una agencia de contrainteligencia americana decide comprar información del tráfico de internet a nivel mundial a una empresa privada para evitar la burocracia de hacerlo legalmente en el reciente conflicto bélico originado en la franja de gaza múltiples grupos ciberactivistas eligen bando entre jamá o Israel o incluso ambos y atacan infraestructura crítica de gobiernos empresas de comunicación y proveedores de energía eléctrica estamos en el mes de la ciberseguridad y lo celebramos con otro episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 17 de octubre de 2023 es el episodio número 109 yo soy Martín vigo y está conmigo como no podría ser de otra manera Alexis porro Hola alis qué tal aquí andamos Martín preparando ya el temilla de de Halloween no sé si habéis escuchado ese audio que circula por las redes What vital feliz Halloween Pues lo mismo aquí ya se ven los colores otoñales Supongo que por ahí también las calabazas en las en las escaleras de las casas y y vampiros y te empieza a pegar fuerte empieza a pegar fuerte Sí sí la gente se se excita mucho y y bueno pone digo madre mía la de dinero que se ha gastado esta persona en en poner toda esta decoración fuera de de la casa pero bueno es interesante eh cuanto menos e nada que comentaros que como siempre estamos en todas las redes sociales nos podéis encontrar como tierr deeh hackers o @ tirad hackers también invitados estáis a suscribiros a tierra de hackers en vuestra plataforma de podcast favorita y también sois más que Bienvenidos en discord ahí tenemos un canal al que podéis acceder vía tirad hackers.com baris perfecto Pues yo por mi parte eh darle las gracias a nuestros mecenas de patreon y a nuestro sponsor como siempre desde el principio monat una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast imon con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon vale Y que está buscando ingenieros con experiencia de ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web monat.com y le podéis enviar el currículum si así lo deseáis a tierrade hackers @m monat.com también antes de empezar recordaros que tenemos pendientes aún abierto el plazo para las votaciones a los premios podcast de ebox si nos escuchas en ebox o si tienes un usuario de ibox o si te gusta tanto lo que hacemos Que estarías dispuesto a crear un usuario de ibox para votar noos por favor hazlo que nos ayuda un montón y sería un lujazo ganar el concurso para votar noos te lo ponemos superfácil vas a tierra de hackers.com bar votar te dejo también en las notas del episodio el enlace pero tierra de com bar votar para así poder votar noos como uno de los podcast que más te gusta y por último recordaros que si eres un desarrollador web o quieres aprender sobre seguridad en ese entorno puedes apuntarte ya al curso cyb Security for web developers que impartiré de manera presencial en Barcelona el 7 y el 8 de noviembre de este año es en inglés y está orientado a que aprendas y comprendas las vulnerabilidades más habituales en la web si quieres apuntarte si quieres venir conmigo a este curso que voy a estar impartiendo puedes hacerlo en tierrade hakers.com bar websecurity ahí tienes toda la información tierrade hackers.com barwe bsec purity y también te dejo el enlace en las notas del episodio empezamos las agencias de inteligencia bueno y para el caso de esta noticia que os traigo de contra inteligencia tienen como misión estar al día de todo lo que está pasando de las amenazas a las que está expuesto Pues el país para el que trabajen pero sobre todo de surtir de información de inteligencia no a otras entidades para que puedan decidir una estrategia de ataque o defensa adecuada estas agencias viven de recolectar procesar y diseminar información a gran escala y la clave de esta noticia está en la recolección gracias a documentación interna del gobierno de los Estados Unidos que fue filtrada al público Bueno más que filtrada obtenida mediante un foer request por parte de un periodista llamado Joseph

Cox que hemos cubierto mucho de su trabajo aquí en este podcast sabemos que una de sus agencias responsables de la contrainteligencia ha decidido acelerar la fase de recolección de información recurriendo al sector privado y todo esto porque recolectar esa información por los cauces correctos en este caso que sería pedírsela a la nsa llevaría días en vez de horas Ya solo con este preámbulo a esta noticia ya tenemos muchas cosas que analizar por un lado agencias de inteligencia saltándose los protocolos establecidos en algo tan sensible como obtener la información de tráfico de internet de millones de personas luego tenemos que esto fue así por no querer esperar un par de días No es que el proceso habitual llevase meses o años y puedo entender que para algo de Pues no sé de extrema urgencia como una amenaza inminente esto sea así pero no parece que fuera el caso de que fuera una amenaza inminente Y ahora os explico por qué pero lo más importante es que ha han recurrido al sector privado para obtener lo mismo que les brindaría nada más y nada menos que la nsa O sea que empresas privadas tienen la capacidades similares voy a decir de recolección que la agencia de inteligencia más importante y probablemente invasiva del mundo es lo que lo que estamos pensando Aquí bueno por no hablar del coste para los estadounidenses que requiere comprar esto del sector privado respecto Pues a obtenerlo gratis de otra agencia no pero bueno Cuál fue la razón por la que esta agencia tuvo que comprar tráfico de internet a nivel mundial Pues según los documentos filtrados para rastrear las actividades de hackers bueno matizo que esto es lo que dice el documento lo de hackers ya sabéis que como decimos siempre y como decimos todos en la industria el hacker no define a un delincuente yo lo digo así pero matizo que se refieren probablemente a ciberdelincuentes a mí De hecho esto me huele a que tiene algo que ver con la Deep web y des desenmascarar a estos ciberdelincuentes porque si no porque ibas a comprar metadatos información del tráfico en internet a nivel mundial es que no tendría mucho sentido acceder a esta información la agencia en cuestión que está comprando estos datos es el defense counter intelligence and Security agency o dcsa y lo que compran exactamente son datos de la actividad en internet como conocida también como netflow Según Wikipedia y cito textualmente netflow es un protocolo de red desarrollado por Cisco systems para recolectar información sobre tráfico IP netflow se ha convertido en un estándar de la industria para monitorización de tráfico de red y actualmente está soportado por varias plataformas los dispositivos con netflow habilitado cuando activan la característica de netflow generan registros de netflow que consisten en pequeños Trozos de información que envían a un dispositivo central o servidor cada registro de netflow es un paquete pequeño que contiene una cantidad mínima de información Pero en ningún caso contiene los datos en bruto del tráfico es decir no envía el payload del tráfico que circula por el colector sino solo los datos estadísticos estos datos incluye dirección de ip de origen dirección de ip de destino Puerto udp o tcp de origen y de destino el protocolo IP y algo más de información que ya se va a otros sistemas como decía antes me tiene pinta de ser un intento de de anonimizar a usuarios de la red Store que navegan por la Deep web según la documentación esta información les cuesta las arcas del Estado millones y millones de dólares y lo compran directamente de una empresa llamada Team simr Okay veamos qué nos dice la web de team simr sobre sus capacidades y productos su producto estrella es Pure Signal recon y lo describen de esta manera herramienta de consulta de inteligencia de amenazas para analistas de ciberseguridad creada por analistas de ciberseguridad proporciona un acceso único a la telemetría de tráfico en internet de Pure Signal el océano de datos de inteligencia de amenazas más grande del mundo los analistas utilizan Pure Signal recon como parte de un proceso de defensa cibernética para identificar y bloquear amenazas cibernéticas externas independientemente de su origen ubicación geográfica o posición en la cadena Bueno yo indagué un poquito más en las capacidades de estos productos y dicen también que puede citotex rastrear actividad maliciosa a través de una

docena o más de proxis y vpns para identificar el origen de una amenaza cibernética Bueno vamos a desgranar esto un poquito básicamente esta empresa está recolectando información de tráfico en internet y lo ofrece lo vende a agencias para que bueno puedan analizarlo y con ello pues luchar contra el cibercrimen no o hacer lo que ellos consideren oportuno la cuestión aquí lo que una de las cosas que más me llama la atención es esto de rastrear actividad a través de proxis que bueno de proxis vale pero de vpns no teórica ente las vpns cifran nuestros datos de tal manera que incluso nuestro proveedor de internet no tendría acceso Bueno al contenido que eso ya en principio pues netflow como explicaba antes no da el contenido del tráfico sino metadatos como la ip de origen y destino pero claro si aquí nos está diciendo que yo utilizo una VPN para visitar una web la que sea y con esto puedes averiguar qué web vps la que yo Estoy visitando se está acertando la protección que brindan las vpns lo cual me dice que o tienen acuerdos con vpns y por tanto las vpns nos están mintiendo cuando nos dicen que no almacena nuestros datos o son vpns falsas o puestas o de alguna manera vamos a decir esponsorizar por gobiernos o o otras empresas privadas para tener a de manera digamos encubierta acceso a sus datos me consta por amigos que trabajan en en temas de inteligencia Y ciberinteligencia que sí eh se puede acceder a datos de ciertas vns nosotros mismos aquí hemos cubierto vpns noticias de vpns que eran falsas donde se está recolectando la información o incluso de vpns que no aparentaban falsas como tal pero que fueron comprometidas por ciberdelincuentes y publicaron información de tráfico de sus clientes por tanto como mínimo estaban mintiendo a sus clientes cuando decían que su información era Era privada o por lo o incluso que ni siquiera se estaba logando tú Alexis trabajaste en temas de ciberinteligencia de inteligencia de amenazas has utilizado algún tipo de estas herramientas y incluso has llegado a poder ver tráfico que que provenía de vp No la verdad que yo no he estado en el mundillo de la inteligencia de amenazas pero sí que estoy de acuerdo con que hay que tener mucho cuidado con las vpns y Bueno hay empresas como lo que sí que s hay empresas como Verizon que lo ven todo más allá incluso que los gobiernos porque son las que ponen ahí la infraestructura de red no y estas empresas en Sí aparte de proporcionar a nosotros servicios de internet venden nuestros datos de conectividad de red como tú dices no están no está el contenido de los paquetes pero está la lo que se llama la tupla esta no de como has dicho dirección IP origen destino Puerto origen destino y protocolo pero yo yo sé de ciencia cierta que eso lo venden a empresas de gobiernos empresas de consultoría y temas similares sobre todo a socs Security operation Center para un poco prevenir ataques como tú dices adelantarse a al atacante y no sé un poco protegerse y mejorar la seguridad de esta forma claro de hecho te estás adelantando la noticia se nota que sabes Mucho del tema porque es eso mucha gente no es consciente de que nuestros proveedores de internet que ya digo entraré luego un poco más en eso están vendiendo nuestros datos a pesar de que estamos pagando un servicio pero bueno cabe preguntarnos Cómo consigue toda esta información una empresa privada Random no que es un poco lo que estábamos hablando cómo puede ser que una sola empresa en este caso Team simru tenga la información de la actividad en internet de Prácticamente todo el planeta en principio quien tendría acceso sería tu proveedor de internet y cualquiera empresa cuyo servidor digamos procese la información de tu tráfico para que llegue a su destino que ya sabemos que si yo visito pues una página web en Corea del Sur pues va a mi proveedor de Internet Pero luego el tráfico pasa por muchos servidores hasta llegar al server que está físicamente en Corea del Sur Pero eso claramente no lo hace todo una sola empresa Entonces qué está pasando aquí pues lo que pasa es que Team simru ha llegado a acuerdos comerciales con nuestros proveedores de internet como decía Alexis y esto les están vendiendo nuestra información para que ellos a su vez se lo revenda a los gobiernos que están dispuestos a pagar por ello gobierno o otra las empresas privadas o

quien sea mientras afloje la pasta sí querido oyente el proveedor de internet al que le estás pagando por un servicio está vendiendo información sobre ti y tú sin saberlo o bueno si lo sabes si llevas escuchando tierra de hackers un tiempo pero es que a mí es algo que me indigna esto porque ya no hablamos de aquello de monetizar tus datos Porque el servicios gratis pues como un Facebook o Twitter o tiktok que o Gmail no que Bueno pues no estás pagando por el servicio pero eh A cambio estás cediendo tus datos para que los monetic yo no conozco a nadie que le den internet gratis a cambio de sus datos pero sí todos estamos pagando y además mientras venden nuestros datos me siento la verdad estafado y por ahí recuerdo en Estados Unidos eh Y creo que lo mencioné en algún podcast que si tú te lees los términos del servicio el contrato que tú firmas con tu proveedor de intern por lo menos en Estados Unidos con algunos pasaba Como por ejemplo bryson que recuerdo y lo mencionaba Alexis te dice el contrato que tu tu cuota de internet está me sale ssad está Uf ayúdame ahí Alexis Cómo era está patrocinada digamos más que patrocinada digamos que como ellos te lo están dando un poquito más barato no es como cuando vas a comer en la universidad Pues que digamos que la comida es tan barata pues por subvencionado pum Ahí estás pues pues en el el en los contratos de algunos proveedores de internet en Estados Unidos Si Tú lees la letra pequeña dice que el precio es así porque está subvencionado y subvencionado de tal manera que están monetizando tu actividad en internet Claro pero es que no te da una a pagar más y así no monetizarlo Entonces esto también es un poco de trampa Pero bueno importante que lo sepáis pero como muestran los documentos publicados No solo son las empresas privadas eh que quieren acceder a toda la información de internet mediante acuerdos con proveedores y y también incluso sensores distribuidos por todo el planeta que recolectan este tipo de información dcsa se planteó implementar sus propios sensores distribuidos por Internet pero justifica la compra en el mercado privado debido al coste que ello tendría implementar su propia solución de recolección de tráfico a nivel mundial ostras cito textualmente un párrafo de uno de los documentos que os dejo en las notas del episodio los datos de la red incluyen información de más de 550 de recopilación en todo el mundo que abarcan puntos de recopilación en Europa Oriente medio América del Norte y del sur África y Asia y se actualizan con al menos 100.000 millones de nuevos registros cada día o sea aquí tenemos creo que mencioné hace un par de episodios que era un un como un poco un Secreto a voces que en San Francisco en uno de por donde sale uno de esos cables submarinos de internet había ahí una eh un aparatejo de la nsa recolectando información pues aquí le llaman sensores no pero distribuidos por todo el mundo 550 puntos de recopilación en todo el mundo y en todos los continentes ahí lo tenéis señores y si creéis que en Estados Unidos eh los únicos interesados en los datos que vende Team simr por decir una de las empresas es esta agencia de contrainteligencia pues estáis muy equivocados entre sus clientes Está también tamb el IRS que es básicamente la agencia tributaria los que te cobra los impuestos también el Us Navy y por supuesto la armada O sea que no solo tenemos el ámbito de la inteligencia También tenemos el ámbito militar e incluso los que recaudan los impuestos para investigar a defraudadores Supongo vamos que no les falta clientes a Team simr y yendo un paso más allá no solo tenemos entre sus clientes agencias gubernamentales tampoco solo a digamos los malos no Por así decirlo que que parece un poco que le estoy dando yo ese tono citizens lab ong cuyo trabajo cubrimos mucho en este podcast en su investigación contra el spyware israelí candiru da las gracias directamente a Tim simru por colaborar con ellos cito textualmente agradecemos al equipo de Tim simru por proporcionar acceso a su producto Pure Signal recon la capacidad de su herramienta para mostrar la telemetría del tráfico con internet de los últimos 3 meses fue el avance que necesitábamos para identificar a la víctima inicial en la infraestructura de candiru está claro que los datos que maneja Team simru son muchos y muy valiosos tanto para lo

bueno como para lo malo también deciros que deciros que no solo Team simru tiene acceso a este tipo de información otras empresas como Palo Alto con su producto cortex expans también qui tiene acceso a datos de netflow ya las limitaciones y regulaciones que aplique cada empresa pues es cosa suya Cómo podemos defendernos de esto para ya ir terminando la noticia pues usando vpns que nos ofrecen privacidad y protocolos como Thor que nos ofrecen anonimato si bien es cierto que Thor hace la navegación muy lenta y ya os he comentado que Team simr en su catálogo dice que puede obtener datos también de muchos servicios VPN la clave está en averiguar investigar y Buscar un buen proveedor de VPN con una sólida política de cero logs con excelente reputación cero incidentes de seguridad y auditorías públicas y llevadas a cabo por organizaciones independientes he visto algún proveedor de VPN que incluso ha llegado a deshacerse de los discos duros en sus servidores y procesa todo en memoria para que sea solo memoria volátil mejor por supuesto Aún si montáis ya vuestra propia VPN eso sería lo ideal y ya si le metéis tor sobre la VPN pues mejor que mejor pero ya os digo que esto sería lo ideal pero realmente no no es lo que puede hacer todo el mundo porque relentiza muchísimo tu conexión a internet también nunca está de más contactar con vuestro proveedor de internet y pedirle información sobre la privacidad de vuestros datos vuestro tráfico etcétera Y obtener un email o carta por escrito de Qué hacen y qué no hacen exactamente porque seguro que la primera respuesta va a ser no vendemos ni comercializamos nada vale vale tú dámelo por escrito por si algún día tengo que hacer referencia a esto y darte en la cara que me has mentido y además por lo menos verán que al público esto le importa y con suerte son más cuidadosos a la era de decidir si quieren vender nuestra información sin ser claros al respecto Eh cuántos muy interesante la noticia como siempre Martín siempre esta frase que siempre digo la digo de corazón muy interesante la noticia Pero cuánto tiempo has dicho que ofrecen los datos de los últimos tres meses o hasta cuánto en el pasado pueden ir em por lo que único dato que tengo Claro pero está muy está muy bien planteada esa pregunta pasé un poco por encima Pero el único dato que yo recab porque era una de las cosas que quería saber es lo de los tres meses que mencionaba antes no que citizens lab como cliente de ellos sí menciona esos TR meses pero vamos eh dado que solo se trata de los datos de ips y puertos y tal eso es que no ocupa nada es de hecho es texto no Entonces me imagino bases de datos optimizadas que sí que es tráfico a nivel mundial pero es que no es tanta información al ordenar por usuario o bueno más que por usuario por conexión no Entonces yo me imagino quees tendrán capacidad de ir meses y meses por no decir años atrás Claro claro e pero no tengo el dato en sí digamos el tema aparte de almacenar sería procesar en plan si tengo que procesar todo el último año de datos igual pero como estáa como citizens lab que que se ha centrado en un periodo de tiempo más corto tres meses que también me parece bastante pues igual se puede acelerar otro tema es que durante estos tres meses o este año tu dirección IP ha cambiado no yy temas similares Así que para encontrarte realmente igual tienen que colaborar con las los isps y todo eso no pero sí pero claro cuánto cambia tu IP tu IP cambia si reinicias el router no Aunque por no hablar los que las tienen estáticas yo me pasé un tiempo monitorizando mi dirección IP no cambiaba cada día pero no sé después de cada semana o algo así eh dentro del mismo Rango barra 24 23 pero si no cambia cada día pero en tres meses yo creo que alguna vez me cambió la dirección IP Pero bueno hay qued dentro del mismo Rango saben a qué isp supongo que luego con una ley una Cómo se dice esto una una orden judicial van y le piden al isp datos sobre la persona y bueno temas similares Claro pero eso eso se podría entender que por orden judicial por eso de hecho iba a decir ahora que como tienen acuerdos con los proveedores de internet ni siquiera tienen que estar monitorizando en tiempo real a mayores tiene sus sensores que ahí sí pero yo entiendo que si tu proveedor de internet está cambiando la IP sin que tú tengas que reiniciar seguro que

ellos tienen también un historial de las ips que tuviste asignadas precisamente para ya a nivel judicial pues tener que contestar a un requerimiento pero aquí ni hablamos de de órdenes judiciales ni nada Hablamos de acuerdos privados con empresas privadas entre empresas privadas para no no aquí tienes nombre usuario contraseña para la base de datos de todos mis clientes sus conexiones a internet y palante otro tema interesante de todo esto que comentas Martín es la privacidad de estos isps de los proveedores de internet en Estados Unidos envían cartas de tanto en cuando no me no me he fijado en la frecuencia pero igual una vez al año en la que dicen Si quieres limitar Cómo se tratan tus datos en favor a la privacidad y no quieres que compartamos tus datos con terceras empresas llama a este teléfono marca un dos o lo que sea di tu nombre y haz un di que no quieres participar en este en este programa no o también te dan una URL típica sitio.com bar privacidad No Y ahí dices haces login y marcas que no quieres participar en eso lo interesante es que algunas de estas cartas me he fijado de proveedores de internet si tien si te internet en casa esto nunca lo hea visto antes eh Por eso me parece interesante comentarlo que si tienes una WiFi de alguna forma No sé no sé cómo pero de alguna forma pueden ver el nombre de tu WiFi Supongo que si utilizas su dispositivo punto de acceso inalámbrico pero si utilizo el mío De todas formas pone si quieres que no e recabemos la información tuya en relación a la WiFi puedes Añadir al final de la WiFi gu baj no map o gu baj opt out digo anda Qué interesante esta medida O sea que la nombre el nombre de tu WiFi tiene que incluir esa palabra clave y entonces ellos dejan de recolectar información sobre ti Aparentemente manera más rara de hacerlo no s Sí sí esto es verídico de verison Sí sí O sea que ostra pero es que me parece aparte como el típico parche de Software que no sabe bien cómo hacerlo va Pues venga así así me vale ostia peroa cl Bueno me ha parecido interesante y Y luego el el otro tema que quería comentar Martín eh Muy interesante el tema de ciberinteligencia no bueno no solo ciberinteligencia sino inteligencia en general de eh contra eh acciones criminales y temas similares justo y voy a hablar de esto ahora en la siguiente noticia pero quería comentarlo porque me parece buen buena transición e todas estas empresas de inteligencia yo creo que se crean con un motivo principal bueno o uno de los motivos principales porque igual no soy experto pero es para adelantarse a estas amenazas no como he dicho antes eh protegerse de potenciales ataques ya sea a nivel Cibernético o físico militar eh preparar defensas y bueno y y todo esto similar pero en el ejemplo más reciente de conflicto bélico en la franja de gaza jamás contra Israel pues no he visto alguna noticia que diga que la las agencias de inteligencia de Israel que son tan famosísimas tan buenas no el mosad y similares y teniendo empresas en su propio país como nso Group y el software pegasus y todo esto no pudieron adelantarse a este ataque lo que sí que he leído es un artículo que decía que la Cia envió una alerta dos días antes del ataque al gobierno de Israel de un aumento de la probabilidad de violencia en la franja de gaza y el día antes el 6 de octubre les dijo a Israel Oye vas a tener un ataque inminente Pero eso no me queda como Ah Israel que es tan potente en temas de inteligencia no y no no pudo al menos algo e bueno eso se me ha quedado un poquito ahí relacionado con la noticia que has comentado sí lo de Israel sin duda el es es Digamos como el tema del momento bueno evidentemente hablo de la parte de ciberseguridad el tema del momento es el conflicto pero sigue en el entorno de la ciberseguridad y la ciberinteligencia era pero cómo este ejército Cómo ha podido pasar esto cómo yo escuchaba a a un experto decir que si un gato se acerca a la valla en gaza lo saben y de repente entran ahí cientos de terroristas unos volando otros por otro lado raptan a gente se los llevan O sea sí que ha sido un fallo catastrófico por parte de uno de los servicios de inteligencia más capaces a nivel mundial como es el del ejército israelí es algo que por supuesto también he leído por ahí conspiraciones que no entro a valorar Pero pero vamos era Jer sí que como mínimo sorprende Pues nada con esta breve conversación eh doy paso a la

siguiente noticia que que queda muy bien dale para adante derecho Pues nada como estamos comentando un poquito contexto qué ha pasado últimamente ahí en la franja de gaza entre como Digo gaza e Israel durante la mañana del sábado 7 de octubre militantes del Grupo hamás se infiltraron en Israel por el sur del país y lanzaron una ofensiva militar tanto terrestre con armas de fuego como vía aire con misiles Y como dice Martín gente volando y y soldados volando y temas similares jamás es un Movimiento Político y militar islamista palestino que gobierna la franja de gaza desde 2007 y lucha por la creación de un estado palestino independiente principalmente de Israel quien posee un control militar sobre la mayor parte de este territorio aunque también quiere Independencia eh reconocimiento global eh Por parte internacional en los primeros días desde que comenzó el conflicto hemos visto una avalancha de ciberataques tanto de grupos que apoyan a Palestina como los que apoyan a Israel como los que se oponen a ambos y quieren la paz que este grupo igual dices Bueno este aún Aún se le permite el ataque no pero todos estos ataques obviamente eh No no van a no no son legales digámoslo así así que se puede decir que son cibercriminales no todos estos grupos la intensa actividad ciber ofensiva se produjo inmediatamente después de que la Cruz Roja emitiera ocho directrices éticas para estos grupos ciberactivistas que participan en conflictos ciber ofensivos pidiéndoles que sean más humanos se cuentan más de 60 grupos de ciberactivismo involucrados en esta ciberguerra Quienes se han dirigido principalmente a infraestructura nacional crítica incluidos gobiernos Comunicaciones y sistemas de energía estos grupos están utilizando tácticas similares a las que se vieron al comienzo de la guerra entre Ucrania y Rusia comparten credenciales de sitios web israelíes para poder comprometer para poder más allá y bueno hacer de las suyas filtrar documentos robados comprometer cámaras domésticas atención a este dato que voy a comentar en más detalle hacia el final de la noticia lanzar ataques distribuidos desde negación de servicio contra como digo páginas web de gobiernos de periódicos incluso de centrales de energía centrales eléctricas desfigurar sitios web como en el inglés se conoce como defacement no cambiar la lo que se ve en la página web y poner algún mensaje suyo a favor de del país al que apoyan y abuso de interfaces de programación de aplicaciones en inglés que se conoce como Api o Api las apis para enviar mensajes a móviles que tienen instalada cierta aplicación esto también lo voy a comentar que es bastante interesante e lo que hicieron en este aspecto las ofensivas se han limitado a tácticas técnicas y procedimientos de poca sofisticación Según dicen los analistas que tienen un impacto disruptivo limitado sin embargo la elección de los objetivos el momento del ataque y la rápida participación de los grupos de ciberactivismo Pro Irán y Pro Rusia resaltan su nivel de coordinación en el intento de apoyar los ataques de jamás y complicar la respuesta israeli según analistas de inteligencia de amenazas los ciberataques contra Israel provienen principalmente de al menos 55 grupos ciberactivistas con sede en Rusia bangladesh Pakistán Marruecos e Irán voy a comentar algunos grupos que han hecho que destacan no del resto de los otros grupos de ciberactivismo porque han hecho temas bastante interesantes dignos de mención en el episodio Uno de ellos es Anon Ghost que es un poco el Ju de anonymus y Ghost fantasma no este grupo C activista Pro palestino afirmó que había comprometido un sitio web de reserva de vuelos israelí y la aplicación oficial utilizada por los agentes de policía de las fuerzas de defensa de Israel el grupo compartió el número de teléfono del jefe de la dirección nacional cibernética motivando a otros ciberactivistas a enviarle spam también el domingo 8 de octubre el día después del ataque Anon Ghost aprovechó un error de la Api en la aplicación red alert Rocket alerts que proporciona a los israelí advertencias de misiles en tiempo real para enviar una falsa amenaza de ataque nuclear o sea Martín imagínate esto Tú tienes tu móvil tienes instalada esta aplicación porque vives en Israel y sabes que hay conflictos de vez en cuando con la franja de gaza y esta aplicación te dice si se acerca algún misil o no a todo esto

Hay que decir que según eh según comentan Israel tiene un sistema antimisiles muy bueno no recuerdo el nombre pero Igualmente se han visto misiles sobrevolando Israel eh Jerusalén y y otras ciudades israelis Pero bueno el tema es que Martín Tú sacas tu teléfono te hace te se te vibra no Y ves ahí un mensajito y pone se acerca una bomba nuclear pum se te cae el alma al suelo creo Anon Ghost mencionó en su canal de Telegram que todos los 20.000 usuarios de esta aplicación deberían haber recibido estos mensajes así que poes esos esas 200000 familias de israelí que recibieron este mensaje y probablemente bueno estarían se les llenó el cuerpo de de escalofríos no el claro claro porque porque eso Perdona que te interrumpa pero claro una cosa que quería matizar claro es el contexto no es lo mismo que a mí me llega en España donde tenemos la suerte de que no pasa nada bueno no pasa nada Gracias también a las fuerzas y cuerpos de seguridad del Estado pero vamos que en principio vivimos o llevamos muchos años de de paz pero claro buen Matiz si yo vivo en Israel y me llega a eso a lo mejor le doy más credibilidad y lo que dices tú que allí de vez en cuando ensayan con sirenas y te tienes que meter en el búnker yo que viví en Suiza una época lo hacían una vez al año también un poco pues ese eh Para saber un poco lo que hacer y sentir como eh Cómo es esto de una alerta donde tienes que llevar a cabo alguna acción de hecho aquí en España pues tuvimos una mini versión de eso con los mensajes estos que nos llegaron a todos respecto a si hay algún efecto eh climático que puede ser peligroso que nos llegaron un mensaje a todos de alerta que en Estados Unidos es muy común el Amber alert Pues eso lo ensayaron aquí en Estados Unidos entonces bueno sin enrollarme más ostra si vivo eh Israel y estoy acostumbrado a esas cosas y a lo mejor le doy un pelín más de credibilidad a pesar de que en principio es un poco absurdo decirte Oye te va a llegar un misil digo Bueno si sabéis que me va a llegar es que ya lo han lanzado cómo llega el mensaje antes que misil Claro pero también comentas el tema que si si estás en Israel que estás bajo estrés no Ahora hay guerra otra vez en esos momento cuando los cibercriminales aprovechan a digamos a abusar de la psicología humana que está que ha bajado las defensas no porque está preocupando de sobrevivir y no preocupándome de que me llegue un mensaje también relacionado con sobrevivir no pero e si te hubiera enviado un mensaje de fishing en ese momento probablemente hubieras hecho click se acerca a una bomba nuclear Haz clic aquí para reservar tu asiento en el el búnker más cercano No pero en plan sí de más información o o qué tengo que hacer o algo así no Porque y sería normal porque pues a lo mejor no te cabe en un mensaje o lo que sea Sí oye a todo esto lo que has comentado es interesante porque justo la semana pasada creo hicieron un Esto no es relacionado directamente con esto pero sí lo es los Amber alerts hicieron una prueba de a nivel nacional en Estados Unidos y enviaron un mensaje a todos los eh residentes en Estados Unidos así que e me pareció interesante luego salían teorías eh conspiran noas de eh Te están probando el 5g y te están intentando dañar el cuerpo y bueno temas similares pero sí sí es el booster de la covid19 pero a través de de hber alert Pues seguimos eh el autor de esta aplicación móvil no comentó al respecto pero la aplicación se eliminó de la Google Play Store porque supongo que el esta persona eh se dio cuenta de que sí esta aplicación tenía vulnerabilidades y obviamente para no causar más pánico dijo la quito aquí y y Bueno listo De todas formas no es solo esta porque hay como cuatro o cinco red alert applications O sea que Supongo que lo hacen por tema de redundancia de alertas por si una falla Pues que las otras todavía comuniquen no e un poco como pasó en Ucrania también que algunas comunicaciones quedaban cortadas pero otras no pues usa esta como backup es muy importante tener información en tiempo real cuando hay un conflicto bélico como este De todas formas Anon Ghost también afirmó que atacaron otras aplicaciones de alerta de cohetes incluidas red alert Israel red alert de elad Nava y red alert de kumta eh según los informes a partir del 11 de octubre las aplicaciones de red alert elat Nava y kumta funcionaban con normalidad Así que causaron un poco de interrupción

del servicio y un poco enviaron estos mensajes falsificados en las aplicaciones pero ya se ha restablecido el servicio al menos en dos de estas aplicaciones el otro tema también interesante que hizo este grupo Anon Ghost es no solo atacar las aplicaciones real sino que los cibercriminales también han creado páginas web maliciosas que servían clones de la aplicación red alert de El ad Nava obviamente estos clones eran maliciosos El dominio original de la aplicación es red alert me pues la página maliciosa se hospedaba en Red alerts me es decir añadieron una s al final de red alert esto es bastante difícil de diferenciar y además como he dicho antes si estás en situaciones de estrés psicológico como este conflicto bélico el sitio web malicioso alojaba enlaces a la versión iOS y Android de la aplicación red alert pero mientras que el enlace a la App Store de Apple hacía referencia a la versión legítima de la aplicación red alert de El ad naava el enlace que supuestamente hacía referencia a la versión de Android alojada en Google Play Store descargaba directamente un archivo apk malicioso la versión maliciosa de red alert imita la aplicación legítima de alerta de misiles Gracias a que el código está abierto es Open source en github pero también simultáneamente recopila datos confidenciales del usuario es decir incluye un componente spyware los permisos adicionales solicitados por la aplicación maliciosa incluyen acceso a contactos registros de llamadas mensajes de texto información de la cuenta y una descripción general de todas las aplicaciones instaladas vamos un spyware en toda regla el sitio web que alojaba el archivo malicioso APK para Android se creó el 12 de octubre de este año pero ya no es accesible los usuarios que instalaron la versión de Android de esta aplicación red alert desde este sitio web específico están afectados y se les recomienda eliminar la aplicación urgentemente obviamente ahora paso con otro grupo de ciberactivistas o cibercriminales kiln del que ya hemos hablado en episodios anteriores es un grupo como digo cibercriminal ruso que también se puso del lado de jamás el domingo 8 de octubre el grupo kiln publicó un mensaje en Telegram acusando al gobierno israelí de de apoyar a Ucrania durante la guerra con Rusia y declarando sus intenciones de atacar a Israel en el ciberespacio kinnet luego afirmó que había eliminado un sitio web del gobierno israelí y el sitio web de la agencia de seguridad Shin bth que es el equivalente de la nsa en Estados Unidos y una de las tres organizaciones principales de inteligencia israelí junto con el mosat y el amán Esto fue confirmado por otros analistas que observaron que ambos sitios web estuvieron fuera de línea durante un periodo ese mismo día en el pasado Moscú ha intentado actuar como mediador en el conflicto y jugar en ambos bandos pero su creciente Alianza militar con Irán enemigo de Israel y partidario de jamás ha complicado la situación ahora comento un poquito anónimos Sudán un grupo de ciberactivistas con motivaciones religiosas dijo ese mismo Domingo 8 de octubre que estaban detrás de un ataque al jerusalem post el sitio web de noticias en inglés más leído de Israel hasta el martes por la mañana el 10 de octubre el sitio web todavía estaba caído esto por qué porque querían evitar que los ciudadanos israelíes pudieran leer las noticias online y conocer las actividades de la guerra en tiempo real el jerusalem post publicó en su Twitter ese mismo domingo que fue blanco de múltiples ataques cibernéticos lo que provocó que su sitio de noticias online quedara colapsado hecho que confirmaba las declaraciones de este grupo C activista anónimos Sudán el martes 10 de octubre este mismo grupo también afirmó haberse asociado con el grupo ciberactivista sieg sec para atacar los sistemas de control industrial y los sistemas de navegación por satélite israelí No tengo más Noticias al respecto de este ataque o de implicaciones e impacto de de este incidente Pero bueno según decían estaban trabajando en ello hay que comentar que a pesar de que la mayoría de la actividad ofensiva se ha centrado en atacar a Israel en el ciberespacio ha habido al menos 12 grupos ciberactivistas que han manifestado su apoyo a Israel y han atacado a sistemas de Palestina la Indian Cyber Force un grupo Pro India conocido por sus recientes ataques al sitio web militar canadiense se atribuyó

la responsabilidad de atacar a una empresa de telecomunicaciones Palestina el sitio web del Banco Nacional un servicio de correo web del gobierno que se encuentra en web mail.gov PS y el sitio web oficial de jamas que se encuentra en hamas.ps hasta el martes por la mañana 10 de octubre la mayoría de estos sitios web eran inaccesibles en respuesta a esto ciberactivistas Pro palestinos lanzaron ataques cibernéticos contra sitios web del gobierno indio el martes acusando a India de apoyar a Israel Aunque funcionarios y personas del gobierno indio dijeron que habían contrarrestado con éxito estos ataques otros grupos de ciberactivistas Pro israelíes incluyen el team ucc Ops vinculado a la India y Bandas ciberactivistas relativamente nuevas y previamente desconocidas como garuna Ops y Silent One Y luego como dije al principio tenemos a ver tenemos tres eh situaciones en este conflicto los que apoyan a Israel los que apoyan a gaza jamás y los que apoyan a ambos o están en contra de ambos en este caso por ejemplo el grupo threats publicó en Telegram que atacaron a Israel en el pasado y que ahora van a atacar la región de gaza todo porque no les gusta la guerra el grupo afirmó haber comprometido un importante proveedor de internet de gaza llamado alphanet y haber tomado control de los servidores de la empresa impactando sus sistemas de televisión se dedican a difundir programas de televisión alphanet dijo que sus comunicaciones se vieron interrumpidas porque la sede había sido completamente destruida y demolida por misiles pero la empresa no mencionó ningún ciberataque como suele ocurrir con la actividad ciberactivista no todos los ataques denunciados son reales algunos grupos simplemente buscan atención mientras que otros quieren alimentar la desinformación y la propaganda en torno al conflicto muchos de los ataques no pudieron verificarse de forma independiente y así es el caso de Cyber av ers un grupo de ciberactivistas Pro iraní que el domingo 8 de octubre afirmó haber atacado con éxito la planta de energía de dorat en la ciudad de ashkelon la segunda central eléctrica más grande en Israel pero los investigadores descubrieron que los datos publicados asociados con esta central eléctrica en realidad fueron robados por la banda de ransomware moses staff en 2022 Cyber Avengers es un grupo conocido por inventarse victorias ciber ofensivas y de crear infraestructura falsa e incluso fabricar capturas de pantalla vamos que son unos profesionales del Photoshop un skill muy necesario para ser un buen cibercriminal queridos oyentes No esto es broma obviamente pero por otra parte y Esto fue confirmado este grupo Cyber Avengers atacó al operador independiente del sistema de Israel que se le conoce como noga nog una organización que proporciona electricidad a través de una red eléctrica y comprometieron su red dejando fuera de servicio su sitio web el grupo también atacó a Israel Electric Corporation el mayor proveedor de energía eléctrica en Israel y los territorios palestinos así como otra central eléctrica de la que no se dan mayores detalles alicia.com oos escribe a l e t h e a que es interesante nombre Porque en griego significa verdad una empresa que se dedica a luchar contra la desinformación ha detectado un grupo coordinado de al menos 67 cuentas en Twitter que publicaban contenido casi idéntico sobre el conflicto y promovían traducciones engañosas y fuera de contexto de declaraciones del presidente ruso Vladimir Putin y el ministro de asuntos exteriores sergey lavrov Alicia observó mensajes de este grupo de cuentas tanto a favor de Palestina como a favor de Israel lo que sugiere que el objetivo de esta red de desinformación puede ser avivar la ira en ambos lados del conflicto o simplemente capitalizar el interés actual en el tema a todo esto se dice que los ataques digitales contra Israel comenzaron mucho antes de que jamás lanzara su ataque militar sorpresa los ataques de denegación de servicio distribuida contra Israel comenzaron a aumentar significativamente ya ya entonces el 26 de septiembre alcanzando su punto máximo el 28 según un informe reciente de Microsoft Israel es el país más frecuentemente atacado por ciberataques en medio oriente este año los investigadores han observado Un aumento en la actividad originada por el grupo con sede en gaza conocido como storm-look.com apoyar la resistencia Palestina sembrar el

pánico entre los ciudadanos israelíes y contrarrestar la normalización de las relaciones árabe israelies según Comenta Microsoft en vista de todo este conflicto bélico qué pueden hacer las empresas para protegerse pues se han dado algunas recomendaciones a alto nivel pero es lo típico no de higiene de ciberseguridad implementar medidas contra ataques de denegación de servicio distribuido es decir contratar servicios con cloudfare o similares lo segundo es preparar planes de respuesta a incidentes y gestión de crisis eh asegurarte de que estos funcionan y los tienes bien definidos y están todas las responsabilidades bien definidas lo tercero sería aplicar parches de seguridad sobre todo a sistemas expuestos en internet y de usuario y obviamente un poco securizar lo que se dice hardening no cambiar eh contraseñas por defecto y aplicar el doble factor y temas similares y ya en último lugar por mencionar las cuatro más interesantes es asegurarse de tener buenas copias de seguridad y que se han probado y que están guardadas de forma diversificada Y por último quiero cerrar la noticia con un evento que me ha parecido interesante cuando estaba investigando sobre todo lo que está pasando en el conflicto bélico en entre gaza e Israel y es que el gobierno israelí ha pedido a sus ciudadanos o a sus residentes que protejan las cámaras IP que tienen en sus hogares esto lo ha emitido más que como una recomendación lo ha emitido como una petición de ayuda al ejército israelí y en este conflicto bélico lo que ha dicho es por favor ciudadanos protegedor de vuestros hogares o apagad lasas por completo porque tenemos temor que estos dispositivos puedan ser comprometidos y utilizados en contra de Israel para espionaje y recopilación de inteligencia en un memorando el viernes de la semana pasada la dirección nacional cibernética de Israel pidió a los propietarios de cámaras que cambien sus contraseñas habiliten la autenticación de doble factor si así lo permite la cámara y habiliten las actualizaciones de seguridad automáticas si los propietarios de estas cámaras no pueden cambiar ninguna de estas configuraciones el gobierno israelí ha instado a los propietarios a cubrir las lentes de las cámaras o a pagar los dispositivos por completo el gobierno de Israel no está tomando ningún riesgo y probablemente haya ido una lección vital del reciente conflicto ruso-ucraniano donde cibercriminales rusos comprometieron cámaras de seguridad de Ucrania para rastrear convois de ayuda militar y ajustar los objetivos de los misiles en tiempo real dado que Israel mueve una gran parte de sus fuerzas militares por todo el país no exponer la ubicación de las tropas y el equipo a través de la cámara doméstica de alguien es imprescindible para el movimiento seguro de sus tropas además también hay que tener en cuenta un aspecto propagandístico desde el ataque inicial de jamás el 7 de octubre también se han compartido ampliamente en internet imágenes tomadas de cámaras de seguridad comprometidas que muestran cohetes de jamás impactando hogares israelíes Y más recientemente cohetes también sobrevolando Jerusalén y otras ciudades en Israel según datos proporcionados por las autoridades israelíes en 2022 había aproximadamente 66,000 cámaras domésticas y de seguridad que seguían siendo vulnerables al compromiso y control remoto debido a que estas cámaras se venden con contraseñas predeterminadas y los usuarios no las suelen cambiar según un informe de calcalist un periódico online israelí ya se están realizando ataques contra cámaras domésticas aunque no está claro si se trata simplemente de Ja activismo o ciberactivismo sin objetivo o de recopilación de inteligencia real sin embargo una lección Clara hay en todo esto como se vio en el conflicto ruso-ucraniano y en el actual israelí palestino los gobiernos ahora pueden utilizar sus cibere ejércitos para vigilar ciudades enteras simplemente comprometiendo cámaras expuestas en internet o incluso routers que todavía usan sus contraseñas predeterminadas para pivotar a través de ellos y conectarse a las cámaras que estén detrás de dichos dispositivos de red y no estén expuestos en internet muy interesante que un dispositivo tan Aparentemente inofensivo como una cámara IP pueda proporcionar tal ventaja en una ciberguerra y ahí lo dejo tú qué opinas Martín muy interesante Alexis como dices tú para

parafrasear con la mía me llamó la atención eso que comentaste del aviso a los ciudadanos sobre la seguridad de sus cámaras por un lado aparte de que es super interesante Pensaba yo ostras y no lo podíais haber avisado antes cuando no había guerra Qué pasa que antes ahí no no había no había prisa no por avisar a los ciudadanos de que tienen tantas cámaras vulnerables y accesibles a cualquiera eh Bueno yo lo dejo Ahí es curioso como siempre me es que me trae recuerdos también al tema de de cuando le robaron las Tools a la nsa Y con esa se escribió el guan Cry que tenían en secreto exploits hiper críticos que afectaban a todos los sistemas de Windows y lo justificaron como Oye es que estos expes los utilizamos para luchar contra el ciberterrorismo ya pero es que estás manteniendo a tus propios ciudadanos eh en un estado inseguro en todo su vida digital porque sus sistemas son vulnerables y tú lo sabes y tú eres el gobierno entonces Eh me trajo recuerdos a eso muy curioso sí como dices es el tema de a ver si sabéis que esto se ha utilizado con anterioridad en en la guerra entre eh Rusia y Ucrania y sabes que se utilizó para obtener una ventaja en temas de inteligencia podríais como dice Martín podríais a partir de ahora por qué no enviáis es que hay un problema general ya esto sería un problema táctico no cambiar la contraseña a estas cámaras pero el problema El el la raíz de todo este problema más estratégica es no enviéis productos iot con contraseñas por defecto no eh haced que el que No ya pero eso ya es cosa de la industria pero digo si el gobierno sabe que hay este problema eh avisa antes manda esas notificaciones antes porque no estamos hablando de yo que sé cambia la contraseña de tu email no Us la no no estamos hablando de las cámaras que apuntan a tu casa o también como no sé si en Ucrania se hizo algo similar pero o con algunos malw no que habido en el pasado wan Cry similares que había este Kill switch y luego no sé si era alguna empresa privada dijo sabes qué voy a ayudar a la humanidad y voy a Desactivar todo este malware hizo algo que en principio no está amparado por la ley no se fue y se conectó a sistemas que no son suyos para desactivar para para el malware para activar este Kill switch Pues aquí igual la la it Army de de Israel se conecta todas estas cámaras hace un escaneo de sus ranjo IP con credenciales por defecto y luego la cambia y luego ya después del conflicto bélico ya la vuelvo a reponer no que ahí entra la pregunta filosófica porque el equivalente Sería bueno hay alguien que ha eh esparcido un virus virus de verdad como si fuera el covid pero mucho más mortal en todo el planeta Y tú tienes el antídoto y te dedicas en la calle estás escondido Cada ciudadano que pasa pa le inyectas la el antídoto por un lado ostra le estás ayudando pero por otro lado no ha sido consentido tú no puedes ir inyectando a la gente pues esto sería un poco el equivalente a ver lo haces por bien pero claro pero esto Martín ya lo han hecho con el Amber alert a nivel nacional el 5g y esto ya está hecho estamos todos inoculados a lo que ya estamos todos vacunados y ya está tío mediante el 5g Claro que sí pues nada a protegerse muy muy buena la muy buena la noticia queridos oyente Muchas gracias por quedaros hasta el final recordar que estamos accesibles en todas las redes sociales en discord bakers.com disord nos podéis votar en ebox lo cual nos ayudaría un montón en tier.com votar y nos contactar en podcast @ticktok 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 y