un nuevo y novedoso vector de ataque contra la autenticación biométrica mediante huella digital en dispositivos Android permite acceder a los móviles y aplicaciones protegidas mediante este sistema barracuda publica un parche para su dispositivo email Security Gateway debido al descubrimiento del grupo apt chino umc-4841 explotando una vulnerabilidad de día cero para espiar a víctimas en todo el mundo incluyendo gobiernos desde la Cyber World con amor ya tienes listo un 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 21 de junio de 2023 es el episodio número 98 yo soy Martín vigo y está conmigo en diferido Pero bueno presente a Alexis porros Hola Alexis qué tal pues muy buenas Martín aquí en otro episodio más contigo oliendo a los 100 Sí sí a los 100 episodios y pensando igual llegando a tan tal número en igual podríamos cambiar el nombre del podcast no de tierra de hackers a tierra de jaquerazos Porque después de tanto ciber criminal suelto en nuestros episodios pues es una broma obviamente tierra de hackers aquí se queda nada os queremos dar las gracias a todos vosotros queridos oyentes por apoyarnos online en redes sociales plataformas de podcast y sobre todo por escucharnos episodio 3 episodio y para no alargarme mucho recuerdo que estamos en todas las redes sociales más populares nos podéis encontrar como tierra de hackers o @tierra de hackers también en todas las plataformas de podcast si no lo estáis ahora mismo pausad y ir a suscribiros a nuestro podcast en vuestra plataforma de podcast favorita para recibir las notificaciones de los nuevos episodios Y tenemos un servidor muy Majo de discord que podéis acceder vía tierra de hacker barra discord ahí tenemos muchas conversaciones interesantes de varios temas sobre todo enfocados en ciberseguridad Así que os invitamos a uniros al servidor de discord Y como siempre cierro la intro Agradeciendo vuestro apoyo a la pregunta del episodio que publicamos en Twitter y que la del anterior fue la siguiente en el contexto de la vulnerabilidad en el proceso de actualización del firmware de placas base de gigabyte estarías dispuesto a seguir usando sus productos en el futuro os dimos cuatro opciones la más votada es un Sí porque se puede mitigar con un 50% Así que la mitad de vosotros queridos oyentes dijisteis que sí luego esta fue seguida por no ya no los veo seguros con un 38% y luego tenemos sí obligado por contrato no me puedo escapar con un 8% y finalmente con un 4% no nunca más pues perfecto yo para variar darle las gracias a nuestros mecenas de patreon que hacen este podcast posible y que pueda ser gratis para todo el mundo y también a nuestros sponsors esta vez con brawler pro una herramienta más completa la más completa en seguridad y en aws empresas de todos los tamaños apoyan diariamente en brawler pro para que sus equipos puedan confiar en su modelo de seguridad de aws puedes probar brawler Pro hoy mismo y de manera totalmente gratuita y obtendrás paneles y gráficas con información concisa y accionable con todo lujo de detalles sobre la madurez de tu modelo de seguridad y visión completa de tu infraestructura en todas las regiones de aws y además tendrás todos los resultados en apenas unos minutos empieza a usar brawler pro y beneficio te de sus resultados visitando tierra de hackers.com barra brawler Pro prw l e r pro y también tenemos a un branding una empresa formada por especialistas en varios ámbitos profesionales que se enfoca en la reputación online a múltiples niveles han ayudado desde personas como tú y como yo hasta famosos a llevar a juicios a juicio casos de ciberacoso mitigar situaciones donde la reputación de empresas estaba siendo mal intencionadamente dañada e incluso borrar la huella digital que dejamos online no Solo han decidido Apoyar el podcast sino que si le contáis que venís de parte de tierra de hackers tendréis un descuento especial en sus servicios si necesitáis algún tipo de ayuda con vuestra identidad digital on branding es lo que estáis buscando visita on branding.es o nbrand y n g punto es y Bueno antes de empezar solo comentaros con transparencia que Alexis y yo estamos grabando por separados la razón es que yo me hallo en la Cyber World uno de los

eventos más chulos que a los que contenido organizado por la Policía Nacional de España y la verdad son tres días muy chulos de charlas amigos y básicamente juntarte con la gente que se dedica a lo mismo que nos apasiona a todos Así que desde aquí estoy grabando desde una de las habitaciones y nada muy contento la verdad estamos también a Solo dos episodios del episodio 100 en el episodio 99 os contaremos que tenemos pensado para celebrar ese episodio número 100 que será un episodio especial Así que a ver qué os parece y Bueno yo creo que ya podemos empezar y en este caso yo os vengo a hablar de una nueva vulnerabilidad que afecta a prácticamente todos los dispositivos de Android Así que si nos estás escuchando desde un dispositivo Android esto te interesa Y aunque sea desde un iPhone también te interesa una vulnerabilidad que permite atacantes desbloquear cualquier teléfono y acceder Su contenido una vulnerabilidad que se centra en atacar la autenticación biométrica basada en huellas dactilares Y la verdad de una manera muy original ya que los vectores de ataque que hemos visto hasta día de hoy a este tipo de sistemas de autenticación era mediante la réplica de huellas dactilares en dedos falsos o bueno copias de las huellas del objetivo que previamente ha robado de alguna manera lo típico que vemos en las pelis de un vaso no O así pero con brooth print nombre que le han dado a esta nueva vulnerabilidad la metodología es diferente de hecho los investigadores no solo encontraron un vector de ataque sino varios Y estos les permite atención interceptar las huellas dactilares de bueno del dueño del teléfono no la clonación de esas huellas dactilares el bypass el saltarse el límite de intentos fallidos antes de que haya que esperar para volver a intentarlo como os explicaré más adelante tú cuando usas la autenticación biométrica de huella digital si falla tres veces pues vas a tener que esperar un minuto para volver a intentarlo o te fuerza a utilizar el pin pero lo más importante es que estos ataques también permiten la fuerza brutal brut for sin de huellas dactilares este la verdad es el que más me sorprendió hacerlo Fuerza bruta a un sistema de identificación de huellas dactilares Pues cómo es eso posible no tienes 50.000 dedos y vas probando uno a uno o no sé te vas haciendo pequeños cortes en el dedo gordo para alterar las huella hasta que aciertas como es esto de Bruce for sin de huellas digitales de huellas dactilares Pues antes de meternos de lleno en este paper titulado brut print exponiendo la autenticación de huellas dactilares de teléfonos inteligentes a un ataque de Fuerza bruta es así como se llama este paper que por supuesto os dejo en las notas del episodio y de hecho los autores son y Jean G que son ambos de que por lo que ponía ahí están haciendo un intensible que viene siendo una beca en la empresa tencent y y lo primero que tenemos que hacer como decía es antes de meternos de lleno Cómo funcionan estas vulnerabilidades entender los detalles sobre cómo se utilizan las huellas dactilares a día de hoy en un artículo de Kaspersky mencionaban un trabajo de 1982 nada más y nada menos Eh ya Ya llovió que asentaba las bases del conocimiento sobre las huellas dactilares y de hecho en el que se basa toda la ciencia moderna en torno a ello ya en este trabajo se estipulaba que si bien es cierto que las huellas dactilares son únicas incluso entre gemelos o mellizos se estimaba que se producía una coincidencia cada dos elevado a 36 veces unos 64 mil millones de veces o sea Dicho de otro modo cada una de cada 64.000 millones huellas dactilares las detectaríamos como si fuera la misma a pesar de que son diferentes por lo menos aquí ya tenemos digamos un margen de error finito no ahora esta ecuación aquí viene lo importante le tenemos que Añadir que los sistemas de lectura de huella digital perdón si estoy diciendo constantemente voy a digital y es huella dactilar Pues bueno estos sistemas de lectura tienen ciertas limitaciones pensad que por un lado el abaratamiento de costes sobre todo en la electrónica de consumo global hace que los fabricantes no incluyen por los sensores de lectura de huella dactilar demasiado sofisticados lo incluyen lo suficiente para considerarlo seguros el tacha ID el de la pantalla de los teléfonos Android pues esos sistemas no son lo más sofisticados del mundo porque se intenta varetar el precio de los

teléfonos Entonces no puedes meter algo demasiado potente sobre todo si no es con que sea suficientemente bueno suficientemente seguro pues ya llega siempre hay un balance no entre entre el precio del coste de dispositivos para formar un teléfono móvil Y lo bueno es que son hay que encontrar ahí el punto intermedio por otro lado tenemos que la detección de la huella dactilar y cotejo ha de ser muy rápida de hecho casi inmediata imaginaros que para desbloquear tu teléfono móvil con el dedo pues pones el dedo y tienes que esperar yo que sé 10 15 segundos a que se escanee la huella y se compare pues con la que tienes almacenada para ver si es correcta No nadie usaría ese método de autenticación si cada vez que quieres bloquear el teléfono hay que esperar 15 segundos por lo que los fabricantes han de reducir el tiempo de verificación de la huella al máximo y esto por supuesto conlleva el incremento de falsos positivos y falsos negativos y aquí llegamos al tercer problema si cada dos por tres al desbloquear nuestro teléfono el sistema lo detecta como la huella equivocada eso también nos frustraría muchísimo Tú piensas que si yo cada 10 veces que desbloqueo el teléfono me da un error a pesar de ser yo al final digo este sistema es un peñazo O sea no no funciona bien cada 10 veces no me detecta que soy yo a pesar de que es mi huella Entonces los fabricantes aquí han de implementar cierta tolerancia al error para no incurrir en bloqueos si la lectura de la huella por ejemplo no es perfecta porque la pusiste un poquito de lado todo esto es en pro de la usabilidad por tanto si resumimos nuestros dispositivos móviles tienen sistemas de autenticación biométrica mediante huella dactilar que para que el teléfono sea barato y usable tiene cierta tolerancia los errores y además no son super sofisticados a la hora de detectar las huellas pongamos un número a esto Apple hace referencia en sus papers admitiendo que tacha ID que por cierto está considerado como probablemente el sistema de lectura de huella dactilar más seguro en un dispositivo móvil Dice que podría detectarse dos huellas dactilares distintas como iguales en el orden de una entre 50.000 veces eso es muchísimo menos que una entre 64 mil millones que el trabajo de investigación del siglo XIX nos decía precisamente por todo lo que os he comentado el tacha ID Una entre 50.000 veces va a detectar dos huellas dactilares distintas como la misma Pero por supuesto los fabricantes no son ajenos a esto y por eso se han implementado límites a los intentos de autenticación por huella dactilar si tú ahora intentas usar un dedo no registrado por ejemplo pues tu dedo meñique no para desbloquear tu teléfono verás que falla y al tercer fallo ya no te ofrecerá desbloquearlo con la huella dactilar sino que tendrás que hacerlo forzosamente con el pin o a lo mejor tu teléfono implementa Pues un sistema de retraso en el que tienes que esperar un minuto en el que teléfono el teléfono no se puede desbloquear ya para volver a intentarlo tiempo que además incrementará si sigues fallando la autenticación es decir si vuelves a poner el dedo meñique entonces tener que parar 5 minutos y luego 10 y luego 20 esta penalización de tiempo es la solución que han encontrado los fabricantes a posibles ataques de Fuerza bruta a sus sistemas de lectura de huella dactilar bueno es aquí donde entra brute print y lo que os mencionaba que han conseguido no solo hacer ataques de Fuerza bruta sino también saltarse esa limitación de intentos algo que por supuesto era esencial vamos a ver cómo lo han hecho teniendo en cuenta que hablamos de sistemas Android muchos de los dispositivos conviene mencionar que tienen El lector de la huella dactilar integrado en la pantalla no es como los iphones un poco más antiguos que tenían el botón este de Home que a su vez leía la huella dactilar los nuevos teléfonos de Android pues ya lo tienen integrado en la propia pantalla No de hecho las pruebas que han hecho los investigadores para para demostrar Brooke print lo hicieron sobre un teléfono móvil One Plus 7 Pro que tiene uno de estos sistemas de huella de lectura de huella dactilar integrado en la propia pantalla Pues bien Lo primero de todo es entender cómo han conseguido interceptar las huellas dactilares eso sería lo primero pensamos en cómo se transmite información hoy en día de un sistema a otro en componentes electrónicos pues

normalmente a través de un cable no tiene que haber una vía digamos mediante la cual se transmite la información que bueno no deja de ser oscilaciones en el voltaje electricidad vamos Ok pues entonces podemos asumir que un dispositivo móvil tenemos varios componentes electrónicos entre reduciéndolo a los que nos interesa se encuentra el sensor de las huellas dactilares o El lector y además un sistema encargado de recibir procesar y almacenar la información de tu huella digital para compararla luego hoy en día por motivos de seguridad y privacidad la información de nuestras huellas dactilares se almacenan un chip seguro al cual no se puede acceder para extraer la información esto Bueno estoy simplificando muchísimo y además la huella dactilar no se almacena como tal en plan una foto de nuestro dedo no sino que a la lectura de los datos biométricos de nuestra huella dactilar se le aplica una serie de digamos operaciones Matemáticas para que sin tener que llegar a almacenar la información real biométrica podemos aún así verificarla algo así como la manera de almacenar las contraseñas con un Hash que ya es que que ya os tenemos comentado muchas veces solo que en este caso pues las huellas dactilares por tanto si Este chip no se le puede extraer la información y además aunque pudiéramos no nos serviría de mucho ya que no almacena la imagen real de nuestra huella dactilar que atacamos pues atacamos a la vía que conecta el sensor de huellas dactilares y ese chip el mecanismo de comunicación por el que se transmite esos datos el cable digamos por el que se transmite toda esa información de un lado a otro y esto lo hacemos con la esperanza de que como sabemos que el lector de huella dactilar no hace los cálculos matemáticos para enmascarar la información biométrica sabemos que esa información se está transmitiendo por esa vía si lo conseguimos interceptar tendremos la información de la huella dactilar en sí como analogía se me ocurre que quieres saber lo que ha comido tu vecino No que ha podido que ha pedido pues por ejemplo comida por Uber eats no comida para traerse a su casa bueno el restaurante hace la comida y la envía con un repartidor que va en su motito hasta la casa de tu vecino en cuanto le llega la comida él la come y lo que queda queda almacenado Digamos como muestra es bueno pues cuando va al baño y lo expulsa por el ojo de las mil pestañas el acto de comer comida y expulsar los desechos es el equivalente a las operaciones Matemáticas que aplica el chip en cuanto llega la comida se la come y lo que queda pues son las heces no claro nos es muy difícil saber que ha comido exactamente nuestro vecino Si todo lo que tenemos son las heces por tanto tenemos que atacar al repartidor ya que sabemos que él lleva la comida en sí no le lleva las heces ya hechas no bueno perdón este ejemplo me ha quedado un tanto escatológico pero es lo mejor que se me ha ocurrido Qué quieres que te diga Ok pues ya sabemos que tenemos que atacar al repartidor o en el caso del móvil a la pista del circuito por el que se transmite la información y cómo hacemos esto pues bueno si lo tuyo es el Hardware hacking pues ya sabrás de esto y si no pues decirte que existen múltiples protocolos para transmitir información entre componentes electrónicos y digamos también maneras de de buguear de de eso de verificar circuitos en el fútbol correcto funcionamiento de circuitos para encontrar errores por ejemplo uno de los protocolos es spi o serial prefierol interface y existen componentes electrónicos que entienden este protocolo y nos permiten interactuar con los circuitos Y esto es exactamente lo que hicieron los investigadores mediante spi se engancharon a la pista por la que circula la información de la huella dactilar y se dieron cuenta que no iba cifrada por lo que les permite acceder y robar la información sin ningún tipo de protección de la huella dactilar esto es como si mientras va el repartidor por la calle tú le das el alto le paras y la comida que la lleva ahí en la bolsa pues no viene digamos cerrada con un candado viene simplemente que tú puedes abrir la bolsa y ver lo que hay esto es uno de los fallos de diseño esenciales de la mayoría de los teléfonos que utilizan Android porque los iPhone según Los investigadores sí que cifran la información de la huella dactilar antes de enviarla al chip mediante spi que es luego quien la

procesa Así que mini punto para los iPhone respecto a Android Ok ya sabemos que podemos interceptar huellas dactilares Pero esto no es realmente un ataque práctico estamos hablando de que tendrías que no sé insertar un componente electrónico dentro del móvil de tu objetivo sin que el usuario lo notase para ir interceptando sus huellas y podría hacerse pero lo comento porque si podemos interceptar huellas dactilares quizá también podemos inyectar huellas dactilares es decir si yo puedo interceptar la comida que lleva el repartidor también puedo sustituirla o modificarla añadiéndole veneno Y esto es el siguiente paso que hicieron los investigadores para lanzar los ataques de Fuerza bruta de huellas dactilares empezaron a inyectar muestras de huellas dactilares con la intención de que insertando miles de ellas debido al margen de error que os comentaba que tienen este tipo de lectores alguna daría una identificación positiva recordemos Apple dice que de 50.000 huellas diferentes dos van a dar como si fueran la misma Y dónde han sacado Los investigadores muestras de huellas digitales en los miles Pues en el propio paper mencionan que hay varios bancos públicos con miles de muestras de huellas dactilares Los investigadores fueron un paso más allá y utilizaron Inteligencia artificial para optimizar el ataque creando como su propio diccionario un poco como se hace también con las contraseñas pues hicieron un diccionario de muestreo de huellas dactilares optimizado para encontrar lo más rápido posible una muestra que no es realmente la del usuario que Desbloquea aún así el teléfono aprovechándose del margen de error muy guapo la verdad utilizar el protocolo spi para engancharse a la línea de transmisión de datos entre el sensor de huellas dactilares y el chip que las almacena para alterar el tráfico de datos y empezar a bombardearlo con las huellas dactilares extraídas de un banco de muestras ole ole pero nos queda una última Barrera por derribar queridos oyentes el límite de los intentos tenemos la infraestructura para bruto forcear huellas dactilares pero necesitamos saltarnos esa protección para que realmente sea escalabre y realista este ataque Y esto es lo que han denominado cancel after match fail Y la verdad es que está guapísimo a ver prestar atención resulta que el sensor de las huellas dactilares de nuestros teléfonos no toma una sola muestra de nuestra huella sino varias es como si sacase varias fotos y las envía todas al chip cuando apoyamos el dedo esto lo hace para una vez más paliar el problema de los falsos negativos mejorar la usabilidad de estos sistemas propensos a errores y que una lectura mala no signifique inmediatamente que detecte la huella como falsa Por tanto se envían tres o cuatro muestras y con que una de las cuatro de positivo pues se desbloquea el teléfono aunque las otras tres den negativo imaginaros que cuando tú vas a apoyar el dedo A veces pues lo apoyas un poquito de lado o lo mueves Pues por eso saca varias fotos y con que una de ellas Ya de positivo pues ya está pero hay otra particularidad más interesante aún y es la que explotan Presta atención los diferentes muestras que toma el sensor cuando apoyamos el dedo pueden dar no solo negativo sino también error Estos son dos estados diferentes negativos es que ha leído correctamente la huella dactilar pero determina que no es la huella del dueño error es que la muestra no tiene calidad suficiente o no se ha tomado bien porque has apoyado el dedo mal y Qué pasa cuando da error en vez de negativo Pues que el contador que establece el límite de intento se resetea vuelve a cero y Sabiendo esto Los investigadores lo que hacen es probar tres muestras del banco de huellas dactilares y añaden inyectan una última muestra que saben con antelación que va a dar error así resetean el contador y pueden volver a enviar otras tres huellas con una vez más otra final que da error de hecho la misma y así sucesivamente sin que nunca lleguen al límite de intentos que les forzaría tener que esperar a que es ingenioso así que resumiendo ya toda la noticia básicamente estos investigadores han encontrado una una manera de lanzar ataques de Fuerza bruta de huellas dactilares contra dispositivos móviles de Android y lo hacen inyectando muestras de huellas directamente en la línea por donde se transmite la información entre el sensor y el chip que lo almacena y además

se aprovechan de una vulnerabilidad en la que saben que cuando hay un error de lectura el contador de que determina si se va a bloquear el teléfono y hay que esperar un minuto para volver a intentar una huella dactilar se resetea por tanto envían tres muestras correctas y una que saben que da error se resetea cero envía entre muestras correctas y un error y así sucesivamente es decir han encontrado un patrón en la huella dactilar quien les permite resetear el contador constantemente y lo que hacen es enviarla cada cada cuatro muestras Pues con todo este conocimiento crearon un pequeño dispositivo físico que les costó en piezas pues unos 20 eurillos con unos besos 20 dólares con con este dispositivo ya puede lanzar el ataque de Fuerza bruta y estiman que en el mejor de los casos tarda unos 40 minutos en conseguir desbloquear el teléfono es decir esto no se trata de algo solo académico han han creado el dispositivo físico un pequeño dispositivo de Hardware en principio este ataque a nosotros no debería preocuparnos mucho si bien es cierto que funcionan prácticamente todos los teléfonos de Android no es a escala tú necesitas tener acceso al dispositivo físico y además se tarda tiempo en desbloquearlo dicho esto brut print En mi opinión tiene un valor inmenso para las fuerzas y cuerpos de seguridad del estado pensad que muchísimas agencias para resolver casos pagan una millonada por licencias de software especializado en análisis forense que para versiones antiguas de teléfonos incluso puede desbloquearlos celebrate reiki y otras pues son empresas que desbloquean ciertos teléfonos pero que valen una auténtica pasta también por ejemplo pensad en la importancia que tiene esto para las agencias como como cuando por ejemplo la lucha del FBI contra Apple no por desbloquear teléfonos o el caso del tiroteo de San Bernardino en Los Ángeles en el que la policía de Los Ángeles acabó pagando un pastón a una empresa australiana llamada azimus para desbloquear el iPhone del sospechoso porque así Podría tener pruebas de que efectivamente él fue el autor pero ahora todo esto en vez de pagar un pastón las fuerzas y cuerpos de seguridad del Estado pueden resolver casos por solo 20 euros y el conocimiento que os Acabo de compartir en esta noticia muy buena noticia Martín por mi parte bueno igual algunos oyentes lo esperan pero mi primer comentario es el siguiente Y para cuándo un ataque similar para el Iris de los ojos para que pueda registrarme un millón de veces y multiplicar por un millón la recompensa de criptomonedas de World coins que me dan al registrarme en World ID Sí sí os acordáis no del episodio y la broma de los ojos arrancados a las vacas para que tener más más digamos más personas para registrarme en ID y obtener más walcoins bueno fuera bromas en cualquier caso este tipo de ataques me parecen muy graves porque esto puede permitir a cibercriminales desbloquear dispositivos y acceder a información personal y confidencial lo que significa correos electrónicos mensajes de texto fotos ya sabemos esas fotos que se hacen a documentos confidenciales no A eso me refiero y datos de aplicaciones de como los gestores de contraseñas que llevamos en los móviles hoy en día los teléfonos móviles son más valiosos que los sistemas portátiles de sobremesa o servidores O al menos a mí eso me lo parece me lo intuye y lo digo porque todo el mundo tiene al menos un teléfono móvil pero no todo el mundo tiene otro dispositivo adicional Además del teléfono móvil y por tanto la vida de cada persona a nivel mundial puede estar en cada uno de sus dispositivos y comprometiéndolos un atacante podría causar mucho daño a estas personas a las víctimas también quiero recalcar el tema de las limitaciones de este ataque porque parece muy interesante pero Digamos como en todo hay limitaciones o lo podemos llamar condiciones no que se requiere para que este escenario este ataque se pueda materializar y se pueda llevar a cabo pues una de ellas es que el dispositivo tiene que estar en posición física del atacante así que ya sabéis prevención número uno no perdáis en vuestro dispositivos físicamente ni de vista por un minuto bueno por un minuto no por unas cuantas horas no porque en este análisis en esta investigación comentan que pueden desbloquear dispositivos a través de este ataque de Fuerza bruta de

huella dactilar en horas no necesitan 7 8 9 10 horas incluso más así que probablemente a no ser que te haya sido a dormir y no te des cuenta dónde has dejado el teléfono antes de llegar a casa pero normalmente en tantas horas uno se da cuenta de dónde está el dispositivo y puede empezar a reaccionar y intentar no sé de anular cambiar contraseñas y anular tarjetas de crédito Aunque Bueno cuando pierdes el dispositivo no piensas que alguien un atacante te lo está desbloqueando no así que bueno pensemos en eso la otra limitación es que los atacantes necesitan la huella dactilar de la víctima como parte del diccionario utilizar durante el ataque de Fuerza bruta para poder desbloquear el dispositivo estas huellas según Comentan los investigadores las pueden obtener de conjuntos de datos de estudios académicos de brechas de seguridad y bueno recuperarlas ellos mismos de forma activa a través de osint probablemente fotos de alta resolución en internet y similares Así que una idea que se me ocurre sería utilizar las huellas dactilares de los dedos de los pies para desbloquear los teléfonos sí sí no ríéis pero fuera broma parece poco práctico pero Oye si sois tan paranoicos pues incrementaría seguro la seguridad de vuestro dispositivo porque obviamente vuestra huella dactilar de los dedos de vuestros pies nos la han pedido al entrar en otros países como por ejemplo Estados Unidos verdad o para no sé para cuando os hacéis el pasaporte o el documento de identidad y lo digo porque si os lo han registrado pues está en algún sitio digital y sabemos que todo lo digital se puede comprometer y Por ende estas estas huellas de actividades en forma digital podrían acabar en manos de los atacantes que quisieran lanzar este tipo de ataque de Fuerza bruta De todas formas no Cantemos Victoria con lo de utilizar las huellas dactilares de los dedos de los pies porque los investigadores comentan que en el futuro podrían crear una base de datos de huellas dactilares de forma sintética mucho más completa que la que pueden obtener como digo a través de datos de estudios académicos de brecha de seguridad y recopilación activa no y cómo lo harían Pues a través de redes neuronales lo que significa que podrían incluso obtener vuestra huella de los dedos de los pies Incluso si no la habéis registrado en ningún sistema online Así que lo mejor es no perder de vista ni de forma física vuestros dispositivos móviles e intentar utilizar otros métodos de protección de los datos confidenciales que vuestro dispositivos móviles contienen que sea diferente a las de las huellas dactilares una combinación de Pin y igual huella dactilar que no sea solo se va a ser en una huella dactilar combinación de más de un factor es lo queremos dar 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 mandarles vuestro currículum a tierra de hackers arroba-monat.commod.com pues la noticia que os traigo ahora va de barracuda no no el pez sino la empresa de servicios de ciberseguridad y dispositivos como sistemas de seguridad de en email un grupo apt chino y finalmente Vais a escuchar que os voy a recomendar esto no no soy yo quien emite esta recomendación sino barracuda que tiréis a la basura vuestros emails Security gateways y Vais a entender porque ahora cuando se explica la noticia así que quedaos hasta el final el 23 de mayo de este año barracuda proveedor de servicios de seguridad de red y protección de correo electrónico advirtió a sus usuarios sobre una falla una vulnerabilidad de día cero que según dijo había sido explotada y probablemente sigue siendo explotada hasta la fecha para comprometer dispositivos de barracuda email Security Gateway la empresa dijo que corrigió y publicó un parche para esta vulnerabilidad el 20 de mayo de 2023 esta vulnerabilidad en concreto se la traquea se la rastrea como cv-2023 guión 2868 esta volaridad se ha descrito como de inyección

de código remoto Remote Core execution que afecta a las versiones de entre 5.1.3.001 a la 9.2.0.006 con una puntuación de cvss de 9,8 para los que no lo sepáis está puntuación es una escala que va de 0 a 10 y 10 significa que es una vulnerabilidad supercrítica que vamos que te comprometen sin casi sin abrir los ojos casi sin respirar y en concreto esta en concreto Debería ser una puntuación de 10 porque no requiere autenticación el dispositivo está accesible desde internet y bueno y permite ejecución de código remoto pero en cualquier caso significa que ya sea 9.8 o 10 significa que es una vulnerabilidad crítica que requiere atención y remediación o un arreglo inmediato la buena idea surge de un fallo en la digamos sanitización del proceso de archivos punto tard en lo que respecta a los nombres de los archivos contenidos en este archivo.tar para los que no conozcáis los puntos tar son muy parecidos a un archivo comprimido zip pero de hecho un punto tar No es comprimido solo es que sea empaquetado en un único archivo es decir es como si concatenaras muchos varios en uno solo y a ese archivo le añades la extensión.tar porque tiene un formato específico no pues el problema es que un atacante remoto puede formatear específicamente estos nombres de archivo de una manera específica maliciosa Obviamente que lo que hace es el resultado es la ejecución remota de un comando del sistema a través del Bueno un componente específico el operador qx de Pearl con privilegios del producto email Security Gateway del usuario que esté corriendo este este dispositivo este apliance vamos es una vulnerabilidad de como digo ejecución de código remoto pero a través de la inyección de comandos porque en este caso si se pone por ejemplo ls barra en uno de los nombres de los archivos contenido en el archivo punto tar pues lo que va a hacer el email Security Gateway es listar los archivos en la raíz del sistema de ficheros un ls espacio barra Por eso digo que se le pueden inyectar comandos y el emailgate ese dispositivo va a correr cualquiera de estos comandos que se especifiquen en uno de los archivos dentro del archivo tar Bueno a nivel de sistema operativo Y cómo identificó barracuda esta vulnerabilidad Pues el 18 de mayo de este año la empresa identificó tráfico anómalo originado en los dispositivos sg y melseadway los voy a llamar a partir de ahora sg y comenzó la investigación solicitando la ayuda de mandiant ahora parte de Google comenzaron a examinar el problema y en un día el 19 de mayo identificaron la vulnerabilidad en los dispositivos sg de barracuda un día después el 20 de mayo publicaron el parche luego el 31 de mayo barracuda publicó una guía de seguridad con instrucciones para remediar el problema de los dispositivos afectados medidas adicionales a las de aplicar el parche Un día después la compañía compartió un resumen preliminar de los hallazgos clave y cinco días después el 6 de junio barracuda reiteró que los usuarios de los dispositivos afectados deberían aplicar el parche publicado y las medidas de seguridad adicionales como parte de la investigación conjunta entre barracuda y mandian descubrieron evidencia de explotación activa de esta vulnerabilidad por parte de cibercriminales que la estaban abusando para acceder a dispositivos de sg muy específicos Vamos en un ataque muy dirigido a víctimas seleccionadas mandiant identificó a unc48-41 como el grupo apt detrás de los ataques que explotaban esta vulnerabilidad que es un grupo que tiene vínculos con el gobierno chino la explotación de esta vulnerabilidad por parte de unc48-41 se remonta al menos hasta el 10 de octubre de 2022 es Entonces cuando tienen la evidencia más temprana de la explotación de esta vulnerabilidad el 2 de diciembre del año pasado es la fecha de la primera evidencia de exfiltración de correos electrónicos luego ya en este año el 16 de Mayo es la fecha de la evidencia más temprana de movimiento lateral a través de la explotación de esta vulnerabilidad es decir una técnica de post explotación un nc48-41 estaba atacando y con por venciendo dispositivos barracuda sg muy específicos para utilizarlos como vector de espionaje contra diferentes organizaciones abarcando múltiples regiones el 55% de las cuales se encuentran en América el 24% en Ema que es Europa medio oriente y África y el 22% restante en apac que es Asia Pacífico que incluye países de Asia y del

Pacífico Sur y contra sectores de diferente índole aproximadamente el 27% de las organizaciones atacadas eran gubernamentales y el resto eran empresas privadas durante la investigación se descubrieron scripts de shell que apuntaban a dominios de correo electrónico y usuarios del Ministerio de asuntos exteriores de asean que es un acrónimo en inglés que significa asociación de Naciones del sudeste asiático una organización regional que comprende 10 países del sudeste asiático que son brunei Camboya filipinas Indonesia laos Malasia miamar Singapur Tailandia y Vietnam así como oficinas de comercio exterior y organizaciones de investigación académica en Taiwán y Hong Kong además los cibercriminales buscaban cuentas de correo electrónico pertenecientes tanto a individuos que trabajaban para un gobierno con interés político o estratégico para china como a gobiernos que participaban en reuniones diplomáticas de alto nivel con otros países los primeros compromisos parecen haber ocurrido en un pequeño subconjunto de dispositivos localizados en China continental a partir del 10 de octubre de 2022 unc48-41 envió correos electrónicos a las organizaciones víctimas que contenían archivos adjuntos tar especialmente diseñados para explotar esta vulnerabilidad Y obtener acceso inicial a los dispositivos barracuda esg en los correos electrónicos iniciales unc48-41 adjunto archivos con una extensión.tar obviamente para para lanzar esta vulnerabilidad en el nombre del archivo mientras que en correos electrónicos posteriores utilizaron diferentes extensiones de archivo como punto jpg o punto dat independientemente de la extensión del archivo los adjuntos eran archivos dar válidos que explotaban dicha vulnerabilidad los correos electrónicos que se analizaron contenían un asunto genérico y contenido del cuerpo del correo Generalmente con una gramática deficiente con errores y en algunos casos incluso aún estos correos contenían valores digamos de una plantilla en plan querido usuario bla bla bla en lugar de decir querido Juan o querido Pepito no esto es muy interesante es una técnica de evasión una técnica disuasoria y probablemente fue para hacer que los correos electrónicos parecieran spam genérico con el fin de ser marcados de tal forma por los filtros de spam o también para disuadir a los analistas de seguridad de realizar una investigación completa Porque si tú ves que es spam normalmente los emails de spam no contienen temas maliciosos que vayan a poder ejecutar código remoto en sistemas y comprometer sistemas o comprometer cuentas no normalmente contienen temas de anuncios no y temas en el que tú clicas no te pasa nada realmente pero estás dándole digamos tu tiempo y tu clic a estos cibercriminales que se benefician porque has hecho el clic en temas en campañas de publicidad y similares eso por eso Supongo que querían que sus emails parecieran más tipo spam que no parecieran sospechosos y que parecieran buenos digamos para evitar análisis posterior un NC 48 41 utilizó varios métodos diferentes para enviar sus correos electrónicos a los dispositivos sg objetivo o incluso a las víctimas en algunos casos este grupo apete utilizó direcciones de correo electrónico de dominios inexistentes en el remitente del email en otros casos mandian observó que los cibercriminales utilizaban direcciones con dominios que probablemente no estaban en uso o que los cibercriminales no controlaban en la mayoría de los casos el grupo apt envió sus correos electrónicos desde un vps de vultur que es un proveedor de servicios de Hosting en un caso en concreto las cabeceras del correo electrónico enviado indicaban que provenía de una dirección IP asignada a China Telecom uno de los proveedores de servicio a internet de China obviamente por el nombre además gracias al análisis de la cabecera smtp x-mailer del email analizado se observó que el cliente de email utilizado por unc48-41 para enviar los emails era el mismo que utilizó otro actor de amenazas para enviar correos electrónicos de fishing con objetivos de espionaje y con nexos con china en otros casos los correos electrónicos provenían de direcciones de correo que pertenecían a organizaciones que habían sido comprometidas a través de este exploit y también incluso algunos emails venían directamente de los dispositivos barracuda sg comprometidos vamos

que este grupo apect chino o nc48 41 se había metido bastante adentro en muchas empresas y abusaba de ese poder esa ubicación para enviar emails en nombre en personando a esas empresas comprometidas lo curioso del Análisis es que mandian dice que un nc4841 según los artefactos y los binarios que han ido analizando utiliza muchas utilidades públicas que se pueden encontrar en github y similares una en concreto se llama csmtp que probablemente fue utilizada para enviar los correos electrónicos desde los dispositivos comprometidos en cuanto estos dispositivos quedaban comprometidos la carga útil o el primer paso después de comprometer a estos emails y gateways era establecer una conexión inversa a los servidores de unc4841 a lo que se conoce también en inglés como una River después de obtener acceso a estos dispositivos y establecer el command en control esta River esta conexión inversa el grupo apt chino descargó otros binarios en este caso puertas traseras secundarias y se identificaron en concreto tres de ellas que se llaman sispai Salt water y sea Side diríamos en español espía Marino agua salada y del lado del mar vamos que parece que les gusta mucho el tema de la playa estos chinos la primera six Pay es la puerta trasera primaria que funciona de forma pasiva y se despliega como un filtro de PK de digamos de análisis de captura de paquetes que monitoriza cualquier tráfico cualquier paquete que le llega al email Security Gateway de barracuda en los puertos tcp 25 y tcp 587 ambos utilizados para correr para ejecutar servidores de correo smtp y funciona de forma pasiva porque esta puerta trasera se activaba mediante lo que se llama un paquete mágico o un Magic packet que básicamente se refiere a un valor en concreto específico que está esperando que tiene hardcoreado digamos en su lógica de Back no de puerta trasera esto es muy similar a la técnica que igual habéis escuchado de port-in y de la que hemos en otros episodios y si no brevemente el tema es que el servidor en este caso digamos sería la puerta trasera que está escuchando de forma pasiva tiene programado una configuración una combinación de puertos específicos digamos 25 22 y 21 Pues si le llegan tres paquetes en ese orden a estos puertos 25 22 y 21 pues entonces se activa esta puerta trasera podríamos verlo como una contraseña pero a nivel de red y el análisis ha identificado una superposición de código entre sispai y CD 00r o se podría leer como seador una puerta trasera públicamente disponible así que ya hemos de nuevo reincidiendo en el tema de que este apt utiliza muchos muchos Software que es públicamente está públicamente disponible luego luego tenemos solt water que es un módulo para el servidor smtp de barracuda que tiene la funcionalidad de puerta trasera también siendo capaz de subir o Descargar archivos arbitrarios ejecutar comandos y también tiene capacidades de Proxy y tunelización de puertos de tráfico esta puerta trasera se despliega utilizando ganchos o en inglés hooks en llamadas específicas del sistema como por ejemplo Send reck V de shift y close luego tenemos sisite que es un módulo basado en Lua que es un lenguaje de programación para de nuevo el servidor smtp de barracuda el mismo que también digamos troyaniza saltwater que monitorea los comandos smtp Hello para recibir una dirección IP de command en control codificada y un puerto para los cuales establece una conexión inversa es decir esta también digamos de alguna forma está corriendo de forma pasiva y cuando Recibe un comando Hello smtp específico Pues digamos que decodifica el contenido de este Comando y extrae la dirección IP y el puerto del servidor al que tiene que establecer una shell inversa una shell reversa luego también tenemos otro componente que se llama Sand bar barra de arena de nuevo otro otra referencia a la playa que es un rootkit en forma de módulo de kernel del sistema de archivos de red troyanizado contiene también como el anterior ganchos o hooks para lo interesante de esto es que ocultar procesos que comienzan con un nombre específico esto tiende de nuevo está adaptado de código routing disponible públicamente de nuevo parece que este apt o sea en base a este análisis parece que es bastante avanzado por como descubrió la vulnerabilidad y todo lo relacionado con ello pero se apoya en muchas herramientas públicamente disponibles no sé si

lo hace para evitar utilizar sus propias herramientas y digamos quemar su sus capacidades o bueno o para digamos también marear un poco a los analistas de seguridad pero en este caso sanvar estaba configurado para ocultar procesos que estuvieran corriendo en el email Security Gateway que comiencen con el nombre bar Es probable que esto estuviera diseñado para ocultar el malware porque fue desplegado con el nombre barracuda mail service Así que cuando un administrador de estos dispositivos se conectará a ellos y hiciera un pies o un listar procesos este Root kit a nivel de kernel estaría ocultando todo proceso que empezará con el nombre bar incluyendo barracuda mil service que es el que estaba troyanizado con con este módulo de rootkit entre el 21 y el 22 de mayo de este año Poco después del despliegue inicial del Script de remediación de barracuda para parchear los dispositivos afectados unc4841 hizo rápidamente modificaciones tanto en los componentes relacionados con 6 Pipe como en saltwater para prevenir un parche efectivo luego entre el 22 y el 24 de mayo unc 4841 realizó operaciones de alta frecuencia en un número de víctimas ubicadas en al menos 16 países diferentes modificando siete componentes de seispa Y al menos dos componentes de Salt water todo esto como digo para seguir manteniendo su persistencia y el control de los dispositivos barracuda afectados además de instalar puertas traseras este grupo apt troyanizó varios módulos Lua legítimos de barracuda insertando lógica de shell o conexión inversa para ser ejecutada cuando ciertos eventos relacionados con el correo electrónico son recibidos por el dispositivo se identificaron y rastrearon un total de tres módulos troyanizados con dos familias de malware diferentes en este caso las han llamado sea spray y skip Jack de nuevo más referencias al mar six Play spray marino y skip Jack es un pescado digamos así azul Que bueno lo venden mucho en enlatado y no está mal fuera bromas six Play es un módulo de troyanización que monitoriza los archivos adjuntos de correo electrónico recibidos Y si alguno de estos tiene un valor especial copia el archivo en el directorio tmp y ejecuta un binario externo que ha descargado este grupo apt al dispositivo comprometido y de esta forma establece una conexión inversa con la ruta completa del archivo como parámetro es decir el archivo contiene una dirección IP y un puerto al que se conecta el módulo sispray mandian también descubrió una variante de este código que fue insertada en el módulo responsable de implementar la funcionalidad de bloqueo y aceptación del remitente eso cuando vas y dices quiero bloquear no quiero recibir más emails de esta persona lo pongo en la lista de bloqueo o lo pongo en la lista de digamos de aceptación siempre y lo que tenemos es skip Jack el pescado azul verdad una puerta trasera pasiva que es una versión troyanizada de un módulo de puerta de enlace de seguridad de correo electrónico de barracuda qué procesa las cabeceras de correo electrónico entrante y los asuntos y decodifica y ejecuta el contenido del campo de la cabecera content - ID en caso de que contenga un valor específico también y la tiene que descifrar primero porque el contenido de esta cabecera viene cifrado sobre el tema de la infraestructura de comando y control Comando en control se observó primero que la infraestructura utilizada por un unc48-41 estaba utilizando certificados ssl temporales autofirmados por defecto que se incluyen en los aparatos sg para fines de configuración esto es muy probable que se utilizará como de nuevo técnica para evadir sus acciones y mezclarse con la multitud con el tráfico normal no sería como intentar pasar su tráfico de shell inverso como comunicaciones legítimas ya que se realizaban a través de la infraestructura de barracuda porque contenían Digamos como digo en los parámetros del certificado ssl referencias a barracuda.com el segundo punto sobre la infraestructura de comando en control es que mandian observó que unc-48-41 comprometía robaba certificados ssl de las víctimas de las empresas a las que podía penetrar digamos a través del compromiso de estos dispositivos y juego pues utilizaba estos certificados ssl en su propia infraestructura de nuevo para pasar desapercibido esto ayuda mucho porque hace que el tráfico del atacante parezca legítimo no y

el tercer punto es que hubo algunos casos en los que los ciberdelincuentes simplemente utilizaron un certificado auto firmado generado con valores por defecto esto que es que aún se permita esto debería levantar muchas sospechas y lanzar digamos a equipos de seguridad a investigar qué es lo que pasa en ese tipo de tráfico pero bueno interesante que también incluso utilizaron este escenario un poco más rocambolesco no que primero con el primer escenario el segundo quieren pasar muy desapercibidos y con este es como están poniendo la música a tope sobre métodos de persistencia comentar que lograron la persistencia a través de Tres formas distintas la primera son trabajos o tareas de Chrome ejecutados cada hora y cada día la segunda es ejecución de todo su malware todos sus troyanos entonces Ruth Kids al reiniciar el dispositivo y la tercera es a través del rootkit de kernel sandbar porque como es un rootkit pues es mucho más difícil de Identificar y de eliminar los ataques estaban dirigidos sobre todo académicos reconocidos en Taiwán y Hong Kong así como a funcionarios gubernamentales asiáticos y europeos en el sudeste de Asia estaban buscando información de estas víctimas dentro de lo que se denomina m Store que es el lugar en el que se almacenan temporalmente los mensajes de correo electrónico en el dispositivo cuando encontraba lo que buscaban los datos los agrupaban en archivos puntotare.gz que como he dicho antes son en este caso sí que son archivos comprimidos sería casi lo mismo que un archivo zip y los ubicaban los guardaban en el sistema de ficheros del barracuda email Security Gateway en la ubicación barra mail barra tmp utilizando una convención de nomenclatura de archivos que contenía tres letras correspondientes a la organización de la víctima seguidas de un número de tres cifras como 001 finalmente los datos se filtraban vía ssl tls a través de Open ssl a los servidores de los cibercriminales y en un número limitado de casos incluso utilizaron el servicio de compartición de archivos Anon files.com que es del grupo anónimos Cuál es el impacto de todo esto a nivel mundial pues la compañía barracuda tiene más de 200.000 clientes globales pero no reveló la escala del ataque sin embargo un investigador ha identificado que a través de búsquedas en shoudan este buscador como Google pero de dispositivos conectados a internet se muestra que hay al menos 500.000 dispositivos barracuda email Security Gateway afectados y conectados a internet a fecha 10 de junio de este año aproximadamente el 5% de los dispositivos sg activos y conectados a internet en todo el mundo muestran evidencia de indicadores de compromiso asociados con esta campaña de espionaje de unc48-41 y tan importante es esta vulnerabilidad que el 26 de mayo la agencia de seguridad de infraestructura y ciberseguridad de Estados Unidos ciza agregó esta vulnerabilidad de inyección de código remoto que afecta a los dispositivos sg de barracuda a su catálogo de vulnerabilidades explotadas conocidas o en inglés el V instando a las agencias federales a aplicar las correcciones antes del 16 de junio de 2023 y con esto queridos oyentes llegamos a las recomendaciones para aquellos que os encontréis afectados por esta vulnerabilidad y por los ataques o los compromisos de este grupo apt chino Aunque esperemos que esta segunda situación no sea la vuestra solo la que tengáis dispositivos barracuda vulnerables y bueno los tengáis que arreglar básicamente Pues bien la primera de las recomendaciones y la más rotunda de ellas proporcionada por barracuda el 31 de mayo fue la de sustituir inmediatamente ipsofacto los dispositivos sg comprometidos independientemente del nivel de parche si están parcheados o no y de cuando los hayáis parcheado barracuda no dijo exactamente el porqué recomendaba tal radical medida pero es probable que sea una indicación de que los cibercriminales hayan logrado alterar el firmware a un nivel mucho más profundo que un parche pueda arreglar completamente además de esto se recomienda que todas las organizaciones afectadas realicen una investigación y actividades de red hunting dentro de sus redes para determinar si aún están afectadas Y si el enemigo se encuentra todavía dentro una investigación puede incluir tareas como las siguientes realizar búsquedas de

indicadores de compromiso proporcionados por barracuda y Mandy y mandiant que por cierto en las notas del episodio Vais a poder encontrar el artículo tanto de investigación de barracuda como de mandiant Y ambos contienen los indicadores de compromiso asociados con la campaña de espionaje de unc48-41 otra de las tareas es los registros de correo electrónico para identificar el punto inicial de exposición también revocar y rotar todas las credenciales de dominio y locales que estaban en el sg en el momento del compromiso También revocar y remitir todos los certificados que estaban en el sg durante el compromiso monitorizar en todo el entorno el uso de las credenciales que estaban en el dispositivo afectado durante el compromiso También monitorizar en todo el entorno el uso de certificados que estaban en el dispositivo cuando fue comprometido revisar los registros de red para detectar signos de exfiltración de datos y movimiento lateral y finalmente capturar una imagen forense de los dispositivos afectados y realizar un análisis forense todo esto está muy bien todas estas recomendaciones publicadas por barracuda Y mandian pues son muy buenas verdad pero no arreglan si nos paramos a pensar con detenimiento no arreglan el problema de la confidencialidad de los datos de El cuerpo del email que se envía de lo que contiene el email incluso de los archivos adjuntos y de hecho el impacto de este ataque contra la confidencialidad de los datos que se envían en los emails podría haberse reducido casi por completo Si organizaciones utilizaran cifrado extremo a extremo en las comunicaciones a través de los correos electrónicos y con esto me refiero a soluciones tipo pgp Pretty good privacy y las vertientes abiertas Open pgp y no pgp O gnu pgp entiendo que esto no se Comenta como recomendación Porque primero disminuye la visibilidad de organizaciones que requieren de la misma capacidad de espionaje contra todos los usuarios es decir contra todos los ciudadanos del mundo que los atacantes Como por ejemplo los gobiernos de los organización de los cinco ojos que es una organización de inteligencia que incluye a cinco países que son Estados Unidos Australia Canadá el Reino Unido y Nueva Zelanda y segundo porque no permitiría De hecho a empresas que ofrecen dispositivos de seguridad de correo electrónico como barracuda Poder De hecho ofrecer estos dispositivos y decir que protegen a sus clientes frente a correos maliciosos ya que no podrían inspeccionar el contenido de los mismos no tendrían visibilidad para poder determinar que contiene cada email que pasa por este email Security Gateway Así que aquí os lo dejo queridos oyentes Esta es una noticia de una vulnerabilidad de ejecución de código remoto de forma No autenticada que no se basa en lo que normalmente vemos no un fallo de corrupción de memoria Como por ejemplo un buffer o un stack overflow sino en un fallo de inyección de código y gracias a esto un apt chino catalogado como unc 4841 pudo comprometer sistemas tan inocentes como los dispositivos de seguridad de email de barracuda porque quién pensaría que estos se pudieran utilizar para llevar a cabo ataques de espionaje o de movimiento lateral no porque normalmente los que se atacan sobre todo son sistemas de VPN o sitios web expuestos a internet pero sistemas de seguridad de email no son tan sonados cuando se se publican incidentes de seguridad no Pues a través de estos dispositivos lograron infiltrarse en las redes de múltiples organizaciones en todo el mundo para espiar los emails recibidos por cada dispositivo y cada organización en busca de información confidencial y luego exfiltrarla como he dicho en algunos casos lo tenían muy claro estaban tras el rastro de personas muy específicas algunos ataques están muy dirigidos sobre todo a de Taiwán Hong Kong y bueno del sudeste asiático en general los atacantes principalmente abusaron de esta vulnerabilidad para espiar los correos electrónicos en tránsito en los dispositivos comprometidos de barracuda pero en alguna ocasión Los usaron también para moverse lateralmente y pivotar hacia dentro de la red de las organizaciones afectadas Esto no se ha determinado qué empresas han estado afectadas por esta capacidad no este movimiento lateral de este grupo pero igual en el futuro vamos a ver más

notificaciones sobre brechas adicionales a raíz de este incidente y de esta vulnerabilidad Así que ya sabéis queridos oyentes los que tengáis dispositivos como este el afectado barracuda email Security Gateway la recomendación principal es tirarlos a la basura y comprarlos otros los chinos y el espionaje la verdad es que no falla Y estoy convencido que vamos a seguir mucho más de esto en tierra de hackers en los próximos 100 episodios Gracias Alexis hasta aquí Hemos llegado vamos cerrando ya esto porque ha sido un episodio especial en diferido Muchas gracias por quedarnos con nosotros hasta el final esperemos que os esté gustando quedarnos quedaros como mínimo hasta el episodio 100 seguir dejando unos reviews comentarios en las plataformas de podcast donde nos escuchéis allí en Spotify que podéis dejar comentarios en Apple podcast y vuestras reviews Pues nos ayuda un montón gracias por ser fieles a tierra de hackers ya queda poquito ya queda poquito para el número 100 queridos oyentes Muchas gracias por el apoyo a todos como siempre seguir así pues nos vemos y nos escuchamos ya en el episodio 99 Adiós adiós chao chao nos escuchamos 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