el protocolo de Apple find m que entre otros usan los axs para encontrar tus cosas perdidas puede ser abusado como red de exfiltración de datos en entornos seguros y aislados sin ningún tipo de conexión el análisis forense de mandiant descubre que sandworm utilizó técnicas de living of the Land para agilizar el desarrollo de un ataque que causó apagones en Ucrania al mismo tiempo que la infraestructura cría del país sufrió ataques de misiles rusos ni una semana ha pasado y ya tienes tu nuevo episodio listo para ser escuchado en tu app favorita comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 20 de noviembre de 2023 es el episodio número 112 yo soy Martín vigo y está conmigo como no podría ser otra manera el señor Alexis porros Hola Alexis qué tal estás amigo pues muy bien Martín aquí otro episodio más eh contigo con todos los oyentes y pues nada esta semana es la semana de Acción de Gracias en Estados Unidos y siguiendo en esta línea en este concepto y poniéndome un poquito sentimental quería dar las gracias a nuestros queridos oyentes patrocinadores eh mecenas comentaristas en redes sociales usuarios de discord ya sabéis y los que no lo sepáis ahora lo sabéis Muchas gracias por hacernos Quiénes somos a día de hoy eh nada y para aquellos que tengáis ganas de más sobre este podcast os cuento que no es un secreto ya lo he dicho miles de veces o o no al menos 111 veces pero nos podéis seguir en redes sociales buscarnos por tierrade hackers o @ tirad hakers y para tener una alerta sobre Cuándo sale un nuevo episodio os podéis suscribir a tierra de hackers en cualquier plataforma forma de podcast y podéis interactuar con la comunidad de este podcast tierra de hackers en nuestro canal de discord donde podéis entrar vía tierrade hackers.com brdc perfecto Alexis y muy bien traído ahí el día de Acción de Gracias Thanksgiving como siempre eso Muchas gracias sobre todo por hacernos finalistas gracias a vuestros votos en los premios de ibox no paramos de crecer estamos reventando todos los charts gracias a vosotros queridos Oy y ya que estamos dando las gracias Pues por supuesto a nuestros mecenas de patreon como no y una mención especial a Bruno porque se acaba de unir a nuestra familia de patreon y además en el en el rank más elevado Así que muchísimas gracias dentro de poco te llegará una pegatina especial nuestra Bruno y desde luego tu colaboración y tu aportación es esencial para que sigamos adelante con esto Muchísimas gracias Muchas gracias Y gracias También a un nuevo sponsor que tenemos esta semana 480 y os vamos a hablar del podcast que tienen que está chulísimo Cuidado con las macros ocultas volar seguro es también volar ciberseguro la tecnología es clave desde que compramos un billete hasta que aterrizamos y recogemos las maletas La pregunta es cómo se integra la ciberseguridad en el sector aéreo con tanto arraigo en la seguridad física Qué papel juega la Inteligencia artificial en la defensa y respuesta a vulnerabilidades de este tipo de infraestructuras críticas pues puedes descubrir las respuestas en Cuidado con las macros ocultas un podcast sobre tecnología para los negocios y que es de 480 en él hablan de uno de los mayores con uno de los mayores expertos en ciberseguridad del sector de la Aviación Hugo teso y con el ciso De nada más y nada menos que iberia Jesús Mérida también participan en el episodio gorc sadowski de exabeam Fabio Peña ciso de Copa Airlines irwin Ferguson vicepresidente de tecnologías e Innovación del aeropuerto de tocumen en Panamá ya puedes escucharlo en tu plataforma de audio favorita o en su página web que la que la puedes encontrar en cuidadocon lasas macros ocultas.com cuidado conlas macros ocultas.com y os dejo el enlace en las notas del episodio y en la del episodio para que os sea más cómoda ir a suscribiros y también queremos hacer otra pequeña pausa para darle las gracias a otro de nuestros patrocinadores monat una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y monat a través de una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley 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 mandad vuestro currículum a tierrade hackers @mon comom mad.com perfecto nos vamos ya a la noticia y hoy os voy a hablar de exfiltración de información de sistemas pero sobre todo en entornos Ultra protegidos donde los sistemas ni siquiera están conectados a internet poneos en situación si conseguís acceso a un ordenador que controla por ejemplo una central nuclear y queréis robar información Bueno cómo lo haríais tenedo en cuenta que ese ordenador está totalmente aislado y no está conectado a internet Lo que bueno se conoce como un sistema Air gapt esto es común en infraestructura crítica donde necesitas ordenadores para controlar los sistemas robótica y maquinaria no pero que necesita estar a la vez Ultra protegido y por tanto no necesita se necesita acceso físico eh para operarlo no está conectado a ningún tipo de red para que no pueda ser precisamente hackeado remotamente pensad en Plantas potabilizadoras donde los ordenadores controlan pues la cantidad de cloro que se mezcla en el suministro de agua de una ciudad o bueno como dice máquinas que controlan maquinaria de una central nuclear de hecho aquí tenemos el ejemplo Perfecto es taxnet muchos lo conoceréis pero a los que no se trata de una operación encubierta entre el gobierno de los Estados Unidos e Israel contra Irán para ralentizar su programa nuclear ya que sospechaban que en realidad estaba siendo usado para avanzar en el desarrollo de bomba nucleares os recomiendo Por cierto muchísimo el libro de los de una de las periodistas Que investigó profundamente esto esto Countdown to Zero day y bueno os lo mira os lo pongo en las notas del episodio el tema es que lo que hicieron en con St taxnet fue infectar los ordenadores que controlaban maquinaria esencial usada para enriquecer uranio específicamente las máquinas centrifugadoras y stax net lo que hacía era bueno oscilar la velocidad levemente para que se estropeas con el tiempo de tal manera que los supervisores no lo podían ver y para infectar inicialmente los sistemas lo hicieron a través de dispositivos USB infectados que los empleados enchufaron en los ordenadores estos que os decía que no estaban ni conectados a internet sin saber que contenían malw es una historia real y fascinante así que lo dicho leeros el libro e pues Martín también iba a decir yo como dicen shameless pl no no doy tantas charlas como tú obviamente pero alguna charla he dado y en la conferencia de de Barcelona no con name en el 2010 cuando me estaba introduciendo en los temilla Industrial hice una charla titulada nuking and defending skada networks y ahí de hecho cubrí todo el tema de stnet que era justo calentito en ese momento y creo que incluso está en vimeo la charla no sé voy voy a intentar encontrar me ha venido la mente el tema del stackset me ha recordado esa charla y voy a intentar poner las slides que las he encontrado y el vídeo si lo encuentro lo pongo también y así Si alguien lo quiere ver Pues mira perfecto Mira Y además así mucho más fácil para en vez de tener que leerse un libro pues ya les das tú el resumen en esa charla no la ha visto O sea que me la voy a ver yo también asegúrate de ponerlo en la notas del episodio y volviendo a la pregunta y aunque bueno como os explicará Alexis taxnet no pretendía ex filtrar información sino alterar el funcionamiento de la maquinaria vuelvo a la pregunta si vuestro objetivo es ex filtrar información de un ordenador que no está conectado a internet y que habéis conseguido infectar haciendo ingeniería social a algún empleado Cómo hacéis para transmitir la información hacia fuera pensadlo por un momento Cómo haces tienes control sobre un ordenador que está en una sala en una jaula farada sin conectar Cómo cómo consigues esa información desde fuera Pues de eso va esta noticia queridos oyentes unos investigadores encontraron una manera muy ingeniosa de hacer eso mismo en un escenario como el de taxnet y no solo eso la novedad es que han publicado hace unas semanas un implante físico camuflado dentro de un teclado para demostrar que podían robar contraseñas y exfiltrate Send my arbitrary Data Transmission vi Apple find my Network de hecho lo cubrimos en su día en el episodio 29 y 30 Ya llovió que vamos por el 112 pero de aquella era

algo más a nivel teórico la clave es que Apple dijo haber resuelto el problema y dos años después hace un par de semanas decidieron estos investigadores ponerlo a prueba pero esta vez desarrollando un implante real y camuflándose un pequeño dispositivo que puedes pegar a cualquier cosa que tiendes a perder como las llaves y te va a ayudar a encontrarlo de la manera en que funciona es que bueno utiliza Bluetooth y todos los iphones que hay en todo el mundo para crear una red mediante la cual transmitir la información de su posición GPS básicamente los iphones como el tuyo o el mío actúan como nodos intermediarios encargados de ir retransmitiendo la información a otros iphones hasta que llega el dueño y lo puede ver en su cuenta de iCloud Esto no es novedoso yo recuerdo cuando en Estados Unidos sacaron tle que hacía básicamente esto El problema es que no era tan bueno porque no había ni por asomo la misma cantidad de personas con un Tile y la aplicación instalada en su móvil como dueños de iphones ipads y macs hay en el mundo y ahí es donde reside el poder de find my en que prácticamente la la mitad de la de la población con un dispositivo móvil tiene un dispositivo de Apple pues ya os podéis ir imaginando por dónde van los tiros han conseguido instalar un virus en un ordenador aislado Bueno pues cómo hacen para filtrar la información pues simula ser un dispositivo perdido de Apple y usa su protocolo para enviar la información robada transmitiendo esta entre los teléfonos de los empleados en la empresa hasta que sale fuera al mundo y llega a ti lo dicho la verdad que es brillante Pero esto no es tan simple como parece uno no puede simplemente reutilizar esta red para enviar lo que quiera recordemos que hablamos de Apple y su ecosistema es altamente cerrado y protegido Y es ahí donde radica el mérito de estos investigadores para empezar el protocolo está diseñado para enviar las coordenadas del GPS del dispositivo perdido y nada más entonces Cómo podemos hacer para que en vez de eso se envíe una contraseña por ejemplo que acabamos de robar insisto recordemos El ejemplo concreto que han puesto los desarrolladores el perdón Los investigadores que es un teclado con un implante dentro concretamente lo que hicieron es abrir un teclado metieron un microcontrolador que hace de key logger es decir cada tecla que se va pulsando pues la graba y luego me mediante un esp32 que es un microcontrolador pues simulan este protocolo de del find my para enviar todas las teclas que se van pulsando por Bluetooth hacia el exterior esperando que haya algún iPhone cerca recordemos el bluetooth Pues tendrá un alcance de de ciertos metros no no tiene el mismo alcance que una WiFi pero con que haya iphones cerca Pues ya va a empezar a retransmitir de Iphone a iPhone de Iphone a iPhone de Iphone a iPhone hasta que que llega al al dueño pues lo que hicieron es utilizar parte de los campos del protocolo find my para alterarlo y codificar la información que querían transmitir partieron de un trabajo de investigación previo por parte de unos investigadores de la Universidad de darmstadt en Alemania que reversear el protocolo find my e hicieron una implementa Open source que llamaron Open hashtag con esta implementación básicamente pueden Añadir o sea tus puedes Añadir tus propios dispositivos que no son de Apple a la red find my y aprovecharte de este protocolo para encontrarlo si lo pierdes es decir este protocolo te permite no solo limitar esta red creada entre dispositivos de Apple a dispositivos de Apple unx sino que ahora puedes desarrollar tus propios dispositivos y aprovecharte de esto y para encontrar dónde introducir la información ex filtrada en code Ada se fijaron en cómo funciona este protocolo que básicamente es así Cuando haces pairing de un airtac es decir te vas a la Apple compras un airtac no y lo quieres asociar a tu cuenta de iCloud pues utilizas por ejemplo tu iPhone no Y para que desde el iPhone puedes empezar a monitorizar Dónde se encuentra ese airtag Pues cuando haces ese pairing no ese enlace se crea una clave pública privada quedando la pública almacenada en el ertac y la privada en tu iPhone en tu cuenta de iCloud cada 2 segundos a partir de ese momento el ertac hace broadcasting mediante Bluetooth low Energy y el contenido de ese paquete de broadcasting es precisamente la clave pública

generada y que cambia Por cierto Cada 15 minutos Bueno aquí se utiliza un secreto compartido cuando se hace el pairing Y esto es básicamente para que no siempre se emita la misma clave pública porque entonces Alguien podría rastrearte ya que tu ertac está siempre emitiendo Pues digamos el mismo token no Por así decirlo Entonces es una medida que implementaron pero con lo que os tenéis que quedar es que todo lo que hace el ertac es enviar cada 2 segundos una clave pública clave pública asociada a la clave privada que quedó en tu iPhone Vale pues los dispositivos de Apple cercanos al ertac identifican este paquete de broadcasting y cifran su geolocalización es decir la del la del dispositivo que acaba de recibir ese broadcast coge su geolocalización lo cifra con esta clave pública y lo manda a apple de manera cifrada y anonimizada que no se sepa de Qué dispositivo viene entonces cuando el dueño deltag activa el modo localización deltag lo que hace su iPhone lo que hace su dispositivo es que genera todas las claves públicas posibles que el ertac hubiera generado durante el último par de días y verifica con Apple si existe la base de datos es decir que algún dispositivo efectivamente escuchó el broadcast del ertac cifró su localización y lo subió de ser así el dispositivo del dueño que tiene la clave privada descifra las coordenadas GPS y ya tiene eh Dónde se encuentra alerta sé que esto es un poco complejo sé que es un poco así explicarlo en un podcast es un poco complicado pero básicamente lo que tenéis que pensar es que el protocolo Envía una clave pública y luego el iPhone se fija si esa clave pública está presente en las bases de datos de Apple para luego descifrar y saber eh qué coordenadas GPS eh tiene Pues bien básicamente como decía estos investigadores Sabiendo esto tenían que implementar un protocolo suyo propio para en vez de enviar la información que se envía no esta clave pública enviar las contraseñas que se están exfiltrate diseñaron un protocolo en el que usan el campo destinado a la clave pública porque es el único paquete que se envía este de broadcasting e para encode bit a bit la información robada luego ellos pueden verificar con Apple si existe dicha clave pública en sus bases de datos bueno clave pública que realmente no lo es y extraer la información la razón de hacerlo bit a bit Es que así solo hay dos claves públicas posibles con un cero o con un uno verifican las dos y la que existe pues ya tienen el el bit a ver Esto es sé que es un poco difícil de comprender pero básicamente lo que están haciendo es en el paquete de broadcasting están enviando al en vez de una clave pública algo como esto eh código del mensaje Hola índice 0 bit 0 y luego envían otro paquete que es código mensaje Hola índice 0 bit 1 y envían otro paquete y código mensaje Hola índice 1 bit 0 código mensaje Hola índice 1 bit 1 código mensaje Hola índice 2 bit 0 código mensaje Hola índice 2 bit 1 ya os hacéis una idea no diseñaron un protocolo en el que hay un código identificador del tipo de mensaje Luego hay un índice para saber en qué sitio iría ese bit en concreto y luego pues lo envían dos veces uno como bit 0 y otro como bit 1 y entonces el que exista en Apple si por ejemplo para el código de mensaje Hola índice cero existe la clave bit 0 pero no bit 1 ya saben que lo que se ex filtró pues el primer bit es un cero Espero que quede más o menos Claro la verdad es muy astuto este ataque y como Comentan los investigadores appel no puede hacer mucho para remediarlo de hecho al estar implementado así ni siquiera salta la alerta de que tienes un airtag cercano y desconocido no Esto es lo típico que a veces te avisa de por ejemplo pues no sé a mí me pasa a veces con con pues familiares o así que que pasan días conmigo de viaje y como no los tengo en mis amigos y cosas así pues de repente me salta una alerta que tengo un airtag cerca mío esto si os recordáis y lo hablamos varias veces en el podcast es para evitar que alguien utilice estos airtags para monitorizar los movimientos de alguna persona Entonces te alerta Oye hay un airtag desconocido cerca tuya pero esta gente estos investigadores como modificaron la información que se envía pues ni siquiera llega a alertarte también Es verdad que tuvieron algunos problemas porque Dado que los dispositivos de Apple esperan una clave pública válida y en realidad envían otra cosa no como decía este este tipo de protocolo encode

e inventado por ellos a veces fallaba porque no se no era una clave pública correspondiente una clave privada pero encontraron cómo solucionarlo y tenéis todos los detalles en su blog que por supuesto os dejo las notas del episodio Pues ahora ya os podéis imaginar cómo funciona el teclado que han creado y que os mencionaba pueden engañar a un empleado para que lo use ex filtrando así lo que vaya tecleando a través del protocolo find m se me ocurre que se lo puedes enviar por ejemplo de regalo o darlos gratis en una conferencia no sé donde sepas que va gente muy interesante como pueden ser pues conferencias de criptomonedas Y entonces lo que ex filtras pues son las contraseñas o los los las palabras semilla de un wallet no la imaginación aquí es el único límite de las posibilidades ya estamos con las criptomonedas Martín Qué pasa si son s seguras siempre nunca se han robado y son a prueba de de fuego echa la ley echa la trampa ya sabes cómo va esto muy interesante como dices la evolución eh el follow up de de lo que ya diseñaron en el episodio 30 no hace en el 2021 y que y que ahora lo como se diría no de forma inglesa lo han guon Y sí estos implantes Hardware Son son muy difíciles de de identificar especialmente como dices Martín si se meten en un teclado que tiene espacio suficiente a ver yo me he comprado últimamente unos teclados y ahora me haces me haces sospechar debería abrirlos o no mejor no Mejor vivir en la ignorancia no vaya a ser pero es verdad que al igual que porj my god cable y todo esto los implantes de Hardware es algo guapísimo es lo más cercano a una peli de James Bond Y la verdad deberían comercializar esto es verdad que el digamos la tasa de transferencia el bandwidth no es muy bajo Pero oye para temas como contraseñas o así vale Es verdad que claro tienes que asumir que en cuanto llegue la persona Bueno si llega por la mañana a utilizar tu teclado para desbloquear el ordenador en principio lo primero que te creas es la contraseña entonces puedes asumir que eso y como son caracteres aleatorios pues tiene pinta de contraseña No quiero decir con esto a lo mejor no es s super útil pero tiene su utilidad en Casos super concretos y me parece guapísimo el ex filtrar información a través del protocolo find my de Apple así a todo esto a cuánto mencionan Como por ejemplo una contraseña de una contraseña muy segura de ocho caracteres eh Es broma pero cuánto tardaría enviarse Pues mira eh Te va a sorprender no es tanto por la tasa de transmisión sino cómo funciona entre un minuto y una hora por qué Porque Apple va actualizando sus servidores con con el tema de las claves no que que le van llegando cada tanto tiempo no solo eso tú puedes que por ejemplo yo voy con mi iPhone no me han dado ese teclado voy con mi iPhone me meto en esa en ese a 10 kilómetros de profundidad a desbloquear eh a poner la contraseña para los misiles nucleares Claro mi iPhone lo capta Entonces lo guarda pero hasta que salga fuera no lo va a intentar transmitir a otros entonces claro depende mucho de eso Pero insisto un escenario así como decía los códigos nucleares si los pones en ese teclado y hay algún empleado cerca Pues eso ya se está transmitiendo mediante el protocolo find my y lo chulo Es que dices que aunque esto Se use para enviar digamos la contraseña que se ha capturado con este key logger no se alerta al teléfono verdad no sale en plan alguien te está claro claro exactamente Yo creo que es por el tema de que como no se envían claves públicas válidas Entonces no no te puede avisar no entran en el porqué solo comentan que que Apple tiene muchos problemas para poder evitar esto precisamente porque están usando su protocolo tal como está implementado solo que están enviando información distinta muchos de los códigos que mucha de la los datos que envían en codeos podría ser perfectamente una clave pública porque recordemos que en principio es son bits aleatorios se trata decifrado Y entonces lo tiene muy difícil Apple pero sí No ni siquiera te alerta pues esto es cómo se diría una feature no del protocolo no es realmente Una vulner idad es un fallo en el diseño que ahí está fallo en el diseño no estoy seguro es que realmente los no están explotando una vulnerabilidad no Cuál es la vulnerabilidad que están explotando solo están reutilizando un canal para transmitir información que no se suponía que no está

diseñado para para transmitir pero ya pero es tal cual eso entonces realmente no están explotando una vulnerabilidad es como cuando se usa protocolos dns o icmp para enviar datos que no deberían ir ahí para una manera justo justo típica de de ex filtrar pero por poner un ejemplo es como Pues un sobre no tú puedes mandar una carta o puedes mandar Antrax como se mandaba hace unos años claro el canal es el sobre puedes enviar lo que quieras no no encontrar una vulnerabilidad Sí sí pues nada ahí queda eh cómo nos podemos proteger Pues no sé como he dicho Mirad vuestros teclados por dentro y no trabajéis en centrales nucleares y ya está eh hombre el tema es si tienes un teclado cableado y tienes un un analizador de radiofrecuencias Y ves que hay emisiones Bluetooth preocúpate Sí bueno Me imagino también que est ser Gap a ver en el mundo real quiero pensar Yo nunca he estado en uno pero quiero pensar que también hay un protocolo de no llevar dispositivos adentro No si vas a una sala donde hay algo tan sabes importante como para que no esté conectado internet pues no en todos los casos pero muchos Pues a lo mejor hay una política de que tengas hay una un portal de seguridad que tienes que pasar y dejar tus dispositivos fuera y todo esto no Pero pero sí si no estoy pensando que dentro Espérate ya sé dentro de la jaula fda y que está la máquina tú le haces una jaula fda y al teclado o sea es una jaula fada y dentro de una J faradise entonces de ahí no puede salir los los broadcasting los beacons del Bluetooth y ya está y como las películas estas de de los de los virus y tal no te pones en las manos dentro de esos dos guantes que están enganchados en la cajita y tocas el teclado Así es verdad como cuando cuando están ahí con virus y cosas así no con las petas estas es verdad Qué bueno pues nada queridos oyentes ahí quedáis avisados no os fiéis de ningún teclado no sí con con cuidado básicamente Pues nada seguimos con la siguiente noticia y os Traigo una de sandworm y Ucrania sandworm es ya amigo es conocido de este podcast ya lo hemos comentado varias veces pero bueno hay cierta edad al respecto de uno de sus ataques más recientes Así que es lo que os traigo porque me ha parecido interesante mandian recientemente ha revelado que a finales del año pasado 2022 respondió a un incidente de seguridad contra una organización de infraestructura crítica ucraniana una empresa de red eléctrica que este ataque fue llevado a cabo según ellos Según mandiant por el grupo cibercriminal ruso sandworm adscrito al grupo al a la organización departamento del gobierno llamada Gru o la dirección principal de inteligencia de Rusia que trabaja Obviamente con este grupo desde el 2009 y es la agencia de inteligencia extranjera como digo ya hemos cubierto ataques anteriores de sandworm en el podcast pero a modo de recordatorio os comento Eh brevemente esos tres ataques que que que están relacionados con sandworm en el contexto de infraestructura crítica que es el contexto de esta noticia en diciembre de 2015 sandworm provocó un corte de energía en Ucrania utilizando el malware Black Energy 3 y el wiper Kill disk con esto de wiper eh lo hemos comentado en otros episodios pero refrescando un wiper es un malware de tipo destructivo que borra datos eh tanto en el disco como fuera del disco Más allá del disco a nivel de sistema digamos en el bootloader o el master Boot record digamos el sistema de arranque Así que deja totalmente inoperable ese sistema no se puede encender y además ha borrado todos los datos en diciembre de 2016 tenemos que sandworm provocó un corte de energía también en una estación de transmisión de Electricidad al norte de kiev la capital de Ucrania utilizando el malware Crash override y también industr y lo que hizo fue consiguió esto activando fusible o disyuntores estos componentes eléctricos que intentan proteger las redes eléctricas de sobrecargas pero si no hay sobrecarga y se activa pues obviamente pasa lo mismo no se corta la energía y luego más recientemente el año pasado en abril actores se dice posiblemente vinculados a Rusia probablemente sandworm comprometieron sistemas con el malware ind Destroyer versión do una versión ionada contra empresas de energía en Ucrania su intento fallido tenía como objetivo causar un apagón así como digo lo intentaron Pero fallaron y de hecho cubrimos esta

noticia en el episodio 50 por si lo queréis refrescar lo novedoso de este ataque es que por primera vez atención sandworm utilizó técnicas de living of the Land las conocidas como LoL o lot por el L TL no y y utilizó estas técnicas para lanzar sus ataques contra los sistemas industriales para como digo similar a otros ataques anteriores querían activar los fusibles de la subestación en la organización eléctrica víctima provocando corte de energía no planificado que atención coincidió con ataques masivos con misiles contra infraestructura crítica en toda Ucrania Así que era un ataque Cibernético que estaba bien de la mano con un ataque físico eh digamos de de guerra con misiles eso es es bastante interesante y ya lo hemos comentado anteriormente pero e las técnicas de living of the Land se basan en utilizar herramientas que ya vienen instaladas en los sistemas atacados para evitar levantar sospechas en en los sistemas de de seguridad como los edrs o en los eh grupos digamos eh los centros de operación de seguridad o los shocks que trabajan para este tipo de empresas y bueno para también evitar tener que eh traer tu propio malware contigo y tener que subirlo a este sistema y tener que tenerlo en disco y todos estos estas características que ayudan a que a que tu ataque sea sospechoso y sea identificado no Si usas herramientas de estas que llamamos living of the Land que ya se encuentran en el sistema que atacas Oye pues mucho mejor sandworm no dejó ahí el ataque y finalmente llevó a cabo un segundo evento disruptivo al desplegar una nueva variante de cady wiper en el entorno de it no en el de ot El Industrial sino el it y lo que hizo fue Borrar todos los datos de los sistemas infectados incluyendo el sistema de arranque como dicho un wiper y los dejó inoperativos aclarar que en la noticia me voy a ir refiriendo al tema de control Industrial como ot del inglés operational Technology o tecnología operacional en español se dice que este ataque muestra una evolución muy rápida en la capacidad de ciberataque físico de cuando lo Cibernético llega al mundo físico de Rusia que ha sido cada vez más visible desde la invasión rusa en Ucrania las técnicas aprovechadas durante el incidente sugieren una creciente del Arsenal ofensivo de ute de Rusia incluida la capacidad de reconocer nuevos vectores de amenazas en entornos industriales desarrollar nuevas capacidades Y aprovechar diferentes tipos de infraestructura de tecnología operacional para ejecutar ataques al utilizar técnicas de living of the Land el actor sandw probablemente redujo el tiempo de desarrollo y los recursos necesarios para llevar a cabo su ciberataque físico como digo en lugar de tener que desarrollar tu propio malware desde cero programático pues Oye directamente utilizan las herramientas que que están instaladas y con parámetros específicos pasándolos archivos de configuración que se necesiten pero mucho más ligero un un desarrollo mucho más ágil el análisis sugiere que el componente utilizado contra los sistemas industriales de este ataque puede haberse desarrollado en tan solo dos meses el ataque acabó como he dicho con dos eventos disruptivos el 10 y el 12 de octubre del mismo año el año pasado que voy a comentar en más detalle a continuación Pero primero voy a comentar que la intrusión comenzó en junio de 2022 o incluso antes pero se tienen indicios y y registros y logs de junio de 2022 cuando ya había actividad maliciosa pero desafortunadamente no se sabe cóm Qué técnica exactamente se utilizó para el acceso inicial solo se vio que ya junio 2022 había actividad eh maliciosa lo que sí se sabe es que se estableció el control instalando una webshell llamada Neo regor que es una webshell Ya lo hemos comentado anteriormente es digamos un archivo que se instala en un servidor web al que se puede acceder a través de un navegador o bueno con corl wget cualquier librería de cualquier e lenguaje de programación no python request lo que sea similar para interactuar directamente y enviarle una petición que es web que parece eh No maliciosa digámoslo así y como web normalmente es un protocolo que está eh permitido en muchos perímetros dispositivos de firewall rutas y similares pues es bastante útil en estos tipos de ataques Pues esta webshell llamada Neo rigor se desplegó se instaló en un servidor vulnerable expuesto en internet primer fallo no no expongas estos servidores

vulnerables a internet de tu red eh de tu organización de de red eléctrica este servidor alojaba una instancia de un sistema escada que ya hemos comentado anteriormente pero esada es e en español se diría gestión de control de supervisión y adquisición de datos eem que se puede ver como sistemas a los que se puede monitorizar y gestionar de forma remota sistemas de control Industrial como sensores eh de luz de de nivel de Electricidad incluso de cantidad de agua en un tanque actuadores que podrían ser como motores o switches o incluso válvulas también para dejar o pasar dejar e pasar o bloquear el el un fluido y se podría ver un sistema escada como un sistema de orquestra de todos estos componentes eléctricos eh analógicos o como una también si lo queremos pasar un poco al mundo más eh de ciberseguridad se podría ver como una botnet de estos sistemas un sistema escada es lo que te permite controlar a todos estos sistemas Así que se podría ver como como una botnet básicamente pero volviendo a al tema Es que este es servidor vulnerable como digo en el que desplegaron esta webshell alojaba una instancia de un sistema escada para el entorno de la subestación de la víctima y a través de este sistema es como los cibercriminales pivotar eh Y obtuvieron acceso al entorno Industrial después de un mes de estar en en la red de de esta organización víctima sandworm desplegó el malware gogetter que está basado en el lenguaje de programación golan que es un cliente de command and control y envía las comunicaciones cifradas mediante tls este este componente pues le permitió mantener comunicaciones con el malware con este sistema infectado y llevar a cabo los subsiguientes ataques sobre el tema de la persistencia como estos sistemas infectados eran basados en Linux pues lo que hicieron fue crear un un servicio eh para que se arrancara para que se iniciara cuando el sistema estaba realmente operativo y cada vez que se reiniciara pues obviamente este este gogetter este componente de command and control se activaba también se tiene que eh según el análisis forense el atacante potencialmente tuvo acceso al sistema escada durante hasta 3 meses porque todo esto como digo Aparentemente empezó en junio eh un mes más tarde en julio desplegaron Bueno este este malware de command and control y luego en octubre es cuando eh lanzaron los dos ataques disruptivos el primero fue el 10 de octubre que es cuando sandworm aprovechó una imagen ISO llamada a ISO para ejecutar un binario de del Software microscada nativo Esta es la parte que es la de living of the Land que es la como la novedosa porque en lugar de traer su propio malware desarrollado por ellos por sandw eh dijeron vamos a utilizar lo que ya he instalado en este sistema que es este software llamado microscada y les permitió ejecutar comandos de control malicioso para apagar las subestaciones para activar como digo estos fusibles estos eh disyuntores el archivo hizo lo podemos ver como una especie de De hecho no sé si muchos de vosotros habéis quemado CDs en el pasado Pero lo típico hace años no que te descargaba una imagen ISO y luego la la cargabas eh en un programa que eh pasaba estos datos a un CD o sea los grabar un CD eh típico Nero borning room o el el bu justo iba a decir ese tío es que me acuerdo perfectamente Qué bueno el Nero Había otro de de una de una oveja cómo se llamaba ship ya no me acuerdo Cloud bites no me acuerdo Yo usaba el Nero sí sí Eh Pues nada Eso es Es una imagen que en el pasado las utilizamos para para grabarlas en CDS pero también se utilizan últimamente se ha visto muchos ataques para similar a como un zip en muchos ataques de fishing se envía protegido por contraseña porque los sistemas de seguridad no pueden adivinar la contraseña y no pueden ver lo que hay dentro Pues un ISO también se utiliza sobre todo porque evita que cuando se ejecuta un archivo que está dentro eh se puedan saltar sistemas de edr porque no se incluye esta la marca de la web no que hemos comentado en otros episodios en el en el podcast Entonces ese es un un probablemente uno de los motivos porque se utilizó este tipo de formato para desplegar el malware y que en sistemas operativos más modernos de Windows basta con o incluso de Linux basta con en Windows basta con hacer doble click y montar el archivo ISO y en Linux pues es muy fácil de montar un

archivo ISO como un sistema de ficheros por cualquier usuario pero en este caso el sistema objetivo era un Windows y así que e con un doble clic básicamente se monta este ISO como un volumen como si fuera un dispositivo USB de memoria externa no y Dentro de este ISO qué había Pues habían tres archivos uno era llamado loon vbs visual basic Script este archivo lo único que hacía era ejecutar otro archivo que que la ISO contenía que se llama n. bat y este bat un un archivo de de batch de de scripting de Windows lo que hace es ejecutar la utilidad nativa o the living of the Lan legítima que se llama sci ic.exe que es una utilidad del Software microescala utilidad de hecho se le pasa en este n. bat se le pasa como parámetro un archivo llamado s1 txt que también viene incluido en la ISO que probablemente contiene comandos micro escada no autorizados desafortunadamente este archivo s1 txt e no se pudo recuperar de la respuesta al incidente del análisis forense pero obviamente viendo el n. bat que hace referencia a este archivo se cree que este archivo s1.0 es el el que contenía los comandos que causaron el el apagón digamos y lo que contenía eran comandos de sci que es un lenguaje de programación de alto nivel diseñado por Itachi Energy para sistemas de control eh de su software microscada el servidor microscada comprometido este sistema de Windows estaba ejecutando sorpresa una versión de software no mantenida es decir que no recibía actualizaciones funcionales ni de seguridad y que permitía el acceso predeterminado a la Api de s Este lenguaje de programación de alto nivel que digo que permitía controlar de forma remota los las unidades eh que se se denominan unidades terminales remotas o rtu Remote terminal units que son sistemas eh de los que que cuelgan más elementos plcs programable logic controllers o lo que he dicho anteriormente no los sensores actuadores y válvulas colgaban de estas RT Así que a través de comprometer este sistema Windows que corría microscada no mantenido que no recibía actualizaciones funcionales ni de seguridad pues pudieron emitir estos estos comandos que hici que que se activaran los fusibles y que se causara este apagón este corte de energía básicamente Y luego el segundo evento disruptivo ocurrió el 12 de octubre cuando sandworm implementó una nueva versión del wiper o malware destructivo de datos cad wiper esta versión fue compilada el mismo mes en octubre de 2022 y la idea se intuye que la intención era destruir más el entorno y eliminar rastros del ataque sandworm desplegó cad wiper a través de una una gpo una una política de de Windows desde un controlador de dominio así que bueno si tenían acceso al controlador de dominio habían tenían control total de la red no directamente y lo que hicieron fue desplegar cad wiper para que se se ejecutara como una tarea programada de Windows lo curioso es que se implementó este wiper Ah para que atacara solo al entorno de tecnologías de la información como he dicho antes y no al entorno industrial y por tanto no afectó a a los a este servidor microscada que que estaba mencionando Los investigadores dicen o intuyen que esta acción fue inusual porque sandworm ya había eliminado otros artefactos forenses de del sistema escada que habían comprometido donde se había cargado esta imagen a punto ISO y se había lanzado estos ataques a través de micro escada Así que creen que esto podría indicar una falta de coordinación entre diferentes equipos dentro del propio grupo cibercriminal sandworm interesante cuanto menos eh Las pistas o los locks descubiertos durante la investigación del ataque indican que los hackers estaban preparados para la disrupción de los sistemas al menos TR semanas antes de que sucediera así que de alguna forma se han visto locks de que no sé igual e ya han visto el a punto ISO que se subió tres semanas antes del ataque en concreto o algún tipo de de lock en el que se ve que utilizaron esta herramienta sci lc.exe anteriormente Pero bueno ya sabían ya estaban preparados solo tenían que hacer enter y lanzar el ataque Los investigadores creen que sandw pudo haber esperado un momento específico para completar su misión y justo Cuál es este momento específico pues como como he dicho antes eh eh la coincidencia fue el inicio de una serie coordinada de días de ataque con misiles contra

infraestructura crítica en varias ciudades ucranianas incluida la ciudad en la que se encontraba la víctima esta organización eh de red eléctrica Eh bueno como siempre no decimos que hay recomendaciones para estos Estos tipos de como respuesta a estos a estos incidentes las lecciones aprendidas que siempre queremos compartir con vosotros queridos oyentes eh desde un punto de vista más de prevención se podría securizar este sistema microscada vulnerable sobre todo actualizándolo porque como digo estaba en una versión corría una versión no mantenida que no recibía parches de seguridad eh configurando microscada Para que requiera autenticación e y con mínimos privilegios eh autenticación De Do factor si es posible segmentación de red entre microscada el entorno industrial y el entorno eh típico de tecnologías de la información habilitar más login para que bueno se pudieran haber capturado los comandos que se ejecutaron en sí y eh Yéndome a esta parte más de monitorización pues capturar también tráfico de red telemetría eh relacionada con todo este tipo de de software microscada los archivos que se transfieren entre estos sistemas Porque al fin y al cabo lo podríamos pensar así estos sistemas esada son en la mayor parte son estáticos así que no van a haber muchas subidas o bajadas de archivos grandes eh Por si hay si hay e preocupación de tamaño de de poder guardar estos datos Pero estos sistemas escada funcionan una vez están desplegados Pues el mantenimiento no es muy costoso y no requiere mucha subida o bajada de datos como digo así que se podría intentar eh loguear todos los los las actividades que suceden en estos sistemas y bueno también esos archivos recién creados con referencias al lenguaje de programación este que que se que se abusó el informe de mandian También incluye indicadores de compromiso y reglas yara que se pueden utilizar para eh Para implementarlas en dispositivos de seguridad o para hacer digamos una inv más tipo de threat hunting de ir y lanzar de alguna forma estas reglas contra otros sistemas que que pueden haber en la red de esta organización o incluso de vuestras organizaciones para ver si si tenéis algún indicador de de este tipo de de infección que esperemos que no así que cerrando la noticia comentar que sandworm no necesita a partir de ahora ya vemos que no necesita crear su propio malware personalizado con el cambio a técnicas de living of the Land Los investigadores creen que sandw probablemente sea capaz de llevar a cabo ataques contra sistemas ot de distintos proveedores el beneficio del uso de estas técnicas como he dicho es la agilidad que proporciona y el rápido desarrollo de malware específico para cualquier entorno mucho más fácil que con malware sofisticado para este tipo de infraestructuras Además de que son herramientas legítimas cuya ejecución es normalmente permitida por sistemas edr en Point detection en levantan poca sospecha también al mismo tiempo el uso de técnicas de living of the Land en entornos scada requiere experiencia en estos entornos y comprensión de los procesos industriales objetivo siendo menos notable o menos requisito el conocer la tecnología utilizada en el ataque microscada en este caso en concreto sandworm Entonces podría repcar un tipo de ataque similar en a este al que lanzó en en octubre de 2022 en otro entorno con con tecnología diferente de forma muy rápida así que ya sabéis atentos a técnicas de este tipo vemos que la tendencia de los cibercriminales está cambiando hacia el uso de técnicas de living of the Land más que el uso de malware personalizado sobre todo por la agilidad y el rápido desarrollo yo de que esto le proporciona me recuerda cuando mencionabas lo de los comandos para desactivar la noticia que dimos hace poco de lo de los trenes también que era un poco enviar en sistemas similares lo del radi stop no que paraba todos los trenes en este caso era una señal estilo acústica pero es como la presencia de estos comandos que tienen sentido Pero desastrosos a la vez en manos de de un ciberdelincuente es muy curioso que estén presentes en infraestructura crítica no es como un autodestruyas y dan bastante miedo Yo creo que ese tipo de de comandos que no sé estaba pensando según lo mencionabas que habría que diseñar la seguridad o hacer como un tabletop exercise no un ejercicio ahí

teórico de vamos a auditar todos los comandos más críticos es decir ponernos en el como todos los comandos que existen se los damos al malo qué es lo peor que puede hacer como categorizamos los comandos del más crítico con y crítico evaluándolo como el más daño que se puede hacer y luego securizar adecuadamente no tiene sentido lo que digo es que estoy un poco ahí hablando lo que lo que reflexionaba según dabas tu noticia Sí sí eh hacer un un ejercicio de de tabletop un ejercicio de Cyber wargame como se diría es sería sería suyo Sí para justo para tener ahí en mente no es ostras con estos comandos el este y este Comando en manos del malo Uf nos revienta todo entonces eh vamos a ser cuidadosos a la hora de diseñar la seguridad en torno a estos comandos tan críticos Sí también No me queda Clara en la noticia Pero supongo que los cibercriminales sandworm obtuvo acceso administrador porque tienen acceso al domain controller Eh Así que Supongo que Ob tuvieron acceso administrador en este sistema Windows Aunque no es requerido para montar como digo un una ISO y lanzar estos comandos pero lo que se podría hacer también es usuarios normales no tienen acceso a este Comando living of the Land que es el s lc.exe de microscada solo los administradores que realmente tengan que lanzar este tipo de Pero bueno Al fin y al cabo si lo pensamos Es que es que los operadores que estén utilizando estos sistemas Windows microscada son los que tienen que tener la capacidad de Sí sí activar y Desactivar los fusiles si pasa alguna si se sobrecarga la red Así que es difícil no sé hay que hacer más monitorización ejercicios de tabletop como mencionas y más concienciación claro es que yo pensaba A ver es que justo además ese Comando es lo que dices tú es un comando de seguridad en el sentido de si todo va mal que podamos quitar El enchufe Por así decirlo entonces a la vez tampoco quieres Añadir demasiada fricción a la hora de ejecutarlo por tanto sí a ver si solo si hay digamos un modelo de autorización bueno es decir solo los administradores pueden ejecutarlo Pues claro se entiende que que sea así que si tenían acceso como administrador pues no van a tener muchas más trabas pero pensab también en temas de no sé el extremo lanzamiento de misiles nucleares no aquello de que el presidente tiene un maletín con unos códigos o lo típico que a veces vemos en las pelis de que dos personas con la llave de manera sincronizada la giran y están físicamente aparte para que una una persona sola no podría con ambas manos hacerlo es decir este estos métodos de de como que tiene que haber mínimo dos personas que estén de acuerdo para ejecutar El Comando no o incluso el tema del dns que lo hablamos alguna vez que hay claves eh cripto criptográficas creo que son siete personas que lo tienen en por todo el mundo distribuidas y mínimo hacen falta cuatro para poder hacer cambios digamos críticos en la infraestructura de todo internet por eso es un poco para evitar que pues que secuestren a uno extorsionen a otro tiene que haber mínimo cuatro personas de acuerdo para poder llevar a cabo cambios críticos Pues iba un poco por ahí mi mentalidad es muy interesante Esto sí espera déjame espera Déjame buscar otra palabra es muy llamativo es muy curioso es muy eh joder es que nos sale interesante Sí que lo es Qué vamos a hacer es interesante el tema es que en entornos los que estamos más acostumbrados Supongo todos la mayoría de los oyentes de it no tenemos la tríada esta que se llama confidencialidad integridad y disponibilidad en ese orden de prioridad pero en entornos industriales se invierte esta pirámide y lo más importante es la disponibilidad Así que eh luego viene integridad y confidencialidad no así que por eso digamos sería al revés yo incluso lo implementaría al revés de lo que dices si hay hay una sobrecarga pues Oye Que se active el fusible pero si se quiere que se envíe una alerta a dos personas que son de mayor Rango Y si quieren que digan No no quiero activar el fusible que siga operando la red pero es el tema se tiene que proteger las la seguridades lo principal en en est en estos entornos industriales por eso así claro claro pero esa es buena por lo menos dar la posibilidad A lo mejor que hubiese un retraso de yo que sé 10 segundos no sé cuánto sería no 10 segundos probablemente no pero claro Hay que encontrar ese punto intermedio pero sí que

se podía sobreescribir una orden por si se detecta que ha sido malicioso eh un poco como aquello de Mira buen ejemplo es que es una conversación super interesante lo del el retraso el la la abertura dada de las cajas fuertes de bancos y de hecho esas pegatinas quizá algún oyente lo haya visto en las puertas de los bancos pone eso eh que aunque tú entres a robar el banco y obligues a un empleado a abrir la caja fuerte por defecto está programada para que se abra a Pues a las 24 horas para precisamente evitar que un delincuente tenga el acceso tan tan fácil como simplemente pues amenazar a un empleado entonces es un poco esto no y y ya si alguien necesita pues acceso más rápido pues hay en otro punto físico del mundo dos personas donde podrían sobreescribir el retraso para eliminarlo y que se abra Pues de repente no la caja fuerte Sí en ese caso aún sí en el tema este de red eléctrica 10 segundos en si si una persona cl claro por eso decía que es absurdo no no tiene sentido en este caso en otros caso sí sí sí sí Por eso no en este sentido no no hay tu tía pero no sé la reflexión sobre todo el el ejercicio mental que conlleva diseñar un modelo de seguridad adecuado a la circunstancia es muy interesante porque es que cambia radicalmente si hablamos de infraestructura crítica de de una empresa de yo que sé ferrocarriles de tensión eléctrica en cuanto a inmediatez digo banca es curioso a ver estos sistemas de control Industrial estas infraestructuras tienen digamos se podría pensar como dos redes o dos o dos plataformas nosotros cuando siempre utilizamos internet o lo que sea tenemos digámoslo un un un plano no una infraestructura en las redes de nuestras empresas hay una red digamos en estas redes de control Industrial está la red que controla todos estos elementos como he dicho plc actuadores RT los H los los human Machine interface que usan los operadores pero también hay una red paralela que es solo de seguridad y y está digamos está como segmentada va o debería estar segmentada va aparte y se encarga solo de ver si hay un pico de tensión o algo así pues pum salta y activa el es incluso eh digámoslo Es inteligente es semi semi independiente y y puede actuar en esos casos Así que también está ese tema que s Supongo que si se ejecuta algún Comando que va en contra de la física de estos entornos industriales como el tema de la electricidad Pues esta esta red de safety podría En caso de que se quisiera causar una una un pico de tensión no igual este safety System esta plataforma paralela al sistema principal podría responder y decir no no pum lo corto y paro este pico de que se ha causado por eso el tema de abrir un actuador e es es algo que es bastante seguro y que este este sistema de de seguridad no diría nada en contra voy Ah parece que lo quieres hacer más seguro todavía no que no haya que no haya sobrecarga pero claro igual este sistema se tendría que programar de alguna forma para decir Oye pero si realmente no es necesario que se abra que se abra el circuito para que se se haga un un apagón Entonces no no lo vuelvo a cerrar podría pod implementarse una lógica me acabo de acordar me pasó hace dos semanas un ejemplo claro de de medidas en contra de variaciones digamos impropias o inesperadas en la tensión me pasó a mí en casa Que bueno encontré una Wii vieja que tenía pero de Estados Unidos y ahí voy yo todo campeón la enchufa pa pegó un petardazo saltaron los plomos menos mal si no lo que decía yo no no que me llegue un mensaje a mí antes de que salten los plomos le doy y mientras se quema toda la casa claro yo Esto no es la primera vez que veo un aparato que solo soporta los 110 volos de Estados Unidos porque normalmente tenemos el rango de 110 no a 220 pero la Wii pues no tío viene con el adaptador con de 110 claro chuf un humo un olor tío reventó el el adaptador entero tío y pero claro Menos mal que saltaron los plomos sin preguntarme antes seguro que en plan clipy seguro que deseas que salten los plomos un caso similar que habí ha pasado es e con un con un secador de pelo que te lo llevas de un continente al otro lo conectas y se empezó a poner rojo los filamentos y digo Y esto y esto y esto lo paré porque di Ah okay Porque estoy usando un adaptador sin sin sin transformador de de voltaje y se estaba poniendo el secador al rojo io digo si si tardo 10 segundos como tú dices Sí sí es que es super peligroso tío Sí sí sí porque el mío ya saltó de

repente Supongo que tendría algo pero el tuyo se simplemente empieza a derretirse no Mola mucho la verdad sí así que porque si es al revés si lo llevamos de Europa a Estados Unidos pues simplemente o Funciona muy poquito o no funciona eso es pero pero traerlo de allí ojo cuidado eh ojo cuidado ojo ojo cuidado bueno queridos oyentes hasta aquí Hemos llegado Muchas gracias por quedaros hasta el final recordar echarle un vistazo a los enlaces de nuestros sponsors que os los dejamos en las notas del episodio y nos ayuda con el podcast también de nuevo gracias a nuestros amigos de patreon que están ahí apoyándonos recuerda compartir este podcast este episodio para que flipen un poco Cómo sefiltra información cómo se apagan la electricidad en una ciudad con tus amigos y compañeros Gracias por quedaros hasta el final Muchas gracias Y de nuevo feliz semana de Acción de Gracias y nos vemos en el siguiente episodio Adiós adiós chao chao 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