tenemos nuevo ataque a cadena de suministro por parte de un atacante muy avanzado técnicamente que será quién será los documentos filtrados Vulcan files dan una visión única de una empresa oscura que ofrece servicios ofensivos y de inteligencia en el ciberespacio al gobierno ruso incluyendo el Gru el fcb y el archiconocido grupo sandward Iván 33 son los años que llevamos contándote sobre lo que acontece en el mundo en torno a la ciberseguridad y aquí Seguiremos como mínimo tres años más estás en tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 19 de abril de 2023 este es el episodio número 91 yo soy Martín vigo y está conmigo de celebración cumpleañera del podcast Alexis porros Hola Alexis qué tal pues muy buenas Martín muy contento y muy buen Feliz cumpleaños tierra de hackers y queridos oyentes Ya llegamos al tercer año desde que empezamos Parece que fue ayer le hemos echado una de horas y otros supierais pero seguro que lo sabéis porque nos seguís episodio tras episodio crear recapitular brevemente las estadísticas tres años 90 episodios con este 91 unas 200 noticias y más de 135 horas de Martín y yo dándolos dándoos la vara con todo lo que pasa en el mundo de la ciberseguridad y muchas gracias por estar con nosotros año tras año queridos oyentes no escuchándonos sino también conviviendo con nosotros online donde nos enviáis vuestros mensajes sugerencias mejoras y demás seguir así la verdad os necesitamos necesitamos vuestro feedback cada semana para mejorar Así que comentarnos en todas las plataformas y redes sociales y sobre todo en las plataformas de podcast también lo que os parece bien Lo que podríamos mejorar y así os apreciamos mucho todos esos comentarios y para aquellos que no que no estén al tanto que se hayan Unido hace poco o que estén algo despistados recordar que estamos en todas las redes sociales más populares como tierra de hackers o arroba tierra de hackers en todas las plataformas decentes de podcast si no lo estáis rápido ida suscribiros y tenemos un servidor de discord al que podéis acceder vía tierra de hackers.com barra discord y lo de siempre de final de la intro agradecer vuestro apoyo a la pregunta del episodio que publicamos en Twitter y que la del anterior fue la siguiente Cómo ocultas las partes de las fotos que contienen algo que no quieres enseñar antes de subirlas a internet tenemos tres respuestas posibles la más votada con un 55,3% fue un no subo este tipo de fotos seguida con un 32,4% de las edito con el móvil y finalmente un 12,4% para las tapo físicamente y sí tres años ya de podcast la verdad es que es una una locura la verdad yo cuando empezamos no pensaba que llegaremos tan lejos pero es que además con las cifras de oyentes y cobertura mundial que tenemos una auténtica pasada apoyo por parte de sponsors apoyo por parte por parte de oyentes la auténtica felicidad la verdad y venimos con sorpresas para para el episodio 100 que tenemos ganas de hacer más cosillas muy bien y yo por mi cuenta pues darle las gracias a escenas de patrón que cada día somos más Muchísimas gracias por vuestro apoyo y a prowler Pro la herramienta más completa de seguridad en aws empresas de todos los tamaños se apoyan diariamente en brawler pro para que sus equipos puedan confiar en su modelo de seguridad de aws puedes probar para lo mismo y de manera totalmente gratuita y vas a obtener paneles y gráficas con información concisa y accionable con todo lujo de detalles sobre la madurez de tu modelo de seguridad y además una visión completa de tu infraestructura en todas las regiones de aws y tendrás todos los resultados en apenas unos minutos empieza a usar brawler pro y benefíciate de sus resultados visitando tierra de hackers.com/uler Pro mencionamos también una cosa para ser totalmente transparente con vosotros Alexis y yo no estamos grabando esto a la vez hoy en el pasado nos habéis comentado como a veces Alexis y yo el episodio digamos pierde un poquito de interactividad habíamos explicado que a veces Alexis y yo por tema de tiempos de vivir en diferentes partes del mundo con diferentes zonas horarias no podemos grabar a la vez pasa muy poco intentamos reducirlo A lo mejor una vez cada tres meses pero está claro que vosotros lo notáis entonces en vez de

utilizar La magia de la edición para que parezca que Alexis y yo estamos grabando a la vez lo que hacemos lo que vamos a hacer esta vez es ser totalmente transparentes Así que esto lo estamos grabando por separados pero intentamos que sea lo más fluido posible Así que es por eso que quizá No vais a ver tanta interacción con entre Alexis y yo mientras damos la noticia dicho esto y con la verdad por delante como no empezamos con mi noticia y esta noticia que os traigo Es de un incidente muy grave de seguridad que ocurrió hace varias semanas os va a traer un recuerdo a solar Wings un retrogusto a casella un post paladar a Leon y un tubisio a toda noticia que hemos sobre supply Chain attacks o ataques a cadenas de suministro 3dx es la última en sufrir un incidente de seguridad que ha afectado a sus millones de clientes una vez más en vez de infectar a las empresas en Sí estamos viendo el trends no de infectar a una empresa cuyo producto es utilizado por miles de empresas en todo el mundo e infectarlas de ese modo a escala 3D x es una empresa dedicada al desarrollo de software de telefonía concretamente a lo que se conoce como soft fones o software de telefonía a través digamos la capacidad de hacer llamadas telefónicas a través de software algo así parecido a Skype no que puedes hacer llamadas telefónicas no te hablo de hacer una llamada de WhatsApp a Whatsapp o una videollamada en zoom sino de llamadas a teléfonos pero que se puede hacer desde Skype que tú marcas el número de teléfono pero evidente tú estás llamando desde un software no no desde otro teléfono físico lo que pasa es que todo esto a nivel mucho más profesional y a nivel empresarial el famoso bitube no que le dicen eso es lo que hace 13 x y yo te pregunto querido oyente qué empresa sobre la faz de la tierra no requiere detener teléfonos la mayoría de las empresas de hecho tiene un teléfono sobre cada escritorio de cada empleado Yo apenas lo he usado en mi vida pero en todas las empresas por lo menos donde yo trabajaba siempre tenía mi número de mi teléfono físico en mi escritorio con mi con mi número de teléfono dedicado Y si bien el teléfono físico era físico estaba gestionado todo por software por el equipo de it Y es ahí donde entran productos como los de 3cx y me imagino que ahora es cuando os empezáis a dar cuenta del Porqué 3cx es un objetivo tan jugoso si tenemos toda empresa en el mundo requiere de soluciones de telefonía y que la mitad bueno por decir algo no usaban las soluciones ofrecidas por 3dx pues ya podéis ver el valor que tendría para los atacantes comprometer a esta empresa si tú eres capaz de infectar el software de 3dx que corre en todos tus clientes has comprometido a todos sus clientes así de sencillo porque por qué vas a poner el esfuerzo de comprometer una empresa si puedes comprometerlas a todas con prácticamente el mismo esfuerzo está claro no y es por eso que los ataques a cadenas de suministro son cada vez más frecuentes Aunque suelen estar reservados atacantes muy sofisticados como de hecho es el caso de esta noticia y que de hecho hablaremos más adelante el 29 de marzo de este año es decir hace unas tres semanas una de las ciberprotecciones que vende la empresa strike en concreto el crows strike overwatch detectaba actividad sospechosa en el comportamiento de un binario llamado 3 CX de stop app Este es el programa de telefonía que os comentaba el software o teléfono blando no y claustro strike detectaba que en su última versión Este programa intentaba conectar con infraestructura que conocían De antemano era utilizada por cibercriminales esto sería lo mismo que si detectase que tu iPhone no solo se está comunicando con Apple algo que cabría de esperar sino que también está comunicándose con China y concretamente con los servidores del gobierno chino evidentemente ahí saltan todas las alarmas No hay ninguna razón por la que tu teléfono debería estar hablando con china porque un software entonces aquí cabe preguntarse porque un software de telefonía estaba enviando y recibiendo mensajes de servidores no sólo eso craustrat también detectó que el software se descargaba software adicional lo que en malware conocemos bueno como un secondstage pailot Esto del secondstage payload lo que viene a ser Es que hoy en día Cuando nos infectan un ordenador con lo que comúnmente conocemos

como un virus Aunque realmente hay diferentes tipos digamos de lo que de manera genérica conocemos como virus o llamamos malware normalmente no viene incluida toda la funcionalidad porque lo que uno pretende hacer a la hora de infectar un ordenador es reducir al máximo el tamaño de ese ejecutable de ese binario de ese programita malicioso y ya una vez hayas picado y lo hayas instalado Pues como tú puedes ejecutar el código que quieras pues se ejecuta una función para que se descargue de internet todo el resto toda la información adicional todas las funcionalidades a mayores que quieres poder tener en el ordenador víctima es decir digamos que la infección inicial es un programita lo más pequeño posible cuya única funcionalidad es que una vez se ejecute vaya internet a descargarse el resto tiene sentido No pues por eso se llama el secan stage paylor no el la carga útil de segundas digamos Bueno pues la app está disponible para la app digamos de t13x no que fue infectada pues está disponible para los tres principales sistemas operativos Windows Mac y Linux pero la actividad maliciosa curiosamente solo se observó en los binarios de macky Windows curiosamente en parte porque bueno son los sistemas operativos que se utilizan en la mayoría de gente la publicación original de crowdstrike realmente no contenía mucha más información por eso he estado esperando a traeros esta noticia un par de semanas porque como les digo Siempre muchas veces se va desarrollando Y prefiero traeros la entera no y efecto lo más completado posible y efectivamente como suele pasar en incidentes tan serios las demás empresas dedicadas a inteligencia de amenazas se pusieron manos a la obra también para descubrir más información sobre este ataque y los detalles de la campaña de malware al día siguiente la empresa al día siguiente de cuando strike crowd strike publicó esto Este primer hallazgo en la empresa volexcity sacó más detalles sobre el comportamiento del malware la infracción se había producido en los instaladores de Windows y Mac es decir lo que te sueles descargar para instalar la aplicación no digamos la aplicación en sí por decirlo de alguna manera no cuando tú te descargas una aplicación sabes que haces doble clic y le vas dando siguiente siguiente digamos que ese es el instalador que luego Te instala el programa en sí que es lo que queda en tu ordenador no y luego pues tú borras el instalador la infraestructura de los atacantes para gestionar las infecciones a escala fue activada en diciembre de 2022 O sea que es una campaña bastante reciente pero lo más curioso de este análisis de volaxicity es que identificaron el payload como un info styler es decir la carga útil las instrucciones concretas que tiene el malware para que sean ejecutadas es robar detalles sobre la máquina infectada nada más que eso La verdad hostname domain sistema operativo y el historial de navegación de los navegadores Chrome brave Edge y firefox digamos que el malware lo único que hace es ver cómo se llama tu ordenador y poco más y el historial de las páginas que has navegado y se lo manda a los servidores del atacante para que te hagas una idea esto puede que pero llama bastante la atención y en principio se podría pensar que están recabando información de ordenadores a través de muchas industrias para un ataque futuro recordemos que 3dx tiene 600.000 clientes por todo el mundo y hasta 12 millones de usuarios esto en realidad se podría ver como una pedazo de bornet por supuesto como todo malware se comunicaba con el comandante en control Lo que os decimos los servidores de los atacantes que estaba funcionando en dominios tales como MS storage azure.com/análisis Office storage box.com yosinc visual Studio factory.com/broucorazure de Play Store MS storage boxes básicamente para nuestros queridos oyentes buenos técnicos son referencias que hacen ver que son páginas de Microsoft para darle credibilidad si alguien mira con quién se está comunicando esta aplicación pero que en realidad son dominios que son de los atacantes registrados específicamente para esto curiosamente mencionan que algunos de estos dominios no tenían el juicio anonimizado esto es una gran sorpresa el Quiz básicamente es una consulta que tú puedes hacer a un dominio digamos a Martín vigo.com y te da datos como la dirección el

teléfono el email de la persona a la que pertenece ese dominio esto no quiere decir que tú ahora te puedas ir a hacer un Juice San Martín vigo.com y veas mi número de teléfono real Mi dirección donde vivo mi nombre o en este caso porque es Martín vigo.com pero si fuera yo que sé cualquier cosa punto es que ni siquiera El dominio te da información Tú podrías tú no no tienes fácil ser que lo ha registrado Por qué Porque hay una cosa que tú puedes digamos pedir que es la protección del juez precisamente anonimizar la información pública de quien ha registrado tu dominio Esto está muy bien porque no queremos que toda persona que registre un dominio tenga toda su información personal publicada en internet que cualquiera puede consultar ya que la ley exige que tus datos personales sean reales por tanto tú puedes digamos proteger de cara al público tus datos personales pero la empresa la que tú le has comprado El dominio pues tiene Los Reales no Pues básicamente los atacantes se han olvidado de pedir la protección el anonimato para que los datos personales del registrador de estos dominios falsos que se hacen pasar por Microsoft fueran anonimizados y de hecho al consultarlo se puede recuperar emails como que el ego Diego punto García arroba protón.mi remake simpson@uu.com Jackie arroba gmail.com philip.y@proton.me y Harold marvel@gmail.com esto parecen correos electrónicos ordinarios con nombres y apellidos de hecho no el el nombre de usuario pero a mí la verdad me suena bastante falso y me da a mí que es para despistar O sea no es que se hayan olvidado de anonimizarlo sino que yo creo que dar por darle un punto de credibilidad si alguien se pone digamos muy rápidamente a investigar dominios un poco le da a Bueno ni siquiera están anonimizados yo creo que este es un dominio real y ya está no Pero bueno ya veremos que eso realmente lo han hecho un poco para engañar mencionar también una peculiaridad de este malware Y es que descargaba el seconds si os acordáis eso lo que os comentaba de una vez infectado pues se descarga más funcionalidad pues se la descargaba de github un repositorio en concreto que contenía entre otros iconos cuyos iconos contenían de manera ofuscada más código quedaba más funcionalidad al malware es decir el malware tú te descargabas lo mínimo infectaba tu ordenador se iba gatehab se descargaba un repositorio que parecía benigno pero ese ese repositorio contenía archivos punto ico que son pues las imágenes de los iconos que sueles ver en tu escritorio y esos iconos eran válidos pero contenían información adicional al final digamos de la ristra de bites y Beach que contenía ofuscado parte del código del malware para llevar a cabo Pues las funcionalidades añadidas que se le quería Añadir no al malware muy guapo la verdad tenéis más detalles técnicos en las notas del episodio que os dejo un par de blogs y noticias donde donde entran más en los detalles técnicos pero ya sabéis que tampoco queremos aquí y aburrir lo que quiero que os quedéis es que tanto ataque y tan sofisticado solo para lo que decía antes no robar información sobre máquinas infectadas y nada más de verdad ni ni robar contraseñas ni ni yo que sé ransomware ni solo cogerte el nombre de tu equipo tu historial de información y ya está bueno pues cuatro días más tarde salía otra publicación de otra empresa contando que habían encontrado otro carga útil que usaba el malware es decir funcionalidades añadidas que este post post de boxality no había cubierto no solo se trataba de robar información sobre los detalles de la máquina como que había esperar sino que había mucho más detrás de este ataque una de las cosas en las que caspersky se fijó fue precisamente si lo único que hacía Este malware era robar información básica y la respuesta como os digo es que no los análisis preliminares de las empresas no habían dado Con todo lo que sucedía y según Kaspersky detrás de este malware se esconde actividad maliciosa centrada en hackear y robar de empresas dedicadas al mundo de las criptomonedas atracos a bancos virtuales básicamente una de las máquinas infectadas que casperskin vestigó tenía una librería dll sospechosa y que se llamaba gart 64 punto dll que se cargaba con el proceso de instalador de 3x básicamente lo que os acabo de decir es que había un archivito

que contiene un código que se incluía dentro del instalador que estaba infectado y esto les llamó la atención a Kaspersky por qué porque esta librería maliciosa con este mismo nombre de gardt 64.dll había sido detectada por Cars Percy hace una semana una semana antes como parte de una puerta trasera usada desde 2020 por actores centrados en robo de dinero y los más fieles oyentes de tierra de hackers sabrán ya atribuir al país adecuado este tipo de ataque Corea del Norte efectivamente este vactor es utilizado comúnmente por lázarus Group el apt o grupo de amenazas avanzado que opera las órdenes de Kim Jong son los que están detrás del famoso ranson Board wanna Cry de hace unos años por sí todavía no tenéis localizado Quiénes son Pues bien como siempre os comentamos Estados Unidos espía china roba propiedad intelectual Rusia crea el caos y Corea del Norte siempre se centra en robar dinero y este caso no es diferente Corea del Norte puso a su equipo profesional de ciberdelincuentes a trabajar e infectar software utilizado por miles y miles de empresas para robar dinero de empresas relacionadas con criptomonedas una campaña súper sofisticada para lucrarse y seguir financiando su programa nuclear porque robar solo un Por qué robar solo un banco Cuando puedes comprometer una empresa intermedia y robarlos todos Pues esa es la filosofía en este caso triste pero una historia fascinante verdad Kaspersky no solo no se queda solo en esto de atribuir Al ataque a lázarus Group no solo se basa en esto que acabo de mencionar bueno y parte de la opinión mía sino también en el uso de una constante en la lógica de ofuscación del malware que ha sido observada en el malware desarrollado por este equipo en el pasado Es decir lázarus Group campañas que hicieron anteriormente con malware diferente que habían desarrollado había una constante en concreto el 0xf55 8f4 de a que bueno es código hexadecimal por no entrar en detalles técnicos digamos que esto es código es como verías algo parte de código ensamblador Por así decirlo pues esto era parte de una esto era parte de una lógica concreta de esta puerta trasera utilizada que se había observado única y exclusivamente en puertas traseras anteriores utilizadas y desarrolladas por lázaro's Group grupo que como decía ópera bajo Corea del Norte Así que esto les da digamos la prueba no definitiva pero muy clara Aparte de todo lo que hemos mencionado de que es Corea del Norte quien está detrás de todo esto x acabó publicando un breve comunicado oficial que dice lo siguiente lamentamos informar a nuestros socios y clientes que nuestra aplicación de Windows electrón enviada en la actualización 7 números de versión 18 12 407 y 18 12 4 1 6 incluye un problema de seguridad los proveedores de antivirus han detectado el ejecutable 3cx de stop a punto exe y en muchos casos lo han desinstalado los números de versión de la aplicación de Mac electrom 18 11 12 13 enviados en la actualización 6 y 18 12 40 2 18 12 407 y 18 12 4 16 en la actualización 7 también se ven afectados el problema Parece ser una de las bibliotecas incluidas que compilamos en la aplicación de Windows electrón a través de git todavía estamos investigando el asunto para poder proporcionar una respuesta más detallada más tarde aquí hay información sobre lo que hemos hecho hasta ahora y Bueno detalla pero muy brevemente digamos un par de toques técnicos pero ya os digo que os dejo enlaces a reportes mucho más técnicos que los que ellos han proveído y hasta aquí la noticia la verdad aquí tenemos otra campaña a nivel gubernamental de Corea del Norte utilizando a su grupo de hackers porque no decirlo Aunque en este caso trabajando para un gobierno pero atacando al resto del mundo utilizando a esos profesionales más sofisticados para comprometer en vez de a un broker de criptomonedas en vez de a un banco virtual en vez de una empresa fintech a una empresa intermediaria cuyos bancos fintex y traders utilizan su software y así penetrar sus redes de manera indirecta la verdad es que el mundo de los ataques a cadenas de suministro es fascinante y ya vemos que el retorno fin investment el dedicarse a de verdad encontrar una y luego encontrar agujeros de seguridad en sus productos y poder explotarlos de manera que puedas explotar a todos sus clientes de manera automática pues está claro que ofrece muchos beneficios sobre todo para

estos delincuentes pues ya pues doy paso a Alexis que como os decía antes no estamos grabando juntos Así que Alexis Dale dale palante con tu noticia muy buena como siempre tu noticia Martín y nada seguimos con la siguiente Pero antes queremos darle las gracias También a monat otro de nuestros patrocinadores una empresa que comparte los mismos valores que tierra de hackers hacer 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 está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echadle un vistazo a su web monat.com y mandarles vuestro currículum a tierra de hackers arroba monat.commod.com hoy voy a hablar sobre una empresa que ofrece servicios Con un objetivo siniestro sembrar el caos y causar destrucción a diferentes naciones y países del mundo por ejemplo paralizar los sistemas informáticos de un aeropuerto para que la torre ya no pueda dirigir los vuelos o desencadenar descarrilamientos de trenes mediante un programa de Software que Desactiva todos los controles de seguridad o interrumpir el suministro eléctrico en grandes ciudades como digo causa del caos todos estos ataques Son elementos de la guerra cibernética una especialidad de las agencias del servicio secreto Ruso y una de las empresas privadas que ofrece ayuda en este aspecto al gobierno ruso es Vulcan y Cómo sabemos esto Bueno pues porque Poco después de la invasión rusa en Ucrania se filtraron un conjunto de documentos llamados los Vulcan files que periodistas han analizado y recientemente han publicado su análisis sus conclusiones todo esto está registrado en mil documentos secretos que incluyen 5.299 páginas llenas de planes de proyectos instrucciones y correos electrónicos internos de Vulcan y entre el gobierno ruso de los años 2016 a 2021 a pesar de estar todo en ruso y de naturaleza extremadamente técnica proporcionan una visión única de las profundidades de los planes de guerra cibernética rusos estos objetivos bélicos son evidentes en Ucrania que ha sido atacada tan implacablemente por militares cibernéticos rusos desde la invasión en febrero de 2022 algo a lo que los expertos han comenzado a referirse como la Primera Guerra cibernética integral jamás vista y Qué es Vulcan pues Antón vladimirovich Mark director ejecutivo de Vulcan fundó esta empresa que cuyo nombre significa volcán en inglés en 2010 junto con Alexander alexandrovich ir sawski ahí haciendo un esfuerzo a pronunciar bien el ruso Espero que lo ha hecho bien y si no pues nada ambos son graduados de la academia militar de San Petersburgo y sirvieron en el ejército en el pasado ascendiendo a Capitán y mayor respectivamente tenían buenos contactos en el ejército algo que les ha ayudado bastante en su empresa privada Vulcan se lanzó en un momento en que Rusia estaba expandiendo rápidamente sus capacidades cibernéticas tradicionalmente el fsb tomaba la delantera en los asuntos cibernéticos en 2012 Putin nombró a sergeygu como ministro de defensa quien está a cargo de la guerra tradicional y cibernética de Rusia en Ucrania a partir de 2011 Vulcan recibió licencias gubernamentales especiales para trabajar en proyectos militares clasificados y secretos de estado volcán es una empresa tecnológica de tamaño medio con unos 120 empleados de los cuales unos 60 son desarrolladores de software la cultura corporativa de Vulcan es más parecida a silicon Valley que a una agencia de espionaje tienen es que si lo veis es bastante cómico tienen un equipo de fútbol e internamente se envían correos electrónicos motivacionales con consejos de acondicionamiento físico para ejercicio y celebraciones de cumpleaños de los empleados incluso hay un eslogan optimista que dice hacer del mundo un lugar mejor que se muestra en un vídeo promocional de la empresa que vamos a poner en las notas del episodio Vais a ver que también salen en una cinta de correr también salen jugando al futbolín haciendo bueno actividades digamos divertidas para como se dice para hacer entablar relaciones entre entre los empleados Vulcan dice que se especializa en seguridad de la información oficialmente sus clientes son grandes empresas estatales rusas

como ver Bank el banco más grande del país la aerolínea nacional e internacional aeroflot y los ferrocarriles ferrocarriles rusos los generosos salarios de Vulcan atrajeron a muchos de sus empleados algunos miembros del personal son graduados de la Universidad Técnica Estatal bauman de Moscú que tiene una larga historia de proporcionar reclutas al Ministerio de defensa Ruso y la agencia de inteligencia fsb el espíritu de la empresa es patriótico en la víspera de año nuevo de 2019 un empleado creó un archivo de Microsoft Excel con música militar soviética y la imagen de un oso junto a él estaban las palabras apt magma Beer la referencia obviamente es a grupos de piratería estatales rusos como cousiver y fancy ver estos osos que bueno los ha elegido como tal como animal esta empresa crow strike que se dedica a temas de Ciber inteligencia Y parece apuntar a las propias actividades que realiza Vulcan Y a lo que se dedica a la empresa en sí los Vulcan files muestran que la empresa ha estado trabajando en cuatro proyectos bastante inteligentes el primero se llama amecith que va de interceptación de comunicaciones tema Man in the middle hombre en el medio y similar el segundo se llama scan V que es un proyecto de situational la werness O conciencia situacional o saber lo que está pasando en este momento el tercero se llama Crystal 2 V que es un proyecto de guerra cibernética en infraestructura crítica y el último se llama fraction que es para vigilancia online y manipular un poco a las masas online a través de plataformas online voy a empezar con el primero Vulcan a messic este es un proyecto en el que Vulcan ha estado trabajando durante la última década cuyo objetivo es obtener el control de los flujos de información en regiones específicas según una descripción en un documento que lleva el título propósito del Software en muchos otros documentos incluidos cientos de páginas de planos diagramas y tablas de relaciones de bases de datos se describe una plataforma Que cubriría prácticamente todos los aspectos de guerra moderna desde la censura y la manipulación del contenido de las redes sociales hasta los ataques a infraestructuras críticas las indicaciones de los materiales de estos documentos conducen indican que los objetivos pasan por incluso granjas de servidores en Estados Unidos e incluso plantas de energía nuclear en Suiza esta herramienta está diseñada para censura vigilancia y desinformación pero también para detectar brechas de seguridad en el software de equipos de telecomunicaciones de compañías como Huawei juniper y Cisco para interrumpir el tráfico de la red se imitan páginas conocidas y se difunden en ellas contenidos falsos o manipulados un poquito de ingeniería social por esta parte con el fin de desinformar se crean perfiles falsos en masa para difundir contenido procremlin obviamente a gran escala a través de correos electrónicos SMS y mensajes en redes sociales los tienen nombres y fotos personales robadas que luego se cultivan durante meses para crear una huella digital realista y utilizarlos para influir en la opinión pública impulsando hashtags específicos una captura de pantalla de este proyecto a messit en los documentos de Vulcan files muestra cuentas falsas creadas por la empresa para imitar perfiles de redes sociales reales Como por ejemplo Twitter otras capturas muestran hashtags utilizados por el ejército ruso desde 2014 hasta principios de este año difunden desinformación incluida la teoría de la conspiración sobre hillary Clinton y la negación de que el bombardeo de Siria por parte de Rusia haya matado a civiles tras la invasión de Ucrania una cuenta falsa de Twitter vinculada a Vulcan publicó excelente líder hashtag Putin una parte de amesid es doméstica lo que permite a los operativos secuestrar y tomar el control del tráfico de internet si estallan disturbios en una región rusa o si el país gana un bastión sobre el territorio de un estado nacional rival como Ucrania tráfico de internet considerado políticamente dañino puede eliminarse antes de que tenga la oportunidad de propagarse un documento interno de 387 páginas Explica cómo funciona este proyecto a messic las fuerzas armadas necesitan acceso físico a Hardware como Torres de telefonía móvil y comunicaciones inalámbricas una vez que controlan la transmisión el tráfico puede ser interceptado obviamente es un poquito hacer trampas porque utilizan igual digamos su poder de gobierno

ruso Pero bueno efectivamente lo que les permite es esta posición de hombre en el medio e interceptar las comunicaciones así que ya sabéis intentado utilizar si estáis en Rusia en la medida de lo posible cifrado ssl tls vpns y similares Los espías militares pueden identificar a las personas que navegan por la web ver qué acceden en línea y rastrear la información que comparten con otros usuarios desde la invasión del año pasado Rusia arrestó a manifestantes contra la guerra y aprobó leyes punitivas para evitar las críticas públicas a lo que Putin llama una operación militar especial todos sabemos a lo que se refiere no a la guerra en Ucrania los archivos de Vulcan contienen documentos vinculados a una operación del fsb para monitorear el uso de las redes sociales dentro de Rusia a una escala gigantesca utilizando análisis semánticos para detectar contenido hostil es decir que tienen ahí digamos expresiones regulares están analizando todo el texto de todo el tráfico que va yendo por internet y bueno Supongo que también a estas alturas incluso estén utilizando temas de Inteligencia artificial o Machine learning a saber en los documentos filtrados hay evidencia de un viaje de negocios del equipo de Vulcan al sitio del fsv en rostov one parte de una relación comercial típica y cuando digo típica me refiero a que aunque los servicios secretos suelen tener sus propios departamentos especiales de guerra cibernética no es inusual que estos trabajen junto con empresas privadas como Vulcan Edward snowden al que todos queridos oyentes probablemente conozcáis ya después de tantos episodios por ejemplo no trabajaba directamente para la agencia de seguridad nacional la nsa era empleado de una empresa asociada o una empresa contratista una empresa Tercera Privada llamada bus Allen Hamilton y que ofrecía Servicios al gobierno de Estados Unidos a la nsa hay varios ejemplos similares de esto en todos los países del Mundo India China y similares esto es debido a es más rápido y eficiente subcontratar trabajos a proveedores de servicios especializados si una empresa determina que le sale más barato delegar en concepto de dinero y tiempo pues así lo van a hacer y no solo empresas piensan así los gobiernos igual en su correo electrónico al ejecutivo de Vulcan maxim andréyevich pidió a su equipo que preparará rápidamente una presentación de nuestra plataforma de software para el representante militar en rostov así lo dijo la demostración de ames it y varios de sus subsistemas se llevaría a cabo en el transcurso de varios días los documentos filtrados no muestran ninguna indicación sobre si el viaje a rostov on fue exitoso o si el fsb está utilizando actualmente a messic pero hubo muchas otras oportunidades para que los ingenieros de Vulcan presentaran sus armas cibernéticas los equipos de desarrolladores viajaban regularmente a la sede del fcb en la plaza lubian Moscú a sólo cuatro paradas de Vulcan en el metro en este edificio es donde antes la kgb de stalin solía torturar y asesinar a los designados como enemigos del comunismo el edificio Está al lado de una librería y la filtración de estos documentos revela que Los espías de la unidad fueron apodados de forma cómica amantes de los libros por estar tan cerca de esta librería el edificio también está a pocos metros del kremlin no todos los empleados de Vulcan estaban contentos con estas visitas esto es debido a que los agentes del servicio Secreto del fsb a menudo les hacían solicitudes técnicamente poco realistas lo típico No yo me imagino no sé si habéis visto el corto cómico de el experto no O the expert ese vídeo en el que hay dos clientes y tres consultores dos de ellos managers y el otro un empleado técnico que es el que realmente va a realizar el trabajo en este caso un desarrollador de software no el cliente le hace peticiones surrealistas como todo esto tuve que mirarme el vídeo para recordar Pero le pide el cliente a la empresa de servicios que haga que dibuje siete líneas rojas todas perpendiculares entre ellas algunas con tinta verde y otras con tinta transparente algo Bastante sencillo Así que ahí lo dejo supongo que el fsb le estaba pidiendo a Vulcan que realizara algunas tareas que son bastante difíciles de conseguir Y probablemente si no proporcionaba ese servicio pues obviamente no no les pagaría no entonces Bueno ahí hay que de tema voy a poner el vídeo en las notas del

episodio para que os riáis un ratito porque es bastante cómico Pero sigo Ahora quiero comentar el proyecto scan V que es una plataforma que los expertos en seguridad y varias agencias de inteligencia occidentales creen que de naturaleza ofensiva scan V tiene como objetivo hacer que los ataques cibernéticos sean mucho más fáciles de planificar reduciendo las semanas y los meses que suele llevar preparar tales ataques los objetivos primero deben investigarse exhaustivamente como está estructurado el sistema de tecnologías de información de la empresa a la que quiero atacar Qué sistemas operativos se han instalado Y dónde se encuentran sus debilidades vamos todo el tema que se suele hacer de ricones sands de reconocimiento antes de atacar a tu objetivo y esto se puede hacer digamos a nivel físico mirando incluso Google Maps nivel de redes sociales a nivel de personas para temas de ingeniería social a nivel de vulnerabilidades saber qué sistemas operativos tecnologías utilizan Bueno pues según los documentos filtrados scan V pretende automatizar todo esto la adquisición de información se basa parcialmente en Fuentes públicas tipo osin incluidos sitios web que forman informan sobre fallos de seguridad como parte de una herramienta más grande este proyecto escanea de forma activa los sistemas objetivo en busca de vulnerabilidades para coordinar los ataques y luego en función de la información recopilada se define un plan de ataque esto es típico de películas militares donde un líder Define su estrategia en un mapa con muñequitos de plomo colocando a sus soldados de tal forma que puedan romper las líneas enemigas y llevar a cabo el ataque completo Esto me recuerda un poquito por ejemplo a la película de gladiator de ver muchas No pero en esta película El general está con maximus marydus ahí que parece ser alguien que vivía por extremadura no me pareció interesante en esa película pero en cualquier caso están mirando el mapa y deciden Cómo la estrategia para seguir adelante el plan de ataque los planes cibernéticos del kremlin no solo se enfocan en el rápido desarrollo de todo tipo de armas cibernéticas ofensivas sino también en la creación de personal experto que sepa utilizar estas herramientas y Vulcan puede satisfacer este requisito la compañía ha desarrollado su propio programa de Educación para los militares cibernéticos un documento filtrado sobre el programa secreto que lleva el nombre en clave cristal 2 V afirma que su objetivo es la formación integral de especialistas en confrontación de información el término que usan las agencias del servicio secreto ruso para describir la guerra cibernética esto incluye destruir los sistemas de control del transporte ferroviario aéreo y marítimo y otras áreas vitales tales como la electricidad y el suministro de agua el programa también está diseñado para formarlos en el bloqueo del acceso al sistema de información pública global una referencia aparente a internet Estos son ataques a las arterias vitales de suministro y transporte y los sistemas de control industrial y tales ataques se han visto en la realidad desde hace ya mucho tiempo en 2017 se descubrió un ataque a una refinería de petróleo de Arabia Saudita los atacantes rusos intentaron manipular los mecanismos de seguridad de la instalación hace un año los funcionarios de justicia de Estados Unidos acusaron a la gente del grof Jenny glad Kids por este incidente el Gro es el servicio de inteligencia militar de las fuerzas armadas de la federación rusa para aquellos que no lo sepáis oficialmente el presunto cibercriminal había estado trabajando para una institución de investigación científica que también proporciona financiamiento a Vulcan dichos ataques se describen en detalle en el programa de entrenamiento desarrollado por Vulcan la atención se centra en el acceso no autorizado redes críticas y la detección de puntos débiles en el sistema de destino un módulo adicional del curso enseña los ataques de denegación de servicio Como una forma de bloquear el acceso a los servicios basados en web los estudiantes deben aprender todas esas habilidades tanto de la instrucción basada en la teoría como de la simulaciones prácticas de laboratorio y finalmente tenemos el proyecto Vulcan fraction que es un software de vigilancia automatizada para controlar a la población rusa utiliza técnicas de

Machine learning y vigila a redes sociales como Twitter Facebook estas dos últimas son rusas y son muy similares a redes sociales como Facebook un sistema para monitorear e identificar actividades en las redes sociales literalmente decía el documento un gran hermano basado en la web diseñado para escanear las publicaciones de las redes sociales en busca de contenido sospechoso y luego guardar ese contenido y lo guardan porque a futuros Si alguna vez se destapa que alguien ha hecho algo y ha dicho algo en contra de Putin pues ahí se le imputa es una forma de identificar a los que critican a Putin vamos a pasar ahora a mencionar algunos clientes interesantes de Vulcan en mayo de 2020 un equipo de Vulcan estaba planeando una visita a uno de los clientes más importantes de la empresa el destino Era kimchi una ciudad Industrial a las afueras de Moscú un documento interno del jefe del proyecto scan V oled n indicaba a sus empleados que prepararan su pasaporte ya que lo iban a necesitar para identificarse dónde se iban a encontrar con su cliente la reunión se planificó en un rascacielos de cristal de 20 pisos a orillas del río moscova esto para aquellos que estén más metidos en temas de Ciber inteligencia igual os suena este edificio se Incluso en la acusación de 2018 derivada de la investigación realizada por el fiscal especial Robert mueller sobre la influencia rusa en las elecciones presidenciales de 2016 en Estados Unidos en el documento en el rascacielos de kimchi se conoce como la Torre se cree que la unidad de la agencia de inteligencia militar Gru que tiene su sede ahí participó en la vigilancia del equipo de campaña de Hilary Clinton en un esfuerzo por lograr que Donald Trump fuera elegido en este edificio se encuentra el equipo militar conocido oficialmente como la unidad militar 7-4455 que obtiene este número debido al código postal del edificio sin embargo redoble de tambor son más conocidos por su nombre en clave sandwarm o gusano de arena son los ciber guerreros más famosos y poderosos del mundo según el gobierno de Estados Unidos San worm estuvo involucrado en ataques de manipulación política en 2016 como digo afectaron las votaciones presenciales en Estados Unidos para que Donald Trump fuera elegido pero también en 2017 trataron de influenciar el resultado de la votación presidencial francesa estuvo también involucrado en sabotajes cibernéticos Y es que provocó dos veces apagones en Ucrania la Navidad de 2015 y la de 2016 y son famosos por ser los primeros apagones provocados por ciberataques también lanzó notpetia ese malware que económicamente fue más el más destructivo de la historia y también interrumpió los Juegos Olímpicos en Corea del Sur bueno Y aparte de eso se ha visto involucrado en muchos temas de volcado y filtrado de correos electrónicos y documentos similares en el Gru el más feroz de todos los servicios secretos rusos trabajan unas 37.000 personas incluidos 25.000 soldados de élite de spets que son las fuerzas especializadas en misiones de vigilancia Sabotaje e incluso infiltración tras las líneas enemigas aparte de estos los servicios de inteligencia occidentales creen que la agencia también emplea a varios miles de cibercriminales externos los expertos en espionaje describen el enfoque de la Gru como impacto sobre cobertura su arsenal de medidas activas incluye Sabotaje y subversión desinformación y asesinato su objetivo desatar el caos y dañar las democracias occidentales según el análisis de los Vulcan files scan V sería una herramienta útil que podría usarse para preparar los ataques lanzados por sandward sin embargo no está claro si el Gru de hecho ha implementado o comprado scan V de todas formas parece claro que el Gru siguió de cerca el desarrollo de esta herramienta y un documento de 11 páginas lleno de jerga sobre sistemas de procesamiento y análisis de datos proporciona evidencia de ese interés la portada lo identifica como un protocolo para scan V centrándose en el intercambio de datos entre diferentes subsistemas y en la esquina superior izquierda está la notificación representante autorizado de la unidad militar 74455 la unidad obviamente sandword O sea que obviamente ese documento que había creado Vulcan lo había creado para enseñárselo a sandward y hace 10 años uno de los empleados de Vulcan estuvo involucrado en un ataque global lanzado por sandward algo

que Google descubrió y que Der spiegel un periódico alemán ahora hecho público por primera vez el ataque que los investigadores bautizaron como mini Duke o mini Duque tuvo como objetivo ordenadores oficiales estatales en países como Alemania Estados Unidos y Ucrania el objetivo robar información secreta de las redes de las agencias los ordenadores de al menos tres representantes del gobierno occidental fueron infiltrados con éxito y servidores de todo el mundo fueron infectados detrás de los ataques estaba un grupo llamado dedux También conocido como coashi Beer vinculado a la agencia de inteligencia extranjera rusa el svr más tarde estos militares cibernéticos atacaron al Pentágono a finales de 2012 Google identificó una dirección de correo electrónico que luego se vinculó a mini Duke Google pudo trazar una línea de Mini Duke a Vulcan debido a un error cometido por los piratas informáticos y es que la misma dirección IP se utilizó para alquilar un servidor de comana en control y también para registrar la cuenta de Google que se usó para enviar el malware vía email un gran fallo de seguridad operacional el descubrimiento llevó a Google a bloquear la cuenta de correo electrónico pero la campaña global de piratería ya no pudo detenerse ahora voy a comentar un poquito de dónde vienen estos archivos Vulcan que se han filtrado como decía al principio de la noticia pocos días después de la invasión rusa a Ucrania una fuente anónima opuesta esta invasión filtró documentos sobre la empresa rusa Vulcan a disposición de varios grupos de noticias los documentos datan de entre 2016 y 2021 y fueron puestos a disposición del diario alemán sudeuche seytún que es traducido el periódico del sur de Alemania y luego ellos compartieron estos documentos también como con el periódico alemán que se traduciría como the mirror o el espejo esta fuente dijo literalmente debido a los acontecimientos en Ucrania decidí hacer pública esta información el Gru y el fsb se esconden detrás de esta empresa refiriéndose a Vulcan la gente debería saber acerca de los peligros posteriormente la Fuente compartió los datos y más información con la startup de investigación paper Trail media con sede en Múnich puede conseguir un enlace a un repositorio de Paper Trail media en document cloud.org que contiene 7 pdfs de estos Vulcan files en concreto hay un documento de amezid unas 333 páginas 4 documentos de scan V en total 288 páginas un documento de Crystal 2 V unas 29 páginas y un documento llamado sandworm con obviamente las propuestas de Vulcan para sandworm y que tiene unas 10 páginas este enlace lo voy a Añadir a las notas del episodio Aunque os advierto que está todo en ruso Así que tenéis que traducirlo los Vulcan files permiten un entendimiento detallado de Cómo se preparan y organizan tales ataques y como Vladimir Putin con la ayuda de empresas privadas planifica e implementa operaciones civil of en todo el mundo durante varios meses periodistas que trabajan para 10 medios de comunicación desde siete países distintos han estado investigando estos archivos en un consorcio común esta investigación la ha liderado paper Trail media y de speagle ambos de Alemania y también incluyó a la emisora pública alemana zdf al periódico de Guardian de Estados Unidos al the Washington post de Estados Unidos al diario austriaco de standard al periódico lemont de Francia a la emisora pública danesa de r hasta media Group en Suiza e incluso el portal de investigación ruso hay Stories Sí sí hasta hasta un periódico ruso estuvo involucrado en este análisis meses de investigación identificaron documentos internos de la empresa de más de información sobre transferencias de dinero tanto Vulcan como el kremlin tuvieron varias oportunidades para comentar pero se negaron a responder no hay razones obvias para dudar de las conclusiones a las que llegó el equipo de investigación cinco agencias de inteligencia occidentales también confirmaron la autenticidad de los documentos Vulcan Parece ser parte del opaco complejo militar Industrial en el que las agencias de inteligencia rusas trabajan en estrecha colaboración con más de 40 empresas privadas de tecnología de la información uno de sus objetivos es desarrollar armas cibernéticas altamente efectivas que puedan usarse contra todos aquellos que el kremlin ha identificado como enemigos de Rusia

especialmente por supuesto occidente la empresa recibió numerosos pagos que suman varios millones de euros de institutos estrechamente vinculados a las agencias del servicio secreto Ruso y al ejército en más de 17.000 transferencias en las que se mencionan temas como scan V a messic y cristal 2 V como motivo de pago el artículo de The speagle tiene muchos detalles sobre esta noticia incluyendo la situación actual de extrabajadores de Vulcan a pesar de que algunos de los soldados cibernéticos rusos se refugian en su propio país algunos de los ahora ex trabajadores de Vulcan han obtenido puestos de trabajo en empresas multinacionales incluidas algunas en Alemania despiggle pudo localizar antiguos empleados de Vulcan que ahora trabajan para siemens y también en empresas que ofrecen servicios a bus Trivago Y booking.com no sólo eso sino que también se pudieron identificar ex empleados de Vulcan que ahora viven y trabajan en dublín uno de los centros de la industria tecnológica europea con empresas como Google IBM y meta y me comentó que sus lazos comerciales con Vulcan terminaron en 2020 me sorprende a mí que esta empresa tan grande tuviera relaciones con Vulcan Aunque igual no sabían en lo que Vulcan estaba realmente metido y bueno menos mal que acabaron sus relaciones en 2020 porque si no seguro que a revelación a partir de estos Vulcan files la hubieran terminado Igualmente los periodistas de The spigle fueron a picar a las casas de decenas de estos ex empleados de Vulcan y cuando ellos abrían la puerta se identificaron y les dijeron Hola somos periodistas de drespigel y estamos trabajando en una historia sobre una empresa llamada Vulcan creemos que trabajaste para esa empresa podemos hacerte algunas preguntas además sabes algo sobre el sistema scan V Obviamente todos estos ex empleados se quedaron con los ojos como platos y contestaron con un no rotundo lo siento y luego cerraron la puerta los reporteros de toda Europa que llamaron a las puertas de decenas de exempleados de Vulcan tuvieron experiencias similares la mayoría de ellos no querían hablar de su antiguo empleador los periodistas dicen que no está claro si esa reticencia se debe al temor a represalias o a la preocupación de que su tapadera pueda ser descubierta aquí tenemos una polémica que no es nueva y que se ha hecho más fuerte a raíz de la invasión rusa en Ucrania el problema o riesgo que supone contratar a empleados rusos especialmente en empresas multinacionales tecnológicas en las que muchas otras empresas y ciudadanos del mundo confían muchos de estos ex empleados de Vulcan dejaron su trabajo antes de la invasión rusa en Ucrania y consiguieron trabajos también antes del inicio de este conflicto bélico y con todo esto queridos oyentes aquí lo dejo un poquito para reflexionar en el tema en estos servicios un poco oscuros que estas empresas ofrecen a gobiernos de todo el mundo especialmente algunos gobiernos un poco más opresivos como los rusos o incluso los chinos pero también hemos visto que hay algunas otras empresas como el caso de bus Allen Hamilton no de Edward snoden que estaba ofreciendo también servicios de dudosa privacidad digamos abuso a la privacidad a todos los ciudadanos no solo estadounidenses sino de todo el mundo y con esto llegamos a la pregunta del episodio que es la siguiente estarías de acuerdo en que las grandes empresas tecnológicas pudieran contratar a personal que ha trabajado antes para compañías que han ofrecido servicios de dudosa legalidad a organizaciones gubernamentales os damos cuatro opciones que son las siguientes si somos todos iguales Sí pero no para trabajos de gobierno sí pero si se les monitorea mensualmente es decir se le hace un poquito de background check cada mes o de forma periódica y finalmente un no nunca me hago eco de Martín y como siempre daros las gracias siempre por apoyarnos en online con vuestros comentarios recomendaciones y sugerencias también nos queremos recomendar que una forma de aprender además de pasivamente escuchando nuestro podcast Es que de forma activa toméis notas de lo que contamos ya sea en papel en digital o en vuestra cabeza y que le hagáis un breve resumen a alguien al que le interese el podcast o la noticia en concreto de esta forma consolidáis lo que habéis escuchado en el podcast para estar protegidos Online para

poder acordaros de lo que habéis escuchado de este incidente de ciberseguridad y evitar caer en ser víctima porque nuestra misión es que aprendáis con nosotros y como digo que estéis ciberseguros además obviamente de haceros pasar un buen rato escuchándonos así que ya sabéis después de cada episodio tomado Unas notas e ir a vuestro amigo vecino compañero de trabajo al que le pueda interesar y servir el episodio y lo comentáis vuestras notas seguro que aprecia que vayáis y os preocupéis por él por ella y me compartáis este conocimiento para que no caigan Víctimas de todos los incidentes de ciberseguridad que cubrimos en cada uno de los episodios y si no Oye también nos puede servir para romper el hielo y entablar conversaciones con desconocidos yo personalmente he comentado muchas veces algunos de nuestros episodios a personas Random que me encuentro por ahí y me ha servido para un poco iniciar conversaciones con con estas personas lo comento porque a mí también otro dato es por ejemplo escucho bastante podcast y audiolibros y Leo bastante y siempre me gusta tomar notas con mis propias palabras de lo que voy aprendiendo es una forma más de lo que aprendo se me quede porque si no si no me pongo a escribir a tomar notas a digerir un poco lo que voy escuchando lo que voy analizando si no hago esto básicamente yo lo que noto es que el conocimiento se me va volando Así que aquí os lo dejo como idea sugerencia para que lo hagáis y lo dicho muchas gracias por escucharnos episodio 3 episodio y nos escuchamos en el próximo pues hasta aquí ha llegado el episodio número 91 quedan nueve para llegar a los 100 Gracias como siempre por quedaros hasta el final haznos un favor hombre Danos una review sobre todo si los skits escuchas en Apple podcast o nos das estrellas en Spotify o nos dejas comentarios en ivoox pero todo eso nos ayuda un montón nos vemos y nos escuchamos en el próximo episodio 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 de tierra de hackers