Kaspersky descubre que varios de sus empleados tienen sus dispositivos móviles infectados con un malware altamente sofisticado y consigue hacerse con el implante y analizarlo archivos joros desatan pesadillas cibernéticas y ponen los pelos de punta a empresas afiliadas a octa como One password Beyond Trust y cloudfare semana nueva crímenes nuevos ergo episodio de tierra de hackers nuevo comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 6 de noviembre de 2023 es el episodio número 111 soy Martín vigo y está conmigo vivito coleando y cara a cara conmigo a miles de kilómetros alis porros Holis Hola aquí y quería decir algo Que supongo que muchos oyentes han han recibido que es lo siguiente feliz harlowe grupo Soy Vanessa Cómo no no Qué es un WhatsApp de esos que se va pasando to Halloween tío sí que acaba de pasar hace poco así que bueno venimos con un poquito el el tema así a mí no me llegó eh No es mítico yo lo levo recibiendo bastantes años atrás así que Bueno ya nos dirá algún oyente si sabe si tiene la remota idea de qué estás hablando bueno que espero que alguien lo haya pillado y si no mis disculpas y nada eh Para no enrollarme más eh Nada dec qué deciros pues que para estar al día de lo que sucede en el podcast nos podéis seguir en redes sociales y nos podéis Buscar como tierr deeh hackers o @ tierr deeh hackers para saber cuándo sale un nuevo episodio ding ding ding os podéis suscribir a tierra de hackers en cualquier plataforma de podcast y os abrimos las puertas de nuestro canal de discord donde podéis entrar vía tierradel comom brdc me ha encantado esa manera poética os abrimos las puertas de discord me encanta me encanta pues Espérate que viene más luego perfecto pues eh siempre tenemos que antes de empezar darle las gracias a nuestro mecenas de patreon cóm no Muchísimas gracias por haber ido a patreon.com bartier radeh hackers o tierrade hackers.com barp como no prefieras ir allí y decidir apoyarnos económicamente para poder pagar las facturas y que todo esto tenga sentido y sobre todo eh que nos dé la capacidad de poder hacerlo gratis para toda la audiencia muchísimas gracias y también a nuestros sponsors esenciales on branding em una empresa que está formada por especialistas en varios ámbitos profesionales que se enfoca en en la reputación online a múltiples niveles han ayudado desde personas como tú y como yo hasta a famosos a llevar por ejemplo a juicio casos de ciberacoso a mitigar situaciones donde la reputación de empresas pues está siendo mal intencionadamente dañada e incluso a borrar la huella digital que dejamos online no Solo han decidido Apoyar el podcast sino que si le contáis que venís de parte nuestra de tierra de hackers Vais a tener un descuento especial en sus servicios ya sabes si necesitas algún tipo de ayuda con vuestra identidad digital on branding es lo que estás buscando y puedes visitar su web en on brandings y también eh queremos hacer una pequeña pausa adicional para 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 inm monat a través de una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contraten en todo el mundo y en remoto así que ya sabéis echadle un vistazo a su web monat.com y mandad les vuestro currículum a tierra de hackers @mon comom mad.com perfecto pues comenzamos la noticia de hoy va sobre espionaje espionaje no sobre político o periodistas o disidentes que es lo que os solemos traer espionaje sobre investigadores que trabajan específicamente en el mundo de la ciberseguridad ya en el pasado si no recuerdo mal Alexis cubrió un par de veces como Corea del Norte intentaba engañar a investigadores a través de linkedin para infectar tenemos precedentes del interés de gobiernos agencias de inteligencia Y o entidades privadas por averiguar de lo que hablan los investigadores de ciberseguridad en qué están trabajando con quién se comunican etcétera y el objetivo en este caso no es diferente Lo que sí es diferente es el nivel de sofisticación del

ataque contra los investigadores y vale mucho la pena entrar el detalle el 1 de junio de este año eugin Kaspersky fundador de la empresa que lleva como nombre su apellido publica en su blog oficial la noticia de que acaban de descubrir un ataque contra empleados de su empresa y que infectaba dispositivos móviles de Apple en su día yo vi esta noticia ya digo hace cosa de dos meses y me la apunté para seguirla de cerca El problema es que Kaspersky ha ido desvelando detalles poco a poco y tres meses después ya tenemos cinco posts sobre este tema en la web de Kaspersky y sobre todo suficiente información tanto del incidente como como información técnica para que valga la pena traeros la al podcast como decía Kaspersky hacía el anuncio en su momento y decía que descubrieron este ataque porque empezaron a observar tráfico anómalo desde los dispositivos móviles de algunos de sus empleados hacia servidores externos que ellos consideraban sospechosos y nombraron a este incidente operation triangul el nombre se deriva del hecho de que el implante que ya os hablaré de eso más adelante utiliza técnicas de fingerprinting basadas en el Canvas y lo hace dibujando Pues un triángulo amarillo esto quiere decir que el malware Bueno intenta identificar de manera única el dispositivo intentando crear una especie de huella digital del del propio dispositivo basándose en las características de como este dispositivo pues procesa imágenes la renderiza etcétera las técnicas de Canvas fingerprinting son muy utilizadas en la web para rastrearte a través de páginas diferentes Y bueno pues mostrarte publicad publicidad específica a ti y a tu actividad online muchos navegadores de hecho hoy en día como firefox o brave contienen medidas antic Canvas fingerprinting en las que pues alteran las imágenes de manera que no se puede derivar un Hash una huella digital fiable en este primer anuncio Kaspersky no contaba mucho más que este detalle del tema del Canvas finger printing y tuvimos que esperar unos días para un nuevo post con algo más de detalle en el nuevo post se especifican más detalles de lo que se sabe hasta el momento la infección por ejemplo sucede a través del envío de adjuntos maliciosos a través de imessage muy curioso esto y algo que hemos visto pues en otros ámbitos como la infección del móvil de Jeff besos el fundador de Amazon que en ese caso fue mediante el envío de adjuntos maliciosos a través de WhatsApp utilizaron la herramienta Mobile verification toolkit para tener una idea del historial de eventos que sucede justo antes de que el dispositivo quede totalmente comprometido esto es muy interesante recordemos que los dispositivos de Apple son conocidos por ser un sistema muy cerrado y que dificulta muchísimo el análisis forense la ingeniería inversa Y bueno pues en general la investigación de de los que hacen análisis forense por tanto mediante esta herramienta observaron que lo primero que sucedía era que la víctima recibía un mensaje por imessage con un adjunto que contenía el exploit como mencionaba antes y el adjunto era ni nada nada más y nada menos que un Apple watch Face interesantísimo Si tú tienes un Apple watch o bueno o no lo tienes que sepas que tú en estos relojes puedes digamos decorarlos no con lo que ellos llaman los watch faces no diferentes diseños para mostrarte la hora y ahora eh Apple permite que third parties o desarrolladores implementen las suyas y se las puedan enviar pues parece ser que aquí encontraron una manera de crear una carátula del Apple watch maliciosa de tal manera que explota una vulnerabilidad que ya os voy a ir contando Bueno pues después de de recibir ese imessage con ese watch Face adjunto acto seguido y sin ningún tipo de interacción por parte de la víctima el mensaje fuerza la explotación de una vulnerabilidad que permite ejecución de código esto es importante queridos oyentes hablamos aquí ya de una vulnerabilidad de tipo cero clic el código del exploit contiene instrucciones que llevan a la descarga de las siguientes etapas del malware por lo que en este caso pues estamos hablando que del teléfono se infecta para instalar un dropper y la misión de este es descargarse el resto del programa malicioso las siguientes etapas del malware que se acaban de Descargar contienen otros exploits adicionales que explotan vulnerabilidades de tipo escalada de privilegios la típica cadena de explotación

esto es primero se infecta el teléfono de manera limitada mediante imessage y luego se descarga código adicional que explota otros fallos que llevan al control total del teléfono acto seguido y con privilegios ya de ejecución de código a nivel de kernel es decir con los permisos más elevados posibles se descarga el implante completo que permite controlar el dispositivo remotamente insisto primero se infecta el teléfono muy de manera muy limitada para conseguir ejecución de código remoto pero en el contexto de la aplicación de imessage luego se descarga código adicional para Elevar privilegios y salirse del sandbox de imessage y luego ya se descarga el implante con completo que permite ya cómodamente la el control no la ejecución de código sino el control del dispositivo remotamente este último eh paso no es para dificultar la tarea a los investigadores en el caso de análisis forense el último paso que se lleva a cabo que es que el implante Borra el mensaje inicial que contenía el dropper y el adjunto el watchface este malicioso para no dejar ningún rastro Una curiosidad es que con todo lo sofisticado que existe malware no tiene persistencia esto quiere decir que si la víctima Apaga el móvil el teléfono dejará de estar infectado cuando lo encienda esto habla de las fuertes medidas de seguridad que van implementando los fabricantes de dispositivos móviles tanto Android como como iOS o sea tanto Google como Apple y esto la verdad es que dificulta muchísimo los hackeos a este tipo de dispositivos per hay que tener en cuenta que aunque no se tenga persistencia si se tiene infección mediante cero clic pues entonces si el dispositivo infectado deja de comunicarse con los servidores de los atacantes Porque alguien lo ha reiniciado pues lo vuelven a infectar mediante otro mensaje de I message malicioso y listo porque no tienes que esperar a que la víctima le dé clic a un link o algo así de hecho insisto esto es precisamente lo que sucedía según Kaspersky descubrieron que esta campaña está de hecho activa desde 2019 y efectivamente hay muchísimos dispositivos que han sido infectados y reinfectados múltiples veces dada la falta de persistencia en cuanto a los dominios utilizados por los atacantes a los que por supuesto el móvil no se conectaba para recibir instrucciones pues tenemos varios Pintos backup rabbit.com topography updates.com virtual.com webtrack pers.com business videon news.com Bueno lo típico vemos dominios que lo que intentan es que si alguien pues echase así un vistazo rápido pues no llame demasiado la atención que no sea un dominio eh hacke automovil.com básicamente en el siguiente post de Kaspersky publicado unos días después Kaspersky publicó una herramienta para que la gente pudiera identificar si sus dispositivos móviles habían sido infectados con este malware y se llama Triangle check y es un Script que corre sobre un backup del iPhone insisto uno no puede instalar fácilmente o hacer Side loading de aplicaciones en el móvil y no la pueden meter aplicaciones así en la app store Entonces esto lo que hace es que te pide que tú hagas un backup con iTunes o lo que sea de tu dispositivo iPhone y sobre ese backup corres este Script y este Script lo que hace es buscar la presencia de ciertos archivos que este malware deposita en el sistema de archivos el resultado del Script de hecho es muy sencillo te pone detected no traces of compromise were identified o suspicious es decir sabes seguro que has estado infectado sab seguro que no estás infectado o ha encontrado trazas pero no es determinante 100% de que hayas sido infectado bueno esperamos unos días y volvieron a sacar otro post Y en este menu a los detalles del implante y el proceso para obtenerlo recordemos que este malware una de las cosas que hace es autodestruirse bueno parte de la cadena de infección se autodestruye no esto dificulta mucho el análisis forense y obtener muestras de malware para ser analizado en detalle para masry lo que hace el implante completo en sí que se instala una vez se obtiene ejecución de código a nivel de kernel explotando la vulnerabilidad en imessage y las de elevación de privilegios Es que reside solo en memoria esto insisto dificulta aún más el análisis porque en memoria pues insisto es volátil no Entonces se pierde todo rastro si se apaga el teléfono de hecho se dieron cuenta de que si el teléfono no se apaga o se reinicia en un

periodo de 30 días el implante se desinstala Así mismo automáticamente a no ser de que los atacantes extiendan esta fecha esta medida una una vez más es para evitar que un análisis forense lo descubra en caso de que por ejemplo se pierda acceso al dispositivo si alguien no lo analiza en en 30 días en ese caso pues desde Bueno digo desde que se perdió la conexión Pues el analista forense no va a encontrar nada porque estaba todo en memoria os dejo como siempre los post de Kaspersky con más detalles técnicos que no voy a cubrir aquí pero sí quería también destacar el hecho de que el implante no solo se conecta con servidor sino que también tiene un segundo servidor almacenado como Plan B digamos en caso de que el primero haya caído o le hayan hecho sinall unos investigadores lo de sall es que básicamente no permitan cambian los dns o así para que el dispositivo móvil no consiga conectarse y se conecta los servidores del de los investigadores Y entonces pores lo que hace es cambiar a ese segundo servidor y esto lo saben porque el implante periódicamente lo que hace es conectar al servidor de los atacantes enviando información básica como el email el número de serie El identificador de la tarjeta SIM bueno información del sistema operativo y otros detalles básicos para identificar el dispositivo y esto lo va mandando no dicen Cada cuánto pero me imagino pues cada 5 minutos o así no para saber que vale todavía tengo control de este dispositivo móvil en cuanto a las capacidades del implante pues ya os podéis imaginar con sobre el sistema de archivos bueno es decir crear borrar modificar cualquier archivo en el dispositivo gestión de procesos por si hay alguna aplicación corriendo que no quieres que se esté ejecutando pues matas el proceso robo del keychain Esto sí es importante porque es donde se almacenan todas las contraseñas en en tu iPhone monitorización de la geolocalización del dispositivo lo típico trace a la persona la víctima donde se mueve físicamente y ejecución de nuevos binarios que pueden ser añadidos mediante el implante es decir si quieres eh tú como atacante pues Añadir una nueva funcionalidad pues te lo escribes en un macho que es digamos el sistema de de binarios que utilizan los dispositivos de Apple y lo subes y lo puedes ejecutar Bueno hasta aquí el tercer post de Kaspersky sobre operation Triangle para luego esperar unas semanas y sacar el cuarto donde siguen dando más detalles como por ejemplo la detección mediante ciertos eh validadores de si el dispositivo a infectar se trata de un móvil dedicado a la investigación Esto me sorprendió mucho empieza así el este este post que que salió Hace unos días esto de detectar si si es un móvil dedicado a la investigación es evidentemente para no infectarlo si ese es el caso y evitar que el investigador analice el malware vamos que han implementado muchísimas medidas para pasar desapercibidos porque ya sabemos que Apple pues una de las cosas que hizo es poner a disposición de investigadores muy top iphones que vienen ya digamos con el jailbreak Por así decirlo y que te permite pues analizar más a fondo y poder hacer tus investigaciones además de bueno de todo lo que ya os he contado Borra todos los logs del móvil y algo interesante es que para borrar el mensaje malicioso con el adjunto malicioso que os comentaba antes lo busca en la base de datos eh de los mensajes porque tiene que encontrarlo ahí y cómo lo encuentra pues buscando mensajes enviados desde una lista de emails específicos HM recordemos que imessage soporta enviar mensajes desde tu cuenta de iCloud que está asociada a un email no tienes por qué mandar Im message desde tu número de teléfono digamos y eso es lo que han hecho los atacantes evidentemente porque es más sencillo crear emails que que obtener tarjeta SIM kasperski encontró la lista de cuentas de iCloud desde las que llegan los mensajes maliciosos y ayudó mucho a su investigación algunos de los remitentes más que nada por si os ha llegado algún mensaje desde ellos pues es Daniel hbn 2@gmail.com mib barham @outlook.com Stefan marínez 122 @gmail.com conamar 91@gmail.com que tienes porque ya sabemos que aunque WhatsApp esté descifrado extremo a extremo Por cierto igual que ha message Claro en tu dispositivo está descifrado si no no lo podrías ver y entonces lo roban ahí una de las capacidades que me llamó la atención pues la

extracción de metadatos de las fotos que tienes en tu móvil Pero es que específicamente chequean si por ejemplo hay un niño en la foto o si en la foto sale una mujer o también hacen la extracción de texto que pueda salir en una foto por ejemplo si sacas no sé una foto a un libro y eso lo hacen pues mediante técnicas de ocr No a mí la verdad esto de detectar si hay niños mujeres detexto y tal a mí me huele a luego poder extorsionar a la víctima no con esta capacidad hasta aquí la noticia queridos oyentes como os decía tenéis todos los posts de Kaspersky en las notas del episodio por si queréis meteros a fondo en los detalles técnicos Pero bueno yo creo que cubierto lo más importante y hasta aquí mi noticia Qué te parece Alexis muy muy interesante sobre todo por el tema de qué sorpresa muy interesante Sí no siempre lo digo parezco muy repetitivo pero tengo que expandir mi vocabulario hombre me va a preocupar el día que el día que me diga Pues sabes qué fue una mierda malo í malo también también no interesante bueno primero quería decir que e en en junio eh Ya hubo indicios de esta noticia y de hecho la trajimos al al podcast en el episodio 99 lo que creo que quedó un poco eh escondida en la noticia en Sí porque de hecho la traje yo y y hablé más bien de una nota de prensa de de la llamada esta de concienciación de los miembros del parlamento europeo que querían que se hicieran más investigaciones y salvaguardas contra software espía y prevenir su abuso como el caso eh archiconocido de pegasus y similares pero en ese caso en ese episodio en el 99 que os invito a escuchar también para enlazarlo con la noticia de Martín que acaba de comentar eh acabé comentando el el tema de Triangle db que que justo salía surgía en ese momento Así que muy muy interesante este follow up a mí lo que me ha encantado eh No no ha encantado lo que me ha dejado un poco alucinado es es que el Delivery la entrega del exploit fue a través de un Apple watch Face Que supongo que es algo que si tienes un Apple watch dices Oh mira un colega me está enviando un Apple watch de Snoopy o algo así como me gusta Snoopy pues me la voy a instalar y tal eh eso fue algo que me ha dejado algo interesante pero eh que en este caso recuerda no te la tenías ni que instalar con recibirla ya estaba justo y entiendo que además de eso no ha de falta que tengas una Apple watch Así que o sea es es es interesante y el tema que has dicho de triangulación ahora también ese misticismo que que había alrededor de Triangle db era por qué Porque triangulación de de del sabes de de normalmente en en ubicación y localización se utilizan tres no puntos para saber dónde estás pero en este caso era lo que has dicho del fingerprinting eh que que es también interesante originales estos de Kaspersky nombrando sí recordemos que ellos son los que le pusieron el nombre careto a un malware teóricamente hecho en España que es a lo mejor todos nuestros oyentes de de latinoamérica no no conocen esa palabra pero careto es una palabra muy española como el careto que tienes cuando te levantas por la mañana ese careto que se te queda de cartón ahí y y de marcas en la cara de las sábanas y bueno y de la almohada eh para que la gente vea un poquito en su mente y lo último que quería comentar también que me ha gustado es que Kaspersky ha ha mencionado cómo pudo hacerse con una copia de ex exploit que parece que que tiene tiene su qu que era algo complicado no pero es bueno que hayan compartido la metodología cómo lo hicieron sobre todo el tema ese saltarse el certificate pinning y el javascript adicional que metieron Esto me parece interesante para que otros investigadores de seguridad o analistas forenses pues puedan ir también y utilizar técnicas similares para obtener realmente otros exploit similares que van a ver ya os lo digo queridos oyentes En el futuro porque esto no se queda aquí has dado en el clavo eh yo me guardé esto aparte de cuando bueno por la semana voy Buscando noticias y me las guardo para el podcast esta me las guardé también en mi sección de hacking de móviles porque ahí hay unos tips en Tri tricks de lujo la verdad que vale mucho la pena y desde luego como siempre ahí está el valor de que os dejemos en las notas del episodio pues todas las referencias de de donde sacamos toda la información que os traemos semana a

semana si hacéis forense si hacéis research Si buscáis exploits o si en general queréis aprender algo más técnico leeros sobre todo el El quinto post que es donde explican todo lo que intentaron y todo lo que tuvieron que hacer para llegar a a conseguir no el exploit y descifrarlo muy buena Martín y nada damos paso a la siguiente noticia Y qué os traigo queridos oyentes pues una historia de terror que involucra a octa y dice así erase una vez un lunes pero no un lunes cualquiera sino ese tipo de lunes en el que sientes escalofríos al despertarte solo por pensar en todo el trabajo que te espera en la oficina en la penumbra del atardecer de ese lunes terrorífico Antonio un laborioso administrador de la empresa beyon Trust estaba trabajando en sus tareas cotidianas sin embargo ese mismo día el destino tenía escrita una trama distinta para los anales del ciberespacio como guardián de la cuenta de billon Trust en octa su misión era proteger las puertas digitales y asegurar que solo las almas autenticadas y autorizadas cruzaran los umbrales de la información poco antes de acabar su jornada laboral un problema insólito en la plataforma de octa emergió de las Sombras digitales un fallo que no seguía ningún patrón conocido sin dudar ni un minuto Antonio con un aura de inquietud flotando sobre él se comunicó con los custodios de octa en busca de una resolución un agente de soporte de octa con voz monótona y de ultratumba le instruyó a generar un archivo har harar desde su navegador y subirlo al portal de soporte de octa era un procedimiento estándar un paso necesario hacia la resolución pero lo que Antonio ignoraba era que el archivo har ese cofre comprimido de peticiones http y claves de autenticación era también un pasaje hacia lo desconocido un pequeño pandemonium digital que una vez abierto podría desatar una tormenta de sombras y secretos en el santuario Cibernético que juró proteger con un clic el archivo se elevó a través de las señales digitales hacia el portal de soporte de octa y al mismo tiempo las puertas hacia un dominio oscuro y sin explorar se entre abrieron listas para arrastrar Antonio hacia las profundidades de un Thriller Cibernético que pondría a prueba los límites de su realidad Bueno hasta aquí llega la narrativa terrorífica Espero que os haya gustado es por darle un toque diferente Pero ahora no os preocupéis que ya sigo como normalmente hacemos y entro en más detalle en la noticia Porque si sigo con tanta bruma Y misticismo pues igual me tiro 3 horas en explicar algo que me llevaría 30 minutos okay seguimos con la noticia pero primero para dar un poco de contexto sobre la empresa octa quiero definir realmente Qué es pues como digo es una empresa que proporciona una plataforma de gestión de identidades y acceso en la nube que ofrece servicios como la autenticación de usuarios la gestión de identidades el acceso único o single Sign on la gestión de accesos ados y la gestión de apis entre otras es la segunda vez de hecho que traemos un incidente de seguridad que involucra a octa la primera vez fue en el episodio 50 en el que os comentamos como el grupo de ransomware lapsus comprometió a octa y afectó alguno de los clientes de octa por si lo queréis refrescar en vuestra memoria pues podéis ir a escuchar el episodio 50 en cualquier caso volviendo a los acontecimientos os sigo explicando Pues dentro de los 30 minutos siguientes a las subida del archivo har har acrónimo de http archive que es un archivo comprimido que contiene archivos json de cada una de las sesiones http del navegador del que se exporta Total como digo dentro de los 30 minutos siguientes a la subida de este archivo har un Bandido Cibernético intentó acceder a la consola de administración de beon Trust en octa desde una dirección IP de Malasia vinculada a servicios Anónimos de Proxy o VPN a pesar de que se registraron eventos de octa desde esta ip de Malasia no hubo eventos de autenticación como normalmente se esperaría qué Misterio cómo es posible bueno seguid escuchando queridos oyentes y os Lo aclaro el atacante se autenticó e intentó acceder a la consola de administración de Beyond Trust en octa pero se le denegó el acceso punto a favor de beon Trust Bueno a favor de octa en contra del cibercriminal el acceso a la consola de administración de billon Trust en octa estaba configurado de tal forma que solo era posible acceder a ella Desde un sistema

administrado por beyon Trust en el que además está instalada la aplicación octa verify que sirve para la autenticación de doble factor de octa debido a que el atacante no disponía de estos requisitos se quedó sin poder acceder a la consola de administración pero no se quedó satisfecho y siguió haciendo de las suyas acto seguido el atacante consiguió generar de forma exitosa un informe del estado de las cuentas y contraseñas de usuarios de billon Trust en octa utilizando la Api de la consola de administración de octa Esto fue posible porque no se aplican las mismas medidas de seguridad en el uso de apis como en el uso de funcionalidades a través de la aplicación web como puede ser el pedir el token de autenticación de doble factor inmediatamente el atac an intentó obtener acceso al panel principal de octa pero recibió un desafío de autenticación de doble factor debido de nuevo a que el atacante no disponía de esta información no pudo conseguir este objetivo otro punto para octa o billon Trust después el atacante utilizó la Api de octa para crear una cuenta de servicio o service account obviamente falsa llamada svc Network backup eligiendo este nombre para que la cuenta se pareciera a otras cuentas de servicio existentes y pasara desapercibida lo que no sabía el atacante es que al crear el informe de contraseñas el sistema envió un email a los administradores de beon Trust quienes supieron de esta forma del ataque que se estaba llevando a cabo después de recibir dicho email los administradores de Bon Trust inhabilitaron la sesión utilizada por el atacante y la cuenta de servicio que este había creado beon Trust inició un proceso de respuesta a incidentes llevando a cabo un análisis forense aisló los sistemas y las cuentas asociadas con el administrador que estaba afectado es decir el usuario asociado con esa sesión que el cibercriminal había secuestrado y había utilizado para acceder a a los servicios de octa la investigación del Análisis forense no encontró ningún otro indicio de compromiso distinto al que acabo de comentar hasta ahora pero sí descubrió el archivo hard que mencionado que se había generado para el caso de soporte en el sistema del administrador lo encontraron en el portátil eh de este usuario este empleado de beyon Trust concluyeron que el atacante robó Las Cookies de sesión Dentro de este archivo har y las utilizó para autenticarse en octa esta forma de autenticación digámoslo entre comillas no deja logs por defecto ya que la sesión del atacante utiliza una sesión ya autenticada y obviamente eh el que se ha autenticado previamente con credenciales es el usuario es la persona que asociada con esta sesión Y he aquí eh Cómo se desvela el misterio de la falta de logs que mencioné anteriormente en el uso de esta sesión por parte del cibercriminal como digo como no hay autenticación en Sí no hay introducción de nombre de usuario contraseña y doble factor de autenticación pues no se ha creado no se han creado esos eventos esos logs simplemente el cibercriminal puso esa Cuqui de sesión en su navegador la inyectó digamos de alguna forma y pudo acceder a los servicios de octa suplantando a este usuario este empleado de billon Trust pero continuemos billon Trust siguió su investigación y el día siguiente el 3 de octubre descartaron la posibilidad de que el compromiso se originara en un sistema de billon Trust porque pensaban que uhu hemos encontrado este archivo hard en el sistema en el portátil de este empleado de de billon Trust puede ser que hayan comprometido el sistema de esta persona eh Así que bueno e vamos a seguir investigando a ver si hay algún malware escondido persistente o de alguna forma que todavía tiene capacidades o que las tuvo para robar este archivo hard pero como digo no encontraron ningún otro indicio de de este tipo de actividad así que todo les llevó a concluir y a pensar que el sistema de soporte de octa era el que probablemente estuviera comprometido Beyond Trust escaló esta conclusión esta preocupación al equipo de soporte de octa pero octa no comunicó ningún compromiso conocido o incidente de seguridad en curso billon Trust demostró su persistencia y su preocupación y siguió escalando este tema a octa en varias ocasiones tanto el 11 como el 13 de octubre y Estos son 9 y 11 días después del incidente inicial respectivamente en todas estas ocasiones octa seguía negando compromiso alguno

conocido o incidente de seguridad en curso no fue hasta el 19 de octubre 17 días después del incidente inicial contra billon Trust que octa notificó a bon Trust de que sí Oye hubo un compromiso en octa y tú Beyond Trust eres uno de los clientes afectados Durante este incidente octa anunció este incidente de seguridad el 20 de octubre de forma pública 18 días después del incidente inicial contra billon Trust como era de esperar no fue solo billon Trust el único cliente de octa afectado por este compromiso sino que otras empresas como cloudfare y One password también fueron afectadas el miércoles 18 de octubre cloudfare descubrió ataques en sus sistemas que pudieron rastrear hasta octa detectaron esa actividad internamente más de 24 horas antes de que octa les notificara finalmente llegaron a la misma conus que vi Trust el cibercriminal comprometió dos cuentas separadas de empleados de cloudfare robando Y utilizando un token de autenticación de una sesión abierta de octa de cada una de estas dos cuentas que interesantemente tenían privilegios administrativos y de esta forma podían acceder a la instancia de octa de cloudfare de esta forma el cibercriminal accedió al sistema de atención al cliente de octa y obtuvo los archivos subidos por clientes de octa como parte de casos de soportes recientes y si habéis estado siguiendo la noticia queridos oyentes os hago una pregunta cuáles son esos archivos os dejo unos segundos para pensar Cuáles son estos archivos pues efectivamente habéis dado en el clavo son los archivos hard que he comentado al principio cloudfare verificó que este evento no afectó a la información ni a los sistemas de sus clientes ya que pudieron contenerlo antes de que el atacante pudiera obtener acceso a los datos de cliente Okay ya vemos que btrust cloudfare ahora sigo con One password que es uno un tanto interesante porque como todos sabéis One password es una empresa que ofrece un servicio de gestión de contraseñas eh Y bueno Esto es preocupante no que pudiera estar comprometido en un incidente de seguridad porque si lo utilizamos eh todas nuestras contraseñas podrían estar en peligro pero ahora os cuento si ese fue el estamos ante el paciente cero de esta historia porque One password el 29 de septiembre días antes del compromiso de Bon Trust detectó actividad sospechosa en su instancia de octa lo que ocurrió es que ese mismo un miembro del equipo de administradores de One password recibió una notificación inesperada por coro electrónico Y de nuevo queridos oyentes si estáis siguiendo la noticia de qué crees que se trataba este correo electrónico os doy unos segunditos pues este correo electrónico se trataba de efectivamente la creación del informe de cuentas y de contraseñas de octa y como en los otros casos One password se dio cuenta de que obviamente no había iniciado la creación de dicho informe y alertó a su equipo de respuesta a incidentes algo le solía mal las investigaciones preliminares revelaron que la actividad en su entorno de octa procedía de una dirección IP sospechosa y luego confirmaron que un usuario no autorizado había accedido a su instancia de octa con privilegios administrativos la actividad indicaba un reconocimiento inicial con la intención de recopilar información preparándose para un ataque más sofisticado Además del informe de usuarios y contraseñas el cibercriminal hizo lo siguiente intentó Acceder al panel de octa del empleado de One password que había creado el archivo hard pero octa lo bloqueó y luego también habilitó el idp o identity Provider de Google vinculado a su entorno de producción que estaba desactivado habilitar el idp o proveedor de identidad en este caso de Google se refiere a que el cibercriminal configuró Google de tal forma que le hubiera permitido acceder a la cuenta de octa a través de la funcionalidad de hacer login con Google o Sign In with Google con cualquier cuenta de Google que el cibercriminal tuviera esto era una gran puerta trasera que estaba intentando se sabe que el cibercriminal también realizó otras acciones menos sensibles como ver grupos pero no resultaron en entradas de registro en en logs que se quedaron en el sistema como os imaginaréis una vez más el compromiso vino debido a que durante una sesión de soporte octa le pidió a un empleado de One password que creara un archivo har y que lo subiera al portal de

soporte de octa Esto ocurrió un viernes pero aún y así One password respondió rápidamente y durante el fin de semana manana realizó una serie de cambios de seguridad en la configuración de octa para prevenir estos ataques en un futuro Pero bueno seguimos adelante porque aquí no acabó el tema se cuenta que tres días más tarde el 2 de noviembre el mismo día de la actividad inicial maliciosa contra la instancia de billon Trust en octa el cibercriminal volvió e intentó acceder a la instancia de One password de octa utilizando el identity Provider de Google que había habilitado Pero esto falló obviamente porque One password había eliminado este identity Provider un par de días antes durante el fin de semana Así que esto fue un gran Win para One password que eliminó rápidamente esta puerta trasera que el cibercriminal había dejado para actividades eh futuras One password confirmó que el cibercriminal No accedió ni ex filtró datos de clientes o empleados así que ya sabéis queridos oyentes podéis estar tranquilos que todas vuestras contraseñas en one password están seguras bueno y ahora finalmente vamos a hablar del protagonista de la historia y quién es pues obviamente Ni más ni menos ya sabéis Qué es octa el 20 de octubre octa emitió un comunicado público en el que indicaban que habían identificado actividad maliciosa de un cibercriminal que pudo Acceder al sistema de gestión de casos de soporte de octa gracias a credenciales robadas aunque no indican Cómo se comprometieron estas credenciales probablemente fuera vía ingeniería social el comunicado decía que el cibercriminal pudo ver archivos subidos al portal de soporte por ciertos clientes de octa como parte de casos de soporte recientes mencionaban en el comunicado que como parte de operaciones normales de su negocio el soporte de octa puede pedir a sus clientes que carguen archivos http archive el archivo hard que he mencionado más de una vez que ayudan a solucionar problemas replicando la actividad del navegador web también mencionaban que son conscientes de que los archivos hard también pueden contener datos confidenciales incluidas cookies y tokens de sesión y que los actores malintencionados pueden utilizar estos datos para robar y aprovechar sesiones válidas luego comentan algo que me parece muy interesante que en general octa recomienda sanitizar todas las credenciales cookies y tokens de sesión dentro de un archivo hard antes de compartirlo Okay esta recomendación es genial y es lo que se debería ha implementado desde un principio pero ya vemos que esto no ha ocurrido De todas formas este comunicado vino eh Como un gran alivio para aquellas organizaciones que detectaron actividad maliciosa en sus cuentas de octa ya que estas declaraciones aclaraban que fue gracias a un compromiso de una cuenta de un agente de soporte de octa que los cibercriminales pudieron acceder a las cuentas de octa de estas organizaciones a través de robar los archivos hard y de ahí utilizar las sesiones los tokens de sesión de sesiones todavía activas y que no se debía a compromisos de sistemas o cuentas de las organizaciones directamente Aunque bueno el efecto al fin y al cabo es el mismo pero bueno al menos sabían estas organizaciones que Oye no investigamos no no pongamos más esfuerzo en análisis forense en nuestros sistemas porque el compromiso no viene de ahí compromiso viene de que de alguna forma han robado las credenciales de un agente de soporte de octa y de ahí han accedido al portal de soporte se han descargado los archivos hard de muchas empresas incluyendo Beyond Trust One password y cloudfare y han extraído las sesiones todavía activas las han utilizado y han suplantado desgraciadamente a más de una empresa voy a comentar algunas medidas de prevención que se podrían implementar la primera es que ya se ha implementado por el cliente o por octa directamente debería haber un proceso de sanitización de datos confidenciales de los archivos har y que se borre todo material de autenticación como cookies o claves de sesión Al compartirse este tipo de archivos tal y como lo dice octa en su comunicado público así debería hacerse y octa son los primeros que deberían comerse como se dice en inglés no comer su propia comida de perro el eat your own dog Food lo segundo sería activar la autenticación de doble factor basada en Fido 2 Como

por ejemplo usando octa verify Google authenticator alguna aplicación y nunca utilizar la autenticación de doble factor basada en mensaje de texto a móvil ya que es vulnerable a ataques de SIM swapping que hemos visto más de una vez sobre todo en temas de criptomonedas pero e cibercriminales podrían obtener estos códigos suplantando la identidad del usuario Llamando al proveedor de conexión móvil y pidiendo que se le envíe una copia de la tarjeta SIM de la víctima lo otro es limitar la duración de la las sesiones de usuarios administradores es decir invalidar Las Cookies de sesión después de un periodo predefinido otra medida es configurar el acceso a la consola de administración para que requiera el uso de sistemas administrados por la propia organización y que tengan instalado octa verify por temas de doble factor de autenticación y otra medida podría ser configurar el acceso a funcionalidades críticas en el panel principal para que pidan autenticación de doble factor aunque esto cause cierta fricción con el usuario estas medidas se aplican en principio a la plataforma de octa pero también se pueden extrapolar a otros cualquier sistema tecnológico que se quiera securizar y comento algunas medidas de detección como digo más enfocadas en octa pero también se pueden extrapolar a cualquier otro tipo de sistema informático la primera sería detectar secuestros de sesión de octa El atacante lo que hizo fue robar las cookies de sesión de octa del archivo har subido al portal de soporte de octa y las utilizó para acceder a octa desde su propia infraestructura la detección debería Buscar sesiones sospechosas sin un evento de autenticación asociado como digo al utilizar una Cookie de sesión que está activa no se generan estos eventos de autenticación cuando se introducen nombre de usuario contraseña y o idealmente el doble factor detectar acciones administrativas utilizando un Proxy este ataque y muchos otros a menudo utilizan proxis o nodos de VPN para iniciar sesiones como usuarios sobre todo privilegiados y realizar acciones administrativas algo que los usuarios legítimos rara vez hacen a no ser que siempre hay casos extremos en los que Eh hay algunas organizaciones que necesitan hacer uso de la privacidad y Por ende tienen que utilizar vpns de forma forzada cuando están en países autoritarios Pues en este caso habría que un poco ajustar este caso de detección pero esa es la idea El otro es detectar creaciones de informes de estado de cuentas y contraseñas de octa este informe rara vez se genera según se Comenta por octa y por las organizaciones afectadas de este incidente Así que es un evento que puede tomarse como indicador de actividad sospechosa de alta fiabilidad otras detecciones a implementar sería eventos de gestión de usuarios como la creación de nuevos usuarios en este caso en Beyond Trust en este incidente el cibercriminal creó una nueva cuenta de io que se parecía a las que ya existían para pasar desapercibido así que debería crearse una alerta cuando se da un evento similar también deberían crearse alertas cuando se reactivan cuentas de usuarios desactivados o la modificación de la forma de autenticación de doble factor de cuentas es decir si se tiene puesto como utilizando octa verify y luego se cambia a SMS pues Oye aquí algo huele mal también porque probablemente Esto indica que el cibercriminal podido hacer ataque SIM swapping a la víctima en concreto y está intentando autenticarse utilizando el la tarjeta SIM que que ahora está en su poder también relacionado con esto no pues eh cuando se modifican estas políticas de autenticación de doble factor como deshabilitarlas completamente y finalmente también se podría detectar modificaciones a los identity providers esas plataformas que permiten el acceso a octa a través de empresas terceras Como pudiera ser Google Apple o Facebook o similares como dicho por ejemplo en este caso recordemos que el cibercriminal activó el identity Provider de Google que estaba desactivado y que lo hizo de tal forma que pudiera tener una puerta trasera para acceder a la instancia de One password en octa solo contener una cuenta válida en Google así que hasta aquí ha llegado la noticia queridos oyentes pero cierro con algunos comentarios el primero es que tanto profesionales de las te tecnologías de la información como menores son culpables de

compartir archivos hard sin saber que estos contienen información confidencial que puede ser utilizada para robar sesiones y autenticarse sin credenciales lo de los menores lo digo porque en episodios anteriores como en el 47 si queréis refrescar la memoria podéis ir a escucharlo en ese episodio comentamos que cibercriminales ofrecían sus servicios para mejorar O Añadir objetos de valor a las cuentas de roblox de menores de edad si estos usuarios compartían archivos hard con los cibercriminales pero lo que acababa sucediendo es que al obtener estos archivos hard al igual que en este incidente de octa los cibercriminales podían acceder a las cuentas de los menores y al final le robaban todos los objetos del mundo roblox Así que si una lección nos tiene que quedar Clara de esta historia terrorífica de hoy es que hay que tener mucho cuidado con los archivos que compartimos Especialmente los archivos har http archive o cualquier tipo de archivo que sea técnico por motivos de confidencialidad y de los datos sensibles que contienen no sea que os roben las sesiones y vuestros objetos de roblox o mucho peor vuestras criptomonedas o activos financieros Así que mucho cuidado pues ha llegado a su fin este episodio queridos oyentes ya estamos en noviembre Casi casi acaba el año pero nosotros seguimos esto Esto no para Gracias por quedaros hasta el final recordad que nos podéis apoyar en patreon.com bartierra deckers y si no podéis hacerlo de manera económica pues hacerlo repartiendo sabiduría hacerlo repartiendo información sobre cómo pueden hacer vuestros amigos y compañeros para encontrar este podcast que puede ser buscándolo en cualquier plataforma de podcasting mismo en Google o le dices Oye Vete a tierr hackers.com que tienes toda la información ahí vas a aprender un montón vas a estar más ciber protegido si empiezas a escuchar este podcast lo dicho lo que dice Martín acabamos este episodio terrorífico que acabamos de pasar Halloween y y esta esta temporada de de que la gente se vuelve más fantasmagórica igual que nuestras noticias y nada eh un placer haberos tenido o en otro episodio adicional de tierra de hackers y nos vemos en la siguiente historia de terror digo en el siguiente episodio Adiós adiós si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers G