65. 0ktapus y HomeLand Justice

y una serie de intrusiones a empresas encadenadas que empezó con una simple campaña de phising termina con cientos de corporaciones comprometidas miles de afectados hackeados y hasta cuentas de signal de periodistas de investigación robadas home and justice el grupo cibercriminal apoyado por el gobierno iraní compromete y ex filtra datos del gobierno al vano con el objetivo de prevenir una conferencia de un grupo opuesto al régimen de irán pero albania no se corta y con una decisión nunca antes vista en respuesta a un ciberataque anula todas las relaciones diplomáticas con teherán sin muelas del juicio pero con la voz intacta os traemos un nuevo episodio de tierra de hackers comenzamos hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 11 de septiembre de 2022 este es el episodio número 65 yo soy martín vigo y está conmigo ausente de todas las muelas del juicio al igual que un servidor alexis porro sol alexis que tal y bien bien bueno aquí aunque no faltarán muelas no nos va a reír tengo que me duele la cara un montón aunque como como decía este el chavo del ocho' no así un poco inflamado no sé yo tengo la cara pues como como si te hubieras metido si eres niño de todos los caramelos en la boca así para que no te los quiten si justo los lacasitos en el bolsillo pues como estados entre tú también como queríamos saber cómo te fue por ahí por el desierto no ahí no había internet supongo no si nada una una pasada una desconexión de una semana en en un evento increíble en el desierto que se llama burning man que bueno seguramente muchos oyentes hayan oído hablar de ello pero básicamente tengas una semana con con hippies al desierto a festejar estilo mad max y ahí no hay ni cobertura ni dinero ni tiempo ni nada o sea es pura libertad una auténtica pasada la verdad llevaba 11 años sin ir y he vuelto por fin increíble 11 años madre mía sí sí me recuerda a la película mad max como has dicho muy interesante no sé si yo podría ir pero bueno igual algún día voy contigo o no al año para el año te llevo de hecho de hecho díaz y una charlita de de temas de cómo se llamaba el título era your guide to avoid ciberespionaje creo que se llama tu guía para evitar el ciberespionaje porque allí como pues como la gente es así muy muy para no hay nada muy para no el que no pero que estás en un ambiente muy guay así estilo eso mad max en medio de la nada aislado de todo entonces dije va a dar una charla sí muy centrada en temas de ciberespionaje de que de los datos y de tal puede estar súper guay y como pues eso tenemos un campo allí tal estuvo estuvo muy guapo completamente of the record hay en perdido por otro micro hombre por supuesto pues muy bien muy bien encantado de tenerte estar aquí juntos de nuevo con todos nuestros oyentes y no sólo eso gracias por seguirnos o seguirnos episodio tras episodio vamos viendo los frutos de que nos sigáis de que nos votéis de que nos deis vuestros comentarios y porque recientemente y box nos ha seleccionado como uno de los 10 mejores podcast de tecnología así que de nuevo ya os lo hemos dicho en las redes sociales y en dischord muchas gracias de nuevo por el apoyo esto es gracias a todos vosotros y nada para hacerlo corto ya sabéis estamos en todas las redes sociales twitter instagram y facebook con el handle tierra de hackers linkedin youtube y tweets tierra de hackers nos podéis enviar nuestros correos electrónicos a podcast a tierra de hackers puntocom tenemos un servidor de discos muy majo al que podéis acceder vía tierra de hackers puntocom barra de escort también os recuerdo que si no estáis suscritos a nuestro podcast deberíais ir a lo mismo a suscribiros a nuestro podcast en vuestra plataforma de escucha favorita y cerrando la intro como siempre agradecer vuestro apoyo con la votación a la pregunta del episodio que en el episodio anterior fue la siguiente cuál

crees que sería la medida más efectiva para evitar el abuso de información de geolocalización de usuarios obtenida a partir de aplicaciones móviles que siguen tus movimientos teníamos cuatro opciones la más votada con un 40 por ciento fue usuarios limitando el gps ya sea desactivando la posibilidad de que las aplicaciones puedan acceder a la ubicación de geoposicionamiento o incluso utilizando falseando en la ubicación verdad en segundo lugar con un 30% el gobierno aplicar leyes más estrictas en tercer lugar tenemos con un 18 por ciento de votaciones los fabricantes deberían aplicar mayores restricciones fabricantes de móviles como apple google android y similares y en último lugar con un 12% tenemos en la votación era desarrolladores con moral es decir estos desarrolladores que ofrecen aplicaciones gratuitas porque hacen dinero su modelo de negocio es vender nuestra información pues bueno deberían pensárselo dos veces antes de vender nuestra información o al menos indagar un poquito a ver a quién se la venden y qué uso van a hacer de esta información pues interesante como siempre y yo pues aprovechar a dar las gracias a la gente que nos apoya económicamente en patrón especial mención a jm barroso en este episodio por subir su aportación de hacker altruista a hacker social esto quiere decir que vamos a tener una llamadita con él mensualmente y con otros que nos apoyan que bueno tenemos debates súper interesantes en persona y en directo que mola muchísimo y no sólo no sólo nos podéis apoyar un patrón a través de patrón puntocom barra tierra de 'hackers' sino que si no podéis económicamente pues ya sabéis como siempre compartir el podcast con amigos y compañeros y dejarnos reseñas que eso ayuda un montón y también nos apoya monas como siempre una empresa que comparte los mismos valores que tierra en hacker se hace en la seguridad más accesible y transparente nosotros a través de un podcast y mont a través de una herramienta de gestión y visualización de telemetría de datos de seguridad una empresa fundada en sillicon valley que está buscando muchos ingenieros sobre todo con algo de experiencia en seguridad para ayudarles a construir y hacer realidad su misión lo mejor de todo es que están contratando en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web como siempre en mont puntocom mn puntocom y les podéis contactar en el correo tierra de hackers monat puntocom en este episodio también nos apoya en branding en tierra de hackers como decimos siempre contamos por decenas los emails que nos llegan de los oyentes que han sido víctimas de robo de sus cuentas en redes sociales y también casos de acoso online pues son branding es una empresa formada por especialistas en varios ámbitos que se enfoca en la reputación online han ayudado desde personas como tú y como yo hasta famosos a recuperar cuentas comprometidas en redes sociales llevar a juicio casos de ciberacoso ayudar a empresas en situaciones donde se respeta donde su reputación estaba siendo mal intencionadamente dañada e incluso a borrar la huella digital que dejamos online no sólo han decidido apoyar el podcast sino que si les contáis que venís de parte de tierra hackers tendréis un descuento adicional en sus servicios así que si necesitáis ayuda recuperando vuestras cuentas o reputación online quizá un branding punto es barra contacto y no os olvidéis de mencionar a tierra de hackers para ese descuento y yo creo que con esto ya podemos empezar yo diría que ya hemos hablado de ok está en el pasado y de ataques contra esta plataforma de single sign-on corporativo y hoy será otro de esos días en los que hablaremos de opta pero con consecuencias y giros muy interesantes por refrescar la memoria ok está es una solución empresarial que permite a los empleados registrarse y loguearse en todos los servicios que una empresa puede tener internamente por ejemplo una empresa puede usar dropbox como solución de almacenamiento en la nube gmail como solución de correo electrónico corporativo duilio para el envío de mensajes sms para marketing mails impuestos para hacer lo

mismo pero por correo electrónico slack para comunicarse entre empleados etcétera básicamente lo que quiero decir es que lo normal es que las empresas utilicen multitud de soluciones que ofrecen terceros para llevar las operaciones diarias necesarias para gestionar la empresa no las empresas no escriben todo el software que utilizan ellos mismos siempre pues se utilizan soluciones que ya en vez de que cada empleado tenga un nombre de usuario y una contraseña para cada uno de los servicios se suele optar por soluciones tipo single sign-on esto quiere decir que tienes un solo nombre de usuario y una sola contraseña única para acceder a todos los servicios de la empresa básicamente esto se traduce en que cuando llegas por la mañana a la oficina te lo veas una sola vez y luego cuando por ejemplo vayas a dropbox punto como a gmail.com etcétera accederás automáticamente sin tener que volver a introducir tus credenciales por detrás lo que está sucediendo básicamente esto cómo funciona que utiliza uno de estos estándares de autenticación de los cuales hay varios y una de las empresas que ofrece esta solución a corporaciones pues es la famosa octa si tú por decirlo de alguna manera accedes ad hoc está de ahí ya puedes acceder a todo lo demás automáticamente gracias al single sign-on esto es con lo que os tenéis que quedar para entender lo que ha sucedido en esta noticia y por supuesto uno diría que que ostras esto es buena idea o no pues tiene ventajas y desventajas y es todo que una empresa utilice el sistema single sign-on por un lado pues tus empleados no tienen que estar eligiendo contraseñas distintas para sus usuarios para cada servicio que tiene es cada vez que tienes un empleado nuevo pues tienes que darle 50 mil contraseñas aparte ya sabemos que los humanos somos malos por defecto utilizando contraseñas por lo que tendrías que utilizar un gestor de contraseñas para almacenar las todas entonces utilizar un sistema que te permite tener una contraseña única pues tienen sus ventajas por supuesto la desventaja es que si eso falla si se compromete si la seguridad de esa contraseña es débil pues ahora ese es el acceso a todos los servicios no pues bien hace unas semanas una empresa de ciberseguridad llamada group ayby publicaba un detallado reporte sobre el uso de una nueva campaña de phishing contra 130 organizaciones y que resultó en 9 1931 mil cuentas de empleados comprometidas a esta campaña masiva de phising le han denominado octavus ya que como os podéis imaginar y dada la intro sobre el acta que os acabo de hacer está estrechamente relacionado con esta empresa y su servicio de single sign-on en realidad el revuelo de estos ataques empezó semanas antes a principios de agosto de este año cuando tulio publicó que había sido víctima de unos ataques de phising a los que algunos de sus empleados cayeron en la trampa entregando a los delincuentes no sólo sus credenciales a sistemas internos de tulio sino también los códigos de autenticación de doble factor cabe destacar que si opta lo podemos ver como un punto crítico para la seguridad ya que da acceso a todos los demás servicios duilio a su vez también lo puede ser ya que es un servicio normalmente utilizado para enviar códigos de autenticación de doble factor a través de mensajes sms o códigos de registro para aplicaciones de mensajería signo por ejemplo tú cuando te vas a registrar en telegram o signal pones tu móvil recibes un código lo pones en la aplicación y ya está no tienes un nombre de usuario y contraseña pues ese mensaje por detrás signal está utilizando la empresa duilio para enviarlos porque tú hilux una empresa que te permite de manera programática enviar miles y miles de mensajes no por eso estudio un objetivo tan valioso para los delincuentes al igual que como explicaba lo puede ser opta tanto es así que el periodista de vice news lorenzo francesco biker ai publicó un artículo en el que no sólo comentaba cómo los delincuentes usaron el acceso que consiguieron a tulio para comprometer cuentas de signal sino que tras las investigaciones de expertos los delincuentes sólo comprometieron tres cuentas

designar sólo fueron a por tres números de teléfono y una de ellas era la suya la de esta periodista aquí la cosa como veis ya se pone mucho más interesante tenemos a un grupo de delincuentes comprometiendo sistemas críticos como tú y oct a que están íntimamente relacionados con los sistemas de autenticación de miles de empresas por todo el mundo para luego pivotar a comprometer otras empresas y sistemas que utilicen estas plataformas como es el caso de signal para en el último paso comprometer a periodistas como francesco que se centran en informar sobre ataques de ciberseguridad y grupos de ciberdelincuentes cualquiera de los pasos de esta serie de intrusiones encadenadas requiere dedicación recursos y cierta sofisticación pero es que encadenar los como lo han hecho pues todavía más bueno o no porque lo cierto es que todo empezó con una digamos sencilla campaña de phising como decía con sencilla me refiero a que simplemente los delincuentes se dedicaron a hablar a enviar miles de mensajes con enlaces a webs falsas que se hacían pasar por las web legítimas de octa y otros y otras empresas utilizando términos relacionados con la autenticación como mf a que viene de multi factor authentication vpn que ellos hablamos mucho o ss o que viene de single sign-on encontraron de hecho 169 dominios únicos utilizados para esta campaña de phising y observaron que todos se automatizó con un nuevo kit de phising que no sólo gestiona todas las web y recolecta los credenciales sino que utiliza telegram para notificar a los ciberdelincuentes cada vez que se roban credenciales nuevos de una víctima algunos ejemplos de estas dominios o urls falsas pues son gente mf puntocom que el cliente y como sabéis es uno de los si no el mayor compañía telefónica de móviles en eeuu o sea que sería idéntico con mf y no como multifactor authentication de haití en ti puntocom otra es mail gran guión o cta puntocom el ghanés un servicio para enviar correos electrónicos masivos otro metro peace ya es un hecho aquí vemos otro ejemplo me tropiece y ese es otro compañía telefónica en eeuu o igor guión que mobile.com una vez más y van a por compañías telefónicas estos son sólo algunos ejemplos de los 169 dominios que os decía que se han conseguido digamos linkar a esta campaña de phising estos dominios que apuntan a páginas web falsas pero muy convincentes ya que estaban diseñadas explícitamente para ser idénticas a las reales se enviaban de manera masiva a través de mensajes sms a las víctimas como se mencionaba y os doy dos ejemplos uno que me encontré que era en el caso en el que lo utilizaban para enviarlo a ingenieros que trabajan para cloud fer decía lo siguiente alerta tu horario de cloud fuera ha sido actualizado por favor haz clic en closer guión o cta puntocom para ver los cambios entonces si el ingeniero le daba en el mensaje a esta url pues le llevaba a una página web falsa pero que se veía exactamente igual a que él normalmente verían los empleados de cloud ver cuando se lo vean por primera vez a través de signal simon como os decía en los sistemas internos de la empresa otro mensaje es este atención to login ha caducado por favor haz clic en tu guión ss o puntocom para actualizar tu contraseña pues aquí vemos el ejemplo que se utilizó contra empleados de tulio y que de hecho funcionó muy bien porque consiguieron acceder a los a los portales de administración internos sólo con este mensaje enviándolo de manera masiva y que algún empleado se fue a y puso los credenciales y luego puso el código de doble factor y como estaba todo automatizado pues consiguieron acceder en el análisis de cloud where mencionan que el dominio falso utilizado contra ellos el que decía de cloud versión opta puntocom ese dominio había sido registrado solamente 40 minutos antes de que se iniciara el ataque esto da una idea de lo automatizado que está todo el proceso es decir utilizaban este kit de phishing no sólo para la parte difícil sino incluso para registrar estos dominios se encontraban dominios interesantes automáticamente se registran y se lanza la campaña todo a golpe de clic y

automatizado analizando el código fuente de este kit de phising al que consiguió acceder esta empresa que os decía que que publicó este detallado reporte pues fueron capaces de encontrar el canal concreto a donde el bote de telegram enviaba los credenciales que iba recolectando y también pudieron analizar más a fondo quién estaba detrás de todos estos ataques esto es porque te alegran permite obtener ciertos metadatos de los canales incluidos quienes son los usuarios que lo administraban entonces como en el código fuente del kit de phishing utilizado para esta campaña estaba en el código justo el enlace al canal de tele es mirando los metadatos vieron que uno de los administradores tenía el apodo de x y en la biografía que telegram te permite añadir a tu perfil ponía lo siguiente 22 años de edad software developer bueno pues a partir de aquí grupo ivi sé que se dedica también a temas de céret intel de análisis de amenazas de inteligencia por lo que gracias a esto tiene un sistema de monitorización de canales de telegrama utilizado por delincuentes conocidos para ayudar a investigar los aseos ellos ya hace tiempo que van digamos monitorizando canales que se sabe que se suelen utilizar para temas delictivos y gracias a ello pudieron correlacionar a este usuario x con actividad previa en otros canales que datan de 2019 y que exponían su cuenta de twitter es decir el usuario que encontraron administrando el canal a donde se enviaban las contraseñas de phising por este kit de phising tenía actividad previa en canales y había puesto su cuenta de twitter la herramienta de grupo ivi también recolectó el nombre real que tenía la cuenta de telegram antes de que la cambiase a equis grupo ivi buscó la cuenta de twitter en google lo cual les llevó a una cuenta de git hub que contenía el mismo nombre de usuario y foto de perfil un poco verificando una vez más que estaban tras la pista correcta pues esta cuenta de grit hub las cuentas de hija te permiten decir dónde dónde vives no o dónde estás localizado pues indica que la persona detrás de esta cuenta vive en carolina del norte eeuu así que ya veis aparentemente sólo se requiere poner a un chaval de 22 años al mando de una operación típica de phising para llegar a comprometer cientos de empresas y que acaba teniendo repercusiones hasta en periodistas de investigación como decía la campaña de phising en sí no ha sido especialmente sofisticada lo bonito por así decirlo ha estado en encadenar y re aprovechar el acceso que iban ganando para ir comprometiendo otras empresas de las que a su vez depende la seguridad de muchas otras corporaciones toda una escalada de privilegios saltando de empresa en empresa para dominarlo todo francesco el periodista que os mencionaba antes menciona que signal tiene mecanismos para evitar que le pudieran robar su cuenta específicamente el registro es john locke pero que él no lo tenía activado este es un gran fallo y que él mismo reconoce nosotros os invitamos a revisar que lo tengáis activado en todas vuestras aplicaciones de mensajería esto previene que aunque alguien intente registrar tu cuenta de signal o telegrama en un nuevo móvil si es capaz de recibir los mensajes enviados a tu número se necesitaría a mayores un pin que han configurado previamente para complete completar el proceso de registro no vale sólo con que sea capaz de recibir los mensajes que te llevan al móvil que era el caso de estos tipos delincuentes al haber de la plataforma de julio sino que además tendrían que saber el pin que debería haber configurado francesco pero que no hizo por eso es vital que activas este mecanismo de seguridad añadido que ofrecen todas las plataformas de mensajería francesco menciona también que gracias al diseño de signal los delincuentes no tuvieron acceso a los mensajes enviados previamente al ataque ni a los contactos pero sí pudieron enviar mensajes a la gente haciéndose pasar por el periodista durante un periodo de 13 horas que fue lo que tardó en recuperar la cuenta ya que comenta en el artículo que no tenía acceso al dispositivo donde tenía instalado signal cuando se enteró de todo esto recordemos que francesco es un periodista de investigación del que

hemos cubierto varias noticias por cierto y que utiliza signal en parte para comunicarse con gente que le manda información pero que quiere mantenerse anónima es posible que ésta sea la razón por la que los delincuentes fueron explícitamente a por su cuenta no está francesco quizá trabajando actualmente en algún tipo de investigación muy secreta y querían saber quién era el que estaba detrás de las filtraciones oa lo mejor teniendo en cuenta que posiblemente pues esté detrás un chaval de 22 años a lo mejor fue justo a por francesco como para que luego él cubriera la noticia y darle un poco pues esa esa familia de salir en vice music que te lo cubre un periodista porque le has demostrado que le podéis te comprometer su cuenta de signo a saber en cuanto a empresas afectadas y centrándonos en las que dieron pie a comprometer servicios adicionales encadenados como os contaba anteriormente tenemos a la empresa de marketing clavillo de la cual robaron listas de correos de personas que tienen alguna relación con cripto monedas estas listas contenían nombres completos direcciones de email y teléfonos que ahora podrían utilizar para enviar más campañas de phishing específicas para temas de cripto monedas también comprometieron mails en la famosa plataforma de envío masivo de correos electrónicos para campañas de marketing pero por ejemplo empresas como digital que ofrece servicios de vps sistemas así utilizan mails para enviar correos de reseteo de contraseñas lo cual facilitaría a los delincuentes comprometer usuarios de digital ouzo y por supuesto como ya os contaba tulio que facilitó comprometer cuentas de signal al poder acceder a los mensajes de registro que contienen el código temporal en cuanto a los usuarios específicos afectados he buscado en las cifras en los reportes he visto que por ejemplo en españa ha habido 12 víctimas en mexico 9 en argentina 4 y en colombia 3 esto pues comparado a los 5.503 afectados en eeuu parece poco aunque bueno proporcionalmente pues hay muchas más víctimas posibles no potenciales en eeuu os dejo en las noticias del episodio como siempre no sólo el artículo de francesco y la nota de prensa de tulio sobre la intrusión en sus sistemas sino también el reporte de grupo ivi para que podáis indagar técnicas tácticas y procedimientos de este grupo de delincuentes me encanta la noticia martín y la he escuchado esta noticia hace poco y me pareció digo me la tengo que leer pero a ver si martín me la cuenta así que muchas gracias por acordarme porque 9 si es que ya te digo porque lo interesante de esto fue yo cuando empecé a fijarme en ella que supongo que tú igual fue cuando tú y yo que esto empezó con tulio publicando que habían comprometido su sistema de a través del phising porque luego fue cuando vino francesco con su artículo diciendo que le habían comprometido signal a través de alguien comprometer tulio pero es que luego vino grupo ivi diciendo que en realidad la campaña contra tú y yo había afectado a otras 168 empresas que a su vez también ofrecían servicios críticos para otras empresas súper interesante vamos que se supo un poquito al principio y luego se fue desarrollando la bomba claro está yo más por eso a veces pues podemos tardar unas semanas en cubrir una noticia primero a veces porque intentamos seleccionar por las mejores o las más novedosas pero también porque esperamos a desarrollarla y las co y las vamos siguiendo para que tener suficiente contenido para que os podamos brindar pues toda la información por supuesto nos queremos documentar y ser buenos investigadores como francesco es activa decir no diga periodista por nuestro signo tanto tú como yo que tanto tú como yo tenemos el registro y son lo justo y estaríamos por face justo marcado está está activado en mención a este antes que que han utilizado una plataforma para comprometer estos factores en ti key son estos códigos no sé si es mencionado el nombre creo que no pero nacionales y line o lo que mencionaba era que utilizaron una un kit de phising que esto viene a ser una aplicación programa a una pieza de software que han escrito ellos mismos que no habían habían visto hasta

ahora los investigadores de hecho la manera en la que encontraron el código fuente fue analizando las páginas de phising que generaba este software y encontraron una imagen que se utiliza legítimamente octa pero en la plataforma de phising está la utilizaba en un directorio muy específico no a nivel de digamos de html y todo esto entonces lo buscaron en virus total y de donde sobra es conocido que incluso los delincuentes utilizan virus para ver si detecta si detecta algún tipo de malware en lo que con lo que estén operando y según el reporte lo que dice grupo ivi es que parece ser que este este kit de fishing lo debían de pasarse entre varios grupos de delincuentes a lo mejor vendérselo y uno de ellos antes de ejecutarlo lo paso por virus total para asegurarse que no contenía ningún malware y es así como entonces el grupo iba buscando ese hash de esa imagen utilizada legítimamente por octa pero que estaba en un directorio muy específico al al kit de malware encontraron bueno el reporte pone pues yo que sé pues como 50 falsos positivos pero un correcto positivo que entonces es como encontraron pues la infraestructura y consiguieron descargar cierto código d es donde vieron todo el tema del canal de telegrama donde se enviaba y todo esto pero vamos que para contestar a tu pregunta utilizaba un software desarrollado por ellos para automatizar todo el proceso en todo lo que hacía era registraban los dominios que creaban las páginas web esto me imagino que ya estaba programado pero dependiendo de a qué empresa quisieras que creaba la web falsa que te la metía en ese dominio y luego cuando la víctima metía el nombre usuario y contraseña y acto seguido le pedían la autenticación de doble factor de manera automática porque pensamos que solo hay una ventana de tiempo de 30 segundos normalmente en estos códigos que se generan cada 30 segundos automáticamente va y ya se logra de manera expresa y automática en los sistemas de la organización que evidentemente ha habido una investigación por parte de los delincuentes anteriormente porque muchos de estos portales están expuestos a internet pero claro no tienes credenciales pues eso es lo que hacían interesantes y lo mencionaba porque bueno igual como lo hice como dices una nueva plataforma pero yo sobre noticias han ido saliendo temas y hay algo que se le parece que se llama world proxy que es un servicio que ofrecen cibercriminales que es justo hace esto ofrecen un servicio de eso de comprometer estos tokens de doble factor tú le exponen si la empresa que quiere suplantar y adonde lo quieres enviar no te ofrecen realmente en los binarios el software para hacerlo sino que te ofrecen acceso a la plataforma fishing access services y pones ahí sus víctimas los emails direcciones de correo electrónico y te dan los tepes los los códigos de éstos y quería comentar también que hay una herramienta open source en beat hub que se llama y buildings 2 bueno está bastante avanzada y se utiliza bueno la hemos utilizado para ejercicios de ingeniería social en ejercicios de red timming para comprometer esto en credenciales y también los los códigos de doble factor que la vamos a poner en las notas del episodio por si todo es para para temas de mejorar la seguridad de las empresas no es para abusar de esta herramienta pero por si lo en nuestros clientes quiere hacer bueno voy a probarlo ellos mismos el otro comentario que me ha apuntado que quería comentar también era el tema de los dominios que se crean automáticamente eso es interesante pero desde un punto de vista de offset no el hecho de que el dominio sea tan joven en los equipos de seguridad debería saltar una alarma y en plan tiene un par de horas de vida esto debe efectiva lanzarse una investigación debería tener algo automatizado que que me lo marque como spam o ponerlo temporalmente en cuarentena y también lo que hay es lo que se da no específicamente para ataques de ingeniería social con un toque cibercriminal pero hay sitios online que venden dominios así como criados no de crianza como el vino que ejerces gente que los tiene durante un tiempo con activa los costes de actividades legítimas con un

un nombre parecido a alguna empresa grande y luego pues eso los crían y después de unos años un tiempo dice monada ahora lo voy a vender y voy a cobrar bastante dinero y seguro que viene alguien con buenas intenciones o malas y lo compra y entonces muchos cibercriminales van a estos sitios para comprar dominios también para que no se note que son tan nuevos muy buen apunte tú lo a lo que hace referencia es utilizarla cuánto tiempo lleva registrar o no un dominio como digamos el indicador de los sospechosos que puede ser es evidente que justo a empleados le estén llegando sms es para que vayan a un dominio que lleva registrado 40 minutos pues se podría asumir como algo sospechoso y de hecho existe muchísimo software que intenta hacer temas digamos de de prevención de phising y tal que uno de los indicadores en los que se fija es esto y como tú bien dices por eso hay muchos criminales o bueno gente con visión de negocio que se dedica a registrar empresas y digo perdón dominios interesantes para el futuro para poder saltarse estas protecciones cuando los dominios ya tienen dos años o tres años pues digamos que tienen cierta reputación a la hora de evaluar la peligrosidad precisamente pues porque tienen ya pues años de existencia de hecho hay servicios yo me encontrado con servicios que detectan dominios que tú puedes monitorizar para cuando se pongan a la venta otra vez entonces tú lo compras y como ya existe hace mucho tiempo y se ha puesto a la venta y lo vuelves a comprar tú pues pues también te digamos que tiene esa reputación establecida ya así que eso es otra otra manera interesante de poder saltarte algunas de estas protecciones sí sí sí bueno incluso a veces hay gente que no tiene el auto ruin you el auto renovar y cuando caduca los extras de ahí y tasca y en la vida está que es de hecho de esta forma así que activar el auto auto relación asegura de que es una buena tarjeta de crédito y estáis seguros pues nada vamos con la siguiente noticia que tiene un toque un transfondo político pero disclaimer comentarios y no solemos comentar noticias un transfondo político pero está principalmente por la reacción de la nación afectada y el transfondo tecnológico en sí sobre los ciberataques involucrados pues bueno creemos que merece la pena traerla al podcast y comentarla así que la comentó recientemente el gobierno albano lanzó un comunicado público sobre un ataque que habían sufrido sus sistemas gubernamentales esto sucedió el 15 de julio y desde entonces los equipos de respuesta a incidentes albanos han estado trabajando duramente 24 por 7 para poder restaurar las operaciones del gobierno y reparar el daño causado por el ciberataque según el primer ministro albano edi rama el ataque falló según él gracias al buen sistema a la buena seguridad de los sistemas cibernéticos del país y a la ayuda de equipos especiales que han venido a apoyar a albania entre los que se encuentran microsoft mandián bueno y equipos de la otan de hecho hay un vídeo que publicó este hombre y rama en twitter pero lo vamos a poner en las notas del episodio es muy interesante de ver porque es no sé es bastante impactante como de película sale el hombre ahí en primer plano con la bandera al banna y europa que no es parte de europa pero bueno para el colegio no para hacerse para demostrar que está de a favor de europa aunque creo que quiere entrar en europa pero bueno esta está en ello no pero tiene un aire de esos vídeos y estilo no sé me recordó un poco ya lo vais a ver cuando los pongamos en la nota del episodio pero aún un estilo así de esos vídeos del grupo anonymus pero este emitido por un gobierno porque dice muy claramente lo que ha pasado que está un poquito bastante decepcionado y enfadado con los acontecimientos y cómo va a responder no es la verdad que es interesante empieza indicando que el 15 de julio de este año albania sufrió un ciberataque contra la infraestructura digital del país que buscaba este ataque lo que intentaba hacer era paralizar los servicios públicos borrar datos digitales de los ciudadanos del país acceder y modificar datos gubernamentales robar datos y comunicaciones internas del

gobierno y bueno en definitiva causar un estado de caos e inseguridad en el país esto es lo que decía que el ataque intentaba hacer pero según el fallo en el intento que no esto no sé si es del todo cierto porque causar un caos en el país bueno esto no se dio pero sí que los atacantes comprometieron sistemas y accedieron a datos y ex filtraron estos datos así que no es un intento un éxito al cien por cien pero tuvo cierto éxito y cierto fallo no a consecuencia de esto y como represalia aunque comenta el primer ministro albano no deseada albania cortó inmediatamente toda relación diplomática con irán con iván bueno ok ahora entró en detalle por qué no y pidió a todos los diplomáticos iraníes en tierra al banna que se marcharán del país inmediatamente en un plazo de 24 horas desde este comunicado de hecho momentos después de que los funcionarios iraníes abandonaran la embajada la policía albanesa allanó el edificio en busca de cualquier prueba incriminatoria que pudieran haber dejado que pudiera haber sobrevivido a probablemente estas prácticas típicas no de cuando te tienes que ir venga vamos a golpear el disco duro vamos a ponerle imanes por encima vamos vamos a intentar destrozarlo en la evidencia digital y también quemar documento en la evidencia física pues bueno querían fueron muy rápidos los el gobierno al vano para entrar en él las embajadas iraníes intentar buscar a ver si había algo que los incriminar a los iraníes comenta que es una decisión no deseada pero acorde con la gravedad del ciberataque y esto de hecho y es la razón por la que tenemos esta noticia el podcast es es que nunca se ha visto antes una respuesta tan contundente y tan fuerte tan grave contra un evento cibernético el gobierno iraní negó estar involucrado en el ataque pero la otan la casa blanca eeuu el gobierno del reino unido publicaron declaraciones en apoyo al gobierno albanés y su atribución del ataque a irán están todos de acuerdo que fue irán el que causó este ciberataque el objetivo principal de la operación parecía ser una conferencia de un partido en oposición al gobierno iraní que se llama organización edén calc o en inglés people's muyaidín cuyo acrónimo sería make mk pues así me voy a referir a ellos no sé si lo pronuncia bien pero bueno next la conferencia estaba programada para el 23 de julio pero finalmente se pospuso no ha tenido lugar debido a las amenazas terroristas a todo el revuelo que ha causado la intrusión cibernética y bueno de ahí se pensaba que podía llegar a mayores más temas físicos y porque iba a tener lugar dicha conferencia en albania bueno pues porque albania alberga a miles de disidentes iraníes que forman parte de este partido de oposición contra el gobierno iraní y el grupo encontró refugio en albania en 2016 a pedido del gobierno de eeuu después de que el régimen iraní declarara al grupo como como una organización terrorista y comenzará a cazarlos ni más ni menos total que los atacantes que se auto apodaron homeland justice justicia de la nación pudieron comprometer diversos sistemas del gobierno albanés con ransomware y malware wiper que hemos mencionado en algunos otros episodios este malware wiper lo que hace es eliminar todos los datos no solo de los discos duros y los sistemas ficheros sino también va más allá intentar borrar o destruir o manipular el master boot tracor no es esta esta zona esta esta función de arranque de un sistema que si se si se toca si se destruye pues es bastante difícil reparar el sistema al menos de forma remota o incluso a nivel de firmware de la bios y wifi también podrían llegar a ese punto total que usaron malware ransomware y wiper y publicaron también los datos que comprometieron en la web home land justice punto r y en su grupo de telegram especialmente no sólo datos de los ciudadanos sálvanos sino más bien los datos de los miembros de este partido m acá en oposición del gobierno iraní curioso porque el top level domain este la extensión digamos del dominio punto rv está asociada con la nación rusa pero bueno ellos iraníes aunque bueno un dato interesante es que tanto las imágenes de la web porque tenían un logo no pusieron su logo en la web y en el grupo de telegram estas imágenes estos logos

se parecen o hacen referencia a las del grupo también cibercriminal predator y sparrow y quién es este grupo pues es un grupo que se dio a conocer en febrero de este año por en declarar haber causado daños físicos contra tres fábricas productoras en irán incluyendo fuegos y destrucción de las operaciones y publicaron incluso vídeos al respecto que demostraban este fuego aunque los directores de las fábricas afectadas comentaron que no que no se dieron dichos ataques y que esto no tiene sentido de todas formas el gobierno de irán atribuyó este grupo de amenazas predator y sparrow con israel y como dato curioso al que luego voy a hacer referencia el logo del grupo predator y sparrow es un círculo con un fondo con pistas electrónicas como de una placa base y en primer plano la cara de uno de los pájaros del juego angry birds que supongo que la mayoría de nuestro siguiente desconoce si no bueno es un juego así de muchos pájaros que se disparan arriba debajo ébano sobre el ataque contra albania mandiá ant junto con microsoft han estado haciendo investigaciones al respecto e intentando determinar quién estaba detrás del ataque mirando los indicadores de compromiso y todos los los ttp es no las los comportamientos tácticas en técnicas utilizadas por los atacantes quienes se bueno bastante listos por su parte intentaron un poco marear la perdiz no intentar disfrazarse disfrazar para que no les pudieran determinar y saber quiénes eran los atacantes intentaron cubrir su origen para evitar que se determinara de dónde venían e intentar evitar una atribución exitosa y de hecho se hicieron pasar por nacionalistas albaneses sin embargo si se presta atención al logo del grupo homeland justice que está en su web y en el grupo de telegram éste muestra un águila cayendo sobre el logo de predator y sparrow mostrando como un pájaro del juego de angry birds como mencioné anteriormente pero dentro de la estrella de david un símbolo judío asociado con israel así que esto sirve de atribución de este grupo con irán porque bueno obviamente están cayendo contra israél el principal enemigo de israel es irán de una parte y luego además en la imagen se muestra un mensaje que dice por qué deberían gastarse nuestros impuestos en apoyar a terroristas de durres esto es una referencia al grupo de oposición iraní make a quienes irán considera terroristas como he dicho y que tiene un gran campo de refugiados en el condado de durres en albania con esto lo que se intenta es disfrazar primero como si fuera un ataque causado por ciudadanos albanos porque mencionan nuestros impuestos verdad pero todo apunta a que es un grupo ciber terrorista iraní por el tema de que el águila cae sobre la estrella de david asociada con israel y de hecho tanto mandián como microsoft confirman la atribución del ataque a un grupo iraní que es el mois que es la abreviación del ministerio de inteligencia y seguridad de irán y de hecho también hay evidencia forense digital al respecto microsoft mencionaba cuatro puntos que apuntan directamente a irán aunque bueno se pueden coger con un poco de escepticismo porque toda evidencia digital puede ser falsificada verdad el primer punto es que se observó a los atacantes operando désde irán bueno aquí uno puede decir bueno pues se coge una vpn y se sale desde irán no pero bueno lo dejamos ahí el segundo punto es que los atacantes utilizaron herramientas anteriormente vistas que habían utilizado otros atacantes iraníes conocidos esto lo mismo si otro grupo las consigue pues la puede reutilizar pretendiendo ser ese grupo que las ha creado estas herramientas el código del malware wiper fue utilizado anteriormente por un conocido actor iraní lo mismo que el anterior sí he encontrado la herramienta wiper del otro actor al que quiere suplantar pues podría disfrazarme y el último punto es que el ransomware fue firmado por el mismo certificado digital utilizado para firmar otras herramientas utilizadas por actores iraníes esto ya igual sería un poco más convincente porque haber firmado un archivo un binario con un certificado significa que tienes la clave privada aunque en ese caso también se pudiera ver del caso que que se hubiera

filtrado de alguna forma y este otro grupo que quiere suplantar al original pues la pudiera haber conseguido y utilizado para firmar sus binarios sí estoy totalmente de acuerdo contigo porque lo que decías ahora que se utilizaba como atribución que si un logo está hecho de cierta manera para interpretarlo así y tal es todo como muy cogido con pinzas él cuando hablas ahora ya de firmar digitalmente con un certificado ahí hablamos de matemáticas lo cual no quiere decir que no se haya robado esa clave privada entonces se puede utilizar pero ya requiere más que simplemente tener creatividad para crear un logo y que otro no puede hacerlo para hacerse pasar aparte en tierra de hackers hemos hablado en miles de ocasiones de ataques de falsa bandera que se sabían que eran de falsa bandera para hacerse pasar por ataques provenientes de una nación rival sí sí de hecho es una buena técnica de cibercriminales hacerse pasar por otro espacio para crearles derecho bueno los grupos de ransomware lo están haciendo no eeuu aplica sanciones contra con ti y con te dice ya nadie me va a pagar me voy a hacer pasar me cambió el nombre ahora me hago pasar por otro bueno o similares pero bueno y como he dicho mandianes y microsoft confirman la atribución del ataque a un grupo iraní del moix como he dicho del ministerio de inteligencia de seguridad de irán que bajo el liderazgo de una persona llamada smile qatif dirige varias redes de actores de amenazas cibernéticas involucradas en espionaje ciber espionaje ataques de ransomware y similares en apoyos en apoyo de los objetivos políticos de irán de hecho el moisés un grupo operaciones ofensivas que desde al menos se tiene constancia desde el 2007 ya están realizando actividades ofensivas de este tipo y bueno sus sus empleados sus actores cibercriminales se han llevado a cabo operaciones maliciosas dirigidas a una variedad de organizaciones gubernamentales y del sector privado en todo el mundo incluyendo infraestructura crítica y este grupo es famoso también bueno por haber causado ataques contra israel arabia saudita los emiratos árabes jordania kuwait y chipre y seguro que deben en algunos más que se nos escapan en sobre los detalles del ataque que han publicado microsoft mandián microsoft en concreto pudo vincular el incidente con cuatro grupos de amenazas iraníes diferentes y detalló cómo trabajaron juntos para violar las redes del gobierno albanés desde ya finales del 2021 microsoft dice que estos cuatro grupos trabajaron bajo la guía bajo el control uno de los grupos hizo un poco un análisis un sondeo de la infraestructura externa del país de albania otro de los grupos implementó desarrolló el software el malware ransomware wiper otro grupo lo que hizo es obtener acceso inicial y extraer algunos de los datos que incluye tanto datos del gobierno albanés como de los residentes albaneses ya sean ciudadanos o su objetivo principal los del grupo a la oposición iraní nec y hubo otro grupo que estaba solo enfocado en extracción ex filtración de datos no voy a comentar brevemente las cuatro fases más importantes digamos del ataque la primera es el acceso inicial verdad como como penetraron el perímetro de los sistemas del gobierno al vano y te voy a hacer un poco esa pregunta a ti martín cómo crees que que penetraron en el perímetro digamos lo bueno a ver albania no sé qué grado de sofisticación tendrá a nivel cibernético no había escuchado mucho de ellos la verdad siempre normalmente bailamos en torno a él israel eeuu irán corea del norte china si gran bretaña algunos países europeos pero de albania pues no sé entonces yo me imagino sin tener ningún conocimiento quizá me apostaría por sistemas sin actualizar alguna vulnerabilidad ni siquiera digo de cero de iu pero sistemas sin actualizar que que no es fácil hacerlo y tener todos los sistemas al día y que a lo mejor pues en un país como albania que tendrá pues digo yo en sus limitaciones en sus recursos pues a lo mejor está todavía está con sistemas obsoletos y que según windows 2000 o algo así no sé para para su administración electrónica no sé pues acertaste martín diste en el clavo los tras 11 pudiera haber me acabas de dejar muy bien esto

con confirmamos que no estaba preparado pero digo yo es lo que me imagino pensando en los recursos de ese país sí sí bueno no sé no sé qué tantos recursos tiene pero un tanto que hablamos de ingeniería social igual algún oyente hubiera pensado pues un ataque de phising y especialmente si habíamos comentado la de tulio anteriormente con todo esto de físicas de service y tal pero no aparentemente en de hecho a partir de mayo de 2021 el año pasado los actores explotaron vulnerabilidades de un servidor de aplicaciones web expuesto en internet para ejecutar código un tomcat de estos no el hecho según parecer a un servidor de sharepoint que no estaba parcheado y pudieron subir una web sheild que es una página digamos sencilla que permite ejecutar comandos a nivel del sistema operativo y de ahí bueno pudieron pivotar y meterse de forma hacia el interior de la red subir descargar archivos ejecutar comandos malware y similares después de ahí bueno lo típico no movimiento lateral pues utilizaron primero utilizaron mmm y cats las herramientas míticas para todos todo este tipo de ataques o incluso en campañas de derretimiento que también usamos para obtener las credenciales digamos de estos sistemas en local y comprometieron al administrador y de esa forma bueno se conectaron vía escritorio remoto remote desktop protocol y con la librería de impact et para conectarse a diferentes sistemas windows y moverse de un sitio de un sistema al otro eso dice mucho o sea ya no sólo que tenían sistemas desactualizados pero si están utilizando impact y mimi cats ya habla también de lo pobre que es su capacidad de detección porque vamos a estas herramientas cualquier mínimo software te las va a detectar digamos para para proteger tu infraestructura o sea que debía ser nula como para que ahora se me ocurre como para hacer atribuciones o sea si tienes los sistemas sin actualizar porque no tienes recursos y oye hay países más humildes unos que otros y con recursos tienes que trabajar con los recursos que tienes y no tienen recursos para detectar ataques internos con herramientas que están disponibles para todo el mundo joder pues no sé yo qué capacidad tienen para atribuir los ataques si la verdad es que no se menciona exactamente qué solución de idear desde en detección en response tienen desde este sistema de como antivirus que combine antivirus y detección y respuesta pero bueno si lo que tú dices igual tenían uno que no estaba tampoco actualizado o uno que no era muy bueno y una vez ahí se movieron lateralmente de un sistema al otro consiguieron encontrar los datos que de hecho se centraron básicamente en correos electrónicos de los sistemas exchange microsoft chains desde el gobierno urbano y de ahí estuvieron recopilando datos desde octubre de 2021 hasta enero de este año así que unos tres meses mirando correos recopilando los todos y luego los ex filtraron también vía correo electrónico yo me pregunto cómo lo hicieron en plan no se excitaría muchísimos datos lo cortarían los archivos en diferentes archivos muchos archivos en un email pocos emails con muchos archivos son muchos emails con pocos archivos bueno esto esto también se ve sospechoso a nivel de sistemas de seguridad que deberían haber intentado investigar antes pero bueno finalmente su objetivo también era causar un poco de de barullo de acá o es un poquito y desplegaron su malware ransomware y wiper y lo activaron el 15 de julio de aquí comentar como he dicho anteriormente albania ha tenido apoyo global de eeuu inglaterra la otan en general y de hecho han han emitido sus reacciones en concreto eeuu emitió una declaración de apoyo a albania confirmando la atribución al gobierno de irán y diciendo que tomará más medidas para responsabilizar a irán por acciones que amenazan la seguridad de un aliado de eeuu y sientan un precedente preocupante para el ciberespacio de hecho la oficina de control de activos extranjeros del departamento del tesoro de eeuu ha acusado al ministerio de inteligencia y seguridad e inseguridad de iran el mois y el suministro de inteligencia por participar en actividades cibernéticas contra eeuu y sus aliados

literalmente decía así el ataque cibernético de irán contra albania ignora las normas de comportamiento responsable del estado en tiempos de paz espacio que incluye una norma sobre abstenerse de dañarla en la infraestructura crítica que brinda servicios al público no toleraremos las actividades cibernéticas cada vez más agresivas de irán contra eeuu o nuestros aliados y socios atacar los sistemas gubernamentales con whiters para detener una conferencia es totalmente desproporcionado e irrazonable por lo que se necesita una respuesta contundente para evitar que este tipo de ataques se consideren aceptables bueno yo básicamente estos actos que los veían eeuu sobre todo como juego sucio no pero yo me pregunto aquí también está diciendo estos ataques no se consideran aceptables pero en la guerra en el mundo en general hay hay reglas en el ciberterrorismo en el ciberespionaje pero si están todos los paises espiándose los unos al otro de esteban esta declaración me parece un poco interesante sí me gustó eso de en en tiempos de paz en el flipper es el ciberespacio para que tiempos de paz ni que tiempos de paz si sólo hay que ver preguntar a cualquier empresa privada que se dedica al crédito martín también es verdad sería que hubiera más paz y no sea hablar de otros temas pero sí estaría bien que este podcast no pudiera existir evolucionamos y comenzaríamos otros temas tecnológicos pero bueno y nada pues como resultado eeuu declara que todas las propiedades con más del 50 por ciento o intereses en la propiedad de los objetivos designados en este caso el mois el gobierno de irán en general que están sujetos a la jurisdicción de eeuu es decir todo negocio o algo todo que esté relacionado con el móvil con el gobierno de irán en general están bloqueados y se prohíbe a las personas de eeuu participar en transacciones con ellos esto esto me parece como he dicho anteriormente como el tema de cuando conti salían un plan tanto ransomware y al final eeuu dijo como alguien le pague el ransom el rescate a conti hoy vamos incluso a dar una colleja os vamos a penalizar y vais a tener que pagar incluso más porque no queremos rosales pedía si le pagas un ransom account y queremos nosotros también otro repuesto forma de museo entre viene un grupo y no vamos a que luego nos vienen que estamos en eeuu en hay que portarse bien pero sí sí y lo dicho tú más o menos ahí y bueno hay una al menos hay una teoría por ahí alguien dice bueno una hipótesis es que los iraníes sintieron la necesidad de responder al ataque a este grupo de predator y sparrow como he mencionado antes este grupo que se asocia con israel y que atacó a tres fábricas de acero en irán y eligieron pues el ataque a la conferencia del grupo make este grupo de oposición contra el gobierno iraní como demostración de poder cifrando datos vía ransomware no y borrando sistemas gubernamentales críticos con el malware wiper y causar un poquito aquí un poco de mareo no una disrupción en la capacidad del gobierno para dirigir el país vamos que igual vamos a ver más ataques similares de otros grupos que quieren demostrar su poderío online yo me imagino que igual ahora la gente se anima y dice bueno irán ha hecho esto y está demostrando su poder no no vamos a de nosotros cualquier país no voy a mencionar pero a cualquier país así malote no de éstos yo también quiero demostrar que tengo poderío vamos a atacar aquí a otro país estos pequeñitos como tú dices que no tiene suficiente el presupuesto y tiene muchos sistemas desactualizados vamos en este caso irán en principio yo creo que tiene más capacidad ofensiva cibernética que albania no así que un poco fue una batalla es plan goliat contra david no no estaba compensada pero bueno si no se le puede se le puede proponer a estos estás estaba pensando estos países vamos a convocarlos a un concurso online de estos de como counter-strike no alguno de estos y que se pongan a competir online y se dejen de dañar a sistemas reales que causan al fin y al cabo han causado algún tipo de instrucción en el gobierno no sé algunos ciudadanos igual no han podido realizar sus actividades online bueno pues a algún tema no y con esto queridos oyentes

llegamos a la pregunta del episodio que os la vamos a plantear de la siguiente forma te parece adecuada la respuesta de albania al supuesto ataques ciberterroristas de irán y tenemos cuatro respuestas si ya que está relacionado con medidas políticas si ya que evita futuros casos para evitar otro ataque de ciberguerra esto sería como un poquito para dar una lección a los malhechores en este caso para dar una lección a irán la tercera opción la respuesta es no no mejor hubiera sido contraatacar a nivel cibernético o militar no y la última opción es no porque bueno la atribución es dudosa no sé realmente si es irán no me quiero mojar igual deberían haber investigado un poquito más antes de cortar toda relación diplomática con irán es muy interesante la pregunta y desde luego está muy bien que diste esos dos ángulos de por un lado las evidencias de por qué irán podría ser uno de los países que ataca albania los intereses políticos y él el razonamiento detrás de ello pero por otro lado también las fallas a la hora de atribuir de que es complicado en esto decir de ciberguerra de ciberespionaje poder poder indicar de manera inequívoca ha sido este no no no es como en una intrusión física que le pillas en cámara y al espía y no eres evidentemente alguien de ahí los retiene sí y todo y le interroga si tal esto son pistas cibernéticas que son muy fáciles de falsear sí sí ya uno no sabe qué es real con tanto de fake verdad sí así que bueno dice aplicado al nivel malo pues hasta aquí hemos llegado por hoy gracias como siempre por quedaros hasta el final no olvidéis dejarnos reseñas reviews comentarios que ayudan a crecer al podcast si os apetece y podéis podéis apoyarnos en patrón puntocom tierra de hackers y lo dicho gracias por quedarnos hasta el final muchas gracias nos escuchamos pronto adiós adiós chau si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente acuérdate de dejarnos un comentario una valoración donde nos estés escuchando también puedes seguirnos en twitter instagram y facebook te esperamos en el próximo episodio de tierra de hackers