67. Augury y Genshin Impact

auguri es la herramienta utilizada por las agencias de inteligencia de los Estados Unidos para obtener los patrones de navegación en internet de los usuarios y el pentágono se niega a dar detalles al respecto el sistema anti chip de Impact además de dejar a muchos tramposos fuera de juego los ha dejado expuestos a vulnerabilidades que cibercriminales han aprovechado para comprometer y desplegar ransomware en sus sistemas no te ha dado casi tiempo para echarnos de menos y ya estamos de vuelta con otro episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 24 de septiembre de 2022 este es el episodio número 67 yo soy Martín vigo y está conmigo poniendo ya los flecos finales a la charla que vamos a dar en amposta los dos Alexis porros Hola Alexis qué tal Muy bien Martín Pues aquí ya acabamos de empezar primero de todo para los que no se dan cuenta el otoño y Bueno y con otoño ostras vienen temas En serio que bajón y se acabó el calor y estamos viendo unas unas lluvias bastante fuertes no por Estados Unidos incluso por Europa España están viendo pero sí aparte de eso pues nada con el otoño vienen todas las flores un cambio aquí tal pues un poquito También nosotros cambiando intentando ir ahí a expandir tierra de hackers y y compartir nuestro conocimiento y como dice Martín nos han invitado a dar unas charlas sobre cibersegu en videojuegos en amposta Así que si estáis por ahí cerca y os queréis pasar podéis tener más información en vag.cat que creo que es Sí esa V ag.t efectivamente tenemos muchísimas ganas de ir y será el próximo viernes Así que encantados con esa invitación y como siempre Aunque parezcamos pesados pero agradeceros a todos vosotros que nos sigáis que nos compartáis vuestras sugerencias mejoras Incluso compartáis el podcast con vuestros compañeros familias amigos y que nos sigáis en todas las redes sociales donde estamos y ahí estamos en Twitter Instagram y Facebook linkting YouTube Twitch no puedes buscar como tierra de hackers o arroba tierra de hackers Y tenemos el email podcast arroba tierra de hack y en discord tierra de hackers.com/discord Finalmente como siempre agradecer vuestro apoyo a la pregunta del episodio que fue la siguiente desde un punto de vista de seguridad y privacidad te parece adecuado el modo lockdown del nuevo sistema operativo de Apple O crees que deberían invertir en otras funcionalidades de seguridad tenemos la primera con un 50% si me protege de spyware le sigue con un 20% si me hace más anónimo le sigue con un 20%, No creo que deberían invertir más en anti rastreo y la última es un 10% no más en securizarlo todo en general Así que vemos que a la mayoría si le parece adecuado el modo lockdown por mayoría absoluta pues muy interesante como siempre que bueno tener esa esa perspectiva de los oyentes mencionar también que la vanguardia un diario español nos ha puesto entre los cinco podcast que no te puedes perder relacionados con tecnología desde aquí nuestro agradecimiento Pues por ese pequeño reconocimiento y por la visibilidad que eso nos da a nosotros ya digo nos ha alegrado el súper encantados muchísima ilusión Muchísimas gracias Muchísimas gracias Pues nada como siempre También dar las gracias a nuestros mecenas de patrón y a nuestro sponsor hormona una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente Nosotros con este podcast y mónate a través de una herramienta de gestión y visualización de datos fundada en silicon Valley ya sabes que busca ingenieros con experiencia en seguridad Sobre todo como puede ser tú y que además permite trabajar en remoto Así que deberías visitar su página web para unirte a este proyecto si te interesa monad.com m o n a d.com y

les podéis contactar directamente en tierra de hackers @mona.com que así saben que venís desde de parte nuestra Y empezamos ya y hoy os vengo a hablar de auguri producto de una empresa conocida como Tim simru y sobre el cual nuestro senador estadounidense favorito Don ron weiden del que hemos hablado muchísimas veces Aquí acaba de escribir una carta al departamento de defensa porque un weezer blower volvemos a hablar de nuevo de un wiser plomer Parece ser que están saliendo ahora mucho pues le ha contactado para advertirle de que la Marina americana acaba de comprar licencias para este producto auguri sí como decía últimamente hay mucho wizard suelto y desde luego cada vez que sale uno da para noticia aquí en tierra de hackers Pero bueno mi intro a la noticia ha sido un poco larga no y hay mucho que desmenuzar ahí así que al lío el senador ron wden es un demócrata muy concienciado con la ciberseguridad y que está siempre metiendo presión en el congreso y dando visibilidad a los problemas de privacidad online que tiene y sufre hoy en día la sociedad conectada en decidimos hay mucho que agradecerle a este senador porque es realmente quien constantemente arroja luz a estos problemas y exige medidas políticas para combatir el alcance y abuso de las empresas privadas en torno a nuestros datos por tanto no me sorprende que un wiser blocker le haya contactado a él directamente o a su oficina Bueno ya que se ha forjado una muy buena reputación como decía según he leído el wiser blower Parece ser que es nada más y nada menos que un marine de los Navy seals se intuye porque según dice la carta del senador ronweiden y cito textualmente porque envió una carta al departamento de defensa dice lo siguiente y la ha hecho pública mi oficina ha sido contactada recientemente por un weezer blower que describe una serie de quejas formales que ha enviado hacia arriba y hacia abajo en la cadena de mando así como al Inspector general del el departamento de defensa y a la agencia de inteligencia de defensa sobre la compra y utilización de datos relacionados con el tráfico de internet por parte del servicio de investigación criminal de los Marines el encis os dejo un enlace a la carta en las notas del episodio para que podáis leer la íntegra pero os dejo con algunas frases interesantes de la carta insisto por recapitular un weezer blogger contactó a este senador que ya estaba haciendo una investigación en Cómo el gobierno de los Estados Unidos Estaba comprando datos de navegación de estadounidenses bueno Y por supuesto de otros Pero a ellos solo le interesa evidentemente de sus propios ciudadanos y ha escrito una carta pública a varias entidades de inteligencia gubernamentales en Estados Unidos para pedir información al respecto pero es que la carta contiene información muy interesante barra acusaciones y es por eso que os voy a destacar os la dejo entera pero os destacó aquí el primer el primer párrafo de la carta dice lo siguiente y esto escrito por un senador no un periodista o alguien que tiene una opinión o algo así les escribo para pedir que se investiguen los departamentos de homeland Security de defensa y de Justicia por la compra y utilización de registros que revelan las páginas web que los estadounidenses han accedido online todo esto sin ningún tipo de orden judicial o sea estamos hablando insisto de que un senador está pidiendo explicaciones a los a las propias agencias de inteligencia de su país porque están comprando registros que revelan según él las páginas web a las que están accediendo todos los ciudadanos O sea si el senador está preguntando sobre los ciudadanos americanos imaginaros estas agencias de inteligencia todo lo que tienen sobre todo los demás que no vivimos en Estados Unidos y no somos ciudadanos Pero bueno más dice lo siguiente durante años he estado investigando la compra de datos de Ciudad de ciudadanos americanos incluyendo información de geolocalización e historial de navegación la conclusión de esta investigación confirma e insisto en confirmar que múltiples agencias gubernamentales están comprando datos de americanos sin autorización de un juez parémonos aquí a pensar lo que

acabo de decir un senador confirma públicamente en la carta que información de geolocalización y las webs que visita la gente está siendo comprada por el gobierno americano a empresas privadas o sea insisto la capacidad de recolección de datos es que no se va a reducir solo a los americanos porque evidentemente eso es donde más problema y porque si la agencia de espionaje se dedica a recolectar de otros países pues es una agencia de espionaje espiando por tanto pues pues era un poco esperar No pero bueno seguimos con otro párrafo mientras que he podido hacer público detalles sobre esta compra de datos de navegación y geolocalización de americanos por parte de agencias gubernamentales mis esfuerzos para arrojar más luz sobre la compra de los historiales de navegación han sido bloqueados por el pentágono Esto es lo que dice la carta que me pregunto yo porque el pentágono está intentando bloquear que esta información se haga pública continuamos Mientras que el departamento de defensa se niegue a publicar información mi equipo ha averiguado que un contrato público ha sido publicado en internet demostrando que varias agencias del departamento de defensa compran información de Data Brokers que revelan el historial de navegación de la gente la agencia de contrainteligencia y seguridad ha gastado más de 2 millones de dólares comprando datos de tráfico en internet y de sistemas de nombres de dominios Pues aquí más claro agua la carta es extensa como decía yo recomiendo leeros y para ello os dejo el enlace como no En las notas del episodio investigando más me encontré de hecho el propio contrato entre Stream Team los desarrolladores de auguri y la Marina estadounidense Así que que os lo dejo también las notas del episodio Este es el propio contrato y dice textualmente los siguientes respecto a lo que van a recolectar con la licencia que ha contratado la Marina estadounidense insisto esto ya es el propio contrato en sí Y dice lo siguiente la suscripción proveerá de acceso a un repositorio online de petabytes de datos de red históricos y actuales que incluyen bgp dnsville datos de Bots pickups de imap pop y smtp así como pickups de rpp y ftp y certificado es x509 los datos provienen de 550 puntos de recolección de información distribuidos por todo el mundo que incluye Europa Oriente medio Norte y Sudamérica África y Asia y se actualiza con 100 billones de registros a diario por supuesto os dejo el enlace al contrato en las notas del episodio pero pensar lo que acabo de decir o sea esto ya está aquí detalladísimo que están dando acceso a petabytes para los que no estén familiarizados con las medidas digamos de espacio en los ordenadores pues normalmente la gente está familiarizado con hasta los gigabytes o terabytes Pues petabytes todavía muchísimo más estamos hablando de cantidades ingentes de información de hecho es una mejor medida pensarlo de la última frase se actualiza con 100 billones de registros a diario después de comentaros todo esto es muy importante también matizar algunas cosas No aquí ha ayudado mucho ver el contrato que contiene más detalles Porque si me hubiese quedado solo en la carta O quizá en alguna noticia que encontré Pues a lo mejor puede dar la sensación de que es mucho peor de lo que es y con esto no quiero decir que no sea malo esto pero el contrato sí detalla específicamente lo que se recolecta o no lo más importante a matizar es que a día de hoy muchísimo tráfico en internet está cifrado esto significa que en principio el contenido de dicho tráfico está seguro los metadatos es lo que podrían recolectar pero nunca el contenido es decir auguri el software del que os estoy hablando no podría obtener los credenciales de tu email cuando los pones en la página para loguearte en gmail o los mensajes que envías por Signal o las fotos que subes a Google Drive pero que haya mucho tráfico cifrado no quiere decir que todo el tráfico esté cifrado Especialmente cuando A lo mejor hablamos de páginas web menos conocidas de países menos desarrollados pues una tienda online de local de un país No no las no Amazon y luego mencionar también que no

todo lo que se está recolectando se reduce a visitar páginas web o términos más técnicos al protocolo http y https recolectan todo como hemos visto en el en la descripción del contrato de hecho tuve un debate muy interesante con un compañero sobre esto que él consideraba el decir un poco amarillista no la noticia que había leído una en concreto device news yo como le dije a él yo no estaba de acuerdo del todo en eso de que era amarillista si bien Si lees el artículo puede dar la impresión que cuando dice recolecta historial de navegación se podría interpretar el historial del navegador que específicamente dice no solo la página sino dentro de la propia página web pues por ejemplo si vas a tierra hackers puedes ir a tierra de hackers barra episodio 55 y puede ser más específico Pues en vez de interpretar y que usamos eso lo que realmente se está recolectando si vemos en el cuando nos paramos a analizar el contrato Sí pues son las ips no no quiere decir que no sea cierto que las ips indican tu comportamiento en internet porque sí que lo sí que lo hace pero recolectar una IP no te da tan específicamente qué página web visitas como si recolectas la propia URL El dominio por tanto no da la precisión digamos que daría el historial de tu navegador porque puede haber varias páginas web alojadas Bajo la misma ip es decir Martín vigo.com alexis.com y tierra.com podrían compartir la misma IP por tanto auguri si recolectas a IP que tú has visitado no no podrás saber cuál de las tres has visitado Pero bueno sabe que una de las tres la has visitado No pues pues eso es algo que vale la pena matizar y todo esto insisto gracias al cifrado De hecho aquí lo que lo que hay que Resaltar es la importancia de que si exista la criptografía por eso Lo importante es matizar que el cifrado nos protege de esto y como les decía mi amigo la cuestión No es que no sea para tanto Porque casi todo el tráfico está cifrado de hecho buscaba por internet y leí que se estimaba que el 93% del tráfico en internet está cifrado el tema es que los datos que se están contactando se está recolectando igualmente y no es porque como todo esté cifrado Entonces no pasa nada la lección aquí es Resaltar la importancia y la consecuencia de que internet esté cifrado que nos protege de que nuestros propios gobiernos puedan espiar nuestro comportamiento online masivamente y sin ningún tipo de orden judicial si están recolectando esta información no es como está cifrada la podemos recolectar es menos mal que está cifrada porque si no tendrían muchísima más datos y de hecho en capturas de pantalla que he visto de la herramienta se encontraban hasta cookies que para acceder a cookies tiene que ser con el tráfico descifrado por tanto no están descartando el tráfico que está sin cifrar les interesa Y mucho aquí una vez más las dos caras de la moneda no en declaraciones públicas por parte de una de los miembros de la oficina de información naval de la marina concretamente Charles expertos él dijo lo siguiente respecto en los comentarios de ron wyden y de esta investigación ensis lleva a cabo investigaciones y operaciones acordes a la ley y regulaciones relevantes el uso de datos de tráfico en internet no requiere una orden judicial Esto es lo que dice esta persona representante de los navys del departamento en concreto que se dedica a Jaque que por cierto es decir que ensis son los de la famosa imagen no sé si la has visto estoy convencido que sí en YouTube de cuando esta serie hay en seasider que es como el csi pero digamos un Spin off y va de temas de hacking un poquito Italia hay una famosa imagen que es buenísima que son cuando la chica y el chico se ponen a hackear los dos a la vez en el mismo teclado que están accediendo al firewall y tal pues esos son este departamento evidentemente en ficción no pero no sabía yo que los Navy seals tenían temas de estos te regresas Pero bueno ese momento en el que parece que están haciendo de piano no más que sí sí hijo esta tela tiene que ir más rápido tienes que ir más rápido y los dos en el mismo teclado hackeando tío que claro te estás limitado a las teclas del lado izquierdo y ella del lado derecho tío Y por supuesto ni ratón ni nada ni qué bueno tío es buenísima esa imagen pero

bueno yo no soy abogado pero matizar que datos en internet metadatos y todo esto O sea cuando dice que no hace falta orden judicial para recolectar datos de tráfico en internet en mi opinión que no tengo ni idea de lo que estoy hablando pero en mi opinión Yo puedo entender que si tú estás recolectando datos como por ejemplo puede hacer una empresa de antivirus para analizar y tal pues si lo necesitas una orden judicial dos que otra cosa es que tú estés comprando datos de navegación que se recolectan de isps masivamente de todos los ciudadanos de tu país Ya no voy de los demás de tu país y los estás comprando a una empresa privada que los ha recolectado de los isps de la empresa de tu país y a la parte de manera masiva y para llevar a cabo investigaciones yo creo que ahí y sobre todo siendo a nivel gubernamental lo de la orden judicial yo no creo que sea simplemente a eso lo recolectamos datos de internet y ya está a mí me da que ahí hay que matizar un poquito más y no simplificarlo no hace falta orden judicial y ya está porque lo que se está haciendo No es comparable a lo que puede hacer Pues yo que sé ya ya digo lo que se me ocurre una empresa de antivirus o alguien que analiza tu tráfico por alguna razón para temas de seguridad pero ya sabéis que a mí siempre me gusta traeros el plot twist Así que agarrados a la Silla el ceo de Tim simrum que se llama rabbie Rock Thomas no solo es la persona que ocupa el puesto más importante de la empresa que está detrás de auguri sino que también es parte del comité ejecutivo de Thor Sí sí me habéis escuchado bien el mismo tío que supervisa la creación y venta de software para la recolección masiva de tráfico en internet y que provee a gobiernos y empresas privadas es también el mismo tío que se sienta en la mesa con los demás asesores para desarrollar el software y protocolo por excelencia para navegar de manera anónima por internet Mátame camión tío yo con esto sí que flipé Cabe destacar que es verdad que Thor fue un proyecto inicialmente militar y de hecho creo que el ensis fue gran parte de la creación de Thor entonces pues una vez más dando las dos caras de la moneda que es importante aquí no nosotros no pretendemos con tierra de hackers intentar hacer aquí un alarmar a la gente para que sea más espectacular y tal siempre intentamos matizar y Buscar el punto intermedio y cuestionar para que vosotros hacéis vuestras propias conclusiones Entonces se podría argumentar que quizá Pues bueno esta persona está ahí porque tiene contratos con el ensis y por tanto fueron inicialmente los creadores de Thor y tal y cual pero bueno a mí desde luego me llama la atención por lo menos hay un conflicto ahí de ética yo creo pero bueno continúo cuando le preguntaron sobre este conflicto de intereses a la directora ejecutiva de Thor que es Isabel lavagueros esta dijo que los potenciales conflictos de interés han sido investigados y publicados siguiendo el proceso de desclasificación estandarizado de dicha información a todos los miembros ejecutivos los miembros ejecutivos no han identificado un conflicto de interés pues pues no lo habrá Pero sabes qué yo voy a tirar de nuestros queridos oyentes de tierra de hackers y preguntarle a ellos saber qué opinan la pregunta de este episodio es crees que hay conflicto de interés en que el ceo de una empresa que se dedica a la recolección masiva de tráfico en internet y venta gobiernos sea a su vez miembro del comité ejecutivo del proyecto Thor y voy a ser muy claro Sí o no las dos opciones que tenéis pues madre la que se ha liado no con todos esos datos recopilados una gran revelación y muchas gracias desde aquí querido senador ron weiden por por publicar esto una vez más eh una vez más tenemos que sí que enviarle algún email de de decirle Gracias pero no muy interesante Martín el nombre que han elegido es lo de team sin Sí muy interesante la plataforma augur y así una palabra italiana no que significa Felicidades tanti auguri Muchas felicidades bueno Ahora parece ser que le cambiaron le cambiaron el nombre ahora a Pro Signal os dejo por supuesto como siempre os queremos dar toda la información para que vosotros también podáis contrastar no lo que decimos aquí y formar

vuestra propia opinión generar debate que esto es lo que nos interesa no se los dejo los a la carta del senador al contrato público a incluso a un artículo sobre este software sino también a la propia web de steam simru como Alexis bien dice para que podáis ver un poco también que son ellos mismos en su propia web que anuncian esta capacidad no interesante porque yo a este grupo lo conozco desde hace muchos años que hacen temas de recopilación de dns y tal no los veía que recopilaran tantos datos y que los vendieran así a empresas bueno empresas organizaciones gubernamentales sin autorización judicial Pero bueno el tema que me da también me ha fascinado un poquito es el que has dicho que el 95% no se ha dicho algún número mayor del 90% del tráfico a cifrado interesante Sí sí 93 sabes qué pasa con esa medida que era cuando estaba aquí en este debate agitado con mis dos amigos les decías que yo creo que esta estadística no se está refiriendo a que el 93% de de los en points de digamos de los puntos que puedes acceder estén cifrado sino al tráfico claro las 10 páginas más visitadas del mundo que puede ser por las redes sociales Twitter Google y tal eso ya lo mejor me lo invento es el 80% del tráfico entonces engaña a decir porque si tú claro es que no no lo estás cogiendo o sea este dato se refiere al tráfico que observas no a que el 93% Por así decirlo de las páginas web estén cifradas y esto era lo que yo contra argumentaba contra mis colegas que me decía pero si Total no pueden recolectar casi nada y tal Por eso yo daba El ejemplo tío Yo me encuentro a veces páginas web que todavía no utilizan https Pero insisto que aquí se recolecta de todo que también está el mail a través de pop y que en el contrato específicamente habla de pickups o sea había una frase muy buena de que entrevistaban a un experto en seguridad no los de los descubrieron los device news Y decía el pickup lo es todo lo único a mayor es que puede recolectar es el olor a electricidad decía decía esa frase porque digamos que los pickups es pues es un formato que representa el tráfico en internet no digamos pequeñas porciones de información en Cómo se divide Pues el tráfico que va en internet del protocolo Es que no quiero entrar en demasiados tecnicismos pero digamos que ahí lo puedes observar todo por supuesto si está cifrado pues no vas a obtener mucha información pero si no lo está lo tienes todo todo entonces claro yo cuando es este 93% de cifrado por supuesto lo quería mencionar en el podcast Porque es importante dar ambos lados no solo alarmar aquí a la gente soltando vanos espían y ya está no es el propósito de tierra de hackers para nada pero sí que por eso me gustó mucho el debate con mis amigos yo les decía que si se refiere al tráfico no representa todas las páginas web Todavía están hoy en día sin cifrar y hay mucha gente a pesar de que los navegadores ya vienen con protecciones para intentar forzar el cifrado y cosas así hay mucha gente sobre todo en países subdesarrollados que todavía operan con un Windows 95 con un Internet Explorer y todo esto que no tiene esas medidas de seguridad todavía si lo del pickup creo que lo hemos comentado en algunos otros episodios anteriores hay herramientas como tisi pidamps Shark que se pueden utilizar para capturar y analizar y de hecho yo cuando tengo algún problema lo primero que hago es Mirar los paquetes porque yo como Martín también dice en el pickup tienes un montón de información y yo digo que el tráfico de red nunca falla nunca te engaña Así que y una frase que una vez me impactó también era si te acercas mucho a la realidad puedes ver los píxeles Así que estamos todos lo de los metadatos muy interesante también porque hay aplicaciones incluso de mensajería instantánea que metadatos se envían que a veces pueden estar no cifrados Aunque la comunicación en sí vaya cifrada así que cuidado también con eso y temas de email sobre todo también Martín has hecho claro Hay que matizar ahí que hay metadatos que es que tienen que ir sin cifrar para que se pueda operar no entonces claro también es que no es que se haga propósito sino que es inevitable es inevitable porque lo diseñaron mal pero sí está

bien Bueno también pero quiero decir que a veces no no es culpa del desarrollador de la aplicación o tal hablamos ya de protocolos A muy abajo a nivel que a lo mejor existe desde los 60-70 en aquella época nadie era malo Todos eran buenos y nada Los hippies hippies pero no también has hecho un hincapié que quería un poquito comentar el tema de por ejemplo aunque esté cifrado o bueno o Aunque el usuario intente establecer una comunicación cifrada con una web pongamos el protocolo http si el usuario escribe dos puntos barra barra y el sitio web al que se visita no utiliza políticas de estas de redireccionarte a https de forma segura pues Oye y hay alguien en el medio que está intentando hacer un downgrade o una degradación de esta comunicación que tú intenta hacerla segura pero o el servidor web te lo intenta hacer segura pero el hombre en el medio te la intenta hacer insegura vhddb pues ahí también te pueden capturar eso puede ser que no te des cuenta en la barra de direcciones y que entiendas que estás visitando una web de forma segura como https pero no lo está y para eso hay extensiones de navegador como https everywhere de la electrónica Frontier foundation que es recomendable instalar y en algún momento deberían Desactivar todos los sitios web del puerto 80 Aunque bueno puede ser que otros sistemas legítimos digamos tradicionales en rompan el tema de que igual bueno se apoyan en el http solo y no https y también el tema del cifrado Aunque todo el tráfico vaya cifrado quería hacer un poquito otro comentario sobre el tema de este cifrado es seguro o no por ejemplo los sitios web usan ssl versión 2 versión 3 el tls 1.0 que todos estos están confirmados de ser vulnerables y se han petado más de una vez utilizan suites cifrado seguras o no como el algoritmo rc4 que es vulnerable utilizan algoritmos de hashing seguros o no como el md5 o el sha-1 que también de nuevo se ha empezado una y otra vez y bueno también un tema el último comentario un tema relacionado que me apasiona mucho el tema de la computación cuántica no esto ya es Next Level Pero en cuanto tengamos ordenadores cuánticos que puedan crackear toda esta todos estos cifrados bueno con muchas ganas de tierra de hackers o no pero bueno que no pase cuando salgan vamos a hacer los primeros ahí para comentar noticias de como grupos cibercriminales están rompiendo cifrado de comunicaciones con computación cuántica que ya le están poniendo el ojo y se están investigando para esos temas grandísimo grandísimo apunte Alexis porque esto lo hemos hablado en el pasado sobre el concepto de forwardsy y también sobre cómo snowden una de las cosas que publicó fue como el gobierno de los Estados Unidos estaba creo que eran Virginia construyendo un centro de datos masivo masivo que era para la recolección de tráfico en internet que claro que dices tú pero si está cifrado da igual pero es con la suposición que ya lo asumen que en el futuro lo van a poder Designar Entonces les vale la pena recolectarlo Ahora aunque a día de hoy no puedan descifrarlo porque saben que entre el incremento no la ley de mur de la crece exponencialmente la capacidad de los microprocesadores y de los ordenadores en general para para hacer que cálculos matemáticos que al fin y al cabo es lo que se basa el romper cifrados pues ya asumen que en el futuro van a poder descifrarlo y esas comunicaciones pueden ser muy valiosas aunque sean del pasado para investigaciones futuras o vete tú a saber el qué Y por eso existe tecnologías como perfect forwardsy que por no ponernos demasiado técnicos lo que hace es que dificulta no el romper el cifrado sino que en vez de tener digamos que romper averiguar una un secreto para descifrar todas las comunicaciones tienes que averiguar muchísimos secretos porque se utiliza un secreto diferente para diferentes digamos porciones de la comunicación por tanto si te cuesta digamos 10 días averiguar la clave privada para descifrar una comunicación entera Pues si se utilizase perfect Forward secretsy Pues tienes que pasarte 10 días para averiguar la clave cifrada que descifra una parte solo de esa comunicación a lo mejor se han utilizado 10 llaves diferentes

Entonces eso va por lo menos a proteger un poco más a dificultar el descifrado de tráfico en un futuro pues a gente con la capacidad para hacerlo como puede ser un gobierno o sea esta tecnología se ha desarrollado también con la con el Samsung con la asumiendo que los gobiernos van a intentarlo por tanto no es ciencia ficción o un por si acaso es el que se ASUME de ambos lados que va a ser así si lo que dices que se que se cifra cada trocito digamos de información con una clave distinta me ha venido la cabeza el tema asociándolo con el tema de metadatos que hemos dicho por ejemplo en los emails no el Front to el asunto esos a veces van en claro digamos o en las cabeceras y si se podrían ver Depende como lo esté cifrando el sistema de correo electrónico Así que si pudieran ver por ejemplo estos grupos que quieren ver tus comunicaciones en el asunto pones aquí te envío el password Entonces ya saben que se tienen que enfocar en los datos de justo ese ese tiempo ese momento de tiempo así que intentar no utilizar de forma explícita estas partes que van más en los metadatos para evitar que os ataquen pero bueno sí muy muy interesante lo de la computación cuántica y seguimos con la siguiente noticia que va de Bueno un poquito ransomware videojuegos sistemas antitrampas Y es que un grupo de ransomware está comprometiendo a sus víctimas al abusar del sistema anti trampas o del inglés anti cheating del popular juego gratuito gameshing impact para que la gente que no conozca este videojuego es un videojuego para consolas ordenadores de sobremesa o portátiles y dispositivos móviles es un videojuego de tipo roll de acción de mundo abierto que hoy en día está es muy popular este este tipo de mundo abierto que puedes irte por donde quieras en el videojuego y tiene digamos diferentes historias puedes crear tu propia historia según lo que vayas eligiendo y es gratuito esto es muy importante porque tiene mucha adaptación no en mucha gente se lo va a descargar si es gratuito Es de estilo animes fue lanzado el 28 de septiembre de 2020 casi hace dos años por el desarrollador chino hoyo vers o en China se le conoce como mi joyo es su quinto videojuego y está disponible para Android iOS Microsoft Windows Playstation 4 y 5 y está previsto un lanzamiento futuro en la Nintendo switch comentar sobre el tema demográfico de los jugadores es que tiene más de 62 millones de jugadores activos mensuales alrededor de 70 millones de usuarios registrados el 27% de los cuales tiene menos de 25 años y la Edad Media de sus jugadores es de 35 años quiero comentar que es un sistema anti trampa para que los que no lo conozcáis es es software que principalmente evita ataques tipo Mods que son digamos software o rutinas para modificar cualquier variable del jugador sus monedas sus vidas sus objetos también hay otro tipo de ataque que se le llama invot que significa robot que digamos apunta o sea te ayudan a apuntar te ayudan a disparar y dar en el objetivo sin hacer ningún tipo de esfuerzo trampa de nuevo otro tipo de ataque otro tipo de trampa es el anti que es justo lo contrario del Inbox evita que los inbots de distintas formas te ataquen te den Te maten digamos y una que me pareció curiosa es intercambia la cabeza de tu jugador con los pies de tu jugador Así que vas caminando como si fuera boca abajo y luego tenemos otra también que se llama World hacking que literalmente es caminar a través de muros como fantasmas O sea estás hackeando el muro también hay otros tipos de ataques un poco más bajo nivel sería directamente modificar la memoria para cambiar variables del jugador como sus monedas vidas objetos como he dicho antes la memoria del sistema operativo que corre el videojuego en este caso la memoria específica del videojuego no Y también Se podrían modificar ficheros directamente que están en el sistema de ficheros del sistema que corre el videojuego que también de nuevo contienen variables de jugador como sus monedas vidas y objetos que estos se van guardando no conforme se va jugando o cuando se cierra también se vuelven a guardar y cuando se abre el videojuego pues se vuelven a cargar estos datos No se podría modificar en

cualquier momento u offline para que cuando se carguen Pues bueno un jugador tenga más vidas o más monedas o más objetos y luego también están los cracks no esos que se utilizan para salta la licencia de los videojuegos en este caso no tiene mucho sentido porque es un videojuego gratuito Pero hay algunos otros que igual pues necesitan una licencia en los sistemas anti trampa antichid están desarrollados normalmente por el propio desarrollador del videojuego así que bueno Esto implica que los usuarios probablemente confíen en ello aunque no están muy contentos algunos los que quieren hacer trampas pero bueno la mayoría en principio dice Bueno pues esto viene con el videojuego que voy a hacer No si viene instalado pues lo dejo como digo se instalan de forma predeterminada muchas veces cuando instalas el videojuego Así que juego instalado anti chip que también se instala a veces incluso siguen corriendo estos sistemas de antichid cuando el juego se ha cerrado y esto ha causado un poquito de polémica en los últimos años porque Bueno a los usuarios esto no les gusta por dos motivos el primero es impacto en el rendimiento de su máquina a veces Depende como el este diseñado el anti chip igual puede consumir más cpu más Ram más memoria de tu sistema y el otro motivo es la incomodidad que algunos les supone algunos usuarios porque piensan que igual les están espiando es que tienes algo ahí corriendo que cuando cierras el videojuego igual debería cerrarse también no pero bueno sigue corriendo ahí podríamos decir lo mismo de sistemas antivirus no pero bueno en un sistema antivirus es que no hay otra si no le dejas correr todo el tiempo Pues igual no no te protege en tiempo real y otro tema importante de los sistemas antitrampas que normalmente corren con privilegios de administrador al menos en los últimos años los han desarrollado de esta forma lo hacen para evitar los el Software que se opone a estos anti chips lo podríamos Llamar anti anti chips o anti anti trampa no Porque algunos de estos corren a nivel de kernel a nivel en núcleo del sistema operativo Y por qué lo hace un de nuevo porque pueden haber formas no solo a nivel de usuarios sino a nivel más de bajo nivel a nivel de kernel de modificar la memoria como digo del videojuego para hacer trampas y añadirle al jugador más monedas más vidas más objetos lo que sea y esto incluso algunos críticos de la seguridad en videojuegos y han comentado que es peligroso hacer esto porque estos sistemas anti chip como todo Otro software no es inmune alguna habilidades está desarrollado por humanos y por tanto puede tener fallos que se pueden explotar y bueno justo de hecho es el es lo que ha sucedido en esta noticia vamos que todo esto pone a los sistemas anti trampa como muy buen caldo de cultivo para desplegar malware desplegar ransomware ni explotar las vulnerabilidades que tiene para comprometer un sistema re Espero que esté utilizando este sistema anti chip Pues en concreto sobre esta noticia una vez explicado el que es el ganching Impact y los sistemas anti trampa recientemente Los investigadores de seguridad de tren micro han publicado un informe en el que detallan como cibercriminales aprovecharon las vulnerabilidades en el sistema de antitrampas de Impact para desplegar ransomware a escala y esto sucedió durante la última semana de julio de este año se aprovecharon mucho de esto Porque primero el sistema antichid está firmado por una empresa legítima en este caso está firmado digitalmente por Microsoft lo que significa que Windows lo ejecutará el hecho de que abusen de vulnerabilidades de un servicio y binario legítimo y firmado digitalmente por Microsoft les hace a los cibercriminales ser más sigilosos y el antivirus o la solución de idear en Point detection and responds anti malware anti chip no previene esta infección no como digo se ejecuta con privilegios de administrador Así que esto ayuda mucho a los cibercriminales que es lo que han abusado para parar o Desactivar servicios de seguridad como el antivirus o el sistema de idear y también tiene bonalidades es conocidas lo que le permite el objetivo de desplegar El ransomware esto es perfecto para poder desplegar un ataque

ransomware para que cifre los datos y pida un rescate económico como todo ataque rasomor verdad el ataque digamos se podría resumir en cuatro actos el primero sería descargarse el ransomware los archivos relacionados con este gran software vía ingeniería social Como por ejemplo sería un caso podría ser digamos vía discord o publicarlo en algún sitio en redes sociales y similares el siguiente acto sería la ejecución del ransomware a través de la instalación de este Driver que es el Driver que viene con el sistema antichichi de Impact que se llama mhyprot 2.6 que es un driver de sistema operativo de Windows que este ransomware instalaría en el sistema lo instalaría ubicándolo poniéndolo en una carpeta específica del sistema de ficheros y añadiendo los las entradas específicas requeridas para el registro del Windows y listo acto Seguido lo que se haría es se utilizaría se abusaría de este Driver legítimo mhy Pro 2.6 para desactivar soluciones de seguridad como el antivirus y el ID Air y finalmente Pues desplegar el rancho muere cifrar archivos y Mostrar la nota de rescate en este ataque en concreto fue más a nivel de empresarial que a nivel de individuo los atacantes lo que fueron fue lo que hicieron fue lo siguiente volcaron credenciales de un controlador de dominio que es un servidor en redes Windows que se encarga de la propia red en segundo lugar lo que hicieron es conectarse vía Remote de stop protocol esto es de forma gráfica desde un ordenador a otro De hecho al controlador de dominio con credenciales de administrador de dominio que habían capturado en El Paso anterior el siguiente paso fue desplegar el ranso muere en una estación de trabajo cualquiera en un sistema Windows de esa red incluyendo la instalación del Driver como digo mhy prot 2.6 este servicio antichip de gameshing Impact y finalmente pivotaron a través de esa estación de trabajo y desplegaron el ransomware a las demás estaciones de trabajo de la red en este ataque en concreto Los investigadores desconocen el vector inicial de ataque pero se sospecha como he dicho antes lo más usual es que probablemente sea fuera vía ingeniería social como muchos otros ataques contra jugadores de videojuegos y de hecho hemos comentado por ejemplo respecto al robo de objetos y esas fedoras de los jugadores de roblox No pues todo esto lo comentamos en el episodio 47 y ahí hicieron uso de ingeniería social vía canales de discord sobre las monalidades comentar que los investigadores indican que bueno que se pueden abusar que tienen vulnerabilidades ya publicadas ya conocidas desde el 2020 que justo hubo al menos dos investigadores en Hace dos años que de hecho hay publicaron dos repositorios en github con una prueba de concepto de cómo podrían explotar el Driver mhi pro2.6 y acceder enumerar procesos del sistema terminar procesos del sistema como pudieron ser antivirus y sistemas edr e incluso leer y modificar memoria del sistema tanto a nivel de kernel como obviamente a nivel de usuario pues muy muy interesante todo el tema de videojuegos me gusta que en el episodio anterior hemos traído el problema con GTA 6 ahora tú mencionas todos estos ataques de ransomware a través de de videojuegos de hecho es que viene muy bien para para la conferencia la charla que vamos a dar en la conferencia de videojuegos es perfecto sobre todo porque últimamente Alexis nos trae esa varios sabores de como atacar a videojuegos no porque también hablabas de roblox para robar dinero o sea ya tenemos ahí todo el popurrí o sea temas de rams un buen robar dinero robar y propiedad intelectual no sé si has cubierto ya en algún videojuego simplemente de robar información para temas de privacidad seguro que algún gobierno en algún lado está tirando de temas de videojuegos para recolectar todavía más información tú qué opinas sino que ataques sobre videojuegos igual no se hablan tanto porque Bueno no sé los de a nivel gubernamental son más espectaculares no y venden más pero los hay y hay que tener mucho como Como he mencionado en las recomendaciones hay que tener mucho cuidado con los más pequeños que juegan estos videojuegos y a veces no tienen la

conciencia de seguridad que deberían tener Y bueno pues desde aquí de tierra de hackers queríamos un poquito también mencionar algunas noticias que nos parecen interesantes para los más pequeños de la casa así para ayudar un poco a los adultos a los padres a echarles un ojo de vez en cuando y decirles eso que que tengan cuidado con lo que se descargan como lo instalan y que no hagan trampas digamos instalando Software que no deberían instalar Pero como dice Martín hemos tenido muchos ingredientes Esto está siendo un poquito aperitivo y el colofón final el digamos El plato fuerte va a venir la semana que viene durante la vaca y como digo los investigadores hacen hincapié en que el juego no necesita estar instalado para que se pueda infectar el sistema objetivo para que se puedan abusar de las vulnerabilidades del sistema antichid de henchin Impact porque como es simplemente un archivo un driver de Microsoft Windows que viene incluso firmado digitalmente por Microsoft Windows este archivo que se llama mhy Pro 2.6 pues lo que los cibercriminales pueden hacer y de hecho han estado haciendo es Descargar traer empaquetar este punto sis este Driver con los otros ficheros maliciosos que componen el ransomware y descargarlo directamente en la máquina objetivo e instalarlo para que paso siguiente puedan explotar las vulnerabilidades y que ha dicho que tiene que decir el desarrollador a todo esto pues Jojo Birds ha sabido de estas modalidades Desde hace dos años como mencionado estos investigadores de seguridad publicaron sus sus resultados y sus dos repositorios en github con sus pruebas de concepto y se lo comunicaron al desarrollador que ya los había desde entonces Pero dijo que porque esto no era tan importante y que no lo iba a arreglar aunque con este nuevo incidente con todo el revuelo Pues los periodistas de esta noticia que han hecho el seguimiento un poco a la investigación de tren micro pues se pusieron en contacto con el desarrollador y le dijeron Oye esto ya Ya lo sabías ya lo tenías en tus informes de vulneralidades no lo arreglaste no sé si vas a hacer algo ahora al respecto y bueno comentaron que sí que que justo ahora están trabajando en ello que coincidencia no que justo después de que este ataque de rancho muere sucediera se pusieran a trabajar en ello pero bueno al menos es algo que da ánimos no para los usuarios para los jugadores de Impact Porque si tienes que tener instalado el sistema anti chip para poder jugar al juego y sabes que tiene vulgaridades y te pueden comprometer tu sistema Pues la verdad es que yo no estaría muy contento de jugar al videojuego en este escenario En definitiva que todos los sistemas ahora mismo que tengan instalado el sistema antichid del juego gameshing Impact son vulnerables Así que mucho cuidado con los que estéis utilizando este videojuego en vuestros sistemas sobre todo Windows que es a los sistemas a los que afecta y comentar que aunque los cibercriminales no abusaron de estas vulnerabilidades en el antichid de gameshing Impact para desplegar ransomware a escala y solo se enfocaron en una empresa en concreto esto utilizarlo sería muy inteligente una estrategia muy interesante por dos motivos principalmente el primero es como he dicho anteriormente es un juego gratuito Así que tiene una gran aceptación como he dicho tiene unos 70 millones de usuarios suscritos 60 millones de usuarios de jugadores activos cada mes Así que todas esas podrían ser las potenciales víctimas y lo segundo es un poquito jugar en el componente humano no con la motivación económica y psicológica de los jugadores que seguro están dispuestos a hacer lo que sea con tal de ganar Incluso si esto significa instalar software en sus sistemas que desconocen que no saben De dónde viene hay que recordar que hoy en día casi todos los juegos online incluyen un componente económico como puntos que se consiguen durante el juego y se pueden canjear por objetos en el propio juego como dinero Fiat ya sean euros dólares o similares o incluso criptomonedas también está el todo el tema de los ennefties no que también están surgiendo pues estos tokens también en

relación a las criptomonedas que pueden proporcionar algún alguna motivación económica también están los niveles al que el jugador puede llegar Por ejemplo si alguien juega durante mucho tiempo y hace que su jugador llegue a un nivel muy elevado revaloriza el personaje Y pues lo puede vender a alguien o digamos le puede dar acceso a torneos internacionales con premios económicos muy suculentos y bueno el otro tema sería la fama los seguidores en redes sociales y En definitiva el dinero no que se puede ganar jugando siendo el mejor haciendo trampas para ser el mejor de hecho los puntos u objetos o incluso los personajes de los juegos se pueden intercambiar por dinero como como digo directamente en los Juegos o sino también hay mercados secundarios ilegales que también permiten esto pero de nuevo mucho cuidado con esto porque muchas veces no es realmente aunque sea ilegal la transacción Bueno se puede dar de forma exitosa pero a veces son incluso las transacciones son falsas es solo una forma de atraer a jugadores que quieren vender sus objetos sus puntos y luego acaban siendo todos ellos mismos se les roban sus contraseñas sus credenciales y lo pierden todo quería comentar que he mencionado que estos sistemas antitrampas normalmenten se Ejecutan a nivel de kernel no con privilegios de administrador puesguen Impact no es el único de hecho vanguard el sistema anti trampas para el juego valorant que es este juego de disparos en primera persona en línea de riot games fue uno de los primeros y de hecho uno de los que también le siguió muy de cerca es ricochet es el sistema antitrampas de activision para sus famosos juegos de la saga Call of Duty Y esto no se releva solo a gameshing Impact como que es un como he dicho antes un caldo de cultivo para cibercriminales del ransomware porque caspersky también ha publicado un informe recientemente sobre cómo cibercriminales están abusando de otros videojuegos para desplegar malware en este caso vieron que casi mil jugadores tuvieron problemas con malware relacionado con videojuegos entre el 1 de julio de 2021 y el 30 de junio de 2022 durante casi un año son bastantes usuarios y luego identificaron que casi 100.000 archivos se hicieron pasar por copias de juegos populares que en realidad alojaban aplicaciones no deseadas como malware o ransomware Minecraft un juego muy famoso entre niños fue el cebo más popular utilizado en casi 24.000 archivos maliciosos que afectaron a 130.000 jugadores en ese mismo periodo de casi un año en la plataforma de PC ordenadores de sobremesa o portátiles tenemos que los juegos utilizados como señuelos para distribuir malware fueron roblox también muy popular entre niños Need For Speed Grand Theft Auto del que ya hablamos en el episodio anterior durante el compromiso a Uber y el siguiente también compromiso a Rockstar games y cuando se filtró el juego Grand Theft Auto 5 y 6 y también Call of Duty es otro de los juegos que se está utilizando como señuelos para distribuir malware en PC en móvil Tenemos también que se han abusado se ha utilizado los siguientes juegos como señuelo para distribuir malware Minecraft roblox Grand Theft Auto de nuevo Player and nouns battlegrounds y FIFA comentar que desplegaban el siguiente tipo de malware no era todo ransomware como en el caso que he comentado en la noticia principal pero desplegaban malware del tipo adware que es el que te muestra ventanas emergentes como anuncios que esto lo utilizan para monetizar también malware de tipo que roba credenciales de sistemas de pago o financieros credenciales de videojuegos o incluso credenciales para acceder a tus carteras de criptomonedas Y cómo distribuyeron este malware cuál fue digamos el vector inicial Cómo se inició este esta descarga de estos archivos pues una forma de distribución fueron los cracks de videojuegos populares anunciados vía redes sociales o canales de discord como mencionado anteriormente recordemos dos cracks son es software que ayuda a saltarse la licencia si hay que pagar por algún videojuego la otra forma de distribución fueron sitios web falsos para juegos Como por ejemplo

Grand Theft Auto y apex Legends que pretenden generar dinero en el juego pero en realidad roban los detalles de la cuenta de los propietarios para apoderarse de ellos de sus cuentas de sus jugadores y otra información confidencial relacionada con ellos Esto bueno sería también un atento a la privacidad de los jugadores Así que Cuidado con la información que ponemos online en estas plataformas estos videojuegos y otro canal de distribución fueron sitios web de aspecto dudoso que ofrecen scripts macros y sistemas para hacer trampas en los videojuegos como siempre desde tierra de hackers en este caso queremos comentar unas medidas que se pueden aplicar para mejorar para protegerse En estos casos unas recomendaciones básicamente la primera sería que parcheemos los sistemas con todos los parches de seguridad que los Microsoft Windows Apple macos y otros sistemas operativos y fabricantes de estos sistemas operativos van publicando no solo eso sino también los parches que los desarrolladores de los videojuegos también publican Porque por ejemplo el desarrollador de gameshing Impact esperemos que dentro de poco publique una actualización un parche de seguridad para su Driver anti chip Pues en cuanto salga por favor ID a instalarlo para que no puedan comprometer vuestros sistemas otra recomendación sería no descargarse archivos de personas desconocidas Como por ejemplo anunciados en discord como hemos dicho este componente de ingeniería social que están explotando por todo el tema psicológico no de que los jugadores quieren ser ganadores y harían lo que fuera con tal de ser los primeros incluyendo hacer trampas y descargándose instalándose Software que venga de cualquier sitio pues mucho cuidado con eso ojo con el fishing que dice que vende juegos más baratos o lo que he dicho anteriormente no que te permite ganar más puntos o más vidas en los videojuegos de alguna forma como digamos una caja negra que no incluso no hay que descargarse nada pero te pide tus credenciales mucho cuidado con eso no bajarse cracks de videojuegos primero por el tema ilegal que esto implica porque sería tema de piratería de videojuegos pero muy importante también el tema de que estos cracks este software puede traer malware y ransomware como ya comentado en la noticia Y en el otro en otra investigación de caspersky no descargarse software anti chip descargar los videojuegos e incluso cualquier otra aplicación a poder ser desde sitios legítimos como a la Microsoft Store el app store steam Google Play proteger la cuenta y aplicar medidas de seguridad como la autenticación de doble factor ya sea por vía aplicación móvil o SMS Aunque mejor la aplicación móvil y utilizar contraseñas únicas y complejas guardadas en un gestor de contraseñas protegido también por una contraseña buena y sobre la privacidad del usuario utilizar formas de pago porque a veces hay que pagar dentro del videojuego utilidad formas de pago de un solo uso como tarjetas de regalo o incluso otras tarjetas que se pueden tener online Como por ejemplo en este sitio web así.com O my sudo es otra alternativa en las que estas aplicaciones estas plataformas te permiten obtener tarjetas de crédito que no es que no están directamente asociadas a ti porque las puedes utilizar con datos que no son los tuyos reales Así que esto sería una una media de seguridad que se podría aplicar para proteger tu privacidad online y Sí aparte de temas de pago también tu información tu nombre tu email tu número de teléfono tu dirección pues todo esto si se puede dar lo menos posible o si no es necesario pues se puede dar algo falso o algún código postal que se haya obtenido o algún teléfono de voz sobre IP que se ha obtenido que no sea directamente asociado con con tu persona pues mejor que mejor en conclusión vamos este nuevo modelo de vía ransomware a través de Software que abusa los programas anti trampas de videojuegos gratuitos y famosos está muy bien pensado La verdad por como he dicho por todo el tema de aceptación especialmente de este videojuego gameshing Impact que es gratis y que lo usan muchos usuarios 60 millones activos al

día y por el tema psicológico no de que todos los jugadores quieren hacer lo que sea por ser los primeros por ser mejor que su vecino Así que pensando más en los más pequeños de casa y no son los más pequeños sino pensándolos más pequeños se piensa en toda la casa en general hay que educarlos bien para evitar tener sustos mayores Porque si comprometen los sistemas que los más pequeños utilizan en casa y están en la misma red que el resto de la familia pues desde ese punto se pueden lanzar ataques a los demás sistemas de la red se puede pivotar a través de los sistemas que se han comprometido que tienen los videojuegos instalados y como digo se puede interceptar tráfico infectar a otros sistemas por ejemplo de los padres que utilicen para hacer sus transacciones bancarias y de esta forma comprometerlos y obtener credenciales para acceder a su cuenta de banca online carteras de criptomonedas información sensible que pudiera ser relacionada con salud o Bueno cualquier otro tema similar de privacidad hay que tener mucho cuidado y quería también comentar un tema relacionado con el ransomware como noticias flash así muy rápida y me ha parecido muy interesante esta nueva forma de cómo despliegan el gran software los cibercriminales hay una nueva tendencia en la escena del rancho muere y es el cifrado intermitente o cifrado parcial de los archivos de las víctimas este método cifrado de archivos ayuda a los operadores de rancho muere a evadir los sistemas de detección y cifrar los archivos de las víctimas más rápido esta nueva forma de es más efectiva y de hecho la están usando para atraer a más operadores o afiliados les están diciendo Oye mira nos hemos inventado esta nueva forma que es mucho más efectiva no la paran los antivirus ni los ideas nadie se da cuenta hasta que ya es demasiado tarde Así que si queréis os podéis os podéis Añadir a nuestro grupo de ransomware Y ser operadores y bueno como hemos mencionado anteriormente en los grupos de ransomware se financian o se establecen en forma de franquicias Así que este Esto es lo que están intentando hacer expande expandir su negocio de rancho muere a través de nuevas franquicias o nuevos operadores el cifrado intermitente es importante para los operadores de ransomware desde dos perspectivas uno la velocidad Cuanto más rápido cifre en los archivos de las víctimas menos probable que los detecten y que los detengan en el proceso el cifrado intermitente provoca daños irreparables en un periodo de tiempo muy breve igual que en un ataque de rancho muere tradicional en el que se cifra todo el archivo en este caso también causa daños que son irreparables pero mucho más rápido y el segundo punto es la evasión una de las técnicas que utilizan los sistemas de detección de ransomware es el análisis estadístico para detectar la operación de cifrado y con este análisis lo que intentan hacer es evaluar la intensidad de las operaciones de entrada y salida de archivos es decir cómo de rápido Cuántas veces se escribe y se leen los archivos esto en un ataque de ransomware es muy elevado porque el ataque de ransomware este programa que está corriendo en tu sistema lo que hace es leer todos los archivos que hay y luego los escribe cifrados Así que se basan en esta sería una de las medidas en las que se basan para determinar si un proceso Realmente está haciendo algo sospechoso y hay que pararlo hay que terminarlo y el otro punto que miran es la similitud entre una versión conocida de un archivo que es legítima que no está afectada por el gran Summer y una versión cifrada y modificada sospechosa del archivo esto Normalmente se tienen una base de datos Pues no sé pueden ser haches de estos archivos conocidos sobre todo los que forman el núcleo del sistema operativo y de vez en cuando pues van comparando el Hash original que tienen la base de datos con el nuevo que pueden ver en el sistema de ficheros Y si hay alguna diferencia pues Oye algo ha cambiado hagamos algo respecto terminemos el proceso que ha modificado este archivo o alertemos al equipo de seguridad o al usuario en sí que esté utilizando este sistema encontraste

con el cifrado completo El cifrado intermitente ayuda a evadir dichos análisis que acabo de comentar al exhibir una intensidad significativamente menor de operaciones de entrada y salida de archivos porque lo hace con menor intensidad Lee menos datos de archivos y Por ende cifra menos datos de archivos y de hecho la similitud de los archivos cifrados es mucho mayor entre la versión cifrada la versión comprometida y la versión original La no cifrada la legítima y esto porque es así porque a veces no se hace un Hash directamente de todo el archivo porque a veces se modifican partes por ejemplo cuando se hace un parche de seguridad en Windows a veces no se instala un nuevo archivo completamente sino que se aplican se modifican partes del extraordinario en sí y las otras partes se dejan tal cual entonces a veces lo que hacen los sistemas de seguridad es calcular haches de partes específicas de un binario por eso si se modifican ciertas partes y se cifran ciertas partes Así de forma intermitente puede ser que justo se toquen las que no se están monitorizando y Por ende el archivo parezca ser igual al original y desde cuándo se está utilizando esta nueva tendencia pues desde mediados de 2021 ya el ransomware el grupo de ransomware loca file fue una de las primeras familias importantes en ransomware en utilizar el cifrado intermitente para evadir los mecanismos de detección desde entonces hace ya pues eso casi un año un número cada vez mayor de operaciones de ransomware se han sumado a esta tendencia sentinel One publicó recientemente un informe en el que investigan familias de ransomware que utilizan cifrado intermitente que son las siguientes quick agenda Black Cat También conocido como alf.v Play y blackbuster para poner un ejemplo el ransomware Black basta cifra de la siguiente forma si el archivo es inferior a 704 bytes si el archivo es muy pequeño pues lo cifra entero en cambio Si el archivo es mayor de este tamaño de 704 bytes lo que hace es lo corta en trozos de 64 bytes y cifra uno Sí y otro no es decir los primeros 64 bytes los cifra los siguientes 64 no lo cifra los siguientes 64 los cifra los siguientes 64 no los cifra esto como digo igual se puede recuperar algunos datos de estos archivos cifrados porque no todo se cifra pero no va a tener la consistencia completa ese archivo van a ver partes que se van a perder Y esto como he dicho antes ayuda mucho a evadir los sistemas de detección de ransomware Así que es una estrategia muy inteligente que se está utilizando y que quería comentar desde tierra de hackers para que todos estemos al corriente y sepamos que hay una forma un poco más sigilosa más Ninja lo podríamos decir de cómo las mafias de rancho muere están operando actualmente efectivamente sí sí tengo tengo muchas ganas de hecho vamos a dar varias charlas no solo una no pero sí que una específica temas de seguridad en videojuegos que tengo muchas ganas de darle pues hasta aquí ha llegado el podcast por hoy como siempre esperemos que os haya gustado echarnos una mano compartiéndolo que así le llega a gente como periodistas de la vanguardia que nos ayudan a ganar visibilidad compártelo con tus compañeros Al fin y al cabo si nosotros nos echamos aquí una hora semanal es para que alguien nos escuche cada vez cada día crecemos más Muchísimas gracias por todo recordad que en Twitter estamos sorteando una entrada gratuita y 10 con descuento a la conferencia de Nou con name Así que si queréis pues podéis ir a Twitter nosotros intentamos siempre conseguir valor añadido para nuestros oyentes así que ya sabéis si estáis interesados pues ir a Twitter y comentáis en ese post para saber que estáis interesados y las sortearemos yo creo que la semana que viene y nada Gracias por quedaros hasta el final Muchas gracias a todos como siempre sin vosotros como dice Martín no estaríamos en la lista de la vanguardia como los cinco top podcast de tecnología y nada desde aquí prometemos seguir trabajando duro y trayendo noticias de ciberseguridad y concienciar a todos vosotros para protegerlos online hasta la próxima semana Adiós adiós chao chao que vaya bien si te ha gustado este episodio y quieres ayudarnos a

seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers