el futuro de la Inteligencia artificial se aproxima y no pinta bonito ya que varios países y concretamente el pentágono planean usar esta tecnología para desarrollar armamento autónomo con capacidad de matar sin supervisión humana las vulnerabilidades de mediodía causadas por fallos en su proceso de divulgación pueden exponer detalles sobre las mismas que cibercriminales pueden abusar y equipos de ciberseguridad pueden utilizar como alerta temprana de amenazas con la Navidad a la vuelta de la esquina Aquí tienes un obsequio 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 5 de diciembre de 2023 es el episodio número 113 yo soyt vio y está conmigo empol el gorrito de Papá Noel Alexis porros Hola Alexis qué tal Muy bien Martín sí como dices a escasos 20 días de la Navidad Así que Jo Jo Jo nos Vais a escuchar decir alguna bromilla al respecto pero también quera decir que con ganas de que llegue la Navidad pero también de resaca de Black Friday Cyber monday Yo espero que nuestros oyentes hayan comprado algunos productos que mejoren en favor de su privacidad no todas estas historias que tanta cámara tanto y más con un poquito la noticia que vas a cubrir Martín pero sí estamos hiper vigilados últimamente Así que cuidado con eso y si no si habéis comprado alguno de estos productos Pues nada seguid escuchando tierra de hackers Porque si surge algún tema de privacidad de estos productos os los vamos a traer de primera mano en cuanto salga y también para aquellos que queráis estar más integrados en la comunidad de Tierra de hackers os cuento lo primero es que nos podéis seguir en redes sociales estamos como tierra de hackers o @ tirad hackers lo segundo Es que para saber cuándo sale un nuevo episodio os podéis suscribir en tierr de hackers en cualquier plataforma de podcasts y también podéis participar en nuestro canal de discord donde podéis entrar vía tierradel comom discord perfecto que por cierto ahora que te decía eso de lo de papá Anel estuve con unos amigos el fin de semana y una amiga que es chilena me me decía sabes cómo le llaman a papá nuel en Chile tío ni idea viejito pascuero Bueno nos estuvimos riendo todo el fin de semana con eso tío viito pascuera de aquí un saludo a nuestros oyentes en Chile que que son muchos además eh Y nada yo por mi parte estuve est este esta semana pasada en una conferencia muy chula el ccn cert allí con muchos oyentes también con mucha gente estuvo muy Guay y y nada quería hacer una mención a un comentario que nos dejaron y y pedirte disculpas Alexis tío Porque Eh sí sé que parez quear sorprendido pero ibox nos dejaron un comentario muy gracioso que era que mira te lo leo porque lo acabo de abrir ahora y pone eh 25 minutos más O sea pone termina Alexis una locución que es historia viva de la radiofonía y dice Martín bueno hemos terminado por hoy en el sentido de que la semana pasada cuando edité tú diste una noticia como siempre muy buena y yo no hice el comentario de turno que solemos hacer al editarlo lo recort Y entonces es como acabas tú de hablar durante 20 minutos y yo venga acabado el episodio Hasta mañana pero que conste que conste que aparte de por supuesto una noticia excelente fue eso fue un fallo a la hora de editar que que recort yo mis mis comentarios pero me hizo muchísima gracia eh esto historia viva de la radiofonía eh o sea lo estás haciendo muy bien Alexis Está bueno está bueno no están buenos esos comentarios si no siempre se aprecian tus comentarios Martín los haan o no Yo sé que siempre tienes buenos comentarios Así que no claro y esta era la idea de cuando te propuse hacer el podcast que fuéramos dos para que no esté yo aquí solo rayando la cuestión también es intercambiar y la conversación por eso baja y los oyentes se quejan cuando no grabamos en los dos a la vez Pero bueno no siempre es posible hacemos lo que podemos que y que s habrán sido cinco o seis veces en TR años que llevamos de podcast Tampoco es tanto Bueno nos ponemos al lío no que si no luego también se queja los oyentes de que hacemos una intro muy larga si es que si es que se están poniendo exquisitos eh los oyentes después de de 3 años que no somos perfectos pero lo intentamos claro bueno y antes de comenzar gracias a nuestros mecenas de patreon

especial mención a un nuevo mecena que se une a esa familia alciber muchísimas gracias y a nuestro sponsor monat una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros lo hacemos a través de un podcasting monat con una herramienta de gestión y visualización de telemetría y datos de seguridad está fundada en silicon Valley y está buscando si es que estáis cansados de oír los ingenieros con experiencia de ciberseguridad qué estáis esperando ayudarles a construir y hacer realidad su misión contr contratar en todo el mundo y en remoto así que ya sabéis echar un vistazo a su web en monat.com mad.com y m les vuestro currículum a tierrade hackers @m.com que así saben que venís de nuestra parte como decía empezamos ya Y es que no pasa una semana sin que veamos avances en Inteligencia artificial que es el de lo que quiero hablar hoy Bueno ni los avances ni en los ámbitos donde se utiliza eh muestra de ello Es que cada mes al menos una noticia en nuestro podcast Es sobre Inteligencia artificial Yo diría que si nos fijamos en el último año cada mes al menos hay una Y hoy no va a ser distinto queridos oyentes volvemos con la Inteligencia artificial volvemos con noticias que resaltan la parte negativa de la Inteligencia artificial o bueno desconocida diría yo después de haber preparado esta noticia de A dónde nos lleva esta tecnología no y me baso en un artículo del New York Times publicado la semana pasada en donde se comenta que Comenta como ya son varios los países que abierta dicen que están trabajando en Añadir Inteligencia artificial a su Arsenal a su Arsenal militar os Leo un par de párrafos de un documento al que apunta el New York Times escrito por el director de la oficina Nacional de inteligencia de los Estados Unidos el reporte se titula el futuro del campo de batalla puedes dar la mes que si no entre entre los ruidos y masticar y tal me desconcentro un montón Ahí estamos Gracias tío el reporte se titula el futuro del campo de batalla y os lo dejo en las notas del episodio porque de verdad eh vale mucho la pena leerlo es de abril de 2021 eh o sea de hace dos hace bueno prácticamente 3 años cuando aún no teníamos los chpt los M journeys ni nada de lo que bueno ahora damos un poco por hecho que todo el mundo tiene al alcance de las manos no dice así En referencia al tipo de armamento que esperamos ver en el futuro próximo que es de lo que va este reporte armas autónomas letales a medida que avanza la tecnología Autónoma algunos países pueden no preocuparse por tener humanos en el ciclo de decisiones de disparo como resultado es posible que para 2040 a pesar de los desafíos éticos y legales asociados con su uso armas letales verdaderamente autónomas pueden recorrer el campo de batalla y tomar sus propias decis iones de selección y combate y hay otro párrafo que os digo que es se titula Enjambre los sistemas no tripulados de todo tipo se Están volviendo más numerosos capaces y económicos ya se han observado ataques por pequeños enjambres de vehículos aéreos no tripulados los uavs por ejemplo cuando las tropas de las fuerzas especiales de Estados Unidos lucharon por retomar la ciudad iraquí de mosul de de que estaba en manos de Isis en otoño de 2016 Fueron atacadas por al menos una docena de uavs armados que lanzaban granadas y explosivos improvisados sin embargo El poder del Enjambre no se limita solo a la cantidad los enjambres de vehículos no tripulados podrían comunicarse entre sí y ajustar sus tácticas y objetivos según cambien las circunstancias ostras es que está describiendo literalmente una escena de Terminator 2 justo De hecho cuando empieza la peli si recordáis se ven así como los drones coordinados volando por encima disparando a los humanos mientras los terminators van andando así por encima de las calaveras no es que es tal cual aprovecho a insistir que el autor de este reporte de esta previsión no es un periodista no es un tertuliano es el director de la oficina de inteligencia Nacional del país del país con el ejército más potente del mundo y termina esta sección del reporte que ya os digo os la dejo la notas del episodio pero con un párrafo que a mí me dejó los pelos de punta es este el desarrollo y las capacidades en evolución de estos sistemas autónomos están estrechamente vinculados a los avances en la Inteligencia artificial la

Inteligencia artificial ya se utiliza para mejorar el redimiento de diversas armas existentes como el reconocimiento de objetivos en cabezas de guerra de precisión y puede utilizarse en apoyo de lo de los humanos en la colaboración hombre máquina incluyendo herramientas de toma de decisiones o como un motor de toma de decisiones en sí mismo para 2040 es probable que la toma de decisiones militares derivada de la Inteligencia artificial incorpore datos disponibles en tiempo real provenientes de satélites para respaldar las operaciones atención a esto por ejemplo china está buscando activamente el uso de la Inteligencia artificial para una amplia gama de aplic acciones incluido el análisis de información y datos para juegos de guerra simulaciones y entrenamiento así como para la toma de decisiones en el ámbito militar el presidente ruso Vladimir Putin declaró en 2017 que la nación que lidera el desarrollo de la Inteligencia artificial se convertirá en el gobernante del mundo disculpad que a lo mejor la traducción suena un poco rara eh De hecho Esta la hice con chpt porque tenía así como unos términos militares pero básicamente esto viene decir que la Inteligencia artificial ya está parcialmente en armamento militar pues para ayudar por ejemplo cuando para apuntar con armas o los drones no tripulados para encontrar objetivos pero que para 2040 insiste aquí que que esto va a estar a la orden del día y sobre todo que la Inteligencia artificial va a ser la que decide si atacar o no y que china ya lo está haciendo en simulaciones y el presidente ruso Vladimir Putin dice literalmente ya directamente ya digo que el que sea el primero en llegar se convertirá en el gobernante del mundo pues ya veis Hacia dónde nos dirigimos queridos oyentes Pero esto no deja de ser una previsión una intuición de lo que está por venir la postura de este tío con respecto a lo que él piensa que sucederá la cuestión ahora es dos años y medios después de que lo escribiera tenía razón hemos dado pasos hacia ese futuro estremecedor tiene sentido lo que aseguraba en su reporte o se ha equivocado estrepitosamente Bueno por lo pronto os diré que el tema es tan serio que se está debatiendo ahora mismo a nivel de Naciones Unidas son muchos los países que han pedido reglas y límites al uso de la Inteligencia artificial en el ámbito militar el representante de Austria por ejemplo dice que este es el punto de inflexión más importante al que se enfrenta la humanidad menuda frasecita eh el representante de un país en las Naciones Unidas comenta que el papel que juega el humano en el uso de la fuerza es absolutamente fundamental en términos de seguridad legalidad y ética y desde luego yo personalmente Estoy totalmente de acuerdo si dejamos en manos de algoritmos el uso de la fuerza las decisiones de atacar o no a otra nación Cómo afrontamos ese de desde los tres puntos que mencionaba y sobre todo qué Qué pasa si algo va mal de quién es la culpa de la Inteligencia artificial del país de quién desarrolló los algoritmos y se los vendió a ese país Cómo se prueba que la Inteligencia artificial no fue ligeramente digamos e manipulada para que tomase decisiones digamos una vez más más agresivas son una mayoría los países que han expresado recelos en permitir usar Inteligencia artificial y armamento autónomo Pero hay algunos países que directamente se han opuesto a cualquier tipo de control y yo os pregunto queridos oyentes Cuáles creéis que son estos países que dicen básicamente que no hay ningún problema y la Inteligencia artificial la podemos Añadir perfectamente al armamento y te pregunto a ti Alexis mientras nuestros queridos oyentes que están al otro lado reflexionan sobre ellos si me tuvieses que decir cuatro países que no quieren poner ningún tipo de Límite a la Inteligencia artificial en el ámbito militar cuál es dirías y ya te digo yo que lo vas a acertar porque es que cuando los vi digo que es que no podían ser otros los de siempre tres los vas a acertar China Rusia y el otro podría ser algún middle eastern country tipo Irán o algo así pues no acertaste tantos eh Mira china sí pero con matices que voy a entrar Rusia 100% Estados Unidos e Israel o sea Estados Unidos Rusia e Israel no quieren poner absol amente ningún eh límite Pero hay uno más Australia que esto la verdad me sorprendió bastante Es verdad que forma parte del grupo de los Five eyes Pero bueno que Australia que suele no sé yo por lo

menos bueno como como ese típico país Por decirlo de alguna manera eh sin querer entrar en política pero como progresista buen rollista de paz mundial e me sorprende que aquí no tenga ningún problema De hecho no es que no tenga ningún problema todo lo contrario sino que empuja junto de la mano de Rusia Israel y Estados Unidos para que no se pongan trabas no se pongan límites a la Inteligencia artificial en el ámbito militar y mencionabas China pero china ha dicho que definiría algunas reglas es decir china está tomando una postura más eh desde mi punto de vista responsable que Estados Unidos para que luego digan Yo creo que mi punto de vista debe ser que china en plan no no yo no quiero dar eh No le quiero dar digamos libertad a mis ciudadanos para construir Ai que luego me puede superar a mi gobierno incluso igual dicen a mi gobierno sí pero a los ciudadanos no entonces por eso tienen ese esas condiciones Supongo digo yo Claro tú lo que dices es que a lo ya no temen tanto a lo mejor a Estados Unidos sino a ver si ahora los propios ciudadanos nos quitan aquí la dictadura que tenemos no al shiping a ver si alguien ahí en una fábrica empieza a construir inteligencias artificiales y drones le instala al firmware mete su propia Inteligencia artificial y se carga la al communist party ahí en China clo en China o sea en Estados Unidos hay muchas empresas buenas no y y y mucho talento pero es que en China eh Hay muchas como tú dices muchas fábricas mucha electrónica la gente solo tiene que incluir un componente que es una llm que para ellos o una Ai o lo que sea que digamos igual podría ser más como una caja negra integrarla en sus procesos y luego ser mucho mejor no y y y sobre todo que China o sea el gobierno chino claro tiene mano dura sobre la población las empresas y quiere un control absoluto mientras yo no digo que un gobierno como el de Estados Unidos Rusia o Israel no lo quiera pero digamos que hay como Pues yo diría que las empresas son un poquito más independientes cosas así no eh estado no está mal pensado estado de welfare no en Estados Unidos la ciudadanía no se quiere rebelar contra el gobierno o al menos la mayoría bueno 6 de enero del Capitolio ahí pero bueno que sí que sí que eso Es más redencin entre los propios ciudadanos con su digamos su línea política que que el propio gobierno en Sí aparte siempre depende de quién gobierna No si es Trump pues son de un lado y si es biden Pues es de otro pero bueno continúo mencionando eso que china realmente sí quería Añadir unas reglas pero pero lo que ha propuesto por lo que veo es básicamente insignificante para el riesgo real que puede conllevar un Arsenal que se gestiona solo y no depende de la supervisión humana a la hora de matar os dejo de hecho un paper traducido del Chino al inglés que que me encontré que presentaron el año pasado China y leyéndolo básicamente lo que dicen Es simplemente que la Inteligencia artificial se debería usar solo para defenderse no para atacar pero claro me da la risa yo os Leo un párrafo aquí que que seleccioné para mencionar pero ya os digo que como siempre os lo dejo en las notas del episodio dice así las aplicaciones militares de la Inteligencia artificial deberían propiciar la mejora de la situación humanitaria en los campos de batalla modernos al reducir Las bajas entre los combatientes proteger a los civiles y prevenir la escalada de conflictos no deseados los países deben mantener una política de defensa Nacional de naturaleza defensiva desarrollar y utilizar tecnologías de Inteligencia artificial en el ámbito militar de manera udente y responsable y asegurarse de que los sistemas de armas relevantes y sus medios de combate cumplen con el derecho internacional humanitario y otras leyes internacionales aplicables al mismo tiempo los países deben encontrar un equilibrio entre el desarrollo legítimo de la defensa y las preocupaciones humanitarias y respetar las necesidades de todas las partes para mantener su propia seguridad a mí esto me suena a no decir nada hablar mucho y no decir nada básicamente está diciendo Inteligencia artificial la podemos usar pero solo para defendernos para que haya Pues sí menos bajas y y y sobre todo que protegemos a los civiles sabes a mí a lo que me suela esto al mismo argumento que se utiliza para las bombas nucleares son disuasorias es verdad es decir el hecho de que Estados Unidos tenga bombas nucleares

Pakistán tenga bombas nucleares Rusia tenga bombas nucleares y China tenga bombas nucleares hace que probablemente no entren en una guerra a muerte No porque entonces se acaba el mundo son disuasorias y y y y se podría argumentar que gracias a eso como no está probada que haya guerras HM pues entonces claro no muere tanta gente se utiliza de manera defensiva pero luego a la vez tenemos bombas nucleares conque a uno se le vaya la pinza recordemos que los códigos de las bombas nucleares estuvieron durante 4 años en manos de Trump y que los de China están en manos de un dictador y que Vladimir Putin está ahora mismo en guerra y ya sacó el tema en su día con Ucrania de las bombas nucleares no sé yo si realmente podemos utilizar el argumento no así muere menos Peña y por tanto es más seguro ya no te digo cuando hablamos de Inteligencia artificial no vamos a tener todo drones que se llevan solos y deciden A quién matar porque s son más precisos a la hora de elegir a quién matar no hay soldados sobre el terreno y todo eso el tema de la defensa que que has dicho hay algunos que eh siguen o bogan no por esta frase que es la la mejor defensa es un buen ataque Así que igual es un poco se quiere cubrir con esa ese ese ese ese tema no una espada de dos filos Y luego el tema que estás diciendo que van a haber muchos drones y menos soldados a mí esto me pinta al final que va a ser solo robots contra robots van a estar luchando en el campo de batalla Así que al final es es qué van a estar haciendo invirtiendo dinero y destruyendo dinero al fin y al cabo es no haber humanos Pues para eso por qué no luchamos en el el campo del ciberespacio así no destruimos el mundo físico es que es un poco un poco raro no porque o sea Las Guerras empezaron humanos contra humanos no eh pistolas cuchillos lo que sea ahora vamos a quitar a todos los humanos y vamos a ver solo a a vamos a usar robots drones que vuelan y y que luchan entre ellos y tú desde casa tomando tu monjito y viendo el el la pantalla de forma remota Cómo lucha tu tu robot contra los otros cuando te quedes sin robot pues insert Coin y sigue jugando como es un poco no s ya es que es que es que suena videojuego suena al Counter strike es ya no mandamos a soldados ya no mandamos a nadie todo el mundo desde su sofá Pero entonces dónde se Libra la batalla en el mar parece que simbólico es en plan jugamos aquí para demostrar que tenemos el poder pero al fin y al cabo si si hay bombas atómicas en plan aprieta un botón y adiós se acaba el juego es plan no sé es y esto da para un debate interesant o sea el hecho de que de que yo Expreso aquí mi opinión de lo lo digamos el doble filo de las armas nucleares Me encantaría tener Pues a lo mejor a a un comandante militar que nos puede dar una postura que me hace cambiar de opinión o a lo mejor pues el de un no sé asociación pacifista o o alguien que haya estado Sabes bajo ataques de bombas y nos dé una postura de esto es completamente absurdo porque estamos hablando de desarrollar armas más inteligentes más capaces para evitar la guerra o sea esta lógica de alguna manera a mí me chirría yo lo siento pero esto de no vamos a hacer bombas mejores más capaces más independientes porque así reducimos la gente que muere sí por un lado pero por otro no y ya te digo tiene que llegar ya tierra de hackers tierra de hackers El Debate porque siempre surgen temas mu inter que sean más inteligentes que que que los soldados que los humanos que las crean Entonces al final se puede ver en contra nuestra y y un ejemplo que ha salido últimamente no sé si nuestros oyentes lo han visto es todo el tema este que creo que que viene bien comentarlo no brevemente el tema este de que Sam echaron a Sam altman the Open Ai Y por qué luego se lió el rumor este de que tiene un algoritmo que se llama qstar o q asterisco y qu es algunos decían que el algoritmo de q asterisco este es muy avanzado y ahora entiende mucho las matemáticas porque los modelos del llm no saben mucho de matemáticas necesitan utilizar lo que se llaman agentes para eh resolver temas que son más de álgebra matemáticas y similares pero algunos decían Oh No este algoritmo qstar lo que hace es entiende mucho muy bien las matemáticas Y es capaz de factorizar eh primos y por tanto puede petar a es 192 un algoritmo de decifrado entonces toda la gente está un poco oh oh se

acabó el cifrado han roto el cifrado Pero los que son un poco más realistas entienden o o un poco prevén que el algoritmo qstar este es eh un algoritmo que puede crear datos sintéticos eh a gran escala y de forma muy fidedigna muy reales y esto para que lo entendamos un ejemplo que que he leído asociado a esta explicación es el tema del Alpha Go que esa Inteligencia artificial que Deep Mine creó en 2016 para competir con los mejores jugadores de go entonces lo que le y alimentaron a la Inteligencia artificial para que aprendieras fueron fueron los movimientos de los mejores jugadores de go la Inteligencia artificial Entonces era tan buena como el mejor jugador de go pero lo dijeron por qué no ponemos dos Alpha goost dos Inteligencia artificiales jugando la una contra la otra y eso lo que hizo fue crear movimientos sintéticos datos sintéticos que la Ai de Alpha Go aprendió fue aprendiendo de sí misma no de los mejores jugadores del mundo y luego qué pasó pues que este Alpha Go era mejor mucho mejor que cualquiera de los mejores jugadores de Alfa Go tal forma que no sabían ni bueno sab sabían que había porque lo había aprendido no pero no tenían un poco un razonamiento lineal de cómo cómo es que ha podido mejorar tanto Pues el tema este que comentas tú Martín que en el futuro en el 2040 va a haber Inteligencia artificial probablemente sea mucho más inteligente que cualquiera de nosotros por encima de Einstein por encima de los más inteligentes en la historia de la humanidad eso da escalofríos porque qué qué va a hacer esa Ai con con las bombas nucleares ya ya ya ves o incluso utilizar rollo PT para la estrategia bélica no el atacamos por el flanco izquierdo derecho No simplifico mucho pero luego a la vez si todos tenemos las mismas inteligencias artificiales estará la la salsa secreta los datos con los que lo alimentas y será entonces lo que determina Cuál es el ejército más potente no sé da ha hay mucha conversación pero pero es que esto no acaba aquí con los que hemos mencionado ahora queridos oyentes si por un lado tenemos que estos países que os mencionaba están básicamente negándose a hablar o o plantearse los peligros de la Inteligencia artificial con declaraciones como las de Rusia diciendo que todavía no es el momento de abordar este problema que era una de las declaraciones que leía en insisto en Naciones Unidas como como si no tuviéramos estuviéramos ya en el momento de preocupante Pero bueno resulta que la semana pasada China y Estados Unidos si os acordáis la semana pasada se reunió biden con shipin en San Francisco de hecho pues se sentaron a negociar en secreto el uso de la incia artificial en la toma de decisiones para utilizar en armamento nuclear me habéis escuchado bien los dos mayores potencias nucleares del mundo tienen que ver a ver si es buena o mala idea que ch gpt decida si lanzamos una bomba nuclear o no Mátame camión o sea esto Me parece increíble tío es algo que se está debatiendo Oye vamos a ver y por lo que leí en en una noticia que hablaba sobre esto pues no llegaron a un acuerdo y solo quedaron los dos presidentes en que sus delegados seguirían hablando del tema yo flipo tío Pero bueno el ministro de Pakistán por hablar como de de del lado coherente lo creáis o no dijo Naciones Unidas que la ventana del tiempo para tomar una decisión un poco por esto de Bueno ya lo iremos viendo eh Para poner límites se está reduciendo cada vez más rápido y y él teme que no haya una regulación a tiempo ya que no falta mucho para que veamos armas autónomas sobre el campo de batalla a su vez las declaraciones del representante de antigua IB barbuda que fue una de las que elegí de la noticia son muy claras dice no estamos hablando de una novela de ciencia o ficción sino de la realidad que se nos aproxima Y es que hay que tener en cuenta que en Ucrania ya están utilizando muchísimos drones no tripulados digo en Ucrania en el conflicto digo se están utilizando muchos drones no tripulados Aunque siguen siendo operados por un humano realmente de hecho Alex descubrió un par de noticias de esto El problema es que debido a los ataques de yaming saturación de las señales que lo que hacen es neutralizarlos porque no pueden comunicarse con la base pues esos ataques son cada vez más sofisticados y por tanto a los drones estos que no llevan a ningún humano sino que se manejan a distancia

para evitar estos ataques de yaming se les añ da capacidad de seguir operando aunque las comunicaciones sean bloqueadas por tanto el siguiente paso natural es que los drones puedan elegir el objetivo sin interacción ni aprobación por parte de un operador que básicamente sea totalmente autónomo para que cuando está sobrevolando el campo de batalla aunque estén intentando neutralizar la señal o bloquearla con ataques de yaming El dron siga siendo útil y pues mato Yo sin tener que consultar al al tal Total ya me encuentro sobrevolando Ucrania O sea que a Rusia le da igual si se equivoca o no pero si aún así no estáis convencidos del futuro que nos viene el propio Pentágono el propio Pentágono ha confirmado Confirmado eh que está listo para desplegar armas autónomas a gran escala hace unos meses el Secretario de Defensa dijo lo siguiente Secretario de Defensa de los Estados Unidos digo las fuerzas armadas americanas van a desplegar de sistemas autónomos sobre el campo de batalla en los próximos 2 años y lo justificó diciendo que tiene que competir con China y estar a la cabeza de la carrera con sistemas autónomos que sean cito textualmente pequeños inteligentes baratos y muchos si nos vamos a la política del digamos a los policis no a la política veros a la reglamentación no del propio Pentágono en cuanto a este tipo de armamento según esta noticia vos algo que por un lado arroja algo de Esperanza Pero por otro lado es aterrador dice así uno de los puntos eh de los policis del pentágono respecto armamento autónomo si las armas son controladas por Inteligencia artificial el personal militar debe retener la capacidad de desconectar o Desactivar los sistemas desplegados que muestren un comportamiento no deseado a ver Yo según leía al principio digo Guay ahora Cuando leo el final digo ostras vale bien que que que el pentágono diga no tiene que haber como un Kill switch no como como en los aviones por ejemplo que tieneen piloto automático pero el piloto siempre puede eh mecánicamente sobreescribir lo que sea que está mandando el piloto automático Por tanto la última decisión siempre la tiene el piloto un humano pero es que aquí me esta frase acaba como por si por si los sistemas desplegados muestran un comportamiento no deseado alguna vez habéis leído algo más semejante al escenario de de Terminator o sea cómo O sea si ya nos estamos planteando que puede haber un comportamiento no deseado ostras yo no sé si esto me tranquiliza o no quiero decir si hay una necesidad de un Kill switch a lo mejor no deberíamos hacer los autónomos eh No sé me resulta bastante curioso yo aquí lo que veo es una situación en la que nos están intentando vender que el uso de la Inteligencia artificial en conflictos bélicos es positivo porque reduce muertes de personas tanto de soldados como civiles no como decía antes esto nos dice China Rusia y y Estados Unidos Al menos que realmente son los big Players No aquí os dejo una frase de cada uno de ellos concreto de Rusia y de Estados Unidos eh con la reflexión con respecto a esto Rusia dice entendemos que para muchas delegaciones la prioridad es el control humano para la federación rusa las prioridades son algo diferentes y Estados Unidos me encontré esta las armas inteligentes que utilizan computadoras y funciones autónomas para desplegar la fuerza de manera más precisa y eficiente han demostrado reducir los riesgos de daño a civiles y objetos civiles pues está claro la postura de de esta dos fuerzas militares y ahora las declaraciones como contraparte de uno de los fundadores de Skype y que ahora es fundador del instituto del estudio del riesgo a la vida y el futuro que yo no no sabía que este eh este digamos nonprofit digo esta ong que creo que es una ong existía de hecho elon Mask o sea es bastante seria elon Mask por ejemplo donó 10 millones de dólares creo e y me lo encontré un otro artículo y dice el fundador O sea que no es un cualquiera podríamos estar creando un mundo en el que ya no sea seguro estar afuera porque podría ser perseguido por enjambres de robots asesinos bueno Y es que el tío da puntos muy interesantes porque él dice que el problema es se elimina digamos un poco el control Porque si Estados Unidos no por poner algo empieza a decir bueno Esto de la Inteligencia artificial no es buena idea en armamento no vamos a hacerlo si china no opina lo mismo si no se llega a un consenso que

para eso existe Naciones Unidas Entonces yo entiendo que Estados Unidos diga pero que no podemos nosotros poner un control Cuando el enemigo no lo pone os pongo el ejemplo un poco más evidente vosotros creéis que Corea del Norte va a llegar a un acuerdo de vamos a esto no evidentemente no entonces claro Esto me acuerdo una frase de un político español en Era sobre otro tema totalmente pero en en digamos en el parlamento europeo decía que que no podíamos ser veganos en un mundo de carnívoros no porque Europa pues normalmente es así más de de de legislar y todo esto mientras que otros países no Claro esto es un poco lo mismo y es un problema porque aunque tengas buena actitud tampoco te puedes quedar demasiado atrás porque te comen es que el futuro no va de tener un mayor número de soldados sobre todo cuando lo que te por mucho que tengas un millón de soldados y lo que te envían son drones No tripulados pues pues ya me dirás tú y luego otro problema que plantea este fundador de de Skype es que el futuro son los enjambres estos que os decía de miniaturas de drones autónomos que dice él sueltas en libertad y no se puede atribuir a nadie es verdad porque imaginaos ahora que pues fuerzas especiales no como Pues los Navy seals o así que hacen operaciones encubiertas como yo que sé cuando mataron a vinladen No pues tienes que llevar a esos soldados altamente entrenados lo mejor de lo mejor sobre el terreno de manera encubierta poniendo su vida totalmente en peligro Pero si tú ahora para un objetivo muy concreto yo s reventar una central nuclear en un país enemigo tú sueltas unos drones que van de manera Autónoma en Enjambre van hasta allí revientan con todo vete luego tú a echarle la culpa a al país enemigo cóm que Qué pruebas tienes tú de que esos drones los lanzó Estados Unidos contra Irán o al revés sea no no tienes y como es totalmente Autónoma nadie lo opera pues ya está tú lo sueltas y ya les das las condiciones que tienen que cumplir una misión pero luego aquí si te he visto no me acuerdo y yo no he sido ya vemos ahora esas guerras diplomáticas que por ejemplo lo vemos mucho con Rusia negando siempre pues hackeos ataques de ransomware que están claramente eh ordenados desde el kremlin y simplemente dicen que no y ya está vete tú a probarlo no porque es difícil a veces establecer una autoría en ataques cibernéticos Pues ahora imagínate con armamento totalmente autónomo y que vuela y que tiene un alcance Eh pues como misiles intercontinentales o por lo menos a nivel de diferentes países muy complicado de escalofríos la noticia Martín de Sí sí la verdad es que tanto tío y un poquito y ha ido comentando en esta noticia he querido comentar más en tiempo real mis pensamientos pero uno que me ha quedado en el tintero es entonces Martín estamos un minuto más cerca de la medianoche qué qué romántico y tétrico a la vez eh la medianoche la entiendo como la el el se apaga la luz en el planeta huela a todo no Ah pensaba que es el y como justo fui hace poco al al al museo este del espía internacional en Washington DC tienen el reloj este que lo llaman reloj del juicio final o reloj de mediane que es eh que es una simboliza digamos eh la proximidad de la humanidad a una catástrofe global medida en minutos hasta la medianoche donde la medianoche simboliza la catástrofe nuclear entonces Cuanto más cerca estemos de la medianoche pues más probable eh sea este final no no tan bonito digamos no bastante triste entonces por eso te decía yo creo que ahora Estamos un minutillo más cerca de la medianoche y creo que que ahora Estamos como a 10 minutos creo que te quedas corto bro te quedas corto un minuto yo diría 10 minutos No sé la escala no sé no sé si ya son las 10 o las 11 de la noche son y pico creo ya creo que son las 11 y pico ostras Pues sí sí como mínimo un minuto más cerca ya me dirás porque insisto yo os he traído declaraciones no de tertulianos sino de líderes líderes mundiales O sea que esto ya es un debate que está en Naciones Unidas no es un presidente de un país diciendo me preocupa esto O sea un minuto como como mínimo más cerca sí Y además con tanto La verdad es que empiezan a ver más y más drones que entregan paquetes por aquí por allá eh en cualquier momento llega el dron vuelve a la base se le hace una modificación rápida y se le ponen ahí un

poco de eh Como yo que sé una pistola o lo que sea y y la gente está acostumbrada es como cuando el típico una un usuario accede a una página web que tiene un certificado eh inválido pero bueno como siempre accede pues no no le Presta atención y luego viene alguien un atacante que eh suplanta esa página web y como tiene un certificado inválido Pues el usuario accede Igualmente la página web sin saber que que ha accedido a la página del del usuario malicioso en este caso en plan estamos acostumbrados a ver tantos drones que yo no sé si es de paquetes si lleva balas y misiles y va a disparar o para mí s no pasa nada luego un día empiezan a disparar y oh oh no lo hemos no lo hemos visto venir sí lo has visto venir Lo que pasa que es como decías Martín nos tenemos que poner como algunas declaraciones de lo que has leído eh nos tenemos que poner ya porque si lo dejamos Pasar mucho tiempo y queremos arreglar como como en el software no Cuanto más tiempo esperes hacia la derecha el tema es está en shift left no mueve intenta mover eh las modificaciones lo más temprano posible en el proceso pues esto un poquito lo mismo hay que educar Es que es que según dices eso de los drones o sea es que estaba pensando Los japoneses los cicac no que tenían que entregar no arriesgar entregar su vida para estrellar aviones y causó muchísimo daño a los americanos claro es que ahora son los drones sin humanos o sea estás acostumbrado a ver drones y de repente pues lluvia de drones contra tu casa cargados de explosivos a reventar Es que esto es el e sabes es el el camic perfecto porque efectivamente no no hay no hay pérdidas humanas pero no sé yo si estamos en un mejor punto como nos intentan vender ciertos países no sé sí pues nada eh interesante la noticia da que ciemos de noticia que que estamos perdiendo oyentes por momento esto es demasiado demasiado chunco cayendo los números no los misiles pero los números sí eh pero da que pensar bueno pasamos para la siguiente la que traigo queridos oyentes va sobre vulnerabilidades de como lo han dicho Half day Pero yo lo voy a traducir un poco para eh la la comunidad hispanohablante lo voy a traducir como vulnerabilidades de mediodía un poco estamos con el tema de del reloj que si llegamos a medianoche ahora con vulnerabilidades de mediodía es un poco pero mediodía con un espacio en medio eh medio día no mediodía no de de a las 12 de la mañana Aunque bueno es os no porque a las 12 del mediodía de la mañana es la mitad del día es un poco Total que de medio día porque decir de día medio queda un poco raro pero anyway el tema es que investigadores de seguridad del equipo de Aqua nautilus el brazo de investigación de la empresa de ciberseguridad aquasec que se enfoca en temas de seguridad en la nube y en containers docker kubernetes y todo esto evaluaron el proceso de divulgación de vulnerabilidades de miles de proyectos de código abierto Open source y revelaron algo muy interesante y esto es que deficiencias en el proceso de divulgación de vulnerabilidades o como se conoce en inglés proceso de vulnerability disclosure pueden permitir a atacantes explotar vulnerabilidades Antes de que los usuarios del Software afectados sean alertados o incluso antes de que se de que hayan parches que arreglen la vulnerabilidad es decir antes de que tú como usuario puedas ir a descargarte el parche o la nueva versión instalarla y arreglar esta vulnerabilidad Los investigadores realizaron un análisis extenso de los commits Pull requests y issues de proyectos en github para aquellos que no estén familiarizados con github es una plataforma de digamos software as a service un software que corre en la nube adquirida por Microsoft en 2018 que se basa en el proyecto git y que permite eh gestionar el desarrollo de aplicaciones gestión de versiones gestión de código muchos temas similares pero básicamente ayuda a desarrollar aplicaciones permite que múltiples personas colaboren en un mismo proyecto de software permite que estos colaboradores modifiquen código con lo que se llama commits que sugieran modificaciones del código con lo que se llama Pull requests o que cualquier usuario cree lo que se llaman issues o problemas para coordinar la resolución de bueno vulnerabilidades o mis configuraciones configuraciones incorrectas o temas similares en el código Los investigadores determinaron

qué atacantes pueden aprovechar este tema esta oportunidad para adelantarse al anuncio y publicación de parches en base a un estudio detallado de toda la actividad de los proyectos públicos en github y además en enriqueciéndolo que es la base de datos que contiene vulnerabilidades de todo el software a nivel global y que seguro que os suena porque es de la que vienen los identificadores de CV que es el sistema de common vulnerabilities and exposures y que es el que se utiliza para asociar para identificar a las vulnerabilidades sobre todo a las más a las más problemáticas cuando sale una vulnerabilidad de un software Normalmente se le asocia un identificador de cve que normalmente es cve gu el año 2022 gu otro identificador numérico que al principio empezó creo con tres o cuatro dígitos porque no habían tantas cada año que se publicaban pero ahora ya incluyen al menos cinco dígitos porque cada año se publican más y más vulnerabilidades se podría pensar que esto Solo afecta a proyectos públicos que estén en github y esto Normalmente se podría argumentar como proyectos Open source o de código abierto pero no hay que olvidar que muchos software de pago comercial o Close source como queramos llamarlos eh Windows macos lo que queramos que corren en nuestros portátiles escritorio ordenadores de sobremesa o móviles incluso webl relojes incluso los teslas Pues muchas veces por no decir casi en la totalidad de las veces este software es que es comercial de pago Close source muchas veces hace uso de proyectos de código abierto por ejemplo en el mundo en el que la privacidad se podría ver casi como un derecho en el que el uso de la buena criptografía es crítico el proyecto open source open ssl es muy importante en este aspecto ya que proporciona las bases de una criptografía que se pueda utilizar y que sea viable y es utilizado por muchas plataformas online de grandes empresas de software en la nube y también en aplicaciones móviles de escritorio bueno en todos sitios eh se usa Open ssl algo que ilustra muy bien este concepto es una de las viñetas del cómic xkcd que voy a poner en las notas del episodio y que probablemente muchos de nuestros oyentes ya hayan visto este cómic xkcd es es el autor es una persona que e de hecho es interesante su trayectoria trabajaba para la NASA era desarrollador hacía temas bueno para para la NASA no y se cansó y dijo que iba a hacer iba a diseñar iba a hacer cómics pero todavía el tema de los cómics se enfoca en temas científicos en temas de matemáticas Bueno es muy interesante muy divertido seguir sus cómics pero en uno de ellos se puede ver una máquina acompañada del texto all Modern digital infrastructure que significa esta máquina lo que simboliza es toda la infraestructura digital moderna y luego se indica con una flecha un componente pequeño sin el que la máquina no podría mantenerse en pie es el componente en el que la máquina se apoya y se apunta con una flecha y el texto al que apunta dice a project some Random person in Nebraska has been thankless maintaining since 2003 que e básicamente viene a decir que es un proyecto aleatorio que una persona en Nebraska ha estado manteniendo sin reconocimiento desde 2003 el mensaje implícito de este cómic es una crítica social a cómo las infraestructuras críticas digitales modernas muchas veces dependen de proyectos de software mantenidos por individuos o grupos pequeños con recursos limitados y sin el debido reconocimiento por su trabajo todo este rollo lo vengo a decir porque esta investigación me ha parecido muy importante Ya que afecta mucho Software que utilizamos no pensemos que solo afecta a proyectos de código abierto Open source y que están eh expuestos en github sino que puede impactar potencialmente A casi todo el Software que utilizamos que que sea de pago que utilizamos en nuestros dispositivos como digo en coches en cuando volamos puede estar involucrado Así que es es una noticia que me ha parecido interesante y por eso la he traído al al podcast para comprender la investigación me gustaría cubrir brevemente un par de definiciones relacionadas con el proceso de divulgación de vulnerabilidades Por una parte tenemos el mítico Zero day o vulnerabilidad de día cero concepto del que hemos hablado múltiples veces en el podcast seguro que ya estáis hartos de escuchar sobre esto y es una

vulnerabilidad desconocida de un software específico en este caso desconocida por el responsable del proyecto analizado en github en el caso de de este análisis de estos investigadores ya hemos comentado como digo antes eh que spyware como pegasus candiru y otros abusan a veces de estas vulnerabilidades para infectar los dispositivos móviles de sus objetivos y hemos también comentado el precio que se paga por comprar estas vulnerabilidades que se marca en un par de millones de dólares según la empresa zimperium por otra parte tenemos el resto de vulnerabilidades que podríamos llamarlas de día un o de día n Esta es la vulnerabilidad que se conoce que es conocida por el desarrollador del Software afectado y Por ende por sus usuarios una vulnerabilidad es de día uno el día en el que se publica el parche que la regla y además el identificador de CV o así se considera aunque a veces el lanzamiento de este parche a veces puede retrasarse un día o más como os voy a explicar en algunos casos o en algunos casos a veces incluso nunca se publica algunos Igual conocéis también el concepto de de día n vulnerabilidad de día n que también sería válido relacionado con el de día un y es cuando n en este caso puede tomarse Como genérico por ejemplo Es decir vulnerabilidad de día 3 que sería cuando hace TR días que se publicó tanto el identificador de CV como el parche pero en esta noticia me voy a referir a este caso solo como vulnerabilidad de día 1 es decir tenemos vulnerabilidad de día cer y vulnerabilidad de día un una de las conclusiones de esta investigación es que la divulgación de vulnerabilidades no es un proceso binario con estos dos estados que digo vulnerabilidad conocida o desconocida de día uno o de día cero sino que es algo más complejo es un proceso digamos más gris estos investigadores encontraron muchos casos de vulnerabilidades que no se pueden clasificar como día oer o día 1 y que según ellos dicen que están entre tiempos por este motivo Los investigadores sugieren Añadir atención dos estados más en el proceso de divulgación de vulnerabilidades el primero y es el que se centra esta noticia es digamos lo han llamado como digo vulnerabilidad de mediodía o lo llaman ellos Half day Que es el caso en el que una vulnerabilidad conocida por el desarrollador del Software de alguna forma la información de la vulnerabilidad se ha expuesto de forma pública a través de plataformas como github debido a los comits Pull request o issues o envd por el identificador de CV o similares en alguna lista de distribución de de correo es posible que se haya creado un commit para solucionar la vulnerabilidad pero aún no hay un parche oficial disponible que los usuarios se puedan descargar instalar y arreglar esta vulnerabilidad y durante esta fase se puede asignar o no puede haber un identificador o no de cve asociado con esta vulner habilidad para ilustrar este punto os podéis imaginar el caso en el que hay un Pull request abierto en github abierto me refiero a que se ha enviado a github pero no se ha resuelto no se ha arreglado en el código sobre una posible vulnerabilidad en un proyecto x este problema Pues fue reconocido por el desarrollador del proyecto que Envía un comentario diciendo okay sí esto es cierto eh voy a al menos dices esto estoy cierto y y lo voy a intentar arreglar y existe un commit que corrige el código vulnerable incluso puede ser que el commit se haga fusionado se haya fusionado con la rama principal del proyecto sin embargo en este caso no está disponible el archivo binario ejecutable que instala el parche o instala la nueva versión de este Software que Resuelve la vulnerabilidad es decir puede ser que el comit esté ahí se haya fusionado con el código fuente pero no es el el proyecto en sí el software no se haya compilado no se se haya creado el binario que se distribuye que se descarga que se instala para los usuarios de a pie obviamente como usuarios avanzados más avanzados podrían descargarse el comit directamente del código fuente que Resuelve la vulnerabilidad y compilar ellos mismos este software Pero esto no es lo normal porque primero tienes que conocer bien el software en detalle tener preparado un entorno de compilación que tenga todas las dependencias del proyecto y bueno saber luego probarlo y que realmente funcione porque a veces los desarrolladores dicen sí está arreglado en este comit luego se lo ponen a probar y

hacen un digamos revierten el comit porque realmente ese no lo arreglaba y crean otro comit otro otro arreglo digamos no y bueno en proyectos mucho más grandes esto puede ser muy complejo y luego por otra parte el otro estado Que sugieren es el de día 0,75 se podría también se podría llamar también vulnerabilidad de las 9 o de tres cuart de dí joder justo Me quitaste la coña tío Sí sí de las 7:30 ponle más o menos es que digo madre mía vamos a bastante tiquis Mikis están aquí pero me parece Interesante pero voy a explicar el Por qué e lo voy a dejar de todas formas en día 0,75 que me parece más en línea con día 0 día 1 mediodía es el único caso que queda así como más gracioso de comentar con dos palabras en lugar de con con un número pero en en este caso la vulnerabilidad de día 0,75 es una vulnerabilidad que el desarrollador del Software afectado conoce hay un parche oficial disponible sí un archivo normalmente binario como he dicho antes que los usuarios pueden descargar para instalar el parche la nueva versión y los identificadores de cve no están disponibles la principal diferencia entre este estado entre el estado de mediodía y el de 075 este estado es que en este estado hay un parche disponible aunque esto parece prometedor y tener disponible el parche que corrige la vulnerabilidad suena más como a vulnerabilidad de día 1o El problema es que debido a que en este estado el identificador de cve aún no se ha asignado ni publicado las herramientas de escaneo de vulnerabilidades no pueden detectar esta vulnerabilidad y por tanto organizaciones no pueden utilizar dichas herramientas para saber que están afectadas por esta vulnerabilidad es decir No sé si si esta vulnerabilidad se puede implementar en en map nesus qualis la herramienta que utilicéis pues aunque la lancé No vais a poder encontrar esta vulnerabilidad porque no está no tiene asignado un cve y estas herramientas de escaneo de vulnerabilidades normalmente digo normalmente porque hay excepciones no pero normalmente siempre tiran de del identificador del del CV para identificar estas vulnerabilidades Entonces aunque paséis Aunque haya un parche y realicéis escaneos de vulnerabilidades Pues como no la identifica vuestra herramienta de escaneo de vulnerabilidades no podéis instalar el parche y cuáles son los riesgos de vulnerabilidades de medio día o día 0,75 pues en ambos estados de una nueva vulnerabilidad los atacantes podrían recopilar información que se esté divulgando sobre esta vulnerabilidad En plataformas públicas github nvd y los atacantes podrían de esta forma localizar referencias al código vulnerable utilizar las pruebas de concepto publicadas que como digo a veces se incluyen en los Pull requests o incluso escribir su propio exploit porque aunque no esté el proof of concept si en el Pull request está hay referencias al código vulnerable pues un poquito Si sabes un poquito puedes acabar encontrando la vulnerabilidad digamos replicándose Los investigadores compartieron varios estudios de caso que demuestran el impacto de estas vulnerabilidades que no son de día cero ni de día uno en el proceso de divulgación de vulnerabilidades de código abierto mencionan dos de ellas en el informe pero solo me voy a centrar en una por temas de tiempos y porque la otra no es tan relevante Y si queréis podéis consultar que el informe que voy a incluir en las notas del episodio esta vulnerabilidad eh la que voy a comentar es archiconocida y es la vulnerabilidad de lock for shell que para muchos profesionales de la ciberseguridad Probablemente esta vulnerabilidad simboliza un punto de inflexión en la gestión de vulnerabilidades Porque muchos tuvieron que trabajar día y noche para parchear esta vulnerabilidad Cuando recién salió y que creo que yo recuerdo si no recuerdo mal salió como a finales de semana tipo un viernes y vamos eh mucha gente tuvo que que trabajar el fin de semana para identificarla arreglarla parchear y evitar que que atacantes que la estaban explotando in the Wild como se dice activamente eh Pues comprometian sus sistemas os comento brevemente el desglose cronológico de cada etapa de la divulgación de la vulnerabilidad lock for shell esta vulnerabilidad fue reportada por alibaba al equipo de Apache el 24 de noviembre de 2021 el 30 de noviembre de 2021 es decir 6 días después el mantenedor

del proyecto abrió un Pull request and github con un commit que solucionaba el problema a partir de ese punto la vulnerabilidad y sus detalles estaban disponibles en dominio público eran públicamente accesibles en github cualquiera podía ir ahí ver el Pull request el commit y ver las referencias al código vulnerable el 4 de diciembre de 2021 4 días después del envío del Pull request el comit se fusionó con la rama principal de proyecto se incluyó en las últimas versiones de de cada una de las ramas sin embargo no había todavía un parche oficial disponible en ese momento esto es muy crítico porque aunque como digo aunque se haya arreglado en el código fuente si no hay un binario un instalador una nueva versión que los usuarios se puedan descargar cómo lo van a arreglar todavía son vulnerables el 6 de diciembre de 2021 dos días después es cuando el primer parche oficial estuvo ya disponible en el sitio web de Apache Así que comentando respecto a la ventana de medio día tenemos que durante un lapso de 6 días desde el 30 de noviembre de 2021 al 6 de diciembre la vulnerabilidad estuvo expuesta En plataformas públicas en este caso github este periodo de tiempo permitió o hubiera podido permitir a los atacantes detectar el problema identificar el código vulnerable y posiblemente crear un exploit Antes de que los usuarios se dieran cuenta de que estaban afectados por esta vulnerabilidad y pudieran aplicar el parche como digo eh quiero remarcar que durante esta etapa las herramientas de escaneo no podían identificar el problema la vulnerabilidad porque aún no se había creado un número un identificador de cve ni tampoco e hay otro concepto que se denomina cpe eh common platform en generation que es es un identificador digamos no tan único como el cve pero es una forma de decir qué tipo de software y en qué plataforma eh afecta la vulnerabilidad publicada estos dos digamos estos dos datos el CV y el cpe son utilizados por herramientas de escaneo de vulnerabilidades para Eh Pues cuando te dan el informe de lo que han encontrado para decirte exactamente dónde está y lo que es y si si está afectado realmente esa plataforma o no es decir si está afectado en un Linux o en un Windows o no así que también es importante tener el CP ayuda más en en hacer más fiable el reporte de la vulnerabilidad luego un poquito sigo con la cronología el 10 de diciembre del 2021 4 días después de la publicación del parche se publicó el identificador cve de la vulnerabilidad ese día marcó el primer momento en el que las herramientas de escaneo de vulnerabilidades tenían los datos necesarios para detectar esta vulnerabilidad Entonces tenemos que con respecto a la ventana de del estado de esta vulnerabilidad de día 0,75 tenemos un lapso de 4 días del 6 de diciembre al 10 de diciembre de 2021 durante tiempo durante el que la vulnerabilidad estuvo expuesta En plataformas de código abierto el parche oficial de de Apache estaba disponible Durante este tiempo sin embargo los atacantes aún podían explotar esta vulnerabilidad contra usuarios que no habían aplicado el parche y esto se debe a que solo después del 10 de diciembre las herramientas de escaneo como digo de vulnerabilidades podían intificar de forma efectiva este cve otro día importante fue el 13 de diciembre que es cuando el cve recibió su puntuación Porque e se le se califica se usa otro sistema cvss que se utiliza para calificar dar una puntu puntuación de critic calidad a cada vulnerabilidad que se asocia a un identificador de cve va de 0 a 10 y Cuanto más alta sea pues más crítica es y en ese ese mismo día el 13 de diciembre También se publicó como digo el CP el common platform enumeration y esto proporcionó a las herramientas de escaneo de vulnerabilidades una visión más detallada del impacto de la vulnerabilidad en diferentes software productos y versiones además ayudó a los usuarios impactados a priorizar este cve en su sistema de gestión de vulnerabilidades porque es otro tema bastante muy importante empresas eh están inundadas con vulnerabilidades y ahora hay que parchear esto hay que parchar lo otro pero las empresas necesitan un poquito de ayuda Eh en este caso del nist un poquito de la comunidad para un poco calificar Cuál es el impacto de cada una de las vulnerabilidades y determinar En cuáles enfocarse primero Por ejemplo si tienen una una cola

de 10 unidades medias justo surgía esta de lock for shell eh si se le califica como crítica pues obviamente van a prestar mucha más atención a esta que a las otras que las van a poner en pausa hasta que arreglen esta eh otro ejemplo breve relacionado con esta es la babilidad text for shell que esta fue incluso peor que con lock for shell ya que la ventana entre día cer y día 1 fue mucho más grande e ilustra un escenario mucho más más Severo el estado de mediodía duró 75 días y el de día 0,75 duró 14 días pero ya vemos que casi durante estos e 90 días e pues cibercriminales podían haber eh abusado de de de este conocimiento y haber explotado esta vulnerabilidad Bueno Este es un tema de un viejo conocido podríamos pensar eh vulnerabilidades de mediodía igual no es nada nuevo para algunos de nuestros oyentes más avanzados que aprovechen este concepto para bien o para mal para mal seguro que después de 112 episodios queridos oyentes ya sabéis lo que se puede hacer con exploits de menos de día uno y Malas intenciones ya hemos comentado pegasus candiru más de una vez así que ya veis por dónde vais van los tiros pero para bien este hecho se puede aprovechar en proyectos de inteligencia de amenazas o threat intelligence para monitorizar proyectos importantes que una empresa esté utilizando en sus sistemas y en cuanto surja una vulnerabilidad de medio día o día 0,75 actuar haciendo algo al respecto como aplicar alguna medida temporal mitigadora preventiva o de detección Hasta que el desarrollador del Software publique el parche y se publique también el identificador de cve y la vulnerabilidad pase a ser de día uno un caso de mal con aplicación de bien sería el uso de esta información en proyectos de penetration test o incluso en ejercicios de red teaming en el que esta esta información de vulnerabilidad de mediodía puede ser muy valiosa en estos ejercicios Yo creo que no sé si lo mencionaste pero el Back boun porquee red teaming y ejercicios pero en Back bounty que hoy en día está super automatizado sobre todo la parte esta que tú y yo siempre meamos con lo de recon no que que parece que hoy en día Back btis solo hace rec y ya está pero si tú tienes esto corriendo todo el rato y te y te pones unas alertas y tal al fin al cabo hablando antes mucho de la carrera ser el primero mucho de Back bounty es ser el primero en encontrar algo porque digamos que hay muchísima gente dedicándose a ello y que técnicamente tiene la misma capacidad para encontrar ciertas vulnerabilidades entonces la carrera ser el primero en verla es importante y ahí es donde entra la automatización sí la tenía inicialmente para comentar también el concepto de Back bounty pero eh el tema es que carrera a ser el primero he llegado antes que claro si la vulnerabilidad ya está publicada probablemente no puedes no puedes decir que es tuya Lo que sí que la puedes aprovechar en temas de yo he visto a veces Ah claro he visto a veces informes de gente que se queja porque he he reportado un crosser scripting y me han dado 5 en cambio otra persona dice no es que lo que tienes que hacer es después de identificar el Cross scripting tienes que enseñar Impacto Entonces igual con estas vulnerabilidades que todavía puede ser que no estén arregladas en en la empresa en la que estás haciendo el Back bounty pues Oye en contra del Cross scripting y me aprovecho de esta vulnerabilidad de medio de medio día que no es mía pero me aprovecho y toma te he sacado todos los datos de una base de datos o he conseguido Remote command execution gracias a Entonces ahí sí que la puedes combinar como un encadenado no una cadena de vulnerabilidades pero esa es buena o incluso a lo mejor no sé si son temas de que encuentras en una vulnerabilidad que afecta a un servidor Pero hay más servidores desplegados A lo mejor está presente en otro lado o utilizarlo en Back bounty más como referencia Qué tipo de vulnerabilidad es Buscar Si ves que yo que sé tienen ids en todos lados yo que sé eh desde luego yo creo que Útil es a lo mejor no es tan útil como inicialmente me planteaba es muy cierto lo que tú dices pero toda información en la parte esta de recognizance va a ser útil y luego yo me planteo que uno podría argumentar que a ve veces es verdad que mucha gente yo estuve de ambos lados del Back bounty tanto de encontrarlos como de lidiar con reportes y tú

podrías argumentar Oye sabes yo no no es que haya encontrado esto en en github sabes el tío no tiene por qué saber eso del programa de backb tú dices esto yo acabo de encontrarlo en producción chiqui chiqui cl te pueden decir bueno bueno pero te pueden decir no pero es que esto ya lo teníamos planteado arreglar Oiga usted yo Yo solo sé que yo ido a a su empresa.com y he explotado esta vulnerabilidad a mí no me cuente películas sabes sí no al menos el tema de el tema de recon y si es una vulnerabilidad que que te da una ventaja competitiva y que obtienes más información que otras personas o otros competidores de Back bounty no tienen pues Oye la puedes explotar y y de ahí tirar para adante y encontrar otras eso sí que te puede ayudar seguro otro tema es si puedes decir no Esta es mía o O pero se puede hacer en el caso de encadenar vulnerabilidades si has encontrado una que es legítimamente tuya y tal sí que sí aplicable en también el Back bounty y cómo es posible identificar tales vulnerabilidades a gran escala Pues los investigadores descubrieron dos fuentes de información que permiten recopilar datos de varios proyectos populares de código abierto con el objetivo de identificar vulnerabilidades de mediodía y día 0,75 a lo largo del tiempo una es ya les he comentado Así que los que estén prestando más atención ya la sabréis pero una es github y la otra es nvd el National vulnerability database eh Los investigadores mencionan dos métodos de recolección el primero es en base a los commits Pull request issues de github lo que los investigadores hicieron fue lo siguiente primero compilaron una lista de alrededor 15,000 proyectos populares en github con sus url respectivas utilizaron la Api de github para analizar para descargarse y analizar los comits p request issues abiertas dentro de las comits prs issues abiertas buscaron palabras clave que están en el informe y podéis ver que podrían indicar vulnerabilidades o comportamientos no deseados a algunas palabras se les dio un peso o importancia mayor que a otras para priorizar la posibilidad de haber identificado una vulnerabilidad como real muchas de estas palabras incluyen categorías de vulnerabilidades como Cross Side request forgery use after free path traversal privilege escalation Okay pero también hay algunas otras que mencionan temas técnicos normalmente involucrados en temas de seguridad aunque no son directamente vulnerabilidades como http only secure flag o xml external entity y el último paso fue que Oye Tenemos tantos datos tenemos que reducirlo de alguna forma y lo que hicieron fue reducir este volumen de datos eliminando los resultados de los resultados anteriores aquellos para los que se para los que haya una Release posterior al comit Pull request o issue abierto que se ha identificado previamente lo que que si si sucede esto no Esto indica que hay una alta probabilidad de que haya un parche oficial para esta vulnerabilidad identificada y finalmente lo acabaron con unas con unos 2200 resultados relevantes que se analizaron más a fondo y se redujeron más aún a un a unos 50 resultados un 2,3 por del resultado inicial que con el que empezaron y lo que digo eran 50 proyectos que además requirieron un análisis más profundo un estudio manual pero algunos proyectos interesantes que tienen vulnerabilidades eh de mediodía sin parche oficial son y están en la lista en este informe son los proyectos de kubernetes El cliente de kubernetes Open CV que es de computer Vision kibana que es un un framework una aplicación web para analizar datos de elastic similar spank luego hay alguna también vulnerabilidad de in tensor Flow que es un framework de Machine learning o Inteligencia artificial tanto que hablamos de los drones antes e Imagínate si hay una vulnerabilidad de Machine learning o Inteligencia artificial en en el Software que gestiona los drones con bombas nucleares eh Martín luego también tenemos alguna volidad en Ruby y Uh en Open ssl Como he mencionado anteriormente yo creo que Open ssl es uno de los más de los más utilizados en en toda la industria porque no hay proyecto que no utilice ssl Y esta es la librería principal que se utiliza Así que es interesante que que se encuentren vulnerabilidades de mediodía en proyectos tan importantes como op ssl como se puede intuir este enfoque produce muchos falsos positivos es esencial comprender el contexto de cada proyecto y

conocer el código fuente algunas palabras clave que pueden parecer indicativas de un problema de seguridad pueden tener varios significados por ejemplo el término desbordamiento aparece a menudo en el contexto del desbordamiento de la gráfic user interface o interfaz gráfica y esto sería cuando un componente visual se superpone a otro algo que no está relacionado con temas de seguridad como sí que pudiera ser el tema de desbordamiento de buffer o buffer overflow o desbordamiento de pila o stack overflow así que como dicen haría falta esfuerzo manual esfuerzo humano para validar cada vulnerabilidad potencial que se identifica siguiendo este método Aunque hoy en día volviendo al tema de la Inteligencia artificial y los e Machine learning y los modelos grandes de lenguaje o llms pues Se podrían utilizar temas como gpt para procesar los resultados y filtrar los irrelevantes pero ahora vengo con el método de recopilación interesante el más bueno y bonito este segundo método utiliza eh que utilizaron se basa en que a veces los CVS atención escuchad esto es interesante los CVS se publican en la base de datos de nvd como he dicho antes justo antes no justo antes sino antes eh De que se publique el parche oficial y esto ocurre demasiado temprano en la vida del proceso de divulgación de la vulnerabilidad esto puede ocurrir por varias razones que no vienen al caso pero lo interesante de esto es que algunos CVS en la nvd tienen referencia a al comit o Pull request o issue específico de github no solo al proyecto Que obviamente se incluye en la URL del comit P request is sino al al al al al código específico al código vulnerable de de la vulnerabilidad exponiéndolo a atacantes que potencialmente podrían estar monitorizando y cosechando esta información para abusar como digo de veces los prs incluyen pruebas de concepto o crear su propio exploit el proceso que definieron los investigadores para recopilar esta información de mediodía de vulnerabilidades de mediodía fue el siguiente utilizaron la Api de nvd para obtener los CVS creados recientemente luego tienen una condición de comprobación Y es que si el cve tiene referencias a github como digo Normalmente se incluyen referencias en forma de URL no solo al proyecto sino al commit Pull request issue en concreto pues Oye Descargar descargarse esto esta información si el CV no tiene referencias a github en concreto se podría buscar directa esto no lo han implementado ni ni lo mencionan Pero a mí se me ocurrió que se podía se podría buscar directamente en github por el identificador de CV específico porque puede ser que a veces incluyo Incluso se haya utilizado esto en en el proyecto de github Y aunque no se haya publicado en nvd le hayan dado este identificador al mantenedor de este proyecto y lo haya puesto en el comit específico en este caso en el de los investigadores eh sigo desde el punto de que han conseguido commit PR issues del proyecto en sí porque está en el cve entonces lo que hacen es verificar si hay una Release una nueva versión del proyecto que contiene este comit o este Pull request este arreglo que hace referencia el cve en la nvd si es así podría ser que se haya publicado una versión que arregla la vulnerabilidad y por tanto es una vulnerabilidad de día uno y si no de lo contrario es podríamos estar ante un escenario de vulnerabilidad de mediodía donde como digo la vulnerabilidad queda expuesta a la espera de un parche a diferencia del método anterior que se enfoca únicamente en monitorizar proyectos en github con palabras clave que que puede generar falsos positivos con el consecuente requisito y esfuerzo manual para cribar toda esta información de vulnerabilidad identificada este segundo método garantiza una alta probabilidad de que los problemas detectados sean vulnerabilidades reales ya sea de mediodía o de día uno debido a que hay referencias entre el identificador de CV y los commits p request issues del proyecto en github lo interesante es que para este método han desarrollado una herramienta que la han llamado CV Half day watcher que han compartido en github y que os voy a poner en las notas del episodio está diseñada para escanear la base de datos como digo del nvd en busca de posibles vulnerabilidades de mediodía solo hay que proporcionarle un token de github para la herramienta para que la herramienta consulte la appi de github

especificar el periodo de tiempo deseado en el que se quiere Escanear la base de datos de nvd por nuevos identificadores de cve Y definir la verificación mínima de estrellas para los proyectos de github en los que se esté interesado ah para los que no seáis muy técnicos es muy fácil obtener un un token en github es muy fácil crearse una cuenta en github es gratis Así que os animo a que os la descarguéis os descargué la herramienta y juguéis un poquito con ella porque es muy interesante lo sorprendente es que seguro que incluso buscando en el último día porque yo he estado haciendo un poquito prácticas y usá la a ver a ver si encuentro alguna vulnerabilidad en el último día Eh sí la verdad que encontraba algo aunque sea una o dos podéis encontrar alguna posible vulnerabilidad de medi día y sentiros como un atacante como un cibercriminal como un pentester o red timer en el mejor de los casos a punto de llevar a cabo su próximo paso esto es bastante excitante que sería aprovechar el el proof of concept que se incluye en el pur requeso comit o preparar un exploit o si no si queréis sentiros más del lado del bien no del lado del de la luz de la fuerza look podíais sentiros como un ingeniero de detecciones de amenazas a punto de crear una regla de detección de amenazas para detectar explotaciones de esta vulnerabilidad porque como digo se se puede aprovechar para mal para explotar abusar esta vulnerabilidad o para bien si tienes el código vulnerable puedes analizarlo y crear una regla de detección de esta vulnerabilidad o incluso como administradores de sistemas o miembros de otros equipos de seguridad proactiva que pueden estar preparando alguna forma de definición de explotación de esta Navidad para incluirla en sus edrs o intrusion detection systems o intentando aplicar algún parche virtual en caliente o incluso segmentar la red porque no no hay otra forma de protegerse de esto que dejar nuestros sistemas aislados de del resto de de otros sistemas un poco menos eh confiables yo os voy a comentar que ejecuté esta herramienta ayer por la noche domingo eh la hora del este de Estados Unidos especificando que quería analizar vulnerabilidades de de mediodía de proyectos de github con al menos 50 estrellas en base a los últimos 5 días y obtuve algunas vulnerabilidades de mediodía interesantes obtuve al menos unos 10 o 12 resultados pero voy a comentar tres de ellas dos de ellas están relacionadas con un proyecto que se llama slims que tiene 152 estrellas y 134 forks en github las estrellas es un poco un indicador de que a la gente le gusta y los forks es un poquito dices Oye me gusta este proyecto pero hay algo que no me acaba de gustar y lo quiero personalizar para mí pues como es de código abierto dependiendo de la licencia puedes hacer una copia un fork y modificarlo a tu gusto así que vemos que al menos 134 personas la han reutilizado Y al menos a 152 personas le gustan así que pinta interesante eh eh este proyecto slims slims 9 es un sistema de gestión de bibliotecas que ayuda a bibliotecas y bibliotecarios gestionar Pues eso ya lo sabéis libros el top Level domain el digamos Com en este caso la página web es slims webid corresponde a Indonesia Así que podemos suponer que principalmente se utiliza en Indonesia entonces este proyecto en concreto yo ayer cuando corrí est herramienta Encontré dos vulnerabilidades y las dos eran de sequel injection la primera para la primera el Pull request es decir la primera notificación de que esta vulnerabilidad existe fue creado el 12 de noviembre y después de tres semanas a día de hoy todavía no hay un comit que arregle esta vulnerabilidad o parche disponible el cve fue publicado el 1 de diciembre de 2023 y por eso Es que la herramienta eh CV halfday watcher me mostró eh el el digamos el comit el el issue a este a esta vulnerabilidad Así que Confirmado eh tenemos un caso de vulnerabilidad de mediodía de squel injection en un proyecto que gestiona libros para bibliotecas al menos en Indonesia qu puede eh permitirte esto pues descargarte la base de datos de de los usuarios de los libros de lo que sea otra relacionada es otro squel injection en otro archivo eh Por cierto esto es un proyecto escrito principalmente en php eh Pero bueno eh otra otra volidad de squel injection lo mismo el Pull request fue creado el 1 de septiembre incluso antes que el otro ya hace meses hay un comit que arregla la vulnerabilidad que fue

publicado el 3 de septiembre dos días después del Pull request pero el comit no se ha fusionado con ninguna de las releases o versiones del proyecto el CV fue publicado el 1 de diciembre por por tanto por eso la herramienta que corrí me devolvió información sobre esta vulnerabilidad y confirmado de nuevo que este es un caso de vulnerabilidad de mediodía ambas vulnerabilidades incluso indican los requisitos para poder realizar la vulnerabilidad porque a veces dices Oh es una vad de squel injection pero la puede explotar bueno en este caso obviamente bueno de forma remota no se puede pero necesito tener privilegios o no necesito estar autenticado No pues también todos esos detalles están incluidos que muchas veces dices esto sería interesante tenerlo para no tener que hacer yo más indagar más No pues sí sí todo esto está incluido y como digo un caso de abuso de esta vulnerabilidad serían digamos las que se relacionan que me vienen más rápido a la mente son temas de abuso de privacidad de los usuarios de la biblioteca que toman libros prestados un grupo de cibercriminales podría extraer la base de datos de este software incluyendo usuarios los libros prestados y información similar explotando estas vulnerabilidades de mediodía de squel injection y vender esta información a gobiernos abusivos estos gobiernos podrían penalizar a estos usuarios ponerles multas ponerlos en prisión en base a los libros que estén leyendo libros en contra del gobierno o similares o incluso estos grupos cibercriminales podrían enfocarse en identificar a potenciales objetivos que estén investigando algún caso polémico en contra de algún cliente suyo típicas organizaciones de hack for hire y luego Bueno ya identificado el este usuario este email le voy a enviar el paylo de pegasus El paylo de candiru un poquito indagar y y hacer el cerco digamos encontrar más información sobre tu víctima yo fui a showan luego para buscar un poquito a ver qu qué podía encontrar Y al menos Encontré dos servidores en Indonesia expuestos públicamente no accedí a ellos pero que están corriendo este proyecto y Google Search haciendo un poco de goog doing puedes encontrar al menos ocho servidores más que me salan en total 10 Así que vemos Que de la nada eh o sea cualquiera yo no creo que esto tenga mucha complejidad en descargarse esta herramienta obtener una un un token de github y un poco indagar en las vulnerabilidades que se que se exponen y luego identificar cuál es el el Attack surface que hay expuesto en el mundo así que me parece algo Bastante interesante que bueno que se puede utilizar como digo para bien o para mal se me ocurren otras técnicas de identificación de vulnerabilidades e podemos partir de de suposiciones como que la mayoría de los investigadores de seguridad que publican CVS están involucrados en programas de Back bounty la mayoría de estas personas se centran en categorías de bgs específicos digamos Cross scripting o pcal injection o combinaciones Esto no es coincidencia Y es que muchas veces para ser más deficientes mejores y por tanto sacar más beneficio al tiempo invertido en buscar vulnerabilidades los Back mounty hunters enfocan toda su energía en una cantidad limitada de categorías de vulnerabilidades y incluso puede ser que solo se enfoquen en una de hecho esto es una filosofía de Back bounty muy popular para obtener un mayor bounty o pago para ser el mejor en lo que estás haciendo en esa vulnerabilidad y como como una metralleta automática disparar ese contra las la mayor cantidad de empresas posibles que estén participando en un programa de Back bounty en base a bgs anteriores publicados por este Back bounty Hunter se podría definir un un perfil de esta persona y saber su especialidad categoría de vulnerabilidades en las que se enfoca e incluso posible definir también en Qué servicios o productos se enfoca Incluso se podría asumir que investigadores de seguridad se enfocan normalmente en componentes específicos de productos software por ejemplo a mí me viene a la mente la herramienta mimicat y su desarrollador yo creo que esta persona igual me equivoco pero el concepto de mimicat está hiper enfocado a problemas de autenticación en sistemas de Windows Así que podríamos decir que si alguna vez esta persona dice he encontrado alguna habilidad pero todavía no la voy a publicar podemos pensar que se

trata de algo de autenticación sistemas de Windows todo esto con tanta información online y combinado con modelos de llm Lo siento lo vuelvo a traer porque ayuda mucho Se podría inferir muy fácilmente el tipo de perfil de de digamos de investigador de seguridad y para identificar vulnerabilidades de mediodía lo que se podría es monitorizar personas que publican mensajes sobre las vulnerabilidades que descubren típico he encontrado una vulnerabilidad en empresa x eh que no quiero desvelar el nombre y en breve proporciono más detalles pues Sabiendo la especialidad de esta persona ya sabes por dónde van a medir los tiros y normalmente muchas veces los investigadores también se enfocan en la misma empresa una y otra vez porque como digo para ser más eficientes ya conoces la empresa conoces sus procesos de negocio conoces su tecnología pues para qué me voy a poner a aprender sobre otra empresa si ya lo sé todo esta cada cada cierto tiempo sacan una nueva versión voy a mirar si esta nueva versión han incluido otra vez una vulnerabilidad de la que yo sé y se la encuentro Pues mira bien y el otro es típico mensaje también que encontrado una vulnerabilidad de tipo No sé Cross scripting en un producto que no menciono y en breve proporciono los detalles Pues lo mismo también Sabiendo Qué servicios o productos enfoca Esta persona es fácil predecir los potenciales serv o productos afectados y Cierro la noticia con breve comentario de resumen y mitigaciones esta investigación tenía como objetivo minimizar el riesgo de exposición temprana de vulnerabilidades durante el proceso de divulgación enfocándose en reducir el tiempo entre el descubrimiento de vulnerabilidades y el lanzamiento de parches y de esta forma acortando la ventana de oportunidad para los atacantes para que nos hagan daño al analizar la actividad de github Y las entradas en el National database relacionados con los CVS Pues definieron un par de métodos para detectar posibles problemas de seguridad antes de que se hagan de conocimiento público los ambos que los dos que he mencionado anteriormente Y para ayudar a la comunidad Los investigadores sugieren algunos pasos de mitigación que todo mantenedor de proyecto de código abierto debería adoptar para evitar el riesgo de exposición temprana de vulnerabilidades durante el proceso de divulgación uno es la divulgación responsable eh sería aprovechar las la función de informes privados en github para gestionar las vulnerabilidades de forma discreta No pongáis que los pool request los comics estén ahí de forma pública expuestos y que cualquiera pueda verlos porque de ahí se pueden aprovechar eh crear una política de divulgación responsable que describa un proceso seguro para la gestión de vulnerabilidades sobre todo incluyendo información de contacto también porque si de alguna forma no se puede contactar con vosotros o no se puede enviar el request a vuestro proyecto Pues que de alguna forma os puedan contactar escanear los commits Pull request issues esto hacerlo de forma frecuente y en busca de palabras clave en commits p request issues para evitar una exposición temprana se podría usar la misma lista que utilizado eh que han utilizado estos investigadores o vuestra propia lista pero Incluso se me ocurre que esto es algo que incluso podría ofrecer github como servicio similar a cóm eh lanzaron el servicio de Secret scanning para proyectos públicos a finales del año pasado que esto lo ofrecieron porque vieron que mucha gente que tiene código en github exponía muchos secretos secretos se refiere a contraseñas pero no solo sino a tokens que hemos hablado en un episodio no hace mucho el tema de octa y los hars no esos archivos eh que se extraen del navegador con toda la actividad del navegador y que incluyen los tokens de autenticación y que muchas veces tienen una validez muy larga pues eh github dijo Oye vamos a ayudar un poquito a la comunidad y sacaron este servicio que lo puedes activar en tu proyecto de github y escanea tu tu código fuente y si tienes algún Secret expuesto te te alerta y tú obviamente tienes que ir a borrarlo y luego también mencionan temas de protección en tiempo de ejecución un poco para prevenirse para protegerse hasta que hay un parche eh público que se puede descargar por ejemplo lo he mencionado por encima antes brevemente pero uno sería

Añadir nuevas definiciones de amenazas en sistemas de edr o intrusion detection systems eh tus sistemas de digamos de login monitoring aplicar segmentación de red aplicar parches virtuales o parches en caliente y también aplication sandboxing o aislamiento de aplicaciones que Esta técnica aisla aplicaciones entre sí y del sistema operativo subyacente un poquito eliminando el el digamos el impacto que pueda causar eh la explotación de dicha vulnerabilidad que todavía no tiene parche muchas de estas eh de estas funcionalidades proactivas de prevención de explotación eh se se pueden activar fácilmente en sistemas Windows eh como tema de prevención de ejecución de datos o dep o tema de aslr e randomización de memoria y otros temas similares que protegen eh sobre temas de explotación que que se han usado durante muchos años en el pasado así que ya sabéis como digo os os animo al menos a descargaros esta este proyecto porque es muy interesante y sobre todo podéis Incluso indagar en algunos de vuestros proyectos que estéis utilizando en vuestra empresa para tener un poquito alerta temprana de potenciales vulnerabilidades eh exploits o ataques que podréis podáis sufrir en el futuro en base a esos proyectos que estáis utilizando y y nada a ver a ver qué os parece lo que más me ha gustado es que hayas probado esto porque así también ponemos en valor que esta herramienta efectivamente funciona y que hayas encontrado ahí ya cosillas nada más es muy complicado el tema de instalarla o tal o es tú te bajas un github y es un Script de python o algo así sí No es no tiene creo que si no recuerdo mal no tiene ninguna dependencia es git clone la url del proyecto y luego suele ser ct en el directorio y python y ejecutar la herramienta y pasarle los Flags De cuántos días en el pasado quieres mirar Cuántas estrellas del proyecto y ya está joder Qué bueno pues sí que es útil añadirlo a vuestro workflow a vuestro playbook de Back bouny seguro y bueno si escribís exploit y tal pues ya también si estáis un poquito de lado del mal pues me ha gustado me ha gustado pero ya te digo sobre todo Bueno ya ya comenté un poco antes pero el hecho de que lo hayas probado eso Mola porque muchas veces hablamos de herramientas o hablamos de temas académicos que bueno de aquí a poder usarlo pero cuando tenemos esa ocasión de dedicarle tiempo y probarlo y poder decirle a los oyentes esto funciona y dar ejemplos pues está muy Guay a ver tengo tenía he probado algunas más he indagado he validado que encontré alguna más vulner realidad de mediodía Pero no quería seguir comentando pero solo comento una brevemente Hay un proyecto que es un erp que es un rp es una plataforma de gestión de empresa digamos no para hacer facturas un SAP un Sí pues eh pero este está enfocado a a empresas pequeñas y medianas que tiene 2573 estrellas que son bastante o sea bastante a la gente le gusta bastante y tiene casi 1000 forks o sea 1000 personas se la han forado se lo han copiado para hacer alguna modificación pues eh hab Hay una vulnerabilidad de control de acceso que permite filtrar toda la información de los usuarios incluyendo contraseñas email número de teléfono y similares Así que y esta como digo no está No está parcheada se podría explotar una búsqueda rápida en showan que también fui a showan me mostró que hay 14 servidores de este tipo en el mundo y ahí lo dejo ostra Qué bueno o sea tienes en github la vulnerabilidad gracias a este escáner está resuelto pero no en producción y luego te vas a Shan y lo encuentras tío ahí tienes el playbook el workflow a ser malo o a ganar dinero con Back bounties acordaos de nosotros cuando seis millonarios por los Back bounty eso un poquito de royalty bueno queridos oyentes como siempre nos despedimos ya esperemos ha sido un episodio bastante largo veo por aquí en el editor más de hora y media hacía tiempo que no nos íbamos Más allá de la hora pero bueno Yo creo que ha sido ante Jo dije interesante mira que no quería hacer eso creo que ha sido super valioso enriquecedor académico informativo valioso y ya Hemos llegado al final estamos muy cerca de las navidades yo creo por cierto Alexis que el año pasado había gustado mucho el típico episodio de Los trends de aquella para 2023 O sea que Quizá el último episodio del año volvemos a hacer algo

me preparo como el año pasado unos trends de 2024 Aunque Bueno ya hemos hecho un poco esto con la noticia de Inteligencia artificial es lo que vamos a ver no en 2024 pero que no pero pero bueno sí y nada queridos oyentes ahú nos queda un par de episodios más O sea que no noos perdáis de vista si no estáis suscritos al podcast suscribiros no sea que esperáis que si os llegue la notificación compartirlo con vuestros amigos dejarnos una review Mira si mira si nos está estás escuchando en Spotify coges ahora el móvil le das ahí a las estrellitas Dale cinco Si crees que lo merecemos si nos escuchas en Apple podcast déjanos también un comentario o por supuesto un ibox que nos ayuda un montón a seguir creciendo atrae más sponsors podemos costear lo que nos va a costando y además venimos con con ideas para 2024 que tienen tienen su coste Que de momento sale de nuestro bolsillo Sí eso Muchas gracias por estar con nosotros casi otro año más ya estamos casi en otro año más y lo que dice Martín comentarios cualquiera bienvenidos de mejora o incluso esos comentarios graciosos como el que ha mencionado Martín al principio también son bienvenidos Pues nos escuchamos dentro de una semanita Adiós 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