el hecho de visitar una página web a través de http en vez de https lleva la infección del móvil del candidato a la presidencia de Egipto nueva entrega de este vuestro podcast comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast Hoy es el 2 de octubre de 2023 es el episodio 107 yo soy Martín vigo y vuelve a estar ausente Don Alexis porros un currante un viajante así que me tenéis a mí solo como siempre recordaros que estamos disponibles en todas las redes sociales esto incluye Facebook Instagram Twitter por supuesto estamos en tiktok bajo el handle tierra de hackers Y tenemos una comunidad fantástica en discord que puedes entrar yendo a tirode backers punc com bar discord y por supuesto si os queréis poner en contacto con nosotros a través del correo electrónico tenéis podcast @r deckers.com antes de comenzar quiero eh comentaros Un par de cositas voy a estar en la conferencia navaja negra en albacete una conferencia que a mí personalmente me encanta así que si hay alguno de los oyentes que están por allí el año pasado me hinchéis a sábado y que llevo el doble de pegatinas porque es que no me llegaron el año pasado así que tengo muchas ganas de veros a todos en persona y hablar con todos vosotros recordaros también que si sois desarrolladores web o queréis aprender sobre seguridad en ese entorno podéis apuntaros ya al curso de cy Security for web developers que voy a estar impartiendo de manera presencial en Barcelona el 7 y el 8 de noviembre con una colaboración con el Barcelona code School es en inglés y está orientado a que aprendas y comprendas las vulnerabilidades más habituales en el entorno web Así que ya sabes apúntate y si quieres más información lo tienes en tierradel comom bar websecurity como siempre no nos olvidamos de nuestros queridas mecenas que hacen este podcast posible en esta semana le vamos a dar las gracias a Juan que acaba de añadirse a la familia de los que nos apoyáis en patreon y también a nuestros patrocinadores que tenemos dos esta vez home branding una empresa formada por especialistas en varios ámbitos profesionales que se enfoca en la reputación online a múltiples niveles han ayudado desde personas como tú y como yo hasta famosos a llevar a juicio casos de ciberacoso mitigar situaciones donde la reputación de las empresas está va siendo dañada e incluso a 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 on branding.xml hacer la seguridad más accesible y transparente nosotros a través de un podcast y monat con una herramienta de gestión y visualización de telemetría y datos de seguridad fundada en silicon Valley que está buscando ingenieros con experiencia en ciberseguridad para poder ayudarles a 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 le podéis enviar vuestro currículum a tierr deeh hackers @mon comom nos ponemos con las noticias vamos a lío hoy toca hablar de los peligros de las comunicaciones no cifradas hoy se trata de viajar al pasado años atrás cuando internet funcionaba mayormente sin la capa decifrado que muchos conocéis como https pasado pero presente también ya que Todavía existen múltiples páginas web que siguen siendo accesibles sin cifrar y que nos llevan a la noticia de hoy la infección del móvil de uno de los candidatos de la oposición a las elecciones de Egipto candidato que pretende arrebatar la presidencia democráticamente al actual mandatario abdel fatah el sisí pero que parece ser que no le ha hecho gracia y ha decidido llevar a cabo su particular watergate esta investigación viene por parte de nada más y nada menos que citizens lab y el equipo tag de Google que ya sabéis porque os hablamos en varias ocasiones que son expertos en análisis de malware y campañas de ciberespionaje global esto es un ejemplo más de los peligros de la oscura Industria del desarrollo de armas cibernéticas software espía y creación de exploits de tipo Zero day que se venden al mejor postor sin ningún tipo de control Esto va a ser un ejemplo de cómo se usa y reusa políticamente sin ningún tipo

de respeto por la democracia este tipo de exploits Esto va a ser un ejemplo también de como decía de la importancia que tiene la criptografía en nuestras vidas empecemos por el principio la víctima de este ataque de espionaje gubernamental es ahmed el tantawi un miembro del parlamento egipcio que hace unos meses anunció sus intenciones de presentarse como candidato a la a presidente en las elecciones que se van a celebrar en diciembre de este año en Egipto el presidente actual ya lo ya os lo he presentado antes pero no os comenté que desde que llegó al poder son numerosos los escándalos de corrupción y abuso de poder en los que se ha visto envuelto amnistía internacional Human Rights watch han publicado neros numerosos informes sobre la represión a la que están expuestos los activistas o simplemente la oposición política en ese país con este escenario el tantawi recordamos el candid el candidato a la presidencia pues un día empezó a sospechar que su teléfono podría estar infectado y como tantos otros a día de hoy contactó con citizens lab que ya conocéis de sobra por este podcast citizens lab ya había encontrado en dos ocasiones teléfonos infectados de miembros de la oposición en el parlamento egipcio concretamente infectados con un malware desarrollado por la empresa crox y que es conocido como PR y del que de hecho tenemos un episodio específico hablando de este malware básicamente pensar que es el equivalente a pegasus desarrollado en este caso en vez de por crox por nso Group pues este caso no iba a ser diferente y tras un análisis forense citizens lab encontró que efectivamente el teléfono del tantawi también estaba infectado con el mismo malware al igual Insisto que en el pasado otros dos miembros de la oposición en en Egipto citizens lab contactó con el tag Team de Google del que también ya os hablé en ocasiones anteriores Y se pusieron manos a la obra concretamente a indagar en el Cómo fue infectado el teléfono con el malware Predator recordemos una cosa es el malware que encuentran instalado en el móvil Pero cómo llegó ese malware ahí Qué mecanismo utilizaron para que el teléfono instalase el software malicioso pues explotaron concretamente tres vulnerabilidades desconocidas hasta el momento y que Apple reportó como la primera CV 2023 41 991 cuya descripción es vulnerabilidad que permite a una aplicación maliciosa instalada en el teléfono saltarse la protección de la validación de La Firma criptográfica la segunda vulnerabilidad que explotaron es el CV 2023 41 992 descrito como un ataque local permite la capacidad de Elevar privilegios un atacante local no un ataque local yo esto lo entiendo como que si tienes ejecución de código limitada en el teléfono no como suelen tener las aplicaciones puedes obtener privilegios reservados solo al sistema operativo como tipo k por tanto estamos hablando del típico privilege escalation que vemos mucho frecuentemente en sistemas operativos como Windows o Linux Vale y explotaron una tercera vulnerabilidad la CV 2023 4193 aquí la descripción comenta que el procesamiento de una página web maliciosa puede llevar a la ejecución de código arbitrario Okay pues como decía explotaron estas tres vulnerabilidades por tanto aquí estamos hablando de encadenar vulnerabilidades vulnerability Chain que le que le dicen y menciono esto porque yo recuerdo o ir a una charla de una de los miembros e del grupo de project Zero de Google e una chica concretamente que es una experta justo ahora pues no me viene el nombre a la cabeza pero se hizo muy famosa por hackear los tamagochis Sí sí pero es una una auténtica crack Pues en una charla dije una frase que me quedó muy grabada que y de hecho fue una respuesta una pregunta de la audiencia que le venían a decir Oye a día de hoy los dispositivos móviles Cuántas vulnerabilidades crees que hacen falta para comprometerla no porque una cosa es las vulnerabilidades pero luego hay que explotarlas para poder llevar a cabo pues por ejemplo la instalación de malware y Ella decía que mínimo dos no una sino dos y lo explicaba de la siguiente razón una vulnerabilidad es la que te da acceso a código en el móvil Pero es que luego tú tienes que conseguir los suficientes privilegios porque normalmente para que tú explotes una vulnerabilidad en un dispositivo móvil pues es a través de una app maliciosa

instalada como vemos aquí pues visitar una página web o que tú pues yo que sé leas un mensaje o en WhatsApp o lo que sea no pero claro normalmente ahí si bien Tienes ejecución de código controlas digamos parte del teléfono Estás limitado por el tema del sandbox por el tema de cómo está diseñado el sistema operativo estás limitado limitado al entorno de esa aplicación que acabas de explotar Pero tú para llegar a instalar malware al nivel que estamos viendo aquí tienes que tener un control total de ejecución de código sobre el dispositivo por tanto tienes que insisto encadenar vulnerabilidades los dispositivos móviles ya tienen una seguridad tan elevada que no vale con una vulnerabilidad tienes que encontrar varias Y en este caso tres tres de tipo cero day Okay pues tenemos el malware que instalaron Y tenemos las vulnerabilidades que se explotaron para llevar a cabo la instalación del malware pero nos falta una cosa Cuál fue el punto de entrada Cuál fue la acción que llevó a cabo la víctima si es que hubo alguna que llevó al escenario posible de poder explotarse estas vulnerabilidades que os menciono y con ello instalar remotamente el software malicioso pues la respuesta a esta pregunta es en parte la razón por la que pensé que merecía la pena traeros esta noticia porque la verdad es que me es bastante inesperada Un Man in the middle pero un Mag in the middle muy interesante antes de nada como Tenemos muchos oyentes menos técnicos un ataque de tipo Mag in de midle o traducido hombre en el medio pues es un tipo de vulnerabilidad en la que alguien tiene acceso a pues por ejemplo en el concepto de internet pues al al tráfico o a los paquetes o a la información que está yendo desde tu dispositivo al servidor que estés visitando Y es capaz de modificar ese tráfico alterarlo de alguna manera aquí no estamos hablando por supuesto observarlo e de tal manera que claro puede hacer que tu dispositivo móvil pues vaya a una página web diferente puede ver qué información estás enviando puede ver qué páginas estás visitando cosas de este estilo el equivalente sería por ejemplo si pues tú imagínate el típico patio de un edificio no Y la vecina del quinto pues habla gritos con la vecina del del tercero no y dice Maruja qué vas a cocinar hoy y la vecina del tercero dice pues croquetas tal y están hablando a gritos en el patio No claro los demás vecinos pueden escuchar eso Entonces claro esto es un problema mientras una vecina se comunica con la otro todos los demás pueden estar escuchando lo que está pas lo que se están diciendo no Esto es lo que sucede cuando tú básicamente visitas una página web sin cifrar Pues todo el tráfico que va desde tu ordenador a tu proveedor de internet ese proveedor pongamos que la página web la estás visitando una página web China de tu proveedor de internet va a un punto Eh Pues en tu país en tu capital de ahí va a un punto dentro de tu continente de ese continente va por el cable transatlántico hasta Asia de Asia va a China de China claro pasa por muchos puntos por muchos ordenadores por muchos servidores esa información y sin cifrar Entonces cuando visitamos páginas web de tipo https no donde se utiliza pues eh cifrados certificados y todo esto Pues eso sería el equivalente a que las vecinas todavía se comunican a gritos es decir todo el mundo puede escucharles pero no de manera que lo puedan entender Pues yo que sé pues ponte que las vecinas como saben chino pues se ponen a hablar a gritos pero en chino entonces el resto de los vecinos lo puede escuchar pero no lo puede descifrar no lo puede entender pues ahí es donde está el valor del cifrado entonces resumiendo un ataque de hombre del medio es tener la capacidad de escuchar de ver las comunicaciones y además entenderlas o modificarlas Pues ahora que entendemos esto por qué hizo falta un ataque de hombre en el medio The man in the middle para infectar el teléfono de este político bien fijémonos en lo que nos dice citizens lab que fueron las vulnerabilidades que explotaron y la descripción que les da Apple y que os mencioné antes concretamente fijémonos en la tercera vulnerabilidad el CV 2023 41 993 recordar decía lo siguiente el procesamiento de una página web maliciosa puede llevar a la ejecución de código arbitrario Ajá aquí podemos sacar la conclusión de que el vector de entrada es una página web maliciosa que es capaz de explotar

una vulnerabilidad en el navegador Safari que trae por defecto los iphones y que lleva la ejecución de código arbitrario ya luego encadenas las otras dos vulnerabilidades para tener ejecución a nivel de kernel okay O sea que la víctima ha de visitar una página web maliciosa para que se infecte el teléfono algo por cierto que ya hemos visto en muchas ocasiones pero que lamentablemente para los atacantes requiere que la víctima lleve a cabo una acción digamos visitar esa página maliciosa y a veces pues se consigue engañándolo enviándole un email lo que sea no no podemos convertir este exploit en uno de tipo cero click donde no se requiere ningún tipo de interacción por parte de la víctima O tal vez sí pues cuando el atacante es el propio gobierno con todo el poder que tiene la respuesta es que sí podemos convertir un exploit de un clic en cero clic y de la manera más compleja y a la vez más sencilla del mundo resulta que nuestra víctima utilizaba Como operador telefónico vodafone de Egipto Sí sí el el vodafone que probablemente existe en tu país y desde luego en España también querido oyente y qué pasa con tu operador Pues que aparte de darte servicio para tus llamadas y mensajes También te da conexión a internet es decir tiene control sobre tu tráfico okay no nos asustemos aún para eso existe precisamente la criptografía y mecanismos de cifrado como ssl tls que cifran nuestras comunicaciones en internet lo que os decía antes de que las vecinas hablasen en chino y además nos protegen de muchos ataques incluidos el de hombre en el medio en el medio mediante cosas como certificados Pero qué pasa si visitas una página web que no está cifrada una web alejada mediante http en vez de https para que los menos oyentes menos técnicos me entiendan pues que no existe cifrado y aparte de que tu operador telefónico puede ver toda la información que se intercambia el servidor que almacena la página web y tu teléfono también puede hacer otra cosa otro ataque redirigir a una página web diferente y eso es exactamente lo que sucedió nuestro querido el tantawi visitó una web que no estaba alojada de tal manera que Us que usase cifrado para proteger las comunicaciones y mediante un ataque de hombre en el medio su móvil fue redirigido a una página diferente una página maliciosa que estaba almacenada concretamente en sefler comom y que contenía el código malicioso para explotar la vulnerabilidad que afectaba al navegador Safari que resultó en el hackeo de su terminal pero ostras dirás tú querido oyente Cómo que le rediriger a una página web maliciosa cuando estaba intentando visitar una benigna vale que si vas a una web sin cifrar se puede hacer pero para eso Alguien tiene que estar en tu misma red No sí y no vale que cuando es un atacante externo efectivamente tiene que estar en en la misma red conectado a la misma WiFi que tú para que me para que me entendáis no para eso eso es requerido para llevar a cabo este ataque Pero sabes quién está en tu misma red también tu operador telefónico ya que es el que te da internet y diréis pero Martín qué me estás queriendo decir que vodafone redirigió después de monitorizar el tráfico del tantawi para para llevarla a una web maliciosa Pues sí querido oyente como dije antes cuando eres el gobierno mandas cuando eres el gobierno tú controlas las empresas privadas cuando eres el gobierno si hay que saltarse la ley tienes la capacidad de saltarte la ley con esto voy a subrayar que no quiero decir que vodafon Egipto esté en el ajo o de acuerdo con ello solo digo que el gobierno controla las infraestructuras críticas que los servicios de inteligencia tienen mucho poder y que no es secreto que incluso en países como Estados Unidos existen puntos que procesan el tráfico de internet y que están cont ados por los gobiernos citizens lab reporta que mediante diferentes pruebas que no me voy a parar a explicar aquí ya que es si no tardaría mucho pero que por supuesto os dejo en la el reporte de citizens lab y de Google tag en las notas del episodio fueron capaces de encontrar un dispositivo en algún punto de la red de hecho concretamente a cuatro saltos del móvil del tantawi con saltos me refiero a máquinas por las que pasa el tráfico de internet y cuyo único objetivo era monitorizar todo el tráfico de internet de Egipto y redirigir a cualquiera que visitase una página web sin cifrar a una página maliciosa

una vez en esta página web maliciosa se verifica si el terminal atención pertenecía a alguna de las personas de interés para el gobierno y de no ser así se le volví a redirigir otra vez a la página web que estaba visitando originalmente pero en caso de tratarse del Terminal de uno de los objetivos del gobierno se procedía a infectar el dispositivo flipa chaval hablamos de un Man in the middle a nivel nacional una pasada citizens lab mediante su investigación dio incluso o sea da Incluso el tipo de Hardware usado para hacer estas redirecciones maliciosas en medio de la red de vodafone un dispositivo de red Industrial conocido como sandin packet logic y cuyo fabricante fue notificado por parte de citizens lab para que supiera cómo se estaba utilizando en Egipto pero citizens lab jamás recibió una respuesta de este fabricante curiosamente este mismo dispositivo ya fue usado en Turquía para propósitos similares el monitoreo y alteración del tráfico de internet a gusto del gobierno Cómo podría haber evitado este ataque la víctima o bueno cualquiera de otros Pues en el caso del iPhone con el famoso lockdown Mode que Apple ha puesto a disposición de los usuarios y que ya cubrimos en este podcast un mecanismo de seguridad existente en todos los dispositivos de Apple que reduce significativamente la superficie de ataque con la consecuencia de reducir por supuesto su funcionalidad concretamente pues para este caso el lockdown Mode nos no permite visitar páginas web sin cif por lo que nuestra víctima no hubiera podido visitar la página web que quería pero tampoco hubiera sido posible infectar mediante este vector de ataque que os acabo de contar desde luego yo recomendaría a cualquier ciudadano de Egipto o bueno incluso a cualquiera persona que quiera visitar ese país y lleve su móvil consigo al fin y al cabo tú te conectas a la red móvil de Egipto cuando pisas ese país pues que active este modo que se puede hacer de manera temporal aunque no seas una persona de interés para ellos si están monitorizando Todo internet a saber qué más cosas hacen por cierto a veces escuchamos voces críticas con las VPN ya que bueno efectivamente hay muchas empresas utilizando publicidad engañosa por ejemplo youtubers exagerando los beneficios de las vpns pero en este caso también hubiera evitado este ataque ya que a pesar de que la web en concreto no estaba cifrada la capa decifrado de la VPN hubiera bastado para evitar que el dispositivo colocado entre la red de vodafone y Telecom Egipto pudiera ver o Modificar el tráfico así que ya sabis queridos oyentes ya tenemos otro uso para las vpns otra justificación si vais a algún país que os da mala espina tenéis la opción por lo menos en los dispositivos de de Apple de meter el lockdown mode y ya veis que a veces no hace falta exploits de cero days para explotar tu dispositivo sin ningún tipo de interacción por tu parte si eres la víctima si estás haciendo un ataque de hombre en el medio a nivel nacional puedes hacer que cualquier persona que visite una web insegura sea redirigido de manera transparente a la web maliciosa que contiene el código que va a resultar en tu móvil estar completamente comprometido y a Merced de quien sea el atacante que en este caso como vemos y por motivos políticos era el propio gobierno sin más queridos oyentes recordaros que nos podéis contactar en podcast @ticktok 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