el departamento de homeland Security de los Estados Unidos ha invertido fondos públicos en desarrollar un programa de monitoreo de redes sociales para clasificar a los usuarios en varias categorías de sospechosos de terrorismo tráfico de drogas y tráfico de personas un fallo en la actualización del firmware de cientos de placas base de la empresa gigabyte podría permitir a ciberdelincuentes obtener control remoto privilegiado y persistente de millones de sistemas online incluido el tuyo 9 episodio disponible para tu uso y disfrute comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 12 de junio de 2023 es el episodio número 97 yo soy Martín vigo y está conmigo ya casi llegando a los 100 episodios Alexis porros Hola Alexis qué tal pues aquí estamos Martínez con ganas de ser centenarios ahí llegando a los 100 episodios y a punto de entrar de hecho en el verano oficialmente también es otro otro hito de al que nos acercamos aunque las estaciones ya han cambiado tanto que el verano aquí ha llegado hace semanas no sé por ahí también creo que por España Y tal Pero bueno no me enrollo más lo que os queremos decir es muchas gracias como siempre en cada episodio por estar con nosotros queridos oyentes gracias a vosotros somos una gran familia y estamos muy contentos por tenerlos siempre episodio 3 episodio con vuestros comentarios mejoras y bueno todo todo eso que nos escribís en redes sociales y en todas las plataformas online Por cierto hablando de plataformas online os recuerdo que estamos en todas las redes sociales más populares en las que nos podéis encontrar como tierra de hackers o arroba tierra de hackers y también En plataformas de podcast si no lo estáis ahora mismo Esto es lo más importante suscribiros a nuestra plataforma de podcast tierra de hackers en cualquier ya sea por el podcast o Google podcast o Spotify ibox todo entonces estamos y Tenemos también un servidor de discord que podéis acceder vía tierra de hackers.com barra discord y finalmente cerrando la intro agradeciéndoos vuestro apoyo a la pregunta del episodio que publicamos en Twitter y que la del anterior si recordáis fue la siguiente estarías dispuesto a registrar tus datos biométricos en la plataforma de World Coin para una identificación global a cambio de unas criptomonedas World Coin tenemos cuatro respuestas la más votada fue un no basta de gran hermano con un 68% seguida de no de momento no con un 21% y luego viene un sí quiero un identificador global con un 8% y finalmente un 3% sí por las World coins Así que vemos que la gran mayoría no quiere donar sus Iris o otros tipos de datos biométricos hubo bastante conversación al respecto en el Canal de discords bueno fueron buenas risas yo de acuerdo también yo desde luego no vendo literal además no no vendo la información biométrica de mis ojos que aparte los tengo precios Bueno yo dar las gracias como siempre a nuestros mecenas de patreon Gracias por siempre estar ahí apoyándonos que sois los que nos ayudáis a que esto pueda seguir adelante y también nuestros sponsors como brawler Pro una herramienta que es la más completa sobre seguridad en aws empresas de todos los tamaños se apoyan diariamente en brawler pro para que sus equipos puedan confiar en su modelo de seguridad de aws puedes probar brawler Pro hoy mismo y de manera además totalmente gratuita y vas a obtener paneles y gráficas con información concisa y accionable además con todo lujo de detalles sobre la madurez de tu modelo de seguridad y la visión completa de tu infraestructura además en todas las regiones de aws y tendrás todos esos resultados en unos minutos Así que empieza a usar brawler pro y benefíciate de sus resultados visitando tierra de hackers.com barra brawler prowl e rpro y también queremos dar las gracias a otro de nuestros patrocinadores monat una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y monat a través de una herramienta gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web

monat.com y mandarles vuestro currículum a tierra de hackers arroba monat.commod.com perfecto Pues nos vamos con la noticia a ver tiktok Facebook Instagram Snapchat Twitter todos son lugares donde vamos a exponer públicamente por nuestras fotos la gente con la que nos relacionamos nuestros gustos nuestras opiniones nuestra personalidad donde elogiamos a unos despreciamos a otros las redes sociales es la biblioteca ideal para conocer a una persona y las agencias gubernamentales esto por supuesto también lo saben y se aprovechan en varias ocasiones hemos hablado sobre ello pero esta vez gracias a una petición folla del centro brenan una Bueno una entidad no gubernamental que defiende los derechos de los ciudadanos e investiga violaciones de leyes por parte del gobierno americano sabemos a ciencia cierta que esto es así que las agencias gubernamentales se aprovechan de todo lo que publicamos en redes sociales el departamento de homeland Security ha invertido millones de dólares en un programa secreto para monitorizar todas las redes sociales en busca de riesgos relacionados con el terrorismo lo han llamado proyecto night Fury que es además supervisado por el centro tecnológico de análisis de datos del gobierno de los Estados Unidos Bueno lo primero recordemos que por si no lo conocéis un folla request que viene siendo el Freedom of information act Es una herramienta muy valiosa para pues investigadores reporteros que permite pedir al gobierno documentación e información sobre cualquier diligencia llevada a cabo llevada a cabo por el gobierno la premisa es que un gobierno debe operar de manera transparente para el pueblo y los follar request pues son mecanismos para precisamente exigir esa transparencia pero si esto es un programa secreto Cómo supo el centro brennan de su existencia Pues gracias a un informe del Inspector general de homeland Security del año pasado donde expresaba sus preocupaciones por las potenciales violaciones de la privacidad de los ciudadanos estadounidenses debido a este programa de vigilancia de redes sociales este informe que por supuesto os dejo las notas del episodio mencionaba lo siguiente como parte de las preocupaciones cito textualmente en marzo de 2020 la oficina del Inspector general del departamento de seguridad nacional recibió denuncias sobre posibles violaciones de privacidad relacionadas con él proyecto night Fury realizado por la oficina de ciencia y tecnología para investigar y desarrollar herramientas de análisis de datos de datos de código abierto para este proyecto de 443 mil dólares se contrató tareas específicas a una universidad para recopilar datos de redes sociales para su uso se buscaba probar y desarrollar capacidades analíticas para identificar posibles riesgos de terrorismo En plataformas de redes sociales públicamente disponibles y otras fuentes de código abierto el denunciante afirmó que el proyecto comenzó en septiembre de 2018 e incluía específicamente la recopilación de millones de registros de redes sociales incluidas publicaciones vídeos y fotos además el denunciante notificó preocupaciones de que el departamento no haya garantizado una supervisión programática efectiva responsabilidad de los empleados gestión de registros federales documentación de contratos y seguridad de la información para este proyecto en particular solo con este párrafo del informe que además Tiene bastantes páginas y lo podéis ir a leer como decía ya tenemos datos muy interesantes project Fury como decíamos se trata del escaneo masivo de redes sociales para detectar amenazas terroristas el presupuesto inicial es medio millón de dólares yo había mencionado varios millones porque como os comentaré más adelante Este no es el programa que primero se hace sobre algo parecido en este caso recolectará publicaciones vídeos fotos pero lo más importante que en esta carta del propio Inspector general de homeland Security que eran base Pues eso a unas quejas hace referencia que este proyecto no respeta las leyes vigentes sobre privacidad no presenta las medidas de seguridad adecuadas para proteger la información recabada y no hay modelos de supervisión de los empleados que tendrán acceso a esos datos tan sensibles bastante desastre para una herramienta que puramente basándose en lo que la gente publica en redes sociales te pone la

etiqueta de sospechoso terrorista o no Pues bien la petición folla fue aceptada y entre los muchos documentos que los investigadores recibieron había uno que describía de qué se trataba concretamente Este programa y cito textualmente se ha contratado a la universidad de Alabama en virgingam para llevar a cabo investigación y desarrollo en Fuentes abiertas y redes sociales lo cual implica la recopilación de información públicamente disponible incluyendo de las redes sociales el trabajo de la Universidad de Alabama se centrará inicialmente en la lucha contra el terrorismo la cadena del suministro ilegal de opioides El crimen transnacional y la comprensión barra caracterización barra identificación de la difusión de desinformación por entidades extranjeras incluido el estudio de la detección de Bots sin embargo los métodos exitosos deberían ser escalables a otros ámbitos de interés para el departamento de homeland Security el objetivo también es comprender cómo evolucionan las amenazas con el tiempo en comunidades de redes sociales de menor tamaño no Facebook o Twitter en estas pues hace referencia a otras como la rusa bike y o Telegram o cosas así Y hasta qué punto el contenido puede indicar la ubicación de información de interés que no está geolocalizada Bueno aquí en esta descripción ya sabemos más información de lo que realmente quieren desarrollar y además quién lo va a hacer la universidad de Alabama una de las frases con las que me quedo es lo de Sin embargo los métodos exitosos deberían ser escalables a otros ámbitos de interés del departamento con la Security O sea que gracias a es foyer request ya sabemos que no solo se trata de categorizarnos y digo me incluyo a mí mismo porque yo tengo redes sociales de categorizarnos como un riesgo terrorista sino también relacionado con drogas con crimen transaccional o con todo tipo de crimen vamos relacionado también con el tema de las fake news no de campañas de desinformación otra frase con la que me quedo es lo de el objetivo también es comprender cómo evolucionan las amenazas con el tiempo en comunidades de redes sociales de menor tamaño por tanto como decía antes Esto no se queda solo en los Facebook los instagrams y los tiktoks también se va a mensajería privada como puede ser un Telegram donde hay grupos y se puede acceder por tanto en principio eso Por lo consideran público y redes sociales propias pues como las chinas beidú o Dj en Rusia o sea que quieren abarcar absolutamente todo pero lo que más me llamó a mí la atención es lo de Y hasta qué punto el contenido puede indicar la ubicación de información de interés que no esté geolocalizada lo que esto quiere decir es que estamos hablando de la geolocalización de empresas cuando no se tiene información de GPS el uso de la información que publicas para extraer En qué parte del mundo puedes estar por ejemplo pues buscando palabras claves No si yo hablo mucho de Barcelona pues se podrá intuir que estoy ahora mismo en Barcelona pero el documento también habla de influencers regionales en el sentido de que si tú sigues a ibai auronplay pues probablemente seas español y si sigues a cuentas que te dan tips de yo que sé restaurantes en Barcelona como alguna he visto por ahí pues pues es bastante probable que seas de Barcelona y si sigues al alcalde de una ciudad en concreto pues es posible que tú además seas de esa ciudad en concreto pues esto también lo van a implementar para una vez más geolocalizar a los usuarios cuando no son capaces a través de la geolocalización normal de Pues metadatos en una foto o que la persona pues en su perfil ponga De dónde es pero es que además pedían que se implementara la capacidad de Designar zonas calientes en el sentido de que sea posible obtener todos los usuarios geolocalizados por estas metodologías en una zona en concreto Pues que este especial interés para la agencia Pues a lo mejor por su actividad terrorista o porque saben que hay un terrorista allí entonces quieren saber quién más vive por allí o cosas así otro documento hacía referencia a que el proyecto night Fury tendría la capacidad de decidir si una cuenta de Twitter estaba asociada de algún modo a grupos terroristas esto lo haría en base a las conexiones con otras cuentas es decir Yo sigo a este o este me sigue a mí y también palabras claves además esto estaría todo automatizado para eliminar

la interacción humana eso es algo de lo que pone los documentos esto Claro si vosotros creéis que se puede determinar si alguien es un terrorista solo por la gente a la que sigue o a la o a la gente que le sigue a esa persona a ver claro que si nos vamos al extremo si si te están siguiendo cinco terroristas que que tú tienes ciertas conversaciones o palabras claves Pues bueno Sí claro que puede haber ahí pues un indicio no para por lo menos Investigar un poco más para determina como persona de interés lo que pasa es que esto que esté tan automatizado y luego me explayaré en esto claro esto es muy fácil que haya errores que haya falsos positivos esto por supuesto que no podemos simplemente determinarlo solo con esa información también hablan de la detección de influencers en el mundo del terrorismo detectando cuentas que publiquen propaganda y monitorizándoles a través de múltiples redes sociales la verdad esto es otra cosa que me llama bastante la atención influencer terrorista Pero bueno que se entiende no lo que quiere decir que una persona un personaje el que sigue mucha gente Pues porque suele publicar mucha información de este tipo también se exige que implementarse que se implementará la detección de Bots como decía cuentas que publican contenido ya sabéis de manera automatizada para expander no el mensaje extremista se hace mención de hecho a la detección de campañas de influencia sobre la población por parte de Naciones enemigas los fake news famosos y el más claro ejemplo es el de Rusia durante las elecciones de Estados Unidos de 2016 pero el objetivo principal de night Fury es la asignación de una puntuación de riesgo a los usuarios lo que os decía al principio básicamente Qué probabilidades hay de que seas un terrorista del 1 al 10 no y así nos asignan una puntuación a todos y en base a eso pues ya toman pesquisas No ya ya actúan esto recuerda un poco al famoso social score la puntuación social china donde evalúan en este caso a sus propios ciudadanos de cómo buen persona son y en base a eso se puede restringir las libertades de los ciudadanos digamos que no se comportan en base a las exigencias del partido comunista chino Pues aquí lo mismo pero versión terrorista y claro cuál es el problema de todo esto si bien en el principio todo querríamos que existiese una manera de detectar a terroristas en base Pues a puntuar sus actividades online no Esto está muy cogido con pinzas y es muy probable que haya falsos positivos y esto no no es algo que solo opine yo y tampoco es algo que simplemente el propio Inspector general de departamento del departamento de la Security haya mencionado porque ha recibido quejas como os contaba sino expertos en estos temas también ponen el grito en el cielo según me documentaba para esta noticia leía un ejemplo claro de ello una palabra que todos asociamos al terrorismo es el yihad no el concepto de yihad está directamente asociado con el terrorismo pero cuando hablamos de que compostear con publicar esa palabra en redes sociales ya te puedes hacer sospechoso de terrorismo se convierte en un problema Eso es porque el término yihad tiene mucho más contexto y significado algo que si no eres un país árabe o no entiendes la cultura no vas a conocer y a esto no me lo saca yo de la manga Esto hace referencia una carta firmada por 56 organizaciones sin ánimo de lucro dirigida a Ice que es el departamento encargado del control de fronteras de Estados Unidos Ya que en el pasado también se ha intentado utilizar tecnología para categorizar a los extranjeros que intentan Acceder al país tecnología automatizada esta carta está súper bien y y tiene muchísimas referencias a estudios académicos algo que me gustó un montón y es donde se hace referencia a cómo falla cuando no se tiene el contexto y Simplemente nos basamos en palabras clave Así que os la dejo también por supuesto en las notas del episodio pero os menciono un párrafo por el momento Los criterios que hay tiene la intención de utilizar para el análisis de redes sociales con el fin de predecir están fuera del ámbito de la tecnología existente el significado del contenido publicado en las redes sociales es altamente dependiente del contexto los errores en el juicio humano sobre el verdadero significado de las publicaciones de las redes sociales son comunes los algoritmos diseñados

para evaluar el significado del texto tienen dificultades incluso para realizar determinaciones simples como si una publicación en redes sociales es positiva negativa o neutral Pues aquí ya vemos y aquí por cierto hacen referencia a varios papers en este en este simple párrafo esta carta de hecho es el resultado de un programa como decía similar anterior en quiero concretar que es de La era de Donald Trump y que acabó cancelándose Pues por razones obvias como estamos viendo en con este simple párrafo de esa carta Este programa lo llamaron Extreme betting initive y buscaba básicamente pues hacer algo muy parecido a lo que ahora intenta el departamento de jornadas Security pero poniéndole otro nombre los que hayáis sido de turistas a Estados Unidos ya habéis ya habéis visto que desde hace un par de años cuando pides el visado de turista has de indicar aparte de tus datos personales tus redes sociales Bueno pues pues ya sabes el porqué en fin resumiendo tenemos que el departamento de hobland Security ha pagado a la universidad de Alabama para desarrollar tecnología capaz de monitorizar proactivamente todas las redes sociales para categorizar a los usuarios como posibles personas de interés puntuándoles en torno a terrorismo drogas o tráfico de personas también intentarán averiguar la geolocalización utilizando referencias de palabras claves personas que seguimos y otro tipo de referencias mencionar también que esto no es la primera vez que intentan un programa de este tipo ya que hay como decía bajo el mandato de Trump intentó poner en marcha algo similar acabemos con un punto positivo Este programa al igual que el que apoyaba Trump se ha cancelado no sabemos la razón pero está claro que incluso ellos mismos se dieron cuenta que inferir si alguien es un terrorista no requiere mucho más que analizar lo que pones en redes sociales por no hablar de lo que eso significa para nuestra privacidad cierto es que es público lo que analizan pero es como si vamos por la calle hablando con amigos y hay micrófonos por todos lados captando lo que decimos para su posterior análisis y categorización en el ranking de peligrosidad Así que queridos oyentes la moraleja ojito con lo que ponéis en redes sociales todo lo que publiquéis podrá ser y será utilizado en vuestra contra tixit mucho cuidado aquí siempre tener a mano chat gpt vuestro abogado más fiel y Leal sí lo de mes justo cuando lo estabas diciendo me estaba acordando lo del esta por ejemplo para la gente que saca el visado para venir a Estados Unidos te piden eso de los datos de las redes sociales Aunque pone opcional puedes proporcionarlo o no pero la gente supongo que en plan yo lo voy a dar porque si no igual No claro es que es eso juegan con el medio ellos pueden Es que a mí me ha parecido perfecto Pueden decir no no pero esto es opcional no violamos la privacidad de nadie dice ya pero es que tampoco hay una rigurosidad depende del tío de la frontera El decirte si entras o no a su propio criterio Entonces sí no sé de otros tipos de Visas o incluso cuando si la Green Card o al hacerse ciudadano americano si te piden eso pero bueno como tú dices esto creo que ha cambiado hace años no se pedía tanto no Pero supongo que en los últimos años no sé cuándo se empezó a pedir pero fue un cambio Supongo que interesante Supongo que todos estos datos se re y se proporcionaban a la universidad de Alabama o no sé si en plan que me imagino no hayas encontrado alguna información pero me imagino que cuando proporcionas esto en una visa en el stack Qué hacen le pasan las urls de tu Facebook de tu tal ahí a un programa que tienen y lo corren y que intentan ver no sé me preguntó Supongo que miran algo no pero debe de ser esto a nivel automático porque es imposible con los millones de turistas que vienen por Estados Unidos analizar esto de alguna forma debe tener algunas reglas algunas keywords o historias de estas no sí sí es que todo a mí a mí a lo que me recordaba Era ese ese gag de Padre de familia de Family Guy cuando cuando actúa como un policía peter y ve a un tío y tiene como una escala de colores y dependiendo de la escala de colores Sabes cuanto más oscuro le ponía terrorista y si es más blanco no es un gas de broma de humor negro pero pero ostras es un poco ese no es ese baremo Baratillo para determinar si alguien es un terrorista Sí muy interesante eso es un buen un buen y el otro tema

comentaste que la oficina que en principio esto es un proyecto secreto pero me parece interesante que el inspector general supiera de ella pero hasta que no comentaste que esto fue porque alguien pues envió hizo una demanda se protestó no se enteró o sea realmente y Quién hizo esa demanda una persona externa al día y chess o alguien interno de forma anónima no sé si se Comenta algo al respecto pero un dato interesante Sí sí la verdad Muy bien dicho y a lo mejor pues no me documenté lo suficiente porque eso No sabría contestarte porque la carta que encontré hablaba eso de que de que le llegaron protestas pero muy buen punto puede ser de alguien que no llegó a ser winsell blogger Pero es en plan subo la queja en las en el Rango no voy al nivel más alto o a lo mejor pues externa de alguien que lo conocía No lo sé Suena a lo mejor más de alguien interno sí poco para saber el secretismo de este proyecto si era secreto incluso para el inspector general que probablemente tiene la pinta que que lo sea como en las películas no programa especial de la Cia de soldados en este caso en este caso como colaboraban con una entidad externa como la universidad de Alabama más difícil que sea tan secreto como lo que bien dices tú de esos Ultra secretos Pero que son más internos No que los conocen me recuerda mi época cuando trabajaba en Apple tío que son están obsesionados con el secretismo yo no sabía O sea compartía la oficina con otro tío y yo no sabían lo que trabajaba ese tío o sea llegaba a ese nivel el secretismo Entonces esto es un rollo interno sí pero si ya tienes que tirar de entidades públicas es más complicado voy a hacer un comentario eso que ahora como todas las empresas están empujando a sus empleados a volver a la oficina ahora eso no sé cómo Apple lo va a hacer porque el Bueno no sé cómo lo hacía antes no pero ahora de nuevo el tema de Apple que se planteó parece como tú dices del principio esa situación no de paranoia Pero hay otras empresas que que no hacen lo mismo y si se tienen que poner ese nivel Me pregunto cómo lo van a hacer porque espacio es bastante reducido últimamente sí Bueno de hecho ya yo como me tocaba de cerca por varias razones sé perfectamente Apple fue de los últimos en permitir a los trabajadores en ir a trabajar desde casa durante la pandemia y fue los primeros en exigir no pedir no sugerir exigir que volviesen a la oficina claro a ver Apple vive de eso y ya vemos que todo el tema del Apple provision este o sea es que yo vi la late que Uruguay y todo eso pero es que básicamente todo era público ya que es una putada porque aquello de la famosa frase de One morcing no que eso era súper Guay cuando cuando en la esquino se la de Apple lo decían Y sabías que iban a lanzar un producto nuevo lo utilizó Steve Jobs con el iPad lo utilizó con el iPhone pero era el one fue como lo utilizó Tim Cook en plan para darle aire y ese énfasis guapo pero a ver ya todo el mundo estaba viéndolo aquí Note esperando a que hablase ya de esto Entonces sí es un poco faena que se filtre todo no Total que hoy en día eso de cómo trabajas tú antes todo el mundo sabe lo que lo que está haciendo el de al lado o el de enfrente el water Cooler este hacen cosas muy guapas pero tampoco sé cuánto puedo decir pero para detectar a la gente que filtra hacen historias muy chulas sabes cuando se publican fotos de un prototipo así digamos que tienen maneras de saber quién fue entonces de esta noticia quería extraer un poquito recomendaciones para los usuarios Martín un poco creada tienen que aprender los usuarios tienen que aprender a crear personas falsas online un poco de obsek y otra sería igual que se lee en el libro este de Extreme privacy de Michael bassell No sí a ver yo creo que la idea más que crearte un Face una persona falsa Claro si tu objetivo de redes sociales es estar conectado que muchas veces hemos hablado tú y yo Alexis que también hay que tener un poco de sentido común y por ejemplo yo mismo Pues utilizo redes sociales para estar en contacto con colegas o el objetivo es o no usarlas y así ya no te pueden escanear y si no pues sentido común no escribas en Twitter cuando te cabrees sabes está lleno de idiotas internet no vale la pena meterse ahí a hablar y insultar y cosas de estas mejor vete a dar un paseo Y luego vuelves Y bueno mantén tus privadas porque recordemos en principio esto es de Open source Entonces

si tú tu cuenta de Instagram Te la pones privada pues y no la pueden ver a no ser de ya tendrían que quedarse un usuario falso que te quiera seguir y que tú lo aceptes para que te siga Pero bueno eso no escala no porque recordemos que esto es de manera masiva Entonces si utilizas redes sociales pero por las privadas y luego pues no seas un dominguero no no pongas cosas chungas en redes sociales sea una persona coherente y educada y en principio pues esto es algoritmos no te detectarán como un terrorista o eso eso esperamos recomendaciones de tierra de hackers sé buena persona online sé buena persona hace el bien ama a los demás pues pasamos a la siguiente noticia Martín muy interesante la tuya Yo vengo a hablar de gigabyte pero no a la unidad de medida de bits de información sino a la empresa de productos electrónicos que vende temas como placas base o en inglés motherboards tarjetas gráficas o gpus no en inglés graphical a processing United dispositivos de almacenamiento como discos duros unidades de suministro de energía o Ups y otros accesorios para ordenadores como teclados ratones monitores y que bueno Estos son estimaciones siempre no pero aproximadamente he visto que tiene digamos el 20% del mercado relacionado a los productos que ofrece no y sus principales competidores son probablemente los conozcáis a la gran mayoría pero Intel a sus msi a ese Rock luego tenemos otros acer del Super Macro todos estos que tienen sus propios ordenadores y que crean sus propias placas base y sus propios tarjetas gráficas y similares Pues en relación a esta empresa investigadores de eclipseum que es una empresa de ciberseguridad que se dedica a investigar problemas en la cadena de suministro o supply Chain de dispositivos especialmente en firmware de dispositivos embebidos ha encontrado problemas en el firmware de placas base que gigabytes comercializa en el episodio 67 ya os hablábamos de vulnerabilidades en el sistema anti chip de este videojuego llamado gameshin Impact que cibercriminales han aprovechado para comprometer y desplegar ransomware en sistemas afectados pues eclipse fue uno de los primeros en alarmar de este tipo de ataque hasta que se hizo tan grave que os lo tuvimos que traer al podcast en dicho episodio y también en el episodio 71 ya os comentábamos también el problema del bring your own volver Driver o by o vd no una categoría de ataques cuya investigación involucró a eclipseum yo de hecho esta empresa me parece bastante interesante y aprecio mucho el trabajo que hacen porque hay muy pocas empresas que se dediquen a buscar este tipo de vulnerabilidades puertas traseras o cualquier otro tipo de tema de ciberseguridad que puede afectar a componentes embebidos que sean tan difíciles de encontrar y que puedan poner en riesgo nuestra privacidad y nuestra información lo digo porque se centran como digo en temas de firmware de sistemas embebidos y no hay tantas empresas o tantas personas que sepan analizar este tipo de componentes y también Bueno pues el tema es que esto afecta a millones de personas porque millones de personas en todo el mundo utilizan placas base de gigabyte o incluso en ordenadores gigabytes que vienen con la propia placa base gigabyte y probablemente tú querido oyente que estás ahora utilizando tu ordenador de sobremesa mientras escuchas este episodio y puede ser que dicho ordenador esté utilizando una placa base de gigabyte potencialmente afectada Así que Quédate con nosotros Y sigue escuchando porque os voy a comentar lo siguiente cuál es el problema exacto de seguridad de estas placas base Cuál es el impacto para todos nosotros los consumidores y un poco más alto nivel como afecta a las empresas Cómo determinar si vuestra placa base gigabyte es una de las afectadas importante y como remediar este riesgo y protegeros Pues el primer paso el primer punto sobre el problema de seguridad en placas base de gigabyte Esto fue durante el análisis que eclipseum realizó del firmware de ciertas placas bases de gigabyte pues identificaron lo que ellos llaman una puerta trasera en el proceso de actualización del firmware de labios o barra uefi Cuando digo puerta trasera se puede ver como esto pero realmente lo que dice eclipseum es que el código analizado está destinado a que gigabyte

instale actualizaciones de firmware a través de internet o desde un servidor en la red local lo que hace el firmware es ejecutar un archivo binario nativo de Windows Así que sabemos que esta vulnerabilidad ya para empezar solo afecta Windows ni a Max ni a Linux ni a otros sistemas operativos Así que aquellos que usen Windows pues seguir escuchando los demás también os lo sugiero por si esto se aplica a otros sistemas operativos No pero lo que digo es lo que hace el firmware es ejecutar un archivo binario nativo de Windows durante el proceso de inicio del sistema y este mismo ejecutable luego descarga y ejecuta binarios para llevar a cabo la actualización del firmware dices bueno Ok no le acabo de ver realmente el problema Alexis No porque los principales sistemas operativos como Windows Mako es Linux iOS y Android ya no si nos vamos a temas de móviles tienen funcionalidades similares para actualizarse y también temas de firmware no como dispositivos por ejemplo de red como routers firewalls puntos de acceso inalámbrico y otro dispositivo similares también ofrecen una funcionalidad similar pues entonces cuál es el problema Pues según Los investigadores el código de actualización no es completamente seguro y a ver te pregunto Martín a ver si tú sabrías decirme Porque Cuáles son Por qué no es completamente seguro este proceso de actualización bueno lo de siempre que vemos que es que no está firmado digitalmente no eso sería lo primero de todo correcto esa es una de las tres pero si esa sería con esa probablemente se arreglaría el riesgo en mayor parte entonces creo que ya sé por dónde vas porque o sea con eso cuando dices con eso se arreglaría me recuerda a un caso con vlc el famoso reproductor de vídeo que la gente O sea como es un proyecto de código abierto de Open source pues la gente puede mandar Pues eso Oye he encontrado este fallo lo que sea o simplemente pues Pull request en github no y la gente mandaba que se descargaba por http en vez de https es decir que el tráfico no estaba cifrado y se puso muy famoso una respuesta de un desarrollador en plan de muy malas formas que decía Mira somos cuatro gatos haciendo este reproductor nadie nos paga por esto está cifrado digitalmente Entonces cuál es el riesgo No me pongas esto Cuál es el riesgo real de esto qué más da que se transmita por un canal No cifrado si está firmado digitalmente Y la verdad es que tenía razón pero claro por otro lado es Pero por qué no lo pones por un canal cifrado y ya está si no tiene No tiene más entonces Supongo que lo segundo sería que iba por http correcto correcto y hay uno más también relacionado pero ahora ahora lo comento Sí pero el tema de http si es interesante porque puede ser que no haya a nivel de nivel de como lo diríamos integridad probablemente no habría tanto problema no pero a nivel a nivel de confidencialidad uno podría ver que estuviera interceptando en plan se está conectando y incluso que qué archivos está descargando porque puedes hacer el Hash de ese archivo descargado no Y claro pero pero aquí es donde sí sí sí pero vale se podría saber alguien que está en tu misma red bueno o tu isp o lo que sea que usa su vlc incluso la versión Supongo pero bueno a nivel de riesgo riesgo es muy muy bajo Pero por otro lado tío por lo cifrado ya Aunque mira yendo Depende como está implementado el tema de si es firma digital Pues a ver el firma digital creo que de momento no se han encontrado fallos No pero si nos ponemos en el tema de Hash no en plan el Hash tiene que ser este Hash y es md5 y ya vemos que hay colisiones de md5 de Hash pues Alguien podría sabes crear un archivo malicioso que tuviera el mismo Hash que está esperando pero para poner un caso que en el futuro cuando tengamos el Quantum computing aquí No empecemos a crackear aquí claves públicas privadas Pues eso va a ser mucho más factible Ah Mira se me acaba de poner una idea de futuro ponte http porque cuando venga el Quantum vas a ver pues como muy bien has dicho Martín uno de los primeros fallos es el tema de que se utiliza http que como comentamos se podría discutir no el tema si si hay temas de mayor riesgo o no pero bueno se puede se pueden realizar ataques de hombre en el medio en este escenario por ejemplo vía dns spoofing de dominios dns y similares el segundo relacionado con http en este caso https que aunque la intención es

buena porque hay dos urls que están configuradas en la placa base la misma URL está configurada con http y con https depende del modelo que te haya tocado Y supongo que alguien se dio cuenta y en las más modernas han puesto https que es una la intención es buena pero no validan el certificado del servidor remoto Así que estamos en las mismas si yo me hago spoofing de dns y digo que soy ese servidor y hago y me consigo un certificado válido por el digamos el catálogo de certificados que tenga el sistema operativo en el que se está corriendo pues pasaría también estaríamos en el mismo caso no algo curioso de esto es que una de las urls Aunque utiliza https es https dos puntos barra barra software-nas barra SW http barra Live update 4 que si os habéis dado cuenta No es un nombre de dominio completo sino un nombre de máquina que presumiblemente estaría en la red local porque el Host es software- nas ya está sin ningún puntocom sin ningún otro top Level domain ni nada de esto esto significa que un atacante en la misma red local podría engañar el proceso de actualización para que se conecte a su sistema porque cuando estás pidiendo eso en una red local sistemas Windows lo hace normalmente por Bueno hay formas no wpads y sistemas similares que hay herramientas como responde no u otras otras que pueden que pueden responder en nombre de cualquier nombre de Host que no existe en la red Pero bueno que es otro tema que se que tiene riesgo de ser atacado con temas de falsificación o spoofing de dns Y luego el último que es el más importante como bien dicho Martín el tema de la falta de verificación de firma digital del archivo de actualización descargado no se implementa esto y por tanto Bueno no es tan fácil no No es que pueda ser crear un archivo y dárselo a actualmente al proceso de actualización tiene que estar firmado digitalmente por Microsoft Pero esto es algo fácil de conseguir con identidades desarrollador falsas y similares no te puedes crear una cuenta en de desarrollador en Microsoft y firmar el archivo y bueno y entregárselo a este proceso de actualización una vez hecho el tema de Man in the middle o bueno Incluso comprometiendo si algún atacante comprometiera estos servidores de gigabyte.com Pues también lo podría servir directamente desde ahí pero no sólo hay estos tres porque indagando me he encontrado con un par de vulnerabilidades adicionales en productos gigabytes Esto fue porque mire en Twitter que siempre un poco lo criticamos Pero oye Twitter todavía sigue dando sus frutos una de estas dos vulnerabilidades se refiere al control Center de White o gcc curioso nombre que también se llama como el compilador DC no pero es un paquete de software diseñado para mejorar la experiencia del usuario con hardware gigabyte no como he dicho placas base tarjetas gráficas y similares pues este componente lo que se encarga es de temas de configuración actualizaciones y en este caso el componente vulnerable se llama file Drop o es una funcionalidad llamada file Drop que se encarga de transferir archivos cuando se habilita esta funcionalidad en el control Center de gigabyte este componente crea un usuario en Windows llamado gtc guión bajo filedrop con contraseña gbt123 gcc tela ahí o sea te crea un usuario por defecto Sin decirte nada y ahí te lo deja porque lo malo es que cuando vas y desinstalas esta aplicación el usuario no se elimina A menos que hayas deshabilitado la funcionalidad anteriormente que dices otro fallo cuando desinstalas la aplicación Borra el usuario pero no solo se borra el usuario cuando deshabilites la funcionalidad y una vulnerabilidad adicional es una vulnerabilidad de inyección de dll que permite persistencia esto ocurre en la herramienta vga de gráficos de gigabyte del mismo componente control Center de gigabyte este software instala una tarea programada que se ejecuta Al iniciar sesión por todos los usuarios con derechos de administrador en el contexto del administrador predeterminado Pues esta tarea en concreto lanza el proceso graphics Card engine.exe con privilegios elevados que sufre de esta vulnerabilidad que comento que es de inyección de dll Y si un usuario que tiene que tener privilegios de administrador puede modificar el archivo dll cargado con una dll maliciosa Pues ejecutaría el código que está en su dll maliciosa Y pudiendo obtener obviamente ejecución de

código e incluso persistencia porque esto se ejecuta cada vez a través de una tarea programada cada vez que un usuario con derechos de administrador hace login en el sistema como digo hay un par de limitaciones no el para abusar de esta vulnerabilidad y ejecutar este exploit tiene que ser administrador y luego que un usuario con privilegios de administrador tiene que haber hecho login en el sistema para que la tarea se ejecute y Por ende el proceso malicioso de persistencia también se ejecute estos dos últimos problemas de seguridad no están asociados a la investigación de eclipseum y fueron publicados recientemente a finales de mayo y sobre estos no he encontrado referencias a respuestas de gigabyte al respecto o que han hecho pero bueno lo que los quería comentar igualmente según Los investigadores las técnicas utilizadas en la actualización del firmware de las placas base de gigabyte son muy similares a cómo funcionan algunas familias de malware de firmware como la puerta trasera de computrace Low Jack También conocido como low Jack Double agent o lojacks que fue abusado de esta funcionalidad por actores de amenazas como el grupo apt ruso setnite También conocido como apt 28 fancy Bear que explotó esta funcionalidad con su malware low jacks para hacerse pasar por una característica legítima de antirrobo de ordenadores portátiles lo que hizo pues es suplantar digamos hacerse pasar por esto e instalaba el malware cuando cuando se ejecutaba cuando se daban estas funciones de estas rutinas de actualización la mayoría de estas familias de malware se utilizaron para permitir la persistencia de otro malware basado en el sistema operativo esto lo conseguían haciendo que sus ejecutables nativos de Windows parecieran herramientas de actualización legítimas en el caso del malware no sé si te acuerdas Martín pero es un implante de firmware de bios weephy que comentamos en el episodio 14 la carga útil de Windows se llama hablamos del año 2020 tío pero está claro que a día de hoy ya hemos cubierto Prácticamente todo Sí pues en este caso lo que hacían era como digo utilizar una carga útil de Windows que se llamaba Intel updater.exe que la verdad es que no no levanta sospechas verdad si vosotros veis Intel update punto exe y utilizáis un procesadores Intel o temas de Intel pues obviamente No levantes sospechas ahora si estáis utilizando temas de amd pues os levanta sospechas o igual lo habéis utilizado anteriormente y decís Oh esto seguro que se me ha quedado aquí archivos que no borré antes cuando cuando me cambié de ordenador no esto es muy común y grupos apt siempre tienen a mezclarse con el entorno no en plan técnicas camaleónicas o como se conoce un poco más oficialmente técnicas del living of the Land o LoL que implican el uso de herramientas y procesos legítimos del sistema para esconder su actividad maliciosa y eludir la detección Pues ahora voy a comentar el impacto para todos nosotros debido a estas vulnerabilidades un ciberdelincuente podría abusar de este hecho y suplantar al servidor de gigabyte o secuestrar la conexión y proporcionar código malicioso para que sea ejecutado por el proceso de actualización del firmware de la placa base y esto es muy preocupante porque este proceso corre con privilegios elevados porque el usuario por lo que el usuario malicioso podría obtener estos mismos privilegios al correr su código malicioso su malware y hacer mucho daño al sistema alturas de episodio 97 no os tengo que decir qué maldades podría ocasionar un usuario malicioso que obtenga ejecución de código remoto como administrador en vuestro sistema porque Supongo que ya lo sabéis ya lo hemos mencionado más de una vez todo todo lo malo que pueden hacer los cibercriminales no pero bueno lo más preocupante para daros algunos y refrescar la memoria para darnos algunos ejemplos sería el espionaje robo de credenciales que les pudiera facilitar acceso a sistemas financieros como banca online criptomonedas suplantación de identidad y similares el problema con esto es que un atacante que abuse de esta vulnerabilidad este proceso de actualización podría comprometer el firmware de la placa base y Añadir componentes de persistencia lo que le permitiría reinfectar los sistemas operativos como Windows que estuvieran afectados aunque se reinstalará el sistema operativo de nuevo desde cero

completamente limpio ya que el malware este ciberdelincuente lo podría instalar a nivel de firmware de la bios o uefi esto es muy difícil de detectar para un usuario normal y la única forma de evitar esto sería reinstalando el firmware uefi que es algo también a lo que no se enfrenta día a día un usuario normal porque por lo que igual le sería algo complicado de llevar a cabo o de arreglar el caso más extremo sería cambiar de placa base no tirarla a la basura obviamente y cambiarse para comprarse otra placa base que no sea del mismo fabricante porque gigabyte tiene cientos de placas bases afectadas pero vemos que hay otras opciones antes de llegar a dicho punto Aunque depende del nivel de Confort del usuario pues lo lleve a cabo o no O igual se tire por esta última opción estos problemas nos exponen a todos Ya que son problemas de cadena de suministro o supply chains no que son como un efecto dominó ya que al afectar a un único componente en este caso la placa base se puede afectar a muchos más sistemas como a los sistemas operativos que corren estas placas base o si lo llevamos al campo Más allá de la virtualización Pues imagínate a todos los sistemas que corren en Hardware específico que tiene una placa base gigabyte Los investigadores identificaron este código en cientos de modelos de placas base de gigabyte según comentan han publicado nombres de 287 modelos de placas base afectadas pero en su blog online mencionan que en una actualización reciente han identificado hasta 406 modelos supongo que en breve actualización actualizarán la lista de los nombres de modelos de placas base afectadas pero en las notas del episodio Vais a poder ver un enlace a un PDF que ha publicado eclipseum que contiene los nombres de los 287 modelos afectados no solo eso sino que como dije cómo podéis determinar si vuestra placa base de gigabyte es una de las afectadas Pues eclipseum también ha publicado otro un digamos un Script en un repositorio en github que contiene código Powers para que los usuarios cualquiera de nosotros podamos descargarlo y correrlo en nuestro sistema y determinar si el sistema está afectado por estas vulnerabilidades Este Script de hecho o sea una de las formas de ver si vuestro sistema es uno de los afectados es iros al enlace PDF que he mencionado anteriormente otra forma es ir a esta Script en Power shell en github y ver la lista de 287 modelos también de nombres de placa de placa base que hayan listado o ejecutar el Powers directamente no no tiene nada malicioso obviamente son unas pocas líneas de código la mayoría del Script son 88 hashes que son los hashes correspondientes al proceso o archivo con nombre gigabyte update service.exe que por lo que veo eclipse Uma determinado que hay 87 88 hashes distintos que están afectados por este código y también lo que hace es obtener el nombre de la placa base del sistema y lo compara con estos 287 nombres de modelos de placa base afectados en respuesta a estas declaraciones de eclipse y hay que decir que eclipse ha trabajado muy de cerca con gigabyte pues la empresa ha publicado parches para las placas base afectadas pero de momento solo para las basadas en Intel 700 o 600 y amd 500 o 400 Y qué ha hecho pues ha implementado verificación de firma de los archivos descargados Martín y verificación de certificados del servidor remoto Así que ha arreglado en principio todo el problema arreglado cada uno de los puntos aunque no menciona el hecho de que ahora solo utilicen https pero yo entiendo que como dicen ahora verificamos certificados del servidor remoto entiendo que como en http no hay certificado pues Supongo que obvian esa parte pero no lo especifican explícitamente que hubiera un poco aclarado mis dudas Sí sí un poco la argumentación exacta de uno de los desarrolladores de vlc pero tus noticias mucho más relevante que vlc porque vlc hablamos de que te puedan instalar pues una aplicación maliciosa Y tal Pero siempre tiene un contexto limitado tú hablas de firmware importantísimo en el ordenador que podrías tener mucho más acceso desinfectarse es algo a ese nivel claro el tema es eso Porque primero corre a nivel de administrador esta rutina de actualización de firmware y el otro tema es que puedes estar como fantasma no escondiéndote entre las sombras porque está a nivel de firmware de placa base como digo de

que alguien bueno ya no uso vlc lo desinstalo Claro claro bueno apunte te vuelven a comprometer la próxima vez que reinicies el sistema Pues cómo podéis remediar este riesgo y como podéis protegeros lo primero como he dicho aplicar el parche que gigabyte ha publicado igual como digo no han tenido tiempo de publicar el parche para todas las placas base afectadas que igual es una de las vuestras Así que os animo a que continuéis monitorizando su sitio web para que en cuanto salga el parche para vuestra placa base lo apliquéis lo segundo es inspeccionar y Deshabilitar la función descarga e instalación del centro de aplicaciones en la configuración de iOS uefi en las placas base o sistemas gigabyte y de esta forma evitáis que bueno de esta forma evitáis que se actualice hasta que se arregle este problema y cuando se arregle obviamente Supongo que queréis actualizar la placa Aunque hay veces que tienes placas base que no hace falta actualizar y a no ser que tenga que instalar componentes muy modernos que hay algún tema de no sé de velocidad del el bus de comunicación con ese dispositivo a veces no hay que instalar parches a no ser que sean de seguridad como este no pero en cualquier caso si no tenéis que actualizarla podéis Desactivar esto y con esto lo que hacéis es que evitáis que se ejecute ese proceso de actualización a día de hoy vulnerable y también establecer una contraseña en la biosf uefi para evitar que alguien malicioso Aunque tendría que ser en persona no vaya y cambie este esta configuración también lo que podéis hacer es bloquear las urls hardcodeadas en las configuraciones de las placas base que son a las que se conecta el proceso de actualización de firmware son tres No las voy a mencionar porque son largas pero las podéis ver en los enlaces de las notas del episodio dos de ellas una es http la otra es https y la última Es https que es la que he dicho que es software-las que se entiende que es un servidor en la misma red local y luego tenemos el tema de analizar firmware en busca de vulnerabilidades esta es una medida un poco más aplicable a capacidades de empresas no con esta con esta que se pueden permitir el lujo de llevar a cabo esta esta tarea pero hoy en día Cualquier usuario puede ir a descargarse el firmware de dispositivos embebidos Como por ejemplo placas base gigabyte y utilizar herramientas Online para llevar a cabo un análisis de seguridad Aunque de nuevo no es algo que sea fácil de hacer y no es algo que sea digamos al alcance de todos los usuarios pero es algo que si alguien está intrigado y tiene los conocimientos Oye pues puede ir ahí y descargarse el firmware y con cierto conocimiento pues analizarlo y compartirlo con la comunidad como de esta empresa y lo último bueno Es relacionado con las otras dos vulnerabilidades que he mencionado una la que te instala el usuario por no por defecto no pero este usuario llamado gtc guión bajo file Drop pues lo primero es si no tenéis esta si no estáis utilizando esta funcionalidad desactivadla y de esta forma se borra el usuario directamente o si no ir a borrar este usuario ahora mismo porque Este es otro usuario que se va a poder utilizar que seguro que grupos cibercriminales lo van a Añadir a su lista de contraseñas lo podemos llamar por defecto o usuarios que podría intentar utilizar para pivotar o para conseguir mis objetivos no porque es un usuario que tiene una contraseña hardcoreada que se instala se crea Cuando se activa esta función de transferencia de archivos a través del control Center de gigabyte y lo otro es bueno con el tema del escala de privilegios y persistencia a través de la herramienta vga del control Center de gigabyte Pues también estar al tanto a ver si publican un parche en breve y si no monitorizar este archivo para ver si se ha modificado recientemente de alguna forma y bueno investigarlo por esa parte quería cerrar la noticia también con muchas veces cuando porque esto me vino me pareció interesante muchas veces cuando hay una vulnerabilidad de una empresa que cotiza en la bolsa como es el caso de gigabyte y que tiene una capitalización de Mercado de 152 mil millones de dólares que no es no es calderilla pues normalmente como digo cuando hay un impacto de este tipo que afecta a usuarios porque como digo este tipo de productos placas base gigabyte o ordenadores gigabytes se usan millones de usuarios lo usan en todo el

mundo pues normalmente cuando sucede algo de este tipo el valor de su stock tiende a disminuir pero curiosamente en este caso He estado mirando un poco la Gráfica del stock de gigabyte y el valor de gigabyte ha ido incrementando de hecho y en el último mes ha subido un 73% que es una barbaridad y en los últimos seis meses ha subido un 134% Así que algo deben estar haciendo bien porque incluso aunque aunque tenga esta este impacto a los usuarios parece que a sus inversores no le ha importado mucho Yo no sé si es que sus inversores no los productos de gigabyte no utilizan las placas base por tanto les da igual que haya surgido este tipo de incidente así bueno en cualquier caso no les importa en cualquier motivo y con esto queridos oyentes llegamos al final de la de la noticia y a la pregunta del episodio que es la siguiente en el caso de esta vulnerabilidad en el proceso de actualización del firmware de placas base de gigabyte estarías dispuesto a seguir usando sus productos en el futuro os damos cuatro opciones la primera Sí porque se puede mitigar el riesgo y hay parches y todo esto no lo que he comentado si me Temo que lo tengo que hacer porque mi empresa tiene un contrato de varios años con gigabyte y no puedo ahora tirar todo esto a la basura No ya que debido a este incidente ya no los veo seguros y la última es no nunca más pues interesante y bueno muy buena esa como vuelta al tema de vlc esta vez con repercusiones mucho más graves porque lo que decíamos no que no es lo mismo que una aplicación pueda ser vulnerada porque instalas una maliciosa que también por supuesto tienes consecuencias que el firmware de placas base yo por mi lado a ver a la hora de la pregunta todo software tiene vulnerabilidades pero también hay vulnerabilidades que es como como puede ser esto posible sabes no es algo rocambolesco un fallo de un Us after free porque un puntero en memoria no sé qué es tío lo más básico o sea firma digitalmente el firmware O sea no quién estaba al mando aquí quién hay algunos checks por los que pasa antes de salir a producción el sistema hubo algún tipo de review por parte de una entidad tercera no un ser parte es que esto es algo de que cantan el momento o sea incluso a la hora de tener una conversación ni siquiera tienes que mirar el código Oye cómo Cómo estáis haciendo esto no sería una de las primeras preguntas que le harías si está no sé de manera un plan le estás haciendo consultoría a la empresa no entiendo cómo esto ha llegado a producción la verdad Y eso es un poco lo que me inclinaría a decir confiaría en esta empresa para que sabes tener toda mi vida digital en sus sistemas claro y es que bueno a ver gigabyte si fuera china diría Bueno no sé pero está echaríamos todos pero al ser taiwanesa dices Bueno está ahí de momento probablemente sea Imparcial pero un escenario de ataque digamos lo claro las placas base están en en Torres no que normalmente son bastante grandotas Aunque si llegaba no he mirado pero igual gigabytes tiene mini PCS Pero bueno no sería el caso no el caso que quiero poner como ejemplo es Imagínate que tienes un portátil Martín de gigabyte y te lo llevas a una red pública tipo Starbucks y lo enciendes justo cuando lo enciendes tu ordenador va a ir a conectarse a una de estas tres urls y una de ellas es software-nas que es un un nombre de Host en la red local y como eso corres un sistema Windows pues va a pedir Oye Quiénes software y tú que eres atacante malicioso dices eh soy yo entonces se conecta a ti le ofreces el la actualización de firmware maliciosa que se va a aplicar a nivel de la bios uefi Y de esa forma vas a mantener persistencia y ser un espectro en el ordenador de esta persona y poderle robar todos sus secretos mucha conspira No ya pero bueno esperemos que haya sido simplemente aunque no sabemos cómo un error de tantos que hemos hablado aquí en tierra hackers en software software crítico pero bueno esperemos que haya sido solo eso y esperemos las respuestas del comité de sabios que son estos nuestros queridos oyentes hasta aquí Hemos llegado episodio 97 a 3 de los 100 algo se nos ocurrirá para hacer especial Muchísimas gracias por quedaros hasta el final no como siempre os decimos nada nada nuevo aquí recordar dejarnos alguna review donde nos estáis escuchando que nos ayuda un montón nos ayuda a ganar visibilidad nos ayuda para que validar frente a nuestros

sponsors que vale la pena apoyarnos nos ayuda simplemente para lo más importante que más gente nos descubre nos escucha cuánta gente vemos entrar todos los días en discord seguirnos en Twitter mencionarnos de ostra acabo de descubrir el podcast y me encanta Muchísimas gracias queridos oyentes por seguir divulgando la palabra de tierra de hackers a vuestros amigos compañeros conocidos redes sociales bueno Esperemos que redes sociales no no se haga un patrón no de un indicador de compromiso de que eres un terrorista y escuchas tierra de hacker pero nada de momento seguir utilizando las redes sociales para hablar de nosotros Gracias por todo eso eso Por ejemplo como cuando comentábamos antes del tema de discord no que vieron comentario graciosos al tema de World Coin cuando vayáis al carnicero de turno y le pidáis ocho ojos de vacas o de bueyes y os pregunta que Vais a hacer con eso le decís escucha los episodios de tierra de hackers y vas a saber lo que es bueno eso bueno queridos oyentes nos vemos y nos escuchamos en el próximo episodio Adiós adiós Chau chau que vaya bien 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 haters