koo a orch España mediante un ataque de reutilización de credenciales pésima política de seguridad y cambios en los cimientos de internet nuevo año nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 15 de enero de 2024 este es el episodio número 115 yo soy Martín vigo y Alexis porros lo tengo fuera de combate después del atracón que se pegó estas Navidades así que me tenéis a mí solo Feliz Navidad Feliz año si es que se puede decir a 15 de enero Pero bueno ya estamos en 2024 y nosotros aquí seguimos la verdad 23 hemos puesto ahí un tweet con los números con los premios que nos han dado y luego está todo este tema de que si Spotify a los a vosotros queridos oyentes os hace ahí como las estadísticas de cuánto nos habéis escuchado ibox lo mismo una pasada he puesto un tweet ahí con todos los números nos escucháis desde 56 países solo en Spotify tenemos como 300.000 escuchas solo en el año an Y eso que tenemos otras tantas plataformas desde donde nos escucháis el episodio favorito fue el de miedo a la Inteligencia artificial en el episodio 89 Así que si no lo habéis escuchado aú escucharlo porque está claro que es fue el que más os gustó de 2023 y nada aquí Seguimos más fuertes que nunca volveremos con episodios Todas las semanas en la medida de lo posible porque ya sabéis que esto no para y de verdad os Traigo una noticia que fue realmente una de las cosas que quería hacer era empezar con nuestra tradición que empezamos en diciembre de 2022 es decir el año pasado con esto de acabar el año o empezar el año con una noticia sobre los trends no sobre sobre lo que está por venir en el siguiente año es decir en este caso en 2024 pero me voy a saltar como haciendo una excepción este año esa costumbre porque la noticia que os traigo es muy reciente muy interesante y sobre todo nos ayuda a aprender cositas nuevas que es de lo que se trata siempre siempre que busco noticias intento que sean algo diferentes o haya algún término tecnología o cosa que vayamos a a aprender como siempre darle las gracias a nuestros mecenas de patreon que en patreon.com bartierra de hackers han decidido apoyarnos este proyecto que lo hacemos gratis para todo el mundo pero aún así tenemos gastos pues toda la familia de patreon muchísimas Muchísimas gracias esta vez eh tenemos nuevo a yo soy es el nombre que ha puesto en patreon Así que muchísimas gracias por unirte a la familia Ya sabes que tienes acceso a un canal exclusivo en discord donde tenemos una comunidad de más de 100 personas desde que Desde que la última vez que lo miré y creciendo y nada daros muchísimas Muchísimas gracias por estar ahí y ayudarnos a hacer esto y también a nuestros sponsors como monat que sigue desde el principio y ya sabéis es una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros lo hacemos a través de un podcast y monat con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y que está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echadle un vistazo a su web monat.com y le podéis mandar vuestro currículum a tierr deeh hackers @mon comom que así ya saben que venís de nuestra parte y yo creo que aparte de mencionar lo que suele decir Alexis que nos podéis seguir en todas las redes sociales nos buscáis como tierra de hackers estamos en todas las plataformas de podcast si todavía no estás escrito o suscrito Hazlo A qué estás esperando y yo creo que podemos empezar también nos podéis enviar por cierto un mail a podcast @ticktok bueno Supongo que ya muchos de vosotros ya lo sabéis quizá bueno quizá no tanto los que nos escucháis desde el otro lado del Charco pero hace unos días Orange España dejaba prácticamente fuera de servicio a todos sus clientes por un hackeo anunciado en directo a través de una cuenta anónima de Twitter como decía me hubiera gustado empezar el año con lo de las predicciones de 2024 Pero bueno lo dejo para el próximo episodio ya que gracias a esta noticia podemos hablar de algo que todavía no habíamos tocado El ripe Bueno

qué ocurrió el 3 de enero de 2024 es decir hace unos escasos días y concretamente a las 2:30 de la madrugada hora española una cuenta recién creada de Twitter con el handle MS Snow owo y cuyo nombre simplemente Snow twitea lo siguiente mencionaba a Orange España y decía miau miau miau he corregido la seguridad de tu cuenta de administrador de ripe Envíame un mensaje para obtener las nuevas credenciales y ponía un guiño y el tweet además adjuntaba dos capturas de pantalla de lo que parece ser el portal de usuario de ripe que reflejaba la lista de rangos de ip de Orange y algunos cambios críticos Poco después la gente empezaba a quejarse de que no les funcionaba internet mencionando a la Cuenta pública de Orange España en Twitter analicemos ahora más a fondo Qué es exactamente lo que ha ocurrido Por cierto Orange por nuestros amigos e en Latinoamérica es uno de los operadores de telefonía y proveedores de internet que opera en España como os decía quería empezar el año hablando de trends pero es que esta noticia es una fantástica oportunidad de aprender algo juntos porque qué es esto del ripe no que son esos cambios críticos que decía que se llevar a cabo que pueden resultar en en miles y miles de personas sin conexión a internet Pues yo de estos temas tampoco controlaba tanto Para serte sincero querido oyente me sonaban pero nunca me había parado a entenderlo en profundidad Así que esta noticia ha sido la excusa perfecta para remangar y ponerme a estudiar cómo funciona internet en sus cimientos más esenciales vamos al lío ripe es una organización que se encarga de la asignación y gestión de direcciones IP concretamente en Europa Oriente medio y partes de Asia su equivalente en Estados Unidos sería la aring que quizás a algunos os suene más a mí me suaba más de hecho y por encima de ambos y de otros depende de la región del país está el iana que es la Organización que opera a nivel global como os podéis imaginar el número de ips sobre todo cuando hablamos de versión 4 es limitada Y al igual que los números de teléfono son finitos y necesitamos una agencia o organización que los asigne de manera equitativa y justa pues pasa Exactamente lo mismo con las direcciones IP Al fin y al cabo las ips lo podemos ver como números de teléfono es el identificador que utilizamos para contactar a un ordenador en vez de a una persona como haríamos eh con número de teléfono que está en la otra parte del mundo esto con Matiz pero es para explicarlo de manera sencilla y que se entienda Okay entonces volviendo al tweet de nuestro atacante ya entendemos que consiguió acceso de administrador a la cuenta de ripe según su tweet concretamente de Orange España que es donde Orange como empresa de telecomunicaciones gestiona el rango de ips que le han sido asignadas volviendo a la analogía el equivalente sería que alguien consiguió acceso al portal del registro de numeración y operadores de telecomunicaciones de telefónica que es donde gestionan los prefijos de números de teléfono que se le asignan a esta operadora de telefonía claro aquí ya podemos empezar a hacernos una idea de la gravedad del asunto y de por dónde van los tiros respecto a que el impacto que causó fue la desconexión de internet de los clientes de Orange pero sigamos indagando nos toca hablar de bgp bgp son siglas referentes a Border Gateway protocol que valga la redundancia es un protocolo de enrutamiento que permite transmitir la información que enviamos a través de internet de manera correcta es decir cuando tú visitas tierrade hackers.com el servidor donde yo he creado esa web está en Estados Unidos Tú desde España desde tu ordenador pones tierr hackers.com en tu navegador Y cómo sabe tu ordenador o tu proveedor de internet a dónde ir a buscar el servidor que tiene la información de mi web Cómo sabe que está en Estados Unidos Cómo sabe exactamente dónde en Estados Unidos está ese pequeño servidor entre los millones que hay expuestos a internet en ese país por encima de los proveedores de internet tiene que haber algún tipo de tecnología que permita saber cómo a gran escala Por así decirlo eh A dónde tiene que ir a buscarlo te planteo esta analogía querido oyente tú quieres ir desde donde vives pongamos pontevedra que es mi tierra natal hasta pongamos un sitio lejano que se pueda llegar por

carretera y buscando pues Estonia no que está al otro lado de Europa Okay Tú no tienes un solo mapa que indique las carreteras exactas de cómo llegar desde tu callecita que está en tu casa en pontevedra hasta el pueblo donde vive tu amigo en Estonia lo que tendrás es un mapa con todo todas las calles de tu país otro mapa con las calles específicas de Estonia y luego tendrás un tercer mapa de carreteras de toda Europa que contiene probablemente solo las autopistas principales verdad A ver hoy en día Ya usamos Google Maps pero de aquella era así así para salir de tu ciudad puedes usar el mapa de España luego vas todo por autopistas hasta Estonia y con el mapa más con el mapa más y vuelves al mapa específico de Estonia para encontrar la casa de tu amigo en ese pueblo perdido que decíamos pues bgp sería el protocolo que nos da la ruta más eficiente para llegar de España a Estonia por autopista es decir ese mapa más genérico de las autopistas las diferentes autopistas lo podemos ver como sistemas autónomos que son routers o conjuntos de redes esenciales de internet y bgp ayuda a interconectar losos de manera óptima para que fluya el tráfico lo más eficientemente posible es decir las ciudades o autopistas son los sistemas autónomos y bgp es el protocolo es decir cuando tú le dices a Google cómo llegar es el algoritmo que dice Oye pues vete por aquí por aquí por aquí que es la ruta más eficiente perfecto yo creo que más o menos queda claro tenemos ips que representan donde vivimos y donde vive nuestro amigo Estonia que queremos ir a visitar y ripe que es quien se encarga de asignar noos los nombres y números de las calles donde vivimos no tenemos sistemas autónomos que son las autopistas Y por último bgp que es el algoritmo que nos permite las que nos brinda las mejores autopistas para llegar a Estonia venga ya solo nos queda por aprender un concepto más para tener todas las variables de este incidente de seguridad source public infrastructure o rpki resulta querido oyente que internet es bastante viejo y en su día cuando se establecieron los cimientos no se tuve demasiado en cuenta la seguridad al igual que un edificio de 1900 en el que la gente aún a día de hoy vive y que de hecho en Europa es bastante común encontrár telos la seguridad en esos tiempos no se tenía tanto cuenta como a día de hoy a la hora de construir los edificios es por eso que estos edificios tan antiguos han de pasar estrictas inspecciones por parte de arquitectos y a veces hace falta Añadir parches no o mejoras para que esos edificios sean seguros como yo que sé Añadir vigas maestras nuevas o refuerzos de los cimientos Pues lo mismo pasa con internet bgp Es un protocolo que carece de seguridad se basa en un modelo de fianza ciega si tú me dices algo yo te creo y ya está o el equivalente en lo de los edificios Si yo te digo que este edificio que se cae a trozos Está seguro no te preocupes pues con eso me vale claro eso no es lo ideal esto quiere decir que si una ciudad Madrid por ejemplo anuncia Que para ir a Barcelona Hay que coger la autopista que lleva al sur a Andalucía camino Marruecos Pues todo el mundo le va y el tráfico que pase por Madrid hacia Barcelona acabará en Marruecos porque insisto el protocolo bgp con que lo anuncie la ciudad pues ya está esto es un problema y hemos visto ataques al protocolo bgp a nivel gubernamental para redireccionar tráfico a otros países con fines de espionaje uno de estos incidentes que os dejo en las notas del episodio sucedió en 2018 cuando durante un breve periodo de tiempo todo el tráfico dirigido a Google pasaba antes por china he de decir que la conclusión fue que con casi toda la seguridad se trató de un horror en la configuración de bgp ese casi es lo que a mí no me convence del todo porque hubo un momento Aunque fuese breve que todo el tráfico que iba Google pasaba por china en fin que evidentemente el protocolo bgp que forma parte del Core del funcionamiento de internet tiene serios problemas de seguridad y cuál fue la solución pues el rpki rpki añade una capa de cifrado y autenticación que evita ataques de toma de control de rutas bgp ya no vale con decir que la autopista de Madrid a Barcelona pasa por Marruecos tienes que digamos demostrarlo criptográficas decirlo Bueno entonces Martín qué es lo que ha pasado pues lo que sucedió es que el atacante accedió al portal de administración del ripe de Orange España y modificó la

configuración añadiendo un nuevo servicio en esto ya no entro porque si no es demasiado técnico pero concretamente un objeto rout origin attestation que se utiliza para verificar que un Rango de ips efectivamente pertenece a un sistema autónomo en concreto como estos roas utilizan certificados digitales que se usan en conjunto con el rpki que os decía para bueno hacer estas verificaciones es lo cual recordar previene ataques contra bgp al ser inválido el que añadió el atacante el resto de internet empezó a ignorarlo dejando el sistema autónomo de Orange totalmente aislado el equivalente en nuestra analogía un atacante entró en el sistema de gestión de mapas de carreteras concretamente el de Madrid el que pertenecía a Madrid que gestiona las carreteras de Madrid modificó la configuración para anunciar que el responsable de gestionar las carreteras en Madrid era una persona diferente a la que debería ser como se activó el sistema criptográfico de verificación del responsable de carreteras en España las demás ciudades se dieron cuenta de que ese cambio no tenía sentido y todos empezaron a ignorar la existencia de Madrid como ciudad en España y Qué pasa cuando sucede eso pues que todo el mundo que quería conducir de un lado a otro de España no pasaba por Madrid produciendo atascos en carreteras y tráfico poco eficiente y la gente que estaba en Madrid no podía salir de la ciudad porque claro estaba incomunicada Qué curioso verdad ya te digo que estas historias que bueno me invento estas analogías es para que se entienda mejor Yo soy el primer aprendiz aquí y me ha molado mucho preparar esta noticia porque aprendí bastante de cómo funciona internet en su base digamos bien Ahora que ya conocemos el qué vayamos al Cómo que también vale la pena hablar de ello la respuesta te sorprenderá amigo seguramente pensaréis que dado el alcance del incidente recordemos desconectar a miles de personas tiene que tratarse de un de ataque de lo más sofisticado para nada querido oyente para nada el ataque el el atacante perdón consiguió acceso al portal de administración del ripe gracias a una contraseña de administrador que encontró públicamente expuesta ya que mirando los nombres de usuario en listas de usuarios y contraseñas filtradas y a ver si veía algún email interesante se fijó en uno que era admin rpe guip nt @orange o sea admin ripe de Orange pero Espérate que hay más esa contraseña de administrador para ese usuario era ripe admin la contraseña más insegura y evidente que podían haber elegido pero Espera espera que hay más la autenticación de doble factor no estaba activada por lo que lo único que hacía falta para un atacante para acceder era esa contraseña y nada más Pero tranquilo querido oyente que siga viendo más gracias a investigadores de una empresa de ciberseguridad que quisieron saber cómo es posible que esta contraseña acabase expuesta públicamente encontraron que el email pertenecía a un empleado de Orange que había sido infectado con un malware de la variedad racon que es un info stealer en septiembre del año pasado o sea un absoluto despropósito todo por un lado de Orange por securizar los cimientos de la teleoperadora con una contraseña Tan débil y sin doble factor de autenticación y bueno en cuanto al administrador de Orange y que su ordenador fuera infectado con malware que se dedica a robar credenciales Pues bueno por un lado puede pasar a la persona más técnica del mundo que acabes infectado pero es que investigando me encontré un iludo Twitter donde ponían exactamente cómo se infectó capturas de pantalla del de escritorio del del del administrador en el momento y más información eh Porque eso viene como parte de del pack digamos cuando compras y te descargas estos datos que recopila este tipo de software malicioso según va infectando usuarios porque por supuesto que está a la venta Parece ser que se infectó al intentar Descargar un programa que se llama ksm pico de una página maliciosa y Qué es ksm pico me preguntarás Pues un programa para activar copias de Windows sin pagar por ellas madre mía o sea el administrador de Orange se infectó descargando de una página maliciosa software ilegal Killer combo os dejo un montonazo de links de esta noticia que fui recopilando para para prepararla desde Twitch en directo del atacante vídeos de cómo lo hacía yos explicando al

detalle que ocurrió Cómo se infectó el empleado bueno todo lo que os ido mencionado Espero que hayáis aprendido tanto como aprendí yo y si os tenéis que quedar con una sola cosa de todo esto usad contraseñas seguras y activad la autenticación de doble factor por favor por favor queridos oyentes hasta aquí ha sido un episodio más corto en Solitario Pero espero que igual de valioso que los otros 114 episodios que llevamos haciendo durante más de 3 años Gracias gracias gracias por estar ahí Un año más un episodio más y yo creo que dentro de poco nos vamos a volver a empezar a ver que tengo ganas ya de que empiece la temporada de conferencias sobre todo locales y me encanta ya lo sabéis repartir swag del podcast a ver si hacemos nuevo este año veros las caras a los que nos escucháis repartir abrazos me encanta seguir ahí seguir escuchándonos suscribiros si todavía no lo estáis y gracias por todo Adiós adiós si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers