Estados Unidos detecta un globo aerostático sospechoso sobre una de sus bases militares que contiene armamento nuclear y lo atribuye a una operación de espionaje China Los criterios nos invaden vigila con las páginas en las que puedes comprar tokens No fungibles ya que pueden ser sitios fraudulentos de robo de criptomonedas ether y nfts y seguro que no quieres perder tus boards verdad planazo de San Valentín acurrucadito los dos escuchando un nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 13 de febrero de 2023 este es el episodio número 82 yo soy Martín vigo y está conmigo con upgrade pendientes después haber sido da un gran ideado a múltiples niveles Alexis porros Hola Alexis qué tal tío pues aquí estamos Martín compensando ese downgrade como dices comiéndome unos prolifteroles no joder anda que no dio cancha eso tío o sea menos mal que no lo que no lo pedimos que lo cortase el editor que tenía mis dudas pero bueno Parece ser que la gente se echó unas buenas risas porque nos llegaron bastantes comentarios con lo de proliferar tío que me cuesta pero estuve ensayando justo justo aquí Estamos ensayando las estamos enseñando las tomas falsas y nada con los profiteroles 13 de febrero nos vamos a San Valentín Ahí estamos ostras si es que todo ocurre por algo tío todo ocurre por algo y os traemos un episodio con mucho amor como siempre así que nada y que disfrutéis mucho San Valentín y como siempre lo primero es lo primero Muchísimas gracias a todos queridos oyentes por apoyarnos online en redes sociales discord y plataformas de podcast Gracias por vuestros comentarios risas sobre los profiteroles proliferar y todas esas historias Nos reímos mucho con vosotros también y hablando de plataformas de podcast os recordamos que estamos en la mayoría de ellas y si no lo estáis suscritos a nuestro podcast Pues por favor ID y suscribiros ya así recibís las notificaciones de los nuevos episodios cuando salgan sobre redes sociales estamos en Twitter infotec exchange Instagram Facebook con el hande arroba tierra de hackers linkedin YouTube y Twitch como tierra de hackers correos electrónicos nos puedes enviar a podcast arroba tierra de hackers.com y podéis acceder a nuestro servidor de discord vía tierra de hackers.com barra discord finalmente como siempre os agradecemos el apoyo a la pregunta del episodio que publicamos en Twitter y la anterior la última fue la siguiente crees que los oficiales de la Cia responsables de la red de sitios web de comunicaciones encubiertas deberían recibir sanciones por los asesinatos y arrestos de sus informantes teníamos cuatro respuestas la primera más votada con un 79% es sí prisión la segunda le sigue un no no tienen culpa con 12% tenemos En tercer lugar Si multa con un 6% y finalmente un 3% para no nunca así que vemos que la mayoría Bueno más de un 70 y esos 69% y dice que sí que vayan a prisión s69% también muy acorde a San Valentín Bueno yo pues comentar que bueno como había comentado en el episodio anterior lo de fue un poquito picante esa broma Barcelona Cyber Security Congress que estuvo súper Guay porque pues como comentaba una pena Alexis que no pudiste venir esta vez Pero Estuve presentándolo allí el hacking Village tuvimos unas charlas espectaculares la verdad hubo bastantes oyentes de tierra de hackers que vinieron a saludar lo cual como siempre os decimos nos hace una ilusión tremenda Así que muchísimas gracias No solo por venir al congreso a la conferencia sino por pasaros por el Joaquín y sobre todo pues parar y venir a saludar y ya buah un montón un montón y aparte también había por allí un Stand de estos con mucha publicidad y tal Y puso pegatinas tío y volaron a los 5 minutos todas encima de la mesa y no sí Bueno yo con con dos con dos pelotas fui allí puse aparte un poco la publicidad y puse las pegatinas si esto es por el bien común y nada ya estoy trabajando tierra de hackers va a estar ahí con comunidad Pues en este caso organizando visage Barcelona O sea que salimos de uno y montamos en otra así que bueno estoy ahí con dos compis ayudando a montar esta conferencia ya está el Cold papers abierto ya os iré dando información todavía no tenemos fecha porque estamos trabajando en el local en Sí pero vamos que es una conferencia

súper top yo creo que vamos a tener más de 300 personas ahí por eso tenemos que encontrar un sitio grande y la idea es que sea varios días con varios tracks de charlas Muy guapas y sobre todo Una vez más amigos y amigas apasionados por las ciberseguridad Ahí todos juntos disfrutando así que ya os iré comentando y lo siguiente voy un poco apurado para no alargar la intro y ya irnos a la noticia que sabemos que estáis aquí por ello el sorteo de entradas que os venimos anunciando Y empezamos en este episodio entradas para la conferencia router que se celebrará dentro de un mes en Madrid y que gracias a cripto red pues os podemos traer el sorteo que tienen un Track el jueves con charlas Muy guapas que no podéis faltar así que tenemos varias entradas para sortear y nosotros lo que queremos es sacarle valor a este concurso también No necesitamos que que no que consigáis gente que nos siga porque sí tal lo que queremos es aportar valor y entonces se nos ha ocurrido que para sortearlo lo que vamos a hacer es una pregunta en Twitter y con vuestra contestación Pues asumimos que es una participación en el sorteo y entonces pues al final de la semana en el siguiente episodio anunciaremos Quién ha ganado y haremos eso pues cada semana hasta la conferencia Y entonces lo que queremos preguntar esta semana que lo preguntaremos tanto en Twitter como en linkedin y luego pues cogeremos cada persona que haya contestado Pues asignamos un número y como un generador aleatorio pues al que le toque le tocó pues queremos que nos ayudéis a contestarnos a la pregunta que os gustaría que fuera lo siguiente que hiciéramos en tierra de hackers a mayores del podcast Y es que Alexis y yo no nos queremos quedar solo en el podcast de después de dos años y pico levantando esto estamos súper contentos con el resultado tenemos una base sólida de tierra de hackers pero no queremos que tierra de hacker se quede solo en el podcast de hecho sois muchos los que nos sugerís pues hacer entrevistas colaborar con otros entonces Queremos saber qué más os gustaría que hiciéramos para que sigáis disfrutando con el contenido que generamos puede ser cualquier cosa Alexis y yo hemos ya tenido muchas sesiones de brainstorming con con ideas pero a lo mejor a vosotros Se os ocurre alguna más o con vuestra respuesta un poco válidais pues las ideas que tenemos nosotros Así que estaríamos súper agradecidos que tanto en linkedin como en Twitter contestaseis Si veis eso decimos que no Vais a poder ir a la conferencia a Madrid Pues nos podéis poner un pequeño comentario que no queréis participar en el sorteo sino que simplemente estáis ayudando a que nosotros lleguemos Tierra hackers al siguiente nivel pero si no ya sabéis vuestra contestación es una participación en el en el sorteo para esa entrada Así que estar pendientes de Twitter y de linkedin que por allí lo publicaremos qué más hemos hablado de la ruta te he hablado de visage Pues como siempre darle las gracias a nuestros patreons que viene siendo en esta semana queremos agradecérselo a werner a Jorge generelo y a Alberto guilarte ellos tres se han unido a apoyarnos en patreon como siempre esencial para nosotros precisamente por eso estamos haciendo también esta pregunta de qué más podemos hacer porque estamos intentando dedicar más recursos a crear más contenido y hacer proyectos nuevos o el branding bajo la familia de tierra de hackers suena bien claro es una familia queridos oyentes Y como siempre También pues a nuestros sponsors mona que no falla desde desde que empezamos una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros lo hacemos a través de este podcast y posiblemente más cosillas y monata a través de una herramienta de gestión y visualización de telemetría de datos de ciberseguridad una empresa fundada en Second Valley y que está buscando a ingenieros con experiencia en ciberseguridad pero que podrán trabajar en remoto así que ya sabéis mandar vuestro currículum a tierra de hackers @monat.com que así saben que venís de nuestra cuenta y esta semana También queremos agradecer el apoyo a on branding Ya sabéis que en tierra de hackers pues no suele contactar mucha gente al igual que otros influencers sabemos de esto de ciberseguridad porque han sido Víctimas de robo de

sus cuentas en redes sociales y también casos de acoso online pues son branding es una empresa formada por especialistas en varios ámbitos que se enfocan la reputación online han ayudado desde personas como tú y como yo hasta famosos a recuperar cuentas comprometidas en redes sociales llevar a juicio casos de ciberacoso ayudar a empresas en situaciones donde la reputación estaba siendo dañada o incluso borrar la huella digital que dejamos online y no solo están apoyando el podcast sino además si le decís Oye mira que he escuchado en tierra de hackers que existís necesito ayuda pues os van a hacer un descuento así que ya sabéis un branding punto es o n br a n d i n g punto es y con esto nos vamos a la noticia a la mía en este caso del episodio si no teníamos suficiente con el conflicto entre Ucrania y Rusia creo que ya empecé varias noticias así Alexis Ahora parece que el turno es de miedo de China y Estados Unidos evidentemente no Al mismo nivel pero sí que es cierto que esta semana han incrementado las tensiones entre estos dos países con la aparición de un globo chino sobrevolando territorio estadounidense que supuestamente y según Estados Unidos su misión era el espionaje Cabe destacar que esto ha sucedido días antes de que el secretario de estado de Estados Unidos iba a ir en visita oficial a China precisamente para relajar las tensiones entre Estados Unidos y China que ya se está hablando de que va a ser la siguiente guerra que va a ser quizá la tercera guerra mundial que esperemos que en eso nunca jamás suceda pero bueno a raíz de esto de la aparición de este globo estratosférico que supuestamente para uso de espionaje se ha suspendido mientras Estados Unidos está investigando lo ocurrido por eso hago mucho inciso en lo de supuestamente las informaciones todavía se están desarrollando pero he recopilado suficientes datos como para traeros la noticia al podcast esta semana Y es que bien Parece ser que esto se aleja un poco de nuestro campo no el hacking la privacidad y la ciberseguridad pues nada más lejos de la realidad porque a pesar de que estamos hablando de un globo vamos a hablar del uso de Inteligencia artificial para dirigir estos globos de un continente a otro continente espionaje continuo en zonas concretas con cámaras Ultra nítidas ataques de denegación de servicio contra misiles nucleares y el uso de armas de pulsos electromagnéticos para dañar equipos electrónicos remotamente qué os parece Nos ponemos a ello no así que venga vamos al lío que hay mucho que cubrir además suena película de James Bond de Hollywood como siempre decimos Sí sí tal cual tal cual empezaré diciendo que si bien los globos aerostáticos con fines expiatorios que bueno Esto de expiatorio no sé si existe este palabra creo que sí no es algo novedoso esto es una de las primeras veces que ha tenido tanta cobertura de mediática eso sí y una de las razones por esta para esta cobertura mediática Es que este globo en concreto tenía capacidad de maniobra es decir el globo no volaba la deriva sin un destino concreto como cabría esperar que se comporta un globo sino que llevaba colgando material que permitía el nivel suficiente de navegación para volar con un rumbo establecido los Globos usados para espionaje ya han sido utilizados en el pasado De hecho hace apenas unos días los medios de comunicación publicaban que en la era de Trump se descubrieron dos globos chinos también usados para espionaje y por otro lado que o sea durante la presidencia de biden ahora mismo este ni siquiera es el primer globo que se que se descubre es más la empresa stratolite vende este tipo de globos a las fuerzas armadas estadounidenses lo más interesante es que esta empresa destaca porque sus globos brindan y cito textualmente aquí la alta calidad de las imágenes incluido el vídeo de movimiento completo y la capacidad de merodear en un área durante un periodo de tiempo muy largo O sea que ya veis que esto de los Globos espías a pesar de que ha saltado a todos los medios y seguro que lo habéis escuchado esta semana no es algo nuevo Pero insisto la capacidad de maniobrabilidad es algo digno de destacar y por eso también la coincidencia de las fechas de la visita o sea que es otra de las razones que iba a suceder por parte del representante del gobierno estadounidense a chino el gobierno chino hizo unas

declaraciones públicas al día siguiente acusando a la prensa africana y al gobierno también de sensacionalizar el hallazgo con fines políticos que bueno que había esperar no iba a salir chino diciendo joder nos habéis pillado china insiste que se trata de un globo dedicado a la investigación meteorológica que se desvió por accidente a territorio estadounidense esto lo que dice China pero si ahora aparte del tema de la capacidad de maniobrabilidad del globo que ellos dicen que se escapó pero joder si pues se puede maniobrar pues pues soluciónalo añadimos que esto sea que este globo se halló sobrevolando una base militar estadounidense la cosa cambia no ya no es que el globo se haya desviado sino que además se desvió justo para acabar encima de la base militar de Mall strong en Montana que o casualidad despliega 150 Silos de mis de misiles nucleares ya es coincidencia eh que el globo acabe ahí Parece ser que el globo de hecho fue enviado desde China y entró en Estados Unidos por el estado de Idaho esto muy al contrario de lo que yo Hubiera pensado que mi impresión era bueno que el que alguien un espía chino en territorio bueno o grupo de espías en territorio estadounidense lo habría lanzado desde desde dentro de Estados Unidos pues no fue así porque recordemos estamos hablando de un globo no de un avión no de un dron no de digamos un vehículo motorizado que puede seguir un rumbo concreto maniobrando porque es propulsado por un motor es que estamos hablando de un viaje intercontinental de un globo por tanto como demonios han conseguido que un globo lanzado desde un continente acaben otro continente y además en un punto tan preciso como una base militar Pues según una revista militar que estuve consultando que gracias a un amigo que me envió el link el globo en realidad la única capacidad que tiene es de ascender y de descender se utilizarían supuestamente algoritmos de Big Data algoritmos de Big Data climáticos para elegir los corrientes de aire adecuadas para que el globo se situarse en ellas elevándose o descendiendo y así ser arrastrado al destino establecido es decir mediante estos algoritmos se puede predecir que si haciendo hay una corriente que me lleva rumbo Sur si voy un poco más abajo me lleva rumbo Norte y un poquito más abajo al este pues si yo quiero ir al este pues hago descender el globo ajusto esa corriente de aire que me lleva al este y luego subo un poquito para continuar hacia el sur pues así puedes navegar Por espacio de continente a otro continente solo subiendo y bajando porque el viento hará el resto de hecho una revista militar china ilustra esto exactamente en un artículo sobre sorpresa sorpresa el uso de flotas de globos dirigidos por corrientes de aire para llevar a cabo misiones de espionaje esto os dejo el link que a la revista China de hecho va más allá el artículo de esta revista habla de que la ventaja de los Globos es que permite hacer una vigilancia duradera en el tiempo ya que los Globos podrían mantenerse flotando en la zona concreta durante meses aprovechando las corrientes del aire como expliqué previamente es decir en esta revista podemos observar como si yo por ejemplo quiero vigilar Pues yo que sé una base militar puedo hacer que el globo vaya ascendiendo y descendiendo para mantenerse en Círculo dentro de una superficie muy reducida por tanto estar sobrevolando la base militar en círculos aprovechando las corrientes de aire a las que me lleva el ascender o descender una pasada la empresa stratolite que os mencionaba antes vende globos estratosféricos a las fuerzas militares estadounidenses dice lo siguiente sobre su producto el que le venden como ejemplo hemos demostrado la capacidad de permanecer dentro de un área de 40 km el tamaño de una ciudad pequeña durante 100 horas cuatro días entonces con este tipo de capacidad se puede hacer un patrón muy detallado de monitoreo de vida monitoreo continuo del movimiento de personas el movimiento de bienes o dónde van los vehículos y cuál fue su ruta Esto es lo que dice esta empresa que le está vendiendo globos estratosféricos a los militares americanos oscito también un texto extraído del artículo de la revista china que está traducido probablemente con Google pero da información interesante y dice esto textualmente en la actualidad los aerostatos estratosféricos que utilizan la tecnología de globos de supresión

pueden lograr vuelos continuos Ultra largos de más de 300 días y vuelos completos alrededor del mundo y con algunas actuaciones y algunas actuaciones son comparables a las de los satélites en 2020 el artículo investigación sobre la navegación Autónoma de globos estratosféricos mediante el aprendizaje por refuerzo publicado en la principal revista internacional nature confirmó por primera vez que la tecnología de Inteligencia artificial puede proporcionar capacidades de control de vuelo para aerostatos estratosféricos en campos de viento para ayudar a los aeroestatos estratosféricos a maniobrar los aeroestatos controlan las rutas de vuelo o logran la residencia regional perdonar Por el tocho pero es que me pareció súper relevante Me he quedado anonadado O sea no no pudiste decir en el episodio anterior proliferar y has podido pronunciar claro estatuto y ya no sé ni qué has dicho parece un trabalenguas lo estuve practicando como hacen los cantantes de ópera antes de salir que hacen sonidos guturales ya me estaba leyendo este texto traducido del Chino tío manual yo no me vuelvo a equivocar en este podcast tío eso no baja no va a suceder tío pero sí una una locura esto tío o sea ahora los Globos Ya llevan Inteligencia artificial tío pero bueno llegados a este punto sabemos que existe la posibilidad de construir globos estratosféricos que son capaces de cruzar continentes y quedarse durante meses flotando por encima de un área indicada todo ello propulsados únicamente por las corrientes naturales del aire y la capacidad de ascender y descender perrito piloto pero la cuestión es todo esto para qué en general el uso de este tipo de globos está extendido entre la comunidad científica para estudios de investigaciones meteorológicas Pero por supuesto también puedo utilizarse para el espionaje como parece ser supuestamente de momento es el caso del globo chino volviendo a estratoline la empresa que os mencionaba ya que es de donde podemos sacar datos concretos de la capacidad de estos globos la empresa dice en su propia web que pueden proporcionar imágenes como una resolución de 5 centímetros por píxel desde los 15 kilómetros de altura pudiendo mantenerse en el aire hasta 45 días imágenes nítidas desde globos que pueden estar sobrevolando en área específica durante meses perfecto para la vigilancia pero es que además se especula que estos globos llevan una carga de dispositivos electrónicos para hacer más cosas que sacar imagen y vídeo siguiendo esta noticia de cerca esta misma mañana que estamos grabando antes de empezar a grabar leía las primeras informaciones por parte del FBI que está investigando la carga del globo después de haberlo derribado sí lo derribaron y os lo cuento Ahora en un minuto pero volviendo al tema de la carga y ya digo esto es información que aún está saliendo a la luz y a Migajas casi especulan que el globo llevaba aparatos para la recolección de Señales lo que se conoce en el ámbito militar como sigguing y que no es más que interceptar Comunicaciones esto insisto es especulación porque la información más actual es que el globo cayó al mar y aún no han podido recuperar la carga de la cual evidentemente el FBI va a hacer un análisis forense y ya sabremos exactamente qué intención real tenía china con este globo sin embargo James stottleberg rescate estas declaraciones del secretario general de la otan esta misma mañana declaró que este globo confirmaba un patrón claro del comportamiento de China y el uso de diferentes tipos y plataformas para inteligencia Y espionaje así que en principio ya están ahí y apuntando maneras qué has dicho que Estados Unidos le derribó y cayó al mar sí correcto y están ahora ahora entro en el detalle Aunque no me preguntaba porque aparte tiene los dispositivos estos como no estén en una cajita así A prueba de digamos de agua Sí de hecho lo que leía era que ese fue uno de los problemas que claro cae con toda la fuerza no tirar algo desde arriba y esto tiene que ser súper ligero para que lo lleve un globo de hecho llevaba varios paneles solares para pues tener electricidad Y tal Pero claro no van a poder recuperar todo pero bueno de momento tenemos que mantenernos en la especulación y sabremos cosas más concretas en los siguientes días pero por ejemplo la revista militar que leía para preparar esta noticia habla de cómo se podrían utilizar estos globos para

eliminar la capacidad ofensiva de Estados Unidos Esto me pareció súper guapo resulta que la base que sobrevolaba este globo como os decía contiene uno de los mecanismos de ofensa y defensa más estratégicamente importantes del país estos misiles intercontinentales son esenciales en caso de que estalle una guerra y si bien Se podría pensar que el objetivo sería destruirlos con misiles enemigos el uso de estos globos podría ser para llevar a cabo para llevar armas de pulsos electromagnéticos o espes que en vez solventar las instalaciones con misiles con otros misiles simplemente las dejarían fuera de servicio pues friando su electrónica ya yo flipo tienes instalaciones por valor de billones de dólares que albergan misiles intercontinentales y yo con un globo te dejo todo eso como si fuera la chatarrería de Manolo es que me parece espectacular hablemos de la detección no de estos globos si bien estos globos en realidad son más grandes de los que nos podemos imaginar pueden llegar por lo que leí a ser del tamaño de un campo de fútbol resulta que son difíciles de detectar por los radares lo cual es una ventaja muy grande a la hora de aplicarlos para uso militar leí que su firma térmica es decir la huella detectable en base Al Calor que desprende es mínima por el material con el que están hechos imaginaros esas armas que detectan la presencia humana mediante el calor que no que se puede ver la silueta de una persona por el contraste de temperaturas que desprende nuestro cuerpo y la temperatura ambiente Pues en eso se basa también los aviones de combate Hasta cierto punto para dirigir sus misiles otro problema es la detección por radar y es que resulta que la velocidad de desplazamiento es un factor importante en la detección por radar y los Globos se desplazan lentamente Comparado con aviones por lo que una vez más hace su detección también muy difícil mediante esta tecnología parece que los Globos son el arma o carruaje de transporte definitivo Quién lo iba a decir no pero es que tienen más ventajas como el hecho de que una vez detectado es difícil de derribar lo cual me lleva a lo que comentaba antes sí O sea si te creías que siendo un globo le pegas un petardazo y listo pues no es tan sencilla la cosa por un lado agujerear este tipo de globos no tendría el resultado que podríamos esperar que el globo explote y la carga se lleve se caiga no Estos son globos que se conocen de presión cero por lo que agujerear el globo resultarían que el globo se empezase a desinflar muy lentamente y puede llegar a tardar días en caer a tierra esto por otro lado daría margen para que el globo se dirigiese de vuelta una zona controlada para aterrizar de emergencia o simplemente en medio del mar para que acabase hundido Ok si no podemos usar una ametralladora o cañón de un avión militar pues le tiramos un cohete un misil y lo reventamos No pues tampoco es tan sencillo según la revista militar que consulte los misiles que llevan los cazas se basan en la utilización de aros de metal que ayudan a cortar partes del avión enemigo o sea cuando te metan un misilazo Pues lleva este tipo de material pues para hacer fisuras No pues estos causarían aún menos daño del que puede ocasionar un cañón volviendo al problema de que se desinflaría muy lentamente pero aún tenemos que Añadir más problemas la altura a la que vuelan estos globos resulta que estos globos pueden volar alturas enormes entre 17 y 42 kilómetros de altura para que os hagáis una idea el caza f-22 vuela a una altura máxima de 28 km así que tenemos que estos globos vuelan por encima de lo que puede volar el avión militar más avanzado del momento el armamento que llevan esos cazas es ineficaz para destruirlo y además son difíciles de detectar con el globito tío Quién lo iba a decir esta revista sugiere que la mejor manera de derribar el globo sería mediante el uso de misiles conocidos Como hit to kill que esto flipé funcionaría contra el globo de tal manera que al impactar lo arrastrase un poco haciendo que perdiese la sustentación es decir en vez de agujerearlo o reventarlo el misil lo arrastraría y tendría el mismo efecto que bueno sucedería a un paracaídas que se enrede y pierde sustentación me parece súper interesante y además es que tío preparando esta noticia aprendí un montón sobre armamento la verdad como comentan Parece ser que en parte esa es una de las razones por las que Estados Unidos tardó

tanto en decidirse a derribarlo lo difícil del tema no al final de hecho fue un caza f-22 usando un misil a&m-9x quien derribó el globo de hecho os dejo el vídeo enlazado en las notas del episodio y comentan que aprovechó el reflejo de la luz solar incidiendo sobre el globo para ayudar al piloto a engancharlo mediante detección infrarroja y bien el misil esto además sucedió a una altura de 17 kilómetros por lo que el caza tuvo que esperar a que el globo descendiese a una altitud donde efectivamente el caza podía llegar una locura tío en fin no quiero alargarme más porque creo que ya llevamos un montón y por supuesto os dejo todas las fuentes que leí para preparar esto En las notas del episodio que aparte son interesantísimas así que ir a nuestra web si queréis indagar más ahí además Vais a encontrar información de cómo se plantean usar láseres para derribar estos globos en el futuro como el pentágono está haciendo pruebas con estos globos para hacer sus propias campañas de vigilancia a través del globo thunderhead de la empresa Raven earstar y también de cómo los Globos son una mejor alternativa para el espionaje que los satélites que esto bueno brevemente mencionar que me pareció súper interesante porque uno de los debates era Bueno te vienes con todo este globo que tiene sus limitaciones pero ya hay 50.000 satélites de espionaje Qué pasa si lo pensáis queridos oyentes los satélites están en órbita Eso quiere decir que están girando a través del planeta Por tanto la ventaja del globo es que tú puedes tenerlo en una zona en concreto y que permanezca ahí como explicaba antes dando vueltas por ejemplo encima de una ciudad o de una base militar en medio del desierto eso con un satélite pues no lo puedes hacer lo cual es una ventaja muy grande con de un globo pero luego por lo que leí Existen los satélites como era decir que esos están enfocando en una zona solo efectivamente Existen los satélites geoestacionarios que como muy bien Dice Alexis están en una zona en concreta pero esos satélites están a 36.000 kilómetros de altura Entonces desde ahí es imposible tener una cámara bueno imposible no lo voy a decir que a lo mejor pues existe No pero en principio no como para poder tener la nitidez que desde un globo que está a 17 20 30 kilómetros de altura pues pueda tener Entonces es otra ventaja de los Globos Entonces esto es súper interesante otra cosa que menciona así muy rápido me pareció súper interesante esto flipé leeros la revista esta militar el tema de la invasión del espacio aéreo Tú sabías que este globo Alexis encima de una base militar americana encima de territorio americano no estaba invadiendo el espacio aéreo estadounidense yo flipé porque estaba muy más arriba de X kilómetros exactamente porque yo pensaba que el espacio aéreo pues era ilimitado hacia arriba no digamos Pero no es así resulta que le o sea tal como hay escrita la ley tiene cierto límite Y estos globos pasan por encima de eso qué pasa que digamos que hay como el acuerdo no oficial de que el espacio aéreo es todo o sea si tú vienes con un caza por encima de España pues estás invadiendo el espacio pero ya existen Quizá no aviones pero sí y ahora lo vemos con los Globos artilugios vamos a decir que pueden Volar por encima de un país desde la perspectiva digamos pero sin invadir el espacio aéreo de hecho militar mencionaba que el equivalente de Estados Unidos habiendo derribado este globo atención es lo mismo que si Estados Unidos hubiese torpedeado un buque chino en aguas internacionales es que por eso o sea Hubo mucho yo estuve viendo un poco pues el debate de la nación que justo Yo ibaiden pues lo hizo hace dos días y estaban ahí los republicanos troleando con todo esto del globo espionaje pero es que en plan Oye cómo pudo llegar esto hasta Montana porque no lo detectasteis en la en la frontera tal Pues sí que lo detectaron porque hubo justo hoy declaraciones de uno de los secretarios de inteligencia Lo que pasa que decían no podemos simplemente ponernos a derribar algo además ni siquiera estaba en nuestro espacio puede ser de un experimento meteorológico y al final claro cuando ya estaba se quedó justo el globo ahí encima de la base militar pues tal pero o sea es fascinante O sea yo flipé porque yo primero también y reaccioné así Oye pero como llega como llega un globo tío del tamaño de un estadio de fútbol que no va tan alto y se puede ver a simple vista

porque están ahí los vídeos como llega esto hasta ahí tío hasta el centro de Estados Unidos pues pues en partes Por esto una una locura tío Ahora tiene sentido esto de las películas estas típicas apocalípticas del futuro que ves ahí Torres gigantescas hasta el cielo y la gente vive ahí por encima de X kilómetros para estar al margen de la torre de Babel tío o sea ahora ya no tienes que irte agua internacionales te acuerdas que a veces hablábamos tú de montar servidores en aguas internacionales para que no haya ley y tal Pues bueno también nos podemos poner a construir para arriba y yo que sé no la planta 8 millones pues ya por ahí estás ya en territorio internacional pero a mí me fascina un poco el tamaño dices que este globo es tan grande como un campo de fútbol si en concreto el chino lo definían como tres autobuses pero los globos de starlight eran del tamaño de un bueno como es una empresa americana poner un tamaño de campo de fútbol americano Pero bueno que sí sí sí un locurón de enormes Wow Sí pues sí que son grandes muy interesante el otro tema que te iba a decir es pero es un globo que está todo esférico o está todo cuadrático estrato triángulo tío O sea me has dejado por un momento volado tíos ostras pues esto no me lo voy a preparado tío no te lo has leído eh Es que yo me he leído cuatro libros de No no es broma te quería decir La broma aquí pero no también el tema que que interesante que la noticia ha empezado con los chinos y le has dado la vuelta a la tortilla hacia Claro que están aquí incluso igual tienen mejor tecnología que lo de los chinos para espiarnos a todos claro tío Es que a mí una cosa que me sorprendió yo cuando lo vi sabes nosotros tanto Alexis como yo cuando vemos noticias de estas que se salen un poco de la norma no del ransomware del hacking del Zero day Pues nos hace mucha ilusión porque sabemos que os resulta muy interesante y nos ponemos manos a la y yo pensaba que esto era algo nuevo pero claro en cuanto me puse a mirar No ya habían detectado otros se utilizan en ciencia investigaciones y además pues tenemos empresas que literalmente están vendiendo estos globos a las fuerzas armadas estadounidenses y claro eso hay que destacarlo va que ahora ya no sirve ni el casco este de papel de plata nos ven en todo momento es que tú imagínate un rey ahí en estos globos tío para interceptar las comunicaciones le metes la y nos hacemos tú y yo lo que pasa es que yo no tengo pulmón no tengo pulmón para echar para echar un globo de este tamaño tío pero hablando de eso hubo creo que ya está muerto un proyecto de Google que era Luna x o algo así que eran globos proporcionar interconexión a internet a través de globos por todo el mundo y de hecho de hecho Facebook Facebook también tenía internet.org justo que era para para dar efectivamente Qué bueno que saques eso porque es verdad Facebook tenía esto que creo que murió el proyecto que era precisamente ofrecer internet mediante relés o sea digamos repetidores de señal que estaban puestos en globos que sobrevolaban zonas incluso creo que lo querían hacer también como con aviones de estos mega ultraligeros de no sé qué pero sí quedó un poco en nada ahora están más al metaverso alguien Mira los chinos alguna empresa estadounidense va a decir no voy a proporcionar internet con estos globos y además sin decírselo a nadie pongo estos esta tecnología espía así Mira dos pájaros por uno Oye a ver y luego Es verdad que siempre no de del ámbito siempre no pero muchas veces del ámbito militar pues vienen innovaciones que luego repercuten positivamente en la población no y Oye si si se desarrolla la tecnología de globos que con energía solar se pueden meter a flote tal Y de repente le puedes dar internet a lugares remotos Pues mira qué guapo sin tener que tirar cable ni tener una conexión satelital un caso de eso ese proyecto militar fue dar panet que es el internet todos hablando de esto seguro que elon musk va a sacar un globo para ir a Marte para que no tienen prisa en plan coges el Express El el cómo se llama el túnel este el no me acuerdo que se llama el túnel suyo el hyperloop te coges el globito No mira el hyperloop lo utilizan en vacío para lanzarte en plan cañón como el hambre avala te tira con el globo suficiente arriba como para subir a la estratosfera y ya de allí pues ya circo que te suben y te coge el que está agacha enganchado en

el globo te da la mano venga Que bueno que ahí entra luego el concepto de que es para arriba en el universo porque eso de para arriba es muy relativo o sea puedes estar subiendo para abajo claro yo ya yo de hecho para entenderlo de los Globos yo me lo pensaba al revés que no estaban arriba estaban abajo que todo el cielo era el mar y nosotros estamos arriba No lo que pasa es que la tierra es plana tío Porque si no esto no tiene sentido Claro está torcida spoiler Es una broma no vaya a ser que no llega un comentario de que estamos aquí difundiendo fake news Por cierto había yo escuché o leí Aunque hubo dos globos uno el de Estados Unidos así recientemente y el otro se fue para latinoamérica no no sé si lo viste eso Ah también gracias gracias Es que a veces como más o menos tengo ya después de 82 episodios aquí cuando escribo todas mis notas más o menos a Ojo Ya sé Uy ya debo de estar en los 20 minutos de hablar y entonces paro no Entonces no me quiero pasar pero es que hay muchísima información y por eso también ponemos tanto énfasis no solo en por supuesto dar crédito a la gente que escribe todos estos artículos sino también pues daros a vosotros para que indaguéis más si queréis y el Mi último comentario es que leí en Twitter que este globo que entró a Estados Unidos como dijiste por el oeste por el estado de Idaho Se saltó el gran cortafuegos del Oeste no sé si sabes cuál es es la aguja espacial o el nidel space ni del Tower de Seattle que es una torre que tiene un pincho arriba Entonces es verdad que yo me subí allí ostras o sea ostras O sea que ahora es verdad los pararrayos pueden tener una segunda vida útil que es pinchar globos espía tío justo Qué buena esa es buena Pues ese es el Salto Pues nada muy buena noticia Martín que nos estamos alargando un poquito pero es muy buena noticia pasamos a la siguiente Dale dale y lo que traigo Es una noticia de robo de criptomonedas y normalmente hemos traído noticias de este tipo pero que afectaban a grandes plataformas a grandes empresas de que hacen intercambio de criptomonedas o esos gateways o puentes entre blockchain pero en este caso me ha parecido importante traer esta noticia porque nos afecta a todos a los usuarios de criptomonedas en algún momento en algún episodio igual hemos comentado el tema de que ha habido cibercriminales que han robado criptomonedas a otros usuarios de sus carteras de criptomonedas a través de por ejemplo cambiarle la dirección de la cartera de criptomonedas por ejemplo que se publicaba en páginas web de proyectos de criptomonedas que no se están lanzando el inicial Coin offering este que hace No es que cuando quieren ser más públicos y captar más fondos pues lo que hacen es Oye quien quiera apuntarse el proyecto pronto pues voy a dar unos cuantos tokens un poco más baratos que con la idea que en futuro se van a revalorizar no y alguna vez pues ha habido cibercriminales que cambiaban esta dirección del proyecto la legítima por una suya falsa y así han robado No pero en este caso es un poco más diferente y es más enfocado a los usuarios de a pie digamos Así que usamos mi internet y sobre todo afecta a nivel de navegador No qué ha pasado entonces pues los investigadores de recorder Future que es una empresa que bueno publica noticias análisis investigación y también recaba mucha información de internet y la publica también en servicios de pago como servicios de inteligencia de amenazas pues ha estado analizando un poco lo que ha estado sucediendo y ha publicado recientemente un análisis en el que concluyen que los cripto trainers están muy de moda y los están utilizando los cibercriminales como digo para robar criptomonedas de víctimas online y que es esto de cripto trainers no hay una forma muy fácil de traducirla pero se podría decir que son como drenadores de criptomonedas o una una más graciosa son escurridores de criptomonedas me imagino estos que en los años 50-60 por ahí que iban a las minas así a sacar un poco de piedra y oro y que salga la Pepita no de oro chupópteros de criptomonedas digo los absorben ahí los esas me gusta es buena también chupóptero ese es un buen logo Se podría poner ahí sí como con el oso hormiguero este tío que así que parece más chupóptero Claro claro los vampiros de las criptomonedas bueno buena idea pues estos Estos cripto trainers son scripts maliciosos

basados en javascript que funcionan digamoslo de manera similar a los skimmers que son los hemos comentado en el pasado en algún episodio de tierra de hackers son esos dispositivos que se montan encima de los lectores de cajeros automáticos y sirven para leer las tarjetas de crédito la información que tienen las diferentes pistas y luego utilizar estos datos de la tarjeta robados para realizar operaciones fraudulentas como hacer compras online bueno de forma física si se puede clonar en una tarjeta que no tiene chip sin autorización o transferencias a la cuenta del atacante y temas similares no estos cripto trainers se despliegan principalmente mediante fishing para robar las criptomonedas de las víctimas en las páginas de fishing suelen imitar a servicios de criptomonedas populares como páginas de intercambio de criptomonedas o plataformas de tokens no fungibles lo están famosos nfts y también utilizan aplicaciones y extensiones comunes de terceros que los usuarios de criptomonedas están acostumbrados a usar como metamask que es una extensión de navegador web que como digo no son inusuales no son ajenas a los usuarios de día a día de las criptomonedas vamos que los cibercriminales no son tontos y obviamente lo que hacen es imitar páginas que los usuarios de criptomonedas están acostumbrados a visitar para que la víctima pues entre en un entorno que al que está acostumbrado de confianza baje las defensas no se percate del engaño y zasca haga clic y Bye bye criptomonedas Los investigadores descubrieron una página de fishing ya lista preparada para ser desplegada en cualquier sistema de Hosting de sitios web que la estaba ofreciendo un cibercriminal en uno de los foros más importantes de la esta página de fishing pretendía acuñar tokens no fungibles los nfts y utiliza servicios de terceros que se usan comúnmente en este tipo de páginas de nft las páginas de fishing para desplegar estos cripto drenadores se empezaron a utilizar el año pasado hay digamos en marzo mayo y no han hecho más que ganar popularidad desde entonces así que queridos oyentes si tenéis criptomonedas y tratáis con ellas Online para comprar nft o hacer transacciones A través de la web tener cuidado y prestar atención a lo que sigue porque una vez que las carteras de criptomonedas se ven comprometidas No hay forma de evitar el robo de las criptomonedas y recuperarlas el 14 de septiembre del año pasado un ciber criminal publicó un mensaje en ruso como digo en uno de los foros más importantes de la Dark web y adjuntó un archivo comprimido un archivo zip que incluía una plantilla para una página de fishing y un cripto drenador estaba diseñado para desviar ether es la criptomoneda nativa de la plataforma ethereum del blockchain y también para robar nfts basados en ethereum de las carteras de las víctimas a las que atacaba y para enviarlas a la cartera de del atacante como todos sabemos ether Es una criptomoneda muy común probablemente la segunda más famosa y así que intentan enfocarse en ella haciendo esto pues le da a los cibercriminales altas probabilidades de éxito Porque muchos usuarios tienen ether el cripto drenador ofrecido por el cibercriminal debe implementarse junto con componentes legítimos como decía la extensión de metamask es presencial que esté instalada en el navegador de la víctima y también se utiliza un servicio una Api de una plataforma que se llama Morales que lo que ofrece es como digo una Api para interactuar con la blockchain de tyrion y con los nfts el orden de operaciones o como iría la estafa sería el siguiente el primer paso es que el ciberdelincuente Configura y despliega su página de fishing como digo en un servidor de Hosting web que atrae a su víctima de alguna forma para que conecte su cartera de criptomonedas esto puede ser mensajes vía pues plataformas de mensajería online email SMS lo que sea no en segundo lugar el código javascript malicioso del cripto drenador abusa de la nueva conexión que se ha establecido cuando se va a la página el usuario tiene que conectar su cartera a través de la extensión de metamask y una vez ha establecido esta conexión el archivo de javascript malicioso de este cripto drenador lo que hace es a través de la conexión de la cartera de metamask crea y aprueba una transacción en nombre de la víctima esta transacción lo que hace es obviamente enviar todos los fondos ethereum ether que tiene la víctima en su

cartera a la cartera del atacante el criptor también Busca nfts específicos en base a una lista predefinida por el cibercriminal en el archivo de configuración que no son más que digamos direcciones de la blockchain ethereum y los transfiere a la cartera del atacante Así que como digo no sólo se lleva ether sino que también se lleva los nfts que hemos visto que algunos de estos nfts se han vendido en el pasado por millones de dólares en el mismo mensaje en el Foro de la Dark web el cibercriminal declaró que ya había usado su cripto entrenador para robar al menos 95 mil dólares entre criptomonedas y nfts el criptoador en concreto es un archivo javascript llamado morales.min.js Aunque Bueno Este es el ejemplo del post este de este foro de la Dark web Podría tener cualquier otro nombre pero en este caso Este era el nombre que tenía y como digo es un cliente que utiliza la Api de morales y se sirve con los otros recursos en la propia página web cuando la víctima la visita antes de desplegar la página de fishing el cibercriminal debe registrar una cuenta con Morales esto se puede hacer usando una dirección de correo electrónico temporal que es lo que probablemente utilicen Aunque bueno en otros episodios anteriores Y ya hemos comentado como a veces cometen fallos de seguridad operacional de estas obsek e incluso pueden haber utilizado su propia cuenta de correo electrónico personal y ahí se les puede cazar Pero bueno en este caso es como lo hacen con una cuenta de correo electrónico Temporal y después del registro de amenazas del cibercriminal debe crear una nueva aplicación descentralizada que se denomina de App o de Central eyes app a través de esta plataforma Morales usando la configuración específica que se menciona en el post del foro el cibercriminal proporcionó como digo dos archivos uno es la página de fishing con el html y todo lo relacionado y el otro archivo es uno de configuración que se puede modificar para que incluya ciertas imágenes y enlaces de redes sociales según el tipo de servicio de criptomonedas que el cibercriminal quiere imitar pues para hacerlo que se parezca más a la página original que se quiere suplantar lo siguiente es configurar la página de fishing para que conecte con Morales es decir se le tiene que proporcionar la clave de la Api de Morales para lo que el cibercriminal como he dicho primero tiene que tener una cuenta en morales y luego tiene que ir a Morales a obtener esta Api luego el cibercriminal tiene también que especificar cómo se llevará a cabo su ataque y para esto lo que tiene que poner especificar es su cartera de ethereum donde el cibercriminal quiere recibir las criptomonedas y también la lista de las direcciones de los nfts que se quieren robar Hay muchas formas de atraer a víctimas a que caigan en un esquema de fishing pero el pretexto es sugerido por el cibercriminal es el de una página que Acuña nfts y esto bueno es porque están tan de moda que todo el mundo está loco a veces por comprarse el último nft no sólo por comprarlo y tenerlo sino por revender lo que es donde creo que la gente piensa que se puede ganar y hacer valor el concepto este de acuñación significa asegurar o asociar el activo digital con contigo mismo es decir enviar una petición a la diciendo Oye blockchain de yo usuario Alexis con este identificador de mi cartera estoy creando un archivo digital x que puede ser una imagen un vídeo un texto o cualquier tipo de contenido mientras sea en formato digital y que puedes encontrar en esta URL Esto no es gratis y generalmente requiere que los usuarios paguen tarifas de transacción de criptomonedas que se llama tarifas de gas no es como una comisión para que alguien en el blockchain te valide esa transacción es como un notario vamos vas a un notario para decirte Oye esta casa la he comprado es mía notario confirma que es mía y el notario Te cobra una vez que la víctima está navegando por la página de fishing del cripto drenador algo muy inteligente que hacen los cibercriminales es mostrarle mensajes emergentes de forma periódica que afirman que otras carteras otros usuarios están acuñando nfts actualmente en la misma página Esto está muy bien pensado y es la presión psicológica para intentar inducir a la víctima a conectar su cartera en la extensión de metamask para acuñar los nfts y de esta forma Obviamente el cibercriminal robarlos Mientras tanto el Script del cripto drenador verifica si la

extensión metamask está instalada o no en el navegador web de la víctima si la extensión metamask no está instalada la página de fishing le pide a la víctima que la instale la instrucciones de cómo hacerlo así que una vez que se ha instalado metamask la página de fishing le pide a la víctima que conecte su cartera en sirium para comenzar a acuñar los nfts si la víctima está de acuerdo el Script del cripto drenador abusa de la Api de Morales para interceptar la dirección de la cartera de la víctima esto a su vez permite que el criptoador cree y firme una nueva transacción en nombre de la víctima de esta forma se hace la transacción para enviar el acer de la cartera de la víctima al ciberdelincuente y esto antes bueno el ciber criminal lo que ha hecho también ha añadido lógica para verificar que se ha realizado de forma correcta y si no pues bueno intentarlo de alguna forma También aparte de eso o sea el primer motivo el primer objetivo es robar los éter No pero en segundo lugar como digo busca de la lista de nfts a ver si tiene alguno de ellos asociado a su cartera finalmente si no hay ningún acer o nft en la cartera de la víctima se le muestra un mensaje de error que está diseñado para evitar cualquier sospecha que pueda tener la víctima reduciendo así la probabilidad de que desconecte su cartera de la página de fishing por si en el futuro en algún momento vuelve a visitar la página y de esta forma no tiene que pedirle que se añada la cartera esta página de phishing normalmente Esto es algo interesante los cibercriminales ofrecen servicios a otros cibercriminales no gratis sino a cambio de algún tipo de comisión no pago en este caso sorprendentemente el cibercriminal que publicó esta plantilla de fishing de drenaje de criptomonedas era muy altruista digámoslo así y no cobró nada a otro cibercriminales por usar su herramienta como era de esperar había trampa y no te puedes fiar de un cibercriminal el cripto entrenador fue diseñado para defraudar incluso a otros ciberdelincuentes y llevarse una parte de sus ganancias de forma ilícita las ganancias eran ilícitas y aquí están robando el ladrón está robando a otro ladrón básicamente Esto fue unas tres semanas después de que la plantilla de la página de fishing y el kriptón drenador fueran publicadas en este foro de la Dark web el 6 de octubre del año pasado otro cibercriminal envió un mensaje advirtiendo en el mismo hilo de este foro de la Dark web que esa plantilla de drenaje de criptomonedas estaba preparada para en Casos específicos enviar criptomonedas robadas a una cartera propiedad del cibercriminal original Los investigadores como he dicho anteriormente en este caso en esta plantilla el cibercriminal había añadido esta puerta trasera digámoslo así así que había incluido su cartera de criptomonedas y gracias a eso Los investigadores pudieron confirmar que este esta página de fishing y este cripto trainer se está utilizando activamente para robar criptomonedas gracias a no pudieron tracear esta cartera de ezer que probablemente pertenece al cibercriminal la dirección de la cartera de sirion se transmite en este caso a través de una conexión de websocket Que bueno que incluía la dirección como digo de este cibercriminal Y utilizando herramientas que como Chain análisis y plataformas de trazabilidad de investigación de transferencias y operaciones en blockchains Pues los investigadores concluyeron que a día 11 de enero de este año y después de un período de observación de 10 días la cartera de éter del cibercriminal original recibió 0,8 ethers Así que esto es un valor aproximado de unos 1000 y algo mil dólares es muy probable es muy probable que este acer se haya obtenido a través de esta puerta trasera que se que el otro cibercriminal advirtió en de hilo Así que sugiere que hay otros cibercriminales que probablemente estén usando esta plantilla para robar cripto monedas y nfts a víctimas que no se dan cuenta de este fraude durante la investigación también se identificaron otras nueve páginas de fishing que habían implementado esta plantilla de drenaje de criptomonedas y direcciones de cartera decirum pertenecientes a los atacantes que las configuraron porque como digo la dirección a donde se envían se roban el ether está jarcodeada en este archivo javascript que se sirve cuando se visita la página de fishing y que conecta con esta plataforma llamada Morales algo que concluyeron

también los investigadores es que las carteras de cierre identificadas mostraban ráfagas de actividad durante un corto periodo de tiempo que es típicamente Cómo funcionan los cibercriminales despliegan la página de fishing defraudan a unas pocas víctimas y luego la cierran y crean otra nueva para despistar lavar un poquito la mala imagen y bueno hacer más difícil el trabajo de los analistas de seguridad de todas formas en el campo de las criptomonedas es muy difícil no dejar rastro Y más si se usa acer como la moneda objetivo y esto ya lo hemos comentado más de una vez en el en el podcast en episodios anteriores Los investigadores estuvieron analizando las direcciones de cartera de sirium y vieron otros analistas de seguridad de blockchain que ya estaban al tanto de este fraude y las habían marcado como asociadas con esta estafa de fishing además de esto también se identificaron 92 dominios de páginas de fishing adicionales de drenaje de criptomonedas que no estaban relacionadas directamente con esta plantilla específica pero sí con el concepto de cripto training Así que como vemos este esta nueva digamos técnica de robar criptomonedas se inició el año pasado digamoslo por marzo mayo en septiembre hubo un post que se compartía en este foro de la Dark web y no es la única plantilla se han utilizado otras otras técnicas diferentes a la que identificaron los investigadores Y esto no no se lo inventan no lo dicen solo por lo que pueden analizar de la cartera de sirium de los cibercriminales sino que también se puede buscar online proyectos relacionados con esto y es que por ejemplo en la Dark web Los investigadores se han registrado hasta 1060 menciones de criptobrainer o nft en marzo de 2022 se creó un canal de Telegram centrado en estos cripto drenadores que ya tiene más de 15.000 usuarios suscritos y también tiene mensajes vistos por más de mil usuarios la captura de pantalla que se incluye en el informe PDF que vamos a Añadir a las notas del episodio muestra un mensaje que dice ethereum más nft guión mintrer es en plan una plataforma un Script para robar y acuñar nfcsyrium ether de forma ilegal y sale la imagen también de un Board ave nft eso es de los primeros nfts tan famosos que salían con unos monos gracias a su amplio desarrollo y facilidad de uso es probable que estos criptoradores sigan creciendo en popularidad y de hecho si se busca por ejemplo la palabra criptobrainer en github se pueden obtener al menos tres repositorios públicos y luego lo interesante es que hay un topic también que se llama cripto trainer que contiene 17 este repositorios de proyectos que contienen la palabra cripto dreamer tres de los cuales son públicos y 14 son privados todos potencialmente maliciosos Esto me pareció interesante el hecho al menos yo no sabía no me he dado cuenta de que se puede saber si hay repositorios privados en github que contienen esa palabra en el nombre yo no sabía que se puede obtener esta información de github ya que si al fin y al cabo son privados pues esto me parece un caso de exfiltración de información de repositorios privados con una búsqueda inguita en cualquier caso también si se busca por cripto-ner se pueden obtener más todavía 45 plazas repositorios y topics o temas no que combinan las palabras cripto trainer nft ether y wallet Así que podéis hacer una combinatoria de esos y Buscar muchos más repositorios en github habría que verificar uno a uno cuál está realmente relacionado con cripto trainers porque el ejemplo de los investigadores me pareció un poco exagerado utilizaban solo la palabra drainers en github y claro salían por ejemplo salían 16 millones de cómics para proyectos de este tipo pero luego si te los pones a mirar muchos de estos driners se refieren a proyectos de gestión de batería de portátiles gestión de batería de coche entonces me pareció el informe está muy bien excepto esa captura de pantalla que me pareció un poco hype por decirlo de alguna forma lo curioso Es que muchos de estos repositorios que he verificado que son Realmente maliciosos bueno no me he puesto analizar el código Pero al menos lo que pone ahí es ven usa este proyecto para robar ether Eso me parece más que prueba suficiente para decir que es un proyecto malicioso pues fueron actualizados en las últimas semanas así que estos Esta técnica de estos proyectos se están

utilizando a día de hoy y Bueno aquí volvemos al tema es la polémica esa no de si github tiene que borrarlos o no en algún caso he ido a visitar alguna página que ponía Este es el proyecto digamos de demo Si quieres el proyecto profesional tienes que comprarlo en esta otra página y te daba una URL Y si haces clic esa URL te lleva a otra página pero te aparece una pantalla que te dice en este proyecto esta página se ha cerrado porque el dueño de esta página el usuario incumplía los términos de servicio así que bueno Total que hay mucho repositorios de cripto drones en github y junto con los 101 dominios de fishing y las carteras de atacantes que han identificado Los investigadores Pues todo esto sugiere que los criptodrotrenadores ya están teniendo un uso generalizado entre cibercriminales y un poquito llego al tema de las mitigaciones o como protegerte querido oyente querido usuario lo primero un poquito es prestar atención a realizar transacciones de criptomonedas online ya sabéis que una vez que las dejan tu cartera ya no se pueden recuperar son como no son como los bancos lo segundo es utilizar carteras de criptomonedas Hardware estas carteras pueden mejorar la seguridad de las transacciones de criptomonedas y las comparamos con las carteras activas o software como metamask que siempre están conectadas a internet a tu navegador para monederos Hardware que están conectados a metamask todas las transacciones deben aprobarse a través del mismo lo que proporciona una capa de seguridad adicional O al menos esos segundos de retraso que le da la victima cierto tiempo de recapacitar y darse cuenta del fraude y pensar realmente esto es legítimo o no también hay que mencionar que han habido buena habilidades en este tipo de carteras Hardware así que bueno no hay nada 100% seguro pero bueno al menos es otra capa adicional de seguridad solo usar aplicaciones distribuidas de la blockchain confiables y verificar las direcciones de los contratos inteligentes para confirmar su autenticidad e integridad Como he mencionado anteriormente se pueden utilizar estas plataformas de análisis de blockchain y en algunos casos las direcciones están tagueadas se les pone una marca un comentario diciendo Oye están relacionadas con phishing o similares también verificar las direcciones web de sitios oficiales y compararlas con las direcciones de la página actual que estás visitando para evitar estos casos de fishing Esto no es específico justo al tema de criptoines pero es un poco tema genérico en a nivel de fishing también tener en cuenta que muchas veces hacen cambios imperceptibles del dominio como una y por un uno o también Usan el alfabeto cirílico que tiene letras muy similares a las del latino también cuestionar las ofertas que son demasiado buenas para ser verdad Como he mencionado antes acuñar un nft no es gratis tú cuando compras el nft primero tienes el precio del nft en sí Y además el precio de la transacción en sí es como una un pago adicional que se tiene que pagar volviendo al caso del notario cuando tú vas a decir quieres validar que algo es tuyo pues aparte de haber comprado lo que quieres validar que es tuyo una casa pues tienes que pagarle esa tarifa no del notario Pues en este caso también están estas tarifas y a veces pues son elevadas bueno considerando el precio del nft en Sí pues estas páginas de fishing lo que hacen es no no el estafi o no te la cobro o esta tarifa te la pongo muy baja es también hay que pensar un poco que si es demasiado bueno para ser verdad Bueno indagar un poquito más puede ser que sea verdad no pero un poco sospechar de eso y resistir esas tácticas presión no que utilizan como en este caso que mencionado que te sale el popup esté diciendo hoy tres personas acaban de comprar un nft y después de 5 segundos en el futuro te sale otro mensaje diciéndote que otras 10 personas han comprado otro nft pues eso causa un poco sensación de presión psicológica que como lo dicen el missing out No pues fear of missing out ese que esa palabra que se utiliza mucho en el mundillo de criptomonedas también tener cuidado con eso así que bueno una nueva técnica digamos de robo de criptomonedas estos cripto dreamers que queríamos traer al podcast y hacer a todos vosotros queridos oyentes conscientes del riesgo Bueno siempre está bien Aquí dando no todo va a ser globos y que no afecta a la gente me Mola ese que yo por un lado una noticia de estas

de espionaje que sí Bueno podría afectar a la gente pero más a nivel global la tuya más desde ostra cuidado que te vas a la página equivo y te quitan las criptomonedas que muchísima gente tiene O sea que esto está súper Guay para mantenerla la gente al día hemos tenido conversaciones en el pasado de noticias de una que habías dado tú que había sido muy útil para uno de nuestros oyentes para ir a verificarlo con clientes suyos y que comentaba que ostras pues varios estaban afectados O sea que siempre muy bueno este tipo de noticias yo lo que destacar es el tema de la automatización como siempre que no es alguien que me va a robar no sé qué tiene que hacer esto aquello no página phishing automatizado el tema de quitarte las criptomonedas todo pasa en un please no tienes margen de reacción y han volado y como dices tú esto no no vas al banco a reclamar que te vuelva la pasta Ese es el tema Sí es que cuando cuando asocias ya tu cartera vía la extensión esta meta más ya ya es Game Over básicamente en tema que no sé no sé cuánto debe tardar no lo he probado obviamente pero debe ser segundos o menos de que se haga la transacción y se fue todo todo lo que se marchó justo y no sé si estos temas de estaba pensando ahora que decías eso cómo hacerlo un poco más fácil para el cibercriminal Añadir semillas de esos de poner una capa encima no de click jacking de cubrirlo con cubrir el botón específico de conectar Bueno tu cartera con la página web en sí Pero supongo que al fin al cabo te va a saltar el popup este de metamask que eso está es parte del navegador Así que no es parte de la página web así que no se podría cubrir directamente con html o css o javascript o te van similares Aunque si no me equivoco creo que en el pasado ha habido alguna vulnerabilidad relacionada con metamask pero No sabría No sabría comentar porque no me acuerdo exactamente Eh Pues sí como te decía tío esta este tipo de de noticias son súper necesarias porque Esperamos que le da valor a los oyentes porque se dan cuenta que esto está al orden del día como dices tú me gustó mucho ese dato de los últimos cómics en github a este tipo de proyectos por así por así llamarlo al orden del día todo el mundo quiere robar dinero automatizas esto y luego es el que caiga ya está automatizado Supongo que esta gente se levantará toda la mañana es como yo bueno Esto va a sonar Así un poco como yo mirando las acciones que tampoco es que tenga yo mucho No pero de esto que miras ahí Oye te lo que pasa es que esta gente mirará a ver a ver mi cripto wallet cuando Cuánto ha crecido hoy no cuántos pardillos han caído en esto y a ver cuándo van Cuánto dinero gana hoy sí como dices en la bolsa unos ganan otros pierden pero sí Supongo que esta gente se levanta por la mañana con la alegría de ver ahí que su que su balance ha subido que la Gráfica la tienen en verde y sube hacia con una montaña rusa sin fin no sí tal cual tío tal cual bueno se nos ha hecho largo el episodio pero convencido de que se ha hecho muy interesante recordar sorteamos Esa primera entrada esta semana ir a nuestro Twitter a nuestro link y nos comentáis allí la pregunta recordar es que queréis que hagamos a mayores del podcast queremos que la marca de Tierra de jaque es que el producto de tierras no solo sea el podcast sino más seguir creando contenido info productos básicamente lo que vosotros queréis para dar todavía más valor agradecer vuestro apoyo que lo compartáis con amigos como siempre por favor esa reviews esos comentarios en las plataformas donde nos estáis escuchando nos ayuda muchísimo porque eso es lo que tiene en cuenta el algoritmo para darnos más visibilidad y más visibilidad ya sabéis que quiere decir más gente que nos escucha que al fin al cabo el esfuerzo es el mismo para que nos escuche o uno o nos escuchen 50.000 personas por tanto muy muy agradecidos y podéis seguir compartiendo el podcast comentando y dejando reviews que nos ayuda un montón Sí muchas gracias a todos como dice Martín vuestras sugerencias son muy bien recibidas no solo para hacer como dice Martín temas nuevos sino para igual Oye igual más es menos igual tenemos que eliminar algo que no resuena bien con la audiencia así que me hacéis llegar nosotros escuchamos y luego pues intentamos hacer más felices mira esa puede ser la pregunta para la semana después para la

siguiente entrada que es lo que no os gusta os gustaría que cambiáramos Pero bueno eso para semana siguiente de momento qué es lo que os gustaría que fuese lo siguiente que hiciéramos Así que nos vemos y nos escuchamos la próxima semana Muchísimas gracias muchas gracias a todos que vaya bien chao chao adiós 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