el grupo apete chino storm0558 abusa de un fallo de validación de tokens falsificados contra Outlook web Access y outlook.com para acceder a correos electrónicos y llevar a cabo campañas de espionaje contra docenas de empresas gubernamentales en todo el mundo seguimos veraneando juntos con otro episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 18 de agosto de 2023 es el episodio número 103 yo soy Martín vigo y está conmigo de nuevo postres sacó en Las Vegas a Alexis porros Hola Alexis qué tal pues muy buenas Martín un gusto de estar de vuelta contigo y con todos nuestros oyentes esta semana justo he estado en la blackjad y la Def con en Las Vegas y genial muy buena experiencia Como cada año ya sabes Aunque la vez con cada vez se masifica más pero muy buenas charlas actividades en las vilaches muy interesantes y concursos la verdad que son dignos de ver igual traemos alguna noticia al respecto en un episodio en el futuro Así que está atentos pero no me enrollo más sigo adelante comentar que como sabéis estamos en todas las redes sociales más populares en las que nos podéis encontrar como tierra de hackers o arroba tierra de hackers también en las mayores plataformas de podcast como tierra de hackers donde debería estar suscritos y si no lo estáis ahora mismo por favor ID a suscribiros eso nos ayuda mucho y os invitamos a formar parte de nuestra comunidad de discord uniendo a través de tierra de hackers.com barra discord perfecto Pues yo como siempre darle las gracias a nuestros mecenas de patreon Gracias por seguir apoyándonos día a día y además tenemos un nuevo sponsor para este episodio Muchísimas gracias a You are safe una app móvil para iOS y Android desarrollada por 480 compañías especializada en soluciones Cloud y de ciberseguridad y te preguntarás Qué hace You are safe incluye una VPN móvil de Última Generación con la que puedes conectarte a WiFi públicas y acceder a contenido geobloqueado de forma segura y sin perder velocidad ni batería tu conexión estará 100% cifrada y tus datos a salvo además también puedes hacer un chequeo a tu móvil para detectar cualquier tipo de malware o configuraciones inseguras Así que ya sabes este verano protege tu dispositivo y navega con total tranquilidad estés donde estés la app es gratuita y para hacer uso de la VPN puedes contratar diferentes planes de precio con el cupón tierra de hacker todo junto podrás utilizar la versión para Android de forma gratuita durante 15 días seleccionando la suscripción anual y si no te convence lo cancelas antes del periodo de pruebas y no pagas nada así que ya sabes prueba gratuitamente You are safe con el cupón tierra de hackers y te dejamos los enlaces en las notas del episodio 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 echarle un vistazo a su web monat.com y mandarles vuestro currículum a tierra de hackers arroba monat.com m o n de puntocom pues ya listos para empezar esta vez me toca a mí tomarme una semanita de descanso Así que os dejo con Alexis que os trae Yo diría que la noticia del momento y que algunos incluso por discord por ejemplo nos habéis pedido que la cubramos Así que Alexis adelante y nos vemos y nos escuchamos para la siguiente semana Pues traigo una noticia de espionaje Estados Unidos y China vamos lo típico no Microsoft reveló recientemente que ha contrarrestado un ataque Cibernético dirigido a dos docenas de organizaciones algunas de las cuales incluyen agencias gubernamentales estadounidenses en una campaña de espionaje diseñada para adquirir datos confidenciales según la investigación este ataque fue lanzado por el grupo de amenazas Storm 0558 asociado con el estado chino los objetivos principales de este grupo tradicionalmente según se ha visto desde que están en activo A mediados de 2021 incluyen los órganos de

gobierno diplomáticos económicos y legislativos de Estados Unidos y Europa y las personas conectadas con los intereses geopolíticos de Taiwán y el grupo huigür si esa minoría ese grupo minoritario del que hemos hablado anteriormente en tierra de hackers que vive en China y que es oprimido de manera muy forzada y obvia por por el gobierno chino no así también como las empresas de medios los grupos de expertos y los proveedores de servicios y equipos de telecomunicaciones todas estas empresas son objetivos de este grupo apt chino de espionaje storm0558 como digo desde que está en activo A mediados de agosto de 2021 este grupo de amenazas lo que ha estado haciendo es recolectar credenciales campañas de phishing y ataque de tokens o aos dirigidos a cuentas de Microsoft para lograr sus objetivos de espionaje parece que les gusta mucho Microsoft y se sobre todo en obtener información de sus víctimas a través de esta plataforma online el acceso inicial a las redes objetivo lo llevan a cabo a través de la suplantación de identidad y la explotación de fallas de seguridad en aplicaciones públicas es decir aplicaciones web normalmente expuestas en internet lo que lleva al despliegue de webs la web esta típica que se llama china Chopper como acceso de puerta trasera y también despliegan y utilizan herramientas malware que ellos mismos han desarrollado Storm 0558 también emplea comandos de Powers y python para extraer datos de correo electrónico como archivo adjuntos información de carpetas y conversaciones completas mediante llamadas a la Api de Outlook web Access a través de bueno de llamadas http los ataques que comenzaron el 15 de mayo de este año implicaron el acceso a cuentas de correo electrónico que afectaron aproximadamente 25 y una pequeña cantidad de cuentas de consumidores individuales es decir como tú y como yo querido oyente la divulgación se produce más de un mes después de que Microsoft expusiera los ataques contra infraestructura crítica lanzados por un colectivo adversario chino llamado bolt taefón También conocido como Bronx siluette o vanguard Panda dirigido a Estados Unidos Bueno y cómo se llevó a cabo este ataque en concreto el acceso no autorizado a las cuentas de correo electrónico en exchange online se realizó a través de Outlook web Access y también accedieron a outlook.com falsificando tokens de autenticación creados con una clave de firma digital de msa msa es el acrónimo de Microsoft service account anteriormente conocido como Microsoft passport.net passport e incluso Windows Live ID y es una cuenta de de Microsoft de inicio de sesión único para que los clientes de Microsoft inicien sesión en los servicios de esta misma empresa Como por ejemplo Outlook también dispositivos que se Ejecutan en uno de los sistemas operativos de Microsoft Como por ejemplo ordenadores y tablets con Windows o consolas Xbox y Software de Microsoft Como por ejemplo visual Studio además de las claves de firma digital de msa de consumidor tenemos las claves de ashd que se utilizan a nivel empresarial para acceder a servicios en la nube de empresas Como por ejemplo exchange online a través de la plataforma de Outlook web Access Bueno pues tanto las claves de firma digital msa de consumidor como las Dei que son empresariales se emiten y administran desde sistemas separados tipo Air Gap y sólo deben ser válidas para sus respectivas plataformas es decir un token de autenticación creado por una clave de firma digital de msa solo Debería ser válido en servicios de consumidor como outlook.com y no en servicios de asherid del mismo modo un token de autenticación creado por una clave de firma digital de ashared solo debería valer En plataformas empresariales como Outlook Access en exchange online y no outlook.com que es una plataforma para consumidores los cibercriminales aprovecharon un problema de validación de tokens para impresionar a usuarios de ID y obtener acceso a su correo empresarial lo que hicieron los atacantes fue comprometer de alguna forma algo que por el momento se desconoce y que Microsoft sigue investigando Pues eso como digo comprometieron de alguna forma una clave de firma digital de msa de consumidor y la utilizaron para crear tokens contra exchange online y acceder a través de Outlook web Access es decir que utilizaron una clave de consumidor para

acceder a servicios empresariales no hay evidencia de que el actor de amenazas haya usado claves específicas de asur ID para acceder a estos servicios de ashore ID o que haya utilizado cualquier otra clave además de la que Microsoft ha identificado que este grupo apete ha utilizado como parte de este ataque es decir Microsoft ha concluido que solo se ha utilizado sólo se ha abusado de una clave y esta clave es una clave de tipo msa de consumidor para acceder como digo a servicios de asherd servicios empresariales La Brecha este ataque en concreto se detectó el 16 de junio de este año después de que una agencia del poder ejecutivo civil Federal de Estados Unidos identificar actividad sospechosa en entorno Cloud de Microsoft 365 los detalles provienen de un aviso conjunto de seguridad cibernética publicado por la agencia de seguridad de infraestructura y ciberseguridad de Estados Unidos la ciza y la oficina Federal de investigaciones el FBI pues este aviso como digo fue publicado el 12 de julio de este año además de esta agencia que acaba de nombrar también fueron atacados el departamento de comercio de Estados Unidos así como las cuentas de correo electrónico pertenecientes a un miembro del personal del Congreso un defensor de los derechos humanos de Estados Unidos y grupos de expertos de Estados Unidos sin embargo nos han hecho públicos los nombres específicos de todas las organizaciones o agencias afectadas ni la cantidad de cuentas que pueden haber sido comprometidas pero se estima que menos de 10 organizaciones fueron afectadas en Estados Unidos Microsoft cuando recibió esta notificación de esta agencia gubernamental de Estados Unidos El Poder Ejecutivo civil Federal pues investigó e identificó el ataque y de esta forma notificó a los administradores de todas las organizaciones comprometidas Microsoft publicó una notificación de seguridad en la que decía literalmente que aunque la clave de firma digital de msa comprometida por los cibercriminales estaba destinada solo para cuentas msa de consumidor un problema de validación de tokens de autenticación permitió que esta clave fuera confiable y válida para firmar tokenshore ID empresariales pero desde entonces desde que se ha identificado ese problema Microsoft ha corregido este fallo no está claro si el problema de validación de tokens se explotó como una vulnerabilidad de día cero o si Microsoft ya estaba al tanto del problema antes de que sufriera este ataque además de arreglar ese problema de validación Microsoft también ha invalidado o bloqueado la clave de firma digital msa de consumidor comprometida por los atacantes cisa dijo que la agencia del poder ejecutivo civil Federal de Estados Unidos pudo identificar la infracción al aprovechar el registro mejorado que ofrece Microsoft por View audit Premium específicamente usando la acción de auditoría de buzón mail items Access Esto se debe a que esta agencia está suscrita a un servicio Premium de pago de Microsoft sixty Five como digo se llama Microsoft por View audit la agencia cisa recomienda que las organizaciones habiliten el registro de polvo odit activen el registro de auditoría unificado de Microsoft 365 y se aseguren de que los operadores puedan Buscar en los registros en los blogs para permitir la identificación de este tipo de actividad y diferenciarla del comportamiento esperado dentro del entorno Es decir para buscar desviaciones del Estado normal que puedan ser indicios de actividad maliciosa esto dice sí genial muy bien tengo logs Pues nada voy a ponerme a investigar no pero esto significa que las empresas ahora tienen que contratar y pagar por un servicio adicional para tener registros con información adicional que les permite identificar esta actividad maliciosa y esto ha causado críticas contra Microsoft por bloquear estas capacidades forenses detrás de Barreras de licencia adicionales evitando Así que los clientes puedan acceder a registros de auditoría detallados que de otro modo Podrían haber ayudado a analizar e identificar el incidente para otras empresas que fueron comprometidas en este ataque pero que no han podido determinar que así lo fueron siguiendo esta polémica ron whited nuestro senador favorito publicó recientemente y a raíz de este ataque una carta en la que dice que Microsoft tiene una responsabilidad significativa por este nuevo incidente y cita varios

argumentos para respaldar su afirmación primero dijo que Microsoft no debería haber tenido una sola clave maestra que cuando inevitablemente se la roban pueda usarse para falsificar el acceso a las comunicaciones privadas de diferentes clientes en segundo lugar como señaló Microsoft después del incidente de solar Wings Supongo que os acordaréis queridos oyentes fue un gran incidente un gran ataque muy sonado las claves de cifrado de alto valor deben almacenarse en un hsm o un módulo de seguridad de Hardware cuya única función es evitar el robo de claves de cifrado pero la declaración de Microsoft de que ahora han trasladado las claves de firma digital de consumidor las msa el mismo tipo de clave que los atacantes han comprometido y abu en este ataque Bueno a un almacén de claves reforzado utilizado para sistemas empresariales plantea serias dudas sobre si Microsoft siguió sus propios consejos de seguridad y almacenar dichas claves en un hsm o no Como dice el dicho en casa del herrero cuchara de palo no para los que no sepáis un poquito más el hsm es una pieza Digamos como un ordenador que solo se utiliza para operaciones criptográficas para calcular hashes para calcular firmas para cifrar datos y todo se hace Dentro de este dispositivo y no sale nada de las claves criptográficas utilizadas ni el pin ni nada que en un escenario más próximo a todos nosotros podemos encontrar hsms en los cajeros automáticos normalmente vienen embebidos en los teclados y todo el tema de variación de pins y creación de firmas criptográficas a raíz del pin que luego se envían se envía bueno mensajes firmados con derivados del pin Bueno al banco en sí no todo esto se realiza en el hsm en este hardware de forma segura y sin que tu pin salga de ahí en principio así así Debería ser aunque se han visto otros tipos de casos y vulnerabilidades en este tipo en cajeros automáticos pero no no es no es caso de este de esta noticia de este episodio volviendo a la carta del senador wyren su tercer argumento Es que la clave de firma digital msa utilizada en este último ataque fue creada por Microsoft en 2016 y atención caducó en 2021 las pautas federales de seguridad cibernética las mejores prácticas de la industria y las propias recomendaciones de Microsoft para los clientes dictan que las claves de cifrados se actualicen con más frecuencia para evitar ser comprometidas Y además que los tokens de autenticación firmados por una clave caducada nunca deberían haber sido aceptados como válidos esto es seguridad one one seguridad básica y Bueno finalmente writen también dice que si bien los ingenieros de Microsoft nunca debieron haber implementado sistemas que violaran Estos principios básicos de ciberseguridad estas fallas obvias deberían haber sido detectadas por auditorías de seguridad internas y externas de Microsoft el hecho de que estas fallas no se detectarán plantea dudas sobre Qué otros defectos graves de ciberseguridad también pasaron por alto estas auditorías de ciberseguridad y con esto biden también ha pedido a las agencias federales de Estados Unidos que lleven a cabo investigaciones en detalle relacionadas con este incidente porque cree que puede haber más chicha de la que estamos viendo actualmente volviendo al tema de los logs con suscripción Premium comentar que las organizaciones afectadas que no tenían esta suscripción que son licencias que Microsoft llama E5 a5 o g5 que incluye información adicional en los blogs cruciales para investigar e identificar este tipo de ataque pues no pudieron detectar que fueron comprometidas verdad según biden cobrar a las personas por funciones Premium necesarias para no ser comprometidas es como venderte un automóvil y luego cobrarte más por los cinturones de seguridad o incluso los airbag a raíz de estas críticas una semana después de la publicación del ataque Microsoft anunció que está expandiendo las capacidades de registro de logs en la nube para ayudar a las organizaciones a investigar incidentes de seguridad cibernética Y obtener más visibilidad todo esto sin coste adicional Muchas gracias Microsoft Pero esto lo tiene que haber hecho hace tiempo se espera que se implemente esto a partir de septiembre de este año para todos los clientes gubernamentales y comerciales como parte de este cambio se espera que los usuarios reciban acceso a registros detallados del acceso al

correo electrónico y más de otros 30 tipos de datos de Registro que anteriormente solo estaban disponibles en el nivel de suscripción de Microsoft por View audit que es Premium Además de eso Microsoft dijo que está extendiendo el periodo de retención predeterminado para los clientes de audits estándar de 90 días 180 días así que ya sabéis queridos oyentes aquellos que tengáis servicios con microsofty Five servicios empresariales a partir de septiembre ya podéis acceder a registros con información adicional y un período mayor de retención de datos sin pagar un duro ya podéis lanzar vuestras campañas de investigación de auditoría de hunting y tener puesto un ojo en la actividad de vuestros servicios en la nube a todo esto obviamente comentar que china ha rechazado las acusaciones de que estuvo detrás de este ataque de espionaje y calificó a Estados Unidos de mentiroso Para cerrar solo comentar que en esta era de tecnología Cloud estamos a la Merced de la seguridad de las grandes empresas que ofrecen estos servicios pero no hay que desmayarse queridos oyentes se pueden aplicar medidas adicionales de seguridad además de lo que ofrecen las empresas en la nube como por ejemplo cifrado extremo a extremo que aunque te comprometan una clave de autenticación a estos servicios en la nube no puedan acceder directamente a tus datos Porque requiere una clave adicional de descifrado que solo tú tienes en tus dispositivos también temas de contratar servicios de shock para tener monitorización continua y temas similares obviamente realizar auditorías de seguridad en los servicios y la configuración de incluso estos servicios de terceros de empresas tan grandes que aunque sus servicios parecen seguros puede ser que tu configuración específica no lo sea también llevar a cabo campañas de Security a wernes sobre todo enfocadas de phishing y ataques de ingeniería social porque aunque no se sabe en a ciencia cierta por el momento Cómo consiguieron los cibercriminales acceso a esta clave de firma digital de msa de consumidor probablemente tiene pinta de que fuera a través de ingeniería social también pues facilitar cursos de seguridad a desarrolladores sobre todo a Microsoft Win Wings deberíais haber implementado esto de mejor forma y bueno también por si acaso no vaya a ser que este ataque además de espionaje acabe en cifrado de datos ya sabemos ransomware pues hacer backups de datos y pruebas de restauración de estos backups pero cualquier caso como digo Microsoft nos deja más tranquilos diciendo que este fallo primero ha sido solucionado segundo la clave comprometida utilizada para crear estos tokens falsificados y acceder a ashore ID también ha sido revocada y luego en último lugar que a partir de septiembre Oye va a poner de forma gratuita logs con mucha más información que va a permitir a empresas poder determinar si están siendo atacadas y si han sido comprometidas y también temas adicionales de retención de datos que nunca viene mal por si los atacantes son un poco más steels no y tardan más tiempo en llevar a cabo su ataque Pues bueno ahora tenéis más tiempo 180 días para poder correlar eventos en todo ese periodo Pues nada queridos oyentes como siempre Muchas gracias por vuestro apoyo en cada episodio Muchas gracias por escucharnos Muchas gracias por dejarnos vuestros comentarios y si no nos lo habéis dejado y estáis un poco Ahí tímidos os animamos a que nos dejéis vuestros comentarios que lo agradecemos muchísimo ya sea bueno ya sea malo para que mejoremos todo es bien recibido desde tierra de hackers y Unidos al discord que ahí Tenemos también mucha actividad y conversación interesante y si no bueno en Twitter y cualquier otra red social también podéis Pon Eros en contacto con nosotros y nada como siempre como digo Muchas gracias chao chao si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers