Cold River es un grupo de ciberdelincuentes muy sofisticado que opera directamente bajo las órdenes del gobierno Ruso y que recientemente se ha centrado en comprometer centros de investigación nuclear un erizo de mar de lo más punzón en la campaña fraudulentain el grupo cibercriminal automated Libra ha creado miles de cuentas en proveedores de nube saltándose los retos captcha para minar criptomonedas de forma totalmente gratuita mediante el uso de tarjetas de crédito falsas o robadas listo el episodio de esta semana con sus dosis habitual de ciberdelincuencia comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 15 de enero de 2023 este es el episodio número 79 yo soy Martín vigo y está conmigo Después de finalizar su periplo por España el neoyorquino Mister Alexis porras qué tal Alexis de tonterías muy bien muy bien querido Martín Pues nada a Mitades de enero de 2023 tiempo pasa volando y como decías por Nueva York yo me he defraudado al volver bueno está por aquí con frío pero sin nada de nieve Así que algo sorprendente para esto a estas fechas no porque nieve Nueva York Navidad enero febrero Pero bueno el cambio climático que ya sabemos Pero nada yo me quería ir a hacer snowboard y parece que aquí en Europa las estaciones de esquí y están básicamente para cerrar Sí para para irse a tomar un café y admirar las montañitas y volverse para casa Ya ves pues era no estamos aquí para hablar de esto sino de las noticias fresquitas de ciberseguridad Pero antes de ello lo primero es lo primero queridos oyentes queremos daros las gracias por estar siempre ahí apoyándonos episodio tras episodio en escuchándonos obviamente y en redes sociales donde nos enviáis vuestros comentarios sugerencias preguntas y misceláneos os recordamos que si no lo estáis deberíais estar suscritos a nuestro podcast en vuestra plataforma de escucha favorita también nos podéis seguir en redes sociales Twitter infoec punto exchange el servidor de mastodon que ya nos han preguntado por esto así que a partir de ahora lo voy a mencionar todo Instagram Facebook con el handle @tierra de hackers linkedin YouTube y Twitch como tierra de hackers correos electrónicos a podcast arroba tierra de hackers.com y en discord podéis conectarlos al servidor a través de tierra de hackers.com barra discord mencionar sobre lo demás que todavía estamos un poquito ahí baby steps como se dice no poquito a poco pero vamos a ir también dándole cariño a esa red social y finalmente como siempre agradecer vuestro apoyo a la pregunta del episodio que en el anterior fue la siguiente quién Debería ser responsable de los daños ocasionados por vulnerabilidades explotadas por potenciales ataques de seguridad como ranson Will contra vehículos conectados para refrescar brevemente la memoria el hipotético ataque de ranson Will y digo hipotético porque todavía no se ha reportado ningún ataque de este tipo era aquel en el que el usuario de un vehículo se quedaría sin poder utilizar el automóvil a no ser que se pague el rescate para que el cibercriminal desbloquee el motor de arranque teníamos cuatro respuestas la más votada fue empresas de automóviles deberían ser las responsables con un 75%, seguida de empresas de ciberseguros con un 15% seguida de gobiernos con un 6% y finalmente 4% consumidores quiero comentar brevemente tres comentarios de Twitter que bueno me ha hecho gracia que al menos los han escrito como mensajes en directo directamente públicos ahí no pero un usuario comentaba que empresas de automóviles deberían revisar su software en busca de vulnerabilidades y parchearlos Totalmente de acuerdo otro usuario comentaba en poco más de broma pero un poco más de verdad es lo más fácil es echar la culpa a Pedro Sánchez y Pablo Iglesias algo así la idea era que los gobiernos definieran Marcos legales y los hicieran cumplir o con sanciones más que echar la culpa no pero sí poco poner las pilas y luego hay otro que comentaba un poquito básicamente decía todos son responsables menos nosotros los usuarios claro Empezando por lo más importante serían los fabricantes de automóviles luego

los gobiernos con legislación y castigos digámoslo así y finalmente las aseguradoras Yo creo que es un poquito lo más acertado no que en todo en ciberseguridad en ciberseguridad no hay una opción mágica que resuelva el riesgo al 100% sino que hay que aplicar mitigaciones en múltiples capas estilo capas y de cebolla no estilo lo que decimos defensa en profundidad defensa en capas sí efectivamente Pues yo como siempre bueno como siempre como la otra vez disculparme si escucháis un poquito de eco pero todavía estoy aquí montando mi nuevo nidito Así que todavía está todo bastante vacío y y mencionar que lo puse lo puse en discord lo puse en Twitter el tema de que vamos a estar colaborando con un par de conferencias que las anunciaremos probablemente en el próximo episodio Porque todavía estamos cerrando ahí unos flecos sueltos que nos quedan pero lo más importante para vosotros queridos oyentes es que con suerte podremos conseguir algunas entradas para para sortear Y bueno pues es una manera de devolveros y daros las gracias por escucharnos si os podéis llevar alguna entradita son conferencias que serán en España tenemos muchísima una aplastante cantidad de gente en Latinoamérica que en este caso pues les va a quedar un pelín lejos pero bueno seguramente ya iremos creciendo por ahí en cuanto a colaboraciones también por por esa maravillosa zona del mundo una pregunta solo por tampoco hace falta que como todavía no los flecos todavía lo cortando no en solo para dar una pista son conferencias de ciberseguridad no y no sé si alguna tiene Sí sería a ver que si Oye si nos quieren si alguien quiere colaborar por no sé una conferencia de modelaje de perros pues Oye pues Oye a lo mejor tenemos se puede hay que tener varias facetas varios gustos varias maneras de pasar el tiempo no todo va a ser hacking no pero bueno sí son de fibra y lo otro es no sé si alguna también ofrece la modalidad en modo remoto que mira igual los que están más lejos pues se pueden beneficiar Sí bueno en este caso creo que no creo que en este caso las entradas serían para acto presencial y no creo que haya streaming pero si no bueno ya os iremos informando cuando sepamos un poquito más así os vamos poniendo los dientes largos y nada pues también aprovechar a darle las gracias a nuestros mecenas de patreo la gente que nos apoya no solo como todos que nos apoyáis el podcast sino además económicamente de hecho una de las ventajas es que cuando tenemos concursos de estos reservamos específicamente un número de entradas o de lo que tengamos para repartirlo solo entre la gente que nos apoya Pues un poco para dar un beneficio añadido a apoyarnos Así que muchas gracias estar al tanto y también gracias a nuestros sponsors como mona de una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast mona a través de una herramienta de gestión y visualización de telemetría y datos de seguridad a una empresa fundada en silcon Valley que está buscando muchos ingenieros siguen buscando gente porque van como un cohete Así que si queréis trabajar en remoto si de verdad se os da bien Esto de la ciberseguridad mandarle el currículum a tierra de hackers arroba monat.commod de dedo.com Y en este caso también nos apoya un branding es que son muchas las víctimas que nos suelen escribir por redes sociales debido a que pierden sus cuentas o sufren casos de acoso online pues son branding es una empresa formada por especialistas en varios ámbitos que se enfoca en la reputación online han ayudado desde personas como tú y como yo hasta famosos a recuperar cuentas comprometidas en redes sociales llevar a juicio casos de fibracoso ayudar a empresas en situaciones donde su reputación estaba dañada estaba siendo dañada e incluso borrar la huella digital que dejamos online no Solo han decidido Apoyar el podcast sino que si le contáis que venís de parte nuestra tendréis un descuento especial en sus servicios si necesitáis ayuda recuperando vuestras cuentas o reputación online ya sabéis o branding punto es y no os olvidéis decirle que

venís de nuestra parte y ya nos vamos al lío que nos alargamos Parece Mentira que ya casi ha pasado un año desde que en tierra de hackers empezamos a hablar de la guerra entre Rusia y Ucrania un año de fake news bombardeos y muertes que parecía que no iba a durar mucho y que ahora parece que no tiene fin y es probablemente por esa razón por la que ya en varias ocasiones el presidente Putin ha hecho declaraciones públicas dejando entrever que estaría dispuesto a utilizar armas nucleares si hiciera falta sobra decir que esto sería catastrófico Y si bien ahora mismo los países con capacidad de efectuar ataques nucleares utilizan esa capacidad como arma puramente disuasoria no podemos descartar que en palabras del propio presidente se utilizasen para invadir a otro país pues puede ser coincidencia o puede no serlo pero recientemente se ha descubierto que un grupo de ciberdelincuentes altamente sofisticados ha estado intentando hackear tres laboratorios estadounidenses dedicados exclusivamente a la investigación nuclear Cold River es el nombre de este grupo que lleva operando desde 2015 y que de hecho es un viejo conocido para la industria de la ciberseguridad se sabe que opera bajo órdenes del kremlin Y como decía casualidad o no las fechas en las que empezaron su campaña para hackear a científicos nucleares cuadraba con las amenazas públicas de Putin sobre la posibilidad de usar armamento nuclear contra Ucrania ojo en septiembre y octubre del año pasado concretamente Cold River se centró en comprometer los laboratorios brookhaven argón y Lawrence Livermore National laboratories las fechas vienen dadas tras un análisis por parte de reuters la empresa este medio de comunicación en conjunto con cinco empresas de ciberseguridad que vieron como en esos meses se crearon páginas de login falsas que se hacían pasar por la de estos laboratorios dedicados a la investigación en temas nucleares no solo eso sino también se observó el comienzo de una campaña de Spears fishing específica contra científicos de esos mismos laboratorios con enlaces maliciosos a las páginas falsas todo esto en ese Rango de tiempo de septiembre y octubre que insisto coincide con cuando Putin empezó a mencionar esto de la posibilidad de utilizar armas nucleares el objetivo claramente de Cold River era engañar a los científicos con páginas que eran iguales a las del laboratorio para el que trabajaban y que introdujesen su nombre de usuario y contraseñas para esto cayese en manos de el grupo de ciberdelincuentes Cold River pero vamos a profundizar un poco más en Cómo configuraron estas webs Y sobre todo cómo diseñaron la campaña de spir fishing para incrementar las posibilidades de que algún científico confiase en el email hiciese clic e introdujese sus credenciales en la web falsa bien col River lo primero que hizo fue registrar dominios que a simple vista parecen iguales a los verdaderos esto quiere decir que en caso de que se fijasen por ejemplo en mi web que es Martín vigo.com que en este caso El dominio más típico.com pues evidentemente no está disponible para ser registrado porque lo tengo yo pues registrarían dominios como Martín vigo.com pero en vez de la i una l minúscula que se parece muchísimo a la y cuando lo miras o por ejemplo un cero en vez de o de mi apellido vigo Y entonces sería Martín Big 0.com Pues eso eso mismo pero para las webs de los laboratorios también de hecho encontraron que registraron otros dominios como guion link.online y online 365 guión office.com que claramente pretenden ser dominios legítimos de Google y Microsoft muy parecidos por ley todos los dominios públicos registrados en internet tienen que estar asociados a una entidad o persona con nombre dirección y teléfono claro otra cosa es que esa información sea correcta sea la cierta ya que es la propia persona que registra El dominio que da esos datos insisto yo cuando registre Martín vico.com como parte del proceso de registro yo tengo que dar mis datos personales otra cosa es que si alguien lo hace de manera maliciosa de los datos reales no tiene por porque eso tampoco es que se coteje Pues bien esta información es pública y se puede consultar

fácilmente es lo que se conoce como hacer un juez a un dominio lo que te muestra los datos personales de quien lo registró tú como persona que registró El dominio puedes pedir que esta información Se oculte al público pero no siempre se hace o más común todavía se hace al cabo de unos días después de registrar El dominio incluso de unas horas Pues porque te has olvidado y precisamente existen muchas empresas de ciberseguridad que se dedican a escanear todo internet recolectando la información de wish de todos los dominios y también su historial de cambios si te has olvidado de ocultar esa información y días más tarde vas y la ocultas porque te has dado cuenta es posible que algún motor de búsqueda de alguna de estas empresas de ciberseguridad ya haya indexado tu dominio y almacenado los datos personales correspondientes pues usando estos mismos datos de Who is y de manera totalmente incomprensible dado que se trata de un ciberdelincuente Los investigadores fueron capaces de identificar una dirección de correo electrónico personal de un ciudadano ruso que estaba asociada a muchos de los dominios falsos registrados por el grupo de delincuentes Cold River esta dirección de email pertenece a Android Core nets un empleado de 35 años dedicado a la administración de sistemas informáticos y bodybuilder también por cierto que viven una ciudad al norte de Moscú para que os hagáis una idea esto es como si yo voy a cometer voy a robar un banco y antes de robarlo alquilo un coche con el que voy a ir a robar el banco y lo alquilo a mi nombre en vez de bajo un nombre falso Claro en cuanto alguien tenga la matrícula pues ya va a saber quién lo ha alquilado pues esto es un poco el equivalente de lo que hizo esta persona pues utilizando un email Los investigadores consiguieron encontrar un rastro muy grande de la vida digital de esta persona como sus redes sociales perfiles de aplicaciones de citas e incluso su perfil en una aplicación de ejercicios musculares donde se puede ver que es capaz de levantar 150 kilos empresas de banca ahí es nada el tío Ruso y además está cachas yo escuché una vez un monólogo que era buenísimo que era Cómo era venía a decir que de los hombres de las personas de piel blanca los que más los que más miedo dan son los rusos por su acento yo creo que se Estaba preparando para como tú dices para alquilar un coche que a su nombre y llevarlo hasta estos De laboratorios y llevarse las cabezas nucleares se las llevaba como mancuernas ya te digo tío es que es verdad que los rusos tío cuando hablan es que dan miedo ese monólogo era buenísimo no me acuerdo dónde lo escuché Si eso lo pongo en las notas del episodio Pero bueno es lo que tiene compartir todo en internet no que cualquier día decides dedicarte a la delincuencia y se hace público todo sobre ti más interesante que el peso que levanta o las fotos que pone para traer a mujeres es el hecho de saber que Android era una figura muy importante en la comunidad de hacking de su ciudad y que era asiduo a foros underground de hacking también había escrito en cines de temática hacking varios artículos de hecho él llevaba un cine de su propia ciudad llamado underground issen que significa es básicamente la ciudad donde vive el que como decía está el norte de Moscú de hecho uno de los investigadores buscó uno de sus artículos Y decía lo siguiente este Android son muchos los problemas asociados con los ordenadores e internet que causan problemas a la gente en general hay una barrera de desconocimiento y una situación desfavorable para la sociedad pero peleemos y aprendemos fac de System que le jodan al sistema básicamente pues vemos aquí que es un poquito también el rollito cripto anarquista no quizá Aquí es donde empezó a irse un poco hacia el lado del mal también hallaron en su perfil en una web donde se anuncia la gente para hacer trabajos de freelance no un poco como adword o fever o alguna de estas su perfillista estaba trabajos previos como la creación de una web de venta de esteroides para ayudar el crecimiento muscular o sea que el tío ya se había hecho la web también con vendiendo esteroides totalmente

ilegales pero todos los hallazgos que se hicieron sobre él gracias a su email me quedo con uno su cuenta de Twitter y os preguntaréis Por qué Pues porque la utilizaba mayormente para postear mins memes sobre Palomas o sea vale su cuenta de Twitter era sobrepalón era su dieta Como así les voy les comen mucha proteína bueno sin ser súper experto pero igual comía palomas ahí con arroz y tal Uy sí a lo mejor en la ciudad esto donde vivía ahí en medio de la nada no llegan las pechugas de pollo Bueno estamos hoy así un poquito con humor racial Por así decirlo pero siempre desde el humor por supuesto todo esto era Blue very Five en Twitter o qué Pues no lo sé porque de hecho cuando que esto lo mencionaré después Bueno lo menciono Ya ahora una de las cosas que hallaron fue también su teléfono y los y los periodistas le llamaron y consiguieron hablar con él una vez donde él admitía que él era el dueño de estos emails Pero él decía que no tenía nada que ver con Cold River Y que nunca había hecho nada de hacking que solo lo hizo una vez cuando tenía 15 años y se metió en un lío Y tuvo un juicio y tal y cual y de hecho el artículo menciona que el kgb es famoso por hacer recruit o sea por emplear no O por ofrecerles trabajo a delincuentes relacionados con la ciberseguridad O sea que no que con lo que dijo casi que corrobora aún que probablemente era él que no me acuerdo porque te estoy contando esto que cuál eras tú en Twitter que se había apagado y además proporcionado su info personal No pues claro yo me acuerdo porque decía esto porque los periodistas mencionan que después de esa conversación telefónica borró todo borró su perfil de tinder Bueno no sé si era tinder pero era una web de citas la lo de levantar pesas e incluso su Twitter Entonces no sé lo intenté ver no sé si tiene blueberry fire no a saber que si no lo que dices tú en vez de pagarlo con criptomonedas lo pagaría con su tarjeta de crédito la de su madre a saber Pero bueno que tenemos aquí un tío que está obsesionado con las palomas Pues a saber tío Pero bueno ahora que saquemos vemos Que call River registraba dominios parecidos a los de los laboratorios y que incluso lo hicieron en alguna ocasión con el email real para qué los usaban pues aparte de para mostrar la web falsa pidiendo nombre de usuario y contraseña enviaban correos electrónicos con un PDF a los científicos Y supongo que ya os estáis imaginando que ese PDF era malicioso Y contenía algún tipo de exploit Pero no es así de hecho me llamó bastante la atención la técnica que utilizaron y por eso la menciono en detalle en vez de un 0d y un PDF sobre todo porque hoy en día es ya más complicado meter malware en un PDF sin sin más sin que sea detectado col River enviaba pdfs normales cuya primera página mostraba un error que decía algo así como ha habido un error y no se puede mostrar la previsualización el tema es que no era un error en sí sino que la primera página del PDF la diseñaron así como si te lo escribes tú en Word y lo pasas a PDF y debajo había un recuadro a modo de botón que ponía ver documento o abrir archivo es muy ingenioso si lo pensáis porque el PDF no tiene nada malicioso en sí y qué pasa con el resto de las páginas del PDF pues esto es lo pensaron muy bien también el resto de páginas contenía palabras sueltas y desordenadas que estaban distribuidas por por toda la página y en varios colores presuntamente para dar la idea de que el archivo estaba corrupto y solo se veía parcialmente y por tanto pues dándole al botón lo verías bien y por supuesto si le dabas al botón te mandaba la página maliciosa que te pedía los credenciales insisto Me parece muy muy ingenioso porque aún con todo esto que os he contado no hay nada malicioso en Sí en ese email El dominio es legítimo aunque se parezca mucho al Real es legítimo el PDF no tiene nada malicioso no tiene nada embebido ningún malware y el email es un simple PDF enlazado sin más la verdad es que es muy guapo la cuestión es que consiguieron engañar algún científico robarle credenciales usarlos para acceder a los sistemas internos de algún laboratorio y robar algún tipo de información confidencial o creer algún tipo de daño pues

lamentablemente no os lo puedo confirmar O bueno sí En realidad no pero sí a ver os explico reuters se puso en contacto con los tres laboratorios afectados y dos de ellos se negaron a hacer declaraciones y el tercero solo comentó que reuters debía dirigirse al departamento de energía de los Estados Unidos para ese tipo de preguntas el cual a su vez se negó también a hacer ningún tipo de declaraciones esto de que todos los afectados por esta campaña de phishing se haya negado a declaraciones a mí personalmente pues me da mala espina pero lo dicho eso no quiere decir nada y por tanto pues no sabemos si con River fue capaz de comprometer algún laboratorio hagan sus apuestas queridos oyentes cabría también debatir qué es lo que estaba buscando los ciberdelincuentes con el acceso a esos sistemas internos de Laboratorios dedicados exclusivamente a la investigación nuclear y aquí da para debate Qué era lo que buscaban teniendo acceso propiedad intelectual A lo mejor pues cómo hacen las armas nucleares Los Americanos o qué tecnología utilizan que piezas específicas o que vendors no para conseguir esas piezas o a lo mejor era más en torno a conocer mejor a su enemigo no que el enemigo número uno de Rusia es Estados Unidos Quizá para saber qué capacidad nuclear real tiene Estados Unidos en caso de que Rusia decidies atacar a Ucrania A lo mejor para saber Oye si nosotros les atacamos estos pueden lanzarnos de verdad bombas desde el otro lado del mundo y tal o a lo mejor como de lejos están tecnológicamente Rusia respecto a Estados Unidos en el llano en la carrera hacia el armamento nuclear que ya la han alcanzado sino en digamos en lo más novedoso no O misiles de alcance a todo el planeta cualquier punto en el planeta o quizás se me ocurre también algún tipo de Niall of service no algún tipo de simplemente para sabotear o boicotear las capacidades nucleares de Estados Unidos pensemos que a lo mejor a estos laboratorios pues forman parte de El lanzamiento quizá de Estas armas nucleares en caso de conflicto bélico o a lo mejor simplemente se trata de un concepto como de célula durmiente en el sentido de que simplemente querían ganar acceso para estar ahí esto lo hemos visto en los delincuentes en otros apts que habían estado hasta años metidos en redes de corporaciones estadounidenses esto lo hace mucho china simplemente pues para aprender y observar no para realmente corromper nada ni robar simplemente querían observar comunicaciones que estaba pasando y mantener digamos el acceso al largo plazo no sé si eso os Ocurre algo más pero de hecho podemos hacer la pregunta del episodio al respecto vamos a formularla algo así qué creéis que era el objetivo de Cold River a peter ruso a las órdenes del kremlin al intentar Acceder al laboratorios estadounidenses dedicados a la investigación nuclear y os doy cuatro opciones la primera el robo de secretos como mencionábamos la segunda pues conocer al enemigo la tercera opción Sabotaje y la cuarta célula durmiente Y como siempre @tierra de hackers en Twitter no olvidéis seguirnos estamos muy cerquita de hecho de los 10.000 y ahí podéis poner vuestra votación contestar debatir y todo eso que Mola tanto de haber creado una comunidad tan gigante en torno a este podcast muy chula la noticia de la paloma digo del ciber criminal que no me lo puedo sacar ya de la cabeza yo de verdad que Estaba preparando así de varias fuentes la noticia y aparecía una Tibe y digo se me empecé a reír y digo pero cómo que de memes de palomas Qué cosa más Random Pero oye que no sea que estuviera me esteganografía en las imágenes estas de Paloma si alguien las estuviera consumiendo a lo mejor era un canal canal oculto de contraindicación para sus command en control a través de palomas Palomas mensajeras claro tío Oye ostras cuidado eh Por cierto ahora eso palomas mensajeras y tal No sé si sabes o si la audiencia lo sabe bueno internet Bueno viene todo de esto del darpanet no que era un proyecto militar de Estados Unidos y luego para definir protocolos y demás salieron estos los rfcs no request Force comments no sé es como un documento de diseño en el que se dice Oye IP va a

funcionar el internet protocolo a funcionar así Asa entonces la gente los expertos dan su opinión y se mejora no le dan vueltas Pues hay uno de ellos uno de estos rfcs que es broma que es de comunicación o sea comunicación por internet a través de humo tambores o palomas algo así Creo que es no sé si las he escuchado no lo había escuchado eso pero lo que sí te digo es que la latencia y el ancho de banda va a ser poquito mira lo acaba de encontrar está buscando rápido y se llama es el rfc es el 2549 y se llama es del 1999 y se llama IP over avian careyers with Quality of service es decir el protocolo de internet sobre portadores aves que sean aves o sea eso funcionaría sobre palomas sobre loros sobre lo que quieras Qué te parece Qué bueno Oye en la en no sé si era en la Primera Guerra Mundial o en alguna de estas lo de las palomas mensajeras era cierto lo que pasa es que era solo tenías un problema que era solo one way era solo una dirección porque se llevaban Las Palomas y Las Palomas lo único que sabían era volver a casa pero no les podías contestar para que volviese la paloma donde a desde donde la enviaba el soldado está bien Sí hombre en tiempos duros tío Pues sí muy interesante imagínate hemos acabado hablando de un protocolo sobre Palomas mensajeras Pero está bien un tema me ha apuntado dijiste que el email que descubrieron estas empresas que es muy interesante el tema de monitorización del cambio del estado de los dominios dns identificaron un email que previamente que habían asociado previamente con actividades a col River No sí efectivamente te habían detectado hasta 80 dominios maliciosos asociados a Cold River y hasta creo que cinco de esos dominios están registrados con un email real que era el del Andrew este Y supongo que en el pasado no se les fue a dar un poco a intentar contactar indagar un poquito más con ese email y contactar con esta persona y fue ahora en esta investigación en la que han dado ese paso más allá no puede ser eso o puede ser que justo los dominios que se utilizaron para lo de los laboratorios que esta es la parte reciente del ataque son los que lo tuvieran la verdad es que o no lo apunté mientras me documentaba pero yo diría que los artículos que leí un hilo de Twitter que como siempre enlazo en las notas del episodio no hacía referencias qué dominios específicos contenían ese email Así que No sabría decirte vale No era por digo si esta información ya la tenían antes igual hubiéramos tenido el tema del cachondeo con la paloma antes en otro episodio Pero bueno Y luego el otro es el tema de los dominios dns estoy Creo que ya lo hemos comentado en algún otro episodio ahora no recuerdo cuál pero el tema este de por ejemplo hay O sea hay una forma que es la que tú has comentado hacer un poquito el crear registrar un dominio que se parezca al que quieres impersonal que en inglés lo llaman taipo squating o ataques homógrafos o como lo quieras llamar no Y para esto hay de hecho hay herramientas que se pueden utilizar que te hacen todo el análisis de los servidores dns una que es bastante popular se llama twist que se puedes cargar de guiza la puedes correr y tal Así que yo justo ese fue fue el que utilicé pero una versión web que se llama creo que era tienes twister.com o algo así y pones un dominio y te dice todos los que están disponibles y se parece un montón con caracteres que se parezcan mucho Pues eso pues de hecho en lo que tú en este caso como medida de siempre nos gusta dar un poquito medida de recomendación no un poco para evitar que pase esto a las empresas una idea sería Oye usar esta herramienta y mirar a ver los que se parezcan más que te devuelve y que están disponibles para registrarlos y Oye si no valen mucho Es que a veces se abusan un poco estos estos estas empresas que ofrecen el registro dns y un dominio que no tiene sentido mil dólares yo lo he visto eso digo pero si pone aquí comprar Donuts con sabor a chocolate.com Pero cómo pones que valga mil euros No pues nada pero los que más o menos en función de vuestro riesgo apetito y capital pues podríais registrarlos para que no os hagan Estos tipos de ataques sería una medida un poquito para

prevenidos y el otro tema también Es que quería comentar que en otro episodio esto lo comentamos el tema de lo podríamos Llamar los dominios dns de crianza no como el vino es eso del tema de cultivar dominios dns para que tengan una buena reputación hay sitios web online que venden estos dominios porque un tema es que se cree un dominio de nuevo que no tiene vida no tiene como cuando vas a pedir una tarjeta de crédito te dice Oye a ver cuál es tu historial de crédito que has comprado en el pasado algo así pues o como Bueno cuando vas a buscar trabajo no soy soy Junior y pedís aquí dos años y tal pues no te cojo Entonces si registras coges Hay alguno de estos que tienen un dominio de crianza que se parece al que quiere es impersonal Oye pues mucho mejor que mejor así que también sería otra forma ir a mirar si alguno de esos y lo podéis comprar en lugar de los cibercriminales o Bueno un poco para monitorizar y saber vuestro vuestro modelo de amenazas como siempre decíéndolo y nada pues esos son mis comentarios y si quieres vamos para la siguiente noticia Martín procede procede vamos para adelante pues lo que traigo va de free jacking y ahora comento Qué significa este concepto un grupo de cibercriminales de Sudáfrica en concreto conocido como automated Libra ha estado abusando de recursos de prueba o cuentas de prueba en la nube para lanzar campañas de minería de criptomonedas algo como digo que se llama free jacking el nombre viene del inglés y en este caso combinación de free gratis obviamente y jacking un poquito el sufijo de High jacking digámoslo que sería como de secuestrar o robar No pues si lo combinamos sería una traducción posible sería robo de recursos gratuitos y realmente de esto se trata el suceso de cibercriminales abusando de los recursos gratuitos de nuevo free no es algo nuevo y ya se ha informado al respecto antes de hecho esto ha provocado que muchos proveedores de continuos integration y continuos Delivery o deployment que básicamente se refiere a un proceso en el desarrollo de software de automatizar todas las tareas de compilación análisis de código empaquetación y despliegue no pues En plataformas de si hay CD como se le dice como github o heroku cambiaron su enfoque de las cuentas de prueba a raíz de Estos tipos de ataques este tipo de ataque llamado free jacking es decir que en lugar de ofrecer más funcionalidades a cuentas gratis pues las han hecho más cortas en duración de tiempo o con menos cantidad de recursos en lugar de 16 Gb de ram 8 GB de ramo menos o más limitaciones no para evitar que se aprovechen de Estos tipos de cuentas gratuitas y los intentos del proveedor de estos proveedores como githuberoku para evitar este fraude van desde hacer que sea más lento la creación de cuentas mediante el uso de captcha y otras tecnologías de prevención de Bots hasta requerir una tarjeta de crédito válida en el momento de la creación de la cuenta y saltarse estas medidas Es realmente la parte interesante de esta noticia Y cómo los cibercriminales han podido automatizar todo el proceso de creación de cuentas de prueba y lanzar su campaña fraudulenta de minería de criptomonedas lo que este grupo ha hecho es abusar de plataformas en la nube que ofrecen cuentas de prueba ya sea membresías con todas las funcionalidades o en algunos casos con algunas funcionalidades limitadas pero válidas sólo por un periodo de tiempo de prueba por ejemplo 15 o 30 días esto es una estrategia típica de marketing para atraer a clientes dejarles probar el producto o servicio y luego que lo compren o se suscriban cuando lo han probado y les ha gustado lo que suele pasar Es que para crear estas cuentas limitadas estas cuentas de prueba gratuitas las plataformas requieren que se proporcione una tarjeta de crédito o débito como modo de pago no permiten tarjetas de prepago solo crédito o débito y lo que los cibercriminales suelen hacer es utilizar tarjetas falsas o robadas O al menos eso es lo que comentan los investigadores normalmente cuando se crea una cuenta nueva las plataformas en la nube piden una tarjeta de crédito débito como digo en los detalles no el número de cuenta la expiración el código cvv hacen

un cargo temporal o simbólico de céntimos de dólar o de euro o de la moneda que sea en la tarjeta proporcionada piden al usuario que introduzca el valor de céntimos para confirmar que realmente posee la tarjeta sería como un código que te envían pero en lugar de enviártelo por email o al móvil te lo envían digamos en forma de cargo a tu tarjeta de crédito o débito Y si la confirmación es exitosa anulan el cargo temporal o devuelven dicho cargo al usuario porque Oye hemos confirmado es válido te devolvemos el dinero o anulamos el cargo temporal igual hay más Pero principalmente hay dos motivos por lo que los cibercriminales han podido abusar de esto con tarjetas robadas el primer caso sería que nunca se comprobó que la tarjeta tuviera fondos suficientes la tarjeta se valida cuando se registra la cuenta pero al final del periodo de prueba para seguir utilizando estos servicios pues Oye ahora ya no son gratis ahora te cobro Entonces el cargo no se puede realizar porque la tarjeta no tiene fondos suficientes el otro motivo es porque la tarjeta deja de ser válida y esto en la tarjeta se valida cuando se registra la cuenta de nuevo pero deja de ser válida cuando se realiza el cargo al final del periodo de prueba esto puede ser porque la cierran de forma legal o porque el usuario utiliza tarjetas de un solo uso Como por ejemplo hay servicios que ofrecen esta funcionalidad como puede ser privacy.com sobre el tema de tarjetas falsas puede ser que no se valide que la sea real y el sistema solo comprueba que la tarjeta tenga un formato válido como todos sabemos los números de tarjetas por ejemplo tienen 16 dígitos pues Oye lo que igual hacen estas plataformas miran que tengan 16 dígitos que la fecha de caducidad sea en el futuro y que el cvv pues tenga tres dígitos o cuatro en el caso de American Express uno de los motivos por lo que esto es posible es cuando digo esto es posible es abusar de esta funcionalidad a saltarse la verificación de la tarjeta de crédito o de débito es porque la tarjeta sólo se comprueba una vez al registrar la cuenta y no durante el período de prueba de vez en cuando no cuando el estado de la tarjeta puede cambiar y al llegar al final del periodo de prueba no es posible realizar el cargo a la tarjeta de hecho este caso ilustra muy bien un tipo de vulnerabilidad que en desarrollo de software se le llama Toc o Time Of Check To Time Of Us que significa que cuando se ha comprobado el estado de un componente en este caso la validez de la tarjeta o que tenga suficientes fondos la comprobación fue exitosa pero cuando realmente se va a usar este componente no se puede completar de forma exitosa es decir cuando se va a usar la tarjeta Esta no es válida o no tiene fondos suficientes a consecuencia de todo esto como digo por ejemplo un caso práctico es que a partir del 28 de noviembre de 2022 heroku ya no ofrece de forma gratuita algunos de sus servicios que ofrecía anteriormente como heroku postres que es una base de datos heroku Data para redes que es otra base de datos de formato key value llave valor digámoslo así y bueno y algunos otros temas que han ajustado para evitar tener fraude como como el que sucedió en este caso pero voy a entrar en detalle En qué pasó la operación se la ha llamado Purple origin es decir erizo morado no sé porque han puesto este nombre Porque Bueno ese es un nombre que como bueno como todos los nombres que le ponen de animales y le dan Algún color No pues esto Así es como lo bautizaron y esta operación salió a la luz en octubre de 2022 cuando Dick que es una empresa que se dedica y ofrece productos y servicios de seguridad en la nube y en contenedores como docker reveló que el grupo detrás de esta campaña automated Libra había creado hasta 30 cuentas de github 2000 cuentas de heroku y 900 cuentas de Buddy en estas plataformas de si hay CD plataformas en la nube para escalar su operación en un reporte más actual publicado por United 42 el grupo de inteligencia de amenazas de Palo Alto networks el grupo de cibercriminales creó se dice calcularon que creo de 3 a 5 cuentas de github por minuto en digamoslo en el apogeo de su actividad que fue noviembre de 2022 configurando creando más de

130.000 cuentas falsas entre github heroku y otra plataforma llamada tokelbox se estima que se crearon más de 22.000 cuentas de github en septiembre y noviembre y se han identificado un total de unas 100.000 cuentas en heroku donde se crearon más cuentas con heroku pero github también se lleva unas cuantas con 22.000 en el caso de github por ejemplo comentar que la cuenta de prueba gratuita ofrece 2000 minutos de github action al mes Estos son unas 33 horas de tiempo de ejecución de nuevo es una plataforma de continuos integration continuos development que de nuevo es una plataforma de ejecución de comandos en serie que se utiliza como digo para analizar corregir compilar y empaquetar código pero que se puede utilizar para ejecutar casi virtualmente cualquier Comando algo que los cibercriminales han aprovechado para minar criptomonedas para obtener estimaciones de costos para los proveedores de servicio de estas plataformas Los investigadores miraron los modelos de precios de las plataformas y compararon los límites entre las cuentas gratuitas con las de pago con respecto a los detalles como los minutos asignados en la cuenta gratis y lo que equivaldría en una cuenta de pago para las cuentas gratuitas se estima que Purple artching esta campaña necesitaría usar varios miles de cuentas gratuitas no ponen Cuántos varios miles así que bueno pongamos que 2000 el caso más optimista para ganar para crear una moneda de monero a día de hoy una moneda monero cuesta unos 176 dólares americanos asumiendo los costes de un usuario que tuviera que pagar por ejecutar las mismas operaciones con una cuenta de pago digamos el sistema la cuenta el tier el nivel más barato de todos los de pago el equivalente de esto sería unos 103 mil dólares americanos de coste así que crear para minar solo una moneda monero Así que si pudieron registrar 22.000 cuentas en github por cada moneda monero un valor aproximado de unos 176 dólares americanos a día de hoy pues por cada moneda monero los cibercriminales causaron a github una factura de 1,1 millones de dólares americanos digámoslo así de nuevo estoy asumiendo que para cada moneda monero utilizaban 2000 cuentas Así que haciendo las matemáticas si pudieron registrar 22.000 pues se llega al 1,1 millones de dólares americanos Por otra parte 6d estima que cada cuenta gratuita de github que crea automated Libra le cuesta a github 15 dólares al mes en este caso con esta Asunción si crearon 22.000 cuentas pues serían unos 330.000 Total que lo dejamos entre 330.000 y 1,1 millones Ese es el daño que recibió github en esta campaña cibercriminal Por otra parte las otras plataformas también se hizo un estudio de los niveles gratuitos comparándolos con los de pago y pues los investigadores concluyeron que pueden costarle a los proveedores entre 7 y 10 dólares al mes por cada cuenta a esta tasa le costaría a un proveedor más de 100.000 dólares para que un actor de amenazas extrayera una moneda monero según el análisis de United 42 que miraron 250 GB de datos de logs según comentan el inicio de esta campaña se remonta a agosto de 2019 y se han descubierto hasta 40 diferentes carteras de criptomonedas y siete criptomonedas que se han estado minando comentan que aunque uno de los balances impagados más grandes que fue de 190 Dólares pero recordemos son cuentas gratuitas que igual los primeros 30 días los primeros 20 días son gratis y luego hasta que se dan cuenta de que no pueden cobrarle pues incurren algunos gastos no con este caso la mayor que encontraron fueron de 190 dólares sospechan que los balances no pagados en otras cuentas y servicios en la nube de estos cibercriminales Podrían haber sido mucho mayores debido a la escala y amplitud de la operación también identificaron que los componentes específicos contenedores docker de la infraestructura que crearon los actores de amenazas no sólo se diseñaron para realizar la funcionalidad de minería de criptomonedas sino que también automatizaban el proceso de intercambio de criptomonedas en exchanges como cratex exchange Market crex24 y 1 no he escuchado nunca

nada de estos tres pero los que son más expertos criptomoneda igual os suena En conclusión la operación comentan que fue muy ofuscada y emplea la automatización a múltiples niveles con más de 130 imágenes de docker y cuentas de nuevo de diferentes proveedores de si hay CD como github heroku y similares que rotan regularmente en varias plataformas voy a comentar un poquito el tema interesante de la noticia que era el cómo registrarán las cuentas de forma tan rápida y sobre todo cómo se saltaban el captcha no Bueno pues para registrar las cuentas el primer paso es completar los campos de texto típicos nombre dirección de correo electrónico contraseña nombre de usuario similares no para ello los cibercriminales lo que hacían era lanzar un navegador Iron browser en este caso en un contenedor docker que habían que tienen ellos no en su poder luego usando una herramienta llamada xdo tool el Script que habían creado completa El formulario de github introduciendo el texto necesario después de darle a siguiente el formulario de github mostraba un desafío captcha Y de nuevo Esto es lo interesante no cómo se lo saltaron pues para ello han utilizado varias herramientas en un caso utilizaron como digo el navegador Iron browser que es basado en Chrome la herramienta x de otool que lo que hace es emular pulsaciones de teclado y clics de ratón y image Magic que es un digamos un conjunto de herramientas para convertir editar y componer imágenes digitales un caso curioso es el de El captcha con galaxias en este caso Comentan los investigadores que para resolver este captcha en particular que consiste en identificar galaxias en forma de espiral Supongo que os lo habéis encontrado alguna vez no sé en github en otros sitios que tienen caps yo lo he visto en persona he tenido que seleccionar la galaxia en sí los cibercriminales utilizaron una forma muy ingeniosa para automatizar la resolución del captcha y utilizaron dos herramientas de este conjunto de herramientas llamado image Magic la una que se llama Converse convertir y otra identify a identificar no lo que hicieron primero es bueno descargarse o coger las imágenes de todas las seis galaxias que se muestran luego las convirtieron en imágenes de rgb rojo verde y azul utilizando la herramienta convert de image Magic Una vez que se convirtieron las imágenes ejecutaron El Comando de identificar identify sobre cada imagen para extraer la característica de asimetría o sesgo en términos más técnicos pero del Canal rojo en concreto de la imagen en rojo el resultado final se ordenó de mayor a menor y la imagen con el valor más pequeño se seleccionó como imagen espiral lo curioso Es que la imagen con menor contenido de rojo es la imagen espiral correcta con esta automatización tan sencilla pudieron resolver el captcha con galaxias Qué te parece o sea flipo O sea si bien es cierto lo que dices tú que es sencillo lo que es implementarlo es el Cómo llegaron a esa Claro porque recordemos que detecta si eres un humano y no un robot y al final utilizar un robot en forma de Script para detectarlo O sea que eso está muy Guay todo el tema de investigación de saltarse captchas es muy interesante pero el tema de sé perfectamente de cuál hablas del de la galaxia Cómo llegaría me imagino que con mucha prueba no a ver que si tiene más rojo menos rojo Entonces es la galaxia está del lado correcto no O sea está con la espiral que tiene que estar sí yo eso o mira en el caso anterior era un ciber criminal con pasión por Body building en este caso debe ser algún cibercriminal con pasión por la fotografía y sabe que Oye podemos identificar la galaxia en el canal rojo si la descomponemos en los tres canales rgb no sé se me ocurre y este te iba a preguntar esto es captcha de Google porque sí que estoy familiarizar el típico de Google de los semáforos o los coches o el rollo el agua en las carreteras que identificarlo ese es el del recaptcha de Google pero este de este lo he visto las Galaxias pero este es un Open source No pues la verdad es que no lo pone estos detalles no te sabría decir estoy y otro y otro que hay otro que hay típico que es de elige la imagen que tiene el animal en la posición correcta que ahí yo creo que no valdría el tema de

detectar que hay un Pixel con un color porque es la misma imagen Solo que girada pero lo de la galaxia es la forma Sabes cuál te digo que aparece un perro y aparece un perro boca arriba un perro de lado y tú tienes que seleccionar al perro que esté pues como tiene que estar no con las patas para abajo pero estoy pensando que esa es diferente al de las Galaxias porque en las Galaxias las imágenes son diferentes mientras que en la de esta de animales es la misma imagen pero girada pues ahora que lo dices estoy aquí un poco mirando online y puede ser que sea el recaptcha de Google estoy viendo que también lo usan en otras plataformas como linkedin y incluso roblox pero si debe ser debe ser del de Google no lo menciona en detalle pero sí debe ser ese y bueno también ese es una de las formas porque también hubieron otras Esto es para el caso en que se muestra un captcha con imágenes que ya está no tiene otra forma de resolverlo Pero qué pasa para esos captchas que también son compatibles con personas que tienen alguna discapacidad No pues a los que te ponen la voz distorsionada no el audio distorsionado pues esos tienen también muestran un icono para utilizar el audio y que lo pueda escuchar la persona y decir Oye es esto y entonces hacer clic por si no pueden ver bien la imagen que esto es para los captchas para clarificar estos son para los captchas que te dice que pongas las letras no r9vt porque claro lo de lo de la galaxia no no hay versión audio de eso no pero las de las letras y números que están así con colores que cuesta verlo a veces Pues sí que tiene versión audio Yo tampoco lo sabía pero Aparentemente no me he fijado y no me ha salido ningún captcha desde que preparar noticias hasta ahora pero los de Google típicos estos que básicamente estamos entrenando a sus coches de conducción Autónoma no porque sale dime que si ves aquí los semáforos pues estos yo no me he fijado nunca igual lo hemos visto siempre tienen ahí como un icono de unos auriculares no sé qué te va a hablar y qué te va a decir pero Aparentemente te dan la opción de audio y es otra forma que han utilizado para saltarse los que se les han mostrado que que son de este tipo no es el de la galaxia pero los otros que tienen captcha de audio no De hecho hay una extensión llamada Buster para Google Chrome que la han utilizado para saltarse los captchas de estos dos proyectos que se llaman octo captcha y fan captcha que son captchas como decimos que utilizan captchas con audio también según la Google Chrome Store está Pues dice que ahí está extensión Buster ayuda a resolver captchas difíciles al interpretar desafíos de audio recapsa usando reconocimiento de voz los desafíos Se resuelven haciendo clic en el botón de extensión en la parte inferior del widget recapcha es decir te sale el de nuevo la imagen con una parrilla con muchas imágenes te sale el botón de refrescar el botón que nunca me he fijado de los auriculares y un botón que es el que añade esta extensión y que te ayuda a resolverlo comentan que no siempre funciona pero hoy es una ayuda No pues esta es una forma que han utilizado para saltarse los captchas que permiten también la opción audio y también de la misma forma que con esta extensión Buster otro método que utilizaron en esta campaña para eludir los mecanismos de captcha de audio fue un paquete de python que tampoco lo conocía llamado with w&t para el reconocimiento de voz de archivos de audio punto web otra forma que no han utilizado en este caso en esta campaña pero quería comentar es un servicio de resolución de captchas que es decir mediante humanos hay plataformas online a la que se suscriben humanos que quieren resolver captchas por un módico precio en mi tiempo libre pues a qué me dedico a resolver captchas que me entretiene mucho como quieren hacer sudokus es que es lo que estaba pensando que hay la versión de utilizar a humanos como robots para resolver captchas que detectan robot justo justo y cuando un captcha cuando un usuario quiere resolver un captcha Lo envía esta plataforma y uno de los humanos recibe la notificación de nuevo captcha lo analiza y devuelve la respuesta correcta resolviendo el

captcha finalmente Entonces el usuario que realizó la petición recibe la respuesta y selecciona la imagen que tenga que seleccionar pero todo esto que comento parece muy manual pero todo esto está automatizado hay apis que se pueden utilizar para enviar la petición recibir la respuesta y que tu Script tu programa seleccione la imagen en concreto para resolver el captcha después lo que hicieron otro tema interesante que me ha parecido digno de mención Es que después de completar el captcha en github envía en este caso un código otp de estos de One time password a su correo electrónico y para automatizar un poquito el proceso de obtención del código los cibercriminales utilizaron una cuenta de Gmail en la que habilitaron el servicio de imap y accedieron a su bandeja de entrada de Gmail a través de la Api de Gmail que con un Script en php atención no sé por qué usan php pero ahí lo dejamos no quiero entrar no entramos en guerras de muebles de programación pero en polémicas después de eso los cibercriminales proporcionaron el código otp y bola completaron el registro de la cuenta y el paso final Cuál es pues finalmente los cibercriminales Ya teniendo la cuenta en github configuraron su entorno de minería de criptomonedas pues crearon las claves ssh pertinentes los repositorios usando lápiz de github los permisos del repositorio e iniciaron el proceso de minería deployando digamos instalando los contenedores docker y scripts en bash Y php de nuevo y ya luego ya es profit beneficio sacar criptomonedas como he dicho e intentaron minar 7 distintas pero en la actualidad se han centrado más en monero y comentar un poquito el impacto de todo esto porque esto parece que no afecte a ningún usuario no me afecta a mí no me afecta a ti Martín y tal y como se dice en broma los cibercriminales no hirieron a ningún gatito durante sus actividades fraudulentas pero realmente en este caso ha afectado obviamente a git happeroku y otras empresas similares no sus facturas de servicios en la nube seguro que se han incrementado por las actividades de estos cibercriminales porque recordemos estas empresas bueno Y aunque no los fueran si fuera una empresa de nube directamente Pues también incurriría en gastos que tenía que pagar ella misma porque el usuario se ha esfumado y apagado pero os comento esto que sirva de lección para otras empresas y que si hay otras empresas que ofrecen servicios de prueba que realicen las comprobaciones de cuenta necesaria por favor Es decir modo de pago como tarjeta de crédito o débito y o que limiten los recursos disponibles en dichas cuentas de prueba para evitar facturas millonarias como ya hemos visto con casos de ransomware las empresas más pequeñas son las que más sufren En estos casos porque al no Tener suficiente capital para pagar el rescate tienen que cerrar un caso de free jacking como este el que mencionan esta noticia que abuse de empresas pequeñas Podría tener el mismo efecto hacer que la empresa no pueda pagar la factura de los servicios en la nube que los cibercriminales han disfrutado a su costa y tener que cerrar su negocio finalmente comentar que algunos analistas también especulan que esta operación a gran escala podría ser un señuelo para cubrir otras campañas que los mismos cibercriminales están orquestando al mismo tiempo y porque las cantidades no parecen ser tan elevadas como para causar un gran impacto pero sí para causar revuelo online en forma de noticias no Y para que las empresas afectadas dediquen esfuerzo y personal a la respuesta incidentes análisis forense y gestión de crisis y de esta forma evitar que otras actividades de mayor impacto que realmente están lanzando los cibercriminales puedan ser investigadas y detenidas Así que automated libra con su campaña es espionaje o motivación financiera Qué guapo tío el nivel de automatización es espectacular y una de las cosas que me doy cuenta es que incluso Podrían haber ganado dinero pero por lo menos para varias charlas en conferencias mega top de ciberseguridad o sea el tema de saltarte los captchas el sudas esa charlan Black en prime Time Por así decirlo por no hablar de otras técnicas pero me

parece espectacular y luego si tú Esto se lo pones al backbounty de Google también te va a pagar mucha pasta porque es que es una protección esencial para ellos sí no solo te lo va a pagar github sino que te lo paga te lo paga Google también porque al fin y al cabo estás comprometiendo uno de esos pájaros de un tiro no Dos palomas he estado rápido bien ahí metida con calzador tío no muy buena muy buena Yo sí Dato curioso también esto parece como el tema de los Bots bueno es esencial no para proteger un poco los servicios online Pero y parece que sea parte no sé de los desarrolladores no o de equipos de blooting de proteger Pero es que yo he visto que ya hay perfiles por ejemplo he visto algunas empresas de content Delivery Network de estas típicas No pues que están buscando tienen perfiles que están buscando que no me acuerdo el nombre Exacto del título no pero era como una persona que se dedicara solo a combatir Bots online un tema de acceso a apis o resolver captchas o hacer un poco la vida más difícil a detectar esto y un poco a prevenir el riesgo Así que es un campo que está está surgiendo se está poniendo más de moda Sí yo que previamente he trabajado en empresas de redes sociales no solo había perfiles sino equipos enteros dedicados a combatir el abuso de la plataforma que venía a ser un equipo para lo que dices tú o sea cómo se está abusando nuestro servicio no y mucho era pues las apis el scripping no el recolectar datos que están públicamente pero de manera masiva o los Bots esto ha tenido mucha visibilidad a través de todo lo que sucedió con elon musky Twitter no que estaba lleno de Bots que está lleno de Bots si es un tema de hecho yo había leído por ahí no recuerdo los datos lo voy a lanzar Así un poco al tun tun pero no sé No recuerdo el dato pero pongamos por decir algo que el 50% del tráfico en internet era basura spa mera Bots será era porquería y de hecho recuerdo un artículo hace años de Bryan crepes un periodista que se dedica se especializa en temas de estafas online de perseguir a grupos que se dedican eso Muchos y todo esto Pues que había el no sé qué no sé qué no sé si fue el FBI o algunos habían básicamente desmantelado la infraestructura de un grupo delincuente que se dedicaba a enviar spam a mansalva y se había notado en en los ponía una captura de pantalla de donde se mide se monitorea el tráfico por internet en cables transatlánticos y todo cómo había bajado o sea por solo desmantelar eso que había sido una operación coordinada se notaba en la Gráfica del tráfico mundial de internet una bajada dramática solo porque habían dejado de enviar spam tío o sea es que son millones y millones de correos electrónicos diarios llamadas telefónicas SMS ese abuso de apis es que es increíble tío O sea que los cibercriminales no solo reciben beneficio cuando roban capital por ahí sino que también están malversando o haciendo mal uso de nuestros impuestos no que van a mantener a internet también y quemando árboles tío que imaginar y entre todo esto consume eso consume consume internet claro luego las palomas no tienen donde posarse tío porque los árboles que claro tío qué hacemos con las palomas Bueno claro último comentario mira que quería hacer era que esto O sea tenemos el tema de los firewalls y tal que sería protección perimetral a nivel de red no tenemos los web application firewalls que serían también a nivel un poquito más de aplicación pero es que está un poquito el tema del captcha y tal no y de la protección contra Bots es un poco más protección perimetral pero más a nivel de lógica de negocio No así que tenemos ahí un poco más el digamos el firewall al mayor nivel abstracto de todos en este tema de Ciber se podría ver como bueno no como fire pero sí en parte lo de los captchas porque detiene no el acceso por parte de robots a la web que sería como un firewall que detiene el tráfico malicioso pero sí ya te digo me ha parecido me ha encantado en esta noticia que hayas detallado Cómo saltarse captchas porque yo cuando me presento a un captcha digo joder tienes que saber mucho de procesamiento de imagen para poder llegar aquí a hacer esto programáticamente es que es muy jodido que yo diría utilizando esas

técnicas cuando el de Google te dice Oye dónde está el rollito este del agua que no me sale Cómo se le llama eso donde los bomberos enchufan un hidro una conexión de hecho es bastante americano eso yo no sé ni si lo hay en España tío o sea es muy americano el rollo ese de tener ahí la Fuente para bomberos ya está boca de incendios pero eso es un poco absurdo no sería como la entrada bueno da igual boca de incendio yo creo que nuestros queridos oyentes han de lo que hablamos pues tío siempre son rojos y yo cuando ves la típica imagen joder es que parece que es lo único rojo en toda la imagen entonces digo yo si se podía utilizar la misma la misma digo yo que utilizaban ahí en tal Claro si en la galaxia que la galaxia es básicamente un arco iris de colores tío eso valía porque no va a valer ahí Ay era que mencionas eso otro tema que no he comentado antes pero me ha venido a la mente ahora es esta extensión que se llama Buster que está en el Chrome web Store que se utiliza para resolver hacks de Google qué hace ahí porque quizás Qué bueno tío sí eso sí Qué raro digo de hecho habían Bueno también hay hay creo que un acuerdo que medio se había llegado con los el tema de los adblockers no porque Google vive de poner Apps y haya Brokers para Google Chrome que dices tú stras pero aunque bueno eso ya no sería tu ejemplo es más claramente se está saltando algo una medida de seguridad Mientras que el adblocker es más quitar algo molesto no es más dentro de la ética más que de la seguridad pero creo que por eso ahora los adblockers en Google Chrome te dan la opción de permitir anuncios no sé cómo le llaman éticos o algo así no Entonces se transforma más en bloquearte anuncios claramente maliciosos o que vienen de redes de redes de anuncios que evidentemente están están relacionadas con el cibercrimen pero sí sí es Otra de esas que dices tú esto no le conviene seguro que querer no quieren tenerlo ahí Pero por otro lado A lo mejor si empiezan a banear saben que la gente les criticaría mucho es que tiene pone aquí 400.000 plazas usuarios O sea que no es que la use Una Pandilla de también Es verdad que Google Chrome Google Chrome te permite instalar un poco como Android no sino aunque no esté en la Play en la Google Store te la descargas desde git happ y lo instalas igualmente y si no te coges un chromium cualquier navegador quizás se dieron cuenta que ese plan tampoco es que nosotros tengamos el monopolio de los navegadores y no lo podamos permitir si no lo hace con nuestro lo hacen con otro pero sí que es un poco contradictorio es un poco absurdo es como es como si la Apple Store te tiene el exploit para hacer jailbreak al Iphone y te lo puedes descargar de la Apple Store es que no tendría mucho sentido Sí eso estaría bien pero no creo que no que siempre nos quejamos de que si el Google App Store es dejan pasar malware y tal en este caso es es blanco y en botella no bastante tiene reviews bueno queridos oyentes Gracias por quedaros hasta el final por echaros unas risas con nosotros Alexis y yo lo paso a caminar aquí grabando como siempre ayudarnos a seguir creciendo Gracias la semana pasada vimos un pico ahí de subidón de muchos de vosotros compartiendo el podcast de dejando en los comentarios y todo esto y es que se nota directamente ya en los charts en visibilidad en nuevos suscriptores en gente escribiéndonos hoy Acabo de descubrir el podcast gracias a que alguien lo comentó en Twitter Así que muchísimas gracias seguir haciendo lo que nos ayudáis muchísimo y os cuesta 10 segundos 15 un minuto máximo Y la verdad es que nosotros os lo agradecemos un poquito Muchas gracias y ahí quedaos a la espera de lo que se avecina con las conferencias tanto Ah que esa es otra muy bien dicho porque precisamente por la visibilidad lo que hemos crecido lo que seguimos creciendo nos vienen ahora a pues estas oportunidades de colaboración con conferencias con todo esto que nosotros primero nos hace una ilusión tremenda segundo al fin al cabo nosotros damos valor a nuestros oyentes pues ya ya es a través de concursos pero también de dar voz y visibilidad conferencias donde pueden ir y seguir un poco todo este tema de la pasión

de la ciberseguridad que al fin al cabo es por lo que vemos el podcast así que ya sabéis compartir es vivir compartir nuestro podcast y que eso seguro que resultan también beneficios para vosotros en pocas palabras que queremos que contagiéis a vuestra familia de tierra de hackers Así que nos vemos y nos escuchamos como siempre dentro de una semanita chao chao chao Muchas gracias 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 una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de la tierra de hackers