# PEGASUS | EL SOFTWARE DE ESPIONAJE MÁS PELIGROSO DEL MUNDO

jeff bezos el hombre más rico del planeta en 2018 20 sus ojos como su relación matrimonial se iba al traste el motivo de la filtración de unas fotos y unas imágenes un tanto subiditas de tono que el magnate había estado enviando a su amante a través de whatsapp todo un cachondo diez besos al principio habían muchas dudas no porque por un lado como era posible que toda esta información hubiera llegado a manos de la prensa eso por un lado y por otro lado cómo era posible que se hubiera podido hackear el móvil el dispositivo móvil de la persona más poderosa del mundo bueno pues tuvieron que pasar dos años dos años después de lo acontecido apareció por primera vez las grandes cabeceras el nombre de un software de espionaje y una compañía que han marcado la geopolítica en los últimos años megasur y la empresa israelí en ese grupo que este caso bueno para entrar en materia y explicar que es pegar sus primero tenemos que narrar una serie de acontecimientos previos vale así que vamos a dejar lo mejor para el final pero os recomiendo que os quedéis os recomiendo que os quedéis porque tengo por aquí el manual de instrucciones del software de gastos y os puedo asegurar que lo que vamos a estar hablando en el vídeo de hoy ser una auténtica locura bien cómo se desarrollan los acontecimientos bueno tras sospechar de que el dispositivo móvil de jeff bezos había sido hackeado entró en juego fti consulting una firma de asesoría empresarial con sede en washington la cual se encargaría de analizar a fondo el iphone de 10 besos para ver qué demonios había pasado y sacar conclusiones en el informe revelado por mother board el cual es público de hecho por aquí lo estáis viendo os voy a dejar un enlace en la descripción de este vídeo por si lo queréis leer todo apuntaba a que no habían indicios de malware en el teléfono sin embargo sí que llegaron a encontrar cierta actividad un tanto sospechosa a partir de un vídeo procedente de whatsapp que el príncipe saudí había enviado a jeff bezos según ft y consulting todo se remonta al 4 de abril del 2018 ese día 10 veces había coincidido con el príncipe saudí mohammed bin salman n bs es como se le conoce también en una escena en los ángeles en la escena pues se llegaron a intercambiar los teléfonos y en los días subsiguientes se habían estado enviando varios mensajes por whatsapp saludándose y todo bien no te invitan a cenar conoces a ciertas personas se crean vínculos de interés o se intercambian los números para mantener el contacto y poco más vamos lo normal el problema vino después unas semanas más tarde se detalla en el reporte que desde la cuenta de mohamed se había enviado un inocente vídeo con la bandera de suecia y arabia saudí- un vídeo encriptado con un peso de 4 con 22 megas el cual fue enviado sin previo aviso ni explicación a partir del envío de este inocente vídeo el análisis forense del iphone de besòs determinó que se empezaron a enviar grandes cantidades de datos claro cuál era el problema en todo esto que al estar encriptado el vídeo ft y consulting indicó que era virtualmente imposible conocer si ese vídeo contenía algún tipo de código malicioso no se llegó a especificar si diez besos llegó a abrir el mensaje tú te pones a ver el reporte y no lo indican en ningún punto igual que bueno tampoco se conoce quién fue el autor de ese mensaje pues pese a que la cuenta fuera del príncipe saud y el vídeo podría haber sido enviado por otra persona perfectamente lo que está claro es que el análisis concluye que el archivo encriptado de web ocupaba ligeramente más que el vídeo en sí mismo por lo que ya era sospechoso y además según ft it consulting el envío de datos transmitido por el móvil de pesos se llegó a incrementar a partir de ese entonces en aproximadamente un disparate por ciento para que os hagáis una idea esto no me lo invento yo lo pone en el reporte 430 kilobytes de datos eran la cantidad enviada de forma diaria

desde el móvil de besòs pero después de recibir el archivo aumentó hasta los 126 megas y mantuvo una media de 101 megas al día durante los meses posteriores con picos de hasta 4 con 6 gb una cantidad inusualmente superior a la media habitual en usuarios de iphone la gran pregunta que os podéis estar haciendo que han roto preocupados es hoy eto'o xavi y qué tiene que ver esto con pedazos o porque se relaciona el hackeo con arabia saudí o con el software espía de la ns o bueno aquí se pone interesante la cosa a raíz del análisis forense realizado el móvil personal de 10 veces se había llegado a la conclusión de que el móvil de decesos había sido comprometido previsiblemente a través de herramientas proporcionadas por salud al castaño presidente de la audi de ciberseguridad y amigo íntimo mira tu por donde del príncipe heredero saudí mohamed ambos pongan bin salman según apunta ft y consulting al qahtani llegó a adquirir el 20 por ciento de la compañía hakim team desarrolladora de programas para espiar a otras naciones entre sus trabajos en 2015 se filtró en wikileaks que llegaron a preguntar cómo se podía llegar a infectar dispositivos a través del envío de vídeos de whatsapp por lo que ya se veía cierto interés en este tipo de prácticas esta relación y filtración es lo que llegó a la firma de seguridad ft y consulting pues a pensar que probablemente ese vídeo sea el origen del hacker y es que más allá del incremento de los datos transmitidos desde el móvil de pesos la investigación descubrió que al menos en dos ocasiones se enviaron textos a besos desde la cuenta de mbs de mohamed que podían revelar un conocimiento de información privada que no se conocía públicamente en ese momento esto que estás viendo por aquí es una imagen enviada por mohamed meses antes de que se diera a conocer la relación de besos con lauren sánchez que es con la que bezos pues le puso los cuernos lo dicho todo esto es público os lo voy a poner todo en la descripción de este vídeo para que podáis verlo por cuenta propia pero está todo ahí bien detallado en el informe en esta ocasión como podéis ver era la imagen de una mujer con el mensaje bueno a preparar vale discutir con una mujer es como leer un acuerdo de licencia de software al final tienes que ignorarlo todo y clickar de acuerdo vale se trataba de un mensaje un tanto sospechoso encima besos por aquella época porque no se encontraba inmerso en su proceso de divorcio y la imagen pues recuerda a lauren sánchez que fue la amante con la que mantenía una relación pero que no se había hecho público por ese entonces entonces bueno era un poco raro todo estas evidencias llevaron justamente a considerar de la mano de expertos de las naciones unidas que la monarquía saudí estaba siendo implicada en la vigilancia a jeff bezos y es aquí cuando un informe de la onu basado en las investigaciones de la firma de seguridad ft y consulting llegó a indicar que la explicación más lógica era el uso de spyware como pegas de la ns o o menos posible de hacking dyn para el que no sepa lo que es un spyware un spyware es un tipo de malware que intenta mantenerse oculto mientras registra información en secreto y sigue todas tus actividades en línea tanto en equipos como en dispositivos móviles puede supervisar y copiar todo lo que escribes cargas descargas y almacenar otorga acceso completo a los cibercriminales de hecho fijaros qué curioso que a finales de octubre del 2019 whatsapp denunció en ese o grupo por usar su aplicación para espionaje según la empresa de zuckerberg hasta 1400 personas podrían haberse visto afectadas por su spyware en más de 20 países e imagínate y es que claro la firma israelí en ese grupo es uno de los vendedores actuales más conocidos de software espía y acostumbra estar relacionada con los problemas de seguridad nacional el teléfono de besòs habría sido por tanto según apunta la investigación hackeado usando el spyware pegas o un poderoso malware privado ofrecido sin supervisión judicial pegasus puede llegar al móvil de sus víctimas mediante varias vías potenciales de hecho vamos a estar viendo algunas más adelante y quiero que veáis cómo es la interfaz como lo ve el

espía como se ve la interfaz y como ves todos los datos como puedes espiar a la víctima es una locura este manual de instrucciones en persona puta pasada o sea esto obviamente está mal cuando digo vaya locura no es que haga apología a que ostia viva el ciberespionaje no pero me refiero te pone los pelos de punta el ver cómo pueden violar toda tu privacidad y sin que te des cuenta tú te lees todo esto tío y te queda loco te quedas loco de la cabeza luego lo veremos y es que vais a flipar es una locura a eso me refiero pero obviamente esto está mal esto no debería de estar pasando llama pegasus puede llegar al móvil de sus víctimas de las siguientes formas estas son las más comunes mediante una videollamada de whatsapp de hecho por aquí hay una noticia del confidencial donde bueno se ve que el software pues podía llegar a instalarse en el móvil a través de una videollamada chimpum digo podía envasado porque a día de hoy la vulnerabilidad ya ha sido corregida lo más alarmante era que ni siquiera hacía falta que la víctima responder a la llamada o sea una videollamada perdida ya era suficiente para contagiarte el teléfono ya tenías pegasus ahí puestos otra de las formas más comunes que se han visto de las investigaciones que se han hecho y tal para infectar un dispositivo móvil con pegasus era mediante el envío de una con enlace malicioso el software pues bueno también puede llegar a través de un sms hay meses y otras apps similares y como lo de la víctima pues la víctima recibe un mensaje de texto incitándole a pinchar en un enlace y si lo hace automáticamente pues muerto pegasus se instala en tu teléfono una vez instalado el poder de pegasus es casi infinito yo creo que estado leyendo aquí es que es que es casi infinito según un informe por ejemplo de citizen lab pues este software puede llegar a escuchar las llamadas de teléfono acceder a tu historial de navegación activar la cámara sin que te des cuenta y el micrófono o acceder de manera impune a todo el contenido de tus conversaciones en aplicaciones como gmail facebook whatsapp telegram y skype también por otro lado según el financial times pues el software es capaz de acceder a tus datos de la nube e incluso suplantar su identidad a la hora de acceder al correo electrónico vamos una locura que qué más falta para flipar claro qué pasa hay que tener en cuenta una cosa todo esto de la llamada de whatsapp que no la coges y aún así estás infectado de pegar su juego lo del ese mes y tal estas son dos formas pero ahí y les hay montones hay que pensar que estas empresas lo que cuentan es con 0 days con vulnerabilidades de día cero qué bueno que es un 0 day es una vulnerabilidad que hasta la fecha no ha sido descubierta que no es pública por lo menos pero que ellos tienen un equipo el cual se encarga de descubrir vulnerabilidades y bueno explotan e infectan dispositivos mediante el uso de estos de exploits básicamente imagínate tú descubres una vulnerabilidad y dices ostia he encontrado una vulnerabilidad en whatsapp por ejemplo que me permite de forma remota pues ver todas las conversaciones de alguien lo sabes tú y nadie más y no lo reportan bueno pues tienes un cero después como estos miles montones que en ese grupo por ejemplo no sé cuántos tendrá pero se aprovechan de esta forma para ganar accesos y violar la privacidad de los usuarios qué excusa tienen detrás de todo esto a lo mejor os preguntáis pero y esto es legal tal bueno ellos se excusan en la pata del terrorismo para prevenir posibles ataques o posibles catástrofes que se acontezcan pues para anticiparse a la jugada por eso en ocasiones pues espían a ciertas personas y aplican esa espionaje para prevenir catástrofes esto me suena un poco a la herramienta x case score de la n s no sé si habéis visto la película de snow then pero en esta peli el habla de esta herramienta de quisqueya course y como la utilizaban para aplicar espionaje masivo pero que se les iba de las manos me sale un poco a todo esto no siempre se escudan en la pata del terrorismo para prevenir accidentes y tal pero bueno se está viendo que no es el caso ya me dirás tú diez besos por ejemplo con esta cara es que coño de atentado terrorista va a ser si tiene toda la cara de niño bueno desde

luego bastante turbio y encima esta empresa israelí ha llegado a vender su solución solución sal pegasus a múltiples países entre ellos por ejemplo pues bueno creo que eran diez azerbaiyán bahrein kazakhstán méxico marruecos ruanda arabia saudí hungría india y los emiratos árabes unidos cuánto cuesta el gas o la gran pregunta cuánto cuesta cuando tengo que poner yo para tener pegas o bueno 6 millones de euros estamos pegasus cuesta aproximadamente 6 millones de euros que sepáis que lo dicho viene con manual de instrucciones digáis como lo he conseguido pero lo he conseguido estamos aquí estamos para ofrecer contenido de calidad voy a ir mostrando fotos de lo que hay aquí dentro se supone que una vez que lo instaladas se tarda un tiempo aproximado de entre 10 a 15 semanas por ello estáis viendo a tenerlo todo preparado para poder operar tenerlo todo preparado en qué sentido te estarás preguntando bueno es que tienes jornadas de formación estamos hay una serie de cursos y de pruebas un periodo digamos de formación el cual vas a tener para llegar al punto de poder usar el software por cuenta propia sin tener ningún tipo de problema y encima que tienen algún tipo de problema no pasa nada hay atención al cliente tiene es videollamada remota ya está asistencia en casa que te vienen para casa para echarte un cable pero me los está inventando yo esto lo pone aquí os lo podéis leer luego puede que os ponga la descripción de este vídeo el enlace a el manual de instrucciones venga me voy a mojar igual entre todos pues descubrimos algo interesante pero eso en plan oye que tienen algún tipo de problemas y que no sabes qué está pasando o te ha surgido algún error no pasa nada tú llamas un número y ellos pues de forma remota tienes asistencia remota bueno ha llegado el momento yo creo que ya estamos preparados para los más curiosos y curiosas esto es lo que ven en la pantalla de su ordenador los espías que trabajan con este programa os voy a poner una imagen mejor para que lo veáis más nítido lamentó de todas formas que se vea tan mal la imagen pero bueno no he podido hacer nada para mejorar la calidad de esta imagen es la que viene con el propio manual de instrucciones en este caso se ve un amplio listado de llamadas con un pequeño reproductor para escuchar todas las conversaciones además de buenos múltiples pestañas como podéis ver por ahí arriba que nos permitirían pues obtener toda la información deseada del dispositivo infectado según el manual de pegasus se puede instalar por un lado a distancia mediante mensajes push mails sms etcétera básicamente se envía un mensaje a la persona que se desea espiar le salta una alerta y si pulsa en la alerta ya está el dispositivo está infectado al parecer si te pones a leer el manual no tienes ni por qué preocuparte acerca de lo que ponga el mensaje porque según la guía nos dice que pega su se encargará y nos proporcionará una amplia gama de herramientas ideales para redactar un mensaje y no sé y personalizado con el objetivo de atraer al objetivo que abra el mensaje o sea que te lo ponen fácil imposible por otro lado estaría la vía de instalación por proximidad si está cerca de la persona que pretende respirar al parecer con lo que ellos llaman una estación de base táctica esto es que alguien se pone al lado de la víctima en cuestión con una especie como de aparatito raros un comentan o bueno ese aparato es capaz de extraer t el número de teléfono de la víctima y la instala a pedazos no sé cómo lo instala pero terroristas os recomiendo que lo lea y de forma detallada porque yo no lo entendí bien pero bueno seguramente se aprovecharán de serlo de hijo movidas raras pero te lo explican aquí y por último y no por ello menos importante la vía de instalación física es decir yo tengo tu dispositivo móvil pues le instaló pegas o según el manual de lo que yo le hice tarda menos de cinco minutos en instalar pegasus de forma física de cualquier forma sea cual sea el método que hayas empleado una vez instalado el software de pegasus pues ya te otorga de un privilegio tanto pasivo como activo porque activo porque al parecer también puedes intervenir para decirle al dispositivo que es lo que quieres que

haga por ti lo cómodo de todo esto es que lo tienen todo pensado es que toda la información encriptada y no directa tienes pantallas o puedes escuchar por el micrófono ver la cámara sin que se active la luz tienes incluso un histórico a través del cual puedes ver imágenes o cualquier otro tipo de contenido multimedia el cual no hubiera llegado a ser borrado en el pasado y lo más tenso de todo es que no deja rastro por cada movimiento que tenga la víctima según comentan en el manual pues bueno al parecer el espía es alertado de hecho hasta puedes generar alertas específicas de forma que cuando estés hablando con alguien o te estés comunicando con alguien por whatsapp por sms lo que corresponda pues eres capaz de aplicar mediante el uso de ciertas palabras clave filtros para que te envíen alertas del plano ya lo mejor si hablan de equis cosa quiero que me alerta pues a lo mejor están hablando de esa cosa de alerta y te dice oye que mediante una llamada o por mensaje están hablando de este tema que te interesa te alerta como veis es un escándalo nos vamos a la mierda bueno se puede comprobar de alguna forma después de todo esto si tienes pegasus en tu móvil existe una herramienta existe una herramienta la cual ha sido creada por la amnistía internacional denominada verification toolkit que se descarga en el ordenador y se conecta para que te escanea el móvil los usuarios de apple como en mi caso pues podéis usar también el programa i'm eighteen para mac o ese que tiene integrada esta herramienta y permite chequear el iphone en el periodo inicial de prueba de forma gratuita os dejaré los enlaces en la descripción de este vídeo por si queréis probarlas para ver si vuestros dispositivos están seguros y así os aseguraré pero como digo siempre la seguridad absoluta no existe y poco más chavales poco más esto es lo que quería traeros para el vídeo de hoy espero que os haya gustado la historia espero que bueno que os voy a decir supongo que estaréis asustados yo también yo también estoy asustado no se te admira que escudarse en que es por todo el tema este del terrorismo para prevenir posibles atentados y movidas en parte lo entiendo porque tal vez ciertos atentados del pasado se podrían haber previsto o prevenidos entiendo por dónde van pero yo no sé cómo están las leyes ahí pero desde luego se ve que no intervienen mucho las leyes es como que si quieren violar tu privacidad pues la pueden violar sin ningún problema vamos por lo que se está viendo ya me dirás tú diez besos ahora también pasó con el presidente de españa pedro sánchez también como que se detectó que tiene el pegaso en su móvil y no sé qué movidas de que le han estado espiando no se os a expiar a cargos políticos altos cargos el mes de mayo que se iba a aplicar palabras clave de terroristas tal oyó que se dio buscar algo más que pinta y pedro sánchez o que pinta y diez pesos no sé esos filtros ahí hay algo ahí que huele mal me gustaría saber vuestra opinión en plan que os ha parecido el vídeo si ha gustado si consideráis que diez besos tiene cara de terrorista como intentar llegar a una conclusión en comunidad es terrorista 10 besos si o no tiene cara de terroristas dejadme en los comentarios y nada espero que estéis bien espero que estéis con los ánimos por las nubes si estáis de exámenes espero que os estén yendo bastante bien recordad que si me queréis encontrar estoy todos los días a las 9 horas de españa peninsular en tweets y siempre estoy todos los días algún día a lo mejor me lo pillo de descanso pero ganar se queda entre tú y yo recordad que tenemos una comunidad en disco que somos más de 30.000 miembros si os queréis unir os lo pongo por aquí en la descripción también somos una comunidad bastante grande si no sabéis por dónde empezar hay un montón de gente dispuesta a echarte un cable y poco más chavales un besito en el siempre sucio en el voto y nos vemos en el siguiente vídeo sí