Rusia redobla sus inversiones En ciberespionaje al centrarse en vigilar de cerca sus propios ciudadanos para encontrar a los que no apoyan la invasión de Ucrania contando ya con tres dígitos ya tienes listo el nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 21 de julio de 2023 este es el episodio número 101 yo soy Martín vigo Y tenemos Alexis de vacaciones Así que os tenéis que confirmar conmigo bueno el episodio anterior fue normalmente tenemos la pregunta del episodio que sería lo que cubre Alexis pero que el episodio anterior fue un episodio especial para celebrar el episodio número 100 con preguntas y respuestas vuestro feedback ha sido totalmente positivo me alegro un montón es algo que no sabía bien como como iba a salir pero muchísimas gracias a todos los que nos enviasteis preguntas quedaron algunas en el tintero pero claro nos fuimos a las dos horas de episodio sobre todo a los que nos mandaron audios Gracias por todas las solicitaciones una pasada ver que nos escucháis desde todos los rincones del mundo increíble Muchísimas gracias qué os parece si vamos a por cien más para llegar a los 200 pues empecemos el camino Agradeciendo ante todo a nuestros mecenas de patreon todo su apoyo que es por ello que Hemos llegado a estos 100 episodios concretamente esta semana mencionar a Edgar que se acaba de unir a la comunidad de patreon muchísimas gracias y por supuesto también no puede faltar el agradecimiento a nuestros sponsors en este caso on branding una empresa formada por especialistas en varios ámbitos profesionales que se enfocan la reputación online a múltiples niveles han ayudado desde personas como tú y como yo hasta famosos a llegar a llevar a juicio casos de ciberacoso mitigar situaciones donde la reputación de empresas estaba siendo mal intencionadamente dañada e incluso borrar la huella digital que dejamos online no Solo han decidido Apoyar el podcast sino que si le contáis que venís de parte de tierra de hackers tendréis un descuento especial en sus servicios si necesitáis algún tipo de ayuda con vuestra identidad digital on branding es lo que estás buscando visita o bra es o nbran de ing punto es y también agradecer como siempre que nos lleva apoyando desde el principio a monat una empresa que comparte los mismos valores que nosotros hacer la seguridad más accesible y transparente nosotros a través de un podcast y monas con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley y que está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echarle un vistazo a su web monat.com y mandarle vuestro currículum a tierra de hackers @monat.commond.com Bueno nos ponemos al lío en este caso sólo Tendremos una noticia que es la que cubro yo ya que nos falta Alexis pero es una muy interesante de esos temas favoritos del podcast como os digo Siempre el ciber espionaje eso es de lo que os voy a hablar hoy centrándonos como no en Rusia la guerra con Ucrania bueno Lamentablemente sigue su curso y no parece que vaya a solucionarse el conflicto en un futuro cercano además unas hace unas semanas hemos visto como los propios aliados de Rusia creaban una revuelta posicionándose en contra de su propio líder Vladimir Putin habló del incidente en el que el grupo paramilitar ruso Wagner que está combatiendo mano a mano con las fuerzas militares rusas decide abandonar la primera línea de batalla y mover sus tanques rumbo a Moscú para bueno teóricamente deshacerse de Putin no al final quedó en nada Pero está claro que muchos ciudadanos rusos Están en contra de la guerra y sobre todo de Putin y Putin no va a permitir desde luego otro desafío a su autoridad como el que pasó hace varias semanas por ello y según un reciente artículo del New York Times el gobierno ruso ha incrementado sus inversiones En tecnologías de espionaje masivo pero para llevarlo a cabo en territorio doméstico contra sus propios ciudadanos se trata de tecnología para poder monitorizar la vida de los habitantes rusos y detectar cualquier amenaza local a su liderazgo espionaje masivo digital con un nuevo arsenal de herramientas compradas

a empresas especializadas en el desarrollo de herramientas de este tipo el New York Times destaca las declaraciones de una política rusa de la oposición en este caso y también activista por derechos en la era digital que y dijo lo siguiente la gente está paranoica porque comunicarte con cualquier otra persona en Rusia es un peligro porque no sabe si esa conversación Es realmente privada están monitorizando el tráfico de internet seriamente solían espiar digitalmente activistas pero ahora lo han expandido a cualquiera que ellos consideren que tiene una opinión contraria a la guerra bueno Y a quién está comprando Rusia todas estas herramientas Pues a empresas rusas de hecho todo es parte de una especie de holding o empresa matriz llamada Citadel Group cita del grupo es un conglomerado de empresas centradas en el desarrollo de soluciones de vigilancia digital y en su momento controlada por Alice share usmanov que fue sorpresa sancionado en su día por la Unión Europea y de hecho es uno de los oligarcas predilectos de Putin según el artículo las empresas en Sí pues son mf y soft experts protay y bueno y otras que en su día se centraban en ayudar Parece ser a implantar un sistema de interceptación de llamadas telefónicas pero que en los últimos años han pivotado a crear herramientas mucho más sofisticadas Esto no es especulación el medio de comunicación de Times obtuvo cientos de documentos internos de estas empresas de un exempleado que mostraban entre otros esquemas técnicos de las herramientas capturas de pantalla emails y de todo esto muchos estaban directamente relacionados con las herramientas de monitoreo que venden o centro más al detalle una de ellas una de las herramientas describe la capacidad de poder detectar cuando la gente hace llamadas por Telegram Signal y WhatsApp clarificar aquí inmediatamente que no es que sea capaz de interceptar el contenido es decir la conversación en Sí porque Signal y WhatsApp están cifradas extrema extremo pero al estar todo internet controlado en Rusia sí pueden inferir detalles y metadatos de hecho una de las herramientas de la empresa mf y soft permite precisamente ver como un tipo de dashboard no de de panel con información categorizada de todo el tráfico de internet generado por cada usuario de cada proveedor de internet es decir esto es como si aquí en España el gobierno español por Cada ciudadano tiene así como una especie de gráficos de todo el tipo de tráfico en internet que estamos generando pues podrán ver con qué servidores conectas a través a través por ejemplo de peticiones dns e ips Si usas tecnologías de anonimato como VPN so Thor ver qué aplicaciones utilizas para comunicarte porque va a ver que le estás hablando con el servidor de WhatsApp de Telegram de Signal ver qué páginas evidentemente estás visitando porque con las ips y tal pues se puede inferir no a ciertas páginas por ejemplo también si un individuo está utilizando Esta es otra de las capacidades de estas herramientas si está utilizando varios teléfonos como un burner phone por ejemplo este programa tiene el nombre de net beholder y fue desarrollado también por la empresa mf y soft y no solo puede detectar Si una persona tiene dos teléfonos sino también si dos teléfonos distintos han estado juntos en algún momento del día esto que no parece tan importante en realidad se utiliza para ver si dos objetivos y dos personas de tu interés han estado juntos en algún momento Como por ejemplo para reunirse también tiene la capacidad de mapear relaciones entre personas a través de las llamadas interceptadas Al fin y al cabo al saber con quién te comunicas sabe con quién te relacionas también puede decir puedes pedirle que triangule qué teléfonos han estado en una zona del mapa en concreto en una zona en un sitio en Rusia por ejemplo donde se ha llevado se me ocurre a cabo una manifestación una manifestación perfectamente pacífica contra la guerra por ejemplo pues puedes saber todas las personas que han acudido ahí porque puedes ver todos los teléfonos que han estado en esa zona en concreto Pues también se detalla en estos documentos un producto que puede interceptar credenciales es decir nombres de usuario y contraseñas introducidos en páginas sin cifrar esto lo puede hacer cualquiera en realidad en tu red local porque estamos hablando de

páginas sin cifrar pero es que aquí estamos hablando de todo Rusia y otra prueba de que controlan y monitorizan todo el tráfico de internet que pasa o toca en algún momento alguno de los servidores localizados sobre territorio ruso la empresa protei por su lado desarrolla tecnología comentan aquí voice to speech que se usa para transcribir de manera automática las llamadas telefónicas interceptadas procesarlas directamente el texto en este caso en busca de palabras clave pero lo más destacable es que uno de los documentos filtrados habla directamente de un wire Tab Market una especie como de App Store de tecnologías varias de espionaje masivo un supermercado de Hardware y Software para mantener vigilados a la ciudadanía según Adrián shabat que es el bueno vicepresidente de freedom House que se encarga de bueno de hacer estudios de casos de opresión política por parte de gobiernos opresores los efectos de estep market No de este supermercado del espionaje se notarán primero digamos en las zonas colindantes a Rusia porque evidentemente ya en Rusia ya está pasando pero él menciona que potencialmente afectará al mundo entero menudas declaraciones asusta la verdad si miramos atrás en las últimas dos décadas Rusia empezó ordenando que se expiasen las llamadas telefónicas y los SMS que bueno por defecto sabemos que no van cifrados no es que recordemos que quiero hacer aquí un hincapié que aquí hablamos de espionaje masivo no hablamos de la utilización de cero days que eso no escala no O sea tú no puedes instalarle Por decirlo un pegasus a todos los ciudadanos de tu país pero lo que sí puedes controlar es internet por eso el cifrado es tan tan importante pero claro vemos Que incluso hoy en día en 2023 con internet mayormente cifrado los metadatos muchas páginas que todavía están sin cifrar los teléfonos móviles el protocolo gsm SMS todo eso todavía da muchísima información súper valiosa para un gobierno sobre todo para un gobierno opresor entonces por eso aunque parece aquí Que bueno que realmente bueno no saben el contenido de lo que escribes en WhatsApp bueno no saben que tus credenciales que en páginas cifradas pero como os comento aquí pues Pueden saber con quién quedas con quién te relacionas Cuando haces una llamada Qué tipo de programa utilizas si has estado en un sitio todo eso es súper valioso Pero bueno continuo ya os comentaba que esto realmente empezó en Rusia hace décadas pues monitorizando pues eso llamadas telefónicas y SMS porque no iban cifrados y ellos controlan todo el tráfico de Internet pero en su empeño por seguir controlándolo y con las nuevas tecnologías y sobre todo que hoy en día la gente se comunica por Apps seguras utilizando cifrado extremo extremo empezaron a demandar que los proveedores de internet almacenasen todo el tráfico que fluye por su infraestructura para posterior análisis es así como luego estas herramientas que os estoy mencionando pueden funcionar Este programa tenía hasta un nombre formal System for operative investigated activities o sorm pero no era del todo eficaz porque por un lado con la implantación como decía de nuevas tecnologías de gsm como 4G LTE etcétera las operadoras telefónicas no podían captar todo el tráfico y por otro lado lo que capturaban y almacenaban pues es que al final era demasiado para ser procesado por el gobierno ruso en busca de enemigos del estado o sea cuántos habitantes hay en Rusia cuánto tráfico en internet se genera por eso el gobierno ha recurrido a empresas privadas para modernizar sus capacidades de espionaje masivo en territorio nacional y Citadel ha sido uno de los grandes beneficiarios de este cambio de paradigma tanto es así que Estados Unidos hace un par de meses anunció sanciones directas contra cita del grupo Porque ahora mismo atención es el responsable de un 70% de toda la tecnología utilizada en Rusia para espiar a sus propios ciudadanos esto es como si en España pues tenemos a una empresa española desarrollando tecnología para espiarnos a todos que va totalmente en contra de nuestra Constitución lo peor de todo es que los ciudadanos rusos no tienen mucha alternativa para protegerse de estos abusos a su privacidad por mucho que usen Apps con cifrado extremo a extremo para comunicarse pues lo que digo como WhatsApp Apo

Signal Rusia controla todo tráfico y la herramienta como net be holder que os contaba utiliza lo que se conoce como Deep paqueting inspection para extraer todos los metadatos posibles e inferir toda la información que os contaba al principio de la noticia esto es un poco pues como funcionan algunos firewalls no que miran un poco tu tráfico para ver si lo quieren bloquear o no tenemos también a veces en empresas temas en este no es el caso pero que se puede utilizar certificados privados pues para descifrar tu tráfico no cuando estás trabajando en tu empresa y asegurarse que no hay malware y luego lo vuelven a cifrar y cosas así Bueno es un poco esas tecnologías el cifrado extremo extremo esconde protege no el contenido de tus mensajes pero no con quién te estás comunicando cuando te estás comunicando qué app estás utilizando para comunicarte etcétera es por esto que Signal ofrece por ejemplo una opción que intenta transferir el tráfico mediante servidores alternativos como dando digamos salto sec adicionales para dificultar un poco la inspección del tráfico o Telegram por su por su parte llega a ofuscar el tráfico para hacer más difícil la detección en este caso de que se trata de tráfico relacionado con Telegram termino la noticia Pues con unas declaraciones de uno de los investigadores de freedom House que dice que si bien china es el culmen del autoritarismo digital Rusia se está posicionando como un claro competidor ya sabéis queridos oyentes podemos vivir en el país más democrático del mundo con el gobierno más Pacífico y progresista del mundo mientras exista la tecnología lo único que hace falta es un cambio de gobierno una guerra inesperada o cualquier otro imprevisto para que todo cambie y empecemos a vivir en el mundo que también describió George orwell en su fantástica novela 1984 hasta aquí hemos llevado queridos oyentes Muchísimas gracias por estar ahí como siempre lo digo no olvidéis dejarnos reviews Esas cinco estrellitas donde podáis que nos ayuda un montón nos ayuda a traer más sponsors nos ayuda a poder seguir creciendo sois los mejores nos vemos y nos escuchamos en el próximo episodio Adiós adiós si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de