70. Metador y Hyperjacking

descubren un nuevo apt o grupos sofisticado de amenazas centrado en el espionaje y presente sobre todo en empresas telefónicas y universidades que tiene además un toque hispano un grupo de cibercriminales desconocidos ha estado infectando hipervisores umware sxy y robando datos de máquinas virtuales en una campaña de ciberespionaje digna de la bluepiel de Matrix una semana más que pasa y otro episodio más que publicamos y así hasta que os canséis de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 15 de octubre de 2022 este es el episodio número 70 yo soy Martín vigo y está conmigo desde la lejanía de su hábitat natural conocido como New York Alexis porros Hola Alexis qué tal Muy bien Martín aquí estamos ya un poco en modo otoño en modo Halloween y yo de hecho me he comprado unas cuantas de estas calabacillas Martín Si me las puedes ver en el vídeo que para Ah sí sí sí oyentes que siempre Martín y yo hacemos Nos vemos en vídeo Cuando hacemos el pues se la estaba enseñando por aquí Así que tengo la casa con unas cuantas de estas para estar en el en el modo Halloween y nada porque aquí las del rollito hojas están Están graciosas ya así de distintos colores tonalidades naranjas y tal y nada pues con ganas de hacer otro episodio contigo Martín y como siempre Muchas gracias a todos por nuestros oyentes por seguirnos en las redes sociales donde nos comentáis enviáis vuestras sugerencias preguntas noticias a que pudiéramos cubrir o no depende del tiempo pues a veces podemos y a veces no pero muchas gracias por seguirnos ahí os recordamos que deberíais estar suscritos a nuestro podcast en vuestra plataforma de escucha favorita si aún no lo estáis y recordaros que estamos en redes sociales Twitter Instagram y Facebook con el handel@tierra de hackers linkedinyoutube Twitch como tierra de hackers correos electrónicos nos podéis enviar a podcast@ tierra de hackers.com Y discord si el servidor de discord en tierra de hackers.com barra discord finalmente como siempre Muchas gracias por el apoyo a la pregunta del episodio por votar en Twitter y voy a comentar la última del episodio anterior que fue la siguiente cuando parecía que ya conocíamos a todos los jugadores del mundillo del cierre espionaje surgen más en este caso intelexa y todas sus empresas en relación a esto Qué medidas crees que podrían implantarse para limitar la proliferación de empresas de software espía teníamos cuatro respuestas como siempre la primera más votada con un 47% leyes internacionales más temilla internacional la segunda con un 28% más transparencia de tema legal de que empresas de este tipo se dedican al software espía la tercera más votada 22% más leyes de Ciber armas y la última con 3% de los votos más leyes de empresa el tema de este de que empresa madre crea empresa hija y se pierde un poco la trazabilidad perfecto Pues yo aprovecho para recordaros que somos candidatos a los premios ivoox os hemos creado aquí una una URL más sencilla por si creéis que merecemos vuestro voto tierra de hackers.com/premios y Box todo en minúsculas todo junto tierra de hackers.com/premios ivoox y estamos en la categoría de empresa y tecnología por si nos queréis votar que nos ayudaría un montón queremos aprovechar a dar las gracias a un nuevo mecena que tenemos Francisco Javier un mecena altruista Muchísimas gracias por tu apoyo es esencial para seguir adelante con el podcast Y por supuesto también como siempre a mona que siempre nos echa una mano en cada episodio una empresa que comparte los mismos valores de tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y morat a través de una empresa de una herramienta de gestión y visualización de telemetría de datos empresa fundada en silicon

Valley que busca muchos ingenieros como tú y ya sabes Te aceptan en remoto lo mejor de todo ya te digo es precisamente eso que podéis trabajar desde vuestra casita si queréis echarle un vistazo a su web monad.com m o n.ad.com y le podéis enviar el currículum a tierra de hackers @monat.com y yo creo que ya empezamos con la noticia os hemos hablado en varias ocasiones del concepto de apt apt es el acrónimo en inglés de Advance persistente lo cual podríamos Traducir como amenaza persistente avanzada esto de La amenaza persistente avanzada hace referencia a grupos de delincuentes muy sofisticados y conocidos que en ocasiones trabajan a las órdenes del gobierno de un país se diferencia de digamos cualquier otro grupo de delincuentes común como puede ser pues grupos de delincuentes centrados en ataques de ransomware en que sus ataques y capacidades son altamente sofisticadas es una de las diferencias suponen también una amenaza real por lo general a otro país o incluso a todo el mundo por eso se les denomina pues esto de que son atacantes avanzados no ejemplos de apetece conocidos pues son por ejemplo el lazarus Group el grupo de expertos a la orden del régimen norcoreano y que estuvo detrás del desarrollo y despliegue del ransomware wanna Cry o fanzibert el grupo de expertos informáticos insisto en no llamarles ciberdelincuentes por el tema de que trabajan para gobiernos Pero esto pues estos forman parte del gobierno Ruso y que se encargaron de hackear los servidores de hillary Clinton y desestabilizar las elecciones estadounidenses americanas lo que decía grupos de expertos en temas de hacking con mucho presupuesto muchos recursos y altamente sofisticados pues bien la noticia de hoy va sobre una investigación de sentinel One que ha publicado hace unas dos semanitas un reporte muy extenso y técnico sobre el Descubrimiento de un nuevo apt nunca antes visto y al que le han puesto el nombre de metador Y por qué le han llamado metador Pues porque al analizar el Software malicioso que utilizan para infectar la empresas encontraron en el código una referencia una frase I am meta o yo soy meta en inglés como parte del protocolo que utiliza y cuya respuesta que esperaba cuando no aparece nada pues está en español Así que en vez de matador pues le pusieron metador por el tema de metano eso es lo que Supongo yo vamos Me parece muy original Entonces yo pensaba que ibas a decir el protocolo dice hayan meta y el otro dice I'm door soy tu puerta Métete Sí bueno está el tema de matador rollos payol pero sí también podría ser por ahí pero luego se entra un poco más en el tema del protocolo pero sí no Solo han descubierto un nuevo apt sino que además hay referencias en el código malicioso a palabras y conceptos del mundo hispanohablante Así que como es nuestro deber y sobre todo con la curiosidad de esas referencias a nuestro idioma tenía que traeros la información al podcast la información habéis sacado del propio reporte técnico que os decía de sentinel One y que han publicado en su web y como no os dejo enlazado en las notas del episodio para que podáis ir a ver más detalles si queréis básicamente sentinel One tiene una solución de ciberseguridad que ayuda a empresas a detectar amenazas y curiosamente uno de sus clientes estaban el proceso de desplegar dichas protecciones cuando los investigadores empezaron a ver actividad que les llamó la atención el cliente estaba infectado como un software malicioso que se estaba actualizando para permanecer indetectable al software de sentinel One que el cliente justo estaba instalando esto lo detectaron los de sentinel One y les llamó mucho la atención y fue cuando empezaron a investigarlo y a mirarlo Pues un poco más a fondo uno de los detalles interesantes y llamativos fue el uso de un lolbin poco habitual para instalar qué es esto de un lolbing como siempre aprovechamos no la oportunidad para aprender algo nuevo en este podcast aunque alguna vez ya os hemos mencionado esto de los lolbings lolvin es el acrónimo de living of Land vinoris pensad que vuestro ordenador si por ejemplo tenéis un Windows viene con

muchísimos programitas preinstalados pensad por ejemplo que viene con un navegador no con un gestor de correo electrónico con un calendario etcétera Esos son los programas preinstalados Bueno más evidentes No pero hay muchísimos muchísimos más que forman parte de algo tan complejo como tu sistema operativo para llevar a cabo otras tareas que seguramente pues nunca has oído hablar de esos programitas no pero están ahí en tu ordenador Pues bien mediante la investigación de muchos expertos se van descubriendo algunos de esos programitas que vienen preinstalados y que tienen funcionalidades muy interesantes y muy útiles para un ciberdelincuente para llevar a cabo tareas sin que lo detecte por ejemplo pues un antivirus imaginaros que vuestro calendario el programa del calendario que viene en vuestro sistema operativo tuviera una funcionalidad que permitiese instalar software por lo que sea un atacante que haya accedido a vuestro ordenador se intenta instalar software malicioso directamente probablemente no pueda porque no tiene un usuario con privilegio suficientes para instalar programas O quizá pues antivirus lo detecte y lo evite directamente pero como si tiene permiso para utilizar la aplicación del calendario Ya que en principio pues es un programa normalito y sin peligro podría utilizar la funcionalidad del calendario de instalar programas y abusarlo para instalar su software malicioso pues este apt utilizaba un programita llamado cbd.exe que es el Microsoft consulty bagger para abusarlo e instalar el implante directamente en memoria sin que llegase a almacenarse en el disco duro es decir Windows te viene con este programita como te mencionaba y Tiene ciertas utilidades o funcionalidades que estos atacantes utilizan para instalar el software malicioso directamente en memoria en vez de incluso que esté presente en el disco duro que muchas veces los antivirus es donde buscan no otra técnica súper interesante que usaba era la conocida como portnocking os lo explico una vez has tenido un saludo Secreto con algún amigo cuando erais pequeños en plan os dais la mano con una combinación de movimientos que solo vosotros conocéis o por ejemplo lo típico de las pelis para entrar en una discoteca privada en la que para entrar tenéis que llamar a la puerta Pues con una secuencia de Golpes en la puerta secreta algo así no pues bien Esto básicamente lo hacen También los ciberdelincuentes para abrir las puertas dentro de su infraestructura una especie de Ábrete sésamo codificado para Ocultar sus servidores cuando el software malicioso intenta enviar información a los servidores de los delincuentes piénsalo por un minuto si tú eres un delincuente y tienes que tener tus servidores expuestos a internet lo ideal es tenerlos ocultos de investigadores que están constantemente barriendo o escaneando internet buscando ese tipo de servidores de gente maliciosa lo ideal es programar tu servidor para que nunca conteste a nadie a no ser de que le llamen con una secuencia secreta de Golpes en la puerta verdad así solo contestaría en ese momento esto en informática es a lo que nos referimos con portnoking se traduce a cuando te intentas conectar al servidor mandas una secuencia específica de paquetes con unas características específicas y con una pausa de milisegundos específica entre ellos el servidor los va recibiendo pero no contesta se queda mudo hasta que Recibe toda la secuencia correcta y en ese momento y solo en ese momento contestará y se establecerá la conexión permanente en el caso de malware de matador el servidor se comunica con el implante tras esta secuencia para que os hagáis una idea se conecta a un puerto que está predeterminado luego a ese número de Puerto más 7 es decir si el puerto que se determinó pues es el puerto 80 pues acto seguido se conecta al 87 luego se conecta al 83 es decir el puerto más tres Y estos tres paquetes se envían Con un retraso entre ellos de exactamente 200 milisegundos luego espera un segundo y después de ese segundo Exacto vuelve a mandar un 9 paquete Pero esta vez a un puerto en concreto que es el 31.443 a partir de aquí ya se puede establecer la conexión y

empieza la comunicación pues esta es la técnica de portnoking que utiliza matador el apt también protege quería comentar si has dicho el pornoking en tema de tiempos Pues me alegro que le funcionara Porque si hay tema de latencia un poquito sabes igual esos 200 milisegundos que están para que llegue ese patrón no de sincronización de que se autentica que es el que el cliente que es lo yo he visto también otras técnicas de pornoking que en lugar de basarse en el tiempo también por Añadir algo utilizan una clave digamos una clave o algo en el paquete en signos cabeceras no del pelo digamos pero no sé en el tcp header o en el udpg de la cabecera tcp odp pues se añade algo de contenido único como si fuera una clave que solo conoce el cliente y el servidor en este caso para autenticarse así que por si el tema del de los 200 milisegundos o así no funcionará porque hay mucha latencia Pues sería otra forma de implementar pornoking sí a veces y no no recuerdo exactamente si si es con este incluso es en la red local que se comunican así entonces es cierto que ese retardo de 200 milisegundos pues puede ser más preciso no pero sí es el punto que me imagino que habrá un poco de margen de error pero en general 200 milisegundos es bastante cuando se trata de tráfico de internet Entonces a lo mejor pues en el reporte Lo ponía así pero se refieren a un mínimo de 200 milisegundos o algo así Algo que está digamos fuera de lo habitual no el apt también protege bien todos sus software malicioso al fin y al cabo desarrollar este tipo de implantes y sichus tan avanzados requiere tiempo y recursos Los investigadores comentan que el apt utiliza técnicas avanzadas de ofuscación para dificultar aún más la tarea de ingeniería inversa no Quiero meterme aún más en lo técnico porque nos gusta que tierra de hacker sea para todos los públicos Pero espero que os haya parecido interesante aprender sobre distintas técnicas utilizadas en el desarrollo de programas maliciosos volviendo al tema de los lazos de este grupo digamos con con el habla hispana no me resultó a mí personalmente súper curioso Los investigadores que analizaron el software encontraron referencias a Mafalda de hecho es así como llaman a su plataforma Mafalda muchos lo conocerán es un personaje de un famoso cómic argentino de una niña que hace críticas burlonas normalmente sobre política por otro lado cuando el implante Mafalda intenta comunicarse con el servidor de los atacantes y recibe una respuesta vacía esto que comentaba al principio el protocolo responde con la palabra nada pero esto no es lo único curioso que encontraron los investigadores analizando el software Encontraron la letra de un grupo británico llamada the sisters of Mere esto lo dejaron directamente los programadores en el código parece que a propósito y dice lo siguiente gerais her voice o escobalt blue o algo así como sus ojos eran de color rojizois y su voz era de color azul algo que me llamó la atención de esta frase es la palabra Cobalt junto con los colores rojo y azul las tres palabras tienen un significado muy fuerte en el mundo de la ciberseguridad Cobalt puede ser de cobalt-strike una aplicación utilizada profesionalmente por pentesters que intentan hackear empresas como parte de su trabajo por ejemplo lo que hago yo y que en realidad es muy parecido a lo que han implementado Este apt no es muy parecido a esta pieza de malware Solo que ellos lo usan evidentemente de manera maliciosa y luego pues los colores rojo y azul pues se podría ver como el reptil y el bluetooth que tantos hemos contado no aquello de que el retiene el Equipo Rojo se dedica a la parte ofensiva y el bluetooth el equipo azul a la parte defensiva Pero bueno hasta aquí anécdotas curiosas y desde luego el tema de Mafalda me parece súper Interesante pero a qué se dedica este nuevo apt que acaban de descubrir pues como decía lo acaban de descubrir y un tema que menciona los investigadores es que son muy buenos con su seguridad operacional utilizan infraestructura completamente nueva para cada objetivo por lo que resulta muy difícil encontrar otras víctimas de sus ataques muchos grupos reutilizan la misma infraestructura para varias víctimas por lo que si

los descubres en uno de tus clientes por ejemplo pues puedes observar si la ip de sus servidores por ejemplo ha sido contactada desde otras empresas y pueda desconcluir que también están infectados Esto no es el caso del grupo metador que siempre utilizan todo nuevo básicamente aún así encontraron datos y mencionan que este grupo se centra mayormente en comprometer empresas de telefonía y proveedores de internet y la mayoría de su actividad la han visto en África y Oriente medio esto de telefonía y proveedores de internet es el típico objetivo de gobiernos porque facilita muchísimo las tareas de espionaje de hecho y aquí Vais a flipar los investigadores hablan del concepto de magnet of strikes o imán de amenazas para referirse a empresas e industrias que tienden a traer atacantes muy sofisticados por el valor que tienen Pero eso no es todo atraen tanto interés que han visto en varias ocasiones incluidas cuando investigaron este caso que es habitual encontrar no Uno sino varios apts dentro de los servidores de una misma empresa Esto es lo mismo que si un ladrón entra a robar un banco y se encuentra allí a otros tres grupos de ladrones robando también lo mejor de todo es que según Los investigadores se respetan entre ellos mismos y no intentan sabotearse honor entre ladrones supongo Martín Me parece muy interesante sobre todo el final pero quería mencionar primero que a Mafalda la conozco obviamente a esa canción No pero el tema de cover strike sí obviamente como has dicho lo usamos tanto tú y como yo y Blue y pues claro somos parte de eso del Purple y el tema del honor entre entre cybercriminales me ha parecido curioso que lo mencioné en el informe que que haya este tipo de honor porque yo a veces he leído algunas otras noticias en las que al revés se aprovechan no sé si eran la voz net mirai Pero había una de estas botness en las que bueno el ataque el atacante inicial infectaba los dispositivos estos de red con el con el tema este de mirai y creo que había otro que había otra vulnerabilidad y o las credenciales por defecto en este en esta bonet y entraba y echaba al otro que había antes Bueno y se iban quitando el acceso unos a otros así que bueno en este caso igual Pues igual son parte de un mismo un mismo gobierno y Oye igual son diferentes partes uno que hace tema de más infección y otro hace tema más de exiltrar datos no sé pero me parece interesante que que haya honor hay entre cibercriminales sí sí sí justo lo que dices tú muy buen apunte el tema de que en general también pues se echan unos a otros de hecho a veces parchean no las vulnerables una vez lo tienen infectado parchean la vulnerabilidad que habían explotado Pero ellos ya tienen puesto su software malicioso y así no dejan entrar a los demás por un lado te hacen el favor Pero por otro se quedan ahí dentro Pues en este caso es eso mencionaban que bueno que no se molestaban unos a otros que aquí hay material para todo el mundo y no y no hay fallo bastante curioso Pues sí pues muy buena Martín y bueno seguimos adelante y queremos hacer un breve inciso para darle las gracias a nuestro patrocinador brawler que nos apoya en el podcast y que Hace unos días acaba de lanzar un servicio en la nube para proteger tu infraestructura en aws hablamos de brawler pro y sus ass el servicio gratuito más completo de seguridad para aws brawler Pro está construido sobre la Popular herramienta opensores frawler y además por el mismo equipo de ingenieros si ya conoces frawler que está disponible en github seguro que vas a aprovechar las bondades que ofrece brawler Pro en cuestión de minutos tendrás resultados del estado de seguridad de tu cuenta de aws podrás mejorar tu postura de seguridad a través de múltiples dashboards que te permitirán ahorrar tiempo y tener una visión completa del estado de tu infraestructura puedes empezar a usar brawler pro de forma totalmente gratuita en brawler.pro PR o w l e r punto PR o desde ya y bueno una vez dicho esto dentro la siguiente noticia esta noticia va del concepto de hyper jacking ahora voy a entrar más detalle en A qué se refiere esto pero es que a finales del mes pasado la empresa de seguridad Mandy ahora propiedad de Google y la empresa de virtualización vmware publicaron

conjuntamente advertencias de que un sofisticado grupo de amenazas desconocido ha estado instalando puertas traseras en el software de virtualización de vmware en redes de múltiples objetivos como parte de una campaña de espionaje antes de entrar en detalle y como aquí queremos desde tierra que es educar a todos un poquito de temas de tecnología y sobre todo de ciberseguridad voy a comentar brevemente qué es esto de virtualización pues la virtualización es el concepto de crear una versión de algo basada en software o en un modo de forma virtual o de forma digamos a un nivel abstracto la virtualización no es un concepto nuevo ya que empezó a usarse en el 1960 la década de los 60 como un método de dividir de forma lógica los recursos físicos digamos procesador memoria almacenamiento y similares de los sistemas Main frame entre los diferentes programas que se ejecutaban en el mainframe aunque se ha hecho muy popular a nivel sobre todo de usuario en los últimos 20 años con empresas como vmware que que se lanzó en 1998 el software hyper B de Microsoft que se lanzó allá en el 2008 y otros proyectos opensores como virtualbox y kvm que es un hipervisor un hipervisor es un software que virtualiza es decir simula componentes Hardware como la el procesador memoria lector de CD d incluso los directores de discate O floppy sí algunas algunos sistemas operativos todavía tiran a algunos algunos datos algunas algunos historias de algunos archivos de disquetes virtuales digamos también el teclado del Ratón para crear un sistema virtual hay dos tipos de hipervisores el tipo 1 y el tipo 2 el tipo 1 se llama digamos ver metal que corre directamente en en metal en un servidor físico y el tipo 2 que se le llama hosted o alojado del tipo 1 tendríamos vmware sx y Microsoft hyper b o el opensores kvm y de tipo 2 tenemos virtualbox y vmware workstation una máquina virtual es el otro componente porque he mencionado que tenemos hipervisores y ahora tenemos las máquinas virtuales son sistemas basados en Software que de hecho corren encima del hipervisor y se recorrer múltiples sistemas virtuales encima de un hipervisor que es el encargado del questrar y asignar los recursos físicos limitados del servidor físico por ejemplo un sistema físico digamos basado en Windows Linux o maco ese podría correr múltiples sistemas virtuales digamos uno con Windows 10 otro con Windows Vista si alguien le gusta otro con Windows 95 y bueno otros con Linux el que sea red Hats suse o incluso con maco s las máquinas virtuales tienen mucha flexibilidad porque se pueden migrar de un hipervisor a otro con mucha facilidad Y de forma casi instantánea los beneficios son múltiples ahorro de costes No porque se reducen entre estructura física la electricidad de mantenimiento tienes también mejora de rendimiento agilidad y velocidad porque puedes instalar y desplegar sistemas mucho más rápido y deformado más fácil que en entornos físicos los desarrolladores pueden crear sus entornos de desarrollo y máquinas de desarrollo y tienes menos dis en el servicio Se podría decir porque como digo puedes migrar máquinas virtuales que estén fallando a otros hipersores para Que corran ahí han habido sobre el ataque que he mencionado al introducir la noticia han habido ataques similares en el pasado pero fueron más académicos y más teóricos No teóricos pero lo implementaron pero fueron más se quedaron digamos en el aire y no los vimos como ataques en la realidad y todo esto empezó desde el 2006 ya cuando se hablaron de potenciales ataques contra esta tecnología de virtualización hubieron dos de estos ataques teóricos que uno a uno lo llamaron hyper virus y otro le llamaron Blue pill el objetivo de estos ataques era que los usuarios maliciosos que desplegaron estos ataques podían secuestrar la plataforma de virtualización para espiar y manipular máquinas virtuales sin que la máquina virtual en sí la máquina virtual atacada se puede dar cuenta de la intrusión como he dicho al introducir la noticia este concepto se le conoce como hyper jacking que es el concepto de secuestrar el hipervisor y controlar las máquinas virtuales en un artículo de 2006

Los investigadores de Microsoft y la universidad de Michigan descubrieron la posibilidad de que atacantes pudiera instalar un hipervisor malicioso al que llamaron hipervirus en una máquina objetivo que coloca la víctima dentro de una máquina virtual ejecutada por el atacante sin el conocimiento de la víctima al controlar ese hipervisor malicioso todo en la máquina de destino estaría bajo el control del atacante sin señales de la intrusión dentro del sistema virtualizado la única desventaja de este ataque es que necesita reiniciar el sistema objetivo algo que no pasaría desapercibido la investigadora de seguridad Johana rutkowska es la que publicó su propia versión de este ataque de hyper yaquin y lo llamó ataque de Blue pill que a diferencia del ataque hipervirus no requiere que se reinicie el sistema con lo que lo haría un ataque mucho más sigiloso Blue pill en este caso o píldora azul es claramente una referencia a la película de Matrix en la que las personas en Matrix viven una realidad simulada ajena al mundo real y es en la escena en la que Morfeo confronta Neo para que voluntariamente elija aprender la verdad inquietante del mundo real eligiendo la píldora roja o permanecer en la ignorancia satisfecha eligiendo la píldora azul Pues cuando se da este este caso de la píldora azul y desde aquí es donde Joana pues cogió prestado el concepto Llamar a su ataque en este ataque de hecho en el bluepiel las máquinas virtuales atacadas siguen sumidas en su ignorancia satisfecha aunque esto también es por diseño no se puede hacer mucho para tomar la píldora roja por parte de máquinas virtuales porque de la forma de que está diseñado un hipervisor las máquinas virtuales no tienen acceso a digamos pueden tener conocimiento de que están virtualizadas porque hay indicadores en un sistema virtualizado de que Hay ciertos componentes en el registro o algunos dispositivos que se pueden listar digamos pero no se puede digamos interactuar con el hipervisor como digo en estos ataques teóricos un atacante tiene que crear un nuevo hipervisor sin el conocimiento de la víctima y migrar los sistemas de la víctima al hipervisor controlado por el atacante mientras que en los casos descubiertos por mandiant los ataques que hemos visto ahora en la realidad los cibercriminales simplemente la infraestructura de hipervisor existente de vmware sxy sin tener que reiniciar y instalaron componentes extras de hipervisor que contienen el malware aclarar que en ambos casos teóricos pasados e incluso en el ataque actual no se ha abusado de ninguna vulnerabilidad parcheable del Software de virtualización de umware es decir no han habido ningún cero Dei involucrado en este ataque sino que los atacantes abusaron de una funcionalidad de vmware esxy que permite instalar nuevos componentes al hipervisor en este caso ellos lo abusaron para instalar malware Esta es una técnica mucho menos compleja de ejecutar y mucho más fácil comparándola con los ataques teóricos del pasado que requerían como digo crear un nuevo hipervisor pero aún así es altamente efectiva y con esto llegamos a la actualidad en cualquier caso quiero comentar que estos ataques han saltado de los trabajos de investigación de hace años a ataques rea llevados a cabo por un grupo de Ciber amenazas desconocido que ha atacado a 10 empresas entre Estados Unidos y Asia esto es interesante no porque muchas veces lo vemos en películas de ciencia ficción o hay estudios académicos de un nuevo ataque que a veces muy rápidamente se ve en ataques en la realidad pero en este caso ha tardado ha llevado un tiempo en verse De todas formas mandin también dice que aunque este es el primero probablemente como los cibercriminales comparten conocimiento entre ellos probablemente vayamos a ver más ataques de este tipo en un futuro al inyectar su propio código malicioso en los supervisores de las víctimas los cibercriminales pudieron observar y ejecutar comandos de manera invisible en las máquinas virtuales que supervisan esos hipersores y debido a que el código malicioso afecta al hipervisor en la máquina física en lugar de las máquinas virtuales atacadas las máquinas virtuales no pueden

darse cuenta las mismas de este ataque de todas formas hay que decir que si el código malicioso del hipervisor ejecuta comandos contra una máquina virtual que corre algún tipo de software de seguridad como un en Point detection en response un edr idear de estos o un antivirus o similares estos sistemas de seguridad podrían detectar los comandos y bloquear alertar al respecto también mencionar Que obviamente las máquinas virtuales pueden tener activados el la recopilación de logs de registros que pueden estar enviando a otros sistemas Así que esto también lo podría podrían verse los ataques de esa forma mirando los blogs aunque los comandos maliciosos también podrían desactivar el tema del login no según mandian estos actores amenazas han utilizado implantes malware contra hipervisores de umware nunca antes vistos Según dicen esto estas técnicas es muy novedosa y de hecho mannien se refirió a estos nuevos implantes maliciosos un ecosistema de malware novedoso que afecta no solo a vmware sxy sino que también a servidores Linux V Center y máquinas virtuales de Windows lo que permite a los atacantes mantener un acceso persistente al hipervisor ejecutar comandos arbitrarios y transferir archivos entre el hipervisor y las máquinas virtuales sobre el ataque mencionar que el vector de acceso inicial o la infección inicial no se conoce con exactitud pero se sabe que no fueron relacionadas con vulnerabilidades en vmware una vez los cibercriminales tuvieron un pie en la red identificaron y robaron las credenciales de administrador de vmware mediante acciones típicas de seguridad ofensiva enumeración de sistemas movimiento lateral explotación de alguna vulnerabilidad o configuración incorrecta extracción de contraseñas en claro de la memoria o hashes para rehusarlos y cuando tuvieron las credenciales que necesitaban las usaron para iniciar sesión en los servidores esxy después de eso los cibercriminales instalaron paquetes de instalación de BS fear o vs fire que se llaman v y b son las el acrónimo en inglés que contenían malware contenían rutinas maliciosas y lo instala esto lo instalaron en el sistema que corre en el sistema propio sxy comentar que sxy tiene capacidades para prevenir la instalación de este tipo de paquetes de instalación para beast fear con firma digital inválida Porque estos paquetes están firmados digitalmente pero en la configuración por defecto este control se puede saltar con un flag que sería Force y es lo que de hecho los atacantes utilizaron el instalar estos paquetes o componentes adicionales en vmware sxy les permitió ocultar dos puertas traseras diferentes que manden ha llamado virtual Pita y virtual Pay o pie en el programa de hipervisor de vmware conocido como sxy bueno y va a comentar sobre lo anterior pero me encantó lo de virtual Pita Mira tenemos más falda ya para decir tienen que ser de habla hispana seguro y con esto de Pita pues tienen que ser indios seguro lo de esto nada quería decir según enumerabas tío es que flipo eh todo lo que cuentas porque muchas veces hablamos de 0 days en dispositivos móviles no y lo complicado que puede llegar a ser encontrar en teléfonos de Apple o incluso en sistemas operativos como Android hoy en día ya también pero es que encontrar vulnerabilidades en sistemas de virtualización sobre todo por el peligro que tendría porque hoy en día todo el mundo tiene su ordenador en la nube es algo algo que que hay que pararse a pensarlo y se paga también por los millones por vulnerabilidades de este tipo y todo lo que estás contando de lo que se llega a lo que llegaron a conseguir me parece espectacular hay un nivel de sofisticación espectacular sí lo que dices de la nube justo lo voy a comentar un poco más adelante en el tema de impacto porque los sistemas de virtualización al principio bueno pueden correr a nivel de usuario no en nuestros macs en nuestros peces portátiles pero como dices lo utilizan mucho los proveedores de la nube porque les permite como he dicho antes abaratar costes tener más flexibilidad desplegar sistemas mucha más rápido y migrar sobre todo cuando tienen que hacer balanceo de carga y similares pues les ayuda mucho

pero sí sí buen apunte y pues con el Virtual Pita y el Virtual Pay que tenemos Spy bueno como dice Martín Pita es el pan este indio y Pay también bueno en inglés es un es un pastel así que tenemos un poco de pan y un poco de pastel nos falta el champán para brindar el con el ataque Pues nada como digo estas puertas traseras permiten que cibercriminales vigilen las máquinas virtuales y ejecuten sus propios comandos en máquinas virtuales administradas por el hipervisor infectado mann dice que los cibercriminales en realidad no explotaron ninguna vulnerabilidad parcheable como he dicho antes ningún cero Dei sino que utilizaron el acceso de nivel de administrador a los supervisores sxy para plantar sus herramientas de espionaje y de hecho este acceso administrador también sugiere que esto les facilitó un acceso persistente también y que les permitió ocultar su espionaje de manera más efectiva a largo plazo después de obtener el acceso inicial e infectar estos sistemas comentar brevemente estos componentes del malware virtual Pita virtual pay y luego hay otro componente que no es realmente malware digamos de acceso pero se llama virtualgate y les da acceso a máquinas virtuales de tipo Windows no pero Empiezo con el Virtual Pita como he dicho anteriormente afecta a gume water sxy y Linux vcenter estos hipervisores y viene con capacidades para ejecutar comandos así como para cargar y descargar archivos virtual Pay que es también para webs x y Linux Center es una puerta trasera de python compatible con funciones de ejecución de línea de comandos transferencia de archivos También incluye un componente que es una shell reversa o inversa con protocolo personalizado y cifrado rc4 virtualgate es un proceso que se instala en máquinas virtuales Windows en el directorio c Windows temps y el nombre del archivo es avp.exe y esto permite a las máquinas virtuales atacadas usar los sockets los canales de comunicación de la interfaz de la máquina virtual de vmware para ejecutar comandos en una máquina virtual desde el Host hipervisor es decir es un canal de comunicación que se abre para que el hipervisor infectado pueda comunicarse y ejecutar comandos en una máquina virtual Windows Cuáles eran los objetivos de este apt desconocido pues como he dicho antes el espionaje No pero en concreto lo que hicieron fue robar archivos de máquinas virtuales y también volcar credenciales de máquinas virtuales a través de volcar la memoria con minidam y la lectura de bases de datos de equipas también buscaron estos estos contenedores de credenciales Cuáles son los beneficios o los miedos digamos para los beneficios para el cibercriminales y el impacto que tendría para nosotros usuarios y organizaciones pues este tipo de malware permite controlar múltiples máquinas virtuales a escala porque infectado un hipervisor normalmente corren muchas máquinas virtuales tienes acceso a muchos sistemas el tema es que no en principio no es fácilmente identificado por sistemas de seguridad que corren en las máquinas virtuales como he dicho antes no no se tiene conciencia de estos ataques a no ser que se ejecute algún Comando directamente en los sistemas virtualizados y se tenga el login activado y similar espero como el hipervisor tiene mayor prioridad corre con privilegios elevados que sería otros de los beneficios pues podrían desactivar el ideal antivirus tema de login y todo esto el tema de la persistencia también porque Bueno al como los supervisores corren con altos privilegios Pues bueno se puede tener persistencia y control total del sistema y el tema también de saltarse sistemas de seguridad no solo en las máquinas virtualizadas sino también en la plataforma que corre el hipervisor en este caso es xy porque no hay en principio muchos o ninguno pues soluciones de detección y respuesta de Punto final en detection en response y tampoco hay antivirus digamos que corran al menos en esta plataforma sxy al menos no por el momento lo mismo pasa con dispositivos de red no routers firewalls y temas similares tampoco corren este tipo de software de sistemas de seguridad Así que es un tema que también es un beneficio que les

permite estar infectar los sistemas sin ser detectados y bueno tener persistencia por mucho tiempo hay una limitación Y de nuevo Resaltar que de nuevo no es una buena habilidad que se haya abusado no es un cero Dei y requiere tener privilegios de administrador para poder instalar estos paquetes maliciosos en el hipervisor sxy sobre la atribución mandian identificó a estos cibercriminales a principios de este año Pero ha comunicado no lo ha hecho público hasta el momento Supongo que estarían investigando a las diferentes empresas afectadas y umware también por su parte investigando si realmente es una vulnerabilidad o no pero comenta que el malware se implementó en 10 organizaciones en América del Norte y Asia aunque como he dicho antes se espera que el número aumente a medida que bueno primero que los cibercriminales sepan de esta nueva técnica y que las empresas también tengan conciencia y vayan a inspeccionar sus logs su infraestructura de vmware y vean si tienen sistemas infectados dado el bajo número de infecciones no está claro si los ataques están dirigidos a un sector específico en este momento pero los ataques se han atribuido a un grupo de amenazas emergentes sin categorizar con nombre en código según mandient umc 3886 cuya motivación sea probablemente el espionaje dadas las actividades que han realizado en los sistemas comprometidos sobre el país de origen mandiant dijo que podría tener un nexo con china Aunque el nivel de confianza de este argumento es bajo y se basan en un análisis de las víctimas del grupo cibercriminal y algunas similitudes entre su código y el de otro malware conocido el nivel del alcance el impacto pues hay que decir que más de 400.000 clientes utilizan la tecnología los servicios de umware incluido el 100% de las empresas fortune Five hundreds y el 100% de las empresas fortune global 100 en las configuraciones en las configuraciones de virtualización Normalmente se pueden ejecutar de 2 a 5 máquinas virtuales en cualquier computadora física y a menudo hay miles de máquinas virtuales en la red de una organización que Ejecutan sistemas de todo tipo No desde servidores hasta sistemas de usuario hasta bueno temas de correo electrónico cualquier tipo de servidor el tema de que infectando a una máquina puedes tener acceso a muchas otras como he dicho hay en Casos normales de 2 a 5 pero en Casos mayores que tienen mucha más capacidad a nivel física estos hipervisores pueden estar corriendo cientos e incluso miles de máquinas virtuales Pues esta capacidad de amplificación del impacto es muy preocupante y por tanto el impacto es grande y bueno uno puede pensar yo no creo que me vaya a infectar No yo no soy importante o si lo soy uso precauciones uso sistemas de seguridad pero como ha mencionado Martín anteriormente no que hay de las empresas de Hosting o en la nube en las que corremos nuestros sistemas páginas web bases de datos todo hoy en día corren plataformas de virtualización o casi todo hoy en día exceptor el hipervisor no que tiene que correr en en Hardware en sistema físico así que por este motivo nos pareció muy importante traer esta noticia al podcast para que todos tengamos algo de conciencia al respecto umware y mandian publicaron ciertas medidas de seguridad al respecto publicaron temas de detección y temas de prevención a nivel de detección mencionar el tema de activar el uso de los blogs en sxy para identificar la instalación maliciosa de estos paquetes también mencionaron que los atacantes manipular un poco el tiempo para evitar que se vieran en los blogs cuando estuvieron instalando malware también el propio malware dejó artefactos a nivel de registro que se pudieron para identificar la infección y también la interacción con las máquinas virtuales esto también deja registros que se pudieran ingerir por un shock y alertar al respecto también mencionan que se debe activar a nivel de sxy la verificación de firmas digitales de la instalación de estos paquetes maliciosos que es el componente principal que los cibercriminales abusaron para instalar el malware y a nivel remoto de forma remota también se puede pues

dampear volcar la memoria y correr digamos reglas de yara que se han definido para identificar este este ataque a nivel de prevención comentan el tema de aplicar parches de seguridad el tema de usar secure Boot envía el chip tpm trasted platform que es digamos un chip Hardware que contiene claves criptográficas para el inicio de sistemas esto lo se utilizaría para como he dicho prevenir que los atacantes pudieran instalar estos paquetes maliciosos que tienen firmas digitales inválidas el tema de poner a todos estos sistemas sxy en su propia segmentado del resto de la red para que no tengan acceso directo los atacantes temas de gestión de identidades y credenciales pues comprometieron estas credenciales Pues que haya un tema de doble factor que se gestionen a nivel en sistemas de Access management que se gestionen de forma segura en un contenedor y temas de jardín pues Deshabilitar servicios innecesarios y que solo se puede acceder a estas máquinas desde el Center server Bueno y con todo esto llegamos a la pregunta del episodio A qué nivel crees que puede afectar este ataque llamado hyper yaquin o secuestro de hipervisor a usuarios normales como tú y como yo tenemos cuatro respuestas la primera es nulo o no uso virtualización la segunda es moderado corro máquinas virtuales en local en mi sistema en casa la tercera también es moderado pero en este caso mis máquinas virtuales corren en la nube y la última opción es elevado vivo en Matrix es decir toda mi vida Corre virtualizado muy interesante la pregunta otra cosa que me trajiste a la mente hablando de todo el tema de vulnerabilidades en máquinas virtuales había sido yo creo que lo llegamos a cubrir hace hace quizá un año quizá un poco menos está este exploit que crearon en sistemas de iOS en el que creaban una máquina virtual explotando la vulnerabilidad para luego poder crear un implante y poder controlar los iphones era una auténtica locura se habían desarrollado a través del exploit no perdón a través de la vulnerabilidad la una máquina virtual para poder ejecutar código y vais pasear de protecciones y elevar privilegios una locura sí la verdad es que eso añadió Supongo una capa de complejidad a la que los sistemas de seguridad no no tenían capacidad de inspección Entonces era una forma de añadiendo una capa adicional me salto los sistemas ddr y antivirus si es interesante interesante ese ataque también sí porque ese plan como ya acañonazos no ahí matar moscas a cañuelas me Monte una máquina virtual en tu iPhone para poder by pasear protecciones una pasada pues pues bueno hasta hasta aquí ha llegado el episodio por hoy recordad por favor que si creéis que lo merecemos nos podéis votar para los premios ivoox en tierra de hackers.com premios ivoox todo junto y eso lleva un formulario donde podéis votar a un montón de podcast en diferentes categorías incluido el nuestro que estamos en empresa y tecnología quiero recordar nos buscáis ahí tierra de hackers El formulario es así un poquito un poquito raro pero ahí nos tenéis y agradeceríamos muchísimo vuestro voto insisto si creéis que lo merecemos también por favor ayudarnos a seguir creciendo compartir el podcast con vuestros amigos hacerlo un favor educarlos en el tema de ciberseguridad a través de nuestro podcast recordar también que estamos un montón de gente yo creo que ya casi 800 en nuestro canal de discord compartiendo noticias con buenos debates podéis entrar en tierra de hackers.com/discord y bueno eso Muchísimas gracias por apoyarnos seguir compartiendo el podcast y a seguir creciendo esta comunidad tan guapa que estamos creando entre todos Sí sí como dice Martín un poquito un minutillo o dos que yo decía 5 segundos de vuestro tiempo para votarnos no sé ayer nos ayudaría un montón y como dice Martín a concienciar a la mayor gente posible no solo a vuestros compañeros sino a vuestros a vuestros jefes a vuestras empresas y también a esos proveedores de la nube porque este ataque de hyper jackeline es muy interesante y probablemente pueda afectar a mucha gente pues nos vemos y nos escuchamos en el próximo episodio como siempre adiós adiós adiós 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