil si sale a la luz unas informaciones que podrían dañar al presidente electo se podría tachar como desinformación y eliminar toda referencia en redes sociales por ejemplo cuando salió el audio y vídeo de Donald Trump hablando despectivamente y haciendo referencias a que podía abusar sexualmente de una periodista sin que ellos supusiese un problema para él no en ese momento no era presidente sino Un mero candidato pero si fuera presidente podría el gobierno decidir tratar eso como fake news y por tanto poder frenar legalmente su difusión por parte de medios y periodistas Pues claro pues eso es algo más sea útil Pero insisto no Tenemos que irnos a casos supuestos tampoco según un exsecretario del dhs en 2004 George Bush que era presidente de aquella presionó al dhs a que subieran el nivel de alerta por el terrorismo en el país porque eso él sabía que influenciaría a los votantes recordemos que Bush fue quien decidió invadir Irak bajo el pretexto de que tenían armas de destrucción masiva lo cual nunca llegó a aprobarse aquí tenemos un ejemplo de cómo un presidente electo presionaba a la agencia a cargo de gestionar esto esto de la información no para una ventaja política y también tenemos los casos de mentiras por parte del gobierno que se remontan incluso a la épica guerra de Vietnam donde también se moldeaba las razones reales por las que Estados Unidos realmente en esa guerra pero uno de los casos más recientes que representa perfectamente el peligro de otorgar El Poder al gobierno de poder decidir Qué es mal information mis information y dice information o no es el caso del portátil de Hunter bidón hijo del presidente actual Joe biden por si no conocéis la controversia el New York post que no New York Times publicó semanas antes de las elecciones entre yoiden y Donald Trump miles de emails supuestamente del portátil del hijo de Joe biden que demostraban que yo ebayden había cometido ciertos fraudes y delitos como decía Esto fue semanas antes de las elecciones momento en el que Rusia estaba a tope con su campaña de desinformación para que Donald Trump volviera a ser elegido y también Añadir que el New York post es un Diario Digital totalmente sensacionalista y con historial de fake news o exageraciones muy muy grande y una Clara postura política Pro Trump Pues bien todo el mundo percibió esta historia de los emails como falsa la historia es que de hecho la rocambolesca porque supuestamente el hijo de Joe biden llevó su portátil para que se lo arreglasen a una tienda en Missouri y jamás fue a recogerlo por tanto uno de los empleados Como nadie venía a recogerlo se puso a mirar lo que había dentro del portátil y mirando los mails se dio cuenta que era de Hunter biden y lo mandó al New York post todos los periódicos digamos serios o creíbles como el Washington post o el New York Times publicaron que esos mails no se podían verificar como reales y claramente poniendo la historia como si fuera completamente falsa hasta aquí uno podría decir bueno Ok pero es que resulta que el FBI pidió a Twitter y otras redes sociales que eliminasen todo contenido referente a esta historia recordemos todo esto sucedió semanas antes de las elecciones

todo rastro de esta historia desapareció de los medios y redes sociales y solo sobrevivía entre las conversaciones de votantes Pro Trump Pero qué pasó pues que casi un año más tarde y ya con Joe biden como presidente esos mismos periódicos tuvieron que admitir que la historia era real y que si bien había muchísimos emails que no se podían verificar si eran reales o no había otros que sí por tanto el FBI forzó a redes sociales y otras plataformas a enterrar una historia que salpicaba a uno de los candidatos en la presidencia tachándolo como información falsa cuando en realidad no lo era no era completamente como siempre yo intento daros no solo supuesto sino ejemplos reales que concierne a las noticias que damos aquí en tierra de hackers para que luego vosotros os hagáis una opinión Así que buscando más ejemplos me topé con un tweet de Edwards noden que publicó de hecho recientemente en el que pone un extracto de una entrevista a Frank Snap un veterano de Vietnam que luego trabajó durante años para la Cia esta entrevista es de 1983 y en ella Este exagente de la Cia explica perfectamente Cómo utilizaban campañas de desinformación para controlar la opinión de los estadounidenses frente a la guerra de Vietnam When we we Don One information me gusta poneros el audio para que lo escuchéis de la propia persona pero si el inglés nos lo vuestro este ex agente de lo hacía Comenta en este audio que una de sus funciones durante la guerra de Vietnam era plantar desinformación en periódicos y medios muy influyentes como el New York Times o el Chicago Daily news lo que hacían era le ordenaban invitar a los periodistas a hoteles y pasar tiempo con ellos para generar una relación amistosa y por supuesto credibilidad de hecho el argot que utiliza en el audio dice le ordenaban cultivarlos a los periodistas En lo cual me pareció súper interesante comenta que lo que hacía para ganar su credibilidad es primero durante un tiempo darles información cierta y en exclusiva para luego más adelante poder manipularlos a que publicas información pues no tan cierta Comenta por ejemplo Que si querían hacer llegar a la población americana la percepción de que los vietnamitas estaban construyendo refuerzos en el sur del país lo que harías comentarle a los periodistas que la Cia ha observado desplazamientos del enemigo a través del Canal sur de Ho chi minh un periodista no tiene manera posible de verificar si esa información es cierto o no y su única opción Pues es lo público o no lo público y mencionan el audio que más o menos un 70-80% de la información de la información falsa que él transmitía a periodistas de manera que no pudieran verificarla acababa publicándose la verdad es que una locura vamos con la segunda parte information information en este extracto Explica cómo generaba situaciones imposibles para que los periodistas pudieran verificar que lo que les estaba contando era falso y el ejemplo que da me parece la leche comenta que cuando plantaba una información falsa a un periodista previamente se lo comentaba Los embajadores Como por ejemplo de Gran Bretaña o Nueva Zelanda dependiendo por supuesto de la historia que quería plantar así el periodista cuando fuera a preguntarle al embajador si lo que le contó este ex agente de la Cia era cierto este se lo confirmaba dando al periodista una fuente que ha veraficado la veracidad de la historia que el ex agente le contó el periodista ya tenía la sensación de haber contrastado la información y por tanto publicarla poder publicarla en realidad la Cia y Los embajadores estaban coordinados y la verificación que recibió no es más que un mensaje falso por segunda vez este extracto acaba con el ex agente arrepintiéndose de haber formado parte de estas operaciones de desinformación en cubiertas por parte de la Cia y dice que no sirven para nada Bueno de hecho acaba diciendo textualmente la propaganda no Debería ser el trabajo de la Cia os dejo un enlace a la entrevista completa y terminó la noticia con la pregunta del episodio Te parece bien que una entidad gubernamental tenga la capacidad de decidir qué es y qué no es desinformación hasta el punto de tener la capacidad de pedir que se elimine y os doy tres opciones

una es que si os parece bien porque la desinformación es un problema muy gordo la segunda opción es que no porque va contra la libertad de expresión Cualquiera podría poder decir lo que quiera en redes sociales siempre que por supuesto vaya acorde a los términos de servicio de eso pero no a gusto del gobierno y la tercera opción también nos diga os digo que no porque quien debería estar a cargo de esto Debería ser a político no una entidad gubernamental así que ya sabéis podéis contestar como siempre en nuestro Twitter arroba tierra de hackers si interesante Martín todo el tema este de la in Miss information this information mal information como como dicen muchos la información vale más que el oro en este caso incluso puede valer más o ser más poderosa más potente que armas de fuego porque con información puedes controlar a masas y con las armas solo los puedes matar y causarle este error no pero esta información que es falsa que de alguna forma estas personas acaban creyendo y es su fe o en lo que se basa sus decisiones día a día es muy escalofriante y la pregunta va muy acorde con el tema de que quién Define Los criterios por los que decimos que algo es desinformation normal information or mis information porque como dices cada país tiene sus intereses Entonces no se puede definir a nivel global o sí o no y cada como digo cada nación tiene sus intereses que no van a ser los mismos de unas de otras así que ya sabemos que a nivel internacional igual no se puede Pero al menos a nivel nacional sí que debería haber algunos parámetros o criterios un acorde con la pregunta que haces claro y de hecho es que me recuerdo un poco porque has hecho tu hincapié en eso no el poder de manipular la opinión ya no solo de una persona sino aparte en masa porque me recuerda la peli de origen que ahora mismo no me acuerdo el título en inglés pero esta de Leonardo DiCaprio lo de un sueño dentro de un sueño dentro de un sueño Ahí dicen esa frase de inception sí de inception esa el el tener la capacidad de implantar una idea en el cerebro de una persona porque es lo que dices tú matar pues puedes matar y tendrías que matar a todos Y tal Pero si tú tú prefieres tener los soldados No si tú eres capaz de manipular a la población para que apoye tu causa es mucho más poderoso que eliminar a los que están en contra de tu Causa porque ahora lo que tienes es más ejército y la verdad esto ya para debates interesantísimos y es un problema muy difícil porque entras un poco en vale quién quién vigila lo que es información y desinformación Y quién vigila al que vigila que que es información o desinformación y así entramos en un en un bucle imposible pero a la vez quedarnos de brazos cruzados como decía yo personalmente creo que tampoco es una buena idea porque porque hemos visto las consecuencias de este nuevo mundo en el que pues alguien con un poco de influencia o puede conseguir influencia incluso comprando likes y tal puede tener un altavoz muy grande para llegar a gente no y y manipularles con información sesgada o directamente falsa y luego pues también como la manera de conseguir de consumir noticias información pues viene filtrada ya pues por buscadores por nuestros patrones por cómo las empresas privadas perciben qué es lo que queremos leer luego también en general por mucha gente cae en el problema de del confirmation vallas no que le llaman el el tener una creencia y Busca información como para redoblar que que es correcta esa información en vez de Buscar información que va en contra de eso Y entonces tomarse una decisión no en base a eso es un problema muy complicado de resolver la verdad pero no sé yo y por eso le preguntamos a nuestros queridos oyentes si agencias gubernamentales deberían ser las que están a cargo de esto y más habiendo por eso insisto casos reales en los que esto se ha abusado con motivaciones políticas sí como dices también el tema de que hay gente que va un poco indaga más no los que en inglés se le dice fake checkers que sea un poquito tipo Snow de no que van ahí investigan un poquito intentan destapar secretos y los publican con el objetivo de bueno de de hacer la verdad un poco

democrática y Que la conozca a todo el mundo Así que un poquito gracias a ellos a veces se destapan todos estos meollos pero seguro que hay muchos que pasan desapercibidos y como has dicho el tema de Clinton todo eso que Comenta Pues a saber cuántos años hace de eso y ha salido a la luz ahora no O sea que Imagínate los que deben haber por ahí todavía tapados Sí claro porque a veces es fácil ir solo por Donald Trump y tal porque Bueno Ese hombre ya está rodeado de bulos y de todo no pero es que también lo tenemos con los presidentes entre comillas los buenos no Por así decirlo que nadie por favor me malinterprete con lo bueno eso los malos no es ninguna opinión política pero creo que que se me entiende Lo que quiero decir No sí pues también ha estado ha estado ahí esto el control por parte del FBI que luego de algo que se provoque era cierto pero ya ya estaba elegido el presidente Entonces esto la verdad como mínimo da para un buen episodio de tierra de hackers Sí sí que no se escapa nadie no que que no haya pecado que tire La primera piedra aquí nosotros arrojando luz sobre todo lo que nos podemos encontrar y explicar y ya que luego los oyentes hagan su opinión con toda la información que es como tiene que ser lo que decías de la información Sí yo creo que es lo más valioso en este mundo me recordaba cuando hacías el comentario Se parecía el tema la filosofía esta del tsum tsum no del arte de la guerra conoce a tu enemigo y Únete a él digamos estilo como sabes como el cuento de La caperucita roja un buen ejemplo de ingeniería social efectiva pero fallida por el lobo pero relacionado con el tema de cultivar a los periodistas no ahí te vas ganando su confianza Y luego les engañas y le das información cultivarlos es que es buenísimo cuando ves el vídeo te dice no así mi trabajo era cultivarlos en plan ahí los tienen como embriones ahí dándoles de comer lo que ellos gustan Ahí va y de repente ya los tienes ahí bailando como me venía viendo un poco el tema de planta porque luego además hemos dicho el tema de que sí ponen una una una semillita de información en su mente y germina entonces un poco el SS el agüita tal a la planta Ah También tenemos un buen jardín vamos Total que muy buena Martín y nada seguimos para adelante queremos hacer un breve inciso para darle las gracias a nuestro patrocinador brawler que nos apoya en el podcast y que hace muy poquito acaba de lanzar un servicio en la nube para proteger tu infraestructura en aws hablamos de brawler pro y sus ass el servicio gratuito más completo de seguridad para aws prunel Pro está y bueno una vez dicho esto dentro noticia esta noticia un poquito va tiene un poquito de ingredientes interesantes digámoslo así ransomware el gobierno australiano la Casa Blanca cibercriminales la policía federal Bueno un poquito de todo aquí traemos para hacer un buen cóctel en esta noticia Y qué ha pasado pues A mediados de octubre medibank un proveedor privado australiano de seguros médicos fue víctima de un gran ataque de ransomware la empresa dice que el grupo de cibercriminales conocidos Como blog XX irrumpieron en su red robaron archivos internos cifraron muchos de estos archivos y exigieron un rescate inicialmente Este era de 10 millones de dólares americanos pero la empresa se negó a pagar ya que no pensaban que pagar al rescate evitar que los cibercriminales filtraran los datos robados entonces blog x x dijo Mira vamos a ser buenos te bajamos el precio del rescate de 10 millones de dólares a 9,7 millones de dólares americanos uno por cada usuario afectado y bueno aún y con esta rebaja que es bastante minúscula comparada con la cantidad inicial mediban que igualmente se negó y sigue sin haber pagado el rescate sin darse por vencidos el grupo de ransomware comenzó a filtrar algunos de los registros de pacientes de medibank para intimidar a la empresa y ejercer presión Pública para que pagaran el rescate una de las primeras filtraciones de los datos de medibank robados por el grupo blog XX fue un archivo etiquetado como aborsions punto csv que es un archivo que contiene información de pacientes que recibido algún tipo de servicio médico obviamente relacionado con

el aborto y las siguientes filtraciones de datos no fueron menos preocupantes había un archivo llamado lista buena Supongo que de personas saludables Pero bueno Igualmente habían recibido algún tipo de servicio médico otra llamada lista de Traviesos o notty list en inglés que probablemente Pues supongamos que puede tener información de pacientes que consumen sustancias de algún tipo o tienen algún tipo de dolencia y otra lista otro archivo filtrado fue uno que se llamaba busy que sería algo así como borrachos que incluye usuarios que buscan ayuda con su dependencia con el alcohol los archivos robados afectan a 9,7 millones de usuarios 1,8 millones de los cuales son internacionales y contienen datos confidenciales personales como nombre completo fecha de nacimiento direcciones de email números de pasaporte y también algunos temas médicos aunque nos especifica exactamente Cuál es de todas formas los cibercriminales también pudieron acceder a datos de atención médica específicamente de 500.000 usuarios que incluye información como nombres de los proveedores de servicio y sus ubicaciones las ubicaciones donde a los pacientes se les facilitó el servicio médico y códigos de diagnóstico y procedimientos médicos es decir los servicios médicos que recibió cada paciente este grupo de rancho muere también accedió a información de 5.200 usuarios de la aplicación móvil medibanks my home hospital en cualquier caso finalmente medibank se puso en contacto con los usuarios afectados algunos de los cuales ya no eran clientes activos de medibank Desde hacía incluso más de 10 años esto es preocupante y no parece que esté muy bien que la empresa no debería guardar los datos de los clientes por tanto tiempo especialmente si llevan tantos años sin ser clientes las leyes de privacidad deberían controlar este problema se ha hablado de que puede haber alguna conexión entre blog XX este grupo de ransomware que ha atacado a medibank y revivel el archifamoso grupo de ransomware y esto se debe a que en primer lugar la operación utiliza un cifrado similar al que se podía encontrar en la web de Rebel en la red de Thor y segundo a que la antigua web de Rebel en la red Thor ahora redirecciona el sitio web de Thor donde blog XX ha filtrado los datos la exposición de datos personales y médicos obviamente no ha sentado nada bien a los usuarios afectados ni al gobierno australiano Ok en resumen quedaos con que medibank fue víctima de un ataque de ransomware por parte de Blog XX Por otra parte tenemos que a finales de septiembre hubo un incidente de ramsember similar optus la segunda operadora de telecomunicaciones más grande en Australia que expuso datos de clientes como nombres completos fechas de nacimiento números de teléfono direcciones de email direcciones postales y documentos de identidad como permisos de conducir y pasaportes y aunque no se indicó A cuántos clientes afectó La Brecha solo decir que optus tiene unos 10 millones de usuarios en resumen otro incidente de ransomware contra optus una empresa australiana y de hecho más recientemente a finales de octubre el departamento de defensa australiano desde lo que había sido víctima de un ataque de ransomware contra su plataforma de comunicaciones llamada force.net según comentan no hay indicios de que datos confidenciales militares fueran comprometidos en el ataque Aunque sí que comentan que entre unos 30.000 y 40.000 registros fueron robados que contienen datos de personal militar activo y retirado así como personal civil el compromiso inicial se sospecha que fue debido a la falta de un parche de un producto de llamado sitecore que es una plataforma danesa de gestión de contenido web que se utiliza para correr forcent aunque esto aún no se ha confirmado también se comenta que el gobierno australiano puede no estar utilizando la autenticación de doble factor en esta plataforma fortnite que fue comprometida al igual que en otros sistemas gubernamentales que es de preocupación y puede haber ayudado a la intrusión de nuevo resumo otro ataque de ransomware contra el departamento

de defensa australiano Total que en respuesta a estos tres ataques de ransomware sobre suelo australiano recordamos medibank optus y el departamento de defensa australiano sobre todo a la de medibank el gobierno australiano se ha puesto en pie de alerta y ha actuado En consecuencia y lo que ha hecho es responder de Tres formas distintas primera es que recientemente el gobierno australiano aumentó las sanciones máximas por infracciones graves de privacidad a través de la enmienda de la legislación de privacidad aplicación y otras medidas proyecto de ley 2022 Mientras que el máximo es actualmente 2,22 millones de dólares el nuevo límite será el mayor de los siguientes tres valores o 50 millones o tres veces el valor del beneficio obtenido por el uso indebido de los datos comprometidos o el 30% de la facturación ajustada durante el periodo de incumplimiento Así que la mayor multa puede ser de unos 50 millones de dólares que es bastante más que los rescates de ransomware en el caso de medibank que he comentado es de hecho cinco veces más que lo que pedía el grupo de randsomware Blog XX la segunda medida es que la ministra de asuntos interiores de Australia Claire o'neal sugirió que el gobierno podría analizar una ley para prohibir por completo los pagos de ransomware y de extorsión con la esperanza de eliminar la motivación financiera detrás de la mayoría de estos ataques claronil elogió la decisión de medibank de no pagar a sus atacantes por el rescate y aprovechó esta decisión para sugerir esta propuesta de ley los que se oponen a esta medida justifican que esto Solo haría que los pagos se hicieran a escondidas incluso utilizando terceros en otras jurisdicciones en otros países y hacerlo todo digamos de forma más ilegal o en negro esto es una medida muy radical porque pondría a las víctimas en un dilema de pagar para recuperar sus datos o no y si ir pagan a tenerse las consecuencias de esta ley ya que sería ilegal por poner otro caso en Estados Unidos la ley no prohíbe el pago de rescate de ransomware Sin embargo sí que pone multas y sanciones a cualquier organización que realice transacciones financieras con grupos específicos de ransomware como Rebel Así que si comprueba esta ley propuesta Australia podría ser el primer país del mundo en el que el pago del rescate de ransomware sería ilegal y como comento la tercera respuesta del gobierno australiano Es que este mismo está organizando una operación permanente a nivel mundial para dar caza a los sindicatos y grupos criminales que tienen como objetivo Australia en ataques cibernéticos la policía federal australiana dijo que tomó medidas inmediatas incluidas técnicas en cubiertas y el rastreo de sitios de delitos cibernéticos para identificar a las personas que abusan de estos datos onil comenta que instituciones como el Banco Nacional de Australia recibe 50 millones de ataques al mes y la oficina de impuestos al menos tres millones al mes estos ataques pueden contener tanto temas de ransomware como no pero es una cantidad muy elevada os dejo ahora con un clip de una en la que comenta la acción del gobierno australiano en respuesta a los ataques de ransomware today y os comento lo que he dicho Neil en español parafraseándola esto es Australia levantándose y respondiendo no vamos a quedarnos sentados mientras nuestro ciudadanos son tratados de esta manera y permitir que no haya Consecuencias al respecto que esta nueva iniciativa sería un esfuerzo conjunto compuesto por personal de la Policía Federal australiana y la dirección de señales de Australia que es responsable de la inteligencia de Señales extranjeras el apoyo a las operaciones militares la guerra cibernética y la seguridad de la información y también es parte de la comunidad de inteligencia australiana como parte de esta iniciativa otro tema interesante de la reacción de Australia la Comenta también o y os dejo un extracto a continuación de la entrevista que le hicieron huevo resumiendo en español la ministra del interior de Australia dijo Esta es una nueva operación una fuerza permanente de 100 de los mejores expertos cibernéticos más capaces de Australia que emprenderán esta tarea por

primera vez atacar ofensivamente a estos cibercriminales Este no es un modelo de vigilancia donde esperamos a que se Cometa un crimen y luego Tratamos de entender Quién es y hacer algo con las personas responsables ofensivamente vamos a encontrar a estas personas cazarlas y debilitarlas antes de que puedan atacar a nuestro país la verdad es que estas declaraciones dan escalofríos son muy buenas y esto es meterse ya mucho en temas de contraataque ofensivo muy interesante Total que Australia está dando a su policía federal Carta blanca para matar digamos así pero bueno en este caso más Cibernético sería Carta blanca para hackear Aunque al más puro estilo James Bond si me lo permitís queridos oyentes se me ocurren dos títulos para nuevas películas desde Australia con amor o licencia para hackear lo que siempre decimos si algún guionista de Hollywood nos está escuchando que nos contrate para que le demos ideas que tenemos unas cuantas vamos que no se van a quedar de brazos cruzados y los australianos van a darles una buena lección a estos cibercriminales sobre todo a los relacionados con ransomware sobre el tema del contraataque ofensivo Aunque pocos en el pasado han habido algunos casos de este tipo por parte de del orden Como por ejemplo la forma en la que los policías holandeses engañaron al grupo ransomware Dead bolt haciéndoles creer que habían pagado el rescate y revertiendo y recuperando la transacción de criptomonedas justo después de haber recibido cada una de las 150 claves de descifrado que pudieron recuperar También tenemos el caso del departamento de justicia de Estados Unidos recuperando la mayoría de los 4,3 millones de dólares americanos pagados como rescate al grupo Dark Side por parte de Colonial pipeline Los investigadores del FBI dijeron que rastrearon el pago del rescate en múltiples direcciones de bitcoin que Dark Side movió de unas carteras a otras finalmente pudieron confiscar 63,7 de los 75 bitcoin pagados después de obtener la clave privada de una cartera y otro caso es el del US Cyber command conjuntamente con el FBI que comprometieron los servidores del grupo de ransomware revill después del ata contra casella algo interesante es que no fue el gobierno de Estados Unidos quien realizó las acciones ofensivas de comprometer los servidores de Rebel sino un socio extranjero del gobierno norteamericano me pregunto si fue para evitar manchar al gobierno de crímenes Porque al fin y al cabo Según la ley de Estados Unidos de acto de fraude y abuso informático que se denomina con Peter flood en avise comprometer sistemas sin orden judicial Es delito aunque sean de cibercriminales y enlazando esto con la nueva estrategia de Australia de licencia para hackear interesante saber si el gobierno australiano va a tirar va a contratar a empresas extranjeras también para realizar esto vamos que es como un bucle infinito se podría ver nunca se acaba el tema porque aunque queramos cerrar y desmontar grupos cibercriminales tenemos que contratar a otros equipos llámales ofensivos de software espía o similares para realizar el trabajo sucio Aunque todo apunta que en el caso australiano van a ser ellos mismos la propia policía federal la que va a obtener los permisos y las órdenes judiciales necesarias para realizar todo el ataque ofensivo así que bueno igual de esta forma se puede hacer de forma más legal a todo esto comentar que tanto Dark Side como Rebel cerraron después de estas operaciones ofensivas contra ellos porque según se ve Incluso en las comunicaciones de los operadores de estos dos sitios de ransomware estaban un poco preocupados por lo que les pudiera pasar ellos mismos ya que fuerzas del orden pudieron comprometer estos servidores Y obtener información relacionada con ellos mismos entonces vemos que estas operaciones ofensivas sí que tienen un gran impacto contra estos grupos de ranson work ya que cierran después de verse comprometidos la declaración de onil llegó el mismo día en que la policía federal australiana emitió un comunicado de prensa que identificaba a blog XX como digo potencialmente

Rebel los cibercriminales que atacaron a medibank como ubicados en Rusia y dijo que Australia mantendrá conversaciones con la policía rusa sobre estas personas el Primer Ministro de Australia compartía el mismo sentimiento que la ministra del interior y dijo que estos incidentes eran muy desagradables que requieren una reprimenda y que sin nombrar a Rusia el gobierno del país en el que se encuentran los cibercriminales debe ser responsable el australiano no es el primer gobierno que decide dedicar parte de su esfuerzo o actividades ofensivas contra cibercriminales tanto Estados Unidos como el Reino Unido Tienen grupos de actividades ofensivas contra cibercriminales desde 2017 Aunque nunca han dicho que tengan un equipo tan grande de 100 personas dedicadas a tiempo completo a esta tarea el hecho de que este rol tan proactivo y ofensivo lo tome actualmente Australia puede jugar a favor de todos porque si fuera Estados Unidos o Reino Unido quien se metiera en el campo de detener a grupos de ransomware atacarlos arrestarlos y meterlos en prisión cuando la mayoría están en Rusia Pues podría tener repercusiones graves debido al conflicto actual en Ucrania debido a que tienen 100 personas full time por un tiempo indefinido estos equipos pueden definir mejores planes para conocer al enemigo y atacarlo donde más le duela en el momento adecuado en lugar de lo que normalmente se hace actualmente A falta de tiempo que es atacar pronto y primero lo que a veces no da éxito porque no se actúa en el momento adecuado otro tema es que Australia puede ser menos burocrática y tener más facilidad y rapidez de actuación si la comparamos con Estados Unidos o Reino Unido al ser más pequeña y las fuerzas del orden conocerse mejor vamos a ver cómo evoluciona el tema y si realmente las acciones de Australia surgen efecto y reciben menos ataques de ransomware o si al menos Se pueden recuperar de forma más rápida y sin tener tanto impacto financiero y perdiendo tanto dinero finalmente comentar que a finales del mes pasado se dio lugar la segunda Cumbre internacional contra el ransomware en la casa blanca y que se enfocó en prioridades Como las siguientes como resistir a los ataques como romper o interrumpir la cadena de los ataques Cómo contrarrestar el movimiento ilícito de las criptomonedas como ejercer presión sobre naciones clave de forma diplomática y Cómo mejorar asociaciones público privadas este evento de dos días de duración tuvo la participación de 36 países la Unión Europea y 13 empresas privadas para discutir estrategias de colaboración internacional sobre Cómo combatir el ransomware no voy a mencionar todas las naciones que participaron Pero algunas de interés son Australia en primer lugar Ucrania Reino Unido España México República Dominicana Nigeria muy interesante Singapur y bueno muchos más y sobre el tema de empresas privadas pues unas muy interesantes que participaron fueron crowd strike Mandy ant la Cyber Street a lions Microsoft e incluso telefónica esta Cumbre fue a puertas cerradas Aunque la sesión de cierre se puso online en internet en YouTube y es interesante escuchar los tres minutos que tiene cada país para concluir el programa Y que en el que comentan sus ideas de futuro para combatir el ransomware vamos a poner el link al vídeo en las notas del episodio Así que si le queréis echar un ojo ahí lo tenéis también Durante este evento comentaron Algunos números de incidentes de ataques y dijeron que pudieron recopilar unos 4.000 ataques de ransomware en los últimos 18 meses fuera de Estados Unidos en el sector de la salud ha habido importantes ataques de ransomware contra el servicio nacional de la salud de Irlanda Nueva Zelanda hospitales de Estados Unidos hospitales de Barcelona y cientos de clínicas dentales en todo el mundo y más recientemente en octubre common Spirit la segunda cadena hospitalaria sin ánimos de lucro más grande de Estados Unidos fue víctima de un ataque de ransomware en el sector gubernamental pues han habido múltiples ataques todos ya sabemos los ataques contra Costa Rica también Montenegro banco de zambia la

ciudad de Palermo en Italia bueno Total que este es realmente un problema global que afecta a tanto a empresas como a gobiernos y bueno a pesar de que haya tanto ataque de ransomware Lo bueno es que al menos gobiernos de todo el mundo y empresas privadas están intentando trabajar de forma conjunta para poder mejorar la ciberseguridad y detener los ataques de ransomware tanto como sea posible en cualquier caso y esto ya lo hemos comentado en episodios anteriores ya sabéis lo vuelvo a resumir lo mínimo que tenéis que hacer para poder salir de una pieza de un ataque de rancho muere es parchear frecuentemente vuestros sistemas y teléfonos activar el doble factor en todas vuestras cuentas usar un gestor de contraseñas y cambiar las cuentas por defecto vigilar con los ataques de phishing e ingeniería social hacer copias de copias de seguridad y limitar la información que publicáis online Así que que no cunda el pánico con el gran Software que Australia ya tiene licencia para hackear Qué bueno lo de la Cumbre de del ranso muere Alexis eso me eso me ha molado y sobre todo que España sea parte de eso es que es un problema gravísimo porque cada vez lo hacen más grupos parecen que no que cada vez sea más sencillo pero es que hay tantas y tantas empresas que están dispuestas a pagar porque si no significan la eliminación de su de sus empresas y quedan totalmente bloqueadas por no hablar del peligro para las vidas humanas cuando se trata de hospitales por tanto entiendo que haya una Cumbre entre países y a la vez es sorprendente que la haya porque Wow Imagínate si es serio que ya tenemos reuniones en plan la ONU el g7 bueno en este caso el g36 para temas de de ransomware me pareció también muy interesante que menciones el tema de licencia para hackear Esto me recuerda a cuando hablamos en tierra de jaggers por primera vez de ello que era entre cuando hicimos ese especial ciberguerra no que que Rusia había dado licencia no como era Ucrania había dado licencia para defenderse y Rusia había dicho que se podía piratear todo el software de empresas que no fueran rusas que no no se consideraba un delito ahí tenemos esa ese primer yo creo incidente de un de un gobierno no dando licencia para hackear dando como una una pausa en la legislación respecto a delitos informáticos diciendo venga para adelante es interesante A veces sí que se dice no que la mejor defensa es una buena ofensa ofensiva O sea que quizás esa un poco el approach no que están haciendo ahora allí Sí sí lo que tú dices el gran Summer yo creo que hoy en día es uno de los ataques más temidos y más impactantes de todos porque bueno tienes temas de fishing no temas de compromiso de identidad ok Te de robo de criptomonedas que se han visto muchos Ok también es muy muy preocupante pero no sé temas de ransomware pueden causar incluso más daño que un robo de criptomonedas depende de las criptomonedas que tengas en esa cartera que has robado No pero en la mayoría de los casos es un negocio muy muy beneficioso para los cibercriminales y yo creo que es lo primero que igual deberían empezar a enseñar ya digamos las escuelas y todo no una terraza ataque de phishing es uno uno de los de los componentes de un ataque igual de ransomware Pero puede venir por cualquier otro por cualquier otra vía una una un fallo de haber parcheado un sistema y hay un exploit que no tiene por qué ser de 0 d y hemos visto y se meten de esa forma ahí en la red interna y luego de ploian despliega en el transfer bueno Y yo como móviles Martín hay mucha concienciación de esta global desde la casa blanca que se haya que se haya que haya dado lugar este esta segunda Cumbre internacional contra el ransomware y tanta gente no solo tantos países sino también el tema del empresas privadas estén involucradas dice mucho y yo te quería preguntar a ti Martín de hecho ahora me ha venido a la mente que hace poco has estado en una en un evento de la guardia civil creo que era de concienciación y educación de ciberseguridad no sé Ahí Cómo se ha visto el tema del ransomware pero me preguntaba si si lo han tocado bastante si es la principal preocupación que sea un poco

motivado a los asistentes a los estudiantes tú como mentor que qué opinas que comentas de allí pues es buena pregunta en este caso no no iba por ahí los tiros porque es una competición de hacking para universitarios y para estudiantes Entonces sí que hubo un par de charlas Pero bueno eran charlas dadas yo de hecho di una sobre hacking a protocolos Y tal propietarios Pero lo principal era un evento de hacking pero las charlas que hubo un par de criptografía y tal se tocó un poquito el tema de ransomware Pero bueno fue un evento super guay Y tal Pero bueno no no se cubrió realmente a fondo la problemática del ranso mujer en este caso Ah ok lo decía yo porque en el pasado cuando trabajaba paraleloide por ejemplo organizaba un evento que se llamaba Cyber Street competition competición de amenazas cibernéticas y teníamos una especie de competición también pero era tema de un día era como un saber work game tenías los estudiantes tenían que responder a un ataque y podía ser cualquier tipo no en aquellas en aquella época lo más lo más sonado era el tema de fishing y robo de credenciales y va a hacer transferencias digamos sin personal a los jefes y conseguir mover dinero de una cuenta a otra no una cuenta que finalmente controlada por el atacante Pero me pregunto si se podía hacer algo así en plan más enfocado a temas de ransomware donde los los participantes tienen que responder remediar el tema recuperarse en restaurar las operaciones de negocio y aprender a lo largo de toda esa respuesta Sí la verdad la verdad es que sí sí pues nada más ya vemos que el ransomware tiene los días contados como se podría decir a ver a ver si es verdad esperemos que que sea así y nada y todos ya sabéis con las sugerencias que hemos dicho para protegerse un poquito y estar alerta sobre esos ataques y sobre todo seguirnos y así sabréis sobre las incidentes de razón web y de otros temas de ciberseguridad tierra de hackers es una de las mejores protecciones contra el gran Support puede ser nuestro nuestro nuevo moto en vez de tu noticiero de diversibilidad ha hecho podcast tu defensa contra el ransomware tierra de hackers bueno queridos Muchas gracias por quedaros hasta hasta el final Como siempre yo ando de rutilla como decía Alexis entre navaja Negra este evento de la guardia civil y vienen ahora otras conferencias donde estaré ha sido una pasada una auténtica pena al éxito todo el mundo pregunta por ti que no andes por aquí Pero bueno ya ya te cuadrará con alguna conferencia por aquí por España que tenemos muchísimos muchísimos oyentes porque es una gozada cuando vienen a saludarte A darte un abrazo a pedir pegatinas pedir fotos buah para mí increíble es una sensación muy muy gratificante así que muchísimas gracias Sí me has contado mucho y me has enviado fotos y lamentablemente me lo he perdido y sí muy a muy pesar pero pero me encanta que tú al menos hayas disfrutado y estés ahí representando a los dos pues así que estoy estoy en vuestro por supuesto Pues como siempre decimos pedimos recordar seguirnos en redes sociales Twitter Facebook linkedin en YouTube Twitch estamos por ahí nos podéis apoyar en patreon.com / tierra de hackers de verdad que marca la diferencia y si no algo que podéis acceder gratuito pero que nos ayuda muchísimo es dejarnos comentarios en la plataforma donde nos estés escuchando darnos cinco estrellas y así creéis que lo merecemos Y como siempre os decimos nos escuchamos en el siguiente episodio y esperemos que volváis a estar aquí chao chao nos vemos nos escuchamos pronto adiós adiós a la vista 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