68. Especial conferencia VAG 2022

la industria de los videojuegos está estrechamente relacionada con el mundo de la ciberseguridad estafas robos vulnerabilidades abusos de privacidad y Zero days todo aplica también a tus juegos favoritos las vulnerabilidades y vectores de ataque han evolucionado Durante los últimos años y no afectan a todos por igual empresas gobiernos Vips y la gente común como tú y como yo somos objetivos de ciberataques pero con diferentes vectores y motivaciones hoy os traemos un episodio especial donde podréis Escuchar dos charlas que hemos dado este fin de semana en la conferencia Bach de videojuegos arte y gráficos esperemos que os guste comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 3 de octubre de 2022 este es el episodio número 68 yo soy Martín vigo y está conmigo micopresentador por primera vez en una conferencia Alexis porros Hola Alexis qué tal pues genial Martín todavía saboreando lo bien que lo hemos pasado recientemente en la conferencia del bac 2022 conociendo a toda la gente que lo organiza Muchas gracias a todos los participantes los ponentes y la audiencia sobre todo muchos de ellos con pasión por la ciberseguridad e incluso algunos estudiantes que conocimos con ganas de iniciar su carrera en el mundo de la ciberseguridad eso nos llena muchísimo el puede haber compartido divulgar todo el tema sobre la ciberseguridad en videojuegos y más allá de los videojuegos nosotros como digo encantados de haber podido dar dos charlas una mesa redonda una entrevista en la radio en directo y bueno y más conversaciones of the record digamos con los ponentes con los que atendieron los que escucharon nuestra charla Y estuvieron ahí sí con el objetivo con tal de llevar la conciencia sobre la ciberseguridad a la mayor cantidad de gente posible como es la filosofía del podcast de nuestro podcast tierra de hackers y nada sin más dilación lo primero de todo y como siempre agradecer a todos vosotros nuestros oyentes el seguimiento que nos hacéis en las redes sociales donde nos comentáis y nos enviáis vuestras sugerencias y preguntas Muchas gracias por todo eso que nos hace mejorar día a día os recordamos que deberías estar suscritos a nuestro podcast en vuestra plataforma de escucha favorita si aún no lo estáis en las redes sociales nos podéis encontrar en Twitter Instagram y Facebook con el handel arroba tierra de hackers linkedin YouTube y Twitch como tierra de hackers nos podéis enviar vuestros correos electrónicos a podcast@ tierra de hackers.com y os podéis unir a nuestro discord en tierra de hackers.com barra discord finalmente como siempre agradecer vuestro a la pregunta del episodio que fue la siguiente crees que hay conflicto de interés en que el ceo de una empresa que se dedica a la corrección masiva de tráfico en internet y venta gobiernos sea a su vez miembro del comité ejecutivo del proyecto Thor the Union router tenemos una aplastante Sí con un 90% que esto es un conflicto de interés y no sería bueno y un 10% de los votantes dicen que no pues sí un episodio especial esta vez como bien dices con nuestras charlas de la conferencia hemos pensado que sería interesante ya que también es nuestra primera charla oficial o una conferencia como tierra de hackers ponerla aquí en el traerla al podcast también por supuesto la tenéis en YouTube por si queréis ver el vídeo También y os dejamos los links en las notas del episodio como siempre darle las gracias a nuestros mecenas que nos apoyan económicamente y que están ahí ayudándonos a poder pagar un editor que nos hace todo trabajo de fondo y nos ayuda un montón y también a nuestros sponsors Como por ejemplo Mónaco que es una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros sacáis de un podcast y a través de una herramienta de gestión y

visualización de telemetría de datos de seguridad estar fundada en silicon Valley y busca ingenieros con experiencia en seguridad pero podéis trabajar en remoto y así la ayudáis incluso desde vuestra casa hacer realidad su misión podéis contactarla en su web monad.com m o n.ad.com y específicamente en el correo electrónico tierra de hackers @monat.com pues sin más os dejamos con nuestras dos charlas que hemos dado en el Bach a disfrutarlas Muchas gracias a todos por venir hoy como he dicho Joan Yo soy Alexis me soy un poco Deco pero Alexis y Martín estamos aquí para hablar un poco de ciberseguridad en videojuegos como he dicho somos luego entramos un poquito en el tierra de hackers que es nuestro podcast en el que llevamos dos años ya y os recomendamos que os suscribáis y escuchéis nuestros episodios algunos hablamos sobre videojuegos y ciberseguridad Este soy yo hace no sé cuando tenía 12 años creo con mi primer ordenador un amstrap cpc 6128 que como la mayoría de vosotros igual habéis comentado las presentadoras anteriores que nacieron con una sega bajo el brazo y yo igual Nací con un ordenador que no era realmente relacionado con videojuegos exactamente pero en aquella época se usaban las cintas de cassette y se cargaba el videojuego que tardaba un ratito en cargar pero bueno me dedico a la seguridad ofensiva en el Red timing que es digamos un concepto militar que ataca empresas para identificar sus vulnerabilidades Y cómo por ejemplo el cibercriminales pueden comprometerles robar datos y yo voy les digo los fallos que tienen y cómo se lo pueden arreglar y bueno fundador de una empresa pequeña que se llama ecoliant que se ofrece servicios de ciberseguridad a empresas soy de parcelloc es decir soy de Barcelona pero vivo en Nueva York y ahí me podéis seguir en Twitter si queréis y en mi caso yo soy Martín vigo también me dedico al tema de ciberseguridad ofensiva o sea nuestro trabajo tanto de él como el mío es intentar hackear la empresa para la que trabajamos y emulando un poco a los atacantes externos que existen y que intentan hacer lo mismo eso lo que nosotros lo intentamos hacer antes para así poder solucionar los problemas de seguridad que existen en mi caso Yo también tengo o sea fundé una empresa que ofrece soluciones de ciberseguridad me caso California vivo en California pero soy de Galicia y bueno mi tiempo libre pues me gusta hacer temas de investigación de hacking divulgación y nos dedicamos al tema de podcast El podcast Pues es lo que os decimos tierra hackers alguno conoce tierra de hackers lo he escuchado alguna vez eh ahí ya tenemos a uno perfecto los que no te allí a otro Bueno pues ya son dos no está nada mal no estará mal el podcast va de básicamente manteneros al día en el temas de hacking Entonces lo Contamos a través de historias para que sea mucho más interesante en vez de contar Pues todo tecnicismos pues historias de hacking reales y actuales por tanto lo recomendamos tierra de hackers.com pero aquí hemos venido a hablar de hacking en videojuegos y nosotros de la manera que hemos estructurado esta charla es hablar un poco de la prehistoria por así decir del hacking de Cómo comenzó los primeros las primeras generaciones de videojuegos que es de lo que voy a hablar yo y luego Alexis se centrará en la actualidad todos los juegos a lo que estáis jugando como afecta la ciberseguridad esos juegos como se abusan como se explotan y las consecuencias de ello esta máquina que veis aquí fue la primera recreativa de la historia de hecho está en un museo que está en el m Haití creo recordar en Estados Unidos y el concepto de la recreativas nació porque en el en el m&t habían creado un juego que era space Wars pero solo está disponible en un solo ordenador recordar que esto era Pues los años 70 80 y solo podían jugar los que iban a la universidad Entonces dos estudiantes decidieron meter el juego en otro ordenador y ponerlo en un espacio público y que tuvieras que pagar para poder jugar Entonces lo hicieron accesible a todo el mundo y crearon el concepto de monetizar El jugar a videojuegos de ahí nació la primera recreativa es una especie de hackeos y lo

pensáis porque cogieron propiedad intelectual de una universidad y la hicieron accesible a todo el mundo Eso sí cobrando 25 céntimos el primer el primer incidente de ingeniería inversa de reversinger en que se conoce sucedió con la recreativa de Pacman también por los años 80 resulta que este juego era bastante complicado Pues también un par de estudiantes decidieron hacerle ingeniería inversa a la placa base que era lo que contenía todo este juego y hacer una versión más fácil a la que llamaron mis Pacman que la verdad es un poquito sexista pero bueno esto era de los años 80 Pero ellos lo que hicieron fue coger una vez más un juego que ya existía y modificarlo haciendo una versión más sencilla de hecho se metieron en problemas legales por todo esto por temas insisto de propiedad intelectual pero es otra forma de hackear hacer una versión diferente del juego luego todo seguro que algunos ya empezamos a estar familiarizados con cosas de estas cuando ya las recreativas se hicieron más populares y empezaron a aparecer en bares salones de recreativas y todo esto también salía el concepto de hacking en este caso para intentar conseguir vidas gratis o créditos gratis no que se traducían vidas lo que veis a la derecha es un mechero esto lo que representa es si habéis visto alguna vez estos mecheros que son más eléctricos en vez de piedra pegan una Chispita esa Chispita si tú lo ponías contra una placa base lo que hacía era alterar el flujo eléctrico y a veces esto no era una ciencia exacta lo que hacía Es que la placa base se comportase de una manera inesperada y a veces se traducían que te incrementaba las vidas simplemente dándole así con La Chispita en vez de a tu compañero en clase lo que hacíamos nosotros pues se lo hacías a la máquina de hecho a lo mejor estáis familiarizados con algo parecido cuando jugáis a por ejemplo al Call of Duty que tienes pues esto el emp no el electromagnético pulses que al fin al cabo lo que hace es Deshabilitar tu electrónica cuando estás jugando al juego pues se vas un poco de crear emanaciones electromagnéticas para inferir en el flujo eléctrico de tus dispositivos que Esto suena así súper Guay y tal igual pero es rafin al cabo para que deje de funcionar los componentes electrónicos que tú tienes o que funcionen mal que en este caso se traducía en vidas gratis luego por supuesto había una técnica seguramente muchos conocemos la de atar un hilo a la moneda meterla y volverla a sacar para que no se la quede Pero había otro truco que era meterla por donde sale la moneda Y entonces le das así un golpecillo subí a la moneda lo suficiente para el que el sensor lo detectase pero no la llegaba a atrapar y caía y entonces así pues conseguías seguir jugando a la máquina recreativa sin que te costase nada al fin y al cabo pues esto son hackeos ya llegó las consolas No aquí ya empezamos a ver cosas más que nos llaman la atención y había el concepto de las consolas funcionaba a través de cartuchos y esos cartuchos tenían patillas que era donde pues se transfería la información entre la consola y el juego No pues por ejemplo una de las cosas que hacía la gente era introducir el cartucho inclinarlo un poquito para que ciertas patillas no estuviesen conectadas del todo o conectadas mal y una vez más el comportamiento no era Exacto pero sucedían cosas interesantes Como por ejemplo la Nintendo 64 con Super Mario podías jugar con Mario sin piernas o en el Zelda pues salía algún programador había codeado de una manera que se lo introducías mal lo detectaba y te ponía I love you un plan pues para hacer un poco no el guiño de ostras estás intentando hacer algo algo de hacking Por así decirlo y al fin al cabo lo que estás haciendo al inclinarlo es una vez más alterar ese flujo eléctrico y que se traducían un comportamiento erróneo en el videojuego luego llegaron los los en la consola por ejemplo aquí en el Metal Gear solid claro el hacking en los mandos hacía más fácil que pudieses disparar más rápido en juegos de lucha Y tal Pero los programadores se dieron cuenta de esto Y entonces por ejemplo en este juego en concreto te dice don't think auto fire oraron Now O sea que ya detectaba Incluso si los patrones con los que

estaba expulsando el botón eran demasiados rápidos para que un humano lo pudiera hacer y por tanto detectaba esos controles que no quería que el videojuego el programador que utilizases porque si no evidentemente era mucho más fácil el juego y luego ya llegó la época de los códigos trampa esto era lo que teníamos en el título y escuché alguna decir vamos arriba arriba abajo abajo quién sabe de este código o lo hago incluso ha utilizado por aquí veo eso lo que me dice es la media de edad o sea los viejunos son los que están levantando la mano ahora mismo pero esto si recordáis era el tema de elegir el mismo luchador en Street Fighter 2 pero De hecho tenía un nombre se llamaba el código o sea le fue uno de los de los más famosos no y existían guías como la de la derecha y la de la izquierda que venían con códigos de estos de diferentes videojuegos y a lo mejor es preguntáis Pero por qué existía esto a ver yo os pregunto Cuál es el videojuego más difícil al que habéis jugado hasta ahora cuál es Ya sabía yo que iba a salir el Dark souls Pues ahora imaginaros que sois los programadores de dark souls hay un error en el monstruo final y cada vez que cambiáis algo en el código tenéis que ir a testearlo y por tanto os tenéis que jugar todo el juego para llegar allí a no ha funcionado pues cambio otra vez código y tengo que jugarme todo el juego otra vez sería no no funcionaría así no pues entonces sobre todo el inicio cuando se programaban consolas se necesitaban códigos de estos que te diesempleo ideas infinitas para poder hacer testing y todo esto mientras desarrollabas el videojuego qué pasaba que estos códigos se pasaban de desarrolladores Pues a sus amiguetes Oye no no se lo digas a nadie tal o entre programadores o dentro de la industria y al final acababa haciéndose público y llegó un momento en el que se entendió que realmente hacía el juego divertido no se trataba solo de hacer trampas porque al principio había el miedo de si yo hago un videojuego y tú puedes hacer trampas lo vas a acabar muy rápido y ya no te va a aburrir el juego pero en realidad la ejecución al final no eso sino que la gente jugaba todavía más al juego porque daba más potencial o se podían hacer cosas nuevas luego vamos un poco más a nivel de Hardware pasaron de los códigos A lo mejor algunos os suena el game Ginny o el game Shark que son dos versiones de un dispositivo de Hardware que lo que hacía era alterar la memoria es decir un videojuego dentro del cartucho al fin al cabo Pues hay temas de todo esto sin entrar demasiados tecnicismos pues esto te permitía modificar la memoria e incluso realizar tus propios códigos para que tú luego pudieses aportar a la comunidad así ya no era solo los que ponían los propios programadores sino que este tipo de dispositivos te permitía hacer testing con tu propio juego incluso llegar a encontrar las partes de memoria que representaban pues las vidas o la barra de energía o lo que sea y así poderla tener infinita el modding de juegos llegó en la era de los PCS Al fin y al cabo los los ordenadores ya no eran Solo consolas que estaban hechas para jugar a videojuegos sino que ya era para correr programas de todo tipo y con eso permitía pues ya cada uno hacer sus propios programas programar en un lenguaje de programación ya no había que hacer esto tan de bajo nivel de cambiar bits y bits y todo esto entonces llegó todo el tema de moddings esto en realidad como contará Alexis se traduce a la actualidad Estoy seguro que todo es alguna vez a lo mejor habéis utilizado Bots para apuntar automáticamente o ver a través de las paredes a los enemigos de hecho muchos hemos visto muchos casos de fraude verdad de streamers que incluso han pillado en directo o han pillado Incluso en competiciones no solo haciendo streaming utilizando chips y han quedado fatal que no estamos acusando no no no no estamos haciendo que esto sea bueno Pero vale incluso la retardo a lo que viene siendo o retraso a la señal no solo para crear algo más más complicado y luego con esto pues evidentemente vinieron los programadores y empezaron a hacer anti chips desarrollar tecnología que detectase y evitarse el uso de esto y esto a día de hoy como contará Alexis todavía

es más importante porque hoy en día mueve mucho dinero el tema de EA Sports Entonces esto antes era un poco pues si estás jugando online o tal pues es una faena si estás jugando con alguien y tú pues le puedes matar Sencillamente pero era un tema de digamos que afectaba solo a la diversión pero ahora mismo también hay dinero detrás con todo el tema de Sports por tanto es muy muy importante la diversidad en esto hasta el punto de que cuando llegaron se te empezó a desarrollar tecnología para detectar chips Pues ahora mismo hay plataformas hay webs donde tú puedes pagar una suscripción donde te van dando trampas de estas chips y las van actualizando según la la industria Pone pone trabas a eso Entonces sale un chip para poder apuntar automáticamente viene blizzard o la empresa que sea activision y lo cambia lo detecta Y entonces ellos van en lo actualizan Y tú como estás suscrito a esto Pues siempre vas a tener el último chip que no es detectable es un poco como el concepto de virus y antivirus por lo mismo el gato y Ratón policías y ladrones lo mismo los juegos en Flash quien ha jugado al farming aquí ya vamos viendo más jóvenes pues esto corría más en una plataforma flash y ahí lo que te permitía era como el código se ejecutaba en el navegador pues podías Modificar el propio código tú del juego y entonces pues hacer Pues que las vacas creciesen más rápido tener dinero infinito o cosas de estas incluso a veces había hacks tan sencillos como temas del tiempo no el tiempo y bueno pasamos a la PlayStation donde ya vemos implantes de Hardware o lo que se llamaba Mode in the chips no la PlayStation 1 para poder jugar a juegos piratas el jailbreak en los teléfonos ya con estos juegos pues al tú poder controlar todo el dispositivo móvil pues ya puedes modificar los binarios lo que son los juegos en sí la memoria pues una vez más para hacer todo lo que quieras esto también existe la PlayStation 3 y 4 y ahora se lo paso Alexis porque esto es un poco la historia que nos ha llevado hasta la actualidad y Alexis nos va a contar ahora todo lo que sucede ahora mismo Quién conoce este videojuego Nombre nombre creo que dicen game Shane Impact ok era pregunta pero abro uno voy público no hay mucha gente que ha jugado este videojuego para arriba que significa es al azar digamos un vídeo yo un videojuego de Open World no de escenario abierto lo interesante es que tiene 60 millones de jugadores activos cada mes creo que son 72 millones de suscritos es gratis que esto es algo muy interesante por lo que voy a comentar ahora en breve y la media de edad creo que la media de edades de unos 25 o 30 años audiencia bastante entonces un escenario imaginaos que estáis jugando a esto y de repente sale se cierra de repente y os sale una pantalla típica de estas de ransomware he comprometido tu ordenador y si quieres recuperar los datos tienes que pagarme tantos bitcoins pues esto es lo que han estado abusando recientemente De hecho salió una noticia que la hemos comentado de hecho en el último episodio de tierra de hackers lo podéis escuchar en detalle lo que hacían era como ha comentado Martín la época de los antichids vino obviamente después de los chips el desarrollador de Impact lo que hizo es crear el anti shit que se llama mh prot 2 Bueno nombre del desarrollador que se llama Hong you o algo así en China y lo que hacía cuando instalas el videojuego es que se instala se instala como un servicio que corre siempre que no gustaba mucho a los jugadores porque consume recursos y luego algunos sospechaban me estáis espiando lo que estoy haciendo está capturando mis pulsaciones de teclado y movimientos de ratón y luego el otro tema es que se instala como usuario administrador eso significa que tiene muchos privilegios Y si hay alguna vulnerabilidad en el juego o en el antichid pues puede causar daños al dueño del desordenador y es lo que pasó no el videojuego pero el antichid tenía una vulnerabilidad que se había reportado hace dos años desde 2020 dos investigadores habían publicado su código en un repositorio en github que permitía acceso a bajo nivel Y eso significa que podían desplegar malware en este caso ransomware para lo

que no los que no conozcáis el ranson bueno a ver quién conoce el rancho mujer alguien puede explicar que es el ransomware no te he preguntado Martín entiendes el Catalán No mucho Bueno no pasa nada no pasa nada sino falo galegos también eso está bueno el ranson mueres Pues un virus vale Te cogen todos los documentos todos los datos y te dicen los hackers vale Te dicen un mensaje ordenador que dice o me pagas tal cantidad de dinero a tal lugar en tal tiempo te damos los datos si no se borra todo Ok falta un pequeño detalle en un pequeño detalle que se añade aplauso aplauso muy bien muy bien nos encanta nos encanta que aportéis en cualquier momento incluso pregunta o lo que sea pero no esperamos al final pero un pequeño detalle era que lo que hace que no recupera los datos es el tema que cifra los datos con una clave de cifrado que no la tienes tú solo la tiene el cibercriminal ese es el pequeño detalle porque también hay ataques de extorsión que te copian los datos pero no te los no te los modifican solo te los copian y te dicen Oye dame dinero o si no lo voy a publicar online tus fotos más polémicas íntimas pues Total que habéis terminado en este caso lo que lo utilizaron Exactamente no era para comprometer a personas como nosotros individuos sino que lo utilizamos para comprometer a una empresa no me preguntéis que está jugando a este videojuego en la empresa igual era una empresa desarrolladora de este videojuego o no pero bueno este juego estaba instalado en algún sistema de alguna forma no se sabe cómo el el vector de entrada que es el primer paso se sospecha que fue ingeniería social enviaron un archivo digamos de alguna forma por email o por discord por red social alguien lo descargó lo instaló entonces abusó de esta Navidad instaló el ransomware cifró los datos y no solo eso sino que además se sacó las contraseñas de todos los sistemas y de ahí bueno se metió hasta la cocina digamos porque pudo Acceder al controlador de dominio que es el ordenador más importante en una red Windows y de ahí pues inyectó malware en todos los sistemas Bueno pues esto era para decir que el malware se distribuye de muchas formas como he dicho bien ingeniería social también crean páginas web muy similares Pues en lugar de Bach punto Cat se puede gracias bueno en lugar de microsoft.com podrían usar Microsoft con la n y si no te fijas bien la m y la n se parece mucho entonces usuarios caerían en el Fish digamos serían pescados y nada lo hacen así Eso lo que quería explicar luego hubo esta operación que la llamaron Chicken drumstick en nombre Interesante como en muslito de pollo es una operación de una de un cuerpo policial en China en la provincia de junán que lo que hizo es arrestar a una banda de cibercriminales que vendía software de Chip lo curioso hay más páginas web como he enseñado Martín antes ha enseñado en su slide que hay páginas web que venden estos chips pero es que está en concreto se había hecho muy habían ganado 77 millones de dólares vendiendo su software cheat y del para hacer trampas Y entonces a los de la policía Pues claro el tema de impuestos y todo esto no le gustaba que que no declara nada sobre todo lo ganaba mucho en criptomonedas tenían coches de lujo como se viene la imagen ahí y al final los hicieron En búsqueda en internet y tal alguno había expuesto su red social y lo encontraron Entonces el tema era que hay mafias alrededor de todo esto la gente se lucra con los chips y no solo ellos sino que instalan malware también en los chips que os descargáis usáis así que de nuevo tener cuidado con sé que ninguno usa aquí ningún software chip Pero por si lo usáis hablando de dark souls habéis dicho antes era ese juego más complicado no Sí eso parece ser pues como he dicho antes el show los videojuegos en el caso anterior del ransomware con games era el antichid el software anti chip que tenía vulnerabilidades en este caso es el propio videojuego el servidor del videojuego de dark souls no solo ese Bueno a principios de este año en enero se publicó una vulnerabilidad de técnicamente se dice ejecución de código remota que es lo mismo que antes no te permite ejecutar controlar el sistema

completamente el sistema me refiero a tu portátil Windows a lo que sea tu de sobremesa y no solo eso sino creo que dos semanas después o tres semanas después también dijeron que elden ring también está afectado los servidores de esos en lo que hicieron los desarrolladores fue que pararon los servidores para que nadie se pudiera comprometer más pero Los investigadores hicieron una demostración en vivo en un en un gamer en su Stream real que lo que hicieron fue cerrarle hacerle un Crash digamos en su en su sesión de videojuegos de dark souls y luego usaron un programa digamos que vienen bebido instalado en Windows que hablaba el texto que le habían puesto en plan tu ordenador ha sido hackeado y se escuchaba por los altavoces que fue algo espectacular de ver no y luego También tenemos el tema de robo de propiedad intelectual un poquito qué juego es ese lo han pillado 17 años tenía 17 años Sí se hace poco en Londres si no me equivoco y muslitos de pollo Igual también bueno como hemos dicho antes el tema de la extorsión no se te entran en los ordenadores tuyos o en este caso de los desarrolladores donde tienen están desarrollando los videojuegos y que hacen pues cogen esta información y la filtran a no ser que tú les pagues en el primer caso un caso interesante fue que notoriamente relacionado con los videojuegos pero sí por el tema de la película No sé si acordáis digamos en el 2015 por ahí Sony pictures Pues bueno público sacó una película que se llama de interview o la entrevista creo que se llama en español Era sobre el líder de Corea del Norte en el que bueno sufría y moría un poco cómica hacia él y entonces esto no gustó mucho ni a él ni en su país entonces lo que hizo fue los hackers en los cibercriminales que al fin y al cabo en Corea del Norte en muchos países trabajan para el gobierno trabajan como mucha gente de aquí de 9 a 5 van allí y se ponen a comprometer a quien sea que le dice su jefe y luego se van a casa y eso es lo que hacen durante el día a día y durante estos estos estos cibercriminales exiltraron mucha información en la publicaron y en uno de los lichtes snowden este bueno se le llama wiser blower no como chivato en el buen sentido de la palabra digamos o no Porque publica secretos que nadie sabía a no ser que divulgar a él pues en alguno de estos archivos Se comentaba que estaba Sony estaba trabajando en una película sobre Super Mario Que obviamente se cayó el tema pero habían emails que confirmaban que estaba hablando con Nintendo para ver si hacía una película de Super Mario dato interesante como venimos aquí un poco de nuestra experiencia yo yo estuve trabajando en Los Ángeles en donde está Sony para intentar ayudar a Sony a recuperarse del ataque estuve en parte del equipo de respuesta incidentes e investigando que había pasado y todo eso el tema de Grand Theft Auto Bueno aquí la audiencia ya lo conoce que hace poco de también cubierto en un episodio de tierra de hackers de hace poco así que lo podéis Escuchar más en detalle ahí pero hackear una Rockstar games y filtraron no solo algunas imágenes y vídeo de GTA 6 sino el código fuente de GTA 5 Esto me parece interesante comentarlo porque al tener el código fuente es más fácil Buscar vulnerabilidades Y de nuevo comprometer los sistemas de todos los usuarios los jugadores que tengan instalado el GTA 5 ransomware en videojuegos el primero el tema de Fifa ahí lo que hicieron un poco lo que había comentado de la audiencia el tema de que se comprometían los sistemas de nuevos exiltró información pero no se cifraron los datos solo era o me pagas o te publicamos estos datos en el tema de Bandai namco hace poco los hackearon sus sistemas y además hicieron desplegaron ransomware que cifraba los datos y dejaba los sistemas inservibles un tema en el primer tema de Fifa Pues bueno alguno aún así pueden intentar utilizar los sistemas intentar recuperarse alguna forma pero es que en el de Bandai namco se quedaban totalmente inservibles porque modificaban digamos el sistema operativo a bajo nivel tenían que hacer eliminarlo todo completamente un poquito de ingeniería social en el tema anterior de hecho en este el de Fifa

también ha habido un caso reciente que si el criminal es intentar no ingeniería social que es de nuevo enviarle emails que parecen legítimos últimamente está mucho El caso de cibercriminales que intentan impersonar pretender ser el ceo el jefazo de la empresa y enviarle a sus empleados Oye estoy en un mitin y no puedo hacer esto por favor me puedes comprar cinco gift cards y demás así Bueno pues el tema de roblox Esto fue también muy interesante en otro episodio también lo comentábamos los llamados bimers son los que robaban el tema de roblox es también preocupante porque muy muchos menores lo juegan juegan este juego entonces hay cibercriminales que según se dice pueden ser incluso adolescentes también por el tema de que lo hacen un poco for the looles no como dicen ellos por la diversión que robaron robaron credenciales de los usuarios de roblox de nuevo vía fishing diciéndole creando páginas web similares del dominio a las que eran de roblox también vía pretexto lo que le decían era Oye soy un creador porque en el tema de roblox son juegos dentro del juego no entonces de muchos creadores de juegos que le decían a los jugadores Oye yo desarrollo juegos o puedo desarrollar tu Avatar si me un código de renderización lo llaman así de apariencia y entonces eso realmente era un engaño para decirle Oye y los usuarios de los jugadores decían no sé cómo darte este código pero ciber criminales le daban paso a paso como extraer esto que realmente eran las cookies del navegador web Que bueno que es digamos un código para decir quién eres al servidor es un código de autenticación con esto cuando se lo enviaron las ciber criminales se podía hacer pasar por ellos y robaban todos sus objetos como veis ahí lo más hay unos objetos llamados limitados porque fueron los primeros que se crearon con un número de serie y cuanto menor sea el número de serie más valioso es Alguien me puede decir por cuánto cree que se vendía por ejemplo el gorro blanco el blanco decían 3000 Pero puede ser que el verde sí por ahí y el azul es de 100 casi 15.000 por ahí lo más lo más impactante de esto es que los cibercriminales no se quedaron contentos con robarle esto sino que les decían a los menores muchas veces oye pídemelo y te lo devuelvo Pero llora y te lo devuelvo o tal Y al final grababan todo esto lo pone haciendo un poco de bullying que está era muy deprimente ver esto lo ponían en YouTube y los niños pues tenían obviamente quedaban bastante deprimidos la respuesta de roblox bueno fue que los devolvían intentaron borrar los servidores de discord donde se utilizaban para enviar estos temas dos likes quedan Esta es abuso de funcionalidades en los videojuegos algunos cibercriminales o que trabajan con el gobierno en este caso yihadistas el titular de arriba es de un documento de la Unión Europea que dice que se ha confirmado que los yihadistas digamos utilizaron bueno cibercriminales en general terroristas utilizaron los chats como método encubierto que nadie monitoriza porque todos sabéis de la nsa la hacía a toda esta no los la congregación de los cinco ojos mundial Australia e Inglaterra y todos estos miran más bien comunicaciones no sé de mensajería o los SMS o los emails pero igual no se ponen a mirar los chats los videojuegos entonces utilizaban esto para comunicarse y para planificar sus ataques y no solo sino temas también de abuso sexual pedófilos que se ha estado investigando y tema de apuestas online y legales sobre todo en Shanghai y el tema de denegación de servicio un tema también interesante porque esto en andorra a principios de año hubo una competición de Sports también relacionada con la teleserie squid Game de Netflix Que supongo que algunos lo habéis visto y bueno alguien algún cibercriminal ya así porque esto no era legal lo que hizo se puso a hacer ataques de denegación de servicio lo que significa que mucho utilizó muchos sistemas para enviar mucho tráfico al servidor de Minecraft de este este torneo Y entonces lo que hizo es que interrumpió un poco el juego en durante la competición no solo eso sino que afectó al el 25% del tráfico de andorra porque el ataque Fue bastante grande para lo pequeño que

es el ancho de banda de digamos del tubo de salida y de entrada de de datos de andorra también hace años en el 2013 hubo un ciber criminal que hizo un ataque similar de generación del servicio mucho mayor contra diversas plataformas de videojuegos la Xbox la PlayStation varios varios juegos y se le pilló como al de GTA 6 y se le dijo igual te caen 10 años lo digo aquí para que no os paséis al lado oscuro quedarse en el en el lado del bien y le podían quedar 10 años y 250 mil dólares de multa al final solo quedó en 27 meses que me parece bastante meses comiendo sopa como decían por aquí y muslito de pollo pero y luego también otro otro similar a blizzard hemos mencionado antes World of Warcraft Pues también hubo un ataque similar de negación de servicio la de delante es de distribuido que significa que en lugar de hacerlo de negación y servicio desde un sistema distribuido pues se hace desde varios sistemas para evitar que bloqueen solo una dirección IP pues es más difícil no y conclusiones hemos hablado bastante Martín y yo el tema es que tenemos hemos un poco pasado de la historia Prehistoria como decía Martín a lo más moderno y actual pues ahí habéis visto como el tema era más hack un poquito más como de diversión más como el concepto hack realmente en sí o hacker no es una persona maligna mala digamos es una persona Esta es la última Joan es es una persona curiosa que quiere ir más allá de lo establecido eso es muy interesante Porque esa esa diferenciación que una persona marca En comparación con el resto pues le da valor y esto es lo que hicieron un poquito estaba en tener la videoconsolas en offline digamos no había multijugador online y intentaban como ha comentado Martín todos esos trucos de tragaperras videoconsolas jailbreaks similares más en la actualidad se abusa por el tema cibercriminal como hemos visto el impacto es mucho mayor y mucho más preocupante por eso hay empresas por eso Martín y yo nos dedicamos a esto por gracias a estos ataques digámoslo así tenemos trabajo pero hay que tener mucho cuidado echa la ley echa la trampa como Martín mencionaba estaban estos chips luego vino los anti chips luego vienen los cibercriminales que abusan el anti chip para desplegar ransomware es un poco bailamos o como el perro que está girando hoy sobre sí mismo videojuego es igual a software esto con esto queríamos decir que como he dicho antes hay vulnerabilidades en los videojuegos hemos visto que comprometieron Dark souls hemos visto que comprometieron los antichids O sea no solo el videojuego sino los anti chips que vienen con el videojuego complementos de videojuego O sea que muy importante si os dedicáis a desarrollar videojuegos el tema de desarrollo seguro de software en buenas prácticas de desarrollo seguro de seguridad pruebas de penetración o retining que se llaman así nosotros lo que hacemos y lo último es que la ciberseguridad está muy relacionada con los videojuegos Bueno no en general cualquier tecnología se puede por tema cibercriminal ciberseguridad así que no sé podéis elegir igual lo podéis elegir en meteros en el tema ciberseguridad y luego especializados en videojuegos o meteros en el tema de videojuegos y especializarlos en ciberseguridad yo en mi caso por ejemplo he hecho casi toda mi vida y hice ciberseguridad y luego me especialicé más en tema de infraestructura crítica ellos son tuberías digamos de petróleo y gas Pues he estado en alguna plataforma del Golfo de México por ahí en helicóptero un vuelo 2 horitas en ahí para mirar los sistemas que tienen ahí y luego volver porque el precio del petróleo es muy caro y tal Y también en Minas por ahí Incluso en huelva estuve en una en España en en Chile por ahí y temas de hidroeléctricas bueno y similares así que por un lado por el otro podéis Entrar en este tema ya está así aquí tenéis no se ve mucho pero muchas gracias y nos podéis seguir en las redes sociales gracias no tenemos tiempo para preguntas que sé que nos vamos preguntas nos tenemos que ir os explico os explico nos tenemos que ir porque hoy voy a estar el programa pop de catalunya radio habla María de Linares en directo con lo cual nos

tenemos que ir ya porque nos espera a Mariola nosotros vamos a estar por aquí o sea que podemos hablar de otro sitio Bueno pues hasta aquí la primera charla de tierra de hackers de la conferencia Back 2022 Esperamos que os haya gustado hoy también queremos anunciar un nuevo patrocinador que además esta semana está lanzando un servicio en la nube para proteger tu infraestructura en aws hablamos de prowler pro y sus ass el servicio gratuito más completo de seguridad para aws Pro está construido sobre la Popular herramienta Open source frawler y además por el mismo equipo de ingenieros si ya conoces frawler que está disponible en github seguro que vas a aprovechar las bondades que ofrece frawler Pro en cuestión de minutos tendrás resultados del estado de seguridad de tu cuenta de aws podrás mejorar tu postura de seguridad a través de múltiples dashboards que te permitirán ahorrar tiempo y tener una visión completa del estado de tu infraestructura puedes empezar a usar brawler pro de forma totalmente gratuita en brawler.pro PR owler.pro a partir de mañana ahora mismo martes 4 de octubre Y ahora os dejamos con la segunda charla de tierra de hackers en la conferencia Bach 2022 dentro audio tenemos el clicker Hola buenas a todos vamos a ir un poquito rápido porque tenemos algún contenido por el que ir y no tenemos mucho tiempo vamos a hablar de la ciberseguridad y el estado actual de la ciberseguridad y los ataques que todos podemos sufrir Mi nombre es Martín vigo me dedico a las ciberseguridad ofensiva en una empresa americana y soy fundador de una empresa llamada trisquel Security soy Gallego pero vivo en California yo al igual que Martín me dedico también a la seguridad ofensiva retimer como se conoce también como Martín Tengo mi empresa que se llama equalian ofrezco servicios de ciberseguridad de empresas soy de Barcelona alrededores y vivo en Nueva York Y juntos martinillo somos creadores y presentadores de tierra de hackers al que os invitamos a que os suscribáis y que para que estéis Al Día de temas de ciberseguridad muy relevantes y en esta presentación vamos a hablar sobre tres Pilares diferentes de los acontecimientos de ciberseguridad más actuales porque creemos que entre la audiencia tenemos estas tres diferentes grupos de de bueno de empresas y gobiernos igual tenemos entre audiencia algunos que caen en esta en esta categoría también probablemente tengamos alguna breve important person or people gente de poder o bueno jueces o políticos políticos y ciudadanos como Martín y como yo los del montón básicamente no somos tan importantes Pero bueno Igual también la gente nos quiere hackear comprometer Bueno pues con esto vamos a empezar con los ataques más dirigidos a empresas y también normalmente incluye gobiernos por ejemplo tenemos el concepto de razón web que seguramente todos estáis familiarizados con estos se trata de acceder a una empresa explotando alguna vulnerabilidad y cifrar la información a veces Pues la base de datos de los clientes o en propiedad intelectual o lo que sea es filtrar esa información también y luego pues amenazar con publicarla esto ha ido evolucionando con el tiempo y básicamente pues esto se hace para poder pedir un rescate normalmente monetario y por tanto Pues yo le robo los datos por ejemplo a Uber se los cifro para que no los pueda recuperar si no tiene un backup y aún por encima los pongo en la Deep web y básicamente lo que digo es o me pagas o los público y entonces pues te estás ahí un poco en la tesitura dos ejemplos muy claros wanna Cry seguramente os suene el concepto de wanna Cry fue un ataque de ransomware que afectó a todo el mundo fue uno de los que de los que más ha afectado perdón y y fue llevado a cabo por Corea del Norte utilizando una vulnerabilidad crítica en sistemas Windows que afectaba todas las versiones que fue robado de la nsa el grupo básicamente la agencia de inteligencia de los Estados Unidos quedaos con lo que acabo de decir Corea del Norte utilizó una vulnerabilidad crítica que la agencia de inteligencia de Estados Unidos no publicó porque la octava utilizando ellos a su vez se la

robaron crearon el wanna Cry y destrozaron un montón de empresas otro ejemplo sería el not pella que se utilizó para atacar a nivel global otra vez pero sobre todo en Ucrania y en este caso pues la gente de Software que es el grupo que lo que se conoce como un Haití Pues estaba detrás de este ataque tenemos el tema de Sabotaje también disrupción de la actividad caos ventaja estratégica no sólo estratégica entre países pero también ventaja económica Por ejemplo si se quiere hacer un short de un stock voy a voy a hacer voy a atacar a una empresa por ejemplo de petróleo y como sé que vamos a impactar su imagen en el pública se puede comprar su stock Pues voy a aprovechar para comprar y hacer un short es decir compro para luego venderlo y aprovecharme de esto uno de los casos más famosos staxnet no el primer malware para infraestructura crítica que atacaba a los digamos la centrifugadoras que enriquecían el uranio en centrales nucleares de Irán ahí vemos la foto del líder del país en poco inspeccionando lo que había pasado en ese momento y también tenemos el grupo fanzibert que si no sabéis le ponen nombres graciosos a los Advance persisten 3 que son grupos de cibercriminales muy avanzados que normalmente trabajan para un gobierno y que en este caso el oso se asocia con Rusia y fanziber pues es un nombre de un grupo de ellos se asociado con el gobierno ruso que supuestamente dicen que impactó el resultado de las elecciones en Estados Unidos las de 2016 Cuando acabó vencedor Donald Trump propiedad intelectual otro problema que sufren las empresas robo de material confidencial normalmente esto suele venir muchos ataques de china en concreto Corea del Norte normalmente va por dinero Rusia va más a crear el caos y desinformación y China suele ir a por propiedad intelectual y Porque da una ventaja sobre pues investigación y desarrollo no Suele suceder a través de soborno extorsión o incluso empleados internos con maliciosos Pues que están cabreados porque no le han habido casos porque no le promocionaban o porque no estaban de acuerdo con la dirección de la empresa y aquí por ejemplo la izquierda tenemos un tweet en el que contestaba el aún más en el que un empleado de la gigafactory de tesla le vinieron unos rusos y lo ofrecieron un millón de dólares por instalar un USB dentro del gigafactory que eso lo que le daría Pues sería acceso remoto a las instalaciones y a la propiedad intelectual de tesla en este caso de las baterías y él lo denunció Y fue así como como lo pudieron detectar en este caso el empleado pues hizo lo correcto y lo tenemos un grupo chino Double Dragon como decíamos un Advanced que le llaman Dover Dragon y por ejemplo pues en la operación de cucovix pues estuvieron investigandolo y habían robado propiedad intelectual de unas 50 empresas estadounidenses una vez más pues para ganar esa ventaja empresarial ciber amenazas estamos un poco rapidito pero amenaza es pues tenemos hay muchas tipo 0d 0d significa que alguien un investigador de seguridad que trabaja por su cuenta o para un gobierno como decimos apt test descubre una vulnerabilidad que nunca antes se ha descubierto por eso dice de día cero porque justo en ese día es el Día cero y hasta que no se parchea pues se dice que no está digamos descubierta y pues expone a muchos sistemas a que sean comprometidos en este caso un ejemplo sería la de hard blit que estaba asociada con una vulnerabilidad contra una librería de cifrado de datos cuando vamos a internet y escribimos https pues es la s significa secure slayer capa de digamos de conexiones seguras pues la librería más famosa Open ssl no y se la conocéis pero o lipsl entonces había una buena Navidad en esa librería que permitía conectarte a servidores expuestos en internet miles y miles y extraer la información que estaba en la memoria que como no estaba cifrada digamos Pues eso contenía nombres de usuario contraseñas Cookies de autenticación tokens de doble factor algo que si alguien los cibercriminal se apoderaban podían impersonar a los usuarios y el caso de solar wins se ataque a cadena de suministro muy famoso creo que hace un año y medio dos fue en el que unos ciber

criminales comprometieron esta tercera entidad digamos para a través de ella comprometieron credenciales suyas que igual encontrarán a dar web porque ahí se venden por 25 dólares cada par de credenciales para entrar a solar Wings y de ahí que solar wins es una empresa que crea un software de monitorización de sistemas de red y a través de ella pudieron entrar a una empresa que se llama fire eye por ejemplo que es una empresa que trabaja para el gobierno de Estados Unidos y desarrolla mucho muchas herramientas para hacer Bueno testing de seguridad ofensiva como martinillo hacemos y bueno eso fue muy sonado no solo a fire sino luego salir muchas otras empresas bueno pasamos ahora a la otra sección que es la de Vips como puede ser insisto político se jueces y gente muy relevante que tiene mucho poder No pues ataques que hemos visto este es muy interesante A lo mejor suena un periodista del Washington post fue y perdonar Por ser directo pero descuartizado en la embajada de Arabia saudí en Turquía esto sucedió tras el espionaje por parte supuestamente voy a Añadir el supuestamente del príncipe de Arabia saudí que utilizó una tecnología de una empresa israelí que se llama en eso Group para infectar el teléfono en realidad el suyo no pudieron porque sospechó inmediatamente sino el de su mujer y poder averiguar que estaba a punto de pedir los papeles del divorcio y le hicieron ir a la embajada a pedirlo en Turquía de Arabia saudí porque este periodista era Saudita Aunque estaba exiliado en Estados Unidos y al llegar allí lo descuartizaron porque hablaba mal del Rey en el Washington post si veis a la izquierda es el verdadero periodista entrando en la embajada y a la derecha a utilizar un doble después de descuartizarlo para que las cámaras captasen que había abandonado la embajada Qué sucede que Se olvidaron de ponerse los zapatos si os fijáis visten igual pero los zapatos son diferentes es una hay una investigación muy larga os recomiendo mirarla pero es una de estas cosas donde fallaron a la hora de intentar engañar a la gente para que hubiese evidencia visual de que había abandonado la embajada y allí no había pasado nada bueno lo que tenemos el tema de los deck fakes ahora están modernos porque hay muchas digamos el acceso a los diffates tanto a nivel de audio como de vídeo y de hecho aquí tenemos un ejemplo de la actriz Jennifer Lawrence que le habían puesto esa cara de otro actor y no se ve que sea un montón lamentablemente no tenemos esto es un gif pero no sé por pero el tema es que se ha desarrollado de forma tan sofisticada hasta tal punto que se ha podido esto utilizar en ataques en comunicaciones en tiempo real por ejemplo una videollamada se intenta suplantar a una persona importante o diciéndole a sus empleados que Oye tienes que hacer esto tienes que hacerlo otro y incluso por audio también un ejemplo y hay muchas librerías disponibles a Papa para todos los públicos sobre todo en github ahí poner la gente de su repositorios y podéis si queréis jugar un poquito con ellas secuestros esto también sucede con gente muy importante un claro ejemplo sucede con la gente que suele publicar en Twitter Pues todo el dinero que ha ganado en las criptomonedas en 2019 y 2021 Entonces eso al fin al cabo cuando tú estás compartiendo información tan importante para lo que puede ser un ciberdelincuente pues se dan casos que lo que se hace conocido como osim que es un campo dentro de la ciberseguridad que es la obtención de información de fuentes públicas Pues tú puedes averiguar muchas cosas en base a lo que una persona pública en internet o simplemente está expuesto por Data Brokers y cuando tú estás publicando dónde estás en todo momento Cuánto dinero acabas de ganar y capturas de pantalla de tu cuenta bancaria Pues es normal que luego vengan y te puedan secuestrar Y eso efectivamente sucede lo que tenemos el tema contra de fraudes del ceo Pues esta empresa de transportes de valencia Aparentemente alguien impresionó al jefazo al ceo de la empresa y engañó de las directivas que tenía acceso al dinero digamos de la empresa y hizo una transferencia de unos 4 millones de euros al ciber criminal Así que está la

comento rápido siguiente todo a través Y por último También tenemos extensión extorsión esto de hecho es una publicación de la propia policía donde pues desde la cárcel muchos reclusos que pueden hacer llamadas pues simplemente te llaman y te dicen que acaban de secuestrar a tu hija que inmediatamente tienes que enviarles dinero y tal creando un poco esa urgencia no te dejan soltar el teléfono para que puedas Llamar a tu hija y a lo mejor es verificar que realmente esto es una mentira y te piden dinero inmediatamente o la van a matar esto pasa mucho sobre todo en países sudamericanos no Y claro se crea su urgencia o por ejemplo una vez más volviendo al tema de o sin si sabes que que ellos pueden averiguar porque tu hija que la siguen en instagram justo acaba de pillar un vuelo Pues hay un espacio de 9 horas donde tu hija no va a tener cobertura no la vas a poder llamar y te están diciendo la que vamos a secuestrar o lo vamos a hacer así y entonces realmente eso no ha pasado tú no lo puedes verificar y evidentemente si te piden una suma que es razonable la vas a pagar y pasamos al tema de individuos como decíamos Martín como yo Y tenemos el tema del escenaje masivo de las grandes los grandes gobiernos por ejemplo los cinco ojos que le llaman son los cinco países miembros sería Australia Canadá Nueva Zelanda Inglaterra y Estados Unidos y tienen por ejemplo lo que se le llaman taps o conexiones digamos de digamos hombre de interceptación no por todo el mundo ya sea porque despliegan a ahí vemos algunos en pequeñitos se ve una pareja de hombre negro y blanco son agentes de la Cia que están infiltrados digamos en otros países de interés También tenemos que en los satélites algunos los controlan y pueden ver nuestras comunicaciones Así que siempre usar https y seguridad también en los cables transoceánicos También tienen interceptaciones en esos casos y luego el tema tenemos de snowden y sus revelaciones de todos los datos de la nsa por ejemplo abajo a la derecha tenemos el logo de X Kiss Core que era una una plataforma en la que digamos de búsqueda de datos en una en una base de datos gigantesca que recopila la nsa de todos los ciudadanos del mundo y vemos la foto de snowden ahí de un documental en la que él decía yo no me fío De nada de la electrónica y lo que hago cuando me compro un teléfono es quitarle desoldarle el micrófono y la cámara de vídeo También y luego Por ende el ningún software Aunque me instalen pegasos candil o lo que sea este spyware no puede acceder al micrófono ni a la cámara Porque lo he quitado y solo uso un micrófono cableado digamos minutos a que vamos a ir a toda leche espionaje masivo lo que sucede aquí que me volví a olvidar que hicimos esto claro vale Estados Unidos y bueno y otras están recopilando toda la información a pesar de que está cifrada en internet porque es valiosa hasta el punto de que saben que en el futuro van a poder descifrarla Entonces es como recopilar ahora información masivamente de internet que no puedo descifrar pero por la ley de mur que indica que la la capacidad computacional crece exponencialmente saben que en un futuro van a poder descifrar los algoritmos que utilizamos hoy en día de hecho muchos ya han sido apartados porque ya se consideran inseguros tanto es así que la comunidad ha creado el una nueva tecnología que se conoce como perfect Forward secretsy y lo que hace es dificultar que en el futuro los gobiernos puedan descifrar comunicaciones que se cifran hoy de manera insegura no voy a entrar mucho más porque no tenemos mucho más tiempo pero para entendáis que esto no es algo de ciencia ficción o unos supuestos tenemos a los gobiernos recolectando datos masivamente y a las entidades creando tecnologías porque saben que eso va a suceder solo quería comentar un tema sobre eso es que recopilan tantos datos cifrados Porque en el futuro va a venir la computación cuántica que va a romper el cifrado en este caso la privacidad todos nosotros somos el producto preguntados Cuántos de vosotros usáis soluciones públicas como las de Google Gmail y similares y si pagáis algo al respecto si no pagáis nada significa que de algún sitio

tienen que ganar estas empresas para pagarle a sus trabajadores no los empleados de Google ganan bastante bien entonces y luego Tenemos también el tema de los Data Brokers que se ha visto mucha polémica últimamente por todo el tema de recopilación de datos y temas relacionados con la salud sobre todo en Estados Unidos y en entrar en mucho detalle y bueno se ha visto también que los de la frontera Cuando entras a Estados Unidos a veces hacen búsquedas ilegales en tus dispositivos electrónicos como teléfonos y portátiles y sin una orden judicial te extraen los datos y bueno es que lo monetizan y de ahí de tu información sacan y lo venden por dinero Vale Nos quedan tres slides esto a lo mejor lo habéis escuchado se trata básicamente de ataques de ingeniería social contra las operadoras telefónicas en las que son capaces de engañar a los operadores para que asignen tu número de teléfono a la SIM Card que ellos tienen muchas de la seguridad hoy en día y autenticación se basa en la seguridad de tu número de teléfono al robar eso pues pueden resetear una contraseña y recibir el código la autenticación de doble factor los registros en Telegram y ensignal y pueden robarte mediante algo tan poco sofisticado como un ataque de ingeniería social robo de cuentas password Spring aquí tenemos la lista de los de las 10 contraseñas más utilizadas en el mundo si alguno de aquí si alguno ha reconocido las identificado ya puede ir a cambiarla ahora mismo o cuando acabemos pero y hay estos dos servicios que son muy interesantes have significa me han comprometido mi contraseña en el que puedes poner tú en dirección de correo electrónico y te dices si estás en algún link en el Dark web o en el Clear web en Google lo que sea y de Hash es un servicio de pago en el que tú puedes comprar digamos credenciales que las han crackeado hombre básicamente dice la contraseña por simplificarlo mucho estafas Pues esta ya es la última Por cierto todos conocemos la estafa del príncipe de Nigeria ahora ya eso ha evolucionado un poquito más de aquello de va a cerrar Messenger Esta vez sí lo van a hacer de pago y ahora tenemos pues haciéndose pasar por Microsoft que tienes un virus en el ordenador y te piden dinero por ejemplo estafas amorosas no sé si habéis visto en Netflix el documental de la estafa de tinder y todo esto sino mirarlo que va un poco de eso y criptos camps hemos visto que relacionado con un hack a la empresa Twitter pues hasta cuentas como la de Joe biden el presidente el que uno de los candidatos a la presidencia estaba twi hablando sobre un scam de cripto O sea que aquí es donde vemos la última está prometida el tema de extorsión for the luse por la diversión como el grupo este el que se llama lulsek que es de seguridad por diversión tenemos varios temas no ahí podéis ver 4 Chan lulsexuating el tema es que por ejemplo tenemos el del zapato en la cabeza que de alguna forma conseguían información sensible de esa persona le decían o me haces un vídeo así raro que yo quiera te pone un zapato y haces un vídeo me lo envías o voy a publicar esta información en la que sales sin ropa o temas así Esto bueno todo el mundo no le le cabríamos le causaría mucha mucha mucha mucha debilidad digamos entonces hacían el vídeo un tema que hemos comentado esta mañana Por cierto relacionado con esto sería el tema de roblox Como algunos los denominados beamers atacaban a los a los sobre todo a los adolescentes o menores de edad les robaban sus sus sus objetos de roblox que tan deseados los habían conseguido y les decían por favor pídemelo de rodillas o llora o lo que sea si no no te lo devuelvo y luego lo que hacía no se lo daban cogían esos vídeos o audios y los ponían en internet y bueno y los niños pues estaban muy muy tristes obviamente y teníamos aquí el fin Pero fin Muchísimas gracias Nos tenemos que ir pues hasta aquí esperemos que os haya gustado las dos charlas esta ha sido un episodio especial sobre videojuegos sobre el estado de la ciberseguridad y lo dicho esperemos que os haya gustado los tenéis también en las versiones de YouTube por si las queréis compartir con compañeros Muchas gracias por haber escuchado como siempre el

podcast y nos vemos y nos escuchamos la próxima semana Muchas gracias a todos por escucharnos siempre nosotros seguimos trabajando duro para poder divulgar y concienciar a todos sobre noticias y temas de ciberseguridad nos escuchamos en el próximo episodio o nos vemos en la próxima conferencia pues lo dicho hasta la próxima semana Adiós adiós chao Hasta pronto 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 último episodio de tierra de hackers