5$1620:$5(5$',2*5$)Ë$ '($0(1$=$

Juan Sebastian Cardenas Hernandez
Sebastian_0912@hotmail.com

Abstract- Currently the ransomware spreads as one of the greatest threats to security level information, not only for large companies but also for natural persons to whom confidential information is kidnapped and why the ransom is demanded that It does not ensure that you can actually recover your lost data

Resumen- Actualmente el ransomware se propaga como una de las mayores amenazas a nivel de seguridad de la información, no solo para grandes empresas si no también para personas naturales a las cuales su información confidencial es secuestrada y por la cual se exige el pago de un rescate que no asegura que en realidad pueda recuperar su información perdida.

Índice de términos- Bitcoin, Dato, Encriptado, Malware Ransomware, Red TOR, Virus.

I. CRONOLOGÍA

El ransomware es una variación de malware que limita o bloquea a los usuarios acceder al sistema o archivos contenidos en el mismo, variaciones mas modernas cifran archivos al azar y solicitan rescates a través de medios informáticos para obtener el archivo original o la llave que decodifique la información.

- En 1989 el DR. Joseph Popp crea el primer ransomware el cual oculto en un programa acerca del virus SIDA una vez infectada la maquina se iniciaba un contador de arranques y luego del arranque 90 se cifraba el disco de forma asimétrica. Con el fin de ser des-encriptado se debía consignar un dinero a una cuenta en Panamá. [1]

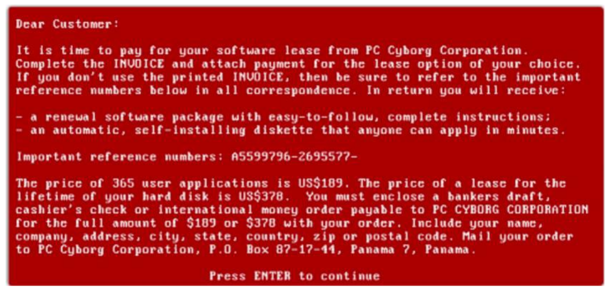

FIGURA 1. Imagen del Virus SIDA [1]

- En 1996 aparece el primer ransomware con el uso de algoritmos RSA el cual cambia el código del archivo fuente, dificultando la tarea de descifrado en relación con la primera variante de este virus. [2]
- En 2005 aparece el gusano GP Code, el cual infectaba archivos de extensiones específicas como .xls, .doc, .txt, entre otros, surge la variante GPCode.AG la cual fue la primera variante en usar cifrado asimétrico.
- En el 2006 aparece el troyano Archiveus, el cual no cifra los archivos originales crea una copia de los mismos elimina los originales y resguarda la carpeta con una contraseña.
- En el 2011 realiza su reaparición este virus con el crypto locker o más FRQRFLGR FRPR [3] GH OD SROLFtD, el propago en Europa TXH V y Américarealizando suplantación de paginas de la policía lo que hacia que las victimas cayeran con mas facilidad. [3]
- En el 2013 aparece el cryptolocker y las variables como el cryptowall, aumentando el número de equipos infectados a través del mundo.
- En el 2015 se ponen a la venta los códigos del malware creando una nueva estrategia de negocio el RaaS, de esta forma se pierde el

rastro de los criminales que usan estos ataques ya que cualquier persona puede tener acceso al código malicioso y usarlo a su beneficio.

II. VARIANTES DE RANSOMWARE

Existen principalmente dos variables del ransomware que de llegar a materializarse pueden bloquear el equipo completo o cifrar archivos del mismo ya sean documentos, fotos archivos de arranque entre otros.

- Locker Ransomware

Este tipo de ransomware bloquea el acceso al computador infectado o al navegador, muchas veces inhabilitado inclusive el mouse y el teclado solo dejando útil el teclado numérico por el cual se realizará el desbloqueo de la maquina una vez el pago haya sido efectuado, la debilidad de este tipo de ransomware es que no toca los archivos por lo cual a través de herramientas y software se pueden llegar a recuperar así sea necesario prescindir del sistema operativo infectado.

Este virus también es conocido como el virus de la policía ya que los cibercriminales en un ataque de ingeniería social infectaron una gran cantidad de equipos por medio de un correo electrónico, el cual era supuestamente enviado por la policía local acusando a la victima de realizar actividades delictivas.

Este virus inicialmente inicio en Europa en países como España e Inglaterra, pero con el tiempo migro a Estados Unidos en el año 2012 y América Latina siendo argentina uno de los países suramericanos mas afectados, los rescates oscilan entre 50 y 150 dólares dependiendo del país en donde explotan la amenaza lo que indica que los cibercriminales realizan estudios de ingresos en los países antes de realizar los ataques, con el fin de asegurar el pago del rescate. [3].

FIGURA 2. Virus de la Policía [3]

- Crypto locker

Actualmente es el ransmoware más utilizado ya que las personas al ser mas digitales almacenan grandes cantidades de información en este medio y no tienen la costumbre de no generar archivos de respaldo o back ups de la información mas importante, por lo mismo tiene diferentes variaciones que buscan infectar todos los archivos como lo son: bases de datos, archivos de Word, PDF entre otros inclusive ya están diseñados para buscar extensiones especificas de juegos de video.

Esta variante no infecta archivos de arranque ni de funcionamiento del sistema operativo por lo que muchas veces no alerta a los usuarios infectados.

Esta variable empezó realizando la infección de equipos en hogares pero con el auge que han tomado las empresas de realizar la digitalización de la información mas relevante han aumentado el interés de los cibercriminales para atacar estos nichos de negocio.

FIGURA 3. Cryptolocker [2]