La HISTORIA y EVOLUCIÓN de los RANSOMWARE

el ramsomware se ha convertido en una de las herramientas más conocidas de los ciberdelincuentes desde el Grupo naviero Internacional paralizado por el cifrado de sus herramientas de producción hasta la muerte de un paciente en un traslado entre hospitales alemanes el ransomware ha demostrado su capacidad para perturbar cualquier empresa y comunidad independientemente de su tamaño y nivel de seguridad pero cómo hemos pasado en 30 años de un programa malicioso en un disquete que pedía 100 dólares de rescate a una verdadera industria criminal estructurada de miles de millones de dólares hoy vamos a estar echando un vistazo a la historia y a la evolución del fenómeno de los ransomware desde el primer ram somware de la historia informática registrado en el año 1989 hasta hoy en día año 2022 analizando todos los cambios que han habido y cuál es la tendencia principal que se está viendo en base a lo que se ha acontecido en todos estos años Bueno antes que nada deciros que he pillado el bicho si me notáis con la voz un poco extraño como que a veces me cuesta hablar no es que esté drogado ni nada por el estilo es que poco a poco fuimos a Noruega y mi pareja de vacaciones para tomarnos un pequeño descanso y Bueno pues se ve que nos contagiemos por ahí y he venido pues con el bicho por segunda vez y por segunda vez porque ya el año pasado sabéis que me afectó bastante pero bueno esta vez ha sido más suavecito por tanto Bueno ahora solamente queda recuperarnos y pronto volverá la carga Pero bueno a mí el bicho no me va a frenar de hacer vídeo estamos así que bueno Espero que disfrutéis de toda esta historia dejado un buen like ahí si os Mola la historia y bueno entraremos en detalle en breve pero primero que nada un mensajito ahí de nuestro queridísimo sponsor casefam casefam es una página que ofrece claves de software OEM baratas y completamente legales las cuales son 100% oficiales y que pueden ser activadas totalmente en línea disponen de un servicio de atención al cliente 24/7 y un servicio postventa de por vida una excelente oportunidad para renovar el sistema operativo Y lograr una mejora en el rendimiento y en la seguridad como podéis ver en la página web Pues disponen de múltiples productos a adquirir desde Windows 10 hasta Windows 11 también con productos de Microsoft Office desde el 2016 hasta el 2019 y 2021 con licencias disponibles desde para un único ordenador hasta para cinco equipos contamos también con la sección de vandle products donde En caso de que quieras pillar un Windows 10 y a la vez la Suite del office 2019 Pues bueno tienes un precio un poco más razonable más asequible y por último una sección de computer Tools de herramientas de ordenador las cuales Pues igual te interesan pillar y por ahí las tienes disponibles Pese a que el precio ya es asequible de por sí puedes utilizar el código de cupón S4 v50 para obtener un 50% de descuento en la serie Windows y por otro lado puedes utilizar el código de cupón S4 v62 para obtener un 62% de descuento en los productos de Microsoft Office y también los van del products yo por ejemplo que lleva siendo hora me voy a pillar un Windows 10 Pro Así que voy a Añadir esto al carrito y Bueno voy a usar el código de cupón S4 v50 para obtener un 50% de descuento y ahí está ahora ya puedo pagar con PayPal o con tarjeta de crédito gracias a casefam por patrocinar este vídeo y ahora continuemos con el vídeo de hoy bien pues primero que nada Qué es un ramsomware un ramsomware o secuestro de datos en español no es más que un tipo de programa dañino que lo que hace es restringir el acceso a determinadas partes o archivos del sistema operativo infectado considerando como un tipo de software malicioso o malware que lo que hace es robar datos cifrarlos y pedir un rescate que generalmente en criptomonedas a cambio

de quitar esta restricción los ataques de ram sonware suelen negar a las víctimas el acceso a sus datos a menos que se pague el rescate y normalmente hay un plazo para pagarlo Antes de que los datos desaparezcan para siempre el pago por una clave de descifrado para que os hagáis una idea puede costar desde cientos de dólares hasta cientos de miles o incluso millones de dólares para casos excepcionales ahora bien al contrario de lo que la gente se suele pensar el primer ramsomware no apareció con internet la historia de estos programas maliciosos comenzó a finales de la década de 1980 con el único propósito de bloquear el funcionamiento de puestos de trabajo este modo afectaban a particulares y empresas con microordenadores Eddie Williams un trabajador de una compañía de seguros de Bélgica fue una de las primeras Víctimas de ransomware en la historia de la informática en 1989 su jefe le había pedido que comprobará qué había en un disquete que habían recibido de la OMS lo que se esperaban encontrar en el disquete era una investigación médica sobre el sida sin embargo cuando Eddie Williams inserta el disquete en su ordenador lo que no sabía es que estaría ante lo que iba a ser el primer ram somware de la historia claro Cabe destacar que tres décadas atrás el Ram somware como tal era más simple e ingenuo que los que conocemos hoy en día 189 dólares es lo que el actor del ransomware pedía como rescate a las víctimas las cuales tenían que enviar el dinero a una dirección de Panamá Eddie Williams se encontró con este mensaje concretamente al cargar el disquete en su ordenador el cual recordad que había sido bloqueado sin embargo según él dice que no a pagar ni perder ningún tipo de dato porque revertir toda esta situación digamos que no era tan complejo era relativamente fácil en 1989 el troyano eights fue el primer ram somware de la historia de la informática en un contexto de preocupación por la aparición del virus del SIDA el biólogo Joseph l pop había enviado 20.000 disquetes con información sobre la enfermedad a grupos de pacientes instituciones médicas y particulares de 90 países pero aunque el disquete contenía información sobre este tema también contenía un pequeño regalito un virus que cifraba los archivos de la máquina infectada después de un cierto número de reinicia el incidente causó bastantes estragos por ser una novedad total a pesar de que eludirlo era relativamente fácil la fuerza del orden comenzaron a rastrear de dónde provenía este ataque para determinar quién estaba Detrás de él finalmente llegaron hasta un biólogo evolutivo de Harvard se llamaba Joseph pop y era uno de los Implicados En las investigaciones sobre el si en ese momento a día de hoy Cabe destacar que sigue sin saberse el Por qué hizo todo esto efectivamente se cree que el punto de inicio de toda esta historia del ransomware comienza justamente por esta persona por el doctor Joseph pop Un biólogo evolucionista conocido por entre otras cosas haber desarrollado lo que sería el primer Ram software del mundo el troyano its de 1989 También conocido como troyano PC Cyborg Obviamente fue arrestado y acusado de múltiples cargos indicó a las autoridades que hizo el ramsomware con el propósito de donar el dinero para la investigación contra el sida errado no es algo que nunca sabremos Y bueno pues falleció en el año 2007 a pesar de este golpe los ataques d.o.s y los gusanos informáticos acapararon toda la tensión en tiempos posteriores Esto se debe a que por aquel entonces el ramsomware podía ser rastreado con relativa facilidad a partir de la información del pago por tanto los siguientes Ram songs tardarían casi 15 años en aparecer llegada de las monedas digitales y posteriormente de las criptomonedas que permitieron una mayor fluidez en los pagos de los rescates y en los cambios de moneda así como un cierto anonimato estos Ram songs solo tenían una función sabotear los datos cifrando todos los archivos del disco sin afectar al funcionamiento del propio sistema operativo así el usuario víctima tenía acceso a su sistema operativo sin poder utilizar Ninguno de los archivos presentes en el año 2005 pgp coder ogp code

apodado el ramsomware de los 20 dólares o uno de los primeros ejemplos de ramsomware distribuidos de forma online su objetivo consistía en infectar los sistemas Windows dirigiéndose a archivos que contenían extensiones de uso común como punto rar punto zip.jpg.dock o punto xls un año después en el año 2006 el ramsomware archivos aumentó la dificultad de los intentos de descifrado adoptando El algoritmo descifrado rsa mediante un mecanismo asimétrico de clave pública y Clave privada al dirigirse al contenido personal de los usuarios almacenado en el archivo mis documentos de Microsoft Windows este ramsomware lo que hacía era depositar un archivo titulado How to get your files back.txt en la misma carpeta el cual se abriría cada vez que un usuario intentará abrir un archivo el mensaje informaba a las víctimas que sus archivos estaban cifrados y solo se podían acceder a ellos con la contraseña larga de más de 30 símbolos es alentando a las víctimas a intentar adivinarla en cambio lo que hacían era encargarse de comunicarle a las víctimas que enviaran un correo electrónico a restore@6mail.net o restore files@yaho.com para obtener más instrucciones cuando lo hacían los atacantes indicaban a las víctimas que hicieran compras en varias tiendas en línea hasta entonces no está claro si los atacantes eran dueños de estas tiendas en línea o si las víctimas debían enviar los artículos comprados a los atacantes Pero lo que sí está claro es que una realizadas las compras el atacante enviada supuestamente la contraseña por correo electrónico los propios archivos como comentamos anteriormente se cifraban con una clave rsa que es una forma descifrado asimétrico el cual pues es ciertamente complejo de descifrar por ciertas razones con el cifrado asimétrico al crear el malware el atacante lo que hace es generar una clave pública la cual incrusta en el rasomware una vez que el ransomware tiene acceso a un dispositivo este cifra los archivos de la víctima utilizando una clave privada la cual es generada aleatoriamente y que a su vez Es cifrada por el ramsomware utilizando la clave pública el atacante por tanto lo que pueda ser es usar la clave pública que ha generado para descifrar la clave generada aleatoriamente y así descifrar a posteriori todos los archivos asegurando de esta forma que no se pueda usar la misma clave si la víctima es atacada nuevamente esto también significa que alguien no podría simplemente aplicar ingeniería inversa a la clave del Código de ci las claves RCA en particular son difíciles de descifrar porque utilizan el algoritmo rsa justamente que viene de ribes chaming atleman para generar ambas claves el algoritmo depende de dos números primos generados aleatoriamente si el descifrador de código no conoce los números primos Entonces es imposible descifrar la clave solo hecho hay una famosa formulita que igual os suena a todos que hemos tocado en directo por Twitch cuando resolvemos retos de criptografía y tal que es n = p * q igual os suena esto o bueno p y q son dos números primos claro Esto fue un giro completamente nuevo con respecto a los virus ramsomwares anteriores Como por ejemplo uno de ellos Eyed troyan que usaba cifrados simétrico y podía descifrarse con bastante facilidad sin necesidad de pagar el rescate los creadores y distribuidores de archivos nunca fueron encontrados mientras que otros virus avanzaban generando imitaciones y variantes la línea de virus archivos término aproximadamente un mes después de su lanzamiento como hemos visto descifrar los archivos de las víctimas era una tarea complicada No la clave cifrado RCA era bastante fuerte sin embargo después de unas horas muy pocas semanas muchas víctimas pudieron recuperar sus archivos sin tener que pagar el rescate atentos aquí resulta que el atacante no tenía una muy buena higiene de contraseña al parecer todos los descifradores que el malware proporcionaba utilizaban la misma contraseña una combinación de 38 caracteres la cual era la siguiente que estáis viendo por pantalla una vez todos tus archivos eran cifrados y te pedían el rescate lo que te hacían era comprar drogas en una de las

tres farmacias online que te indicaban solo si pagaba entonces posteriormente te compartían la clave que te permitía poder recuperar todos los datos Y esta clave justamente era esta que estés viendo por aquí que es la que se vio que podía reutilizarse para descifrar cualquier archivo infectado vaya cagada una vez que está contraseña se distribuyó ampliamente Pues el malware ya comenzó a perder poder y ya pues dejaron de usarlo en la primera mitad de la década 2000 la adopción de internet creció sin cesar acercándose a un nivel del 87% de estadounidenses conectados a finales de 2014 ensajería redes sociales foros redes Esta es la base sobre la que el ramsomware winglock y sus variantes se distribuyeron ampliamente desde 2011 hasta 2014 su particularidad era que no cifraba los datos del ordenador infectados sino que este ramsomware tenía la función de bloquear el acceso a la máquina mostrando una ventana que contenía una foto pornográfica y una solicitud de pago mediante un servicio de SMS denominado Locker esta primera evolución del ransomware tenía como objetivo principal bloquear el inicio del sistema operativo tras este ataque exitoso aparecieron variantes que usurpaban la imagen de las fuerzas de seguridad este fue el caso del ramsomware reggaeton en 2012 que se hizo pasar por el FBI bloqueando los ordenadores de sus víctimas y exigiendo el pago de una multa de 200 dólares este ramsomware se distribuyó ampliamente En plataformas los internautas pagaban rápidamente para evitar cualquier represalia relacionada con la infracción de los derechos de autor o la distribución de contenidos pornográficos a partir de entonces las solicitudes de rescate pasarían a ser cada vez más creativas para aumentar las posibilidades de pago el año 2013 marcó un punto de inflexión tecnológico con la aparición del ramsomware criptolocker y su servidor de Mando y control controlado por el atacante con el uso de un servidor de Mando y control el grupo atacante puede hablar ahora con la víctima o negociar así como ampliar o reducir el plazo antes de la destrucción de los datos en este caso digamos que tienen la capacidad de ejercer una presión adicional sobre la víctima y aumentar así sus posibilidades de pago esta nueva estrategia dio sus frutos ya que cripto Locker llegó a generar 27 millones de dólares en sus dos primeros meses de funcionamiento también hay que señalar que se trata de uno de los primeros programas que solicitaban un rescate en bitcoin en 2014 el frente de ataque se amplió con los primeros ataques a tabletas y móviles Android los ramsomware por ejemplo simple Se propagaban a través de falsos mensajes de actualización del Software Adobe Flash como dato puntual antes de llegar al año 2016 en el año 2015 un año después de lo que hemos estado hablando los usuarios de los sistemas operativos Linux serían el objetivo del ransomware encoder A lo mejor alguno de vosotros os suena en 2016 petier allenaría el camino para los ataques de phishing al dirigirse a las direcciones de correo electrónico de las empresas en este caso ocultan un documento de Word o PDF la propia víctima activaba el ramsomware al abrir el archivo este ramsomware concreto no solo bloqueaba el acceso a determinados archivos sino que también bloqueaba todo el disco duro al cifrar la tabla maestra de archivos una calavera Roja de hecho aparecía en la pantalla para pedir el rescate Más allá del efecto psico sobre las víctimas este ramsomware fue comunicado por parte de los medios de comunicación tradicionales y concienció al público general sobre la ciberamenaza los años 2017 y 2018 marcarían un nuevo punto de inflexión en la propagación de los ciberataques gracias a la publicación de vulnerabilidades serodei robadas a una agencia gubernamental estadounidense la nsa los ataques de ramsomware presentaban entonces la capacidad técnica de propagarse masivamente de una empresa a otra cuando las redes coexistían en 2017 wanna Cry fue posiblemente uno de los ramsomwares de los que más se habló en pocas semanas llegó a afectar a 300.000 ordenadores en 150 países al propagarse por medio de los sistemas operativos Windows

a través de la vulnerabilidad eternal Blue al Mostrar la famosa calavera en sus pantallas las empresas veían como el ransomware se propagaba de un sitio a otro en cuestión de minutos debido a su carácter de movimiento lateral era prácticamente imposible llegar a contener el ransomware logrando así in al mayor número posible de equipo con cientos de miles de empresas Víctimas de este Ram somware Y ante su propagación incontrolada las empresas comenzarían a invertir masivamente en productos de copias de seguridad y recuperación de datos en respuesta los ciberdelincuentes también pues empezaron a atacar los puntos de copias de seguridad con el fin de eliminarlos de esta forma se aseguraban que los datos no pudieran restaurarse si no se pagaba el rescate posteriormente en un contexto de conflicto Estatal entre Rusia y Ucrania una variedad de malware llamada not petier aparecía de entre las tinieblas este malware la verdad es que tenía muchas similitudes competia y además tenía la particularidad de reutilizar elementos iniciales de guanacry como la explotación de las vulnerabilidades eternal Blue y eternal romance las dos vulnerabilidades robadas unos meses antes a la nsa teniendo mismamente la capacidad de movimiento lateral si bien Microsoft había publicado un parche una semana antes este ransomware demostró la capacidad de los administradores de actualizar sus sistemas con celeridad para hacer frente a este ataque el verdadero objetivo de not petier no era la extorsión sino la destrucción de datos y a muy gran escala al dirigirse a todo un país se estaban enfrentando a lo que estaba haciendo considerada un arma bastante potente de destrucción digital este Ram software para que os hagáis la idea también camufló intentos de Sabotaje del metro ucraniano el aeropuerto de kiev la central nuclear de chernóbil El Banco Central y el operador Nacional de energía a finales del año 2018 el gobierno estadounidense estimaba que el daño atribuido a todos estos ataques estaban más de 10.000 millones de dólares según Cyber cover el número de incidentes de ramsomware aumentó un 365% a finales de 2019 Y entonces nos adentramos a la era del big game junting bueno big game hunting que luego os ponéis en los comentarios Oye no se pronuncia así con el objetivo de no ser detectados por las herramientas de seguridad los ciber ahora comenzaban a optar por no lanzar campañas a gran escala como fue el caso de wanna cray prefiriendo En consecuencia dirigirse directamente a las grandes empresas esta nueva estrategia la cual denominaban justamente big game hunting hace referencia a un modo de funcionamiento basado en el reconocimiento del entorno del objetivo y el desarrollo de escenarios de ataque avanzado los grupos de atacantes estudiaban entonces su objetivo para adaptar su demanda de rescate hoy durante este periodo cuando se introdujo el mecanismo de doble extorsión este mecanismo era sumamente poderoso ya que la empresa afectada no solo era víctima de la petición de rescate sino que también se veía amenazada con la reventa de sus datos en la darknet así revelar parte de los datos críticos robados podía ser decisivo para convencer a las empresas contrarias de que pagasen el rescate y el mecanismo también Cabe destacar que podía llegar a afectar a clientes cercanos de la empresa en question de forma que los atacantes los cibercriminales también amena es poner y publicar datos de clientes esta estrategia resultó exitosa ya que a finales de noviembre de 2022 se llegó a contabilizar 300 empresas víctimas del ransomware ya por último una de las últimas revoluciones en el modus operandi de los cibercriminales ha sido la aparición de plataformas de ramsomware a service igual has visto por ahí como ras esto brinda a los grupos de atacantes menos experimentados la oportunidad de acceder a una infraestructura completa y beneficiarse de campañas de ransomware listas para desplegarse las plataformas alquilan sus soluciones maliciosas y también pueden cobrar un porcentaje del rescate de las víctimas algunos grupos de atacantes que han invertido en la

investigación y el desarrollo de ramsamware crean después franquicias para comercializar su ramsomware a otros grupos delictivos Este es el caso de la franquicia de ramsomware conti este grupo Pues bueno forma a perfiles Junior y les ofrece un salario fijo y un plan de participación en los beneficios como veis la lista de ramsomware es bastante larga ya hasta el punto de que a día de hoy se estima que existen como unas 192 familias de ramsemware activadas esparcidas por todo el mundo que de hecho seguramente sean muchas más además con la aparición de nuevas tecnologías véase web 3 nft movilidad Autónoma etcétera cabe esperar nuevas formas de ciberamenazas con la proliferación y la llegada de las criptomonedas que permiten cierto anonimato en los pagos de rescate las transferencias de dinero se han convertido en algo casi seguro entre comillas para los grupos de atacantes Por tanto la historia del ransomware está desgraciadamente bastante lejos de terminar poco más para el vídeo de hoy Espero que os haya gustado me he dejado la voz mira que tengo el bicho y no sé ni cómo lo he hecho no sé en cuanto se habrá quedado Este vídeo pero la verdad es que tengo la voz que y encima ahora tengo que arrancar directo cabrón esto es un espectáculo eh Bueno espero que os haya gustado de corazón toda la trama toda esta historia un poquito de cultura general no viene mal de vez en cuando por el canal Dejad un buen like ahí si os ha molado la temática del vídeo y Dejad un comentario indicando también qué os ha parecido todo hemos visto obviamente es probable que algún que otro Ram somware o familia de ramsomware no la hayamos llegado a contar he intentado por lo menos escoger las más significativas las más importantes Pero bueno si ves que hay alguna que otra que se me ha olvidado se me ha ido por el tintero dejando en los comentarios con una pequeña descripción para saber en qué consistía ese ramsomware que es lo que hacía y cómo operaba y poco más de resto espero recuperarme pronto poco madera yo creo que para el próximo vídeo ya estamos perfecto nos vemos en el siguiente vídeo un saludo chao