el FBI desmantela la infraestructura del grupo de ciberdelincuentes conocido como quak Bot pero no es suficiente para terminar con su actividad delictiva prestad atención a esos archivos comprimidos recibidos cibercriminales han estado abusando de una vulnerabilidad en winrar para robar criptomonedas y apts rusos y chinos como sandworm apt28 y apt4 la han explotado en campañas de ciberespionaje en conformidad con la costumbre arraigada de Halloween os traemos un episodio de lo más terrorífico comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 1 de noviembre de 2023 este es el episodio número 110 yo soy Martín vigo y no está en directo pero sí en diferido mi buen amigo Alexis porros Hola Alexis qué tal Muy buenas Martín aquí estamos otro episodio más viento en popa toda vela para grabar otro más para los históricos y para no enrollarme más lo típico que siempre comentamos al principio de cada episodio nos podéis seguir en todas las redes sociales donde nos podéis encontrar como tierr deeh hackers o @r adeh hackers también os invitamos a suscribiros a tierra de hackers en vuestra plataforma de podcast favorita y podéis entrar en nuestro servidor de discord eh A través de tierradel comom baris ahí tenemos varios canales varias temáticas en donde se comentan Bueno pues eso hay conversaciones interesantes y os invitamos a que os deis un paseo por ese Rincón del ciberespacio Claro que sí sí y yo por mi parte justo antes de comenzar recordaros que estamos a una semana del curso for Cyber Security for web developers que voy a estar impartiendo en Barcelona presencialmente el 7 y el 8 de noviembre es en inglés y está orientado a que aprendas y comprendas las vulnerabilidades más habituales en la web Si estás interesado y además te gustaría tenerme a mí como profesor puedes apuntarte en tierradel comom barwe ahí tienes toda la información y darle las gracias a nuestros mecenas de patreon que son esenciales para que este podcast siga adelante y os lo podamos traer a todos de manera gratuita Si estás interesado en ayudarnos si te gusta lo que hacemos si aprecias las horas que dedicamos a esto puedes contribuir en patreon.com bartierra de hackers y te estaremos enormemente agradecidos además si te haces un patreon de nivel merch te llegará a casa un un regalito por nuestra parte y otra parte esencial es nuestros sponsors como 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 con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y que está buscando ingenieros con experiencia en ciberseguridad para ayudarles a hacer y construir su misión contratan en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web monat.com mad.com y le podéis mandar vuestro currículum a tierr deckers @mon comom empezamos con la noticia para no liarnos más y esta noticia que os traigo Pues realmente comienza con un comunicado del propio FBI de hace unas semanas concretamente a finales de agosto esta agencia bueno y otras eh de otros países llevaron a cabo una operación para desmantelar la infraestructura y los activos de criptomonedas utilizados por el notorio malware qub este comunicado y os traduzco literalmente los dos primeros párrafos del FBI comienza Así que publicaron en la página web de justice.gov el departamento de justicia anunció hoy una operación multinacional que involucra acciones en los Estados Unidos Francia Alemania los Países Bajos el Reino Unido Rumanía y letonia para interrumpir la red de Bots y malware conocida como quak Bot y desmantelar su infraestructura el código malicioso de qubo está siendo eliminado de las computadoras de las víctimas impidiendo que cause más daño el departamento también anunció la incautación de aproximadamente 8.6 millones en criptomonedas como ganancia como ganancias ilícitas esta acción representa la mayor interrupción financiera y técnica liderada por los Estados Unidos de una botnet utilizada por ciberdelincuentes para cometer ransomware fraudes financieros y otras actividades criminales habilitadas por la tecnología la mayor interrupción financiera y técnica liderada por los Estados

Unidos de una bonet utilizada por delincuentes ahí es nada esto la verdad por lo que he visto causó un daño significativo a las operaciones de este grupo de ciberdelincuentes de qub lo que nos lleva a plantearnos una pregunta clave cubot y todos los afiliados desaparecieron para siempre Gracias a esta operación del FBI o simplemente quedaron temporalmente inactivos esto es precisamente lo que llevó al equipo de investigación de talos a mirarlo más de cerca dicen que con moderada confianza afirmaron que los actores detrás de quak Bot siguen activos y están llevando a cabo de hecho una nueva campaña esta campaña se ha puesto en marcha justo antes de la operación del FBI que en principio había acabado con toda su infraestructura entonces aquí ya tenemos algo jugoso para para lo primero es cómo esta empresa talos llegó a esta conclusión de que Todavía siguen en activo Supongo que eso es lo que te estás preguntando querido oyente por la respuesta radica en los metadatos incrustados en los archivos lnk utilizados en la nueva campaña estos archivos son Cuando haces un acceso directo por ejemplo en el escritorio de tu ordenador para un archivo pues esos esos archivos que tienen así Digamos como la flechita no para indicar que en realidad no es el propio archivo sino un enlace directo al archivo en cuestión porque a lo mejor lo tienes almacenado en otra parte del disco duro pues ahí Hay ciertos metadatos que talos utilizó para poder rastrear a este grupo publicaron previamente información sobre cómo utilizar estos metadatos para como decía Identificar y restrear a este tipo de grupos de delincuentes específicamente detallaron en este caso como una máquina que se utilizó en la campaña que ellos llamaron aa tenía una relación directa con la nueva bnet que llaman BB sin embargo después de que thalos compartiera esta información en un artículo el año pasado sobre verano de 2022 los actores principales detrás de las campañas aa y BB y una nueva que llamaron Obama y que todos pertenec a quot comenzaron a borrar los metadatos de los archivos elenque dificultando así la detección y el seguimiento en su propio blog como decía el año pasado detallaron Cómo se hace y os dejo en las notas del episodio junto con otros enlaces relacionados con esta noticia para que podéis ir a indagar ya que entran bastante en lo técnico yo me quedaré en la superficie y lo que es crucial de comprender para entender Cómo opera esta Campaña en agosto de 2023 hace cosa de mes y medio talos identificó nuevos archivos lnk creados en la misma máquina que estaban investigando lo más llamativos que estos archivos lnk apuntaban a una red compartida y su payload por así decía estaba relacionado con una variante del ransomware llamado ransom k tras un análisis más detenido vieron que estos archivos apuntaban a powershell.exe y pasaban argumentos para descargar la siguiente etapa de la infección ya sabéis que normalmente Pues el primer payload la única función que tiene es descargarse el resto de del malware no del software malicioso para que así el archivo que te envían o lo que sea sea lo más pequeñito posible hay como varias etapas en la infección lo que resulta particularmente interesante es el método que empleaban para la descarga intentaban acceder a un recurso remoto en una dirección IP específica de ellos a través del protocolo webdav apuntando al puerto 80 webdav por si no lo conocéis es un protocolo que se encarga de de permitirnos de forma sencilla guardar editar copiar mover archivos desde servidores web básicamente un ftp pero es un protocolo diferente que funciona a través de de la web Por así decirlo esto en concreto puede haber sido un intento deliberado de eludir la detección de la línea de comandos al descargar un ejecutable remoto mediante powershell qué quiero decir con esto pues hoy en día Ya eh muchísimos fabricantes de software tipo antivirus y detección de digamos actividad anómala en los ordenadores para detectar si ha habido un compromiso en la seguridad pues H monitorizan mucho los comandos que se Ejecutan en una máquina específicamente en powershell Entonces esto puede haber sido una manera de descargarse la segunda etapa del malware sin tener que ejecutar comandos en powershell Pues yo que sé como un wget un curl o algo de esto un detalle importante a destacar es que los nombres de estos archivos lnk

insinúan que se distribuyen en correos de fishing una táctica pues istente con las campañas también anteriores de cubot por lo que volvemos a tener aquí no un poco el tema de los ttps alguno de estos nombres de hecho está en italiano que nos puede sugerir que estos actores pues pueden estar actuando no en esta región aquí quiero hacer un paréntesis y detenerme en la parte del fishing porque es otra de las razones por la que elegí esta noticia para traeros la Y es que hablamos de Spear fishing pero pero muy fishing Bueno brevemente ya sabéis hacer fishing pues es por ejemplo enviar correos electrónicos a las víctimas intentando que lleven a cabo alguna acción como descargarse un archivo y abrirlo no y cuando hablamos de spearfishing pues hablamos de que ese correo electrónico en vez de ser super genérico para poder enviarlo a cuanta más gente mejor pues alguien el atacante digamos te ha estudiado previamente pues ha visto en tus redes sociales Pues yo que sé que te gustan los gatos y cre a un email falso que está relacionado con algo que te gusta a ti para digamos Elevar las posibilidades de que atraiga tu interés o que pues no sospeches tanto y lleves a cabo esa acción para infectarte vale aquí esto del spearfishing esto de de digamos crear un email de manera que sea más atractivo para ti lo llevaron al nivel extremo resulta que los ciberdelincuentes habían previamente comprometido los servidores de correo electrónico de otras empresas de de muchas y lo que hicieron fue exfiltrate fueron hackearon otras empresas y descargaron todos sus correos electrónicos de manera automatizada en todos esos miles y miles de correos electrónicos de empresas ajenas que comprometieron buscan correos electrónicos de que estén dirigidos a las empresas que quieren comprometer y los de correo electrónico pasados donde ya hay una digamos conversación en marcha entre empleados de la empresa que han comprometido y la empresa que quieren comprometer es como si pues yo por ejemplo tengo emails con no sé con tiktok los atacantes quieren comprometer tiktok Ponle que yo soy un algu que trabaja con tiktok pues me comprometen a mí descargan todos mis correos ven que yo soy una de las personas que habla con alguien en tiktok y ahora pues me utilizan a mí como baza para hablar con tiktok Así que lo que hacen es enviar correos electrónicos continuando el hilo de la conversación que yo tengo con un empleado de tiktok y hacen Crean un email falso como respuesta de digamos y es donde adjuntan el archivo malicioso esto es brillante no hablamos de que de la nada te llega un email raro para que hagas clic en algo ni siquiera de un correo que como decía aunque te llegue de la nada tenga sentido para ti que te lo envíen no hablamos de que te llegue un correo en respuesta a otros correos que has estado intercambiando con una persona un correo que es la respuesta que estabas esperando recibir Esto hace complicadísimo detectar que en realidad es un correo falso y demuestra una vez más que necesitamos mecanismos automatizados Más allá de la concienciación de las personas que por supuesto es importantísimo pero necesitamos algo automatizado para ayudar a detectar los correos maliciosos que existen muchas soluciones Pues llega un punto que o eres la persona más desconfiada del mundo o vas a caer y eso es algo que los que nos dedic amos por ejemplo a temas de red teaming ya damos por hecho es cuestión de tiempo no se trata de caerá o no sino de cuándo caerá pero bueno volviendo al tema del malware utilizado es vital destacar que los archivos xxxll que se encontraban en los archivos cip junto con los lnk os recuerdo os dejo las notas en las notas del episodio todo el tema técnico porque si no no quiero hacer la noticia ni muy larga ni muy aburrida para la gente menos técnica Pues actuaban con el backdoor remcos este backdoor se ejecuta junto con ramom k lo que permitía a los actores de amenazas a estos apts acceder a las máquinas de las víctimas tras la infección en cuanto a ransom kight esta amenaza representa una versión actualizada del ransomware cyclops que fue rescrit desde cero esto deciro Simplemente porque es muy bueno como va van cogiendo versiones antiguas de ransomware las reescriben en parte para mejorarlas en parte para hacerlas más eficientes y en parte pues para evitar la

detección que pues que los antivirus tienen para ransomware ya muy conocido es importante también subrayar que no se cree que los actores detrás de qub están involucrados digamos en la oferta de ransomware aquello del ransomware As a service no para ransom night sino que son simplemente clientes de este servicio O sea que tenemos un grupo de ciberdelincuentes muy potente siendo clientes de otro grupo de ciberdelincuentes que desarrollan ransomware a pesar del ataque a la infraestructura de qub por el FBI talos bueno comenta que los operadores de esta amenaza siguen siendo una amenaza activa la operación del FBI no pareció afectar la infraestructura de entrega de correos de fishing que os comentaba de qub sino que se centró los servidores de comand en control es decir cuando ya estás infectado Pues el virus se comunica con los servidores del de los atacantes es a eso a lo único que afectó porque no utilizaban la misma infraestructura para mandar los emails de fishing para infectarte que la infraestructura que utilizan para controlar tu ordenador Por así decirlo no se ha visto a los actores de amenazas distribuyendo estos este malware después de esta operación aunque se que este malware probablemente Va a continuar siendo una amenaza significativa en el futuro Dado que los operadores siguen activos podrían optar por reconstruir la infraestructura de qub que maneja digamos los ordenadores infectados y reidar por completo sus actividades previas a la operación Pero antes de terminar la noticia quiero leeros otro párrafo del comunicado del FBI con el que empecé esta noticia y del que solo sabía leído los dos primeros párrafos presta la atención como parte de la operación el FBI logró obtener acceso a la infraestructura de qub e identificar más de 700.000 computadoras en todo el mundo incluyendo más de 200.000 en los Estados Unidos que parecen haber sido infectadas con quak Bot para interrumpir la botnet el FBI redirigió el tráfico de la B de qub a través de servidores controlados por el FBI los cues a su vez instruyeron a las computadoras infectadas en los Estados Unidos y en otros lugares a descargar un archivo creado por las autoridades encargadas de hacer cumplir la ley que desinstalar el malware de qub este desinstalador fue diseñado para liberar la computadora de la víctima de de la B de qub impidiendo la instalación adicional de malware a través de qub ostras o sea que el FBI ha instalado su propia cura en los ordenadores infectados y tú sin saberlo el FBI ha escrito código que se ha ejecutado en tu máquina sin tu consentimiento el FBI Según estipula la ley ha accedido a tu ordenador y ha hecho modificaciones sin una orden judicial que sí que sí que en este caso es por una buena causa y no quiero eludir ese hecho pero para mí aún así Bueno me resulta digno de debatir esto qué creéis vos os queridos oyentes es legítimo si nos quejamos por otras acciones de las fuerzas y cuerpos de seguridad que también Vienen con buenas intenciones por ser demasiado intrusivas Como no nos también nos vamos a quejar de esto que hay más intrusivo que esto quiero decir muchos ponemos el grito en el cielo Yo que sé porque Apple va a escanear nuestras fotos en nuestros dispositivos y con con constra const joder contrastar los hashes con una base de datos que contienen hashes de pornografía infantil El razonamiento detrás de esta acción es más que loable Todos queremos proteger a las víctimas más vulnerables pero no con cualquier método no a Costa de nuestra privacidad sin por lo menos intentar antes otros métodos pues tío que ahora tenemos al FBI ejecutando su payot de nuestras máquinas me resulta bastante más llamativo no sé en este caso es complicado me imagino que muchos de los que están infectados pues es porque son usuarios con pocos conocimientos sobre ciberseguridad el usuario habitual de un ordenador que lo usa como una herramienta en el día a día no es necesariamente un experto informático no tiene nociones de los peligros de usar internet no sabe manejarse con el el ordenador más allá bueno pues de usar el Software que necesita en su día a día vamos el 90 por de los usuarios acabo de escribir por tanto cabe pensar que arreglarle o protegerle el ordenador de manera transparente es algo bueno que eliminarle el software malicioso sin que tenga que hacer nada Solo trae beneficios a ese usuario Pero por

otro lado lo que decía abrimos la veda para que un gobierno para protegernos tome control de nuestros dispositivos electrónicos Dónde está el límite y si mañana La idea es no sé monitorizar nuestra actividad directamente desde nuestro ordenador como hace un antivirus básicamente que tenemos instalado y lo hacen entre comillas por nuestro bien o yo que sé evitar que visitemos ciertas páginas que podrían Mostrar contenido malicioso ya lo que el gobierno de turno defina como malicioso ya es cosa suya No sé no me gusta sinceramente Aunque Reconozco que es fácil para mí decir lo que no necesito de la ayuda del FBI para proteger mis dispositivos o para limpiarlos en caso de infección pero es que recordemos otro punto importante del párrafo que a lo mejor no recordáis insisto y repito el FBI pudo redirigir el tráfico de la red de Bots de quak Bots hacia y a través de servidores controlados por el FBI los cuales a su vez instruyeron a las computadoras infectadas en los Estados Unidos y en otros lugares a descargar un archivo creado por las autoridades encargadas de cumplir la ley que desinstalar el malware de qub y en otros lugares he dicho qué potestad tiene una agencia de un país extranjero para operar sin permiso en mi país para tomar control de mi ador por muy infectado que esté oiga que en mi país rigen las normas de mi gobierno de las fuerzas y cuerpos de seguridad de mi país yo la verdad es que flipo bastante Y me gustaría mucho conocer qué opináis queridos oyentes a ver si soy yo el único loco aquí al que bueno pues esto le chirría un poco y le incomoda en fin queridos oyentes que ya tenéis otro aliciente para proteger vuestros dispositivos de malware no solo para evitar perder vuestros datos sino también para evitar que una agencia de inteligencia extranjera venga a soluciono sin que te enteres lo que me sorprende y lo que resalto de esta noticia es que aunque la incautación de la infraestructura de quak Bot por parte del FBI en agosto fue un golpe duro digámoslo así para este grupo de ransomware la actividad continuada aunque le les tumben su infraestructura siguen renaciendo de las de las cenizas no como dicen Pues esta actividad continuada demuestra la resiliencia de estos actores de amenazas que no se rinden siguen adelante sacan infraestructura en otro Hosting en otro proveedor de servicios siguen creando modificando su ransomware es un lo que decimos siempre un gato de un juego de El gato y el ratón no me pregunto si esta resiliencia eh esta estas ganas de seguir adelante sea eh facilitado Por el ransom weas service por este modelo de negocio seguimos viendo con esta noticia que has traído al podcast que esta tendencia sigue creciendo en la ciberdelincuencia sobre todo porque este modelo negocio democratiza es decir hace más baja la entrada eh más fácil digamos la entrada en este tipo de negocios para los cibercriminales alguien que no necesariamente sea un experto en ciberseguridad podría meterse en este mundillo criminal digámoslo así alistándose no en uno de estos grupos Y utilizando no solo el malware que ofrecen que esto facilita mucho las cosas sino a mí me parece incluso más valioso es la metodología de cómo comprometer empresas Y cómo llevar a cabo todo el tema del ransom ya hemos visto como con conti cuando se publicó se lió su su guía de cómo hacer todo esto que eso realmente para los que no saben son tan expertos en todo este tema de ciberseguridad digamos en el del lado oscuro esto les facilita mucho es como un un bootcamp no un un curso acelerado de de cómo convertirse en cibercriminal y llevar a cabo estos ataques de ransomware de forma muy muy prometedora muy exitosa En definitiva lo que quiero comentar es quedemos todos alertados una vez más de estos riesgos de ransomware y intentemos fomentar la educación frente a ataques de fishing sobre todo ya que es una de las principales vías utilizadas por los cibercriminales para comprometer organizaciones cierto es que muchas veces el acceso inicial de estos ataques de ransomware es vía explotación de servicios vulnerables en internet o mal configurados pero la verdad es que si esto falla y a veces falla eh lo que siempre normalmente da mucho éxito es explotar El eslabón más débil que en este caso somos los humanos Así que cuidado ahí e mucho ojo a a bueno todos los ataques de fishing vía email teléfono sobre todo

últimamente muy exitosos y mensajería discord y en general eh también por móvil mensajes de texto y similares Pues nada Martín seguimos adelante con la siguiente noticia que os traigo y que que va sobre vulnerabilidades en winrar que se han utilizado en ataques de ingeniería Social para robar criptomonedas y también para lanzar campañas de ciberespionaje por parte de apts archiconocidos en el podcast eh Como sandworm y apt 40 y apt28 rusos y chinos aquí siempre aprovechándose de vulnerabilidades de día cero un poquito dar contexto para aquellos que han vivido debajo de una piedra o en una cueva durante la época de la informática moderna no quería comentar Qué es winrar pues esta es una aplicación que se utiliza para gestionar archivos comprimidos tanto para crearlos como para descomprimir losos y digamos desempaquetar losos no para acceder a los archivos que contiene este archivo imprimido es una aplicación que tiene más de 500 millones de usuarios en todo el mundo es una de las herramientas de compresión más populares y sobre todo en sistemas Windows probablemente muchos de vosotros queridos oyentes hayáis instalado y utilizado esta aplicación múltiples veces en múltiples dispositivos que tengáis en casa Es una herramienta muy utilizada también en entornos empresariales así que por consecuencia los actores de amenazas invierten tiempo en identificar vulnerabilidades en este tipo de programas y otros programas también populares comúnmente utilizados por usuarios de internet sobre todo en entornos corporativos porque es ahí donde está digamos el dinerillo no donde está lo lo que se puede robar y por tanto lo que os traigo es un retrato de un par de vulnerabilidades recientes en winrar que han sido utilizadas por cibercriminales para infectar a usuarios en internet principalmente inversores de criptomonedas pero también otros usuarios interesados en temas financieros y sin más dilación voy a comentar una de las vulnerabilidades en un informe publicado a finales de agosto de este año los investigadores de grupo IB dijeron que descubrieron un cero day una vulnerabilidad de día Cero en winrar que está etiquetada digamos con el número cv-22 por este año gu 38 831 y que se ha estado utilizando ellos han observado esto en en el mundo en internet se está utilizando esta vulnerabilidad desde abril de este mismo año también para comprometer a usuarios de foros de inversión de criptomonedas donde los ciberdelincuentes hacían pasar por otros entusiastas eh gente que un poco sabía del mundillo no y que intentaban compartir sus estrategias de trading se veían en estos foros mensajes con títulos como mi mejor estrategia personal para invertir en bitcoin esto obviamente en foros más de bitcoin no pero también habían otros mensajes que contenían estrategias para forex intercambio de digamos de Divisas extranjeras como no nonsense forex indicators algo que se podría Traducir como nada de tonterías en inversión forex indicadores no que son e mensajes de este tipo fueron publicados en múltiples foros de inversión Sobre todo como digo criptomonedas eh que contenían enlaces que permitían Descargar archivos comprimidos Y maliciosos estos archivos maliciosos se distribuyeron en al menos ocho foros públicos de trading de inversión infectando 130 dispositivos de traders el número de víctimas y las pérdidas financieras resultantes de esta campaña se desconocen estas publicaciones en los foros contenían enlaces a archivos zip o rar punto zip o punto rar eh Para winrar especialmente diseñados de tal forma que pretendían incluir estrategias de trading útiles como digo o consejos e de tal forma que son atractivos no para alguien que está metido en el mundillo y que quiere un poquito pues hacer dinerillo No en el tema de la inversión y que contenían pdfs eh También podían algunos contener archivos de texto incluso imagen cuando los usuarios abrían estos archivos comprimidos y hacían clic en los archivos Aparentemente inofensivos que este archivo comprimido contenía como digo normalmente eran pdfs pero también podían ser imágenes o archivos de texto esto desencadenaba la ejecución de un payload malicioso o un Script malicioso que infectaba sus ordenadores y te preguntarás querido oyente pero cómo puede ser si si no están haciendo nada solo está están abriendo el PDF Y si el sistema estaba

parcheado y todo eh estaba correcto Por qué sucedía esto pues la vulnerabilidad en winrar se activa al crear archivos Especialmente diseñados con una estructura ligeramente modificada diferente de un archivo winrar normal y Esto hace que se ejecute una función de winrar específica que se llama shell execute ejecutar una shell ejecutar una consola no y que esta función en este caso de tal forma este archivo malicioso está creado de tal forma que esta función Recibe un parámetro incorrecto cuando el usuario intenta abrir este archivo inofensivo que es el archivo señuelo y en su lugar winrar ejecuta un Script de batch o command de Windows que está dentro de una carpeta con el mismo nombre que el archivo inocente y para aclarar esto os pongo el siguiente escenario digamos que recibís un archivo punto rar de alguien que está compartiendo su estrategia de inversión en formato pdf este archivo como digo es un PDF pero podría ser una imagen un txt cualquier otro tipo de archivo no dañino por ejemplo que no sea un ejecutable porque eso obviamente va a ejecutar algo en tu ordenador y no lo vas a ejecutar tiene que ser un archivo que parezca inofensivo el archivo señuelo como digo eh estrategia de inversión en PDF Okay entonces como usuario que recibe este archivo comprimido vas abres haces doble clic en el punto rar y se te abre winrar y ves que está el PDF ahí pero también ves una carpeta con el mismo nombre que ese archivo inofensivo que ese PDF entonces haces doble clic en el archivo PDF para abrirlo y leerlo y Boom ya demasiado tarde te han infectado el ordenador porque como digo por un fallo por esta vulnerabilidad de día cer que se ha descubierto en winrar en este caso eh está creado el archivo comprimido de tal forma que cuando se hace doble clic en el PDF winrar Se confunde y lo que hace es ejecutar el primer archivo que hay dentro de la carpeta que tiene el mismo nombre que el archivo PDF y este primer archivo dentro de esta carpeta es un Script de Windows que lo que hace obviamente en este caso en estas infecciones es eh lanzar un archivo auto extraíble que contenía un payload malicioso final y que infectaba el ordenador con varias versiones de malware Como por ejemplo Dark me gader y remcos rat eh proporcionando acceso remoto a los dispositivos infectados todo este este tipo de malware es rat como digo del inglés Remote Access troyan son troyanos o formas de conectarse remotamente a los sistemas infectados Los investigadores dicen que no está claro quién aprovechó esta vulnerabilidad en la reciente Campaña cibercriminal en la que se intentaron robar criptomonedas sin embargo parece que estas infecciones están motivadas de forma financiera que es la misma motivación detrás de los grupos apt que aprovechan malware como Dark me esta cepa de malware en concreto ha sido asociada con el grupo Evil num También conocido como ta 4563 que es un grupo de amenazas incentivado como digo por motivos financieros y que ha estado activo en el Reino Unido y Europa desde al menos 2018 el grupo es conocido por atacar principalmente organizaciones financieras y plataformas de comercio en línea Bueno ahora os comento queé podéis hacer como usuarios para protegeros de esto para que no os roben vuestras criptomonedas o credenciales de vuestra banca online o temas similares pues os recomendamos que queridos oyentes En cuanto acabéis de escuchar este episodio o si no antes de abrir el próximo archivo comprimido vayáis a actualizar vuestro winrar con la última versión que debería ser a fecha a este momento Debería ser la 6.24 que fue lanzada el 2 de Agosto de este año lo curioso Es que la aplicación winrar no se actualiza automáticamente por lo que Vais a tener que descargar e instalar manualmente el parche esta versión de winrar también resuelve varios otros problemas de seguridad incluida otra vulnerabilidad de winrar un fallo de tipo overflow que puede desencadenar la ejecución de comandos al abrir un archivo rar especialmente diseñado Así que mucho cuidado con los archivos winrar que estéis abriendo estos días y por favor ID a actualizar winrar ahora mismo alternativamente si estáis utilizando Windows 11 simplemente podríais utilizar el soporte nativo para archivos rar o 7zip que se incluyó en la última actualización del sistema operativo o simplemente descomprimir el

archivo comprimido y abrir los archivos que necesitéis ya sea el PDF la imagen o el archivo de texto con esto me refiero a hacer botón derecho en el archivo comprimido y decir descomprimir aquí y entonces se va crear la carpeta con los archivos que contiene el archivo comprimido no de esta forma la vulnerabilidad no se abusara no se ejecutaría porque no estáis haciendo doble clic en en winrar sino que estaríais haciendo doble clic directamente en el sistema de archivos de Windows y ahí esta vulnerabilidad no no tendría cabida y ahora os traigo un twist un poquito interesante de la noticia Y es que no solo los crypt traders han sido el objetivo de esta vulnerabilidad de winrar sino que también otras empresas otras organizaciones fueron Víctimas de campañas de ciberespionaje el grupo de análisis de amenazas tag de Google ha descubierto Que varios grupos apt vinculados a Rusia y China han estado explotando esta vulnerabilidad desde principios de este año cuando la vulnerabilidad aún era desconocida por una parte tenemos al archiconocido apt sandworm Google tag en un caso descubrió a sandworm vinculado a Rusia entregando documentos PDF señuelo y archivos cip maliciosos que explotan esta vulnerabilidad de winrar este grupo de ciberamenazas alineado con la dirección principal del Estado Mayor de las fuerzas armadas de Rusia el Gru como se le conoce utilizó la explotación para entregar un infoser común llamado radamantis que puede recopilar y ex filtrar credenciales de navegador e información de sesión de las máquinas infectadas en esta campaña sandworm apuntó al sector energético a través de una campaña de fishing que se hacía pasar por una escuela de entrenamiento de drones de Guerra de Ucrania utilizando un señuelo temático con una invitación para unirse a la escuela el correo electrónico contenía un enlace a un servicio de compartición de archivos anónimo llamado fex.net que entregaba un documento PDF señuelo benigno con un currículum de entrenamiento de operadores de drones y un archivo zip malicioso que explotaba la vulnerabilidad de winrar y este archivo tenía el título de programa de entrenamiento para operadores algo digamos que iba con la temática del mail no para hacerlo más más creíble por otra parte tenemos al grupo apt28 También conocido como Frozen Lake que es otro grupo de cibercriminales vinculado también con el Gru de Rusia y que utilizó un proveedor de alojamiento gratuito para servir el exploit de esta vulnerabilidad de winrar enfocándose en usuarios en Ucrania la página inicial redirigida a los usuarios que la visitaban a un sitio mbin que es un proyecto que utiliza microservicios para peticiones web sin entrar mucho en detalle lo que este sitio mocin hacía era realizar controles de en base a la dirección IP del usuario si esta dirección IP versión 4 venía de alguien correspondía a alguien en Ucrania lo que hacía era dirigirle a la siguiente etapa a la siguiente petición http para que se descargara un archivo que contenía la vulnerabilidad de winrar si no era así si era una IP que estaba fuera de Ucrania pues le dirigía a otra página que no servía este exploit digamos en este caso el archivo infectado que se servía era un documento señuelo que contenía una invitación a un evento del centro razumkov que es un think Tank político en Ucrania finalmente lo que hacía este archivo era desplegar la carga útil de Iron jaw que es un pequeño Script de powershell que roba los datos de inicio de ción del navegador y de los directorios de del sistema de ficheros vamos otro infoser además la infección creaba un túnel ssh inverso para que los cibercriminales pudieran controlar el sistema de forma remota y finalmente Google también dijo que observó a grupos respaldados por el gobierno vinculado con china como ap pt40 que estuvo lanzando una campaña de fishing dirigida a papúa Nueva Guinea los correos electrónicos de fishing incluían un enlace de dropbox a un archivo zip que contiene el exploit de winrar que contenía un PDF protegido por contraseña como señuelo y un archivo lnk un un archivo link de acceso directo de Windows la carga útil la carga final era Box rat una puerta trasera un troyano en net que utiliza la Api de dropbox como mecanismo de command and control En definitiva la explotación de esta vulnerabilidad de winrar destaca que los exploits para las vulnerabilidades conocidas

pueden ser altamente efectivos a pesar de que haya un parche disponible y que los actores maliciosos van a continuar confiando en estos n days como se les llama exploits de día n cuando n es más de cero porque ya hay parche no ya es una vulnerados y eh También aprovechan el hecho de que las tasas de parcheo son lentas y a su favor en este caso recordad que winrar no tiene funcionalidad de actualización automática Así que si no es que el usuario actualiza winrar Eh pues winrar va a estar desactualizado y vulnerable a a este exploit a mí todavía me me parece curioso que herramientas digamos tan utilizadas no en el día a día como archivos comprimidos que todo el mundo intenta utilizar para ahorrar eh A veces ancho de sobre todo en en países donde el ancho de banda es es escaso pues que no tenga funcionalidad de de actualizarse de forma automática es algo que que es bastante curioso a día de hoy si se implementa la funcionalidad de actualización automática de forma correcta vía https e incluso se intenta Añadir de alguna forma una verificación de firma digital pues no habría por qué preocuparse bueno y os he comentado al principio que os traía dos vulnerabilidades la primera hasta aquí ha llegado y la segunda Pues a finales de agosto de este año se reveló otra vulnerabilidad grave En winrar que podría ser explotada por un actor de amenazas para lograr la ejecución remota de código en sistemas Windows identificada como CV 2023 40477 y con una puntuación de cvss de 7.8 que es bastante elevada el cvss digamos es un marco de asignación de riesgo a vulnerabilidades en base a diferentes factores eh si tiene se puede explotar de forma remota o no Si permite escala de privilegios o no Bueno no voy a entrar en eso pero bueno es una puntuación bastante elevada y Total que la vulnerabilidad Fue descrita como un caso de validación incorrecta al procesar volumen volmenes de recuperación lo que causaba un desbordamiento de buffer y proporcionaba ejecución remota de código sin entrar en mucho detalle técnico comentar que la explotación exitosa de este fallo requiere la interacción del usuario para que visite una página maliciosa o simplemente abrá un archivo comprimido malicioso que reciba vía email o que se lo descargue de alguna página web ya sea un foro como dicho en el caso anterior en la vulnerabilidad anterior de un foro de inversión de criptomonedas Pues algo SIM no el usuario básicamente lo que tiene que hacer para activar esta vulnerabilidad para para que se active el exploit es abrir eh un archivo winrar malicioso y aunque esta vulnerabilidad eh se reveló dos días antes de la vulnerabilidad anterior no se ha observado que se haya utilizado esta en concreto para comprometer sistemas una razón podría ser que aunque haya una prueba de concepto de este expl públicamente disponible y que se pudiera utilizar fácilmente en un ataque los sistemas operativos modernos incluyen mecanismos de prevención de seguridad que podrían detener el ataque los sistemas modernos de Windows implementan medidas de prevención de ejecución de código abusando errores de memoria como es el caso de esta vulnerabilidad pero lo más probable es que la vulnerabilidad anterior es mucho más fácil de construir mucho más fácil de de armar de We nice como se diría en inglés no porque es un archivo PDF con una carpeta con el mismo archivo PDF o no cualquier tipo de archivo y con un Script dentro de esa carpeta en este caso esta vulnerabilidad más de de fallo de digamos de errores de memoria necesita un poco más de complejidad y relacionado con esta segunda vulnerabilidad finalmente comentar que eh un actor malicioso publicó en github una prueba de concepto para el exploit de esta vulnerabilidad y era malicioso y estaba destinado a infectar a usuarios que descargarán este código esta prueba de concepto con el malware Venom rat otra otro troyano que da acceso de forma remota a los sistemas infectados esta prueba de concepto se basaba realmente en otra públicamente disponible que explotaba una vulnerabilidad de inyección de sql en una aplicación llamada geoserver que estaba identificada como cve 2023 de este mismo año También 2517 la cuenta de github que alojaba el repositorio Con este código esta prueba de concepto maliciosa ya no es accesible se dice que esta prueba de concepto se subió a github el 21 de agosto de este año 4 días después

de que se anunciara públicamente la vulnerabilidad ya vemos que este actor de amenazas estaba al acecho y en cuanto surgió una vulnerabilidad así interesante Pues nada Oye voy a publicar este esta prueba de concepto maliciosa y a ver si alguien se la descarga un análisis del repositorio reveló un Script en python y un vídeo que demostraba Cómo usar el exploit el vídeo atrajo al menos 121 visitas en total Así que esa podría ser la muestra de de potencialmente usuarios infectados este Script en python en lugar de ejecutar el la prueba de concepto real para esta vulnerabilidad de winrar lo que hacía era comunicarse con un servidor remoto eh hospedado en check blacklist Worlds euu eu de Europa no para descargar un ejecutable llamado windows.github.com concluyendo con esta noticia cierro con unas lecciones aprendidas la primera es que los grupos apts se regocijan en el oportunismo de vulnerabilidades que permiten ejecución de código abusando del eslabón más débil el usuario el Humano nosotros queridos oyentes tú y yo y combinan este tipo de vulnerabilidades de día n con la ingeniería social aplicaciones como winrar son objetivos interesantes para cibercriminales porque saben que no tienen actualizaciones automáticas y los usuarios raramente actualizan dichas aplicaciones por lo que aunque haya parche son vulnerabilidades muy atractivas y que son válidas durante mucho tiempo la segunda es que como usuarios debemos activar las actualizaciones automáticas de software y parchear aplicaciones que no ofrezcan esta funcionalidad Tan pronto como surjan estos parches esto en entiendo que no es fácil pero si se quiere estar seguro y sobre todo si se tratan temas digamos importantes No si tratas temas financieros y Tienes muchas criptomonedas vigila con los sistemas y vigila que abres en esos sistemas Y si tienes aplicaciones que crees que puedan ser vulnerables actualízala antes de abrir algún archivo que te hayas descargado de algún sitio de dudosa reputación y finalmente no fiarse de las pruebas de concepto publicadas en internet este tema un poco más enfocado a aquellos oyentes que tengamos que sean más investigadores de seguridad lo mejor es analizar todo código descargado desde internet especialmente si es una prueba de concepto y bueno utilizar temas como virus total y similares no y si no se tiene esta capacidad de analizar eh si un tipo de código específico es malicioso No pues o o usar la ayuda de alguien o mejor no arriesgarse así que ya sabéis queridos oyentes ahora mismo cuando acabéis de escuchar el episodio y a vuestro winrar y actualizarlo ya mismo buah Qué recuerdos me has traído winrar yo llevo muchísimos años en los que no utilizo Windows pero creo que mi último Windows fue Windows 98 pero es que recuerdo que esa época el 95 el 98 Windows 2000 el primer Software que te descargaba era el winrar crack es que no fallaba porque aparte todo venía comprimido y y de aquella no venía por defecto algo instalado en el sistema operativo para poder descomprimir Entonces era un winrar y como era de pago crackeado es que no fallaba De hecho he visto alguna vez memes por ahí en plan haciendo referencia ostras breaking news Alguien ha pagado la licencia de winrar Qué bueno qué bueno la verdad es que es que me trae muchos recuerdos de aquellos juegos pirateados que te venían con un CD y y nada demandaba este famoso winrar y la verdad encontrar fallos es es también bastante curioso porque hoy en día no se ve demasiado archivo comprimido en este formato la verdad por lo menos lo que yo manejo y hasta aquí ha llegado el episodio queridos oyentes muchas muchas muchas gracias por quedaros hasta el final siempre un placer trabajar para vosotros para manteneros informados gracias por todos esos arios que nos dejáis en redes sociales en los episodios en Spotify en Apple podcast ayuda un montón nos da más visibilidad crecemos en los rankings lo cual se retroalimenta y más gente nos descubre por lo que más comentarios nos llegan por lo que más justificación tenemos para dedicar el esfuerzo que le dedicamos a esto Muchísimas gracias sois los mejores un gusto haber grabado otro episodio para nuestros oyentes y muchas gracias queridos oyentes por seguirnos otra semana más Muchas gracias por vuestro apoyo en las redes sociales y en internet en general Adiós adiós chao chao si te ha

gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio tierra de hackers