71. Tik Tok y BYOVD

tenemos nueva polémica en torno al seguimiento y espionaje de usuarios de aplicaciones móviles esta vez por parte de tiktok que ha decidido usar las capacidades de su equipo de auditorías internas para rastrear a ciudadanos americanos sin su conocimiento ni consentimiento Microsoft falla en actualizar una lista de drivers bloqueados que ransomware ha abusado en ataques del tipo bring you on bonaebol driver en la última década y que pudiera haber prevenido muchos de estos incidentes de los últimos dos años Bienvenidos a un nuevo episodio de tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 24 de octubre de 2022 este es el episodio número 71 yo soy Martín vigo y está conmigo en modo Root con privilegios de administrador y con acceso a nivel Dios Alexis porros Hola Alexis qué tal Muy bien Martín aquí como me des como tenga tantos privilegios yo necesito un poco de control aquí que a ver si se me se me va la olla como dicen por ahí no pero nada nada por aquí con gran poder viene gran responsabilidad no o algo así que decía despido justo justo o no sé quién o el abuelo no joder yo de Marvel y todo esto se pone bueno igual lo dijo igual haciendo las palabras de su de su tío creo que era peor Anyway Como sea pues nada sigue aquí contigo Martín un día lluvioso por aquí por la costa este y nada a todos nuestros oyentes allá donde estéis en el mundo con Días nublados o soleados en casa o en la playa que sería lo suyo daros siempre como siempre las gracias por seguirnos en todas las redes sociales todas las preguntas comentarios sugerencias noticias que vais viendo que nos enviáis Muchas gracias queríamos recordaros también que os podéis suscribir ya mismo en vuestra plataforma de escucha favorita para estar al día de todos los episodios que hemos publicado y que los puede escuchar justo cuando salen calentitos del horno estamos en todas las redes sociales Twitter Instagram y Facebook con el handel@tierra de hackers linkting YouTube y Twitch como tierra de hackers los emails A dónde Pues al podcast @ tierra de hackers.com y en discord tenemos hay bastantes usuarios llegando a los 800 pronto pues podéis entrar vía tierra de hackers.com/discord Finalmente pues agradecer vuestro apoyo la pregunta del episodio que publicamos la enviamos siempre en Twitter y podéis votar Y en este último caso en el episodio anterior la pregunta fue la siguiente A qué nivel crees que puede afectar este ataque de tipo hyper jacking o malware de hipervisor a usuarios normales como tú y como yo tenemos cuatro respuestas como siempre como normalmente la más votada de hecho con un 51%, Pues el nivel que votaron fue medio que porque corren estos estos votantes corren sus máquinas virtuales en local seguida de un 23% elevado riesgo Porque vivo en Matrix tenemos un 16% la tercera con nulo la verdad es que no uso virtualización Así que es esos usuarios bastante interesantes y nos gustaría estudiar su caso y en último lugar tenemos un 10% medio porque mis máquinas virtuales están en la nube y también es preocupante que que estén ahí que puedan ser vulnerables a este ataque así que tenemos a 18% de oyentes nos escuchen desde Matrix Me gustaría saber qué plataforma de podcast utilizan para escucharnos en Matrix tío Bueno yo por mi cuenta comentar que tierra de hackers va a estar en la conferencia navaja negra voy a intentar ir yo que es dentro de dos semanitas así que a ver si me veis por ahí con la camiseta de tierra de hackers seguramente tenga pegatinas en el bolsillo O sea que venir a saludar que como os decimos siempre nos encanta estar y conocer a los oyentes es una pena que Alexis no pueda Pero bueno intentamos ir a todas las conferencias de ciberseguridad que podemos también agradecer a un nuevo mecena que tenemos de patreon Muchísimas gracias Jordi Rivas por hacerte patreon y

apoyarnos económicamente tierra de hackers es esencial vuestro apoyo Así que si tú también crees que puedes apoyarnos pues tierra de hackers.com/patreon o bueno patrón puntocom barra tierra de hackers como tú quieras Así que muchísimas gracias También a nuestros sponsor monad como siempre una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast de monad a través de una herramienta de gestión y visualización de telemetría de seguridad una empresa fundada en sirocon Valley y ya sabéis que está buscando empleados Incluso en estos tiempos tan turbulentos y además en remoto así que ya sabéis les podéis contactar en su web monad.com m o nad.com y concretamente le escribís a tierra de hackers @monat.com y yo creo que ya con esto empezamos y yo pues vengo a hablar de un artículo que Forbes el conocido medio de comunicación norteamericano ha escrito y es que ha tenido acceso al documentación y grabaciones de llamadas internas entre empleados de tiktok que muestran que la empresa madre de tiktok pite tens ha planeado acceder a la geolocalización de ciertos ciudadanos americanos Forbes publicó Hace cuatro días un artículo cubriendo esto y me ha llamado bastante la atención no solo por el tema de que tiktok es usado por millones y millones y millones de personas sino también porque es una empresa china basada en China y que parece que está usando la app pues para espiar a individuos de otras naciones en bytes hay un equipo que se encarga Digamos como de asuntos internos investigaciones contra empleados ex empleados de byteens cuando ocurre algún tipo de denuncia despidos etcétera no esto la verdad es que es bastante habitual en empresas sobre todo en grandes y hasta ahí pues todo bien Esto este equipo forma parte del departamento de auditorías internas y control de riesgos y está liderado por sonye que reporta directamente al ceo de bytes como decía hasta aquí todo correcto Supongo no el tema es que la investigación de Forbes menciona que los ciudadanos americanos de los cuales se planeaba extraer información de geolocalización no habían sido nunca empleados de tiktok ni de bytes dance dicho de otra manera si bien existe la capacidad de geolocalizar a empleados de tiktok para teóricamente gestionar investigaciones y recopilar más información Parece ser que esa capacidad está siendo abusada por el mismo equipo de la empresa que es responsable de dichas investigaciones para rastrear a ciudadanos de otro país que nada tienen que ver con la empresa a nivel laboral insisto la investigación deformes no dice que se extrajo información de geolocalización de estos americanos sino que se estaba planeando hacerlo hago este inciso porque quiero ser lo más preciso posible y no consiguieron pruebas de que ya lo Hubieran hecho pero tal como está redactado dejan la posibilidad de que sí haya sucedido Solo que como no han encontrado pruebas de que ya se haya hecho sino que la documentación que obtuvieron era que se planeaba en algún momento hacerlo Pues claro lo dejan solo ahí aún así el hecho de que se estuviera planeando es motivo de Gran preocupación Porque si bien el representante de tiktok dijo que se recolecta información de geolocalización en base a la IP con fines publicitarios e investigaciones requeridas por las leyes vigentes del país eso es lo que dice el representante de tik Tok Lo cierto es que Forbes dice que la documentación obtenida muestra que el objetivo en el caso de los americanos era la y cito textualmente vigilancia Lamentablemente Forbes no da más detalles sobre la naturaleza de esta vigilancia porque dice que no puede ya que expondría a sus fuentes y los pondrían peligro es decir si da más datos sobre lo que contiene la documentación que la que contiene más información pondría en peligro no sé si su vida pero por lo menos que a lo mejor de perder su trabajo a las personas que les han contactado y les Supongo que les entregaron toda esta documentación interna es una pena porque nos quedamos así un poco con esto pero bueno sigamos cuando

Forbes preguntó a peitens si el equipo de auditorías internas y control de riesgos había espiado específicamente a activistas periodistas o miembros del gobierno norteamericano vitens no contestó A ver no tiene porque contestar pero a la vez cuando es un rotundo no no cuesta nada decir que no a veces El silencio es un poco revelador no pero bueno Esto es especulación mía hasta este punto lo que tenemos Es que es que by Dance la empresa que desarrolla tiktok entre otros productos supuestamente ha planeado utilizar las herramientas y capacidades de investigación de su cupo de asuntos internos Por así decirlo para rastrear la geolocalización de individuos en Estados Unidos que la verdad sabemos de Estados Unidos porque Forbes Supongo que eso es lo que se centró pero si planean hacerlo a ciudadanos americanos Supongo que a españoles mexicanos colombianos argentinos y todos los demás países también porque porque iban a limitarlo no esto por supuesto ya una vez más es especulación mía sin ninguna base más que mi opinión Pero bueno es de estas noticias que que muchas veces cubrimos sobre Estados Unidos pero nos enteramos Pues porque allí Pues hay muchos periodistas y muchos medios que está muy centrado es en temas de abusos de privacidad porque allí hay muchas empresas y todo esto pero no os olvidemos que a pesar de que nosotros cubrimos noticias a veces citando específicamente a Estados Unidos porque eso es lo que dice la noticia es extrapolable perfectamente a otros países incluido los nuestros y de toda nuestra audiencia Pero ha habido precedentes del abuso de aplicaciones populares para espiar de manera ilegal o cuando menos sin consentimiento de manera ilegítima a todo tipo de gente como tú o como yo querido oyente porque esto sería interesante o es tik Tok el primer caso pues no no es el primer caso hay precedentes el propio artículo de Forbes me ha recordado el incidente ocurrido con Uber en 2015 en el que se le acusó de rastrear la localización a periodistas críticos con la empresa esto lo hacían de modo parecido al que lo estaba haciendo tiktok utilizando herramientas internas que en el caso de Uber llamaban modo Dios y que permitía ver todos los datos que recolectaba la aplicación de los usuarios registrados en Uber incluyendo su geolocalización lo que era más grave Es que el acceso a esta herramienta tan poderosa no estaba realmente restringida Como debería y básicamente por lo menos a nivel ejecutivo todos tenían acceso a ella y Esto fue exactamente de lo que fue acusado uno de los ejecutivos de Uber monitorizar la geolocalización de una periodista de vas news que había publicado varios artículos críticos con la empresa recientemente recientemente me refiero a en el momento que sucedió todo esto este mismo ejecutivo fue pillado en una conversación privada con otro periodista del cual Él pensaba que era of the record pero no lo era diciendo que tenían que invertir un millón de dólares en contratar un equipo para ir a por periodistas críticos con la empresa investigar su vida privada Y cito textualmente darles de su propia medicina Cuando esto salió a la luz El Ejecutivo dijo que esto había sucedido una conversación privada que no reflejaba a su punto de vista y el de la empresa de Uber y que se disculpaba y todo esto pero bueno ya vemos de que de qué palo iba la gente ahí Uber también fue denunciado por el electronic privacy information Center También conocido como Epic por continuar monitorizando la geolocalización de los usuarios incluso después de que finalizase el viaje sin ningún tipo de justificación por lo menos en acorde a Epic no esto quiere decir que hace años tú utilizando Uber pues pides el taxi y cuando te deja el taxi Uber ya no necesitas saber a dónde vas o tal pues seguía registrando todos los movimientos después de haber finalizado ese viaje lo cual pues no no se explica mucho Uber lo que decías que eso ayudaba a mejorar Pues el servicio y todo esto un poco palabras genéricas no pero bueno uno de los factores diferenciadores del caso de Uber con tiktok es que tiktok recientemente ha estado trabajando con las diferentes

entidades jurídicas norteamericanas que regulan el acceso de los datos de los datos de los usuarios en Estados Unidos y les ha dicho que el acceso a los datos de ciudadanos americanos lo cual incluiría también los datos de geolocalización estará limitado a personal autorizado y siguiendo los protocolos establecidos por el gobierno de los Estados Unidos Esto es lo que dijo tiktok a los legisladores meses antes de que salías este artículo de Forbes esto es de hecho lo que tik toca denominado como proyecto Texas internamente en un intento de mantener toda la información de los usuarios de tiktok americanos en Estados Unidos físicamente básicamente han recreado toda la infraestructura de tiktok y la han copiado en servidores de hora que él que físicamente en Estados Unidos no solo eso sino que también teóricamente han restringido el acceso a estos servidores a solamente empleados de tiktok que trabajan en Estados Unidos físicamente también esto limitaría el acceso a China a información como fechas de nacimiento números de teléfono geolocalización y vídeos pues que evidentemente no se han llegado a publicar por parte de ciudadanos americanos no pero sorpresa sorpresa en junio de 2022 basfit publicó una investigación en la que mostraba que china seguía accediendo a toda la información generada por los usuarios norteamericanos mostrando que tiktok había mentido a los reguladores estadounidenses y por si eso es poco se filtraron un par de llamadas telefónicas en una de ellas un empleado del equipo americano de tiktok en concreto del equipo trusten safety le contaba su manager preocupado que Chris levytag el jefe de auditorías internas de tiktok en China le citó en un restaurante en Los Ángeles por la noche para presionarle a que le dijera dónde se hallaban los servidores de Oracle y los detalles técnicos sobre ello el empleado le decía a su jefe en esta llamada que se publicó que estaba Freak out no que estaba en shock por las presiones que había recibido para revelar esa información ahora que él ante este incidente hizo unas declaraciones públicas un poco lavándose las manos diciendo que ellos no tenían ningún control o información sobre quién o desde donde se está accediendo a los servidores de tiktok diciendo básicamente que si tik Tok china está accediendo a los servidores de hora que él en Estados Unidos ellos eso no lo saben esto encaja de hecho con la información publicada en la segunda llamada que se filtró en este caso entre un ejecutivo de tiktok en China y su amigo en el que decía que era casi incorrecto decir que en Estados Unidos tiktok corre sobre servidores de horakel que ahora que les había dado servidores ver metal y que eran ellos quienes instalaban sus propias máquinas virtuales todo esto qué quiere decir para nuestros oyentes menos técnicos pues esto es como si Oracle les da los ordenadores tal cual los servidores y tiktok instala ahí lo que les dé la gana con esto queriendo decir que ahora que él no tiene mucha monitorización o acceso de ningún tipo a esas máquinas a pesar de que son de hora que él pero como se las dan digamos enteritas para ellos En vez de tener Pues los servidores compartidos o digamos máquinas virtuales preinstaladas pues que tienen software de monitorización y cosas así pues en este no es el caso de tiktok y por tanto por eso ahora que él tiene tan poca visibilidad sobre lo que ocurre en esos servidores tiktok no contestó a las preguntas de Forbes en relación a toda esta investigación pero sí hizo una declaración pública que a mí me llamó bastante la atención a ver si a vosotros También cito textualmente estamos confiados de que estamos en camino de satisfacer todas las preocupaciones razonables del gobierno de los Estados Unidos repito y hago énfasis estamos confiados de que estamos en camino de satisfacer todas las preocupaciones razonables del gobierno de los Estados Unidos Esto es lo que a mí me llamó la atención la palabra esa de razonable o sea estamos en camino de satisfacer las que son razonables bajo nuestro punto de vista las otras Pues a lo mejor no no es un poco como interpreto yo estas declaraciones Qué pasa que si no son razonables desde su punto

de vista Entonces no la satisfacen y aquí no ha pasado nada bueno Esto un poco de modo jocoso pero si me llamó la atención porque estas declaraciones públicas sobre todo cuando son tan breves están las palabras muy muy muy estudiadas Entonces eso de razonables ahí me llamó bastante la atención es muy de no me mojo Pero te voy a contestar algo porque lo que estoy diciendo el silencio implica algo más claro un lenguaje muy muy político muy diplomático muy muy legal no Pues sí se veía venir yo creo porque bueno como otras empresas grandes no como Google y otras empresas así de de social media no que que se ha visto alguna noticias de vez en cuando Que bueno que por ejemplo en Europa no en la gdpr la el gobierno de Europa no creo que la multado alguna vez a Google creo que también por aquellos años 2015 por hacer aquello de las direcciones Mac no de los usuarios que las almacenaba y con ellos se podía digamos poder identificar la ubicación de usuarios de Google de alguna forma pero sí eso no no me no lo no lo recuerdo Qué interesante pero como con direcciones Mac sí que si no recuerdo mal sabían la localización pero como no entiendo eso cómo funcionaría si creo que registraban las direcciones Mac o de los teléfonos o de los puntos de acceso a los que se conectaban una E2 a de los routers o así entonces quizá porque estoy pensando a lo mejor en algo como google.net que tienes el s ID y el tal y como Google justo tenía los Street los coches cierto vale vale Ya ya recuerdo ahora mira Sí vale Vale ahora ya recuerdo es que estaba pensando en las direcciones Mac del teléfono o del ordenador Entonces no no sabía yo como traducirlo pero claro routers o así o que vale vale vale vale vale Sí sí sí sí sí ostras sí pues sí sí el gdpr claro Sí en parte también Europa en principio ha habido ahí incidentes con el tema de compartir datos con Estados Unidos porque allí están todas las empresas de tec mucho tema con esto de poder servir publicidad y tal como se intercambian entre empresas que tienen 50.000 otras empresas un rollo como alphabet no que también está muy regulado como entre las propias empresas de alphabet se pueden intercambiar datos pero sí tiktok desde luego claro cuando le damos el enfoque de China pues como que de repente nos asusta más no que a lo mejor es un poco inocente esto porque lo que debería asustarlo sería Estados Unidos pero pero bueno sí sí o sea esto aplica digamos Estados Unidos pero no sé si has leído no he visto mucho Yo tampoco Pero esto como aplica en Europa no creo que quisieran rastrear a o sea esto era algo que tenían planeado ellos hacer es decir en plan rascar los datos que iban almacenando o era una funcionalidad solo desplegada en aplicaciones para usuarios en Estados Unidos O también se despliegan en usuarios de resto del mundo Europa y se activa o no se activa o o se almacena la información igualmente y luego es cuestión de buscar o no buscar utilizarla para rastrear o no O como el tema es que utilizaban herramientas internas que están desarrolladas para como decía investigar casos de empleados específicos no que hasta ahí pues Puede ser normal lo que pasa es que pues esta documentación claro es que Forbes no da muchos detalles es lo malo en esta documentación aún así me pareció interesante traerlo Pues por todo tú incluso has cubierto noticias también de tik Tok según estaba polarizando porque un poco Empezamos el podcast un poco antes de que estuviera tiktok y presente o por ahí cuando estaba despegando pero básicamente claro es que no cita ni Solo dice ciudadanos americanos no sé si era Pues a lo mejor unos políticos unos periodistas o a lo mejor alguien crítico con el régimen chino es que no lo sé la cuestión es que no era una una fichar una funcionalidad o algo así sino que utilizaban sus herramientas internas al fin al cabo si tú tienes la aplicación instalada de tiktok y tienes el GPS actual activado No pues para Geo taguear pues donde haces tus tik Toks o a través de la IP mismo se podría pues entonces ya está eso lo tienen en sus bases de datos la cuestión es que teóricamente está regulado a lo que tú puedes acceder nadie debería en ninguna empresa

debería poder acceder a todo sin ningún tipo de justificación no y es ahí pues eso lo que lo que estaban abusando y claro si recordamos incluso tú hablabas de esto ya había digamos tiranteces no y cueste y era cuestionable todo el tema cuando empezó con Huawei que si la tecnología china desplegada en Estados Unidos era un problema Por supuesto lo de Huawei es todavía más preocupante no digamos por el tema de que son las redes Es por donde van todas las comunicaciones pero claro tiktok cuando estás hablando de billones de usuarios de que se está pues toda la información biométrica no estás grabando tu cara pones tus máscaras eso tendrá que estar regulado a ver cómo se está utilizando el lado de China y desde luego en tierra de hackers hemos hablado Ya varias veces de la capacidad de traqueo y de seguimiento de China las cosas que se están desplegando allí tenemos un episodio yo creo que hace cuatro o cinco episodios que hablamos de eso concretamente con incluso micrófonos en la calle reconocimiento facial entonces Claro si estamos dando toda esa información biométrica pues yo por un lado Me gusta no que haya países como Estados Unidos que que dice un poco Oye vamos a poner aquí un momento el freno y vamos a poner algo de legislación y vamos a hacer que los datos de los usuarios de nuestro país de nuestros ciudadanos se queden aquí en nuestro país y los de otros países no tengan acceso pues Oye pues no no lo veo mal cuando no se enfocamos en nuestra privacidad no sí sí probablemente si definen algo en respecto al acceso a estos datos debería propagarse a otros países pero sí Supongo que como has dicho tú la medida para protegerse de esto es no hay otra que desinstalarse la app porque vamos si tienes activado el GPS lo desactivas pero como has dicho tú te pueden Georgia geolocalizar por dirección IP Pero bueno usas una VPN Pero bueno si pones la ubicación del post que acabas de poner pues ya te han pillado Así que No uses tiktok pero no eso es una opinión Yo no digo que use eso sigue aparte de nosotros bueno tener la cuenta registrada nunca lo usemos Y por supuesto No no somos somos somos conscientes de que hoy en día pues la gente tiene que utilizar redes sociales muchas veces tiene que ver con trabajo personal branding diversión tampoco nos vamos a amargar todos no nosotros mismos estamos en instagram en Facebook en Twitter en tal y constantemente sacamos noticias sobre claro Hay un poco que decidir Alfred model sí que es un poco más problemático desde mi punto de vista y el tuyo seguramente Alexis el tema de los vídeos de la parte biométrica porque por ejemplo estamos en Twitter Pero bueno pues publicamos en Twitter y el teléfono que tenemos en la cuenta que nos obliga a poner Twitter no es nuestro teléfono personal es un teléfono específico tenemos un email específico Un poco pues estamos protegidos tenemos información personal ahí pero muy muy limitada cuando ya utilizas todas estas cosas de grabarte de tal de cual que a lo mejor ya es que ya se puede recopilar de internet porque tú y yo tenemos charlas Y tenemos de todo no pero bueno no es lo mismo que servirselo en bandeja a un país que sabemos que la privacidad pues brilla por su ausencia son esas cosillas no y cada uno que tome sus decisiones desde luego mejor no utilizar tiktok Sí pero tampoco tampoco estaba diciendo Alexis que si usamos eso es el fin del mundo ni muchísimo menos no correcto correcto justo lo que tú has dicho iba a decir todo depende de tu modelo de amenazas querido oyente y a mí lo que lo que me hace mucha gracia a veces la gente hace strowbacks de estos no en plan voy a enviar una foto del voy a publicar una foto del pasado Pues igual lo mismo no publiquéis en tiempo real publicarlo un poco en diferido y así aunque nos quieran seguir pues no siguen lo publicas Un día después y te llevan un día después detrás tuyas y le llevas un poco la ventaja yo me acuerdo de leer por ahí cuando esto había sido hace un par de años bueno a lo mejor aún va por tren pero que había el tema de Ah público una foto tuya de niño publica el tal y todo el mundo publicando y era pero no os dais cuenta que estáis

entrenando los algoritmos de reconocimiento facial proveyendo de fotos antiguas que en general solo tienen las actuales pero ahora le estamos dando eso También esa fue una y fue la otra fiebre también fue la de cómo te ves de mayor y la gente posteando sus caras para ver cómo se veían de mayor ostra es verdad es verdad es verdad o sea literalmente dándosela a Apps que te que ya te Calcula Cómo vas a ser de mayor para ostra que bueno pues muy buena Martín y seguimos para adelante y en este caso brevemente queremos hacer un inciso para darle las gracias a nuestro patrocinador brawler que nos apoye en el podcast y que hace unos días acaba de lanzar un servicio en la nube para proteger tu infraestructura en aws hablamos de prowler 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 brawler que está disponible en github seguro que vas a aprovechar las bondades que ofrece prowler 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 prowler pro de forma totalmente gratuita en brawler.pro PR owler.pro desde ya y bueno una vez dicho esto dentro noticia voy a hablar de Windows drivers y ataques de ransomware si os gusta esto pues quedan seis bien sentaditos recientemente ha habido cierta polémica relacionada con una tecnología de protección de Microsoft contra ataques del tipo bring you on bonerable Driver O trae tu propio Driver o controlador vulnerable que las siglas en inglés son by o uvd lo digo por si queréis un poco buscarlo en internet y indagar más sobre el tema aunque lo que os voy a contar os va a satisfacer al menos eso es lo que esperamos antes de seguir en detalle con la noticia comentar que son los drivers no en este caso en Windows Pues los drivers también llamados en español controladores son piezas de Software que generalmente permiten que los sistemas los sistemas Windows en este caso funcionen con periféricos que son pueden ser sistemas dispositivos Hardware como teclados ratones impresoras cámaras webcams tarjetas de sonido u otro dispositivo por poner unos ejemplos e incluso también la bios o uefi que es el o este componente este sistema que se encarga de arrancar el sistema Windows desde el estado de apagado quiero hacer un breve inciso relacionado con lo de periféricos porque he comenzado a ver una serie en Netflix de ciencia ficción de misterio y suspense llamada periferal que no sé Martín si tú la has visto anunciada o algo No todavía no Pero bueno ya me la punto porque entre el neuromanceer siempre das todas esas buenísimas recomendaciones que me las voy apuntando tío Pues mira muy bien muy buena memoria muy bien enseñado porque justo esta serie está basada en un libro de William Gibson publicado en 2014 y recuerdo a los oyentes como muy bien ha dicho Martín William Gibson es junto con Neil stephenson uno de son mis dos escritores favoritos del estilo cyberpunk y tienen libros muy recomendables como Martina ha dicho el más famoso de Gibson es el neuromander Así que os invito a que veáis la serie que leáis sus libros y esta serie bre sin hacer mucho spoiler está ambientada en un futuro cercano con una visión post apocalíptica en la que se mezclan los simuladores virtuales el metaverso la realidad virtual dispositivos periféricos para controlar avatares físicos reales mediante la mente y métodos cuánticos para la interacción con el futuro una serie de ciencia ficción muy interesante que yo sobre todo con el tema cuántico y el futuro me quedé un poco Bueno estoy en el primer episodio creo que hay dos así que vamos a ver que nos trae más esta serie en los futuros episodios volviendo a los drivers los hay que corren a nivel de usuario y a nivel de kernel que estos últimos son los más preocupantes no los drivers de kernel se utilizan para muchas funcionalidades por ejemplo para periféricos control análisis y estado del

Hardware para la bios UFC pues para actualizar el firmware lanzar procesos de diagnóstico de los componentes que corren en el sistema o personalización de componentes y también lo usa sistemas de antivirus anti malware incluso anti chitting esos sistemas anti trampa que utilizan los videojuegos lo utilizan para secuestrar específicas funciones específicas y apis que son sospechosas porque normalmente son abusadas por malware para realizar sus fechorías para que muchos controladores funcionen para que estos drivers funcionen a nivel de kernel necesitan un canal de comunicación directa con el kernel el núcleo del sistema operativo donde reside el código más sensible digamos lo más potente y lo más vulnerable al mismo tiempo debido a que los drivers de kernel tienen una posición muy privilegiada en el sistema hablan con el kernel directamente Microsoft decidió proteger el kernel Y a partir de Windows 10 lanzado allá en julio de 2015 requiere que todos los controladores o drivers estén firmados digitalmente por una fuente confiable ya sea Microsoft o un proveedor autorizado por Microsoft al que se le otorga un certificado emitido por Microsoft y certificados por Microsoft es decir que Microsoft los ha revisado o verificado de alguna forma de lo contrario si el Driver cargado no está firmado lo que ocurre es un bluescreen of Death está típica mítica pantalla azul y el subsecuente inicio reinicio del sistema para hacer cumplir esto Microsoft implementó un mecanismo llamado driver signature en forestment dse que bloquea el sistema operativo si se carga un controlador en modo k sin firmar Como he mencionado anteriormente esto era interesante porque definían nuevos requisitos uno de ellos muy importante era que se requieren para firmar el este Driver los firmantes los autores de este Driver necesitaban obtener un certificado de validación extendida para firmar esos drivers y para conseguir uno de estos certificados había que pasar estrictos procesos de verificación reduciendo de esta forma el riesgo de que autores de malware puedan conseguir este tipo de certificados y firmar sus creaciones Por qué Porque si se tiene que hacer una verificación validación extendida de la identidad del cibercriminal No creo que estas personas fueran a dar detalles de donde viven o sus identificadores pasaportes y similares no Ok hasta aquí todo bien pinta bien pero hay algún algunos problemillas y es que solo los nuevos controladores se ven afectados es decir esto no aplica a jugadores firmados antes de Windows 10 lo que significa que antes de la publicación de Windows 10 el 29 en concreto de julio de 2015 estos drivers pueden ser cargados por Windows Incluso si el certificado que creó la firma digital del Driver está caducado y esto de hecho hay un ejemplo deben de haber más de uno pero yo en concreto encontré uno en internet Investiga un investigador hizo una prueba de concepto y pudo cargar el Driver Mimi de rv.sis que es un Driver que implementa funciones de esta herramienta llamada mini cats que lo que hace es comprometer o dampear sacar credenciales que están almacenadas en memoria y la saca en texto Claro entre otros tipos de ataques No pues este driver en concreto es este componente que se utilizó por el investigador en esta prueba fue firmado por Benjamin delpi el autor de mimicats en 2013 con un certificado digital caducado desde 2014 y esto esta prueba está documentada de 2020 aún así en 2020 se pudo cargar este controlador aunque estuviera firmado por un certificado que llevaba caducado pues bastantes años Así que este es uno de los problemas y el otro problema es que los controladores de todas las versiones anteriores de Windows anteriores a la 10 no no se verán afectados no requieren no tienen estos requisitos por lo tanto los actores malintencionados recurren a explotar vulnerabilidades en controladores de kernel legítimos y firmados para ejecutar malware en el kernel ya que de otra forma debido a esta nueva medida de seguridad driver signature informen de Microsoft no pueden cargar sus drivers porque no están firmados digitalmente O si aunque los intenten firmar Pues están firmados por un

certificado que no es autorizado no está Emi por Microsoft el tema del Driver pues es una técnica de código malicioso utilizada por malware por cibercriminales que sería traducida digamos al español es como trae tu propio controlador vulnerable que facilita que un atacante se salte las protecciones del kernel de Windows en lugar de escribir un exploit desde cero en lo que el atacante Es simplemente hace es instalar cualquiera de los más de mil controladores de terceros que tienen vulnerabilidades conocidas Y es que Microsoft tiene una lista de casi unos mil Así que dices Bueno los atacantes tienen la verdad son un buen abanico donde elegir un Driver vulnerable y luego explota esas vulnerabilidades conocidas para obtener acceso a algunas de las regiones más protegidas de Windows el kernel en este caso y por qué esto es interesante para atacantes Pues porque escalar privilegios es un componente más de un ataque que requiere otros pasos no Al fin y al cabo los atacantes normalmente quieren bueno causar daño robar datos cifrar los datos como parte de un ataque de ransomware Pues hay diferentes pasos que se tienen que dar antes de llegar a un objetivo en este caso la escala de privilegios es uno de los pasos que requiere otros pasos abusar de un driver de kernel vulnerable sería otro paso que además puede facilitar siguientes pasos como pudieran ser saltarse o Deshabilitar mecanismos de seguridad de Windows y sistemas antivirus o anti malware acceso directo al Hardware y periféricos y potenciar modificación de estos drivers y firmwares y Modificar el firmware del sistema ya sea bios o u-fi esto lo que puede permitir es muy y muy impactante porque permite persistencia al atacante incluso después de la restauración del sistema es decir que si te das cuenta que algo está es sospechoso en tu sistema y haces una restauración del sistema por completo Pues tú piensas que lo has eliminado todo lo has instalado está limpito tu sistema desde cero pero como el malware está a nivel de bios u-fi Pues cuando se reinicia tu sistema en cualquier momento se puede inyectar se puede hacer un Drop de una dll de cualquier componente que vuelva a hacer de las suyas establezca una conexión inversa a un servidor de command en control o vuelva a cifrar tus datos que que con un ataque de rancho bueno el escenario de ataque en concreto sería supongamos que un atacante ya comprometido un sistema objetivo y ahora tiene una ejecución de código arbitrario pero este código tiene los permisos de un proceso de modo de usuario que puede ser un usuario con privilegios administrador pero Incluso el administrador tiene permisos limitados hay que clarificar que en Windows los privilegios de administrador no son los mismos que los de kernel a pesar de que hubo administrador suena súper modo súper privilegiado kernel modo kernel todavía es mucho más privilegiado no entonces el objetivo de un ataque antes escalar sus privilegios aún más Más allá de administrador a nivel de kernel para hacer más daño y por esta de esta forma se puede ver a esta técnica de dringer on bonable Driver como un Proxy para que el atacante realice operaciones privilegiadas Como kernel por ejemplo un controlador de Dell por poner un fabricante de los que son vulnerables con sus drivers puede tener una función para escribir en un archivo en el sistema en digamos en la carpeta System 32 que está muy protegida y incluso administradores no pueden escribir en esa ubicación solo a nivel de kernel pero este driver vulnerable de Dell no realiza una verificación adecuada de los parámetros de qué se va a escribir de quién lo está escribiendo y de qué archivo se va a sobreescribir Entonces el atacante lo que a descargar este controlador vulnerable y abusa de la vulnerabilidad y utiliza la función que permite que le permite Modificar un archivo en System 32 y pues a partir de ahí ya realiza todos sus objetivos del ataque que como he dicho puede ser exiltrar información sensible credenciales o realizar ataque de ramsomo y cifrar los datos una de las limitaciones de este ataque de bringer on bonable Driver Es que para instalar y cargar un Driver se necesitan permisos de administrador Ok pero no para usar de un Driver ya

instalado y cargado que es vulnerable en este caso si hay un Driver vulnerable instalado y cargado en el sistema con ser un usuario normal es suficiente voy a comentar algunos ataques reales de bring young Driver que han habido a lo largo de los años empresas de ciberseguridad como eclipseum que se enfoca en seguridad en Hardware y firmware y esset una gran empresa de antivirus y anti malware han publicado sus análisis e investigaciones a lo largo de los años enumerando todos los ataques de este tipo y las vulnerabilidades que explotan así como potenciales medidas para protegerse se tiene constancia de que cibercriminales llegan utilizando malware que abusa de este ataque de trae tu propio Driver vulnerable desde 2012 y el primer malware que utilizó este ataque fue slingshot que es una plataforma de ciberespionaje descubierta por caspersky en 2018 y se cree que ha estado activa desde al menos 2012 los actores detrás de este malware decidieron implementar su módulo principal como un controlador en modo kernel Luego se añadieron más casos de malware que abusaban de este ataque como lowjacks invizimalte y Robin Hood lojax fue interesante porque abusó de una funcionalidad de controlador similar para instalar implantes maliciosos dentro del firmware de un dispositivo víctima y persistir incluso después de una reinstalación completa del sistema operativo Esto fue Pues que se infectó el labios WiFi y por eso tuvo persistencia incluso después de una restauración completa del sistema más recientemente hemos visto una ola de nuevos ataques de este tipo uno de estos ataques a finales del año pasado fue llevado a cabo por el grupo archifamoso La que hemos cubierto anteriormente en el podcast respaldado por el gobierno de Corea del Norte utilizó un driver de Dell de hecho el que el caso de ejemplo que mencionaba antes que estaba dado de baja estaba digamos bloqueado o marcado como vulnerable con una vulnerabilidad de alta gravedad para comprometer a un empleado de una empresa aeroespacial en Holanda y también a un periodista político en Bélgica en junio de este año los delincuentes que propagaban el gran software a voz Locker también abusaron de un Driver vulnerable del antirrod kit de Avast una solución de ciberseguridad anti malware anti rutkit antivirus para saltarse el análisis del antivirus y de esta forma ser indetectable en julio luego vino un grupo de amenazas de ransomware que comprometió una empresa y luego instaló el controlador mh y pro2.6 en sus sistemas un controlador antichit del videojuego games Impact para abusar de vulnerabilidad en este controlador y de esta forma escalar privilegios ex filtrar datos moverse lateralmente en una empresa la que comprometió Y de ahí pues desplegar finalmente su ransomware en varios de los sistemas de la empresa de hecho si queréis saber más detalles sobre esta última noticia este último incidente podéis escuchar el episodio 67 de tierra de hackers donde cubría este suceso y más recientemente los ciberdelincuentes de hecho esto ha sucedido esta semana se ha publicado esta semana pero debe haber sucedido hace unas semanas o incluso un mes pues unos ciberdelincuentes desplegar en el ransomware blackbyte instalando y luego explotando un controlador defectuoso de otro fabricante en este caso msi que es una utilidad de overclocking de tarjetas gráficas ampliamente utilizada como veis todos los drivers que se abusan y son vulnerables son legítimos y se utilizan no para hacer el mal sino para hacer el bien según el análisis a fondo de eclipseum en 2019 encontraron que el problema de los controladores inseguros está muy extendido y afecta más de 40 controladores de al menos 20 proveedores diferentes incluidos todos los principales proveedores de bios así como proveedores de Hardware como ASUS Toshiba envidia y Huawei no sólo eso sino que todos los controladores vulnerables que descubrieron fueron certificados por Microsoft si hacemos avanzamos hacia el futuro eso fue en 2019 vieron a 40 controladores ahora como he dicho anteriormente la lista de Microsoft actualmente que tiene

digamos la lista de bloqueo de estos drivers vulnerables tiene hasta 1000 drivers sino incluso más así que ha habido un incremento considerable desde 40 a unos 1000 o más en estos escasos tres años que han pasado los drivers firmados quiero hacer una mención esto trae firmados y certificados parecen seguros pero no siempre lo son Por qué Pues porque a pesar de que están firmados y certi y digamos validados le han dado el visto bueno Microsoft les ha visto bueno pueden tener una habilidades y abusarlos sería como se ha visto en los ejemplos anteriores que he mencionado sería como usar una capa de invisibilidad para los sistemas de seguridad de Windows o cualquier otro tipo de sistema de seguridad se abusa un poquito esta puerta se intenta impersonar a funcionalidades legítimas para pasar desapercibido la única opción universalmente disponible hoy en día es bloquear o incluir en esta lista de bloqueo los controladores vulnerables sin embargo los proveedores afectados o alguien investigadores de seguridad o incluso la propia Microsoft tiene que hacer investigación de este tipo determinar Cuáles son vulnerables y incluirlos en esta lista de bloqueo de drivers vulnerables para protegerse de este tipo de ataques las organizaciones deben mantener su firmware y drivers actualizados Buscar vulnerabilidades en ellos monitorear y probar la integridad de su firmar y drivers para identificar cambios no aprobados o inesperados como digo otra medida de mitigadora sería que los usuarios pueden aplicar descargarse esta lista de controladores bloqueados vulnerables que ofrece Microsoft y aplicarla sus sistemas para así evitar el abuso de estos drivers vulnerables aunque esto no puede ser del todo fiable y por qué Pues aquí entra un poquito la polémica que ha surgido últimamente en relación a Microsoft con la actualización de Windows 11 en 2022 la lista de bloqueo de controladores vulnerables está habilitada de forma predeterminada para todos los dispositivos y se puede activar o Desactivar a través de la aplicación de seguridad de Windows un usuario puede activar la desactivarla pero por defecto viene activada Esto está muy bien para evitar esos tipos de ataques pero en 2019 Microsoft dijo que iba a combatir este tipo de ataques creando esta lista de bloqueo de drivers vulnerables y dijo que la haría pública y la iría actualizando a medida que surgían más drivers de este tipo que estaban abusados Por recibir criminales y que eran vulnerables sin embargo resulta que Windows no estaba actualizando esta lista de drivers vulnerables y por lo tanto no la estaba distribuyendo a sus usuarios lo que dejó a todos los clientes de en este caso de Microsoft los que usan Windows vulnerables y expuestos a Estos tipos de ataques de trae tu propio Driver vulnerable y de hecho han habido un par de investigadores que se han puesto manos a la obra y han dicho vamos a ver vamos a probar Realmente si hay algún impacto con que esta lista de drivers no esté actualizada uno de ellos Peter Callie un investigador de la empresa de seguridad de eset instaló un sistema Windows 10 Enterprise en su laboratorio y cargo el controlador del vulnerable que el grupo Lázaro sabía explotado recientemente todo esto sin tener ningún problema con Windows Así que vemos que este investigador confirmó que esta lista no estaba teniendo los resultados y que estaban esperando los los usuarios de Windows que sería prevenir la carga de este controlador vulnerable Will dorman Por otra parte analista senior de vulnerabilidades de la firma de seguridad análisis había estado tuiteando derecho durante semanas recientemente Que varios controladores que se habían usado para que le echéis un ojo y si queréis aplicarla en vuestros sistemas Aunque según se Comenta Es un poco difícil de ejecutar Así que el propio investigador dorman ha creado un Script en powershell mucho más fácil de aplicar de ejecutar que se descarga la lista la aplica el sistema y de hecho el mismo muestra que una vez aplicada está esta lista que tiene como digo más de 1000 drivers vulnerables no se pueden cargar y estos ataques de los últimos dos años no hubieran tenido lugar si esto se hubiera aplicado

por parte de Microsoft los sistemas Windows en los que es este esta funcionalidad puede correr lo que no queda claro es si Microsoft va a cumplir con su promesa y seguir enviando actualizaciones automáticas a la lista de bloqueo de controladores a través de Windows update porque viendo que ha fallado en su intento de hacerlo en los últimos tres años pues ahí queda el tema no toda esta polémica es la que queríamos traer así que uno a veces se cree que está protegido por temas de antivirus por una configuración segura que ha desplegado Confía en los fabricantes del sistema operativo en este caso Microsoft y Bueno aquí nos ha dejado un poco decepcionados pero con todo esto en cualquier caso llegamos a la pregunta del episodio queridos oyentes que es la siguiente Qué medidas aplicas para protegerte de este tipo de ataques de bring your on burner O trae tu propio Driver vulnerable tenemos cuatro opciones la primera es nada no me afecta la segunda es yo me fío de Microsoft Así que lo que lo que Microsoft me aplique Pues yo confío en Microsoft la tercera es uso antivirus o los ideas xds estos en Point Direction and responds o extender detection en response y la última utilizo muchas capas de seguridad y con eso intento estar muy interesante la pregunta si el tema de los drivers y tal ya entra eso lo hemos visto sobre todo con ataques sofisticados a nivel de apetece no es algo que sea tan común no que solemos ver De hecho estaba pensando en segunda es la noticia el tema de staxnet había sido a los drivers no de las centrifugadoras donde habían encontrado la vulnerabilidad No ahora la memoria no me llega tanto yo recuerdo que abusaban de tres vulnerabilidades o cuatro de Windows una de ellas era un acceso directo o algo así pero no sé si era un Driver o era de hecho un Driver el que ellos hacían un Drop no se tendría que tendría que investigar pero sí para los oyentes que nos recuerdan lo destacnet staxnet fue una operación encubierta por parte de Estados Unidos de Israel supuestamente pero fue Estados Unidos e Israel contra el programa nuclear de Irán en el que consiguieron infectar pues ciertos componentes de las centrifugadoras Y la verdad es que fue una operación muy exitosa y por tanto Pues podría ser un claro ejemplo de problemas no que puede surgir de vulnerabilidades en drivers y componentes así sí lo que es mencionado antes también quiero volver un poquito a ese comentario Si parece que esto y de hecho la noticia igual se ve un poquito más técnica que muchas de las noticias que comentamos pero digamos el trasfondo es que no solo Esta técnica puede ser más vista más digamos más espectacular no más avanzada grupos apt utilizándola pero también quería mencionar que tampoco hay que irse tan lejos porque hay gente que abusa de de estos drivers vulnerables para instalarse no sé sistemas por ejemplo los sistemas de antichid pues algunos los han abusado para desactivarlos y de esta forma poder jugar poder aplicar sus propios chips en videojuegos y Estos son usuarios normales personas de hecho lo que usan que juegan a videojuegos que Que bueno que son bastante técnicos no pero no son a nivel de apt Así que estas personas estos jugadores pues se han descargado pues archivos estos frameworks que abusan de vulnerabilidades en estos drivers por ejemplo de sistemas de antichid para desactivarlos de esta forma poder hacer trampas en videojuegos Así que normalmente igual como como hemos mencionado antes de la anterior noticia todo depende de tu modelo de amenazas Pero bueno es hoy en día después de 10 años Esta técnica está un poquito democratizada así que sería relativamente fácil que usuarios de pie como tú o como yo pudiéramos lanzar este tipo de ataques Pues bueno muy interesante hemos tenido una de privacidad Otro Un poquito más técnica y hasta aquí Hemos llegado como siempre recordad que nos podéis seguir en redes sociales como mencionaba Alexis nos podéis escribir a podcast@tierra de hackers.com recordad por favor compartir el podcast con amigos con compañeros con toda la gente que sepáis que les va a gustar crecemos día a día y queremos seguir creciendo Y como decía

vamos a estar en esa conferencia si alguno de los oyentes estará por allí asegurados de venir a saludarme y a lo mejor os doy alguna pegatina en el seguro que os la doy y nada Muchísimas gracias por escucharnos hasta el final sí pues me encantaría ir contigo a la conferencia Martín pero no va a poder ser aunque De todas formas Mira me quedo con que veo a los oyentes a través de tus ojos y por cierto Martín Dónde tiene lugar esta conferencia albacete y una de las mejores cosas de la conferencia son los miguelitos que reparten por allí a diestro y siniestro que es un postre típico de la zona que está buenísimo Me convierto ese fin de semana me convierto en un zampabollos literalmente además que bueno pues me encantaría probarlos pero qué fechas es la conferencia es dentro de dos semanas te digo ahora es es del 10 al 12 de noviembre en albacete Les estamos haciendo aquí public gratis porque se la se la merecen que es una conferencia muy chula a la que ya he ido en alguna ocasión Pues nada lo dicho que me encantaría estar ahí contigo Martín para disfrutar de la conferencia y conocer a los oyentes pero si no se puede para la próxima y os invitamos a todos a asistir a conocer a Martín y a que sea alguna alguna pegatina venga nos vemos si nos escuchamos Adiós adiós Chau chau que vaya bien si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu sencillo 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