66. Uber y Apple Lockdown

el Uber Hack de esta semana es el hackeo a Uber han comprometido todos sus sistemas y el autor ha publicado toda la información en Twitter para burlarse el nuevo sistema operativo de Apple viene cargado de nuevas funcionalidades incluyendo el modo lockdown que protege contracomisos de software espía pero que podría facilitar el rastreo en internet tiramos los dados a ver que toca y sorpresa nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 19 de septiembre de 2022 este es el episodio número 66 yo soy Martín vigo está conmigo en un apasionado de los juegos de rol el dungeon master Alexis porros Hola Alexis qué tal Muy bien Martín Sí sí justo ayer ayer estaba en una campaña matando trolls goblins y todo lo que se me metiera por delante y no solo eso también y estoy viendo un poquito al menos por aquí por la costa este no si tú lo ves también por la costa Oeste El temilla más naranja semilla de calabacillas calabazas y tal y cierto la gente ya se está preparando así que ya ya la gente está en ese humor y nada con mucho humor también venimos a agradeceros vuestro seguimiento que nos hacéis siempre en todas las redes sociales allá donde estemos en los chats en discord en las plataformas de podcast con vuestros comentarios sugerencias de nuevo Muchas gracias y os recordamos que deberíais estar suscritos a nuestro podcast en vuestra plataforma de escucha favoritas si aún no lo estáis si vais a tierra de hackers.com ahí sale todas en las que estamos Spotify Google Play Apple podcast y más También estamos en casi todas las redes sociales yo diría Twitter Instagram y Facebook con el handel @tierra de hackers linking YouTube y Twitch como tierra de hackers correos electrónicos no los podéis enviar a podcast@ tierra de hackers.com Tenemos también un servidor de discord al que podéis entrar tenemos diversos canales interesantes para mantener conversaciones bueno eso interesantes podéis acceder a el vía tierra de hackers.com guitarra discord y finalmente como siempre agradecer vuestro apoyo a la pregunta del episodio que en el anterior episodio fue la siguiente te parece adecuada la respuesta de Albania al supuesto ataque ciber terrorista de Irán tenemos cuatro respuestas y la más votada con un 37% fue Sí por tema de medidas políticas es una respuesta política Así que sí que me parece adecuado el tema tenemos la segunda más votada del 32% si evita futuros casos es decir esto sienta un precedente para que Oye si otros países intentan atacar a otros países entre ellos pues que esto no vuelva a suceder Porque Irán está abusando usando demasiada demasiada artillería para su objetivo que era solo interrumpir una conferencia no así que sí un poquito en enseñar dar una lección a los demás para que no sigan los pasos de Irán con un en tercera posición 20%, no dudosa atribución sabemos Realmente si es Irán o no así que no no sé si estoy de acuerdo con la respuesta y la última La menos votada 11%, no mejor contraatacar así que hay algunos que piensan que Albania debería haberse puesto ahí el cogiendo coger las armas y empezar a repartir balazos en contra de Irán Así que ahí lo tenemos pero claro a lo mejor se refieren a contraataques cibernéticos Entonces sería empezar a repartir balazos cibernéticos no O cero days o lo que sea justo justo Me faltó el Cibernético lo que pasa es que es tan caros Pero bueno un misil o algo así también debe de valer millones un misil son 10 Zero days bueno y yo aprovecho como siempre a dar las gracias a nuestros primeros a nuestros mecenas de patreon en concreto esta semana nuestro nuevo mecena upton Muchísimas gracias por unirte a apoyar el podcast y de hecho tenemos nuevos beneficios verdad Alexis porque hemos sorteado entre los mecenas como beneficio adicional Pues un curso de ceret Intel verdad Y

también estamos trabajando con unos descuentos para la conferencia no con name que pronto os daremos más información Así que beneficios añadidos para nuestros mecenas como agradecimiento todos los descuentos para trainings para Educación para todo lo que sea relacionado con ciberseguridad que podemos conseguir pues os los vamos a ofrecer por supuesto Sí se lo comentar ese curso en donde ha ofrecido un compañero de nichopis que desde aquí Muchas gracias está valorada creo en 150 dólares es de respuesta incidentes Así que empieza hoy Así que esa persona que que lo está aprovechando le hemos dicho que nos diga su feedback cuando acabe el viernes Así que a ver que nos cuente que tiene buena pinta Así que a ver si traemos más cursitos de estos para para vosotros perfecto y justo antes de empezar Pues como siempre darle las gracias a monad una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente Nosotros con este podcast sino nada a través de una herramienta de gestión y visualización de telemetría y datos de seguridad está fundada en silicon Valley Busca ingenieros sobre todo con algo de experiencia en seguridad para ayudarles a construir y hacer realidad su misión están contratando todo el mundo y en remoto Así que ya sabes Échale un vistazo a la web monas.com m o n.ad.com Y además lo podéis hacer directamente en su correo tierra de hackers @monal.com así saben que venís de nuestra parte y que les compensa pues seguir apoyando el podcast a pesar de que lo hacen porque es una empresa que le gusta todo el tema de la divulgación y ya con esto yo creo que empiezo Alexis hace tan solo un par de días Me encantan estas noticias que están súper frescas y las recapitulo ahí investigo para justo traerlas al podcast bien fresquitas nos enteramos por capturas de pantalla publicadas en Twitter que han reventado a Uber y elijo el verbo reventar para hacer hincapié en la magnitud de la intrusión que acaba de sufrir esta empresa presente en todo el mundo y que estoy convencido que vamos no hay oyente que no la conozca o no haya usado Uber El hijo del verbo reventar también porque por Norma general cuando hablamos de hackeos a empresas en este podcast por ejemplo normalmente es un ataque ransomware que afecta algunos sistemas o el robo de información pues almacenada una base de datos en concreto la de clientes o dicho de manera genérica parte de la empresa suele estar afectada en el caso de Uber les han entrado hasta la cocina se han paseado por absolu exactamente todos los sistemas con privilegios de administrador han tenido capacidad de hacer lo que quisieran y como quisieran tenían la llave maestra todas las puertas acceso a toda la infraestructura y privilegios de administrador como el empleado que sea que tiene el mayor acceso en Uber lo dicho les han reventado Qué pasó pues como decía hace cosa de tres días por ahí empezaba a circular por Twitter capturas de pantalla de los diferentes Portales y datos de varios sistemas usados por Uber como blues Google workspace confluentes y otros no no hablamos solo de capturas de pantalla de la red interna sino también de los servicios de terceros contratados por Uber Y todo empezó con un primer tuit con la captura de pantalla de nada más y nada menos que hacker One la cual mostraba la cuenta de Uber en esta plataforma de backbounty poniendo lo siguiente Uber ha sido hackeado domain admin y también esta cuenta de hacker One Bueno vamos por partes lo primero que es hacker One muchos oyentes ya lo conocerán pero es una plataforma de backbounty o de recompensa por encontrar vulnerabilidades básicamente Los investigadores Alexis lo ha hecho yo también pues hay empresas que deciden colaborar con hackers legítimos Y si tú encuentras una vulnerabilidad en su empresa pues la puedes reportar a través de hacker One y decirles Oye mira he encontrado este fallo en vez de ir y actuar como un delincuente intentar explotarlo Entonces estás Ayudando proactivamente a la empresa y la empresa te paga pues hacker One es una de las mayores

plataformas que hay para que empresas se pueden digamos publicitar su programa de recompensa por vulnerabilidades y así tú puedes le porque hay Digamos como un term of service o contrato tú puedes legalmente a lo que ellos decidan pues intentar hackearlo Y si encuentras algo pues se lo reportas y ya está pues lo segundo que quería mencionar una vez explicado que es hacker One es matizar que los mensajes que mencionaba antes no fueron posteados como un investigador que reporta una vulnerabilidad en Uber sino como el propio Uber no solo postearon en el perfil principal sino como respuesta a todos los tickets abiertos por otros investigadores que habían reportado recientemente vulnerabilidades de manera legítima a Uber a través de hacker One básicamente el hackeo el que hackeó Uber completamente lo anunció en la plataforma que Uber usa para recibir vulnerabilidades pero como si fuera el propio Uber o sea brutal luego qué es eso de que mencionaba de que dice el mensaje y todo esto Bueno pues el delincuente está haciendo referencia al nivel de privilegios que obtuvo a todos los sistemas que ha conseguido comprometer por ejemplo domain admin pues explicandolo así un poco más sencillo viene siendo la capacidad de gestionar todas las cuentas de usuario de los empleados en la infraestructura de Uber lo de eida Blue es admin pues es el nivel de administración en el sistema utilizado por Uber para gestionar toda su infraestructura en la nube lo de víspera admin esto es una referencia al control total sobre todas las máquinas virtuales virtuales usadas por Uber o Digamos como tener control sobre todos los servidores o máquinas de Uber y lo de G Suite pues es el control absoluto sobre todos los servicios profesionales que ofrece Google pues como el correo electrónico Google Drive y todo esto en fin que como estos públicos empezaron a circular Las capturas de pantalla por Twitter y empezó la especulación no primero la duda y luego que si simplemente pues lo que habían hackeado era simplemente la cuenta de hacker One de Uber porque eso fue la primera captura de pantalla y fue unas horas después cuando el autor del ataque a Uber empezó a publicar capturas de pantalla de los sistemas internos que había anunciado en el mensaje publicado en hacker One hablo de imágenes mostrando la consola de administrador de hacker One de Uber es decir mostrando que tenía todo el control el panel de control de slack del sistema de comunicación entre empleados internos utilizado por por Uber el panel de control de sentinel One que es una solución de ciberseguridad pues También tenían acceso a eso Y por supuesto también el panel de control de edabrioes que os mencionaba como prueba de que efectivamente tenía acceso a todo y además con esos privilegios tan elevados y es en este punto donde ya la gente empezó a darse cuenta de que esto era mucho más serio el responsable del hackeo Uber no Solo lo había hecho sino que se estaba burlando públicamente de Uber a través de Twitter con Las capturas de pantalla pero empezó a surgir otra imagen que para mí y para mucha gente fue la más llamativa una captura de pantalla en slack con el siguiente mensaje en el slack de Uber Hola a todos y todos Ya sabéis que bueno en slack puedes mencionar a Every One para que le llegue la notificación a toda la empresa a todos los empleados de la empresa Hola a todos anuncio que soy un hacker y que Uber ha sufrido una brecha de seguridad se ha robado slack información confidencial de confluencias stage y dos repositorios de fabricator también han sido robados además de secretos de sneakers hashtag Uber underpace drivers o Uber le paga muy poco a los conductores bueno primero explicar este mensaje esto como decía es un mensaje que el que hackeo a Uber publicó en slack para que lo hubiesen los miles y miles y miles de empleados que tiene Uber a la vez y la movida es que bueno y ahí menciona eso que robot secretos que consiguió acceso a slack información confidencial código fuente y lo de además secretos de sneakers entiendo que sneakers debe de ser pues una solución que tienen ellos de almacenamiento de

secretos pues probablemente también pues tuviesen acceso a eso el tema es que la captura de pantalla se ve a los empleados de V reaccionar con emojis y con todo esto a ese mensaje porque nadie le creía al principio la gente pensaba que era un empleado pues gastando una broma un poco atrevida porque estás Ya digo mencionando a toda la empresa Pero al principio no le creían pero no tardaron en empezar a publicarse tweets donde gente con con credibilidad digamos no en el mundo de la ciberseguridad comentaba que había hablado con conocidos que trabajan en Uber y confirmaban la brecha los sistemas de Google con toda la atención vertida en este asunto alguien contactó con el delincuente a través de Telegram ya que había dejado una referencia a su nickne el cual era tipot o taza de té y el autor de todo esto por supuesto no se iba a quedar solo en las publicaciones de Las capturas de pantalla sino que explicó también cómo lo hizo se publicaron imágenes de esas conversaciones entre esta persona que le contactó y él en Telegram Y tipot menciona que consiguió acceder a la red interna de Uber a través de a través de qué crees Alexis que en el episodio anterior me preguntabas cómo habían accedido a los sistemas de Albania y yo lo acerté A ver es que esta no sé si voy a hacer trampa porque he leído un poquito y me imaginaba pero me imaginaba que habías leído hombre Albania igual no era tan famosa pero esta de Uber pues la he encontrado hasta en la sopa vamos en podcast que están escuchando en noticias en todo entonces creo que que leí que era tema había ingeniería social y que a la una de la mañana o así le estaban haciendo el m ay ay ahí voy sí efectivamente ingeniería social has dado en el clavo han comprometido completamente Uber con ingeniería social la conversación es muy breve en el Telegram digo y como ha pasado el otro día Aún se están publicando información a diario pero por lo que he podido Investigar para traeros esta noticia Parece que fue en tres actos listos os voy a explicar cómo se hackea una empresa multimillonaria con presencia mundial en tres pasos como una ópera en tres actos que esto me lo contagió Alexis paso 1 obtén el nombre de usuario y contraseña de uno de los ingenieros a través de ingeniería Social es decir engaña de alguna manera aquí no pude encontrar muchos detalles pero posiblemente haya sido enviando emails para que visitase alguna que parecía la interna de Uber y pudiese sus credenciales ahí pero básicamente a través de ingeniería social algo tan simple como puede ser un email con un enlace a una página falsa obtienes el nombre de usuario y contraseña de uno de los ingenieros que trabajan Uber paso 2 consigue Que el ingeniero apruebe el login mediante autenticación de doble factor escameándole a la una de la mañana con notificaciones como tú ibas a comentar Alexis Qué quiere decir esto Pues que el delincuente os hemos hablado muchas veces del tema de autenticación de doble factor la autenticación de doble factor lo que previene es que alguien consiga acceso a los sistemas aunque tenga el nombre de usuario y contraseña los menos conocidos en todo esto de ciberseguridad que nos encanta tener muchos oyentes así estarán familiarizados con estos cuando A lo mejor intentan entrar en su correo electrónico y a veces desde un ordenador nuevo y a pesar de que pone que el nombre de usuario y dice Oye te voy a enviar un código al móvil No pues tú has puesto el nombre de usuario contraseña aún así te pide información a mayores que que básicamente estés en posesión del móvil no para poder ver ese código Vale pues hay soluciones de autenticación de doble factor que para digamos evitar el coñazo o evitar la incomodidad de tener que recibir un mensaje leer el código ir al teclado poner el numerito pues han desarrollado un sistema en el que recibes un Push notification es decir cuando te vas a lograr pues simplemente te mando una notificación al móvil y tú le das así o no es Oye alguien está intentando bloquearse eres tú y a veces te pone desde donde están intentando bloquearse Con qué navegador para un poco darte la pista así Este soy yo evidentemente no solo

no solo estoy intentando bloquearme sino que además pues la información tiene sentido que viene de mi ordenador no vale pues el problema de estas notificaciones es que tú puedes enviarla una y otra vez y otra vez y otra vez y otra vez y ahora imagínate que es la una de la mañana Eres un ingeniero de Uber estás durmiendo y de repente te llega le está notificación de Oye están están entrando con tu nombre de usuario y contraseña eres tú entonces no y a los tres segundos te llega otra Oye eres tú no y así Otra vez y otra vez y otra vez cada tres segundos cada 5 segundos pum pum pum el móvil no para pum pum pum durante una hora pues esto es lo que hizo este delincuente porque hay un momento que te causa tanta factiva fatiga que lo vas a probar pero el ingeniero no lo daba hecho Entonces paso 3 Manda un mensaje al móvil del ingeniero diciendo lo que eres de Haití para que confirme que el login es legítimo o sea como el delincuente no conseguía a través del spaming de notificaciones de autenticación de doble factor que el ingeniero le diese así A pesar de que estaba durmiendo le mandó varios mensajes diciendo Oye mira somos los de it si quieres que pare Esto del spam tenemos un problema en nuestros sistemas y tal Tienes que darle aceptar porque es que si no no va a parar y continuaba y continuaba y hubo un momento pues que el ingeniero dijo bueno pues que pare ya y le dio a aceptar pum el delincuente no solo tenían los credenciales de este ingeniero sino que además consiguió by pasear la autenticación de doble factor forzando al ingeniero a través del spamming a que aceptase que era un login Legítimo y con esto ya tienes acceso a la red y sistemas internos de Uber el poder de la ingeniería social señores y señoras no tiene nada de sofisticado Pero continuemos porque yo hablé de que el delincuente reventó Uber accediendo absolutamente todo y de momento Aunque grave y muy significativo digamos que solo tiene acceso a la red interna de Uber no así que paso 4 o acto 4 explora los sistemas internos en busca de credenciales toques de acceso llaves criptográficas o cualquier información secreta expuesta que te dé acceso a otros sistemas Esto es lo que se conoce en parte como pivotar no esto es como si alguien consigue entrar en tu casa pues porque te engaña para que le abras la puerta Pero eso no quiere decir que se vaya con todo el dinero que tienes en la caja fuerte no O sea a lo mejor pues te puede robar la televisión te puedes robar pero digamos que eso es como tener acceso a la red interna no de Google pero ahora te interesa digamos pivotar no acceder a sistemas dentro del sistema interno en este caso pues la analogía sería la caja fuerte pues Pues imagínate que tú tienes la combinación a la caja fuerte escrita con un papelito para no olvidártelo debajo del colchón pues esto es lo que hace referencias que una vez estés dentro de la red interna pues te pongas a hacer la fase de lo que se conoce como rincones que es ir mirando por todos sitios a ver si encuentras algo más que te ayude a seguir accediendo otros sistemas en este caso pues sería que el atacante encontrase ese papelito debajo del colchón Pues en este caso lo que encontró y aquí cito actualmente de los chats de Telegram uno de los scripts en Power shell encontró el nombre de usuario y contraseñas de un usuario administrador en psicotic usando estos credenciales pude extraer los secretos de todos los demás servicios de omein admin Dúo One Sweet Qué quiere decir este mensaje Pues un poco con lo que decía con la analogía el atacante fue capaz una vez dentro de la red explorando los sistemas a los que tenía acceso de encontrar más secretos que daban acceso a otros sistemas los que mencionaba antes pero es que aparte encontró digamos la Joya de la corona porque esto de psicotic es lo que se conoce como un privilejacks es management o digamos que es un sistema de gestión de privilegios lo cual utilizó para obtener todos los secretos de que daban acceso como insisto a los servicios comodidad Blue es y Suite y mención aquí lo de Dúo du la evolución de autenticación de doble factor One login es un poco como hablábamos en el episodio anterior de opta esto de single

Sign on y que te da acceso a todos los sistemas domain admin que ya explique lo que era vamos que engañó al ingeniero para que le abriese la puerta y después buscando un poquito por dentro encontró más secretos que ya le daba acceso absolutamente a todo y esto es todo señores cuatro sencillos pasos para comprometer una corporación en palabras del propio delincuente en las conversaciones en Telegram que me encontré la seguridad de Uber es lamentable también comentó el motivo de porque lo hizo que lo hizo por diversión y Parece ser que también como queja para porque según según él Uber abusa de los conductores lo cual explicaría un poco ese hashtag no que puso en slack de hecho comentó que quizá en unos meses publicaba el código fuente interno en Uber yo creo que una vez más por tocarle por tocarle los pies a Uber un par de días después super confirmaba que estaba investigando una brecha de seguridad en sus sistemas y que estaba trabajando con las fuerzas y cuerpos de seguridad del estado es decir realmente Uber tuvo la suerte de que este no fue un ataque de ransomware o no parece ser que el delincuente quisiese digamos que entorpecer no la ejecución de Uber porque la app seguía funcionando se podía pedir comida por Uber eats simplemente lo hizo para demostrar que podía hacerlo y Uber tardó un par de días en ya digo en publicar que efectivamente confirmar no la brecha de seguridad tan grave y Quién es la persona detrás de todo esto al que me he estado refiriendo como delincuente no como ciberdelincuente pues parece ser que es un chaval de tan solo 18 años la verdad es que tiene tela que un chaval de 18 años que bueno que con 18 años pues es tan capaz como cualquier otro no pero digamos que ha tenido menos tiempo para aprender el arte de la ciberseguridad y de la delincuencia con cuatro sencillos Pasos Por así decirlo haya conseguido comprometer una empresa tan significativa como Uber Pero ha llegado un plot twist esta mañana de hecho ayer por la noche que quería avanzar aquí y es que los que conocen el que serán todos el videojuego de GTA pues saben que uno de los juegos más esperados es el GTA 6 Pues justo ayer se publicaron 90 vídeos de Gameplay de este juego que se supone que va a salir dentro de bastantes años es decir han comprometido Rockstar el creador de este vídeo de esta saga tan popular y de este videojuego que está en desarrollo ahora mismo tan tan esperado y el que lo publicó que lo publicó en unos foros dedicados a hablar del GTA tenía como nicknam tipot Uber hacker esto como siempre Alexis y yo siempre hacemos hincapié en lo difícil que es hacer atribución no quiere decir que sea el mismo chaval que hackeó a Uber Pero bueno es Interesante como ha utilizado ese nombre entonces queda todavía por confirmar esto ya digo que pasó ayer a la noche 90 vídeos de Gameplay de este videojuego tan esperado fueron publicados que lo podéis encontrar por Twitter y ya os digo que utilizó el mismo nicknem y además ponía tipot Uber hacker Así que a lo mejor era como un quitarse el sombrero ante lo que había sucedido tres días antes o es la misma persona que le da todo igual o bueno no sabemos luego quiero terminar la noticia también comentando brevemente que me encontraba por linkedin Y eso es por si hay gente en ventas que nos escucha que ha habido muchísimas críticas a varias empresas que ofrecen soluciones de ciberseguridad por utilizar esta situación para empezar a mandar email sasquat a ingenieros de Uber intentandoles vender sus productos tiene muy poca clase y y muy poca ética profesional desde mi punto de vista Por supuesto estoy abierto a debatirlo en que en un momento es que estamos hablando de que han reventado Uber o sea en un momento tan crítico que llevan tres días intentando lidiar con este incidente además esto pasó el viernes creo el jueves o viernes se han estado trabajando 24 horas durante el fin de semana tengas agente de ventas mandándote mensajes como me encontré un par de ellos Oye sé que estás un poco estarás ocupado pero si tienes 15 minutos me gustaría contarte Cómo nuestra solución tampoco quiero aquí avergonzar a

ninguna empresa O sea que me salto las empresas que me encontré que hicieron esto o bueno los vendedores en concreto pero si tienes unos minutos podemos hablar y te hago una demo y para que veas cómo podía haber ayudado tal no procede no procede aprovechar esto y sobre todo solo tres días después que esta gente está trabajando a destajo para lidiar con los problemas que le empieces a enviar spam para venderle tu solución por lo menos Espérate un poco y luego ya solo mencionar también que me encontré esto mientras se investiga la noticia no me acordaba y era que en 2016 el chico Security o digamos el cabeza de la el responsable de seguridad en Uber fue despedido por ocultar un pago a ciberdelincuentes responsables de un ataque de ranson Where a Uber para que no publicaran la información es decir hackearon Uber le hicieron un ataque de ransomware que suele ir acompañado no solo descifrar los datos sino de robarlos y pedir un rescate para No publicarlos pues parece ser que yo es Sullivan que era el responsable de seguridad hizo Ese pavo pago y jamás hizo público que todos los datos de los conductores que incluía pues información de su carnet de conducir y otra información sensible había sido robada por ciberdelincuentes así que ya vemos que también pues Uber ha tenido incidentes y brechas de seguridad significativas en el pasado pero desde luego ninguna como esta Pues nada ya sabéis los que estáis buscando trabajo aplicar las miles de ofertas que han salido de Uber de Security en niñez porque no para empezar cierto cierto es verdad me encontraba por la inteligente también un poco metiéndole caña a Uber porque salieron habían capturas de pantalla y era hace un día hace dos días tres inteles tío de seguridad un poco tarde no Pero además ves hay 20 aplicantes y dices Ok si saben dónde se están metiendo no O bueno igual aprovechan y aprietan ahí en la negociación del salario en plan y ahora mismo es un buen momento para entrevista Google para conseguir bastante más pasta Pero bueno no sé yo no sé yo el tema quería un par de comentarios el tema de las aplicaciones de seguridad tipo el two factor of indication este que has dicho estaba pensando así mientras estás comentando la noticia digo deberían incorporar algún tipo de funcionalidad que desactive notificaciones fuera de horarios de trabajo porque bueno en este caso igual el empleado de Uber Este era uno de esos de que estaba trabajando en respuesta incidentes y estaba como se dice oncoln Y entonces se esperaba que tuviera el teléfono encendido cuando se va a dormir pero bueno o el empleado de Uber también podía ver bueno en iOS Supongo que Android también se tiene esto los perfiles estos de que dices ahora estoy durmiendo ahora estoy en una llamada Ahora estoy y se pausan digamos estas notificaciones se silencian Así que eso podría haber sido una idea yo cuando me voy a dormir y yo lo pongo en modo avión Así que a mí que nadie me busque pero bueno este hombre igual le pagaban mucho y estaba como digo a un call Así que eso era un comentario que quería hacer y el otro es en Creo que nunca hemos entrado un poquito solo entre el 30 segundos en el tema de estas herramientas de privilege account management está de soluciones de gestión de cuentas privilegiadas como administrador como has dicho psychotic hay muchas pero algo que cuando yo he asesorado a clientes míos en configurarlas de forma segura por el tema que mencionas Martín Porque si tienes una contraseña y puedes acceder a todas las contraseñas que tienen Pues bueno habría que definir diferentes roles de acceso y similares pero algo que que cuando me enteré me sorprendió que tenían capacidad de hacer es que estas estas soluciones pueden grabar sesiones también pueden grabar toda la pantalla en plan el vídeo que que está sucediendo en el sistema al que te conectas si te conectas por Remote de stop protocol pues graba todo en la pantalla imagínate que es un administrador que está grabando su sesión y obviamente es administrador igual Abre en algún editor de scripts pues su Script que tiene creencia credenciales harcodeadas o una tercera empresa que se conecta que

es lo Normalmente se hace para grabar la pantalla la función esta en plan voy a grabar a esta tercera persona por si hay temas legales algo que ha hecho que que luego tengamos una evidencia y no solo eso sino que también graba las teclas Aunque salga que el password no se ve en el vídeo pero las teclas también se graban de alguna forma Así que esto podría haber indagado el atacante o atacante es igual podrían indagar aquí que es un sitio donde se puede encontrar muchos más tesoros ni nada Eso me parece interesante comentar es mencionar esto Qué bueno sí sí muy bien muy bien que siempre tenemos que aprovechar oportunidades para hablar de nuevas cosillas Nosotros siempre utilizamos como referencia las noticias pero sí buen apunte ahí así que que hasta aquí es la noticia que tenemos hasta ahora con la información que tenemos hasta ahora iremos actualizando si así procede o sale nueva información sobre todo Yo creo que por el frente del GTA 6 Así que yo sé que hay muchos jugones entre nuestros oyentes que a lo mejor no sabían esto pues ya pueden si quieren ir a ver que no no es que estemos invitando a ir a ver información que no Debería ser pública Pero bueno está todo por Twitter todas estas imágenes y vídeos además de Gameplay del GTA 6 si yo les he visto algo he hecho esta mañana que si decían que era un empleado descontento que ha hecho un clic o algo o igual hizo un link y se lo dio a este hacker de Uber y lo ha aprovechado y este es el que ha dado bombo y platillo Pero bueno Ahí está sí y tendría sentido con el rollo de justo ponerte Pues el mismo nickname no el mismo apodo que el que justo hizo lo de Uber un poco Pues a lo mejor como un guiño un poco a lo mejor pues para echarle la culpa a otro a saber Pues nada Sí pues Sabes que se me acabo de acordar ahora también que con todo el tema de esto hablar de hacker One de poder hacer temas de background y tal pues quería recordarles a nuestros queridos oyentes el tema de la competición organizada por la guardia civil en España para estudiantes y gente que está en formación profesional y universitarios pueden ir a la página de National cyberlink.es y apuntarse ahí yo creo que el año pasado Ya lo hablamos Yo soy uno de los mentores y es una competición de hacking que no solo toca el aspecto práctico digamos de hackeos sino también el jurídico Así que y de comunicación también así que es muy interesante recomiendo a todo el mundo que me está escuchando y que cumpla los requisitos ya digo creo que ese ser estudiante pero lo podéis mirar en la web de apuntarse porque aparte hay premios súper interesantes hay un reconocimiento que vas a obtener también y luego pues vas a codearte con con expertos en ciberseguridad que actúan como mentores en España y además pues conocer nuevos amigos que tiene la misma pasión que tú National cyberlink.es ir y apuntaros ya que creo que es el caso para el plazo en unos días muy buena Martín pues se animando a todos a que vayan yo si eso Si pudiera iría también con martinico Así que para el año para el año te metemos completo Pues nada seguimos con la siguiente noticia que la traigo sobre Apple Y es que la semana pasada y con la publicación del nuevo iOS 16 para iphones Ipad es 16 para ipads obviamente y Marco es Ventura para Max Apple ha introducido una nueva funcionalidad a favor de la seguridad y privacidad llamada modo lockdown no es algo así nuevo que haya surgido de la nada porque ya llevan hablando un poquito del un sistema incluso desde julio ya he visto Noticias al respecto Aunque justo ahora ya pues desde la semana pasada todo el mundo se puede instalar la nueva versión del sistema operativo gente un poco con más suerte igual tenía acceso a las vetas a las versiones betas Pero bueno desde aquí nosotros yo al menos me la he instalado me la instalé la semana pasada creo que Martín también y he estado jugando de hecho un poquito con este modo lockdown en los últimos días y voy a comentar un poquito mi experiencia pero primero quiero comentar bueno de qué va Esto del modo lockdown me hace gracia el el nombre que le han dado un poquito porque no sé si esto alguien le va a venir a

recordar al menos a mí me vino a recordar todo el tema de la pandemia el covid 19 en los blog Downs los confinamientos Podrían haber elegido otro modo locks modo kiosco modo no sé pero bueno Ese es el nombre modo lockdown Y por qué esta funcionalidad Y por qué ahora pues recientemente turistas Defensores de los Derechos Humanos activistas políticos toda esta gente interesante que va en contra de otra digámoslo se han convertido cada vez cada vez más en objetivos de sofisticadas campañas de spyware y hemos comentado en más de un episodio los revuelos y los acontecimientos recientes de estas infecciones de spyware como nso pegasus en campaña de espionaje entre gobiernos y partidos políticos en diversos países Sin olvidar el tema de abuso de poder por parte de gobiernos y el uso de este software espía Incluso en campañas ofensivas y en asesinatos en el pasado para determinar dónde se encontraba esa persona y similares pues Apple ya está un poco hasta los mismísimos diríamos que comprometan sus dispositivos tanto y esto viene motivado por todo lo que he dicho no por todo el abuso de estas organizaciones y su software espía que recordemos que hay bastantes no Tenga sus dns Group También tenemos candiru Ermita de rcs lab helios de intelexa y otros creo que todos los hemos cubierto en episodios anteriores y de hecho si queréis Escuchar estos episodios podéis ir a nuestra web tierra de hackers.com Y tenemos etiquetas que utilizamos por ejemplo tierra de hackers.com/t en inglés de etiqueta barra espionaje o barratag/martware pues ahí podéis ver esos episodios Y qué trae esta funcionalidad del modo lockdown Pues esencialmente el modo lockdown aumenta las funciones de seguridad en los dispositivos de Apple al limitar ciertas funciones que pueden ser vulnerables a los ataques de este tipo de spyware más que de hecho más que aumentar la seguridad lo que lo hace es no es que añada nuevas funcionalidades de seguridad es que de hecho elimina funcionalidades de usuario que me parece interesante su su diseño de esta nueva funcionalidad no pero la primera es una de las importantes Es que la mayoría de los archivos adjuntos de mensajes SMS excepto las imágenes están bloqueadas y funciones como las vistas previas de enlaces ese minipop que sale están deshabilitadas también Esto bueno hemos es muy bueno porque hemos visto en muchos de los pays de spyware como en ese opegassus lo ha desplegado para infectar iphones son de hecho archivos o documentos enviados vía SMS por ejemplo la vulnerabilidad kissmet que afectaba hay message de iOS 13 permitió al spyware en ese opegasus infectar a dispositivos de Apple quién reaccionó introduciendo el sandbox una funcionalidad de seguridad llamado Blast door en iOS 14 para la integridad de los mensajes un poquito para protegerse no pero luego forst entry que fue un exploit de 0 clic que fue diseñado por nso permitió ape Jesús eludir saltarse Blas door y permitió seguir la infección en iOS 14 esto vamos es un juego de gato y Ratón pues esta es la primera que se Desactiva el tema de los archivos adjuntos en mensajes También algunas tecnologías web como la compilación en tiempo de ejecución de javascript o en inglés Justin Time compilation el jeet que se le llama están deshabilitadas Esto está deshabilitado a menos que el usuario lo excluya para sitios específicos esto se hace porque hay muchos ataques también que se les llaman jeeps o spray de jeep que abusan de esta funcionalidad inyectan código que se saltan otras funcionalidades de seguridad para poder ejecutar cualquier tipo de código esto no significa que se desactive javascript completamente pero sí que igual podría impactar al rendimiento de la navegación web mencionar que git es una tecnología utilizada por intérpretes de lenguajes descripting como podría ser javascript en este caso y python el problema es que estos lenguajes el programa en sí se recibe en forma de código fuente en forma de texto y no en forma de código máquina o binario en el sistema que lo va a ejecutar Entonces el intérprete tiene que compilarlo antes de ejecutarlo

específicamente para ese sistema arquitectura procesador y optimizaciones del sistema de la cpu definidas en cualquier caso para tecnologías web en lugar de compilar todo el código Fuente del programa que podría Añadir bastante latencia impacto en el rendimiento si el tamaño del código fuente es muy grande porque igual tendría que tardar No sé un minutito en compilarlo no es mucho pero es el usuario lo notaría y se quejaría No pues qué diseñaron qué es lo que se hace pues se utiliza la técnica de compilación en tiempo de ejecución esta que estoy mencionando lo que significa que a medida que se van alcanzando funciones en el código fuente que se van a utilizar pues se van compilando y ejecutando pero no antes la primera vez que se compila cada función igual se nota cierta latencia pero es mucho mejor que compilar todo el código fuente de una vez y una vez se ha compilado esa función no se tiene que volver a compilar Así que es bastante mejor y mejora bastante el rendimiento y traigo aquí una analogía que se me ocurrió para explicar esto un poquito más de forma más clara entre código compilado e interpretado digamos que el ejecutar un código binario compilado vía web sería como pedir comida a un restaurante y que te la entreguen a domicilio el restaurante tiene la receta o el código fuente el cocinero sería el compilador el que compila el código fuente en código máquina y te lo entrega a domicilio te lo envía vía web y tú te lo descargas el cocinero ha seguido todos los pasos de la receta que están es el código fuente ha utilizado todos los ingredientes librerías dlls o similares y ha completado y creado el plato de la comida por otra parte el ejecutar código interpretado sería como comprar un libro de recetas que sería el código fuente a una librería online y que te lo entreguen a domicilio que sería la descarga vía web antes de eso tú ya has contratado a un cocinero para que esté en tu casa para que siempre te cocine el cocinero es el que interpreta la receta las instrucciones el código fuente y la cocina es decir lo con pila en código máquina Ok pues en el caso del Justin Time compilation sería tener al chef sería tener al cocinero pero que no cocinara toda la comida como una cena de golpe en que no cocine los tres platos primero segundo y postre Porque si un comensal quiere empezar por el postre Pues el chef el cocinero que no cocine todo porque se enfriaría no digamos que primero cocina el postre y los demás platos cuando el comensal lo expida o también igual se podría apreciar que fuera como ir a un restaurante a la carta no es más sería como código interpretado en tiempo de ejecución porque tú le vas diciendo qué platos y te los cocinan cuando tú los pides en lugar de ir a pedir un menú que ya tienen toda la comida precocinada digamos no que Estaría compilado pues ese sería el símil Espero que que aclare un poquito el tema que sea que sea desactivado no es que se desactive javascript completamente solo que se desactivan ciertas partes de javascript que solo ayudan al rendimiento pero que introducen muchas vulnerabilidades y agrandan la superficie de ataque la otra que también se ha deshabilitado es relacionada con una la navegación web es el web asembly que es una tecnología que sea diseñado que tira de javascript pero diseñado para que digamos se envíe código máquina código binario directamente a un intérprete que corren en los navegadores web y que bueno y que se hace también para tema de rendimiento lo malo de esta tecnología que se ha abusado sobre todo para hacer finger printing para identificar a los navegadores web y de esta forma los usuarios detrás de esos navegables navegadores web de manera muy rápida y efectiva a través de por ejemplo diferencias en el procesamiento de imágenes o también se puede escanear puertos locales y esto se ha utilizado para eso mucho más rápido que utilizando javascript esto puede ser un problema importante para los sitios que utilizan huevasemble ya que simplemente no funcionarán al estar esta funcionalidad desactivada que se apoya también en javascript aunque como digo javascript no está desactivado pero el Justin Time lo está tener desactivadas estas dos tecnologías web puede causar pérdida de

rendimiento en la navegación online o incluso en los navegadores embebidos en aplicaciones nativas como tiktok por qué porque esto estas funcionalidades web están desactivadas a nivel de motor webkit en iOS en Ipad oes Y aunque se utilicen otros navegadores que no sean Safari como firefox brave o Chrome estas funcionalidades no van a estar disponibles en estos navegadores porque Usan el motor webkit así que de esta forma y para calcular el impacto en el rendimiento del modo lockdown un investigador utilizó ciertos frameworks javascript para determinar el impacto del modo lockdown como un framework de Google que diseñó que se llama optain que ahora mismo no está en desarrollo igual por eso los resultados un poco digámoslo que no está en desarrollo ahora mismo y por eso igual los resultados un poco agresivos pero de todas formas concluyó que sin el jeep habilitado el rendimiento de la navegación web se reduce hasta un 95%. según sus pruebas comparativas y como resultado tiempos de carga más largos en las páginas web incluso mayor consumo de batería también hizo pruebas en base a otros dos frameworks de una página que se llama browservenge.org que tienen dos que se llaman speedo meter y Jet Stream que se enfocan en otras tecnologías como carga de siss que es lo que hace que la página se vea de una forma u otra los colores de las fuentes y de las capas y el otro hace pruebas de huevas en bly yo personalmente en los en los par de días que llevo con el modo lockdown activado no he notado ninguna penalización tanto como un 95%, ni en la navegación web ningún retraso ni en mi batería he notado mucho tampoco es que me haya fijado y me haya puesto ahí a medirlo Como hizo el investigador pero yo por mi parte no lo he visto no sé si alguno de nuestros oyentes nos quiere comentar en las redes sociales como como lo ha notado si he activado el módulo down y ve Alguna algún impacto en el rendimiento pero yo personalmente no he notado nada Ok estas son las más importantes creo yo desde un punto de vista de navegación web y de superficie de ataque pero también Apple ha ido Ya desactivado otras tecnologías por ejemplo la de reconocimiento de voz esta Api que se puede abusar para grabar el audio de un dispositivo comprometido esta Api es diferente a la de dictado de iOS o Siri y estas dos funcionalidades funcionan sin ningún problema en modo lockdown y no son accesibles a sitios web también Ha desactivado una Api de dispositivos multimedia que se abusa para rastrear de forma única al usuario en sesiones web a través de su propiedad de identificador de dispositivo de una cámara web altavoz o una cámara que esté conectada de forma externa el problema con esto es que la mayoría de los dispositivos que requieren acceso al micrófono o las cámaras del dispositivo no funcionarán como cualquier página web de videollamadas Como pudiera ser Gipsy que funciona vía web verdad y también relacionado es el tema de la Api de web rtc realtime Communications que de nuevo es otra Api que se ha abusado para incluso filtrar la IP pública y local Privada de un dispositivo Incluso si se está utilizando una VPN mediante bueno en la arquitectura esta de rtc hay servidores externos intermedios que se llaman ese tune que pueden permitir filtrar esta información Aunque tengamos cortafuegos que estén bloqueando estas comunicaciones también una muy importante relacionada con la primera que es está el visor de PDF de webkit está desactivado para evitar que ataques a través del procesado de documentos de PDF puedan comprometer el dispositivo por ejemplo de nuevo algunas infecciones con el exploit message de cero clic de nso pegasus el llamado Force entry que he comentado antes pues el spyware enviaba un paylock en forma de documento PDF que abusaba de buenavidades en las días de iOS de procesado de imágenes en cualquier caso Aunque el visor de PDF embebido digamos en webkit en navegadores web Safari y otros este desactivado al hacer clic en un documento PDF se puede descargar el documento y se puede abrir con la aplicación files en la aplicación archivos fuera del

navegador web también hay otros otras funcionalidades como la reproducción de MP3 Que Se Ha desactivado por que anteriormente se han explotado por una navidades vía archivos MP3 maliciosos El problema es que si no se ofrecen audios con otro formato como ogg o similares o el Au de Apple pues no se va a poder escuchar el audio también en la librería más ML pues es otra Que Se Ha desactivado porque se utilizaba aparecer fingerprinting y el impacto es que igual fórmulas matemáticas que se veían en alguna página algún algunos de nuestros clientes que sean más científicos estén en el tema más académico Pues igual van a ver que que no van a poder ver estas fórmulas en las webs que navegaban antes También tenemos la Api de gamepad que es la de videojuegos que se abusaba para rastrear a usuarios a través de las propiedades de nuevo del identificador y también de los botones una vez que los usuarios han interactuado con la página web al Deshabilitar esta Api pues se va a interrumpir la mayoría de los videojuegos basados en navegador y plataformas de transmisión de juegos que usan un controlador para jugar que algunos utilizan el iPhone directamente solo para jugar También tenemos la Api de audio web que también se abusa a veces para hacer cineprinting a los usuarios de navegación web a través de una interfaz específica y también tomando variaciones de la señal o sea se puedes utilizar esa Api Para grabar audio y luego compararlo con otro audio que tengas de base para determinar si es el usuario x o los usuarios y esta funcionalidad se utiliza para servir audio elegir archivos de audio Reproducir procesar el audio Añadir efectos de audio y visualizaciones y similares es una Api bastante potente que permite hacer digamos retocar editar audio digamos on the flying en tiempo real y pues bueno Desactivar esta funcionalidad podría impactar a sitios web que ofrezcan este audio estilo Spotify no me han puesto a mirarlo pero igual habría un tipo de impacto también la web gl está librería está Api según de nuevo se usa para hacer finger y es una de las más antiguas que se conocen para hacerlo si se Desactiva esta funcionalidad pues páginas que utilizan gráficos como representaciones en 3D o páginas por ejemplo estas de casas que te muestran una casa y te muestran varias fotografías y parece una una visa atención visualización en 3D pues podrían no Mostrar esto de forma correcta Entonces no no podrías disfrutar de esa experiencia un poquito más inmersiva no el jp2000 Se Ha desactivado esto digamos no es tan crítico porque Safari es el único navegador que utiliza este estándar el jp2000 Así que se podría utilizar para identificar que utiliza Safari Y de esa forma algún dispositivo de Apple no en este caso Desactivar esta funcionalidad no va a tener mucho impacto ya que hay otros estándares como el png y similares solo tema interesante del jp2000 dos temillas uno que es en la misma imagen lo que le hacía interesante al jp2000 es que uno en la misma imagen se pueden incluir varias versiones con diferentes resoluciones Y luego el navegador en función de tus prioridades elegía una mayor una menor y segundo que permitía el uso de transmisión progresiva de la imagen esto yo lo experimentado Bueno cuando estaba estudiando hice algún tema de multimedia y esto era Era una Revolución en aquel entonces porque permitía cargar que una página web de forma muy rápida no que saldrían todos los cuadraditos con las imágenes y salía la imagen completa digamos pero a muy baja resolución Y a medida que se iban enviando todos los bits de la imagen pues se iba mejorando la resolución A diferencia de en la actualidad Si te vas a alguna página web y tienes una conexión muy mala muy lenta lo que se van cargando son como barritas No desde arriba poco a poco y eso da eso hace que la página sea un poquito sea bueno no sé yo creo que el jpg 2000 esa forma de transmisión progresiva me parecía bastante interesante para que se viera desde el principio un poquito toda la estética de la página web Pero bueno desactivado está en el modo lockdown así que no se podría disfrutar de eso en este modo la otra también que se ha

deshabilitado es las fuentes gráficas de vector escalable de forma similar al jpg 2000 este estándar solo soportado por Safari Así que Desactivar esta funcionalidad no tendría mayor impacto ya que hay otros formatos de fuentes que pueden utilizar otras páginas web las ventajas que proporcionaba este formato de fuentes es que es un documento de xml De hecho no es un documento binario y puede definir las características de la fuente y bueno tiene mayor resolución se puede ver mejor y todo esto Pero puede permitir ataques de como sxml Pues de inyección html o Crossing scripting por lo que se considera un formato de fuentes inseguro también todo esto tema web No pues eso de una parte que era lo más importante que querían cubrir Porque casi todo bueno casi todos los ataques de compromiso de spyware venían por tema de vía web pero también han aplicado otros temas interesantes de seguridad Como por ejemplo que las invitaciones entrantes y la solicitudes de servicio Como las llamadas de facetime se bloquean si nunca se ha llamado a la persona que llama así que solo se pueden recibir llamadas de facetime de números conocidos también se eliminan todos los álbumes compartidos de fotos y se bloquean todas las invitaciones nuevas para álbumes compartidos también cualquier conexión por cable entre un iPhone y otros sistemas o accesorios está bloqueada por defecto y los dispositivos no pueden registrarse en sistemas de administración de dispositivos móviles en lo que se conoce en inglés como mdm Mobile device mana esto para algunas empresas podría ser un problema Aunque el líder de ingeniería de seguridad y arquitectura de Apple confirmó un vía tweet que los perfiles de estos de mbm existentes se conservan cuando se active el modo lockdown así que si tiene que hacer algo que implique una tarea corporativa con el mdm se puede desactivar el modo lockdown momentariamente realizar la tarea y luego activarlo de nuevo no es que se borren Solo que no se aplican en el modo lockdown y finalmente los perfiles de configuración esos que normalmente envían las empresas a sus empleados o escuelas a sus alumnos o incluso las aplicaciones de VPN verdad cuando te dicen instala este perfil para que pueda inspeccionar todo tu tráfico Pues en esto se definen como digo configuraciones de red y otros parámetros pues no se pueden instalar en el modo lockdown comentar brevemente que si no lo tenéis activado pues podéis ir a configuración privacidad y seguridad modo lockdown te pone una breve descripción de muy en buen resumida de lo que he comentado y podéis activarlo desde ahí el iPhone se reiniciará en ese momento después justo cuando se reinicia Pues el modo lockdown ya está activado De hecho si abres Safari debería ver un banner en color gris justo encima de la barra de direcciones encima de la URL que dice modo lockdown activado así que ya lo tienes activado a partir de ahí pues puedes ir cuando vayas navegando sobre todo en Safari en otros navegadores no he visto la funcionalidad Pero creo que es de Safari cuando estés en una página web puedes Añadir exclusiones no puedes Justo a la izquierda de la barra de navegación donde sale la URL salen dos letras aa a la izquierda pues se puede hacer clic ahí y se puede decir que se en la configuración del Website o Website settings se puede especificar que no se active el modo lockdown para una página web en concreto porque crees que segura y porque quieres disfrutar de todas las funcionalidades que sean desactivado en esa página web también se puede hacer lo mismo con aplicaciones porque hay algunas aplicaciones como digo algunas estilo bueno tiktok que tienen un navegador embebido pues Oye estas no quiero que se aplique el modo lockdown porque me impactará mi productividad entonces también se pueden Desactivar aplicaciones excluirlas del modo lockdown yendo a configuración privacidad y seguridad módulogdown y dicho esto bueno Esto pinta muy bien verdad es bastante interesante para todos pues tiene algunas implicaciones de privacidad y cuáles son estas pues primero voy a comentar un poquito a cómo funciona o al menos cómo queremos que funciona un

grupo de ci no por todo lo que conocemos de ellos Pues antes de que despliegue o intenta infectar a una víctima con su programa espía por ejemplo un en ese pegasus lo que se hace es asegurarse de que el dispositivo al que envía el exploit que normalmente es de día cero o muy reciente y de poder ser de cero clic No pues esto implica que es muy costoso como decía Martín incluso del valor de un misil o medio misil no entonces para esto lo que realizan son tareas de reconocimiento y seguimiento activo se quieren asegurar de que esa persona es a la que quieran atacar una de ellas es la identificación del dispositivo de muchas formas Como pudiera ser la carga de fuentes remotas desde sitios web que también se puede aprovechar para explotar vulnerabilidades en librerías vulnerables No pero en el caso del modo lockdown la descarga de fuentes remotas svg como mencionado anteriormente está deshabilitada y de esta forma Sería fácil para un atacante determinar que el dispositivo objetivo no carga Fuentes remotas mediante el uso de un pequeño fragmento de javascript en la página web esto permitiría el cibercriminal sospechar que el usuario el dispositivo es alguna persona que está preocupada por su seguridad y privacidad sobre todo de su dispositivo y probablemente esté utilizando el modo lockdown debido a que lockdown se ha implementado en la última del sistema operativo y que se acaba de publicar para todos los usuarios desde la semana pasada muy pocos dispositivos lo van a tener instalado el sistema operativo y muchos menos van a tener activado el modo lockdown lo que va a permitir a cibercriminales determinar fácilmente esta aguja en el pajar no por ser un modo común poco común digo entre los usuarios de Apple es decir va a haber muy pocos usuarios que lo tengan activado Y si cibercriminales pueden identificarlos pues van a saber que algo están escondiendo sobre todo de cibercriminales no no del resto de la población pero algo indica que estos estos dispositivos pueden ser interesantes y jugosos para comprometer sin embargo aclarar que esto no significa que de esta forma se pueda identificar individualmente al usuario detrás que del modo lockdown no solo se determinar que Oye este usuario tiene el módulogram activado pero no sé qué usuario es digamos que estás en un país abusivo no y estás usando el modo lockdown pues cualquier sitio web que visites podría detectar efectivamente que estás utilizando el modo lockdown no solo cualquier sitio que visites Porque si estás en un país abusivo que puede incluso manipular las comunicaciones e inyectar código imagen una librería javascript pues cualquier página web que visites podría contener este código javascript determinar Si usas el modo el octágono no y comunicárselo a los cibercriminales o al gobierno abusivo a lo que sea de esta forma se podría obtener tu dirección IP Y bueno ya te habrían fichado te habrían asociado tu dirección IP con un usuario en modo lockdown un usuario sospechoso un objetivo potencial un objetivo al que interrogar un investigador publicó código fuente que permitía determinar esto en base a las fuentes en remotas que no se cargan Y aunque solo lo hizo enfocándose en esta funcionalidad también se podría crear código adicional javascript para determinar si alguna de las otras funcionalidades deshabilitadas en el modo lockdown que he mencionado anteriormente están realmente deshabilitadas O sea no solo hay una forma de determinar si tienes el modo lockdown activado no sino que con todo lo que mencionado antes no sé pero parece que igual se ha mejorado la seguridad porque no se puede explotar digamos el software de Apple pero igual se ha empeorado la forma en la que se puede identificar si hay alguna persona de interés detrás de un dispositivo Se podría decir debido a que se ha diseñado de esta forma actualmente no hay nada que Apple pueda hacer para mitigar este problema de privacidad que podría permitir a sitios web como digo determinar si tienes activado el modo lockdown o no sin cambiar todo el diseño del modo igual no vas a actualizaciones del sistema operativo hacen algo al respecto pero de

momento no es además y nos vamos a mantener atentos en cualquier caso a la larga Incluso si Apple no hace ningún cambio lo que podría suceder un escenario a mejor es que si hay suficientes personas que activan el modo de lockdown ya habrá más ruido digamoslo así en la red y sería más difícil identificar a un usuario en modo lockdown como un objetivo interesante Así que igual por el bien de todos podríamos Activar el modo lockdown así entre todos hacemos más ruido y no se sabe quién es quién quién es interesante ver sus quiénes no Interesante pero como digo activarlo Y veis si os impacta el rendimiento de vuestro dispositivo vuestra productividad día a día y Oye si yo de momento lo tengo activado hasta que no me no me encuentre con algún problema de momento lo voy a dejar ahí tal y como está sí que he encontrado que algunas páginas web como digo estas Fuentes que hacen uso del tipo de framework bootstrap estas estas Fuentes digamos de los estados icónicos icónicos típicos no se muestran un cuadrado vacío entonces alguna página web que se aprovecha de los iconos para indicarte la función que quieres utilizar pues es más difícil no porque me la sé de memoria no porque el primero significa guardar el segundo abrir y el tercero significa exportar No pero si no pues tendría que excluir esa página web Pero bueno ya tenemos solución solo se excluye una no tengo que desactivar el modo lockdown entero la ff la electronic Frontier foundation de la que ya hemos hablado anteriormente en otros episodios que es está muy a favor de la privacidad online tiene una herramienta que de hecho creo que la hemos comentado Incluso en otros episodios que se llama cover your tracks que la vamos a poner en las notas del episodio que cuando la visitas y corres digamos ejecutas el código de esta aplicación web te muestra un informe en el que te dice si tienes el modo lockdown activado también te dice si tu navegador bloquea rastreadores de anuncios y también desbloquear arrastradores de anuncios invisibles esos tipos vía cookies supercuquis o dimensiones de la pantalla y similares Qué puedes hacer al respecto para ser más anónimo en internet lo hemos comentado más de una vez pero ya comentar tres temas a alto nivel rápidamente un primero es usar bloqueadores de rastreadores por ejemplo hay bastantes como youblock origin pruebas y Bayer disconnect bueno todos estos tienen una lista una base de datos de muchos de estos sitios web que son rastreadores que los bloquean bloquean el código javascript que se carga en la página web una otra medida un poco más radical sería completamente Desactivar javascript igual no se recomienda del todo porque igual la funcionalidad de la web se cae pero Oye si eres uno de los usuarios que visita páginas web que no tiene tanto javascript la página es más bien estática o bueno se genera se envía todo de forma dinámica desde el navegador pero en el cliente no se se utiliza el javascript pues puedes activarlo y la otra la última sería usar un navegador resistente a fingerprinting que bueno los principales son tor y bueno brave es que está invirtiendo mucho en ese tema comentar que si se quiere hay algunos usuarios que igual quieren hacerse más anónimos mediante la configuración o el ajuste de algunos parámetros específicos del navegador esto puede servir o no incluso puede hacerse contraproducente porque por ejemplo si tienes un navegador Safari y quieres cambiar el user agent para que parezca un firefox Pues un rastreador puede utilizar código javascript de una u otra forma como digo determinar el Canvas determinar las aves que están expuestas en el navegador y determinar Oye esto es un firefox esto es un Safari quiero decir pero el user agent dice un firefox aquí algo huele mal entonces sospechoso no así que cuidado con intentar estos estas personalizaciones así individuales muy individuales se tendrían que hacerse un poco más a modificando parámetros que solo ese la protección ideal sería un una huella digital un fingerprinting tan común que un restaurador no pueda diferenciarlo de la multitud o un o que sea aleatoria para que un rastreador no pueda decir que eres tú como como digo esto podría

proporcionarlo navegadores más como brave como motor y comentar que el modo incógnito aunque parece en pro de la privacidad lo único que hace realmente es que no se guarden datos de la sesión Cuando se cierra el navegador o esa sesión incógnito no previene el tema de que te rastreen online Así que que no se tenga esa falsa sensación de seguridad Cuando se navega en modo incógnito lo único que se hace Es que bueno no te pueden asociar con sesiones anteriores pero sí que te pueden hacer un finger printing en la sesión actual en cualquier caso El peor de todo es el navegador Chrome quería comentarlo de Google que no brinda protección contra arrastrado de rastrea huellas digitales ninguna en modo incógnito y volviendo al tema de Apple quería comentar que para motivar a los investigadores de seguridad a que le echen un ojo al modo lockdown para ver si tiene alguna buena habilidad Apple ha establecido una nueva categoría dentro del programa Apple Security bounty para recompensar a quien encuentre vulnerabilidades en el modo lockdown y prometen pagar hasta una friolera de 2 millones de dólares el pago de recompensa máximo más alto de la industria Martín a ti que como como se te quedan los pelos Al escuchar dos millones de dólares con cuánto los exploits estos de cerodium la tabla esa periódica de los exploits el mayor vale unos 2 millones de dólares creo así que están están ahí No si tú eres un ciber criminal decidirías eliminarlo a un investigador de 0 days se lo darías a apple en este caso que te paga lo mismo que hacer odio te contesto a la primera pregunta como escarpias no a ver yo en mi caso sí no lo digo que a lo mejor Hay alguno ya Rolling therace como dice no a ver yo tengo una no podría con mi conciencia se lo vendería Apple que dos millones pues Oye es un pastón no lo bueno es que como nunca va a suceder porque yo no tengo ese nivel técnico como para llegar a encontrar fallos y escribir exploits así que bueno algún día a lo mejor sí pero sí yo creo que se lo vendería por así decirse haría responsable tengo entendido que así como ha subido Apple y por eso decía la coña de lo de como escarpias con el tema de que de que apela siempre ha tenido la familia de pagar poco me hace cosa de un par de años hablábamos de que su máximo payout el máximo pago que hacía era como 200.000 por ahí y recuerdo que en algún episodio hace poco era cuando cuando comentábamos que lo habían subido un millón que Apple pues ya te digo es sorprendente y ahora dos millones Eso habla de del nivel de sofisticación una vez más que tiene que tener los exploits para pasear algo como como Pero sí yo se lo vendería Apple porque bueno con dos millones vamos firmo ya no sí la verdad que sí a ver si a ver si nuestros oyentes que están en el mundillo del cero de ahí también para que no lo abusen luego estas empresas de spyware otro tema también en los que se están poniendo un poquito las pilas Apple es también a subvencionado han dado 10 millones de dólares al fondo de dignidad y Justicia de la fundación Ford que se dedica a investigar exponer y prevenir ataques cibernéticos altamente dirigidos como obviamente los relacionados con spyware quería comentar también que bueno Apple tiene el modo lockdown pero también Android tiene un modo lockdown Aunque no es tan glamuroso digámoslo así porque el modo lockdown Android solo bloquea solo Desactiva los sensores de huellas dactilares el reconocimiento facial y el reconocimiento de voz de esta forma lo que pide es el pin una contraseña o el patrón de desbloqueo para Acceder al móvil y una vez se accede de forma exitosa se Desactiva Así que luego lo tienes que volver a activar vamos que no te protege el modo lockdown de Android no se parece en nada al modo lockdown de Apple solo es digamos para hacer el login y no te protege sobre exploits online o sobre tu privacidad online en conclusión Apple se ha tomado muy en serio el evitar que cibercriminales comprometan y abusen de la privacidad y la seguridad de sus usuarios en los productos de Apple y para ello ha implementado el modo lockdown que reduce mucho la superficie de ataque de dispositivos de Apple aunque esto tiene el

compromiso de la privacidad del usuario ya que puede permitir recibir criminales determinar si el usuario objetivo tiene el modo lockdown activado y Por ende indicar que el objetivo sería interesante sería un objetivo que potencialmente fuera jugoso para atacar en paralelo a papel también quiere mejorar este componente mediante una recompensa por vulnerabilidades muy atractiva como hemos dicho y una contribución sustancial al fondo Ford a favor de la privacidad de las personas acabar diciendo que sin desmerecer Apple parece que está arreglando a base de parches fallos en sus sistemas operativos algo que esperemos que funcione y que nos proteja a todos de Las garras de spyware pero igual Apple debería invertir más en desarrollar códigos seguro desde los cimientos no y no hacer lo que hace ahora intentar apañar el código inseguro que ya han desarrollado y con esto queridos oyentes llegamos a la pregunta del episodio que es la siguiente desde un punto de vista de seguridad y privacidad te parece adecuado el modo lockdown del nuevo sistema operativo de Apple O crees que deberían invertir en otros temas en otras funcionalidades de seguridad tenemos cuatro respuestas la primera es Sí porque evita que comprometan mis dispositivos Apple con spyware Sí porque ayuda con mi privacidad y me hace algo más anónimo es lo que más bien preocupa no deberían invertir en desarrollo seguro más que en tapar agujeros así tipo chapuzas Igual olds también algunos usuarios el modo lockdown les impacta su vida diaria con los productos de Apple y la última es no deberían invertir más en temas anti rastreo muy interesante la pregunta porque de hecho por un lago no se puede plantear no vale me estás haciendo pagar un teléfono de mil y pico pavos que hace 50 cosas y lo primero que voy a hacer es activar algo que quita 20 cosas entonces justo es un poco es un poco raro y por otro lado es Oye ha habido bastantes críticas a apple con el tema de su seguridad en su día hablábamos mucho de que Apple era en sistemas bastante más seguros también por la naturaleza de que es un sistema cerrado Pues que era mejor que Android pero hubo ese punto de inflexión donde cerodium por ejemplo esta empresa que paga por 0 days empezó a pagar más por lo de Android entonces un poco como que la seguridad de Apple se estaba quedando atrás hemos visto incontables vulnerabilidades a través de hay meses con los caracteres estos raros que hacía que se reiniciarse el teléfono temas que has comentado tú de de en esos grupos aprovechando el renderizado de imágenes para explotar el teléfono entonces a lo mejor todo todo este tema de desarrollo del lockdown hubiese sido mejor poner los recursos a hacer el móvil más seguro pero bueno por otro lado también es positivo que haya un tema de lockdown porque uno podría evaluar y es muy difícil hacer un software 100% seguro por tanto a lo mejor no es mala la idea de hacer de reducir la superficie de ataque no el fletcher pues ya que no lo puedo hacer perfecto vamos a reducirlo lo máximo posible A lo mejor podrían sacar un nuevo iPhone porque ahora ya está con el iPhone 14 extra Plus de no sé qué Pues a lo mejor pueden hacer un mainos no iPhone minus y entonces pues es el iPhone como el se que es el más barato pero todavía más barato porque te viene con menos capacidad no sé pero muy buena la pregunta Alexis si esto lo que has dicho es esta funcionalidad en lugar de Añadir reduce no es como consigas a comprar un coche último modelo y tiene aire acondicionado ahí o es híbrido y tal Y dice Bueno es híbrido pero sabes que mejor No uses la parte eléctrica no va a ser que te explote la batería tiene aire acondicionado pero no lo uses no va a ser que que se te vaya a acabar el agua del radiador tiene vas a comprar un Ferrari pero está limitado a 120 para que no te pases de velocidad que es peligroso para eso para eso me compro el coche normal pero si nada es aún así es interesante las dos caras de la moneda Pues yo comentar lo que lo que son las cosas del directo querido Alexis porque según ibas comentando tu noticia estaba yo mirando Twitter y ha habido una actualización en la noticia de Uber que acabo de dar hace un

momento y es que hasta cuando yo la estaba dando había mucha especulación como comentaba porque está todo fresquito fresquito pero Uber acaba de actualizar según dabas la noticia Alexis su publicación sobre el incidente y ha dado muchísimos más detalles concretamente no solo ha dicho que la manera si os acordáis yo mencionaba que había cuatro actos Pues en el primer acto yo mencionaba que era Haz la ingeniería social a uno de los ingenieros para que te dé ese nombre de usuario y contraseña y yo comentaba que especulaba ya que faltaba esa información en el cómo hacerlo pues que me imaginaba que había sido es un email Pues no ha sido todavía más fácil comprar un y esto ya son hechos esto dicho por Uber os pongo el enlace en las notas del episodio aparte de a todo lo que he mencionado Las capturas de pantalla de Twitter y todo noticias donde he recopilado la información y todo esto a la publicación de Uber pues ahí mencionan que la manera el acto 1 el cómo obtuvieron esos primeros credenciales de una persona en Uber fue comprándolos en la Deep web y resulta porque esto lo vi en el tweet del grupo ID que es esta empresa que se dedica a la cere tintel que de hecho comentábamos en el episodio anterior Pues he visto un tweet suyos y lo que hicieron fue coger Las capturas de pantalla que el individuo publicó sobre Uber y se fijó que en una de Las capturas de pantalla se ve abajo sabéis cuando descargas un archivo en el navegador pues te queda como abajo no en la ventanita Pues el archivo que te has descargado sobre todo en sistemas Windows con el nombre pues se dieron cuenta que había nombres que les sonaba y los buscaron en sus en sus temas de monitorización y de datos que tienen ellos que investigan en la Deep web y encontraron que los archivos que habían descargado correspondían a una lista de credenciales provenientes de dos steelers si os acordáis los estilos son programas maliciosos una especie de virus que se dedican a recopilar todos los credenciales de los ordenadores y enviárselos a los malhechores a los ciberdelincuentes Y estos luego los ponen a la venta es decir te pueden infectar el ordenador de tal manera que en vez de simplemente pues hacerte un ataque ranso morital pues se queda el software recopilando credenciales cada vez que detecta que vas a entrar en un banco que te vas a lograr en algún sitio y los va enviando sin hacer más ruido sin hacer más nada pues a la persona que te lo ha instalado Esto es lo que se llaman los steelers no los robadores que sería digamos la traducción literal Pues resulta que dos según grupo y b 2 contractos es decir ni siquiera eran empleados directos de Uber sino que eran subcontratados pues dos personas subcontratadas una en Brasil y la otra no recuerdo ahora mismo porque lo estaba mirando antes estaban infectados con dos estiras diferentes uno era el Viper y el otro tampoco me acuerdo pues con eso que simplemente está recopilando todos los credenciales y automáticamente se pone en webs por decirlo de alguna manera especializadas en la Deep web a la venta todos estos blogs y credenciales Pues el autor que que comprometió Uber consiguió los crediales de Uber comprando los logs que estaban a la venta que se habían recopilado a través de los estilos que habían sido instalados por otras personas en dos de los ordenadores personales de estos contractos que utilizaban para hacer trabajo temporal para Uber toma ya y esto lo confirmó Uber en su en su escrito que acaban de publicar hace lo dicho hace unos minutos por tanto ahora ya sabemos que el acto 1 el obtener los credenciales de Uber ha sido a través de comprarlos en la Deep web Así que ni siquiera tuvieron que hacerle ingeniería social y no os creáis que todos estos vlogs valen mucho dinero No sabría deciros ahora la cifra porque no lo he visto todo es súper reciente pero a lo mejor por 50 dólares ya lo puedes comprar o sea no estamos hablando de miles y miles de dólares Así que aquí en vivo y en directo actualizando la noticia señores nos llega nos lleven las noticias nos lleven las actualizaciones estamos hiperconectados pero sí lo que dice Martín sí esos creo que se lo llaman

los iniciales Brokers se dedican solo a robarques reales para penetrar el perímetro y eso sí Yo creo que valen las credenciales están por 25 dólares Entre 25 y 50 seguro que están por ahí sí porque yo recuerdo de haber visto algunas por ese estilo me ha hecho interesante lo me ha hecho gracia es que has dicho que estaban comprometidos los ordenadores personales de esos dos eran personales o eran digamos los que había eso eso es lo que pone es lo que pone Google de hecho puedo intentar otra vez mientras estamos hablando aquí un segundo ir al tema pero es que lo leí hace un ratillo Pero pero bueno ahora justo no encuentro el enlace pero el tema es que sí sí O sea pero sobre todo es interesante una vez más ni siquiera engañaron a empleados de Uber sino ampliados subcontratados o sea una subcontrata tiene sus empleados Uber los contrata a ellos y Y esto es lo que pasa como tienen bastante acceso o si no está bien controlado pues ya está Mira lo estoy leyendo mira aquí está Iris likely Daddy attakers de contractors Uber corpore password In The Dark web after the contractors personal device hotwing infected with malware expositions por tanto efectivamente en el comunicado oficial de Uber menciona que uno de los de los contractos es decir uno de estos empleados subcontratados tenía su ordenador personal infectado y de ahí se sacaron los credenciales para acceder a Uber una vez más aquí tenemos un problema muchas empresas lo que hacen Esto me consta porque he trabajado en varias cuando subcontratan a gente les envían portátiles propios de la empresa para hacer ese trabajo y están súper monitorizados súper controlados y Súper restringidos de hecho muchas veces hay pues soluciones directamente en las nubes en las que acceden a máquinas virtuales que todavía pues se puede monitorizar más pero parece ser que en este caso Uber decidió aceptar que que la gente supro tratado pudiese utilizar sus ordenadores personales para hacer trabajo corporativo No pues qué pasa que de 9 a 5 estás trabajando en con acceso ilimitado ahí a los sistemas de Uber y luego a la noche te instalas software pirata para Ver pelis de Netflix sin pagar y entonces Esto es lo que pasa los peligros del brindieron device entre el propio dispositivo hay que Exacto Pues bueno queridos oyentes esperemos que como siempre os haya gustado el episodio y si es así tenéis una manera muy sencilla de mostrarnosla simplemente compartirlo con un amigo vas ahora y te pones a pensar según escuchas nuestra voz y dices a quién le podría interesar Escuchar estos podcast Kim quién quién podría beneficiarse de esto a quién le gustan las historias de hacking en este caso reales sin ciencia ficción pues mándale un mensaje Dile Hola Qué tal Cómo estás Mira una cosita tierra de hackers es un podcast súper guapo Por qué no lo escuchas eso creáis o no queridos oyentes nos ayuda un montón Porque nos ayuda a crecer y a ganar más visibilidad como espíango diciendo siempre sí sí muchas gracias si lo podéis compartir como dice Martín nos ayuda nos empuja para adelante nos ayudan en todas las listas y llegar a más gente pues hasta aquí Hemos llegado nos vemos y nos escuchamos la próxima semana en el próximo episodio Pues eso lo he dicho Hasta luego nos vemos pronto adiós 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