uno de los grupos de ciberdelincuentes más importantes en la actualidad cae ante el FBI que según ellos y parafraseándoles hemos hackeado a los hackers reuters y Citizen lab han publicado detalles sobre fallos fatales de sistemas de comunicación encubierta que permitieron a los gobiernos de Irán y China Identificar arrestar y asesinar a decenas de espías de la Cia se vienen conferencias sorteos y un nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 29 de enero de 2023 este es el episodio 81 yo soy Martín vigo y está conmigo algo pochillo pero al pie del cañón Alexis porros Hola Alexis Qué tal cómo te encuentras Pues ahí bien bien Ahora ya estoy recogiendo las como tú dices el cañón pues estoy recogiendo la munición para empezar a disparar de nuevo a toda leche digámoslo así pero nada con mucha emoción no porque estamos a unos días del Barcelona Cyber Security Congress Qué pena de nuevo que no pueda estar ahí pero Martín va a estar ahí ondeando hablando de cañones y tal pues vamos a vamos a seguir con el tema Martín va a estar ondeando declaró la bandera de tierra de hackers y la va a plantar ahí así que nada con muchas ganas de ver como como se cuece el temilla y que surge de todo eso y nada bueno lo primero es lo primero Muchas gracias a todos vosotros queridos oyentes por apoyarnos online en redes sociales discord en todos sitios y plataformas de podcast también sobre todo y hablando de esto os recordamos que estamos en la mayoría de plataformas de podcast sino en todas y que si no lo estáis deberíais suscribiros ya También estamos en redes sociales decir que estamos en Twitter infoeck.ec exchange el servidor de mastodon Instagram Facebook en todas estas estamos con el handle arroba tierra de hackers como tierra de hackers los correos electrónicos no los podéis enviar a podcast arroba tierra de hackers.com y en discord Pues estamos también ahí podéis acceder vía tierra de hackers.com barra discord finalmente como siempre os agradecemos vuestro apoyo a la pregunta del episodio que publicamos en Twitter y que fue la siguiente estás de acuerdo con que el gobierno de Estados Unidos comunique a las personas de que añadido su nombre a la no Fly list recordemos que la Nou Playlist es esa lista estadounidense que incluye personas sospechosas de ser terroristas Pues como siempre tenemos cuatro respuestas la más votada fue Sí total transparencia por favor con un 64% de los votos seguida de no confío en el gobierno con un 16% seguirá también de otro no pero en este caso avisaría a terroristas No pues no quiero que se comunique con un 14% y finalmente Sí para evitar el trauma que mencionábamos de padres que tenían que ser bueno investigados delante de sus hijos en aeropuertos con un 6% Así que ahí lo tenemos muy bien y yo pues como dices tú como siempre vamos dándole las gracias a nuestros mecenas de patrón que aparte se nota que esta semana hubo movimiento porque tenemos a tres oyentes nuevos apoyándonos en patreon a Tony sansano a Carlos vals y luego tenemos a zolomeo paredes que bueno yo he de agradecer a Alexis que me dio así como una pistilla que a lo mejor este nombre iba con segundas esto de solomeo paredes porque yo no me hubiera dado cuenta pero bueno Oye que a lo mejor Esto es así no sé en cualquier caso Muchísimas gracias por vuestro apoyo de verdad como siempre os digo hace una diferencia tremenda nos ayuda a crecer tenemos cositas en las que estamos trabajando Y muchísimas gracias por por estar ahí y luego pues como siempre agradecerle a mónad también nuestro sponsor 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 monata a través de una herramienta de gestión y visualización de telemetría de datos una empresa fundada en silicon Valley que está buscando muchos ingenieros sobre todo con algo de experiencia en seguridad para ayudarlas construir y hacer realidad su misión lo mejor de todo es que están contratando en todo el mundo y en remoto así que ya sabéis monart.com les podéis escribir y mandar vuestro currículum a tierra de hackers @monat.com que están creciendo a tope decía Alexis también el tema de la Barcelona Security Congress que empieza

Este martes martes miércoles y jueves y tierra de hackers va a estar ahí haciendo mil historias por un lado somos media partners de Barcelona saber Security Congress por otro lado Yo estaré llevando en nombre de tierra de hackers todo el hacking Village presentando los speakers haciendo de moderador en tres debates durante dos días y en general pues estaré allí todo el día así que si os vais a animar a venir ya sabéis pasaros por el hacking Village venir a saludar a lo mejor tengo pegatinas y otras cositas Así que no no dudéis en venir a decir hola también estaremos posteando porque hemos conseguido descuentos del 50% en las entradas tenemos un código que lo pondremos en Twitter Así que lo tenéis ahí también y luego pues ya había mencionado también que vamos a sortear entradas para la ruta en Madrid esto lo haremos probablemente dentro de para la semana o la siguiente lo anunciaremos por Twitter como siempre y ya os decíamos que algunas de esas entradas pues las tenemos reservadas solo para los mecenas de potro de patreon pues como como agradecimiento no a su apoyo y por supuesto otras para el resto de los oyentes como no así que muchísimas gracias como siempre por vuestro apoyo por dejarnos reviews en las plataformas porque eso ayuda a la gente que nos siga descubriendo y yo creo Alexis que ya nos vamos con la después de esta intro con la primera noticia Sí sí el apartado el departamento de Justicia de los Estados Unidos Pues nos sorprendía hace apenas unos tres días publicando en su canal de YouTube una rueda de prensa donde anunciaban el desma conocimiento de uno de los grupos de ciberdelincuentes más dañinos en la actualidad heinz que por cierto menciono también Perdón por el eco como vengo pidiendo perdón Durante los últimos tres episodios aún estoy aquí montando todo mi hacker space todo mi playroom y así que de momento lo tengo muy vacío y me fastidia un montón que se escuche este eco Pero bueno perdonad y espero que no sea demasiado grave total Dónde estaba que bueno decía que si bien este desmantelamiento podría ser una historia más de tantas que concierne la captura de un grupo de ransomware las cosas se ponen más interesante cuando en esa misma rueda de prensa del FBI podemos Escuchar lo siguiente esto se traduciría como en pocas palabras mediante métodos legales hemos hackeado a los hackers esto desde luego llamó mi atención y me parece muy importante destacar aquí tenemos a la fiscal general de los Estados Unidos en declaraciones oficiales comentando que han hecho aquello de hackback no o si tú me hackeas yo te hackeo Uh interesante Esto del hackback que comentas ese me recuerda a lo que cubrí en un episodio anterior sobre el gobierno de Australia que creó su equipo de contraataque ofensivo con 100 personas full time para combatir el ransomware efectivamente de hecho planteabas tú la pregunta a los oyentes sobre qué les parecía esto y como decía Alexis lo hemos comentado varias veces en tierra de hackers como los gobiernos no están a utilizar como defensa la ofensiva remangarse ante el teclado y comprometer los sistemas de los malhechores en vez de simplemente centrarse en defenderse de los ataques se han digamos dejado de tonterías y han dicho a tomar por saco Vamos a ponernos serios y a reventar a esta gente desde luego interesante Este cambio de narrativa Y si bien sabemos que por operaciones del pasado esto ya lo hacían en parte el caso no de en crochet por ejemplo ahora ya lo dicen abiertamente y con énfasis sin pelos en la lengua Pero antes de ver cómo el FBI hackeo a hype dejarme que os presenta este grupo de delincuentes y sus fechorías porque de hype todavía no habíamos hablado jaifer es el típico grupo de amenazas que se centran ataques tipo ranson como mencionaba y sigue todas las pautas típicas de este tipo de grupos como bien sabéis de habernos oído hablar en episodios anteriores comprometen empresas de todo tipo y se dedican a exfiltrar toda la información que pueden para luego cifrar todos los sistemas comprometidos Así pueden hacer una doble extorsión por un lado vender la capacidad de descifrar y desbloquear los sistemas de la empresa comprometidos que muchas ocasiones causa la incluso la disrupción del servicio que ofrece la empresa y por otro lado exigir un pago

rescate por los datos robados amenazando incluso con ponerlos a subasta o directamente publicarlos normalmente Pues en una página en la Deep web pues hyve hace Exactamente eso según el FBI son responsables de haber comprometido más de 1.500 empresas en más de 80 países ahí es nada y es y todo esto contando solo desde junio de 2021 es decir en menos de dos años de operaciones Y por supuesto la razón por la que se dedican al tema de ransomware es por lo lucrativo que es cuánto crees tú Alexis que ha dicho el FBI que han ganado ya Cuánta pasta 200 millones Bueno te has pasado un poquito 100 millones de euros 100 millones de euros tío Esas son las cantidades que se están moviendo en la industria de los ataques tipo ransomware me parece una locura pero su modelo de negocio No es únicamente hacer ataques ellos mismos sino que alquilan su tecnología a otros ciberdelincuentes y de acuerdo al FBI estipula que se llevan un 20% de las ganancias lo que conocemos como ransomwaras a service y que ya también varias veces os hemos mencionado otro punto a destacar es la moral si bien puede parecer llamativo muchos grupos de ciberdelincuentes tienen cierta ética y no atacan hospitales nada que tenga que ver con niños y cosas así pero este no es el caso de hyve cuyo malware ha sido utilizado por ejemplo para comprometer hospitales incluyendo uno durante la peor parte de la pandemia que daba servicios críticos a pacientes que sufrían severamente de las consecuencias de la infección por covid-19 esto hasta el punto sucedió que tuvo que pasar a usar lápiz y papel debido a la magnitud del ataque que dejó sistemas críticos utilizados en el día a día en el hospital totalmente bloqueados hasta que no se efectuase un pago millonario en este caso el modus operando de hype para comprometer empresas se centraba mayormente en encontrar empresas cuyo acceso a redes internas mediante escritorio remoto o portales de VPN no estaba protegido por autenticación de doble factor Aquí como siempre la lección de turno siempre siempre hay que activar el doble factor y ya no te digo si hablamos de portales corporativos que dan acceso de una manera u otra a sistemas o redes internas también hubo ocasiones en las que directamente encontraban maneras de saltarse la autenticación de doble factor que yo recuerdo ver por ahí Creo que es un libro de la editorial Now Stars press que va sobre un libro entero sobre cómo saltarse autenticación de doble factor que me pareció súper interesante no me lo leí pero leí varios trozos y había ataques bastante interesantes esto En parte de esto de centrarse en sitios que o se pueden saltar la autenticación de doble factor o simplemente no la tiene nos dice que de alguna manera tenían acceso a credenciales de empleados o directamente los adivinaban mediante pues Fuerza bruta o diccionarios de contraseñas comunes Aunque últimamente el mercado de los steelers está muy en auge y se sacan muchos credenciales de ahí de hecho una vez más en tierra de hackers os hemos hablado varias veces de los famosos steelers este tipo de malware que se instalan máquinas y lo que se dedica a ser recolectar toda la actividad todo el tráfico en internet todo lo que se pueda digamos lograr y subir esos logs a los servidores de los malos para luego simplemente venderlos puede contener cosas útiles o contener simplemente pues cosas que no tienen mucha utilidad pero se suben en la cantidad de los gigas y gigas y los puedes comprar súper baratos un poco para para buscar petróleo ahí no para buscar oro por supuesto cuando nada de esto funcionaba recurrían al tan Afamado y efectivo fishing mandando emails falsos que llevaban a las víctimas a revelar sus credenciales de hecho también se observó que en ocasiones explotaban los sistemas mediante archivos maliciosos en esos propios emails que explotaban ciertas vulnerabilidades vulnerabilidades que según lo que leía en la propia página del cisa que Ahí os la dejo en las notas del episodio para que podáis ver los indicadores de compromiso Pues eran vulnerabilidades centradas en Microsoft exchange concretamente el CV 2021 31207 el 20 21 34 473 y el 20 21 34 523 Estos son tres vulnerabilidades críticas que ayudan a vaipasear a saltarse ciertas protecciones dan ejecución de código remoto y la otra la tercera es para elevación de privilegios O sea que un poco

explotando el mismo software tienes todo el pack de lo que necesitas curiosamente para exfiltrar la información utilizaban mega punto nz el famoso servicio de almacenamiento en la nube de Kingdom Que tanto se usaba para piratería hace años bueno Supongo que a día de hoy pero antes de que profilerasse pero es viteroles proliferase antes de que profile me cago antes a ver antes de que no me sale proliferase Cómo proliferas a vale antes de que profile al cerebro macho antes de que profe no me sale que lo estoy haciendo a propósito Pero te lo juro que no me he quedado Atrapado tío es que me rayaste con lo de profiteroles digo antes de que proliferase antes de que proliferase ya no sé ni dónde estaba antes de que proliferase la piratería decía por el tema de de Mega punto nz el Mega aplaude famoso si os acordáis Pero bueno lo que decía os dejo la lista de indicadores de compromiso en las notas del episodio Bueno o sea que ahora que ya conocemos un poco más no los tejemanejes de hype cómo hizo el FBI para hackearlos Y qué hizo una vez los hackeó esto es muy interesante pues lo malo es que como cabría esperar el FBI no dio muchos detalles al respecto indagué bastante pero no pude encontrar mucho más aparte de las propias declaraciones del departamento de Justicia de los Estados Unidos Lo que sí mencionaban es que fueron capaces de y cito textualmente robar las claves criptográficas y dárselas a las víctimas y este es un punto súper interesante porque convierte este caso de desmantelamiento de un grupo delincuentes en algo único normalmente los casos que hemos visto sucedían un poco a posteriori y los cuerpos y fuerzas de seguridad del Estado no solo paraban las operaciones del grupo sino que además solían recuperar pues millones en criptomonedas No desde que habían hecho a través de las estafas de los de los sobornos y todo esto en este caso no es así ya que parece ser que el FBI estuvo infiltrado en los sistemas de hype desde julio de 2022 no sólo eso sino que en vez de limitarse a monitorizar los movimientos de hype para averiguar Quiénes eran Y a quién atacaban el FBI se dedicó a ir exfiltrando las claves criptográficas usadas para cifrar los sistemas de las víctimas cada víctima tenía su propia clave y el FBI no solo las filtraba sino que de manera secreta se las pasaba a las víctimas para que no tuvieran que pagar el rescate y pudieran descifrar todo toma ya o sea yo me quito el sombrero con el FBI no solo me meto en tu casa sino que me quedo escondidito ahí viendo todo lo que haces Y te voy robando las llaves con las que encierras a tus víctimas para que puedan liberarse sin pagarte Me parece muy top esto según el FBI robaron más de 300 claves criptográficas Aunque bueno en otro artículo que recopilé hablaban de mil claves criptográficas que entregaron como decía a las víctimas para descifrar sus equipos ahorrándoles millones y millones de dólares en pagos al grupo criminal entre las víctimas liberadas estaba una escuela de Texas a la que le pedían 5 millones de dólares un hospital de alusión al que pedían 3 millones de dólares e incluso una empresa de alimentación a la que pedían 10 millones de dólares por esa clave que el FBI luego se la dio de manera gratuita el director del FBI curiosamente mencionó que solo el 20% de las víctimas les contactó para pedir ayuda se especula que esto este bajo número no de de víctimas que que van a las fuerzas y cuerpos de seguridad del estado se debe a que en muchas ocasiones las empresas prefieren pagar y mantener en secreto que han sido comprometidas lo cual Por cierto va en contra de la ley me pregunto si el FBI dada esta ocasión única en la que podían ver en tiempo real las empresas que estaban siendo comprometidas usó esto para ver si las empresas daban parte de esto a las autoridades o se los callaban en plan este viene el FBI te dice tengo una noticia buena y una mala te voy a ahorrar 5 millones en el pago del rescate Pero te voy a meter 10 millones de multa por no decirnos nada Me pregunto si hicieron algo así y no sé bien Por qué el FBI dejó de espiar a hype y dio digamos carpetazo a la operación pero solo unas horas antes de la rueda de prensa la web de hype accesible en la Deep web dejó de operar y mostraba un mensaje del FBI que decía lo siguiente el FBI ha confiscado esta página como parte de una operación en contra ransomware Por cierto esta página no sólo Lucía el logo del FBI sino

también entre otros el de europol la policía de Alemania y holandesa y debajo se podían ver las banderas de varios países europeos incluyendo la de España lo cual nos dice que esto ha sido una operación coordinada entre muchos países europeos con el FBI a través de europol o sea que bravo por ellos me quito el sombrero según el propio comunicado de europol con esta operación de hackeo a los delincuentes han ahorrado 120 millones de euros a las víctimas a las que le pasaban las claves de descifrado que se dice pronto así que bueno hasta aquí la noticia Y como siempre os dejo muchos enlaces en las notas del episodio para que podáis ir a revisar e indagar un poco más me ha gustado mucho traeros esta noticia por lo que comentaba de lo especial de este caso tenemos a las fuerzas y cuerpos de seguridad del Estado a la ofensiva infiltrándose en los sistemas enemigos y permaneciendo como una célula durmiente mientras monitorizan nuevas Víctimas de los delincuentes y les roban los secretos para liberarlas la verdad es que toda una declaración de intenciones de lo que se viene en el futuro un futuro Parece ser en el que ya no solo Vamos a limitarnos a defendernos sino que activamente vamos a neutralizar a los ciberdelincuentes les pregunto qué opináis de esto no es una pregunta parecida a la que ya hicimos en el pasado pero que da para mucho debate que qué pros y con Alexis le ves tú a esto de que haya habido Este cambio no hacia una posición o reacción más ofensiva cómo lo ves tú para mí es muy interesante Sobre todo como haydes para ahorrar eso de 120 millones de euros a dólares a las víctimas Aunque claro dándole ponen poniéndome en el otro lado también me pregunto quién quién da quién otorga el poder a este grupo de contraataque a elegir a las víctimas obviamente hype Supongo que se ve que se les ve el plumero no a kilómetros de distancia que son malos Pero los que están ahí en una zona gris que no lo son O sí lo son o quién decide que son malos o no un poquito como lo comentábamos en el episodio anterior no lo de la noufly list que pone ahí a personas que son sospechosas de ser terroristas Cuál es el criterio que se utiliza para definir eso y para decir que son terroristas Pues también un poquito sería el problema este de que quién Define quién ayuda quién dirige al FBI para definir A quién contraatacar No sí está bien planteada la cuestión he de decir en este caso no solo hicieron el énfasis no cuando dijeron eso dijeron utilizando métodos legales hackeamos a los hackers esto de los hackers lo decía el FBI no lo digo yo no estoy intentando asociar la delincuencia ser un hacker pero claro yo creo que hacían el énfasis ese para que la gente no especularse con empezamos a soltar hay cero days que quizá lo hicieron pero pero claro no dan detalles tampoco de cómo lo hicieron Cómo estamos hablando de Thor O sea no no hablamos de hay una web y entonces yo puedo hacer un sapanima de estos al Hosting Provider y pedirle los datos de quien ha registrado esa web es que hablamos de Thor en principio tú no sabes ni Cuál es el servidor que tiene esa página web almacenada donde se está publicando los datos robados de las empresas Entonces eso por un lado y luego Bueno quiero pensar que todavía tiene que dar orden un juez para poder llevar a cabo este tipo de respuestas ofensivas y que bueno lo dictaminó un poco las leyes No si cumples tantas leyes pues se te ve como alguien muy peligroso o potencialmente claro No sé a qué nivel llega para ser terrorismo no creo que o sea habíamos hablado en el pasado de que se no recuerdo muy bien Los detalles pero hablamos en el pasado del tema de incluir a los grupos de Run software sobre todo cuando sucedió todo esto de que se jaque se paralizó la tubería de gas en Estados Unidos en en la zona este luego lo de la industria cárnica esta pues ahí sí que se hablaba ya de de ponerle la etiqueta de terrorismo al tema de la ciberdelincuencia sobre todo relacionada con ransomware entonces claro no sé no sé hasta qué punto llegará pero desde luego en el momento que lo ves como terrorismo la respuesta se vuelve mucho más agresiva y ahí tenemos un poco el ejemplo del caso de snowden no que en cuanto Cómo cambió totalmente las cosas a partir de septiembre de 2000 de 2001 cuando cuando sucedieron los ataques terroristas y empezó todo el programa de espionaje masivo de la nsa entonces dices

esto el hype lo consideró el FBI como terrorismo no no digo que lo considerase digo que recuerdo que episodios anteriores lo habíamos hablado así y simplemente hago el comentario de que un poco contestando lo que tú decías Cómo se determina no Quién es el malhechor ponía lo delist y todo esto no vaya a ser que ahora se les empiece a ir de las manos al FBI jaque todo por hackear da igual lo que hayas hecho la gravedad del asunto pero es un poco comparaba en el extremo no de los malhechores el terrorismo que ahí es donde Normalmente se le abre un poco la mano a los fuertes y cuerpos de seguridad del Estado para hacer lo que sean para detenerlo Ah okay okay O sea no no lo habían categorizado como terrorismo pero estaban más decantados a que se viera más como terrorismo que no terrorismo por eso igual a ver teniendo en cuenta que estamos hablando de paralizar hospitales escuelas robo de más de 100 millones de euros y que llevaban operando año y medio nos insisto quiero pensar hablo desde el absoluto desconocimiento lo quiero dejar claro no sé qué criterio se pone para definir algo como terrorismo no a nivel digamos a nivel legislativo no cómo está definido cuando algo es terrorismo no terrorismo doméstico terrorismo no sé no sé cuál es el criterio Pero bueno Y entonces mencionar eso que en el momento Ah no quería preguntar también si también mencionan si consiguieron recuperar el dinero robado que creo que dijiste que eran 100 millones de euros no o sea es cierto que llevaban operando desde 2021 y el FBI consiguió acceder en julio de 2022 no mencionaron nada de si habían recuperado algo de dinero pero sí que un poco la vuelta a la tortilla del concepto de evitaban que se llegase a pagar por eso era lo especial de este caso no que eso era muy interesante porque el problema de me imagino que también una de las decisiones dentro de pasar a la ofensiva Es que esto no es como robar un banco recuperas el dinero que está en bolsas ahí escondidas Es que esto es criptomoneda Aunque paralices a o consigas detener a los delincuentes si esto está en criptomonedas con javas criptográficas enterradas que ni ellos tienen ya acceso ha volado no lo puede restrear o están moneros que eso ya olvídate no lo puede recuperar e insisto hablamos de muchísimo daño económico o sea sólo en un año hicieron 100 millones de euros solo con la operación de coordinada por europol con el FBI países europeos evitaron un pago de 125 millones de euros es que es muy significativo sí sí sí sí O sea totalmente beneficio de las víctimas no van a estar muy contentas de que de que no tengan que pagar esto pero está pensando Sabes quién también va a estar muy contento de todo esto que ha hecho el FBI las ciber aseguradoras porque así no van a tener que seguir pagando no lo había pensado aunque hemos comentado recientemente que se están poniendo más duras y se están negando a dar ciber pólizas sobre todo por el impacto de tanto ransomware en plan Oye a ver ok Te doy una póliza solo si no sé tienes haces escaneos de buenavidades una vez al año o contratas a una empresa externa para que te haga un pentest y te diga lo que tienes pero si no no te voy a dar una póliza Así que ahí se están poniendo eso por un lado está bien porque puede ayudar a hacer el Push no para que las empresas se Tomen las audiovisualidad más serio y por otro lado lo entiendo hay diferentes pólizas o a lo mejor no te aseguran si tú te dedicas a deportes de riesgo en vez de ser una persona que lleva una vida normal y aburrida Por así decirlo no sí un seguro te va a querer o si tienes 80 años en vez de 20 y no eres fumador pues también te van acordar más o a lo mejor ya ni te hacen el seguro claro es lo malo de estas cosas Está buena esa la idea el ransomware afecta a empresas y las hace pagar pero luego vienen las si se quieren tomar una póliza las ciber aseguradoras le dicen que necesitan tener la seguridad en orden y esto ayuda eventualmente a que todas las empresas se suban el listón O sea que realmente el ransomware está haciendo un servicio público a la comunidad no es broma estoy estoy haciendo No una conclusión un poco se podría ver así pero estaba pensando que ostras está muy bien pensado el negocio es yo te doy un seguro pero solo si te configuras de manera que para lo que te estoy asegurando no te vaya a pasar Entonces en realidad es un win-wing en todos lados claro más

segura No le va a pasar nada y la empresa aseguradora no tiene que pagar o reduce la probabilidad de que tenga que pagar y los usuarios ganamos porque las empresas a nosotros como usuarios no nos sirve de nada que una empresa tenga una aseguradora sin la única diferencia Es que en vez de pagar unos pagan otros lo que nos sirve es cuando las aseguradoras obligan a estas empresas como condición que se que sean más seguras Entonces es cuando nos Bene con nosotros por tanto Oye pues Guay no sí sí así que bueno vamos a ver el otro tema que has comentado que me ha quedado un poco así se me ha quedado en el tintero es dices que consiguieron Supongo saber las direcciones ip de estos cibercriminales que operaban en la red Thor pero no mencionan como no Y ya creo que allá del 2017-18-19 también Hicieron Algo similar pudieron abusar de una vulnerabilidad no sé si era en los navegadores Tails o algo así de con javascript o algo que conseguían obtener la dirección IP de las víctimas No pero en este caso como tú dices no la han revelado Y entonces la pregunta está un poco Ahí deberían revelarlo o no Porque una vez que ya han quemado digamos esta vulnerabilidad que si nadie la conoce si no está parcheado en los en los sistemas que la gente usa para conectarse de forma legítima a Thor podríamos pensar o considerar que es un no entonces seguro que alguien le ha cazado las empresas de inteligencia de amenazas que están por ahí analizando la rector o incluso los mismos malhechores Aunque les hayan pillado igual puede haber alguno que se ha escapado y que tiene ese exploit ahora en sus manos pero el resto de la población no lo tiene entonces un poco que queda ir también la pregunta de En estos casos así que ya se han publicado ese sea bueno se ha hecho público todo el arresto que estaban infiltrados desde julio deberían hacerse un poquito públicos el tema de O al menos decirle a los productos afectados que arreglen esta vulnerabilidad aunque no quieran publicar el exploit en sí por parte del FBI un poquito ese era un poco Line mi inquietud Sí sí yo creo que incluso en algún episodio hemos hecho una pregunta muy similar y claro se podría plantear de otra manera incluso para que se entienda mejor Si las fuerzas y cuerpos de seguridad del Estado tienen una varita mágica para poder detectar a los ciberdelincuentes que operan en la Deep web deberían hacer pública cómo funciona esa varita mágica de manera que se puedan arreglar y que ya no funcione o no y os damos cuatro opciones no pero claro cuando lo planteas así Dices hombre casi prefiero que el fb que las fuerzas del Estado tengan una varita mágica para poder pillar a los malos pero ahora hay que acordarse de siempre lo mismo claro tener ese poder de tener una varita mágica por mucho que sean las fuerzas y cuerpos de seguridad del estado siempre existe la posibilidad de que se utilice mal ahí volvemos al caso con el FBI de Apple cuando fue el famoso caso en que el FBI quería obligar a apple a hacerles una puerta trasera para acceder a los para poder saltarse la criptografía que protege el teléfono móvil y Apple se negó precisamente utilizando este argumentación en el momento que utilizamos creamos una varita mágica por un lado ya no cuestionamos que lo vayas a utilizar bien o mal todos deseamos que lo utilices bien pero es que esa varita mágica ahora hemos la hemos creado y es cuestión de tiempo que los malos descubran Cómo utilizar esa varita mágica por tanto es mejor no crear un escenario donde exista una varita mágica que se pueda utilizar ya estamos y vamos todos a Disney con las varitas mágicas Ah no Harry Potter en el santo de las varitas pues pues ya te digo ya a ver en este caso salió muy bien el tema del FBI lo mismo con el caso de encrochat y también en el caso de aanón cuando el FBI decidió crear su propio móvil seguro para que fuera usado por delincuentes y que los dos ya os hemos contado en el episodio anterior la verdad es que por un lado entre estos ataques en crochet Ah no tiene que molar un montón currar para el FBI Sí la verdad que muy interesante Aunque Bueno también te iba a decir o es que me acordaba que en el episodio 75 en concreto también mencionábamos Algo similar pero era una empresa privada que se tomó digamos la justicia por su cuenta y abusó de una vulnerabilidad en servidores de control Dealer también que has mencionado en este caso Marx steeler para

quitarle el control a los operadores y liberar a sus víctimas y en ese caso decíamos que era una empresa privada y que estaba haciendo esto Uh qué cool no pero vemos que el FBI obviamente lo puede hacer y con mucha más legalidad que una empresa privada porque se quedó un poquito ahí el tema de Y eso lo que han hecho Es legal o no le van a caer consecuencias de esa empresa o no no sabemos pero bueno hicieron una acción digamos de Gracias una buena acción hacia la comunidad pero sí lo que tú dices trabajar en este temilla ya sea con el gobierno o en empresa privada debe de ser muy interesante tenían que hacer becas para ya que tanto problema en conseguir talento deberían hacer la policía el FBI agencias de inteligencia una especie de becas de colaboración con expertos en ciberseguridad tío a mí me encantaría ir ahí colaborar unos claro la gente tiene su propio trabajo y no no quiere renunciar a su trabajo bien pagado una empresa guapa para poder colaborar Pero deberían hacer cosas así seguro que seguro que algo aparece o a lo mejor ya existe pero te llaman ellos no existe oficialmente pero sino que te llaman sí no de hecho ahora que dices Lo de becas y tal No estoy tan metido en el tema gubernamental pero que le llamo le llamo becas como simplemente decir colaboración en plan contractor ahí échame una mano prima que viene mi novia a verme sabes y mira cómo tengo el pelo ayúdame ayúdame no pero sí lo de no podría ser incluso becas y que les enseñe a esos ciber en el trabajo no pero es que se me acordaba que incluso con tanto ransomware que ha ido saliendo han salido incluso cursos especializados para protegerte detectar y responder a ransomware yo que estoy un poquito metido en sants este grupo esta organización que tiene cursos no de ciberseguridad tienen uno ahora que han sacado específicamente para ransomware para cómo identificarlo porque es una casuística muy especial Porque combina un poquito de todo no combina que te comprometen los sistemas luego que te hacen identificación y clasificación de los datos a veces Buscando los datos sensitivos no luego que te cifran todos los datos luego que exfiltran esos datos Y luego que bueno obviamente querrían un poco evitar que se puedan rastrear no así tengo un poquito también de seguridad operacional y luego Bueno claro te dejan ahí la nota No de rescate pero sí la verdad que van saliendo temas así más especialidades de este de este concepto sobre todo el ransomware que Que supongo que igual en el futuro van a salir hasta si no las hay ya que no he mirado ofertas que sean específicas para esto como tú dices aunque sean que colaboraciones becas o trabajos full time de este tipo pues ya veremos Cómo evoluciona pues muy buena Martín y nada seguimos para adelante con la siguiente noticia y lo que traigo va de espías de la Cia Sí sí pero primero comentar lo siguiente Es que este mes ha surgido una noticia sobre una acusación delictiva contra un agente del FBI de hecho Charles mcgonigan un ex oficial de alto cargo del FBI en Nueva York que se jubiló en 2018 recibió dos acusaciones separadas una en Nueva York y otra en Washington DC tras una investigación de su propia agencia y Fiscales federales durante su trabajo en el FBI este agente supervisó algunas de las investigaciones de contra inteligencia más secretas y delicadas de la agencia como las investigaciones de oligarcas rusos incluido olec derypasta Y quién es esta persona pues enteripasca es un oligarca Ruso vamos es alguien que tiene una gran riqueza y conexiones cercanas con el estado ruso en este caso con Putin y todo el kremlin pues este señor derivasca era cliente también algo interesante de Paul mana Ford que para los que no lo conozcáis como yo que me tuve que documentar pues era una persona que durante varios meses en 2016 desempeñó el papel de presidente de la campaña de Donald Trump y en 2018 fue condenado a 47 meses en prisión por fraude financiero y otros delitos vamos que derivasca se codeaba con la crem de la crema comentar que desde el 6 de abril de 2018 la oficina de control de activos extranjeros del departamento del tesoro de Estados Unidos designó a derivasca como nacional especialmente designado en relación con las acciones del gobierno de la federación rusa con respecto a Ucrania que constituyen una amenaza extraordinaria para la seguridad nacional y la

política exterior de los Estados Unidos o así es como lo determinaron el gobierno de Estados Unidos según un comunicado oficial del departamento de justicia de Estados Unidos en 2021 macgonigan y una persona llamada sergeist que es un ex diplomático soviético que luego se convirtió en ciudadano estadounidense e intérprete ruso para tribunales y oficinas gubernamentales pues ambos conspiraron para brindar servicios a deripasca en violación de las sanciones estadounidenses impuestas aripasca en 2018 específicamente Después de sus negociaciones con un agente de derivasca mcdonigan y shaestakov acordaron e investigaron a un oligarca Ruso rival a cambio de pagos encubiertos de derivasca como parte de sus negociaciones Con el agente de derivasca mcgonigan y shaestaff y el agente intentaron ocultar la participación de dery pasca entre otros medios no nombrando directamente a esta persona en comunicaciones electrónicas utilizando empresas ficticias como contrapartes en el contrato que describía los servicios que se prestarían usando una firma falsificada en ese contrato y además usando las mismas compañías ficticias para enviar y recibir pagos de derivasca mcgonigal y shestaff sabían que sus acciones violaban las sanciones estadounidenses Pues bien Charles mcgonigan de 54 años y natural de Nueva York y ser James de 69 años de Morris Connecticut están acusados de lo siguiente un cargo de Conspiración para violar y evadir las sanciones que Estados Unidos había impuesto a deripasca un cargo por violar la ley esta ley directamente que sancionaba adripasca es decir el primer cargo es por conspirar e intentar violar y evadir estas sanciones y el segundo cargo es por directamente haberlo hecho haber violado esta ley el tercer cargo es por conspiración para cometer lavado de dinero y el otro el último cargo es por lavar el dinero así que se llevan cuatro cargos cada uno de los cuales puede llevar una sentencia máxima de 20 años de prisión Así que en el peor de los casos Se podrían llevar 80 años en prisión que la verdad sería bastante malo para ellos pero bueno como digo sabían que lo que estaban haciendo era delictivo chesta coff también está acusado además de un cargo de hacer declaraciones falsas que conlleva una sentencia máxima de 5 años de prisión esto es porque en algún momento se le preguntó sobre sus relaciones con derivaska y mcgonigan y obviamente reportó mentiras ambos fueron arrestados mcconegal la semana pasada en el aeropuerto de jfk y el señor stakov fue arrestado casi al mismo tiempo en su casa en Morris en Connecticut Bueno ahora voy a explicar un poquito la carrera profesional de mcgonegal porque es bastante interesante y de ahí surgen más temitas de nuevo el agente mcdoll sirvió en el FBI durante más de dos décadas trabajando en proyectos de contrainteligencia rusa crimen organizado Y contraespionaje tuvo un papel en la investigación sobre la interferencia rusa en las elecciones de 2016 dirigida por Robert muller tercero y pidió a los jueces que renovarán las escuchas telefónicas a Carter page un ex asesor de la campaña de Donald Trump Aunque el FBI le denegó la petición de vigilancia por no estar justificada esta gente también asumió tareas extremadamente delicadas en la comunidad de inteligencia liderando un equipo del FBI Que investigó porque varios informantes de la Cia en China principalmente pero también en otros países estaban siendo arrestados y asesinados Y esto es lo que me cazó el interés y me puse a indagar un poco a él y a leer noticias relacionadas porque no me sonaba haber leído o escuchado esto anteriormente era bastante interesante y me preguntaba cómo fue que cazaron a estos espías informantes de la Cia porque obviamente en todo esto de espía se trata de que no te cacen Así que si te cazan y además esto sucede en la empresa digamos la empresa en el organismo de espionaje más poderoso del mundo Pues algo no está funcionando ya en 2018 se remonta a la historia a esa época Yahoo se sobre estos hechos publicando una noticia con algunos de los detalles aunque no todos menos aún los detalles técnicos como digo ese año en 2018 dos reporteros de Yahoo news informaron que un sistema utilizado por la Cia para comunicarse de forma encubierta con sus activos o informantes en todo el mundo había sido comprometido por Irán y China alrededor de 2011

según los informes el compromiso provocó la muerte de más de dos docenas de fuentes en China en 2011 y 2012 y también supuestamente llevó a Irán a ejecutar algunos activos de la Cia y meter en prisión a otros debido a que la red de sitios web de comunicación encubierta fue utilizada por activos de la Cia en todo el mundo el compromiso También permitió a Irán y China rastrear actividades de espionaje fuera de sus fronteras relacionadas con otros países increíble o sea estos gobiernos no solo destapan esos esas dobles personalidades no que que son ciudadanos y también espías para la Cia sino que también pueden identificar a Estos tipos de espías en otros países ya juneus informó que los responsables de las fallas de inteligencia nunca sufrieron las consecuencias ni fueron imputados que es algo que deja mucho que desear no porque hacía por favor haberte puesto las pilas y un poquito ayudar a estos espías porque no fueron Ni uno ni dos al menos una treintena de estos espías fueron lo más interesante es que en 2008 un empleado de una empresa de ciberseguridad que estaba ofreciendo servicios a la Cia publicó abiertamente es decir tipo wizard blower como Edward snowden que estos sistemas de comunicaciones encubierta tenían fallos obviamente redactó muchos de los detalles de sus comunicados para evitar exponer a los agentes de la Cia que lo usaban Pero esto fue bastante preocupante la Cia respondió quitándole su nivel de autorización top Secret y básicamente le hundió el futuro de su carrera profesional además la Cia no prestó mayor atención a estas declaraciones o descubrimientos de este empleado de esta empresa de ciberseguridad que publicó abiertamente hasta que en 2009 empezó a ver que algunos de sus informantes en China eran asesinados bueno Y entonces con esas declaraciones del 2018 bueno hubo unos periodistas Inquietos de reuters que supuestamente han estado haciendo entrevistas a más de estos informantes que ya están fuera de prisión y de hecho en noviembre del año pasado el periodista yo el ketman de reuters publicó que un miembro de la Cia Que Fue capturado en Irán y que posteriormente cumplió siete años de prisión por estar trabajando para la Cia y que lo pillara el gobierno iraní se comunicó con los encargados de la agencia a través de una aplicación o una página web de comunicaciones ocultas en un sitio web hospedado en El dominio airanian goes.com reuters informó que el compromiso por parte de Irán de la red de sitios web de comunicaciones encubiertas puede haber llevado a la captura de este informante y muchos más y que gobiernos similares como el chino pueden haber utilizado una técnica similar para identificar a otros espías Los investigadores de citizenlab analizaron el sitio web aeranian goles.com para identificar las vulnerabilidades aprovechadas por Irán y China y para saber si Estados Unidos había estado utilizando un sistema protegido de manera irresponsable para la comunicación de activos y obviamente como ya hemos comentado de nuevo confirmaron esta vez con sus propias manos y sus propios ojos con más nivel detalle técnico que esta red de comunicación encubierta era altamente y fatalmente insegura de hecho usando un solo sitio web como digo la página que fue proporcionada a reuters por parte de uno de los informantes de la Cia entrevistados los investigadores de Cities en lab utilizaron material disponible públicamente online como hemos mencionado anteriormente en otros episodios a esto se le conoce como ausent Open source intelligence inteligencia de fuentes abiertas esto incluía resultados históricos de escaneo de internet y también el wayback Machine del internet arcaif que se encuentra en arcaif.org que es esta página web que tiene copias en distintas puntos a distintos puntos del tiempo de páginas en concreto que se pueden buscar y se pueden recuperar es como un archivo de todo Internet Pero bueno no es todo No es de muchas de las páginas más famosas de internet y a través de todo estos datos como digo de osint pudieron identificar una red de hasta 885 sitios web que la Cia usó para la comunicación encubierta con sus informantes Hay tantas porque la hacía lo que muchas veces hace es dedicar solo una página web por informante Y esto es bastante preocupante porque no beneficia a la seguridad operacional básicamente si tienes a una persona que se conecta a una

página web tendrías una alta fiabilidad para poderla asociar con esa página web en cualquier caso Los investigadores concluyeron que los sitios web incluían componentes similares entre ellos dejaba javascript Adobe Flash Sí sí Adobe Flash Claro en esa época todavía se utilizaba y otros componentes de tecnologías web que implementaban o Aparentemente cargaban aplicaciones de Comunicaciones encubiertas y con esto a lo que me refiero es que en estas páginas cuando iban los informantes había un campo de texto en el que tenían que introducir una contraseña y acto seguido se introducían la contraseña correcta aparecía un DIF una nueva digamos ventanita dentro de la página web hecho en html no la típica el no el típico popup no O sea un nuevo div una nueva Capa en la que se mostraba un campo de texto en el que se podía escribir el mensaje encubierto que querían enviar a la Cia y darle click a enviar listo así así de fácil la verdad es que hicieron las páginas tan fáciles de usar que todos los informantes y todos los agentes de la Cia se se acostumbraron mucho a utilizarlas y por esto Esto fue uno de los motivos también por los que tardaron tanto en dejar de utilizar estas páginas web porque las hicieron que eran tan user friendly digamos tan fáciles de usar que se hizo se hizo difícil desatarse de estas páginas web Bueno pues ya he dicho que muchas de estas páginas web sino todas compartían muchos indicadores digamos así similares no Además de esto se utilizaron bloques de direcciones IP secuenciales registradas a empresas estadounidenses Aparentemente ficticias para alojar algunos de estos sitios web esto olía mucho a sospecha aquí había chamusquina escondida porque elegir en direcciones IP secuenciales y además una empresa estadounidense ficticia primero de todo esto ya salta alarmas no pero luego que el tema de que se hubieran registrado las direcciones ip de forma secuencial también daba un poquito a entender que lo había hecho una única entidad así que de alguna forma estaban relacionadas ciertamente finalmente comentar que sí esto no fuera poco muchas de estas páginas web o probablemente todas obviamente no he mirado no las No las he podido conseguir todas porque como digo los detalles no no los han publicado para evitar daños mayores a los agentes informantes de la Cia Pues al menos la página que se Comenta de ejemplo a Irene goes.com y seguro que muchas otras no utilizaban cifrado ssl o tls ni tampoco redes a favor de la privacidad como motor Así que obviamente estos gobiernos opresivos pudieron identificar claramente el tráfico entre los diferentes informantes y las páginas web Y si los informantes no utilizaban vpns o similares que es más que probable que no lo hicieran porque estos informantes bueno para empezar se utilizaban estas páginas web no es que fueran muy técnicamente sabios digamos así porque usarlo con http pues ya me puedes decir tu querido oyente no que a estas alturas debe saber que eso no es no es seguro y no se debería utilizar pues probablemente no estuvieran utilizando vpns para ocultar su dirección IP por lo tanto estos gobiernos los pudieran haber identificado muy fácilmente a través de eso de obtener su dirección IP asociarla con una ubicación geográfica probablemente en su casa o incluso con su identidad y de esta forma pues arrestarlos meterlos en prisión y como he dicho en algunos casos Lamentablemente asesinarlos lo interesante es que la Cia recluta muchos espías muchos muchas personas en todo el mundo no como informantes pero como hemos visto en este ejemplo podrían educarlos a estos informantes en temas de ciberseguridad enseñarle que es una VPN enseñarles solo a utilizar https verdad Y también utilizar redes Store un poquito de seguridad operacional hubiera estado bien para evitar estos daños y estas pérdidas debidas Pero bueno todos estos puntos probablemente ayudarán a los gobiernos de Irán y China y otros países en los que se encontraban los informantes descubrir estos sitios web encubiertos los sitios web parecían estar disponibles en al menos 29 idiomas y dirigidos al menos 36 países y pretendían ofrecer páginas de fútbol como digo a Irán y and goes.com otras tenían títulos como airanian Go kicks también había otras páginas de noticias clima deportes atención médica incluso otras también con contenido de Star Wars otras páginas de músicos

como Bob Marley se ve una captura de pantalla en la noticia en la que se ve el texto Rasta directt páginas de comediantes estadounidenses como Johnny Carson el mensaje que ponía en la página web era set Meet your favorite Carson comment no Envía tu comentario favorito de Carson esto obviamente era un poco una tapadera no para hacer clic y como digo de nuevo si ponías la contraseña correcta te mostraba el campo de texto para escribir tu mensaje y enviarlo y también otros sitios web legítimos Bueno un poco para no levantar sospechas como digo no yo personalmente vosotros queridos oyentes podéis ir también a ar y Buscar esta página web que comentan en la noticia a iranian goes.com y mirar un poquito cómo estaba hecha he mirado yo personalmente el código javascript del archivo hay un archivo en concreto que se llama journal.js que es el que tiene un poquito toda la lógica de demostrar este campo de texto está esta nueva capa cuando se introduce la contraseña Y la verdad es que está bastante ofuscado así que bueno De todas formas como dicen los investigadores es fácil sacar indicadores de esta página en concreto y utilizarlos Online para identificar otras páginas similares pero así a primeras la verdad es que es como digo está bastante ofuscado y hay que dedicarle un ratillo no para de buscarlo y ver realmente lo que estaba haciendo el código no sólo incluso también mencionar que está escrito en árabe Así que el texto está en unicode y es muy difícil de interpretar para personas como nosotros no que venimos de un alfabeto latino Bueno pues estas páginas web estos sitios web que descubrieron Los investigadores estuvieron activos en varios periodos entre 2004 y 2013 de hecho en la noticia Se comentaba que se usaron desde 2009 a 2013 pero Aparentemente probablemente se hubieran estado utilizando con anterioridad en base a los resultados que obtuvieron los investigadores de citizenlab probablemente porque vieron que habían versiones guardadas en arcade.org de estas páginas web de incluso antes como digo de 2004 no no los investigadores no creen que la Cia haya utilizado recientemente o estén utilizando esta infraestructura de comunicaciones actualmente sin embargo un subconjunto de los sitios web está vinculado a personas que pueden ser empleados o activos de la comunidad de inteligencia anteriores y posiblemente todavía activos varios están actualmente en el extranjero otro abandonó china continental en el marco de tiempo de la represión china otro fue empleado posteriormente por el Departamento de estado de Estados Unidos y otro ahora trabaja para una empresa contratista de inteligencia extranjera de nuevo Cómo han conseguido obtener esta información y determinar esto sobre estos potenciales agentes y como digo no lo comentan pero yo me imagino que han podido inferir esta información y llegar a esta conclusión Pues de nuevo a información que han obtenido de registros dns de la base de datos de whois de registros del Hosting de los sitios web código fuente y comentarios de los sitios web y similares sobre la divulgación de estos hallazgos comentar que los investigadores consideran que dado que no se pueden descartar riesgos continuos y actuales para los empleados o activos de la Cia por ello por este motivo no han publicado detalles técnicos completos sobre el proceso de mapeo de la red de comunicaciones encubierta Los investigadores Solo han realizado una divulgación limitada a los organismos de supervisión de gobierno de Estados Unidos Bueno y con esto llegamos un poquito al final de la noticia no mencionar que aquellos que les atraiga la vida del espía pues mucho cuidado con las comunicaciones y si os metéis a ello casi es mejor verse en persona o utilizar los trucos de antaño de dejar un paquete en un banco en el parque no que vas te sientas miras de un lado al otro y no hay nadie lo dejas ahí te vas y luego el digamos tu contacto en la Cia te ha visto y va al banco se sienta y lo coge o el dejarlo en el típico buzón no del que luego el tu contacto en la Cia de nuevo puede meter la mano y sacarlo como típico como las pelis antiguas de estas espías no un poco más rústico un poco más métodos de estar por casa bueno Y cerrar comentando que estos sitios web como digo se siguieron utilizando hasta 2013 cuando abandonaron completamente Pues bien Me pregunto qué deben de estar

utilizando en la actualidad los informantes y espías de la Cia para comunicarse con sus superiores y si han aprendido la lección y ahora utilizan sistemas más seguros y sobre todo si la Cia está educando sobre todo como digo en temas de ciberseguridad y seguridad operacional a todos sus informantes y espías porque si no les puede pasar un caso similar al que estamos reportando en esta noticia así que por favor Cia los de la Cia si nos estáis escuchando poneos las pilas para para vuestros para poder ayudar a vuestros informantes y espías Bueno pues con esto queridos oyentes Hemos llegado al final de la noticia y con ello a la pregunta del episodio que es la siguiente crees que los oficiales de la Cia responsables de la red de sitios web de comunicaciones en deberían recibir sanciones por los asesinatos y arrestos de sus informantes os damos cuatro opciones la primera es sí prisión por unos añitos o lo que diga el juez sí multa de varios miles de dólares o lo que se decida durante el juicio no no tienen culpa la culpa fue de los informantes que no se protegieron bien y la última es no nunca por favor es la Cia el gobierno de Estados Unidos buah pues me quedo flipando con con el tema del fallo operacional de utilizar a ver también comentar Es que esto era en los años 2010-2011-2012 que es verdad que la criptografía en páginas web todavía no estaba tan importante pero si es que estamos hablando de muertes de agentes joder que mínimo que ponerle un cifrado comentabas el tema de que las páginas web Incluso aparecían archivadas en internet lo cual es normal no porque como al fin y al cabo quieres parecer una página web como cualquier otra pero se podía llegar a ver el contenido que enviaban los agentes en estos formularios o no supongo que no no porque soy iría un servidor claro creo que los comentarios eran se enviaban digamos y no se podían no eran digamos públicos o accesibles a otros miembros no era como un foro claro es un poco una pregunta tonta por mi cuenta porque puede ser que los mensajes pero O sea que los mensajes los mensajes a lo mejor se enviaban de manera también codificada en cierto sentido que transmitías la información pero a lo mejor de manera que solo los agentes de la Cia y así lo pueden entender pero no no tendría sentido claro esto es utilizada para mandar el mensaje en texto claro de Oye sé que en China van a atacar este día o lo que sea no pero la pregunta que haces también es interesante porque pudiera ser que enviarán los mensajes para que pareciera más más real un foro público no Y entonces enviaban el mensaje y en plan con este ganografía o no sé la primera letra de cada palabra es el mensaje o alguna historia no O sea y se hubiera grabado en internet era eso lo que quería decir creo no Claro claro porque tendría incluso más realismo no sé qué Y a lo mejor escribe rollo El pájaro está en el nido Pero sabes hablar de esa manera en vez de decir en vez de decir tal pero claro entender como es más fácil tener un sistema donde puedes escribir directamente lo que quieras escribir Claro pero es que esto es tan fácil O sea si ni siquiera hay cifrado entre cliente y servidor en el momento que tú conoces una web de esa Y es que no tienes ni que hackear el propio servidor O sea si tú estás en la misma red que está en la gente enviando la información la vas a poder interceptar porque no va cifrada o sea es que me parece una cagada tantos niveles por no decir de que en ese año ya existía Thor que por cierto Mira el propio Estados Unidos pues pues pues mira si deberían un poco más precavidos o haberles educado un poquito más de Cómo ser más utilizar mejor la privacidad online no pero ahora que has comentado lo de si se guardaban las páginas O sea si se guardaban los mensajes o no se me se me ocurría la pregunta también tú puedes ir y decir que borren una página del internet arcaid o no creo que puedes solicitar o sea en general tú puedes poner en el robots.txt en el archivito este que utilizan los spiders para tal lo digo sobre todo por los oyentes menos técnicos tú puedes Añadir un archivito extra tu página web donde tú das las directrices que tú quieres de cómo qué es lo que puede indexar y no los motores de búsqueda como Google y tal pues ahí Creo que hay una directiva para que tú puedes poner para que no se haga no lo archive claro esto los que lo respetan porque siempre lo pueden hacer pero bueno un arcaital de internet Esto sí lo va a hacer pero no me refiero yo

creo que también ya ya tú dices que una vez archivado es eliminarlo yo creo que sí Pero supongo que tendrás que demostrar que la página web te pertenece a ti pues claro era el otro tema ese dices el Cia por favor sois la Cia no podéis tener un poquito monitorizar temas así de Porque no solo es internet hay otros también otras plataformas que también hace un poquito de archivo no monitorizar Y si alguna de vuestras webs utilizadas para que los vuestros informantes envían mensajes se guardan ahí por favor enviar un mensaje corriendo a ese plataforma y os autenticais diciendo que sois vosotros quién son los dueños de esa página y que la borren no porque Bueno pero de todas formas cuál sería el daño porque insisto si es un formulario donde tú mandas un mensaje y ya está pero no se ve nada en el arcaif vale se va a poder lo que decías tú un poco con el fingerprint No gracias vas a poder encontrar Otras webs donde a lo mejor se mantiene la base de datos o hay copias de seguridad y entonces sí bueno por ahí sí que podría ser un peligro O sea tú lo que planteas es ahora te viene Irán y ya encontró el finger printing no esa señal de Cómo encontrar otras páginas web porque ahí también la cagaron evidentemente y se y se encuentra Hosting providers donde puede ir y obligarles a que le den la información Pues quizá tienen copias de por mucho que la hacía haya borrado las webs de esos hostings tiene todavía copas de seguridad la propia empresa y pueden ver todos esos mensajes sí ahí sí que sería una cagada es verdad sí claro se guardan como como decimos fingerpring que incluye todas las imágenes o el javascript o la forma No sé el contenido específico de alguna sección de la página Pues todo eso claro lo pueden utilizar de forma retroactiva o incluso para el futuro Oye también decir Oye si en el futuro también sale alguna más pues la pillamos rápidamente pues muy interesante Qué buena esta noticia todo lo que tenga que ver con espías Cómo se comunican Cómo funcionan y tales están tan interesante me Mola me Mola muchísimo Sí esta es de nuevo como siempre comentamos esos guionistas de Hollywood que nos estén escuchando ya pueden enviarnos algún comentario para para que le demos ideas porque esta es Otra de esas típicas noticias de espías ahí como James Bond Me conecto a esta página que sale Bob Marley y envía un comentario aquí me gusta mucho la canción No sé la canción 4 minuto 3 y no sé cuánto segundo 8 y ese es un mensaje codificado es como de película de Hollywood Sí ya ves Aunque está bien pensado lo que pasa es que a la hora de ejecución la cagaron bastante pero está bien pensado porque yo que sé si tú sospechas de que alguien es un agente de un gobierno rival y yo que sé empiezas a monitorizar su actividad en internet donde como está cifrado solo puedes ver a qué páginas va a través de dns y así de Bueno pues le molará Bob Marley y todo esto pero no puedes llegar a ver el contenido Que Manda Qué pasa que ahora que la has cagado y no pones ni cifrado Pues claro en ese caso Sí además en estos países Irán y China ahí no tienes privacidad tú solo al nacer ya te dan un papel que dice Has rechazado toda la privacidad online Así que casi usen o no ssl tls o algún tipo de cifrado va a haber alguna forma estos gobiernos de interceptar las comunicaciones así que puede ser que como tú decías antes usar antor o algún tema similar pues van a estar bastante en problemas haciendo este tipo de hazañas Pues bueno queridos oyentes ya Hemos llegado al final de un episodio más gracias gracias por estar ahí recordad compartir el podcast dejarnos Esas cinco estrellitas y así lo consideráis donde nos estéis escuchando y comentarios que ayuda un montón a que más gente lo descubra este podcast que tanto os gusta y así sigue creciendo la comunidad recordar también estar atentos a nuestro Twitter y discord@tierra de hackers porque ahí es donde vamos a poner el sorteo de esas entradas para las diferentes conferencias y códigos de descuento y todo lo que podamos conseguir conseguir para vosotros que os traiga valor Muchísimas gracias eso Muchas gracias Esperamos que disfrutéis todas las entradas que podamos proporcionar y esperamos poder seguir mucho más aparte de episodios no como mencionamos entradas pegatinas y todo lo que sea así que nada Bueno nos vemos en la próxima nos escuchamos en la próxima eso

mismo Adiós chao chao si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers