BUENAS PRÁCTICAS PARA MITIGAR LOS ATAQUES CRIPTOGRÁFICOS CON MALWARE RANSOMWARE

Deisy Mosquera Perea

Lina Andrea Castañeda Salazar

Ingeniería de Sistemas

Director Gabriel Taborda

INSTITUTO TECNOLÓGICO METROPOLITANO

07/09/2017

RESUMEN

Ransomware es un programa de código malicioso que infecta el computador, el cual se propaga rápidamente cifrando los datos que se encuentran almacenados en la maquina o en su defecto bloqueándola. Este malware evita que las personas puedan acceder a la información o archivos que se encuentran en el computador, ya que estos están encriptados, los creadores de este malware exige un rescate y el pago debe realizarse en bitcoin.

Ransomware surgió en el año 1989, su nombre fue AIDS Trojan este tenía como función ocultar las carpetas y encriptar ficheros. Ransomware cuenta con dos tipos: bloqueadores y cifradores, los bloqueadores son los que no permiten acceder a la información del computador porque el disco duro se encuentra todo cifrados, los cifradores son los que no te permiten acceder a los archivos o carpetas, pero no bloquea el computador.

La finalidad de esta investigación es darle a conocer a las personas o empresas buenas prácticas para mitigar los ataques criptográficos con malware ransomware, para cumplir con el objetivo anteriormente mencionado, se realizó un estado del arte donde se investigó diferentes tipos de ransomware, el año que se fundó, su forma de ataque etc. después de esto se clasificaron con su respectivas funciones, algoritmo de encriptación y medio de propagación, a continuación estos malware fueron clasificados de mayor a menor riesgo, y por último se realizaron algunos ejemplos de estos malware para conocer cómo es su funcionamiento y así conocer el impacto que este causa al momento que infecta nuestro sistema. Como conclusión nos dimos cuenta de la importancia de realizar esta investigación ya que este malware se está haciendo cada vez más perjudiciales y las personas o empresas por su poco conocimiento se están viendo sumamente afectas por los diferentes tipos de ransomware.

Palabras clave: Ransomware, malware, virus informático, criptografía, criptoanálisis, seguridad informática.

RECONOCIMIENTOS

A Todas las personas que participaron e hicieron posible este proyecto, muchas gracias por Su apoyo y enseñanza: al profesor Gabriel Taborda

Por su guía, comprensión, paciencia y valiosos consejos a lo largo del proceso de investigación, sin ustedes no hubiera sido posible

A Dios, padres y madres

ACRÓNIMOS

- SISSI (semillero de investigación en seguridad de los sistemas informáticos)
- SMB (Server Message Block) = Protocolo de bloqueo de mensaje de servido
- RSA (Rivest - Shamir - Adleman) = Sistema criptográfico de clave publica
- SND (Software-Defined Networking) = Redes definidas por software
- MBR (Master Boot Record) = Registro de arranque principal
- AES (Advanced Encryption Standard) = Estándar de cifrado avanzado
- IBM (International Business Machines) = Maquina de negocios internacionales
- P2P (peer-to-peer) = red entre pares
- C & C = Comando y control
- UAC (User Acount Control) = Control de Cuentas de Usuario.
- TOR (The onion router) = La red de comunicaciones superpuesta a Internet y basada en un sistema de enrutamiento por capas.
- IC3 (Internet and Computing Core Certification) =Certificación básica de internet y computación.
- PGP (Pretty Good Privacy) = privacidad bástate buena

TABLA DE CONTENIDO

LISTADO DE IMÁGENES

LISTADO DE TABLAS

1. INTRODUCCIÓN

Ransomware es un programa de código malicioso que infecta el computador, el cual se propaga rápidamente cifrando los datos que se encuentran almacenados en la maquina o en su defecto bloqueándola. Este malware evita que las personas puedan acceder a la información o archivos que se encuentran en el computador, ya que estos están encriptados. El creador de este malware exige un rescate para poder recuperar los datos, que consiste en enviar una clave para poder desencriptarlos, este pago por lo general se solicita en bitcoin, que es una moneda digital de amplio uso en internet.

Ransomware ha demostrado su lado destructivo, porque desde la primera infección hasta ahora ha venido evolucionando como se puede observar en la figura 1, en sus inicios solo mostraba anuncios, bloqueaba el servicio, desactivaba el teclado, en la actualidad encripta los datos y bloquea el sistema, dejando a las victimas sin información. A este malware se conoce como ransomware criptográfico.

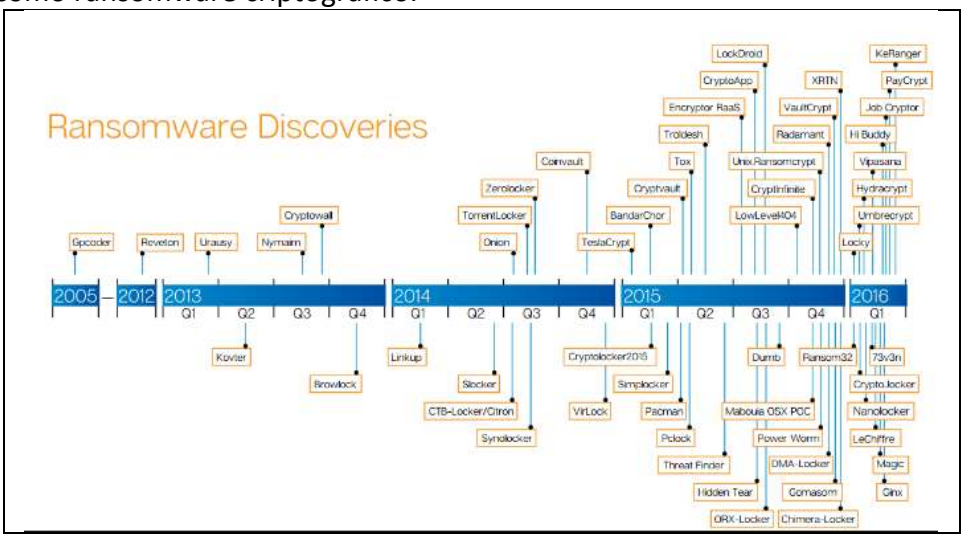


Figura 1 evolución del ransomware (Samuel, 2016).

Según un informe presentado por ESET, se han identificado más de 200 mil nuevas variantes de códigos maliciosos por día. (Orfila, 2016). Los ataques de ransomware manejan una cantidad de sistema operativo que afecta Windows, Linux, MAC, iOS y Android etc. Algunos de los casos que se ilustran a continuación muestran que este malware está afectado tanto a personas como empresas.

El día 12 de mayo del presente año se presentó una infección a nivel global del malware ransomware llamado Wannacrypt. Este malware afecto a empresas y particulares en más de 150 países, incluyendo Estados Unidos, Reino Unido, Taiwán, Francia, Japón y España,

siendo este malware capaz de ejecutarse en más de 27 idiomas distintos. En solo una hora de propagación infecto a más de 7000 equipos. Este malware pide un rescate de 0.1787 Bitcoins, el cual equivale a 300 dólares. Según este informe, hasta la fecha de dicha publicación ya se llevaba más de 80.000 dolores recaudado (Telefónica, 2017).

El día 27 de junio del presente año se presentó un ataque por el ransomware NotPetya, este Ransomware afecto varios países y uno de los más afectados fue Ucrania como se muestra en la figura 2. Este ransomware está pidiendo un rescate de 300 dólares. El objetivo principal de este malware es muy diferente a las versiones anteriores debido que este no cifra archivos con extensión PNG (de imágenes) y se centra en archivos con extensiones de lenguaje de programación como python, visual basic etc. (Pastor, 2017).

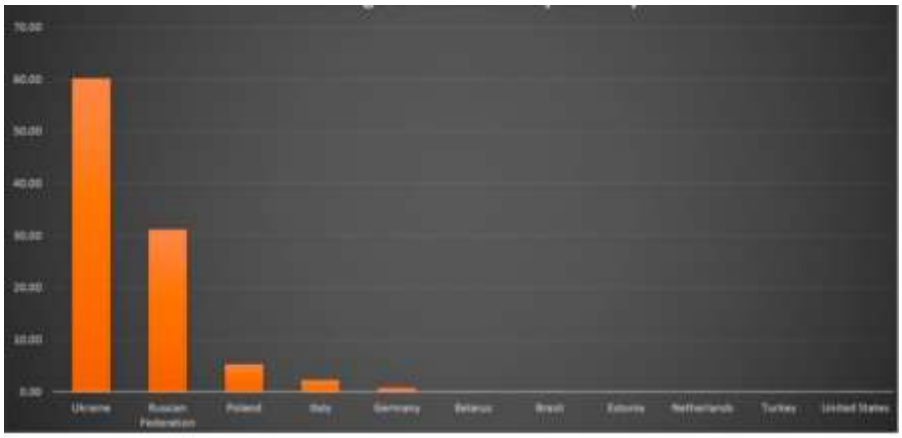


Figura 2. Infección del ransomware NotPayte por países (Pastor, 2017)

Cryptolocker entre septiembre de 2014 y 2015 infecto a más de 500 computadoras en todo el mundo, incluidas dos de la NASA. Del cual los ciberdelincuentes pudieron recaudar alrededor de US$ 3 millones.

Las siguientes estadísticas nos muestran la propagación de este malware en los últimos años: la cantidad de usuarios afectados en el periodo de 12 meses entre abril de 2015 y marzo de 2016 aumento en un 17,7 % en comparación al periodo de abril 2014 a marzo de 2015 aumento de 1.967.784 a 2.315.931 de usuarios en todo el mundo. (Orfila, 2017).

1.1. Planteamiento del problema

En la presente investigación se va mostrar que debido al problema que hoy en día se presenta con los ataques de ransomware criptográfico donde las personas y empresas se están viendo afectadas por este malware, surge la necesidad de proponer unas buenas prácticas para evitar que los usuarios que por falta de información sean vulnerables a estos ataques y puedan conocer y aprender que hay varias formas de tratar de evitar ser afectado por alguno de estos malware. Esta investigación se centró en proponer buenas prácticas

debido a la dificultad de aplicar técnicas de criptoanálisis para recuperar la información afectada.
Este estudio se realizó por medio el semillero de investigación en seguridad de los sistemas de información -SISSI- en la línea de criptografía y criptoanálisis.

1.2. Objetivo General

Proponer Buenas prácticas para mitigar los ataques criptográficos con el malware Ransomware.

1.3. Objetivos Específicos

- Crear un estado del arte sobre el malware ransomware
- Clasificar los diferentes tipos o mutaciones que se utilizan con ransomware criptográfico
- Analizar el comportamiento de los ataques con ransomware que representan mayor riesgo
- Proponer buenas prácticas para mitigar los ataques por ransomware criptográfico.

1.4. Organización de las memorias

Este informe está organizado por seis capítulos:

Capítulo 1: Introducción, este capítulo consta de la pertinencia de la investigación donde se explica que es el ransomware, datos estadísticos y algunos ejemplos de afectación de este malware, también se explica el planteamiento del problema y la justificación de la misma, se ilustran los objetivos generales y específicos de la presente investigación.

.

Capítulo 2: En el marco conceptual podremos encontrar todas las definiciones que requiere para entender todos los términos que se van a utilizar en este informe y contextualizar al lector con los conceptos más relevantes del área del conocimiento.

Capítulo 3: Estado del arte, a partir de la revisión a la literatura se presenta la recopilación de la información reportada de la evolución histórica del ransomware criptográfico.

Capítulo 4: Metodología, en este capítulo se describe las etapas que se utilizaron para poder cumplir con el objetivo de esta investigación. Las cuales son: a partir de la revisión de la literatura se realizó una clasificación, donde se desarrollaron las siguientes etapas:
Etapa 1: estado del arte, etapa 2: clasificación del ransomware, etapa 3: top 10 del ransomware y por último en la etapa 4: buenas prácticas para tratar de mitigar el ataque por ransomware criptográfico.

Capítulo 5: Resultados y Discusión, en este capítulo se presentan buenas prácticas, donde podrá encontrar algunas recomendaciones que se deben seguir para evitar ser infectado por algún ransom, también encontrara otras recomendaciones en caso de que se hayan

visto afectados por algún tipo de malware y por último algunas pautas en caso de que se vean infectados por petya o wannacrypt

Capítulo 6: Conclusiones, recomendaciones y trabajos futuros, en este capítulo se puede encontrar algunos resultados y recomendaciones que se tomaron de acuerdo con el desarrollo del proyecto, también se puede evidenciar algunos trabajos futuros que se pueden realizar con base al adelanto de esta investigación.

2. MARCO CONCEPTUAL

Este capítulo contiene las diferentes definiciones que se necesitan para la comprensión de los términos más relevantes que se van a ostentar en este documento y que requieren para una compresión de las memorias.

2.1.1. Malware:

Es un software malicioso que engloba todo tipo de programa o código informático cuya función es causar mal funcionamiento en un sistema infiltrándose al equipo sin consentimiento del usuario. Las principales características son: es un programa dañino; es decir causa daño en el sistema que infecta, es autorreproductor; lo que quiere decir que crea copias de sí mismo y por último utiliza varias técnicas para evitar que el usuario se dé cuenta que está infectado (Pérez, 2015)

2.1.2. Sistema Informático:

Es un sistema que se basa fundamentalmente en el procesamiento de la información empleando la computación, también se puede definir como un conjunto de funciones interrelacionada; hardware, software, información y recursos humanos. Esta emplea un sistema que usan dispositivos que son utilizados para programar y almacenar datos. No solo esta echo para almacenar la información, sino que también funciona como un sistema de gestión de información y conocimientos, la cual desarrolla dos actividades fundamentales: la toma de decisiones y el control del mismo. (Ecuared, 2017).

2.1.3. Seguridad Informática:

Es la disciplina encargada de proteger la integridad, privacidad y disponibilidad de la información almacenada en un sistema informático. La seguridad informática se divide en varios pilares pero estos son los cinco más conocidos en el mercado: la integridad; es la encargada de verificar que los datos almacenados si son los verdaderos, confiabilidad; es la que asegura que solo las personas autorizadas accedan a los recursos que se intercambian, la disponibilidad; garantiza el correcto funcionamiento de los sistemas informáticos, evitar el rechazo; esta se encarga de evitar la negación de una operación autorizada y la autenticación; es la encargada de asegurar que solo las personas autorizadas tengan acceso a la información.(ccm,2017)

2.1.4. Criptografía:

La criptografía es la ciencia que se encarga de ocultar o resguardar documentos y datos, esta actúa por medio del uso de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o internet, además de mantener la seguridad del usuario, la criptografía preserva la integridad del mensaje, la autenticación del usuario, así como también la del remitente y el destinatario. (conceptodedefinicion, 2014).

La criptografía se divide en dos grandes ramas, la criptografía privada o simétrica y la criptografía de clave pública o asimétrica.

2.1.5. Criptografía informática:

Es una rama de la matemática encargada de proporcionar las herramientas necesarias o idóneas para solucionar los problemas relacionados con la autenticidad y la confiabilidad. La confiabilidad utiliza o se vincula usualmente con técnicas de encriptación, y la autenticidad utiliza técnicas de firma digital, aunque la solución de ambos se centra en una sola tarea que es la aplicación de procesos criptográficos de encriptación y descripción. Se puede entender que esta forma de encriptación es la manera de codificar la información de un archivo o de un correo electrónico para que no sea descifrada por un tercero. (Espinosa, 2009). En la figura 3 podremos observar el proceso criptográfico (cifrado/descifrado).

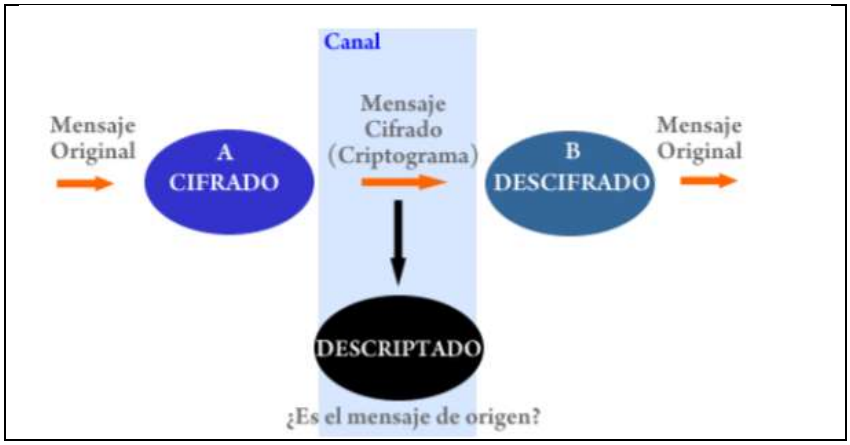


Figura 3. Proceso criptográfico (Sanjuán, 2012)

2.1.6. Firmas digitales:

Son mecanismo que proporcionan la integridad y autenticidad, la cual nos permite saber si un mensaje lo ha enviado realmente una persona o ha sido alterado en su trayectoria. En la figura 4 podremos observar su funcionamiento. (Sanjuán, 2012).

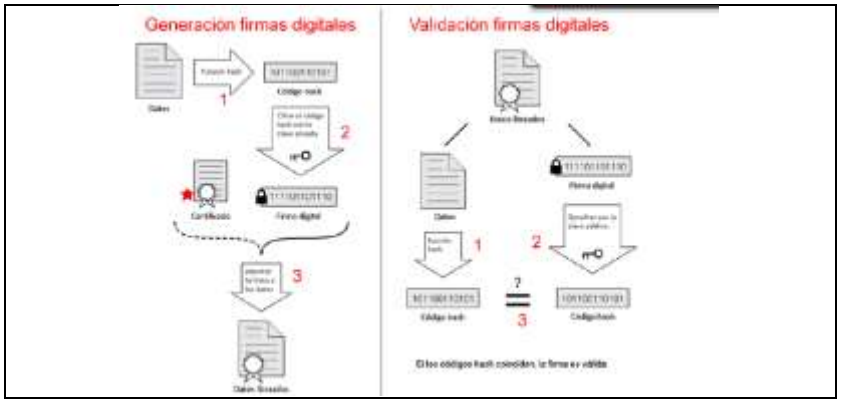


Figura 4 Funcionamiento de las firmas digitales (Sanjuán, 2012).

Leudis San Juan en un artículo que escribió en el año 2012, explica algunas definiciones y métodos de la criptografía. Los cuales se pueden observar continuación.

2.1.7. Sistema de Clave Único o Método Simétrico:

Son aquellos donde el proceso de cifrado y descifrado utilizan una única clave. Esta forma de cifrado utiliza una clave secreta denomina secreto compartido, la cual es generada por el emisor y el receptor requiere de la clave secreta para poder desbloquear los datos que son enviados por el emisor, como se ilustra en la siguiente imagen.

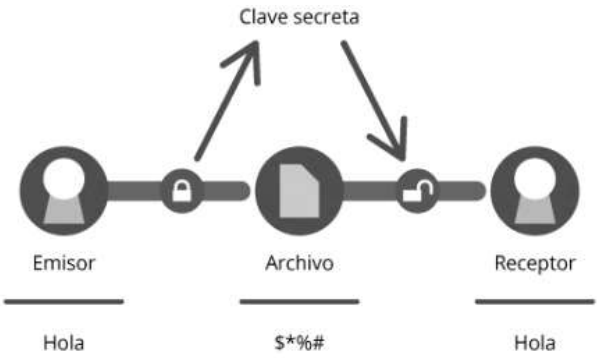


Figura 5 proceso de clave único o método simétrico (Gutiérrez, 2013)

Dentro del cifrado simétrico existen dos tipos de algoritmos los cuales son:

2.1.8. Cifrado por bloques:

Este se encarga de cifrar el mensaje original agrupándolo en grupos de bit de una longitud fija por lo general de (64 a 128 bits), es decir divide el texto en bloques relativamente largos. Ejemplo, el algoritmo AES (Advanced Encryption Standard).

2.1.9. Cifrado por flujos:

Es aquel que cifra el mensaje original bit a bit o byte a byte. Es decir, divide el mensaje en bloques pequeños. La transformación se aplica sobre cada carácter del mensaje original, cada bit del mensaje. Ejemplo el algoritmo RC4 o ARC4 y es empleado en transport layer security (TLS/SSL).

Ventajas de los sistemas de clave única o simétrica:

- Es un método de fácil uso
- Es muy útil para cifrar archivos de datos personales
- Los algoritmos tienen mucha velocidad y cifran grandes cantidades de datos. (redeszone, 2010).

Desventajas de los sistemas de clave única o simétrica:

- La distribución de las claves es en un medio público la cual puede ser interceptada.
- Se dificulta por la capacidad de almacenar y proteger muchas claves diferentes. (Sanjuán, 2012).

2.1.10. Sistema de Clave Pública o Asimétrica:

Son aquellos donde el proceso de cifrado y descifrado son llevados por dos claves distintas y complementarias. Esta forma de cifrado utiliza una clave secreta y otra pública. El mensaje se cifra utilizando la clave pública del destinario y para poder descifrarlo utiliza su propia clave privada.

Ventajas del sistema de clave pública o asimétrica:

- Es versátil es decir resuelve muchos problemas
- seguro
- no tiene problemas para la distribución de claves. (ma1.eii.us (S F))

Desventajas del sistema de clave pública o asimétrica son:

- Para tener una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje de cifrado ocupa más espacio que el original. (Sanjuán, 2012).

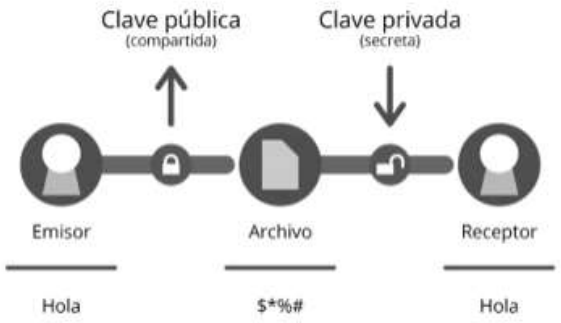


Figura 6 proceso de clave pública y privada (Gutiérrez, 2013)

2.1.11. Métodos criptográficos asimétricos

2.1.12. Cifrado de Cesar

También conocido como cifrado de desplazamiento, es una de las primeras y más simples técnicas de cifrado. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra en un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc. (ugr, S.F)

2.1.13. Cifrado por Sustitución:

Este método está encargado de establecer una comunicación entre las letras del alfabeto en las que se encuentra escrito el mensaje original y los elementos de otro conjunto, que puede ser el mismo o distinto del alfabeto. Es decir, cada letra del texto original se sustituye por un símbolo correspondiente en la elaboración del criptograma. Por otra parte, el receptor que conoce la correspondencia lo que hace es sustituir cada símbolo del criptograma por el símbolo correspondiente del alfabeto original, recuperando así el mensaje enviado inicialmente.

2.1.14. Cifrado por Transportación:

Este método lo que hace es reorganizar los símbolos del mensaje original en un orden diferente, de tal forma que el criptograma contenga los mismos elementos del mensaje original pero ubicados en forma diferente, el receptor conociendo el método de la transposición organiza los símbolos que se encuentran desorganizados del criptograma en su posición original.

2.1.15. Cifrado de Curva Elíptica

Este cifrado se encarga de generar claves en inglés es decir genera claves difíciles de resolver, pero no imposible, aunque implementando la tecnología actual tardaría miles de año. Este cifrado es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas. Sus autores argumentan que la curva elíptica puede ser más rápida y usar claves más cortas que los métodos antiguos
(Preukschat, 2014).

2.1.16. Cifrado Xor

Este cifrado utiliza el operador XOR y una clave secreta. Dicha clave es proporcionada por el emisor y el receptor del mensaje utiliza la clave para poder descifrar el mensaje original.
Funcionamiento

- El emisor manda un mensaje a.
- Este mensaje es decodificado con una clave b
- (a) $\oplus$ (b) de esta forma se crea la clave para ser enviada al receptor
- Para que el receptor puede ver el mensaje original se vuelve a utilizar la operación xor (a) $\oplus$ (b). (Cárdenas Gaby García, 2011)

2.1.17. Algoritmos de Cifrado para el Proceso de Encriptación Simétrica

A continuación, se van a describir los algoritmos más usados para realización de la criptografía simétrica

2.1.18. Des

Es un algoritmo de cifrado por bloques de 64 bits fue ideado por IBM (International Business Machines) y aceptado por NIST (National institute of stander and tecnology). Como se

menciona anteriormente es un algoritmo de 64 bits donde 56 bits contienen la clave de cifrado, mientras los 8 bits restantes son utilizados para la corrección de errores.
Funcionamiento: utiliza un dato y una clave de 64 bits cada uno al inicio y al final del algoritmo, se utiliza dos permutaciones al dato que se va cifrar, después que se realiza la primera permutación el dato es pasado por dieciséis rondas de cifrado en las cuales es necesario la utilización de unas subclaves las cuales se obtienen a partir de la clave que se ingresa al inicio del algoritmo, es decir son 16 subclaves, una para cada ronda. Finalmente, cuando se termina de hacer todas las rondas se realiza la segunda permutación y de esta manera se obtiene el cifrado por medio del algoritmo DES. Este método fue roto en enero 1999 con un sistema de cómputo que analizaba más 250.000.000.000 claves por segundo.

Ventajas:

- Rapidez de cálculo
- Sencillez e implementación

Desventajas:

- Maneja poca longitud de clave.
- Incapacidad de manejar claves de longitud variable.

2.1.19. Triple-DES

Este algoritmo fue inventado poco después que se rompe el algoritmo DES, el cual consiste en utilizar tres veces el algoritmo DES en un orden especifico. Este algoritmo utiliza un cifrado de 192 bits de los cuales 168 bits son efectivos y 24 bits es de corrección de errores.
Funcionamiento: Lo primero que hacen es cifrar el dato con una clave, el resultado de esto es descifrado con otra clave y por último el resultado del descifrado es nuevamente cifrado donde la clave que utilizan en este último paso puede ser cualquiera de las dos claves utilizadas o puede ser una nueva clave.
Ventajas:

- Mayor aumento de seguridad del sistema DES

Desventajas:

- Mayores recursos utilizados en el ordenador

2.1.20. RC4

Este algoritmo fue diseñado en el año 1987 por Ron Rivest, está orientado a generar secuencias de bits, además permite generar claves de diferentes longitudes. Forma una parte vital del sistema de cifrado en capas SSL (Secure Sockets Laye), ampliamente utilizado en navegadores de Internet tales como Netscape Navigator y Microsoft Internet Explorer.
Funcionamiento: Lo primero que hace es a partir de la clave secreta se elige una permutación del grupo simétrico 256, es decir lo que hace en primera instancia es ordenar los números del 0 a 255. Luego hace el proceso de cifrado que consiste en tomar el primer bit del mensaje y le hace un cifrado efectuando una XOR con una parte de la permutación. Y esto lo realiza con cada byte del mensaje.

Ventajas:

- Ejecución rápida en software.
- Fácil implementación

Desventajas:

- Tiene una llave de 40 bits lo que la hace vulnerable a ataques por fuerza bruta (Ecured, S.F)

2.1.21. RC5

Este algoritmo fue diseñado en el año 1994 por Ronald Rivest en sustitución del RC4. Este algoritmo opera por bloques de 32, 64 o 128 bits

Funcionamiento: Utiliza número de palabras variables, numero de vueltas variables y clave secreta de longitud variable. Luego realiza tres operaciones primitivas, tales como suma módulo 2w, Or exclusivo bit a bit y por último hace una rotación de un número y de un bit a la izquierda.

Ventajas:

- Adaptables a procesadores de diferentes tamaños.
- Bajo consumo de memoria.
- Proporciona alta seguridad. (Murillo, Flores, Jiménez S.F)

2.1.22. AES

Este algoritmo también conocido como Rijndael, utiliza un esquema de cifrado por bloques de longitudes de 128, 192 o 256 bits. Con la misma caracterización que definió el tamaño del bloque, las claves son de la misma longitud. Este algoritmo es basado en bits.
Funcionamiento: Cifra el mensaje de longitudes de 16, 24, o 32 bytes con claves de longitud 16, 24, o 32 bytes. Los mensajes y claves se manejan en forma de matrices con 4 filas: en donde los mensajes son matrices de 4 x Nb bytes, siendo Nb= 4, 6, 8 y por otra parte la clave es de una matriz de 4 x Nk, Siendo Nk= 4, 6, 8.

2.1.23. IDEA

Este algoritmo fue creado por Xuejia Lai y james Massey en el año 1990.
Este es un cifrado de bloque, que trabajo sobre mensajes de 64 bits con una clave de 128 bits.
Funcionamiento: Utiliza 8 transformaciones idénticas las cuales son llamadas una ronda y una transformación de salida la cual es llamada media ronda. Este algoritmo es derivado de las tres operaciones: Operación O-exclusiva (XOR) bit a bit, suma módulo 216 y multiplicación módulo 216+1.

2.1.24. Safer

Es un algoritmo que utiliza cifrados por bloques, esta emplea un tamaño de bloques de 64 bits y claves de 64 0 128 bits, maneja varias rotaciones, pero lo más recomendable es usar como mínimo 6. (bibing S.F).

2.1.25. Blowfish

Es un algoritmo de cifrado por bloques de 64 bits creado por Scheiner, está diseñado para máquinas de 32 bits y es considerado más rápido que el algoritmo DES. Cada rotación necesita de una permutación que debe tener una clave y de una sustitución que depende de una clave y los datos. La clave permite valores variables con un máximo de 448 bits (bibing S.F).

2.1.26. Algoritmos de Cifrado para el Proceso de Encriptación Asimétricos

En el siguiente contexto se podrán encontrar los algoritmos criptográficos asimétricos más populares.

2.1.27. RSA

Este sistema criptográfico de clave pública fue creado en el año 1977 por Riverts, Shamir y Ademan. Este algoritmo surge con la necesidad de factorizar grandes números enteros. En un sistema de cifrado de clave pública, cada usuario contiene una clave pública y otra privada. Cuando se envía el mensaje el emisor la envía con la clave pública del receptor, y este, es decir el receptor descifra su mensaje usando su clave privada.

Funcionamiento:

- Lo primero que se hace es buscar dos números primos lo suficientemente grandes p y q
- Se obtienen el número n = p * q y Ø = (p-1) * (q-1).
- Se busca un número e tal que no tenga múltiplos comunes con Ø
- Luego se calcula d = e-1 mod Ø, donde mod = al resto de la división de números enteros.
- Y luego de hallar las operaciones anteriores, n es la clave pública y d es la clave privada, los valores p, q y Ø se eliminan, y es necesario hacer público e para el funcionamiento del algoritmo.

Cabe aclarar que el cálculo de estas operaciones se realiza en secreto en la máquina que va guardar la clave privada. (Córdoba, 2016).

2.1.28. Diffie-Hellman

Este algoritmo fue creado en el año 1976, la función del algoritmo es crear dos claves secretas entre dos máquinas, a través de un canal inseguro y enviando únicamente dos mensajes

Funcionamiento:

- Sea q un número primo muy grande
- Sea α una primitiva de q
- Ana elige un número A y transmite XA= α A mod q

- Juan escoge un número B y transmite XB = α B mod q
- Ana calcula la clave de sesión K = (XB)A modulo q
- Juan calcula la clave de sesión K = (XA)B modulo q
- Se establece sesión con la clave K. (campos Javier,2011)

2.1.29. El Gamal

Se refiere a un esquema de cifrado basado en el problema matemático del logaritmo discreto. Es un algoritmo de criptográfico asimétrica basado en la idea de Diffie-Hellman y funciona de una forma parecida a este algoritmo discreto. Este algoritmo puede ser utilizado tanto para generar firmas digitales como para cifrar o descifrar, el algoritmo no está bajo ninguna patente lo que lo hace de uso libre. La seguridad del algoritmo se basa en la suposición que la función utilizada es de un solo sentido debido a la dificultad de calcular un algoritmo discreto.

Funcionamiento

- Después que se tenga el mensaje que se va cifrar, lo primero que hay que hacer es convertir este texto en un elemento G
- Después de estar convertido queda como resultado M
- Luego se escoge un numero arbitrario en este caso que se llame b, el que viene siendo $b \in \{2, \ldots, p-1\}$
- Después de lo anterior se calcula esta siguiente formula $y_1 = g^b \pmod p$
- Y el mensaje cifrado quedara como una dupla $C_b(m, b) = (y_1, y_2)$ (redyseguridad.fi, 2017).

2.1.30. DSA

DSA (Digital Signature Algorithm, en español Algoritmo de Firma digital) es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. DSA se hizo público el 3 de agosto de 1991, este algoritmo como su nombre lo indica, sirve para firmar y no para cifrar información. Una desventaja de este algoritmo es que requiere mucho más tiempo de computo que RSA. DSA emplea un algoritmo de firma y cifrado distinto al del RSA, aunque ofrece el mismo nivel de seguridad.

Funcionamiento

- Lo primero que se debe hacer es escoger un numero primero con una longitud 512 bits como mínimo P.
- Luego se escoge otro número primo Q con una longitud de 160 bits.
- Se genera un parámetro para calcular la clave pública G.
- X es la clave privada del remitente.
- Y es la clave pública del remitente.

Para aplicar el algoritmo de firma se aplica estos parámetros

- K es un número pseudoaleatorio único que es necesario para cada forma.
- S es el valor que corresponde a cada firma.
- R es el valor total de comprobaciones de la firma. (redyseguridad.fi, 2017)

2.1.31. Función Hash:

La función hash son técnicas de cifrado moderno, que por medio de una entrada ya sea texto, contraseña o un archivo, crea una salida alfanumérica de longitud fija, es decir que por medio de una entrada crea una cadena que solo puede volverse a crear con los mismos datos. Esta sirve para verificar la integridad del contenido del elemento al que se le saco el hash (Gutierrez,2013)

Características:

- Unidireccionalidad: lo que implica que deberá ser computacionalmente muy difícil por no decir imposible obtener el mensaje original a partir del código hash.
- Compresión: no importa la longitud del mensaje, el hash h (M) debe tener una longitud fija normalmente menor.
- Coherencia: Tanto el mensaje original de entrada como el mensaje original de salida deberán producir la misma salida.
- Facilidad de cálculo: A partir de un mensaje el cálculo de la función hash debe ser fácil.
- Único: Es casi imposible encontrar dos mensajes que generen el mismo código hash.
- Difusión: el resumen H (M) debe ser una función compleja de todos los bits del mensaje M.

En la figura 7 podremos observar el funcionamiento del algoritmo hash

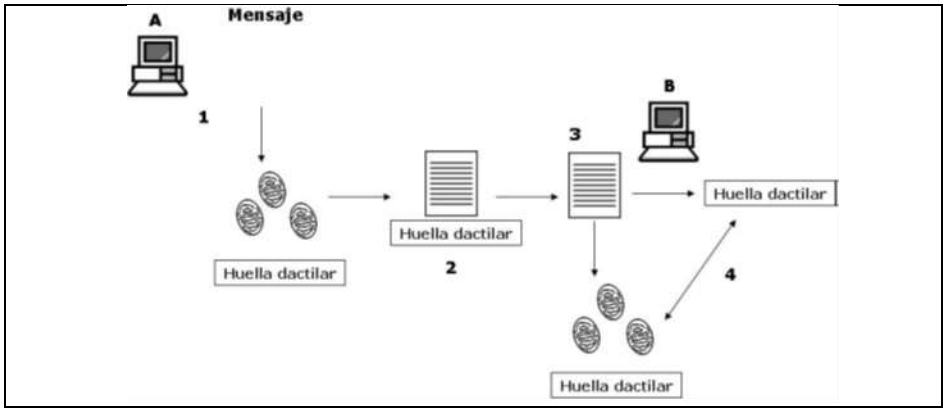


Figura 7 algoritmos hash (Sanjuán, 2012)

Funcionamiento:

- A escribe un mensaje que sirve como entrada de función hash.
- El resultado de la función hash se le adiciona la huella dactilar al mensaje que se envía es decir B.

- B separa el mensaje y la huella dactilar adjunta y utiliza el mensaje como entrada de la misma función hash que utilizó A.
- Si los hashes coinciden, B puede estar seguro de que el mensaje no ha sido modificado. (Sanjuán, 2012)

2.1.32. Funciones Tipo Hash:

2.1.32.1. MD5

Es un algoritmo de reducción criptográfico de 128 bits inventado por Ronald Rivest en 1991, Este algoritmo recibe una cadena de texto como entrada y devuelve un numero de 128 bits.

Funcionamiento:

- Lo primero que se hace es adicionar bits de relleno, es decir el mensaje es rellenado con n bits, de tal forma que le falte a su longitud 64 bits para ser múltiplo de 512. El primer de los n bits es 1 y el resto son 0.
- Luego se agrega longitud, es decir la longitud es agregada a una representación de 64 bits ay esta es añadida en formas de dos palabras de 32 de bits, luego se muestra los bits más significativos, si esta es mayor de 264, se usan los 64 bits menos significativos.
- Luego se inicializan los bufferes, en este caso A, B, C Y D, los cuales son registros de 32 bits.
- Después el mensaje se procesa en bloques de 64 bits, donde la entra y salida es de 32 bits.
- Luego se obtiene la salida que es un mensaje producido por A, B, C Y D con los bits menos significativos de A y terminando con los más significativos de D. Independientemente de la longitud del mensaje, su tamaño será de 128 bits. (seguridad en redes, 2009).

2.1.32.2. SHA

Este algoritmo cuenta de varias ramas la primera de ellas fue publicada en el año 1993, sin embargo, este cambio al nombre SHA-0, y dos años después crearon SHA-1, luego de estas se crearon cuatro familias más que en lo único que se diferencia es en la modificación del diseño y rango de salida incrementas, estas familias reciben el nombre SHA-224, SHA-256, SHA-384, y SHA-512. (Sanjuán, 2012).

2.1.33. Comparativo de los Sistemas Simétricos y Asimétricos

A continuación, se encuentra la tabla 1 donde se hizo una descripción de los sistemas simétricos y asimétricos, con el fin de tener de forma resumida las ventajas, desventajas y usos de estos diferentes tipos de sistemas.

TABLA 1 Sistema Simétrico y Asimétricos

ALGORITMOS SIMÉTRICOS				ALGORITMOS ASIMÉTRICOS			
TIPO	**VENTAJAS**	**DESVENTAJAS**	**USOS**	**TIPO**	**VENTAJAS**	**DESVENTAJAS**	**USOS**
DES	Hace los cálculos rápido Es fácil de manejar Es un algoritmo de bajo costo	No maneja claves variables. Tiene muy poca longitud para las claves Es inseguro para algunas aplicaciones porque cifrado de claves es muy corto	Cajeros automáticos y señales de videos	**RSA**	Incluye firma digital que lo hace más fuerte ante un ataque Tiene mayor seguridad	En muchas ocasiones genera claves débiles o demasiado cortas Es más lento al momento de hacer los cálculos	Productos comerciales de software Sistemas de Microsoft y de Apple Redes de ethernet y en tarjetas intelegentes.
TRIPLE DES	Tiene mejor seguridad que el Des	Utiliza mayor recurso en los ordenadores	En tarjetas de crédito y otros medios de pagos electrónicos	**DIFFIE HELLMAN**	La distribución de claves es más segura. Este algoritmo es más rápido y menos costoso	Mayor tiempo de proceso El mensaje de cifrado es más grande que el original es vulnerable al	Red anónima Tor

						ataque de hombre en medio	
RC4	Es de fácil ejecución en el software Fácil implementación Posee buena velocidad para cifrar la información	Es muy vulnerable a los métodos por fuerza fruta, ya que utiliza una clave mi corta	Tarjetas wireless y TLS	**ELGAMAL**	No es necesario transmitir la clave privada entre el receptor y el emisor Es flexible a la hora de usar	Mayor tiempo en los procesos Se requiere de una gran infraestructura El mensaje cifrado es el doble de largo que el original	DSS (Digital Signature Standard) es un algoritmo de firma digital
RC5	Es adaptable a procesadores de diferentes tamaños Utilice clave de longitud variables Es de fácil uso es decir que es sencillo a la hora de implementar	No tiene una longitud determinada de claves.	Este se usa en varios productos de RSA como Data Security	**DSA**	Su velocidad, rápido a la hora de hacer operaciones fácil de implementar	Usa una clave demasiado corta. Es vulnerable a ataques de fuerza bruta. Requiere más tiempo de computo que el RSA	Firmas digitales

AES	Tiene alto rendimiento Encripta y descripta rápidamente los datos Es lo suficientemente seguro para la protección de información	Problemas en la seguridad de la comunicación de las claves Se incrementan las claves cuando necesita conectarse varias personas entre si	Utilizados en programas hechos en flash				
IDEA	No es vulnerable a los ataques por fuerza bruta, porque las claves tienen mucha longitud. Es uno de los cifrados más seguros. No presenta claves débiles	Es fácil de implementar Maneja muy buena velocidad al momento de cifrar los datos	PGP (Pretty Good Privacy), es un programa que sirve para cifrar contenido. OpenPGP.				
BLOWFISH	Tiene mejor velocidad	No permite autentica	Teléfonos				

	que el DES para cifrar los datos Infraestructura sencilla	r al emisor porque utilizan la misma clave	celulares				

Fuente Propia (2017)

2.1.34. Criptoanálisis

Es la ciencia que se encargar de descifrar un mensaje por medio de técnicas Criptoanálisis, sin conocer las llaves correctas. El objetivo principal del criptoanálisis es encontrar debilidades en los sistemas criptográficos que le permitan elaborar ataques donde romperá su seguridad sin conocimiento de la información secreta. (Medina, 2015).

El señor Sanjuán en el año (2012) nos cuenta cuales son las diferentes técnicas o Ataques del Criptoanálisis a los sistemas criptográficos.

2.1.35. Técnicas De Criptoanálisis

2.1.35.1. Ataques de búsqueda de llave Fuerza bruta

En lo que consisten estos ataques es probar muchas claves posibles hasta encontrar la llave correcta. No hay una forma de protegerse contra estos ataques ya que es imposible impedirle al ciberdelincuente que ensaye hasta que encuentre la llave correcta, sin embargo, es una técnica muy poco recomendada ya que muchas veces ni siquiera es posible ensayar todas las claves ya que son demasiadas y no hay tiempo para probar todas.

2.1.35.2. Ataques sólo a Texto Cifrado

Esta técnica en lo que consiste es en descifrar el mensaje sin conocer nada del contenido del mismo.

Según el artículo de dc.uba.ar (S.F), se describen algunos ataques que se hacen a las funciones hash:

2.1.35.3. Ataques de función hash

- **Ataque del cumpleaños**

  Es un ataque criptográfico que se basa en la paradoja del cumpleaños, consiste por ejemplo que en un conjunto de 23 personas hay una probabilidad del 50,7%, que al menos dos personas de ellas cumplan el mismo día. Lo que se quiere decir es que, si una función matemática produce h resultados diferentes, pero igualmente probables y h es lo suficientemente grande, después de evaluar la función entonces el resultado que se espera es que los argumentos sean diferentes pero que coincidan como una colisión (donde dos entradas distintas producen la misma salida).

- **Ataque por pseudo-colisiones**
  Son las colisiones producidas en la función de comprensión (no importa la longitud del mensaje, el hash h (M) debe tener una longitud fija normalmente menor.) que se utiliza en el proceso iterativo de una función de dispersión. Es decir, no importa el número de elementos elegidos al azar se debe verificar si hay algún tipo de colisiones (dos entradas distintas producen una misma salida)

- **Ataques encadenados**
  Este ataque está encargado de quebrantar la función de comprensión f, es decir lo que pretende este ataque es encontrar diferentes combinaciones de bits en la entrada que genera puntos fijos en las sucesivas iteraciones encadenadas.

- **Ataques al motor de encriptación**
  Este ataque lo que pretende es encontrar por medio de la entrada de la función de comprensión del motor son claves débiles o que las colisiones de clave del motor se trasladen a colisiones de hash etc.

2.1.35.4. Ataque a Texto Sin Cifrar Conocido o en claro

Esta técnica consiste en descifrar el resto de los bloques del texto cifrado utilizando la información que ya se conoce.

2.1.35.5. Ataque a Texto Sin Cifrar Elegido

Esta técnica consiste en encontrar la clave utilizada para el texto cifrado por medio de claves que ya conoce y han sido utilizadas en cifrados previos.

2.1.35.6. Ataque man-in-the-middle

Esta técnica consiste en que el atacante se coloca en medio de las dos partes legítima en este caso el emisor y el receptor que son los que se comunican, de tal modo que estos están intercambiando la información creyendo que es un medio seguro, pero este está interceptando todo.

2.1.35.7. Ataques de diccionario

Este ataque consiste en probar varias palabras del diccionario para validar una clave o contraseña. Generalmente las personas utilizan palabras de uso común para crear claves y esto le facilita el trabajo a la memoria, pero no solo a ellos sino también a los atacantes ya que ellos se basan de técnicas como estas para entrar a su sistema. (Webtriplex,2017).

2.1.35.8. Criptoanálisis Diferencial, Lineal y Lineal-Diferencial

Este es un método que por lo general se aplica a cifradores iterativos tales como algoritmos simétricos o de clave secreta (DES, IDEA, etc). Lo que hace este método es un ataque sobre un texto sin cifrar escogido y se basa en un análisis de la evolución de las diferencias entre dos textos sin cifrar relacionados cuando se cifran bajo la misma clave. Luego realiza un

cuidadoso análisis de los datos disponibles, donde genera posibles claves y la clave más probable se identifica como la correcta.

2.1.36. Bitcoin

Es una moneda virtual e intangible. Sirve para intercambiar bienes y servicios, que a diferencias de otras monedas es una divisa electrónica, esta moneda es descentralizada ya que nadie la controla. (Muñoz, 2014).

Su origen fue en el año 2009 cuando Satoshi Nakamoto, seudónimo de una o varias personas decidió lanzar la moneda virtual que solo sirve para realizar operaciones dentro de la Red de redes. Bitcoin hace referencia tanto a la moneda como al protocolo y a la red P2P en la que se apoya. Esta estructura P2P y la falta de control imposibilita que cualquier autoridad manipule su valor o provoque inflación produciendo más cantidad. De hecho, su producción y valor se basa en la ley de la oferta y la demanda.

Funcionamiento: Para hacer uso de esta moneda virtual es necesario descargar un software en el ordenador o nuestro móvil que hará las veces de un monedero virtual, este genera una dirección bitcoin, que se podrá usar para enviar y recibir dinero de otros usuarios. Además, el envío de bitcoin es instantáneo y toda operación puede ser monitorizada en tiempo real. La moneda virtual usa la criptografía para controlar su creación. El sistema está programado para generar un número fijo de bitcoin por unidad de tiempo a través de unos ordenadores llamados miners. Actualmente, ese número está fijado en 25 bitcoin cada diez minutos, aunque está programado de forma que se reduzca a la mitad cada 4 años. Así, a partir de 2017, se emitirán 12,55 bitcoin cada diez minutos. La producción continuará hasta el año 2140, cuando se alcance el tope de 21 millones de unidades en circulación. (Finanzasparatodos, 2010)

2.1.37. Ransomware

Es un malware que restringe el acceso a al sistema y después le exige un pago para poder quitar la restricción, este malware ataca a al sistema o equipo por medio de un enlace a sitios comprometidos en correos masivos, páginas web con contenidos pornográficos, juegos o descargas de internet indebidas (como películas, libros, videos, etc) de modo que cuando los usuarios seleccionan alguno de los anuncios, se le redirige a otra página comprometida que les infecta con ransomware, también por medio de las redes sociales se pueden infectar con este malware, otra técnica es ataques a través de protocolo de escritorio remoto (RDP), ya sea aprovechando una vulnerabilidad en el sistema o por un ataque de fuerza bruta. (Avast, 2017) (Infodasa (S.F)).

3. ESTADO DEL ARTE

El ransomware no es un malware moderno, a pesar de su popularidad actual, su fecha de origen fue en el año 1989. Como podemos ver en la Figura 8, el primer ransom de Windows comenzó a extenderse en el año 1989 y desde entonces ha estado presente hasta ahora, pero ha cambiado significativamente en esta trayectoria.

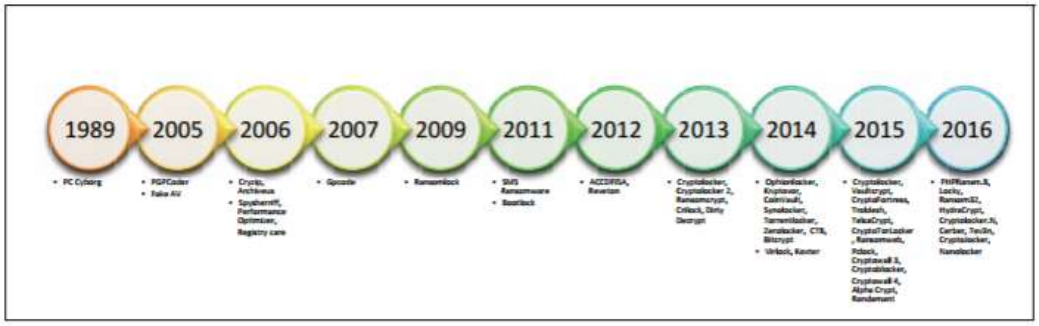


Figura 8 Cronología para ransomware basado en Windows (Monika, Zavarsky, Lindskog 2016).

Como se muestra en la figura 9 el ransomware se ha distribuido en los diferentes países de Latinoamérica siendo México el país donde más se ha visto afectado por este malware.

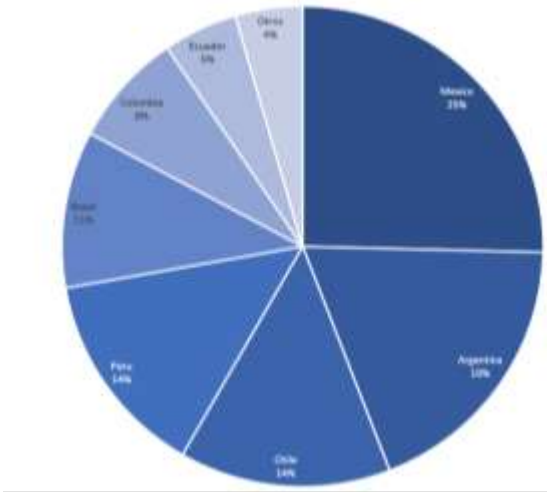


Figura 9 distribución de diferentes familias de ransomware en los países Latinoamérica (Gutiérrez, 2016).

Este malware, como se mencionó anteriormente, a medida que avanza el tiempo se va expandiendo con mayor potencia. El primer ataque de ransomware recibe el nombre de PC Cyborg, que fue visto en diciembre de 1989. Fue el primer tipo de malware criptográfico ya que utilizo la combinación de una clave simétrica y un vector de inicialización para cifrar los archivos que se encontraban en las unidades de la computadora, esta familia comenzó a evolucionar y esto claramente indico la era del ransom del cripto. Gpcode utilizo un esquema de cifrado personalizado para el cifrado de datos. Este se propago de forma desenfrenada hasta el año 2008. (Monika, Zavarsky, Lindskog, 2016).

En el año 1989 se descubrió el primer ransomware de cifrado, pero en el año 2013 fue cuando este se hizo más fuerte y comenzó a usar algoritmos de cifrados seguros, en este año también se vieron otras mejoras significativas como el uso de Redes anónimas como TOR y P2P.a mediados del año 2014 aparece el uso de anónimos ocultos en las redes que se utiliza para la verificación de pagos, desde entonces, tres cuartas partes del ransom variantes, utilizan algún tipo de servicio anonimato para permitir una comunicación segura. (Hampton, Baig, 2015).

En el 2007 en Rusia se originó Zeus un malware bancario. Se estima que ha infectado millones de máquinas y ha causado decenas de millones de dólares en daños en los EE. UU. En el año 2011 el código fuente de Zeus se filtró, lo que permitió conocer su funcionalidad interna. Uno de los principales aspectos de Zeus es su dependencia de la comunicación con un servidor C & C de trabajo. Gran parte de la funcionalidad de Zeus es dinámicamente configurable a través de este servidor, Zeus periódicamente se pone en contacto con su servidor para pedidos adicionales. (Ben Herzog, Yaniv Balmas, 2016).

Ransomware fue evolucionando y cada año va saliendo una familia diferente, en el año 2013 salió las familias de Cryptolocker, Cryptolocker2, Ransomcrypt, Crilock y Dirty Decrypt. Y cada versión es más fuerte que la anterior, en el año 2015, salieron nuevas variantes de Ransomcrypt, Cryptolocker, Vaultcrypt, CryptoFortress, Troldesh, TelsaCrypt, CryptoTorLocker, Ransomweb, Pclock, Cryptowall 3, Cryptoblocker y Cryptowall 4. Cryptowall 3, en la cual ya utilizaban la red de anonimato Tor para la comunicación C & C. que es una nueva forma de encriptación. (Monika, Zavarsky, Lindskog, 2016).

En el año 2014, surgió la primera variante de Simplocker, es el primer virus de móvil que cifra imágenes, videos y documentos usando Advanced Encryption Standard (AES). Antes este malware en móviles solo aseguraba cifrar datos como tácticas de miedo, pero realmente no cifraba ningún archivo. Aunque la primera variante Simplocker fue algo revolucionario, se logró conseguir la clave de descifrado porque los creadores de este malware usaban el mismo cifrado para todos los dispositivos infectados y con ello se creó una aplicación llamada Avast Ransomware Removal que puede descifrar todos los dispositivos infectados con Simplocker. (Perez, 2014)

Las compañías de video juegos no son ajenas a los ransomware porque también se han visto afectadas por ataques por parte de TeslaCrypt es uno de los ransom que se especializa en jugadores de videojuegos. Funciona de una manera muy similar a la mayoría de otros virus, se introduce en secreto en los computadores, luego encripta archivos y pide un código específico para desencriptarlos, TeslaCrypt utiliza un método de encriptación llamado AES. No está muy claro cómo se propaga este malware, sin embargo, está claro que una vez dentro, esta aplicación escaneara todos los archivos en su computador y encriptara algunos de ellos. Hasta ahora no hay manera de desencriptar los archivos. (Malwarerid, 2015).

En el año 2015 apareció la segunda variante de Simplocker. Los cibercriminales que crearon este malware tuvieron que mejorar su método de ataque por uno más fuerte, comenzaron a generar claves únicas para cada dispositivo infectado. Esto por supuesto hace que sea más difícil descifrar los dispositivos infectados.
Se pudo evidenciar que más de 200.000 usuarios móviles se vieron afectados por este malware. Se observó un crecimiento del 5-6% al año entre principios del 2015 y principios del 2016, y no se cree que este crecimiento baje a corto plazo (Perez, 2016).

A principios del año 2014, el laboratorio de ESET ha descubierto una nueva versión malware, llamado Jisut que cuenta con una gran novedad porque los mensajes de secuestro lo hacen por medio de llamadas de voz. Este virus se distribuye a través de un downloader que se utiliza para descifrar e instalar los archivos maliciosos. El proceso de infección se activa una vez que el usuario abre la aplicación y pulsa sobre la opción “activación gratuita”. A partir de ese momento, la victima cede los derechos de administración y ya no puede desinstalar o borrar la aplicación. Además, se bloquea el dispositivo y se escucha el mensaje de audio grabado por los delincuentes. Jisut se ha extendido sobre todo en China.
Según se observa desde ESET, el número total de detecciones de este tipo de malware se duplico en comparación con 2015. No todas buscan extorsionar a las víctimas, ya que algunas solo buscan vender aplicaciones o su código fuente y otras solo pretenden bloquear el dispositivo (Albors, Awareness y Research, 2017)

Desde octubre del año 2015 ha estado activado el ransomware CryptoWall 4.0, usando el tráfico de red para comunicarse con el servidor C&C CryptoWall utiliza nombres de dominio en lugar de direcciones IP directas. El Análisis de tráfico de máquinas infectadas revelo que la comunicación de CryptoWall se basa en mensajes HTTP POST. La comunicación se dirige a los scripts cargados en los servidores web hackeados (servidores proxy) y se cifra usando el algoritmo RC4. Sin embargo, la clave de cifrado es muy fácil de recuperar, ya que se incorpora en la solicitud HTTP. (Cabaj, Mazurczyk, 2016).

En el año 2016 Cabaj y Mazurczyk por medio de un artículo nos informan que, en mayo de 2015, una construcción de ransomware Kit llamado TOX fue descubierto en la tela oscura de los laboratorios de McAfee. TOX adopta un modelo de negocio "ransomware-as-a-service", permite incluso a los cibercriminales sin experiencia crear su propio malware

personalizado y utilizando el sitio web TOX (que reside en la red TOR), para manejar infecciones y beneficios, a cambio de estos "Servicios", TOX recoge el 20 por ciento de cada rescate pagado.

En el primer semestre del año 2015 CryptoWall fue el malware más utilizado, la figura 10a, representa el número de intentos de CryptoWall durante un año desde octubre de 2015 a octubre de 2016, sin embargo, la figura 10b representa el número de víctimas reales de CriptoWall durante el mismo periodo de tiempo.

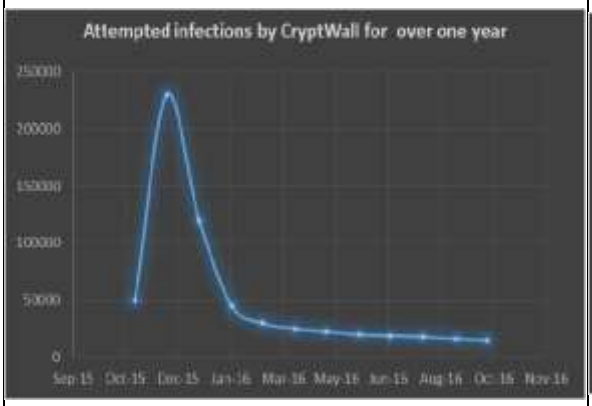


Figura 10ª. Intento de infección por criptowall durante más de un año (Gagneja, 2017).

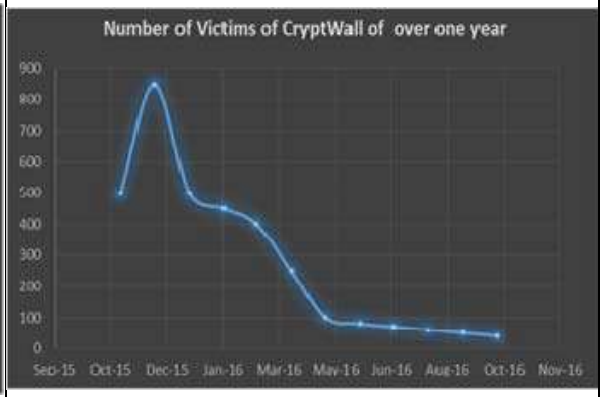


Figura 10b Número de víctimas de CryptoWall por un año (Gagneja, 2017).

CryptoWall se hace responsable de un 41.01% de los ataques a usuarios de Windows y lo hace de un modo muy similar a CryptoDefence, tras filtrarse en un ordenador, encripta todos los archivos y solicita hasta 500 dólares de bitcoin para recuperarlos. Este malware se propaga por visitas a sitios web maliciosos, haciendo clic sobre falsos mensajes que supuestamente actualizan determinados componentes, etc. El país más afectado fue Rusia, sin embargo, se han evidenciados registros en Estados Unidos y España. (Gagneja, 2017).

En febrero del año 2016, las soluciones de ESET comenzaron a detectar a *win32/Filecoder.Locky.* un nuevo ransomware que se propaga a través de adjuntos con macros maliciosas. El laboratorio de investigación de ESET Latinoamérica ya detecto algunos casos, que, dado el corto tiempo de vida de esta amenaza, hablan de su impacto. Los países en los que se reportó la presencia de Locky son México, Perú, Colombia, Chile, Argentina y Guatemala. Además, según Kevin Beaumont, investigador que lo analizo inicialmente, el correo electrónico que lo propago esta traducido a varios idiomas, ampliando su alcance y demostrando el trabajo de preparación que tiene detrás. Así, identifico su presencia en los Países bajos, Alemania, Arabia Saudita, Croacia, Pakistán, Polonia, Rusia y los Estados Unidos.

Las extensiones que puede cifrar son más de 100, es decir, prácticamente todo lo que un equipo pueda tener almacenado: imágenes .JPG, .PNG o .GIF, base de datos como .DB, OBD,

.MDB, SQLITEDB o .DBF, videos como .MP4, .MOV o .FLV, proyectos de propagación como .JS, .VBS o .JAVA, comprimidos como ZIP y muchos más. Todos son cifrados con la extensión "Locky". Además, cambia el fondo de pantalla por el aviso de rescate y crea un archivo de imagen .BMP y uno de texto.TXT y los abre para mostrar las instrucciones de pago. También puede cifrar archivos de la red, considerando que haya más de un equipo conectado a la misma. (Pagnotta, 2016)

Los señores Kessem y Barlow, en el año 2016 informan que el ransomware fue una de las amenazas más prominentes para los consumidores y las empresas, en el año 2016 IBM Security predijo estos ataques que se materializo excesivamente durante el año pasado.
Los primeros tres meses de 2016 las compañías de los EE. UU. desembolsaron hacia fuera más de $ 209 millones en pagos del ransom. Se trata de un dramático aumento de 771 por ciento de los casi 24 millones de dólares que se gastaron en 2015. Los ciberdelicuentes están propagando estas amenazas a un número creciente de personas y organizaciones.
Según IBM X-Forcé, el volumen de spam se cuadruplico en los últimos 23 meses. Aún más preocupante es el marcado de aumento del ransomware asociado al spam, cuya tasa es de hasta 6.000 por ciento, en el año 2015 ha aumentado a casi 40 por ciento que en el año 2016. El FBI estimo que este malware está a paso para convertirse en una fuente de ingresos de mil millones de dólares para los cibercriminales a finales de 2016, un número que se espera que continúe aumentando en 2017. Europol advirtió recientemente que este virus es una de las mayores amenazas en línea que afectan a personas y empresas.

Según una encuesta realizada por IBM (International Business Machines), solo 1 de cada 3 consumidores había oído hablar de ransomware. Por ello era poco probable tomar medidas protectoras para evitar un ataque de este malware. Cuando se les preguntaba sobre la importancia de los datos, el escenario se hizo más realista para los encuestados. Por ejemplo, el 55% de los padres pagaría para recuperar recuerdos preciosos, en comparación con solo el 39% de los no padres. En cuanto a otros archivos, la mayoría de los encuestados rechazaron la idea de pagar a un ciberdelicuentes por sus datos. Muchos indicaron que, si considerasen ceder a las demandas de los defraudadores, no pagarían más de $ 100 dólares para recuperar datos importantes. Sin embargo, los consumidores a menudo terminan pagando muchos más de lo que imaginarían, ya que el ransom exige un promedio de al menos cinco veces esa cantidad. La encuesta de IBM encontró que la mayoría de los empleados no son conscientes de lo que es este virus o cómo puede afectar a su empresa, Los resultados de la encuesta mostraron que tanto la conciencia como la voluntad percibida de pagar para recuperar los datos dependían del tamaño del negocio y la experiencia previa con ataques.
El 70% de los negocios previamente golpeados por este malware indicaron que habían pagado el rescate para recuperar datos de la compañía. El 50% pago más de $ 10.000 dólares y el 20% pago más de $ 40.000. Además, el 60% de los ejecutivos de negocios encuestados creían que pagarían para recuperar los datos en el futuro dependiendo del tipo

de datos perdidos, indicaron que estarían dispuestos a pagar entre $ 20.000 y $ 50.000 para recuperar el acceso. (Barlow,2016).

En el año 2016 el negocio de los ransomware llegó a 638 millones de dólares lo que supone un incremento de 3,8 millones con respecto al año anterior según ha publicado la firma de análisis de seguridad SonicWall. 2016 se llegaron a pagar 209 millones de dólares en concepto de rescates por parte de las empresas. Ahora bien, si este malware ya fue un problema preocupante durante 2016, la firma de seguridad confirma que el 2017 será un año con un grado alto e infección. (Agudo, 2017).

En el 2016, el Departamento de justicia de Estados Unidos revelo que el Centro de Quejas por Delitos de internet (IC3), había recibido cerca de 7.700 denuncias públicas relacionadas con el ransom desde 2005, por un total de $57.6 millones en daños. Esos daños incluyen recates pagados generalmente $ 200 a $ 10,000, según el FBI, así como los costos incurridos en el manejo del ataque y el valor estimado de los datos perdidos. Solo en 2015, las victimas pagaron más de 24 millones de dólares en casi 2.500 casos notificados al IC3. (ESET, 2017)

En el año 2016, los daños ocasionas por ransomware ocasionaron pérdidas de $ 1.5 mil millones, según el investigador de mercado Cybersecurity Ventures. Eso incluye la pérdida de productividad y el costo de llevar a cabo investigaciones forenses y la restauración de datos. Las pérdidas económicas y financieras globales del ataque “WannaCry” que paralizo las computadoras en al menos 150 países en el año 2017 podrían aumentar a miles de millones de dólares, lo que lo convierte en uno de los incidentes más dañinos que involucran a los llamados ransom. La firma de modelos de riesgo cibernéticos Cyence estima que los costos potenciales de la piratería en $ 4 mil millones, mientras que otros grupos predicen que las perdidas estarían en los cientos de millones. El ataque es probable que haga 2017 el peor año para las estafas de rescate, en las que los hackers toman el control de las computadoras de una compañía u organización y amenazan con destruir datos a menos que se haga el pago. (MoneyWatch, 2017)

Un gran porcentaje de la población mundial utiliza un teléfono inteligente, este crecimiento es ideal para los cibercriminales porque las personas almacenan una gran cantidad de datos personales en sus móviles, eso significa que estarían dispuestos a pagar un rescate para recuperar sus datos en peligro. “Las claves de cifrado de ransomware en móviles son cada vez más fuertes, pero todavía son aproximadamente cinco veces menos sofisticadas que las de los ordenadores “dice Filip Chytrý, investigador de seguridad en Avast. Este malware en móviles cifra los datos usando un algoritmo AES de 256 bits, que todavía es imposible de descifrar sin la clave correcta". En 2015 es habitual que el ransom solo aparezca en ordenadores, pero como ya se informó anteriormente, existe en teléfonos móviles. Pero aún no está del todo extendido. Sin embargo, un reciente informe de la firma de análisis y seguridad Kaspersky Lab afirma que este malware en móviles ha despuntado en lo que llevamos del año y alerta de una futura propagación a teléfonos móviles y tabletas a muy corto plazo (Hernández, 2017).

El señor Gross, en el año 2017 informa sobre las diferentes estadísticas de los ataques por Ransomware. En el año 2016 se vio una enorme pérdida financiera por los ataques de este malware. Los criminales ya no se adhieren a su "código de ética" a lo contrario y en muchos casos, cuando se pagan rescates, los atacantes no devuelven el acceso a los archivos a sus dueños legítimos. También informa que de acuerdo con una encuesta realizada por Bitdefender y Spiceworks entrevistó a 250 profesionales de la tecnología de la información que trabajan en pequeñas y medianas empresas para obtener alguna información sobre este malware. Informan que una de cada cinco PYMES había sido infectada con ransom en el último año; de ellos, el 38% pagó el rescate (un promedio de $ 2,423), Pero de los que pagaron el rescate sólo el 45% obtuvo sus datos.

El siguiente estudio realizado por Pew Research Centeren en enero, descubrió que a pesar de que hay más personas que nunca han estado en riesgo de ser hackeado, la mayoría de las personas todavía no están tomando precauciones de seguridad para evitar ser infectados con algún tipo de malware, casi el 30% de los usuarios de teléfonos inteligentes ni siquiera utilizan una contraseña de pantalla de bloqueo en su teléfono. Un 54% de los usuarios de internet han accedido a redes públicas de wifi, lo que las pone en riesgo de ser hackeadas, y uno de cada cinco de ellos admite utilizar una red pública para servicios sensibles, como ingresar a una cuenta bancaria.
Un estudio realizado por Pew dice que al examinar las prácticas de contraseñas se encontró que el 25% de los encuestados están usando contraseñas que no se consideran necesariamente seguras, simplemente porque son fáciles de recordar.
Un informe del proveedor de seguridad Splashdata encontró que las contraseñas "123456" y "contraseña", se encuentran en la parte superior de la lista para contraseñas publicadas en foros de hackers por segundo año consecutivo.
Casi dos tercios de los usuarios de Internet han sido víctimas de algún tipo de piratería informática. Por ejemplo, en Yahoo por el incumplimiento de las cuentas de correo electrónico de los usuarios afectó a más de 1 millón de usuarios. (Gross, 2017).

En el año 2016, se tomaron a los ordenadores pertenecientes al Hollywood Presbyterian Medical Center en los Ángeles como rehenes usando un ransomware llamado Locky. Las computadoras estuvieron fuera de línea por más de una semana hasta que los funcionarios cedieron ante los extorsionistas y pagaron el equivalente a 17.000 dólares en Bitcoin.
El Hospital en Herdeson, Kentucky fue infectado por el ransomware Locky, un ataque que impidió a los proveedores de salud acceder a los archivos de pacientes. La instalación declaro un “estado de emergencia”, los funcionarios metodistas, sin embargo, dijeron que no pagaron el rescate; los administradores en ese caso simplemente habían restaurado los archivos por medio de copias de seguridad.
Ransomware ha sido un flagelo de internet durante más de una década, pero solo recientemente ha hecho titulares de los medios de comunicación. Eso se debe principalmente a una nueva tendencia en los ataques de ransomware. Los hospitales son la

marca perfecta para este tipo de extorsión porque proporcionan cuidados críticos y se basan en la información actualizada de los registros de pacientes.
Sin un rápido acceso a las historias clínicas, cirugías y otra información, la atención al paciente puede demorarse o detenerse, lo que hace que los hospitales tengan más probabilidades de pagar un rescate en lugar de arriesgar retrasos que podrían resultar en muerte y demandas judiciales. (Zetter, 2016)

Los meses transcurridos del presente año se evidencian que el número de archivos de ransomware móviles detectados llego a 218.625 durante el trimestre, en comparación con los 61.832 de trimestre anterior. La familia Congur es el ransomware más popularizado, representado más del 86%. Este es principalmente un bloqueador, que configura o restablece el PIN del dispositivo (código de acceso), dándole a los atacantes derechos de administrador en el equipo. Algunas variantes del malware aprovechan estos derechos para instalar su módulo en la carpeta del sistema desde donde es casi imposible eliminarlo. A pesar de la popularidad de Congur, Trojan-Ransom.AndroidOS. Fusob.h sigue siendo el ransomware móvil más utilizado. Se contabilizo que casi el 45% de los usuarios atacados estuvieron expuestos a esta amenaza durante la investigación. (Aluzardo, 2017)

En septiembre del año 2016 el ransomware de Erebus (RANSOM_EREBUS.A) apareció por primera vez, siendo distribuido por malvertisements (anuncios maliciosos). El kit de explotación Rig, es el que se encarga de infectar los sistemas de la víctima con este ransomware. Este malware tiene como objetivo 423 tipos de archivos, archivos de codificación con el algoritmo de cifrado RSA-2048 y anexa los archivos afectados con la extensión. Ecrypt esta versión de Erebus se observó utilizando sitios web comprometidos en Corea del Sur como sus servidores de comando y control (C&C).

En febrero de 2017, se descubrió que Erebus había evolucionado y cambiado de táctica, utilizando una técnica que evita el Control de cuentas de usuarios (UAC), una característica de Windows que ayuda a prevenir cambios no autorizados en el sistema para ejecutar el ransomware con privilegios elevados. En su nota de rescate, Erebus amenaza con borrar los archivos de la víctima dentro de las 96 horas a menos que se apague el rescate, que es 0,085 Bitcoin (US $ 216 al 15 de junio de 2017). Esta versión (RANSOM_EREBUS.TOR) también elimina las instantáneas para evitar que las victimas recuperen sus archivos. (Trendmicro, 2017)

En mayo del 2017 en la semana del 13 al 19, el conocido WannaCry logro infectar miles de sistemas a través de múltiples industrias en todo el mundo. WannaCry fue descubierto utilizando el servicio de alojamiento de archivos Dropbox como parte de su método de propagación. La nueva variante aprovecha MS17-010, una vulnerabilidad en el bloque de mensajes de Windows server (SMB) con un código de exploit llamado EternalBlue, para entregar su carga útil, que incluye el archivo de ransomware. Los archivos afectados en el sistema de destino se cifrarán con un apunte WNCRY.

Lo que hace que Wannacry sea particularmente peligroso es que también tiene un componente de gusano, que escanea e intenta infectar las maquinas con un puerto abierto 445 tanto en la red de área local (LAN) como internet. Analiza todas las direcciones enumeradas dentro de la red y busca específicamente maquinas con un puerto 445 abierto. Para la parte de internet, buscara de nuevo direcciones IP aleatorias para comprobar un puerto abierto 445. Cuando encuentre una dirección IP con un puerto abierto, comenzara a escanear todos los dispositivos del mismo rango IP/24 como blancos adicionales. Esta rutina de gusanos permitió que el ransomware se propagara rápidamente en un corto periodo de tiempo. Mientras que Microsoft ya había arreglado el MS17-010 es una actualización de seguridad anterior, WannaCry afecta ingeniosamente a los sistemas basados en Windows más antiguos, especialmente aquellos que ya no están incluidos en los sistemas operativos compatibles de Microsoft. Los sistemas sin parches también son vulnerables a ser infectados por WannaCry (Trendmicro, 2017)

El 27 de junio de 2017 nuevamente WannaCry se propago rápidamente en todo el mundo y alcanzo su objetivo en España, Francia, Ucrania, Rusia. Este día varias empresas privadas supuestamente sufrieron un ataque de ransomware. Aunque no está claro si cada caso está conectado, al menos varios de ellos parecen estar relacionados con la misma variedad de malware. Los ataques tienen cierta semejanza con la reciente actualización de WannaCry, en el que miles de sistemas informativos fueron bloqueados con ransomware en todo el mundo. (Cox Joseph, 2017)

Mayo 2017, WannaCry o WannaCrypt atacaron a más de 230.000 ordenadores en más de 150 países, con el servicio nacional de salud del Reino Unido algunas empresas de España, entre los más afectados. Los expertos en seguridad informática de Symantec confirmaron que el ransomware en el ataque actual estaba utilizando la misma vulnerabilidad, un programa que aprovecha una vulnerabilidad software como WannaCry. Las compañías instalaron el parche para protegerse contra WannaCry, pero el ransomware de NotPetya parece tener otras dos formas de propagarse rápidamente dentro de una organización, dirigiéndose a las herramientas de administración de la red. Aún no está claro como las computadoras se infectaron con el ransomware en primer lugar, no parece ser a través de correo electrónico como sucedió con WannaCry. (Henley, Solon, 2017).

En junio del presente año NotPetya causo graves problemas en grandes empresas, entre ellas el gigante de la publicidad WPP (World Press Photo), la empresa francesa de materiales de construcción Sain-Gobain y las firmas rusas de acero y petróleo Evraz y Rosneft, La producción en la fábrica de chocolate de Cadbury en Hobart se detuvo después de que su empresa matriz se encontró envuelta en el ciber-ataque de ransomware que se ha extendido por los Estados Unidos y Europa. La firma legal DLA Piper, la gran empresa de transporte y transporte AP Moller-Maersk y Heritage Valley Health System, que administra hospitales y centros de atención en Pittsburgh.
Algunos expertos en tecnología dijeron que el ataque parece ser coherente con una “variante actualizada” del virus conocido como Petya o Petrwrap, pero los analistas de la

firma de seguridad cibernética Kaspersky Labs dijeron que habían rastreado las infecciones a “un nuevo programa de rescate que no se había visto antes”. El ataque “NotPetya” golpeo a 2.000 usuarios en Rusia, Ucrania, Polonia, Francia, Italiza, Reino Unido, Alemania y Estados Unidos. (Kaspersky, 2017).

El 27 de junio del presente año fue un día importante para el ataque cibernético que golpeo a A.P Moller-Maersk, la magnitud del daño que un virus informático puede desencadenar en la industria dependiente de la tecnología e interconectada. Alrededor del 90% del comercio mundial se transporta por mar, con buques y puertos que actúan como arterias de la economía mundial. Los puertos dependen cada vez más de los sistemas de comunicaciones para mantener las operaciones funcionando sin problemas, y cualquier fallo de TI puede crear grandes interrupciones para las complejas cadenas logísticas de suministro.

El ataque cibernético fue una de las mayores interrupciones jamás registradas en la navegación global. Varias terminales portuarias operadas por una división de Maersk, incluyendo Estados Unidos, India, España y los países Bajos, tuvieron que luchar para volver a las operaciones normales después de experimentar interrupciones masivas.

Aparte de la dependencia de los sistemas informáticos, los buques están cada vez más expuestos a la interferencia a través de dispositivos electrónicos de navegación como el Sistema de Posicionamiento Global (GPS) y carecen de los sistemas de respaldo que los aviones deben evitar los accidentes.

No hubo indicios de que el GPS y otras ayudas electrónicas de navegación se vieran afectadas por el ataque de esta semana, pero especialistas en seguridad dicen que estos sistemas son vulnerables a la pérdida de señal por interferencia deliberada de los hackers. El año pasado, Corea del Sur dijo que cientos de buques pesqueros habían regresado temprano al puerto después de que sus señales GPS estuvieran atascadas por Corea del Norte, que negó su responsabilidad. (Reuters, 2017)

Figura 11. Funcionamiento del ransomware (Black, 2016)

4. METODOLOGÍA

Para cumplir con el objetivo de la presente investigación, proponer buenas prácticas para mitigar el ataque por el ransomware criptográfico, se desarrolló cada una de las metas propuestas.

4.1. Etapas de la metodología

Etapa 1: se realizó un estado del arte, la cual se hizo por medio de los siguientes pasos: lo primero que se hizo fue la recopilación de la información donde se obtuvieron 159 artículos de revistas científicas, base de datos y Google académico. En el segundo paso se hizo la evaluación de los datos y análisis de los mismo donde se clasificaron 106 artículos de base de datos como IEEE Explore, Science Direct, arxiv.org, se calificaron pertinentes para esta investigación. Estos artículos sirvieron de apoyo para realizar el marco conceptual, el que se puede encontrar en el capítulo 2 y el estado del arte que se puede observar en el capítulo 3.

Etapa 2: se hizo la clasificación de los diferentes tipos de ransomware o mutaciones, el cual se elaboró con los siguientes pasos:

En el primer paso se hizo la clasificación de los diferentes tipos de ransomware existente los cuales se tomaron de acuerdo con la información administrada en el estado del arte. En el segundo paso los ransomware fueron categorizados como los malware que representan mayor riesgo. Los cuales se puede encontrar en este capítulo en el ítem 4.1

Etapa 3: se realizó un top 10 de ransomware de mayor afectación, el cual se realizó por medio de los siguientes pasos:

En el primer paso se clasifico los ransomware de mayor a menor riesgo en el top 10, donde se encuentra almacenado el nivel de afectación y forma de afectación. El cual se puede observar en este capítulo en el numeral 4.2.

En el segundo paso se realizó un estudio de la forma como estos malware afectan a los usuarios y se buscaron posibles soluciones de alguno de estos tipos de ransomware, las cuales se encuentran en las siguientes tablas: en la tabla 7 se comprobó que por medio extractor Petya no se puede eliminar este malware porque al momento de ingresar a la página no carga el debido contenido. En la imagen 12 se intentó eliminar el Petya por medio de la clave que lanzaron los creadores Janus Cybercrime Solutions, pero como se observa al momento de ingresar dicha clave indica que esta clave es errada. En la tabla 9 se muestra que por medio del software ID Ransomware no se encontró algún software que pueda recuperar los archivos encriptados con Wanna decryptor. En la tabla 10 se intenta eliminar el ransomware por medio del software Software Spyhunter, pero como se puede evidenciar este no fue posible eliminarlo porque pide que se debe registrar el cual no fue posible hacer dicho registro porque para ello pide un costo adicional y el proyecto no cuenta con recursos para esta inversión. En la tabla 11 se intentó eliminar el malware con el programa Software Spyware Terminator y no fue posible eliminar como se observa en la tabla ya que no reconoce el malware. En la tabla 12 se intenta eliminar el malware wanna decryptor por

medio de restauración de sistema, pero como se ve en la tabla este no elimina por medio de este procedimiento. En la tabla 13 se intenta desencriptar los archivos por fuerza bruta con la aplicación con john the Ripper pero como se evidencia en la tabla no fue posible hacerlo. En la tabla 14 se intenta desencriptar los archivos por fuerza bruta con la aplicación con Jhonny pero como se evidencia en la tabla no fue posible hacerlo.

Etapa 4: se realizó el proceso de la creación de las buenas prácticas que el usuario debe tener con respecto al malware ransomware.
Ya cumplidas las etapas 1, 2 y 3 se procede a realizar la creación de las buenas práctica las que se pueden encontrar en el capítulo 5, allí puede encontrar algunas pautas o pasos para evitar ser infectado por algún tipo de ransomware o si fue infectado por algún tipo de ransomware que se debe hacer y por último lo que se recomienda hacer en caso de que se vea infectado por los ransomware Petya y Wanna decryptor, que son en la actualidad los más populares.

4.2. Clasificación de Ransomware

Los ciberdelincuentes han optado por varias técnicas para poder lucrase de la información del usuario, pero una de las más actuales y peligrosas es la infección a dispositivos por medio de ransomware criptográfico, este malware cuenta con varios tipos de encriptadores, que pueden funcionar de forma diferente, pero tienen la misma finalidad que es pedir un rescate para poder recuperar dicha información. En la siguiente tabla se puede observar los ransomware más perjudiciales hasta el momento, esta clasificación se hizo según la información obtenida en el desarrollo del estado del arte, la cual está organizada de acuerdo con la fecha en que surgió y de acuerdo con el nivel de búsqueda que se encuentra en Google Trends.

TABLA 2 Tipos de Ransomware Criptográfico

NOMBRE	DEFINICIÓN	CARACTERÍSTICAS	AÑO EN QUE SURGIÓ	TIPO DE ALGORITMO	MEDIO DE PROPAGACIÓN
Zeus	Este malware fue diseñado para robar información de los ordenadores	Se propaga por medio de correo electrónico con adjuntos haciéndose pasar por organizaciones como fdic, irs, myspace, facebook o Microsoft	2007	P2P	Se distribuye por medio de Correo electrónico spam En coche de descargas

		Unas de sus funciones es infectar con otros ransomware			
CryptoDefense	cifrar los archivos que se encuentran almacenados en el pc	se expande por medio de campañas electrónicas Usa el algoritmo RSA 2984 para cifrar los archivos.	2014	RSA-2048	expande por medio de Correo electrónico de phishing
TorrentLocker	Este malware ataca directamente los archivos del usuario	Se propaga por medio de correo electrónico span Se hace pasar por empresas postales o filiares de internet.	2014	AES-256-CBC	Este usa Mensajes de correo electrónico para expandirse
SimpleLocker	infecta los archivos que se encuentran almacenados en los dispositivos móviles y tablas que tienen como sistema operativo Android	El mensaje de extorción está Escrito en ruso y el pago debe hacerse en moneda ucrania. toma la información del teléfono como IMEI, sistema operativo Escanea la tarjeta SD	2014	AES 256	Se propaga por navegación insegura, archivos adjuntos corruptos, drive-by downloads, aplicaciones maliciosas, etc.
Bandarchor	Malware que cifra los archivos de tu ordenador	la cantidad de bytes cifrada por archivo es de 16.000	2014	AES-256	Se propaga por medio de correo electrónico o
Citroni	encripta los archivos,	Este malware también cobraba en bitcoin, pero solo da plazo de 3 días Se comunica por medio del servidor Tor	2014	Cifrado de curva elíptica	Se propaga por correo electrónico

		Los archivos se encriptan con la extensión. CTBL			
Virlock	encripta los archivos.	infecta archivos binarios	2014	XOR	Se propaga a travez de la red, a través de almacenamiento en la nube
Lockscreen	Este malware bloquea la pantalla de tu dispositivo donde hace el celular inaccesible hasta que se pague el rescate	Este malware exige un pago para darle la clave que desbloquea al dispositivo	2014	AES	Descarga de programas que no vienen de Play Store
Cryptolocker y Cryptowall	Estos malware lo que hace es cifrar tus archivos, haciendo que estos se vean en cuarentena, luego como todos los ransomware pide un rescate para recuperarlos.	Estos ransomware generan una clave privada y una única de 448 bits. cifra el servidos C&C con el algoritmo RSA DE 1024 o 2984 bits para así evitar que la clave sea recuperad	2015	RSA-2048	Este malware infecta al equipo por medio de un correo electrónico adjunto. Por el puerto remoto 3389.
TeslaCrypt	Encripta los videos juegos que se encuentran almacenados en el dispositivo	Este malware encripta fotos, videos, imágenes y archivos de juegos.	2015	Cifrado asimétrico RSA-2048 cifrado de curva elíptica	Se propaga por medio del correo electrónico
Tox	cifra y bloquea los archivos con la extensión Jigsaw, y va eliminando periódicamente los archivos de su ordenador	Modifica la página de inicio del sistema Cambia la configuración del navegador Generación masiva de pop-up, con el fin de afectar la rapidez	2015	AES	Este malware se expande por medio del correo electrónico. Descargar ficheros de redes P2P

		y rendimiento del navegador			
CryptoFortress	cifra los archivos de tu equipo	Usa la librería Microsoft cryptoapy direccionamiento. onion Llave de cifrado RSA-1024	2015	AES-256 ECB	se propaga por medio de Exploit kit
Chimera	cifra los archivos locales y los de red	Los correos infectados tienen como adjunto ofertas de empleo entre otros. Cambia la extensión de los archivos a nombre. Crypt	2015	AES	Se distribuye por medio de correo electrónico maliciosos en campaña de phishing
Radamant	cifra los archivos de la víctima y los cambia a extensión RMD.	puede infectar a todas las versiones de Windows	2015	AES-256	Este se propaga por medio de métodos de infecciones troyanas
Petya	Encripta el disco duro por completo evitando así entrar al sistema operativo y para poder recuperar los archivos exige un pago	Modifica el gestor de arranque donde sustituye el sistema operativo por el malware Petya	2016	RSA 4096 algoritmo de bits y AES 256	Correo electrónico
Kimcilware	Este malware se encarga de cifrar los datos de los servidores web	Este malware añade su propia extensión. Kimcliware Secuestro de los servidores de diferentes tiendas online en Magento. Dícese de la plataforma de comercio en línea.	2016	AES	Se expande por medio de Correo electrónico de spam. Descargando programas de software en página web sin verificar.

DMA Locker	Cifran datos en unidades de red, incluso cuando éstas no están almacenadas en una red de acceso local.	Este malware cuando afecta el sistema muestra una pantalla de color rojo en dos versiones de lenguaje polaca o ingles	2016	AES y RSA	Se Propaga por medio de correo electrónico Se adjuntos Redes P2P, por falsas actualizaciones de software
Locky	Este Ransomware cifra los archivos con la extensión. Locky	Encripta los archivos con extensión. locky Instala .bmp y txt Puede cifrar archivos de red	2016	AES-1024	Este se propaga por medio de Recibirá un correo electrónico con un documento adjunto (Troj / Docdl-BCF). Por medio de macros
Cerber	Este malware lo que consiste es cifrar los archivos del usuario.	Crea 3 tipos de archivo diferentes (#decrypt my files#.txt, #decrypt my files#.html, #decrypt my files#.vbs)	2016	RSA y cifrado RC4	adjuntos de email maliciosos, redes P2P
Maktub	comprime los archivos antes de cifrarlos.	el creador de este malware al inicio de la infección pide un valor y a medida que transcurre el tiempo lo aumenta. Los correos electrónicos tienen como adjunto las extensiones PDF o TXT	2016	AES de 256 bits	Se propaga por medio de correo electrónico

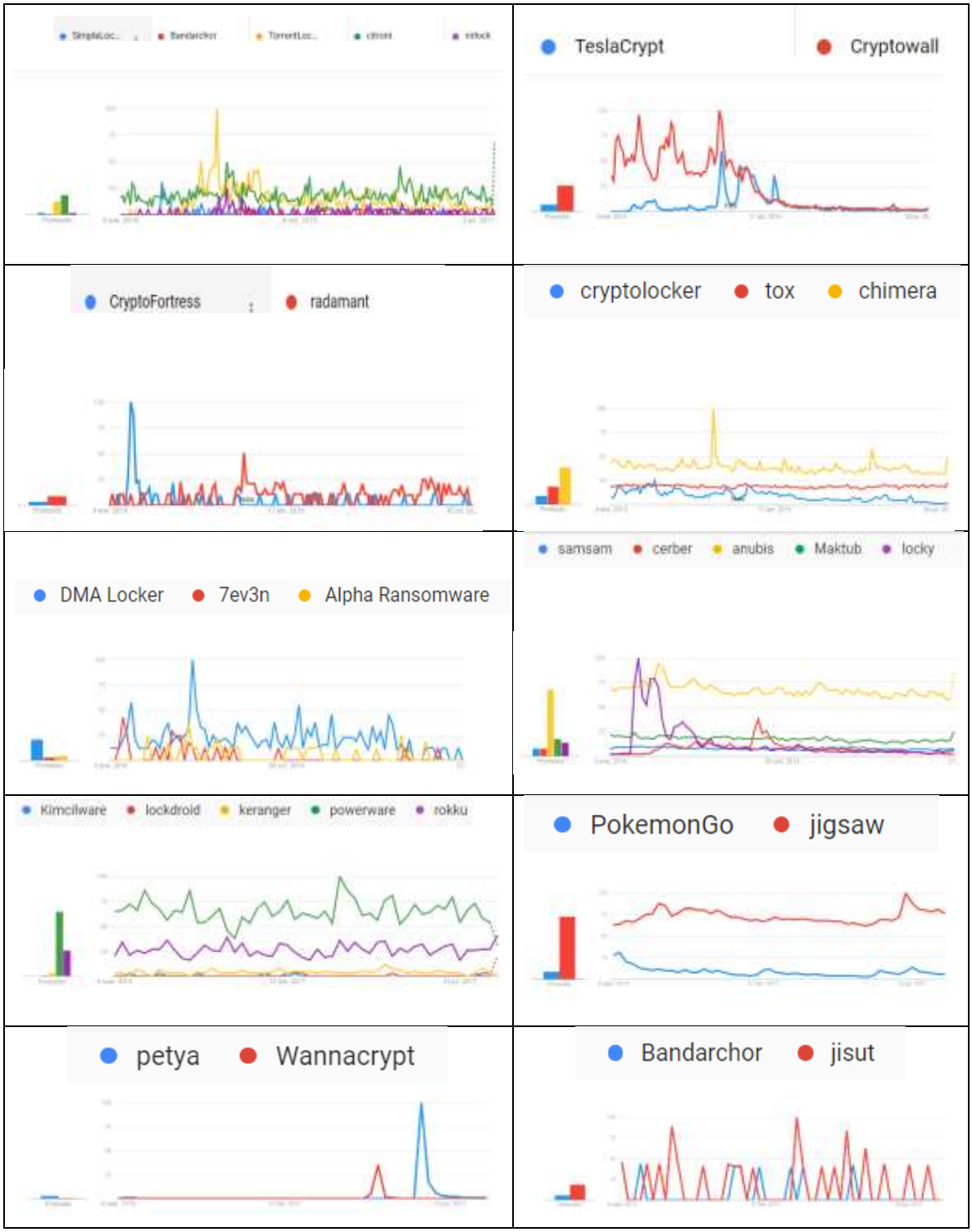
		cambia la extensión de los archivos a. IAALIXR			
PokemonGo	Este malware invade los ordenadores y cambia las claves de registro de Windows	crea cuentas de usuarios con el nombre Hack3r. Añade una extensión. Lockey	2016	AES-256	Este se propaga por medio de un archivo ejecutable llamado pokemonGo.exe
7ev3n	cifra los archivos con la extensión. R5A	Cifra los archivos con la extensión R5A Este malware se instala en la carpeta % LOCALAPPDATA%	2016	R5A	Se propaga por medio de correo electrónico
Alpha Ransomware	encripta sus archivos	El pago que exige este ransomware también es con tarjeta de regalo en este caso iTunes	2016	AES (128)	Se propaga a través de archivos adjunto de correo electrónico
Anubis	Este ransomware cifra el contenido de tus archivos	Estos malware para recuperar la información exigen un pago de 2.5 y 3 bitcoin codifica la mayoría de los contenedores de datos. Utiliza la extensión. Coded	2016	AES-256	Se propaga por medio de correo electrónico
Samsam	que cifra los archivos de los usuarios.	Este malware es capaz de infectar toda la red.	2016	RSA	Correo electrónico de spam
Lockdroid	Este malware afecta a los usuarios que utilizan dispositivos móviles, este se encarga de Cifra los archivos y	después de infectar su dispositivo muestra un mensaje en pop ups solicitando el pago para recuperar los archivos	2016	AES	Este malware se instala al momento de instalar cual quiera aplicación que no sea de Google Play

	recopila la lista de contactos				
Keranger	cifra los archivos de los ordenadores que tienen sistema operativo de Apple Mac Os X	Después que este malware se instala este hace una conexión con el servidor remoto en la red Tor. Este genera una clave después que se instala para así tomar control del dispositivo	2016	AES	Se propaga mediante una versión infectada de una aplicación de BitTorrent legítima de código abierto
Powerware	cifra los archivos a través de Microsoft Word y PowerShell.PowerShell	Después de infectada este intenta evitar que se instalen nuevos archivos en el disco	2016	AES	Se propaga a través de correo electrónico
Jigsaw	cifra tus archivos y si no pagas en el tiempo establecido elimina todos los archivos	Este malware cada 60 minutos elimina archivos de tu pc	2016	AES	Correo adjunto de correo spam
Rokku	cifra todas la imágenes y documentos en su disco duro	Apenas infecta el equipo este malware elimina todas las copias de seguridad. El desarrollador permite que el usuario selección su idioma	2016	RSA-512	Este malware se transmite a través de correo electrónico
Wannacrypt	cifra los archivos y los pone extensión. wnry, .wcry, .wncry y .wncrypt.	afecta principalmente a los sistemas operativos de Windows Crea una clave aleatoria. Cifra el fichero copiado utilizando el algoritmo AES	2017	AES-RSA	Este se propaga por medio del puerto 445(SMB) Correo electrónico o spear phishing,

		Añade una cabecera con la clave AES cifrada con la clave pública RSA que lleva la muestra Sobrescribe el fichero original con la copia cifrada Finalmente renombra el fichero original con la extensión. Wnry			
NotPetyta	encripta todo el disco duro dejando al usuario sin poder acceder al sistema	Encripta principalmente los archivos que tienen como extensión lenguaje de programación No encripta archivos como PNG.	2017	RSA	se propaga a través de exploit EternalBlu y EternalRomance
Jisut	se encarga de cifrar los archivos de los usuarios que utilizan Smartphone con sistema operativo Android, una vez infectados este malware realiza la extorsión por medio de llamadas de voz.	tiene la capacidad realizar las extorsiones por medio de llamadas de voz. Este malware propaga a través de un dropper malicioso que se usa para descifrar y ejecutar el playload	2017	AES	se propaga a través dropper

(Fuente propia, 2017).

Tabla 3 comparaciones de los ransomware en Google Trends



(Fuente propia, 2017).

4.2.1. Análisis de las comparaciones de los Ransomware

A continuación, se hace un análisis de las gráficas que se encuentran en la tabla 3, las cuales fueron tomadas de Google Trends.

- En fila 1 columna 1 de la tabla 3, se compararon los ransomware SimpleLocker, Bandarchor, TorrentLocker, Citroni y Virlock desde que surgieron estos malware que fue en el año 2014, según el nivel de búsqueda que se muestra en Google Trends se puede observar entre los 5 tipos de ransomware quien tuvo un mayor nivel de búsqueda o mejor promedio fue Citroni, en el periodo del 14 al 20 de diciembre del 2014 TorrentLocker obtuvo el mayor nivel de búsqueda que fue de 100% y Citroni solo obtuvo el 20%, el 27 de agosto del presente año se puede observar que citroni vuelve y toma un nivel de búsqueda superior a los anteriores con un 70%, mientras que los otros se muestran en cero.

- En la fila 1 columna 2 de la tabla 3, se hizo un análisis de los ransom que surgieron en el año 2015, como lo son TeslaCrypt, Cryptowall, al momento de hacer la comparación en Google Trendes, de acuerdo con su fecha de creación y hasta el

- momento se puede ver quien tuvo un mayor promedio de búsqueda en todo el recorrido fue Cryptowall con un 26% a diferencia de TeslaCrypt que solo obtuvo el 7%, en el intervalo de tiempo entre el 24 de marzo y 4 de abril Cryptowall tuvo un mayor nivel de búsqueda con un 96% a diferencia de TeslaCrypt que solo obtuvo un 4%, se puede observar en todo el trayecto de búsqueda que Cryptowall siembre obtuvo mayor nivel de búsqueda que el malaware TeslaCrypt, en el único intervalo de tiempo que tuvieron un nivel de búsqueda similar fue entre el 6 al 12 de diciembre del 2015 que Cryptowall con 90% y TeslaCrypt 60%, en el intervalo de tiempo del 20 de agosto al 27 de agosto tuvieron un nivel de búsqueda muy similar pero con muy pocos porcentaje de búsqueda, con una diferencia de un dato mayor que otro.

- En la fila 2 columna 1 de la tabla 3, Los ransomware CryptoFortress y Radamant también surgieron en el año 2015 según el nivel de búsqueda que muestra en las gráficas de Google Trends el que tuvo mejor promedio de búsqueda fue Radamant con un 9% durante todo el trayecto a diferencia de CryptoFortress que solo obtuvo un 4%,en el intervalo de tiempo del 1 al 7 mayo del 2015 CryptoFortress tuvo el mayor nivel de búsqueda que fue de 100% a diferencia de Radamant que obtuvo 11%, como se puede observar y de acuerdo al promedio de búsqueda Radamant obtuvo mejor promedio de búsqueda, en los intervalos de tiempo desde el 20 al 26

de agosto no se presentaron ningún tipo de búsqueda de ninguno de los dos malware.

- En la fila 2 columna 2 de la tabla 3 se hizo la comparación de los ransomware Cryptolocker, Tox y Chimera, se puede analizar que el que obtuvo mayor promedio de búsqueda fue el ransomware Chimera con un nivel de búsqueda del 39% a diferencia de los otros dos malware, Tox con 19% y Cryptolocker un 9%, Chimera en todo el trayecto de búsqueda fue el que mayor nivel de búsqueda obtuvo, en el intervalo de tiempo del 25 al 31 de octubre del año 2015 Chimera obtuvo el mayor nivel de búsqueda que fue el 100% a diferencia de Tox que consiguió el 8% y Cryptolocker 12%, hasta la fecha se puede observar que Chimera siembre fue el más buscado a diferencia de los otros dos malware.

- En la fila 3 columna 1 de la tabla 3 se analizaron los ramsomware DMA Locker, 7ev3n y Alpha Ransomware, estos malware surgieron en el año 2016, se pudo verificar el que el Ransom que obtuvo mayor promedio de búsqueda es DMA Locker con un porcentaje del 21% a diferencia de Alpha Ransomware que obtuvo un 5% y 7ev3n 3%, DMA Locker fue el malware que mayor nivel de búsqueda obtuvo en todo trayecto desde que surgió hasta la fecha, en el intervalo de tiempo del 22 al 28 de mayo del 2016 fue donde este malware DMA Locker, obtuvo el mayor nivel de búsqueda que fue de un 100% a diferencia de 7ev3n que obtuvo un 13% y Alpha Ransomware un 12%, finalmente se observa en la gráfica que a la fecha del 27 de agosto de 2017 los niveles de búsqueda de estos malware disminuyeron significativamente a diferencia de los otros intervalos de tiempo, dejando a DMA Locker con un nivel de búsqueda de 12% , 7ev3n 0% y Alpha Ransomware 0%.

- En la fila 3 columna 2 de la tabla 3 se analizaron los malware Samsam, Cerber, Anubis, Maktub y Locky, se puede observar que le malware que obtuvo un mayor promedio de búsqueda fue Anubis con un 68% a diferencia de Samsam 8%, Cerber 8%, Maktub 18% y Locky 14%. Según la gráfica se puede analizar que Anubis obtuvo mejor promedio de búsqueda, porque en todos los intervalos nunca obtuvo un nivel de búsqueda en cero, es decir en todo el trayecto desde que surgió hasta la fecha han realizado búsquedas de este malware, en el intervalo de tiempo entre el 21 al 27 de febrero del 2016 se observa que Locky obtuve un mayor nivel de búsqueda que todos los demás fue un 100% a diferencia de Samsam 10%, Cerber 2%, Anubis 70% Madtub 19%.

- En la fila 4 columna 1 de la tabla 3 se analizaron los ramsonwares Kimcilware, Lockdroid, Keranger, Powerware y Rokku y se verifico que el que obtuvo mayor promedio de búsqueda fue el Powerware con 65% a diferencia de Rokku con un

26%, Keranger 4% y Lockdroid 1% y Kimcilware con un 0% es decir que este último malware en toda la trayectoria de búsqueda fue el que menor búsqueda tuvo, desde la trayectoria de búsqueda es decir desde que surgieron estos malware en el año 2016 Powerware siempre obtuvo mayor nivel de búsqueda que los otros 3 malware a excepción del 27 al 29 de agosto del 2017 Rokku tiene mayor nivel de búsqueda con un 41% a diferencia de Powerware que obtuvo un 31%.

- En la fila 4 columna 2 de la tabla 3 se analizaron los malware PokemonGo y Jigsaw que también surgieron en el año 2016 de esta grafica se puede analizar que el malware obtuvo mayor promedio fue Jigsaw con un 73% a diferencia de PokemonGo que obtuvo un 9%, en el intervalo de tiempo del 16 al 22 de julio del año 2017 Jigsaw obtuvo el mayor intervalo de búsqueda que fue un 100% a diferencia de PokemonGo que obtuvo un 9%, a la fecha de hoy 29 de agosto de 2017 Jigsaw obtuvo siempre el mayor nivel de búsqueda.

- En la fila 5 columna 1 de la tabla 3 se analizaron los malware Petya y Wannadecrypt, en el que se analiza que el que obtuvo mayor nivel de búsqueda fue el Petya con un 3% a diferencia de Wannadecrypt que obtuvo un 1%, Petya siempre obtuvo mejor nivel de búsqueda, excepto en el intervalo de tiempo del 14 al 20 mayo que Wannadecrypt obtuvo un mayor nivel de búsqueda de 35% a diferencia de Petya que obtuvo un 0%, pero del 25 de junio al 1 de julio Petya volvió a subir su nivel de búsqueda con un 100% y Wannadecrypt no hicieron ningún tipo de búsqueda en esa fecha, al día de hoy 29 de agosto del 2017 se observa que el nivel de búsqueda ha disminuido en los dos malware.

- En la fila 5 columna 2 de la tabla 3 se analizaron los malware Bandarchor y Jisut el cual se puede observar y analizar de la gráfica que el que obtuvo mayor promedio de búsqueda fue Jisut con un 19% a diferencia de Bandarchor con un 6%, en el trayecto de la búsqueda se puede observar que Jisut siembre obtuvo más nivel de búsqueda que Bandarchor como lo indica el promedio, a la fecha 29 de agosto del 2017 ninguno de los dos malware obtuvo búsquedas.

4.3. Ransomware de Mayor a Menor Riesgo de Afectación

La siguiente clasificación se sacó de acuerdo con el nivel de afectación que se tienen cuando se infecta el computador, es decir cuando el malware cifra todo el disco duro, en este caso es un malware más importante que cuando solo cifra los archivos, porque cuando el malware infecta todo el disco duro es imposible acceder a la información que se encuentra almacenada en ella y se hace más complicado recuperar la información, además basándonos al tipo de algoritmo o cifrado que utiliza para encriptar los archivos si es RSA Y AES es un tipo de algoritmos más complicados de descifrar como se puede observar en el capítulo 2 donde encontramos la definición de estos tipos de cifrado. Y por último de

acuerdo con las estadísticas del nivel de búsqueda que se muestran en Google Trends. Ya después clasificados los malware del Top 10 se organizaron de acuerdo con el total de daños reportados en orden de importancia. Para este top 10 también se tuvo en cuenta la clasificación que realizo Bisson en el año 2016, la cual la hizo de acuerdo con nivel de daño que estos causaron en el año 2016, por ello la llamo las principales tensiones del ransomware en el año 2016.

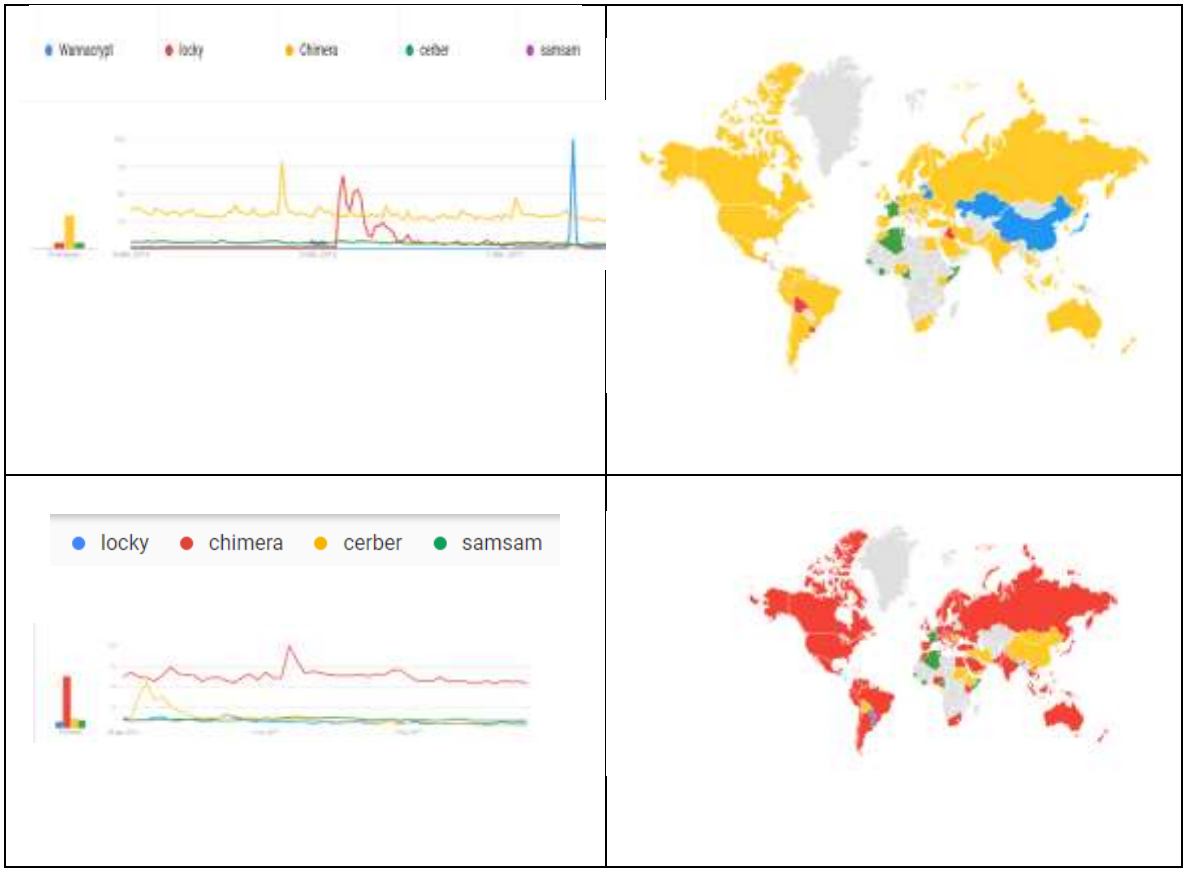
Tabla 4 Clasificación de los Ransomware de Mayor A Menor Riesgo

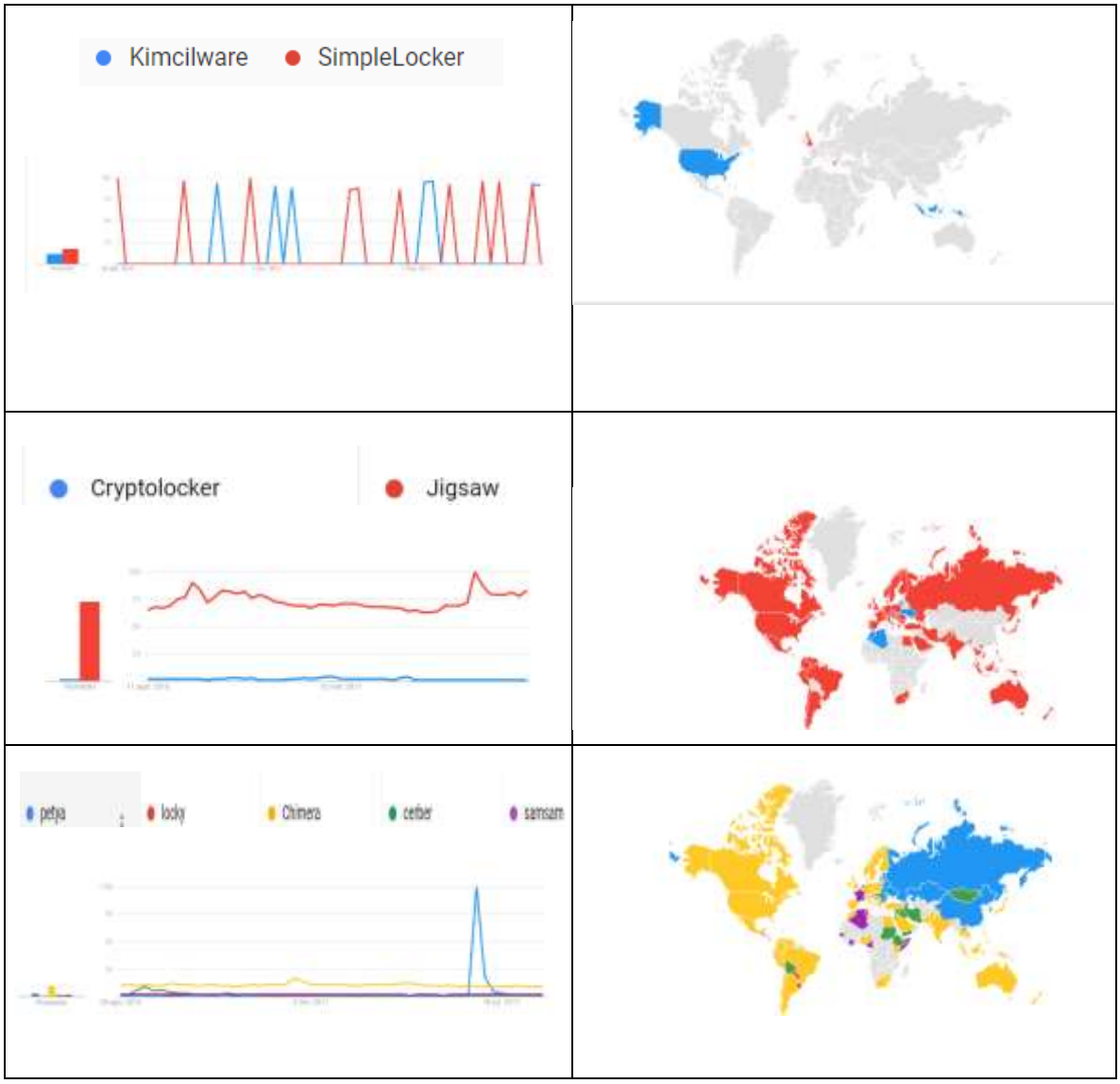
NOMBRE	DEFINICIÓN	AÑO EN QUE SURGIÓ	Tipo de algoritmo	DAÑOS REPORTADOS
1. Wannacrypt	cifra los archivos y el disco duro evitando que las personas accedan a la información que se encuentra en el computador	2017	AES-RSA	200.000 mil computadores en 150 países aproximadamente
2. Petya	encriptar archivos con extensiones de lenguaje de programación o en su defecto encripta todo el disco duro	2017	RSA	2.000 mil computadores en los países Italia, Alemania, el Reino Unido y los Estados Unidos aproximadamente.
3. Cryptolocker	Estos malware lo que hace es cifrar tus archivos, haciendo que estos se vean como cuarentena, luego como todos los ransomware pide un rescate para recuperarlos	2015	RSA-2048	Más de 500 computadores aproximadamente
4. Locky	Encripta los archivos que se encuentran almacenados en el computado	2016	AES-1024	114 Países
5. Jigsaw	cifrar los archivos, y si no se paga en el tiempo establecido los elimina	2016	AES	Más de 100 archivos eliminados aproximadamente
6. Kimcilware	cifra los datos de los servidores web	2016	AES	10 tiendas afectadas aproximadamente

7. Cerber	Este malware se encarga de cifra los archivos	2016	RSA	24,17 usuarios, afectados de Windows aproximadamente
8. Samsam	cifra los archivos de los usuarios	2016	RSA	70.000 USD pagos en bitcoin
9. SimpleLocker	se encarga de cifrar los archivos de telefonía con sistema operativo Android	2014	AES 256	No se encontró registro
10. Chimera	cifra los archivos de red local	2015	AES	No se encontró información

Fuente propia (2017).

Tabla 5 Nivel de búsqueda de interés a lo largo del tiempo por Google Trends





Fuente Propia (2017)

4.3.1. Análisis de comparación de los ransomware de top 10.

A continuación, se realiza el análisis de las gráficas de la la tabla 5 obtenidas a partir de la búsqueda realiza en Google Trend:

- En la fila 1 columna 1 de la tabla 5 se analizaron los ransom Wannacrypt, Locky, Chimera y Samsam, se puede analizar que Chimera obtuvo el mayor promedio de búsqueda con un 31% a diferencia de Wannacrypt que solo obtuvo un 1%, Locky un 6% y Samsam un 6%, se puede observar que Chimera siempre obtuvo un mayor nivel de búsqueda, a excepción del intervalo de tiempo del 14 al 20 de mayo del 2017 que Wannacrypt obtuvo el mayor nivel de búsqueda que fue el 100%, a diferencia de Chimera que obtuvo el 29%, Locky un 4%, igual que Samsam con un 4%. A la fecha

se observa que Chimera sigue siendo el malware más buscado con un 26%. Del mapa se puede observar que según la búsqueda por regiones el ransom que se buscó más en los países como estados unidos, Canadá, México, Brasil, Argentina, Colombia Venezuela, Perú etc. Fue el chimera que es el que está de color amarillo, Lo que quiere decir que en estos países fue donde pudo causar mayor impacto, en el caso contrario de Wannadecrypt que causo más impacto en los países como China, Kazajistan etc. Como conclusión el ransomware Chimera fue el más buscado en las diferentes regiones del mundo.

- En la fila 2 columna 2 se analizaron los malware Locky, Chimera, Cerber y Samsam, se puede verificar que Chimera fue el ransom que obtuvo mayor promedio de búsqueda con un 63%, a diferencia de Cerber que obtuvo un 12%, Samsam 10% y Locky 8%, chimera en el intervalo de tiempo que mayor porcentaje de búsqueda obtuvo fue entre el 22 al 28 de enero del 2017 que fue de un 100% a diferencia de Samsam que obtuvo un 13%, Cerber 11% y Locky 8%. A la fecha de hoy 30 de agosto del 2017 a comparación de los otros malware ya mencionados sigue teniendo un mayor nivel de búsqueda con un porcentaje de 54%. Del mapa se puede deducir que el interés de búsqueda por región de mayor interés fue Chimera, que es el color rojo es el que se encuentra más distribuido en todas las regiones como lo dicen las estadísticas anteriores.

  En la fila 3 columna 3 de la tabla 5 se analizaron los ransom Kimcilware y SimpleLocker de acuerdo al análisis se observa que SimpleLocker obtuvo mejor promedio de búsqueda con un 18% a diferencia de Kimcilware con un 12%, las gráficas nos muestra que SimpleLocker obtuvo mayor nivel de búsqueda, en el intervalo de tiempo del 28 de agosto al 3 de septiembre del 2016 SimpleLocker obtuvo un 100% de búsqueda y Kimcliware no tuvo búsquedas, pero el intervalo de tiempo del 20 al 26 de agosto Kimcliware obtuvo 91% y simplocker no tuvo búsquedas, delo que se puede deducir que aunque Simplelocker fue el el que obtuvo mayor nivel de búsqueda tuvo intervalos de tiempo donde no se hiceireon busquedas. Según el análisis que se saca del mapa de la búsqueda por regiones, se muestra que ocurrió todo lo contrario a la gráfica analizada anteriormente, porque en este mapa se observa que obtuvo mejor búsqueda Kimcilware que son las zonas en color azul.

- En la fila 4 columna 4 se analizaron los malware Cryptolocker, Jigsaw, el que obtuvo mejor promedio de búsqueda fue Jigsaw con un 73% a diferencia de Cryptolocker con un 2%, en todo el trayecto de búsqueda se observa que el Jigsaw siempre estuvo por encima del otro malware, ya que el porcentaje de búsqueda del ransom Cryptolocker el máximo fue de un 4% en todo el trayecto a diferencia de Jigsaw que si obtuvo el mayor promedio de 100%. Del mapa se puede analizar que según la

búsqueda por regiones si coincide con la gráfica anteriormente analizada, porque se puede evidenciar que las regiones hay más zonas rojas que es el malware Jigsaw.

- En la fila 5 columna 5 se puede observar que de los malware analizados Chimera obtuvo mejor promedio de búsqueda con un 11% a diferencia de los otros malware que obtuvieron un promedio no mayor a 2%, se observa en todo el trayecto de búsqueda de estos malware, que Chimera fue el más buscado, pero nunca obtuvo un nivel del 100%, como si lo hizo Petya en el intervalo de tiempo del 25 de junio al 1 de julio si obtuvo un nivel de búsqueda del 100%. Del mapa se puede se observa que, en Rusia, China etc. Petya fue el ransom más buscado a diferencia de Canadá, México, Brasil, Colombia etc., donde Chimera fue el malware más buscado.

4.4. Prácticas de ilustración de infestación con ransomware

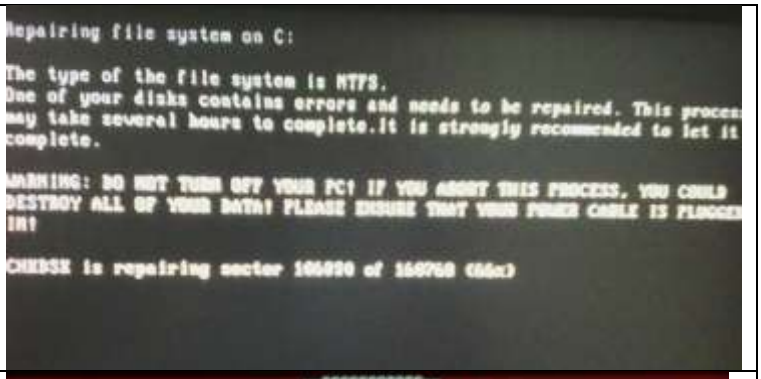
A Continuación, se muestran algunos ejemplos de los ransomware que se clasificaron en el top 10. Estos malware fueron los únicos que se pudieron descargar de la página de internet para hacer las pruebas, ya que como son virus, es muy difícil encontrar el ejecutable en la web.

4.4.1. Ransomware Petya 1.0

Este malware se descargó a través del enlace https://mega.nz/#!doqgxb4c!rbu9ho3baf ohcilgck1f1bcrt-bicfjf6jw5vyuhvu, este es la versión 1.0 de Petya fue proporciona un block de YouTube llamado Ender's Show.

TABLA 6 Ransomware Petya

Cuando este malware entra al equipo lo primero que muestra es una pantalla azul indicando que hay una falla con el sistema operativo	

Después de reiniciarse el equipo muestra esta pantalla donde indica que se está reparando el sistema operativo, supuestamente.	
Después que termina de reparar el sistema operativo, es decir carga hasta el 100%, es cuando se observa que el disco duro ha sido encriptado por el ransomware Petya, muestra una pantalla roja con una imagen de calavera donde indica que se debe presione cualquier tecla	
Después que se presiona la tecla, sale otra pantalla donde indican que el ordenador fue encriptado por el ransomware Petya, el disco duro ha sido encriptado de grado militar. No existe manera de recuperar el acceso sin la clave principal, también indica unas URL donde se debe ingresar para obtener y comprar la clave, si no se compra esta clave, no es posible recuperar los archivos de ninguna otra forma.	

Si se ingresa una clave que no es la correcta o presionar enter de inmediato le indica que esa no es la clave.	

(Fuente propia, 2017)

4.4.2. Prácticas de ilustración para eliminar Petya

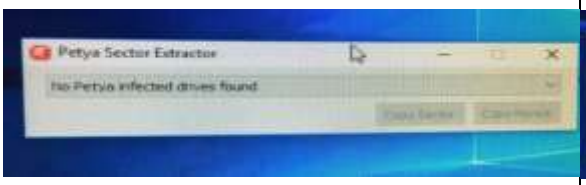
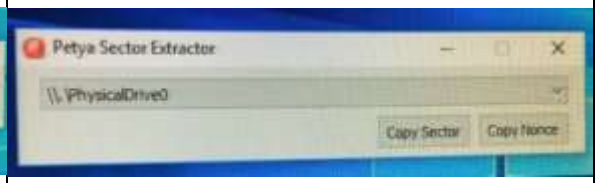
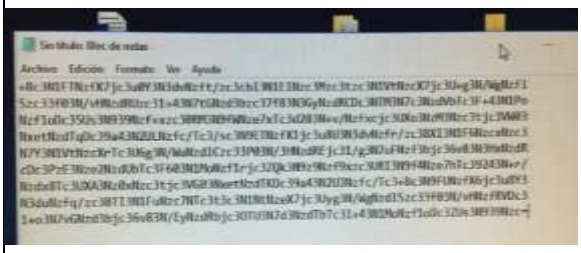
A continuación, se describen algunas prácticas que se encontraron en algunas páginas de internet donde indican que es posible eliminar el ransomware.

Eliminar Petya por la opción modo seguro

Hay páginas de internet donde dicen que hay manera de quitar el virus de Petya ingresando al computador por la opción modo seguro con F8 (esto solo es funcional para los sistemas operativos hasta la versión Windows 7), luego se busca panel de control, programas y por último se busca el programa en este caso Petya y se desinstala. Pero esta práctica no es correcta porque al momento de intentar ingresar al sistema operativo después que el disco duro se encuentra afectado por este malware no es posible ingresar a la opción modo seguro porque este virus encripta toda la parte de MBR(Master Boot Record) es la que se encarga del arranque del sistema, evitando así ingresar a esta opción por medio de la tecla F8,en cuanto a las otras versiones más actuales de este sistema operativo (Windows 8, 8.1 Y 10), tampoco es posible ingresar a la opción de modo seguro con la tecla F8 porque Microsoft desactivo esta opción, y se debe hacer con el sistema operativo funcionando, pero no es posible hacerlo porque como se mencionó anteriormente el Petya encripta todo el sistema de arranque evitando así ingresar al sistema operativo.

En unos de los block de Kaspersky también informan que este programa Petya extractor acompañado de esta página https://petya-pay-no-ransom.herokuapp.com/, permite encontrar la clave que descifrara todas las unidades de disco duro que se encuentran afectadas, pero al ingresar a la página y descargar el software, este programa muestra que alguna unidad del disco duro se encuentra afectada, se procede a copiar el código que da para ingresarlo a la página que va generar la clave, pero es allí donde termina el proceso porque no es posible ingresar dicho código, dado que en la página no se encuentra en donde ingresarlo. En esta investigación, esta página se abrió con diferentes navegadores y en ninguno aparece una caja de texto o elemento para ingresar dicho código.

Tabla 7 Programa Petya Extractor

 Este es el programa Petya sector extractor, aquí está mostrando que ninguna unidad del disco duro se encuentra afectado.	 después se conecta el disco duro afectado a otro pc que no esté afectado y se ejecuta el programa y se muestra que alguna unidad está afectada.
 Este es el código que se genera al darle al botón copy sector y es el que se debe copiar en esta página de internet https://petya-pay-no-ransom.herokuapp.com/.	 Esta es la página donde se debe ingresar el código anterior pero como se puede observar no hay en donde ingresar el código, por tal motivo no es posible verificar si esta herramienta si es funcional para desencriptar el disco.
 Esta es la página según los autores del block que debe salir para ingresar el código, pero como se mencionó anteriormente no sale con esta presentación.	

Fuente propia (2017)

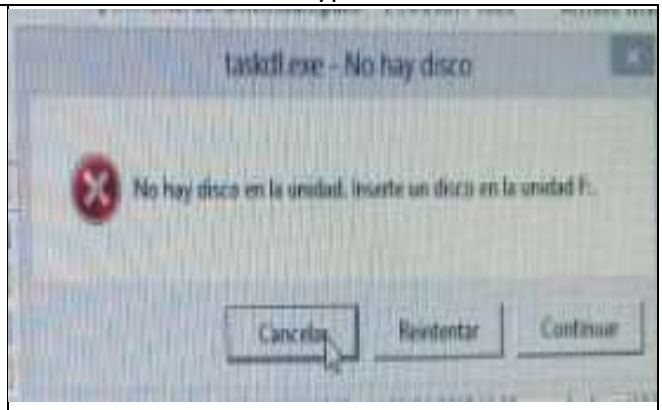
Arteaga (2017) informa en un artículo, que el autor del ransomware Petya original, que es una persona o grupo que se hace llamar Janus Cybercrime Solutions, ha hecho pública la clave de descifrado de todas las versiones pasadas de su software malicioso 38dd46801ce61883433048d6d8c6ab8be18654a2695b4723, esta clave fue ensayada en un Petya anterior, pero esta no funciono ya que dice que la clave es incorrecta

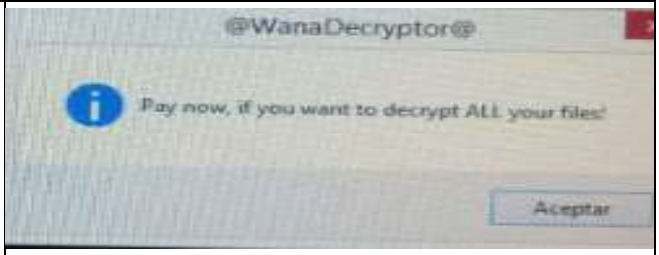
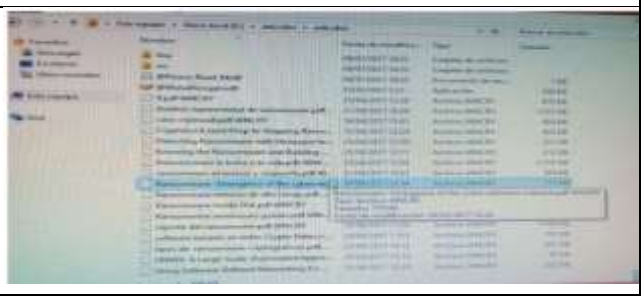
Figura 12. Eliminar petya con clave (Fuente propia, 2017)

4.4.3. Ransomware Wannacrypt

En la siguiente tabla se puede encontrar el ransomware wannacrypt, este malware fue descargado del enlace https://mega.nz/#!kfYzBabZ!bYPl7Y4sXuLo5ArHCFvWKFHdaQRleFkIpgWSzCou6Jg, el cual proporciona el block de YouTube Ender's Show.

TABLA 8 Ransomware Wannacrypt

Cuando el computador fue afectado por el ransomware Wannacrypt, lo primero que sale en la pantalla, es un recuadro donde indica que no hay disco en la unidad y que se debe insertar un disco, después de darle continuar este mensaje, sale en todas las particiones que tiene el disco c,d,e,f etc.	
Después de salir del recuadro anterior sale un mensaje en la pantalla principal donde informa que los archivos han sido encriptados por el ransomware Wannacrypt, indica que se debe buscar un archivo con el nombre @nameDecryptor.exe la cual está en una carpeta de algunos de los archivos encriptados o también la encontramos ubicada en el escritorio.	

Después de abrir este archivo sale otro pantallazo donde están informando que los archivos importantes del equipo fueron encriptados tales como fotos, videos, base de datos etc. Y es perder el tiempo buscado la manera de recuperar los archivos porque esto no es posible sin el servicio de descifrado. También informan que ellos garantizan que, si puede recuperar los archivos, pero para eso tiene que pagar y solo tiene 3 días para realizar el pago y después de esto el precio se duplicara, pasado 7 días ya no podrá recuperar los archivos. Luego indica que debe ingresar a este link about bitcoin para saber cuánto se debe pagar	
Al darle clic al botón que dice Decrypt que es para desencriptar los archivos, sin pagar el valor del rescate saldrá este recuadro donde indica que se debe pagar si quiere recuperar los archivos.	
Este malware encripta todos los archivos que se encuentran en el computador y en todas sus particiones, este encripta imágenes, pdf, doc., etc. A todos los archivos le pone la extensión. Wncry	

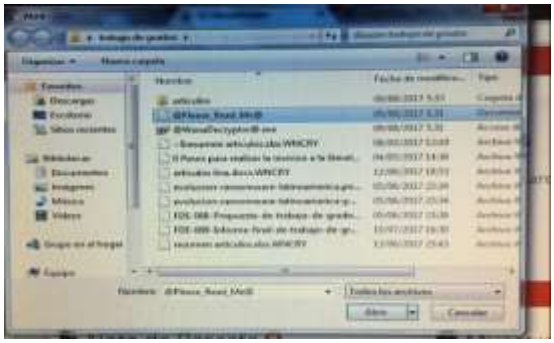
Si reinicia el computador después de estar infectados con este malware se observa que no se puede acceder al escritorio ni a los archivos almacenados en el computador	

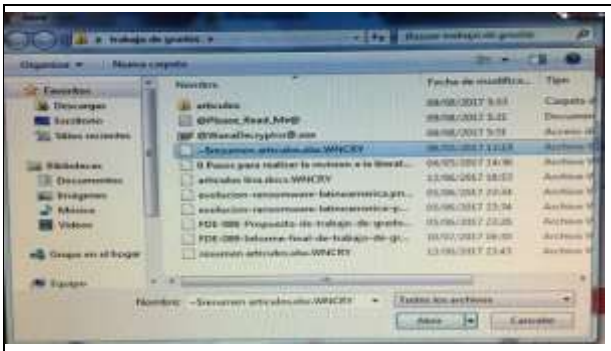
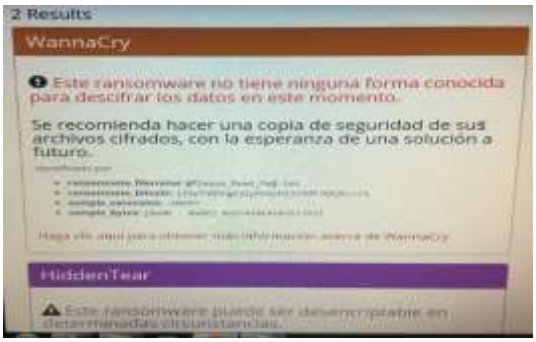
(Fuente propia, 2017)

4.4.4. Prácticas de ilustración para eliminar wannacrypt

A continuación, se hace algunos ejemplos de eliminación o recuperación de archivos cuando el equipo está infectado por este malware, estas aplicaciones se bajaron de algunas páginas de internet donde indican que es posible eliminar este malware por medio de estas prácticas.

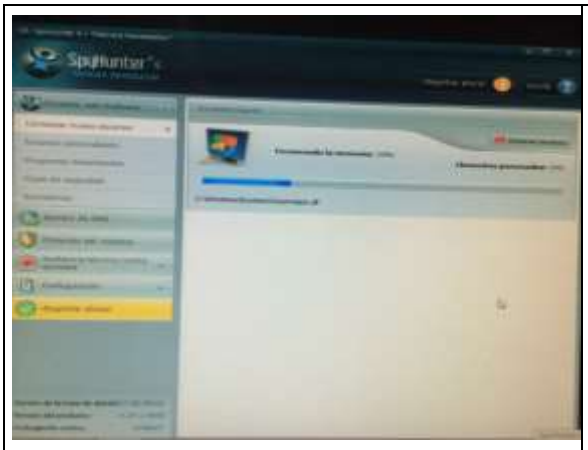
Tabla 9 Eliminar Wanna Decryptor Por El Software Id Ransomware

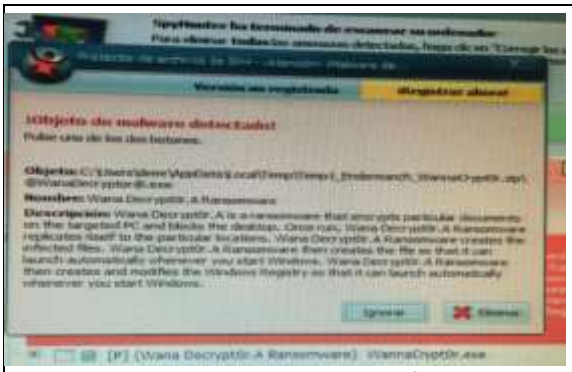
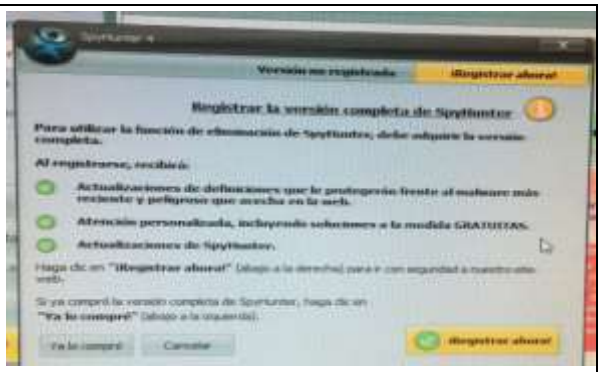
	
Este es el programa utilizado para verificar por cuál de los ransomware fue afectado	En esta imagen se muestra donde se selecciona el archivo donde los creadores del ransomware dan las indicaciones de la forma de pago

	
Aquí se selecciona uno de los archivos encriptados	en esta imagen se muestra el resultado, donde se informa que este ransomware no tiene ninguna forma conocida de descifrar los datos.

Fuente propia (2017).

Tabla 10 Eliminar Wana Decryptor Por El Software Spyhunter

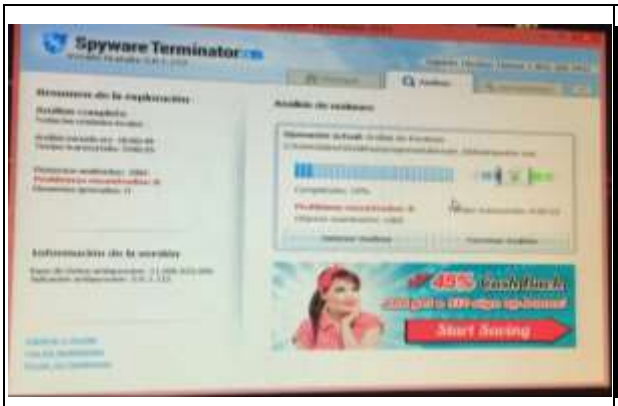
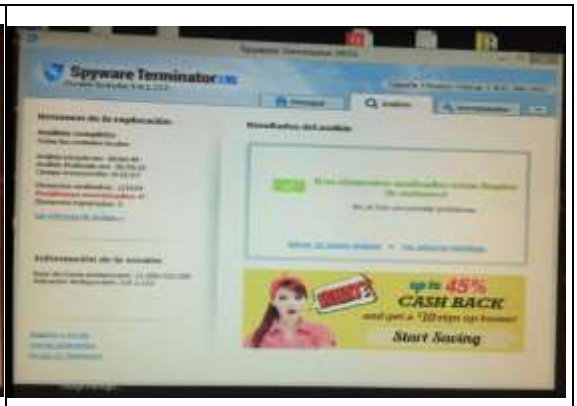
	
Este el programa spyhunter está escaneando todo el equipo para encontrar las posibles amenazas que existan.	En esta ventana muestra en el proceso de instalación y detecta dos amenazas y efectivamente está infectado con el malware Wanna decryptor

 Een esta ventana muestra cual fue el objeto detectado y da la opción de eliminar, al presionar esta opción pide que se debe registrar para que el software termine el proceso de eliminar.	 Ventana donde se muestra que se debe registrar para continuar con el proceso.
 En esta pantalla se intenta hacer el registro, pero como se evidencia este tiene un costo. No fue posible comprar el software porque el proyecto no cuenta con saldo disponible para adquirir dicho aplicativo. Y por ellos no fue posible verificar si este es funcional	

Fuente propia (2017)

También se realizó un practica con el software spyware Terminator, también fue descargado de internet donde informan que con este se puede eliminar el malware, pero no es cierto, lo que hace es escanear el equipo y como se muestra en las imágenes dice que no encuentra ningún malware y por ende no lo elimina.

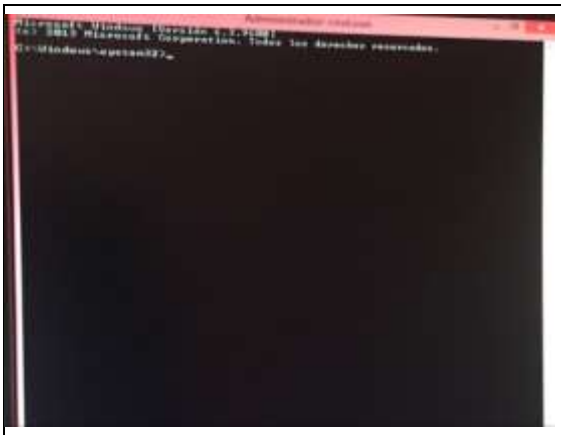
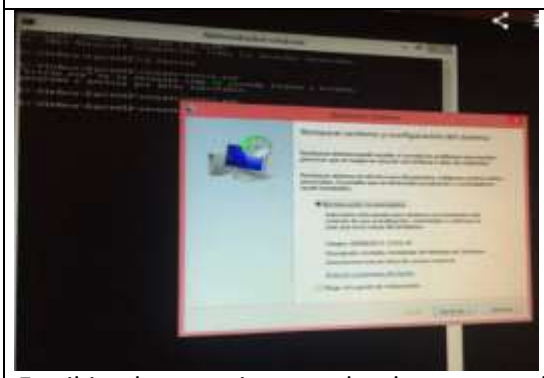
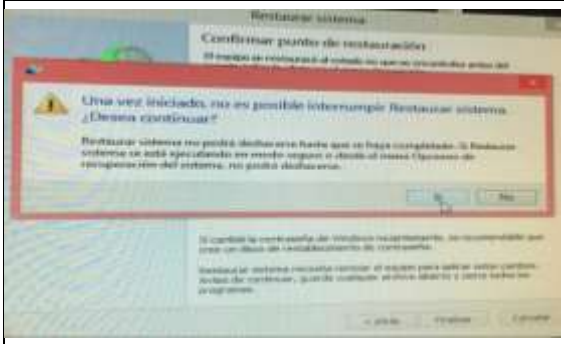
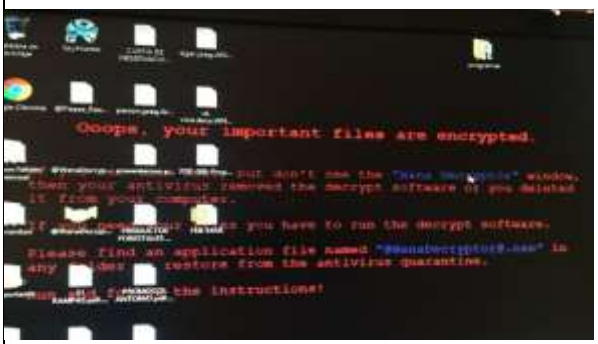
Tabla 11 Eliminar Wana Decryptor Por El Software Spyware Terminator

	
Aquí el software está escaneando el equipo para saber si encuentra algún virus.	En esta parte informa que el software termino de escanear el equipo y no encontró ningún virus, lo que quiere decir que el software tampoco funciona.

Fuente propia (2017)

Se intenta otra opción para intentar eliminar este malware ingresando al sistema operativo en la opción de modo seguro con símbolo del sistema, luego cuando se carga la ventana del símbolo de sistema se escribe cd restore, luego se escribe rstrui.exe para que se abra la ventana para restaurar el equipo en una fecha anterior en que se instaló el malware, pero como se evidencia en las imágenes con esta opción tampoco es posible eliminar este malware.

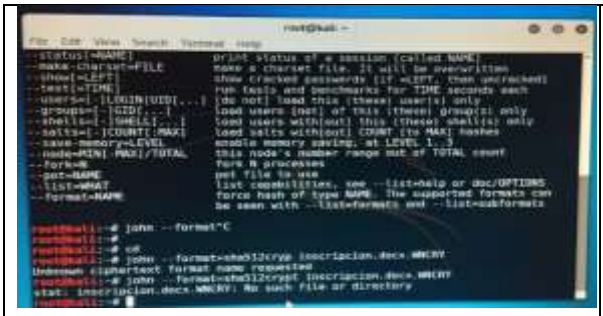
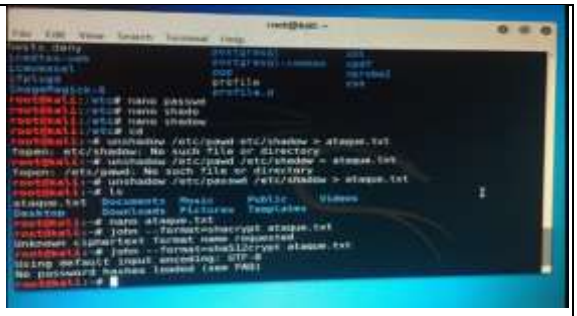
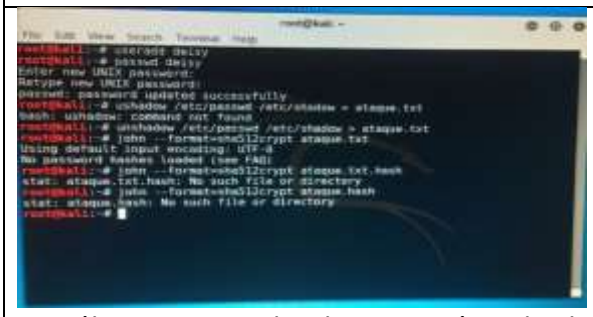
Tabla 12 Eliminar Wana Decryptor Por Medio De Restaurar Sistema

 Aquí ya se ingresó a modo seguro con símbolo del sistema	 En esta ventana se escribe cd restore
 Escribiendo rstrui.exe sale la venta de restaurar sistema la cual se escoge una fecha anterior a la que se infectó el equipo	Aquí se escoge la opción para escoger un punto de restauración
 Aquí ya se eligió el punto de restauración y se procede a reiniciar el equipo	 Como se puede observar en esta imagen el punto de restauración del equipo no funciono porque el equipo sigue infectado.

Fuente propia (2017)

En la siguientes tablas se intenta encontrar o desencriptar un archivo por medio de algunos programas rompe claves que tiene el sistema operativo Kali Linux, lo que se hizo fue guardar un archivo encriptado y probarlo con las siguientes aplicaciones John the Ripper, Jhonny, estas aplicaciones permiten buscar una posible clave por medio del diccionario de datos que estas aplicaciones poseen, pero como se muestra a continuación no es posible encontrar dicha clave porque estas aplicaciones no manejan este tipo de encriptación o en su defecto piden que se agreguen la clave al diccionario de datos para poder ser encontrada.

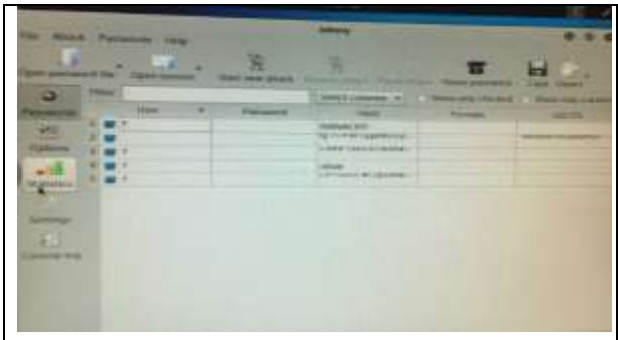
Tabla 13 Desencriptación de archivo por medio de John the Ripper

 En esta imagen se intenta hacer fuerza bruta al archivo, con la extensión que trae por defecto en este caso es WNCRY, Pero como muestra en el mensaje dice que no es un archivo o directorio.	 En la siguiente imagen se crea un nuevo usuario y una contraseña, como estas quedan en carpetas diferentes, lo que se hace es unificarlas en un solo archivo llamado ataque.txt y luego se copió el archivo encriptado dentro de este, pero como muestra la imagen indica que no encuentra la clave.
 Por último, se cambia la extensión a hash para ver si funciona, pero como se muestra a continuación indica que no es un archivo o directorio.	

Fuente propia (2017)

Como conclusión aplicar esta técnica de fuerza bruta con un archivo encriptado por wannacrypt no es funcional, porque esto lo que hace es buscar claves, pero a los archivos hash.

Tabla 14 Desencriptación de archivo por medio de Jhonny

	
En esta imagen se seleccionó el archivo, como se muestra en la segunda casilla de password no se ha encontrado ningún tipo de contraseña.	Después de seleccionado el archivo se le da clic en la opción encontrar contraseña, que son las llaves que se encuentran en la parte de arriba, pero como muestra el mensaje dice que no es posible encontrar dicha contraseña para este formato.

5. RESULTADOS Y DISCUSIÓN

5.1 Resultados

De acuerdo lo realizado en esta investigación se puede concluir que los ransomware son un malware que puede afectar a cualquier persona o empresa, los cuales puede causar un daño significativo a los archivos o todo el disco duro evitando así acceder la información que hay almacenada en el computador. También se demostró con algunas prácticas que obtener la clave de descifrado de algunos malware no es posible y que hacer algunas prácticas que se mencionan en internet no son funcionales, por ahora la única posibilidad de restaurar los archivos es haciendo copia de seguridad periódicamente.

5.2 Buenas Prácticas

5.2.1. Preventivas.

En la siguiente lista se muestra algunos consejos que se deben tomar para evitar ser atacados por algún tipo de ransomware.

- Como primera instancia y más importante se debe realizar un respaldo de la información de forma habitual o se recomienda utilizar algún tipo de servicio que protegen la información, los cuales pueden ser Backus gurú y sec gurú etc.
- Se debe usar antivirus y anti- spyware en los equipos y no olvidar que estos softwares deben de estar actualizados
- El sistema operativo debe estar actualizado
- Es necesario evitar el uso de software piratas
- En caso de que reciba un correo electrónico de una persona o empresa que no conoce es necesario verificar la información antes de abrir dicho correo.
- Si el correo electrónico que recibe es de un idioma diferente al de su país y usted no conoce al remitente lo más recomendable es eliminar el mensaje
- En caso de que reciba un correo electrónico con las extensiones SCR, EXE y COM, lo más recomendado es eliminar el correo ya que estos son archivos que son ejecutables y posiblemente contienen algún tipo de malware.
- Si recibe un correo con un archivo ejecutable con extensiones PDF, DOCX(Word), XLSX (Excel) si no proviene de una fuente confiable lo más recomendado es eliminar el correo porque estas extensiones no son de archivos ejecutables. Los archivos ejecutables con estas extensiones por lo general tienen el nombre del archivo con la extensión.docx.exe, es decir que es un archivo ejecutable y posiblemente contenga un virus es por ello por lo que no se debe abrir.

- En el momento que se encuentre navegando en la internet lo más recomendado es evitar entrar a páginas web que no son recomendadas, por lo general en estas páginas se almacenan más malware.
- Utilizar aplicaciones reconocidas para hacer descargas de software, música, juegos entre otros

5.2.2. Correctivas

El siguiente listado muestra algunas recomendaciones que se deben tomar en caso de que se vean afectados por algún tipo de malware.

- Lo primero y más importante es desconectarse de la red de internet y quitar todos los medios extraíbles (memoria USB, Discos duros etc).
- Después lo que se hace es desinfectar el equipo es decir eliminar el virus el cual lo más recomendado es formateándolo para que no quede ningún rastro del virus.
- En caso de que no se tenga copia de seguridad de los archivos y optaron por realizar el pago que les solicita los ciberdelincuentes, se les recomienda que lo hagan bajo su propia responsabilidad ya que no se les asegura que se les vayan a devolver la clave con la que van a recuperar los archivos. debido a que los atacantes no son personas de confiar y solo tienen un objetivo que es ganar dinero de forma ilícita.
- Si desean pagar el rescate de la información, reiteramos no es lo recomendado, asesorarse del tipo de ransomware que está infectando su dispositivo pues algunos destruyen la información y no es posible recuperarlos ni con la clave que asignan los ciberdelincuentes.

5.2.3. Recomendaciones sobre Petya

El siguiente listado es algunas recomendaciones que se deben tomar en caso de que se vean infectado por alguno de los siguientes ransomware Petya.

- En caso de que se vean afectado por el ransom Petya lo más recomendado es formatear el equipo debido que este malware encripta todo el sistema de arranque del disco duro evitando así ingresar al sistema operativo
- En algunas páginas de internet indican que el ransom se puede eliminar ingresando al sistema operativo por la opción modo seguro, pero como se mencionó anteriormente este virus afecta todo el sistema de arranque y bloquea todas estas posibilidades es por esto por lo que no es posible eliminar este malware por esta opción y no es recomendable practicarla.
- Si se infectó con las versiones anteriores petya 1.0, 2.0 y 3.0 según kasperky existe una clave 38dd46801ce61883433048d6d8c6ab8be18654a2695b4723 que puede desencriptar los archivos. Esta fue ensayada en la versión 1.0 de Petya, pero no funciono, como se mencionó en las pruebas realizada con petya. Pero posiblemente funcione en las otras versiones.

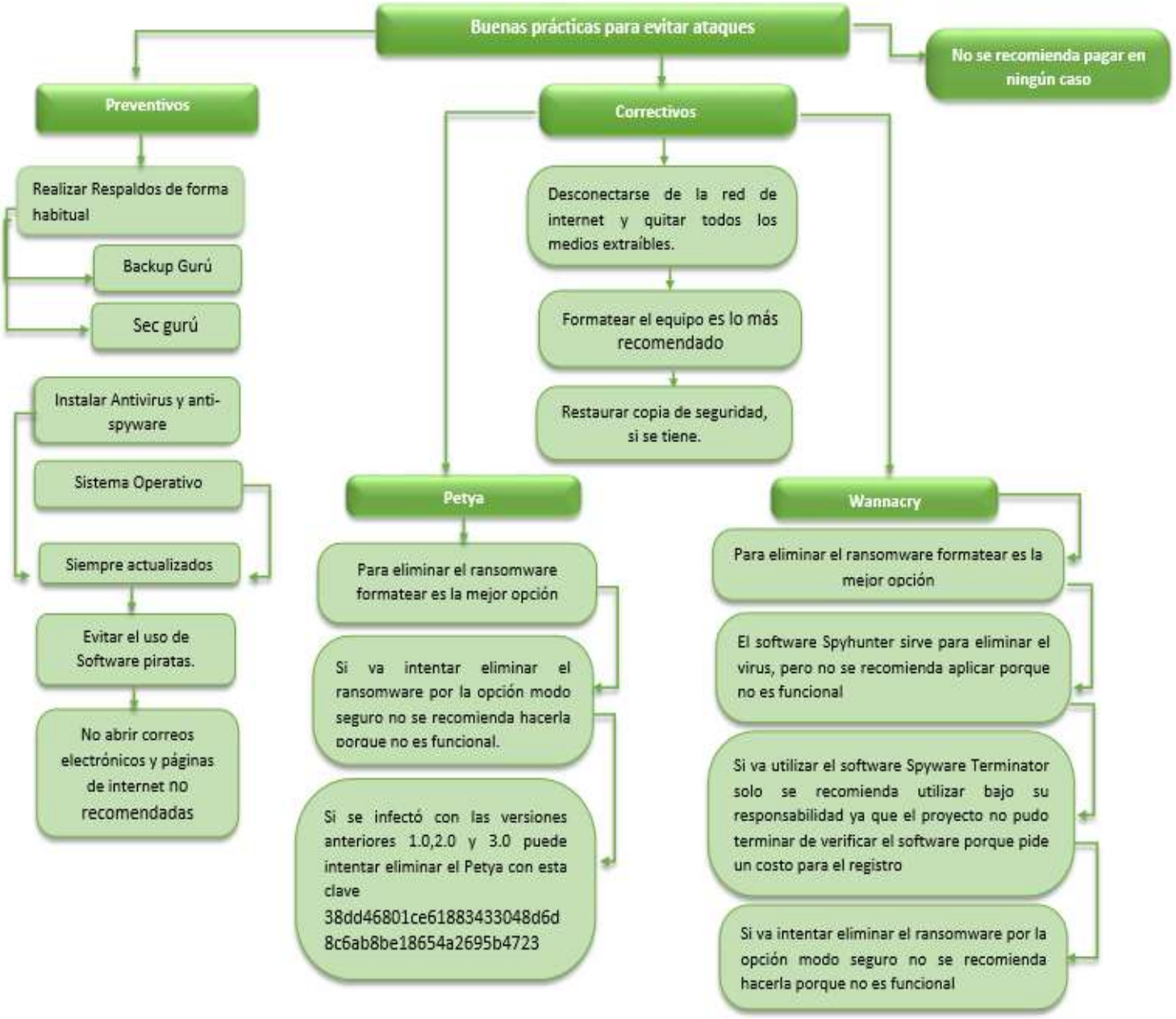
- La conclusión después de realizar las pruebas anteriormente planteadas es que solo hay una forma de eliminar el petya que es formateando el computador, pero no se puede descartar la opción de la clave anteriormente mencionada ya que es posible que funcione en otras versiones y puedan recuperar los archivos, también que es muy importante hacer copia de seguridad de los archivos diariamente para que en caso de que se vean afectados por este malware restaurar los archivos.

5.2.4. Recomendaciones sobre Wannadecrypt

El siguiente listado es algunas recomendaciones que se deben tomar en caso de que se vean infectado por alguno de los siguientes ransomware wannadecrypt

- Cuando su equipo es afectado por el ransomware Wannadecryptor lo más recomendando es formatear el equipo, porque hasta el momento no se han encontrado programas que puedan descifrar los archivos, como se pueden observar en la página id ransomware que es un software que sirve para verificar si existe algún programa para recuperar los archivos, pero esta indica que no existe alguno hasta el momento.
- Como se puede evidenciar en las pruebas anteriores se ensayó con estos dos programas spyware Terminator y software Spyhunter que según páginas de internet eliminan el virus, pero como se puede verificar software Spyhunter no es funcional, spyware Terminator no se pudo verificar porque pide un costo y el proyecto no cuenta los recursos para esto, es por ello por lo que se les recomienda solo usarlo bajo su responsabilidad, pero no son confiables.
- En caso de que quieran eliminar el virus por la opción de restaurar sistema operativo, como se evidencio en las pruebas anteriores esta no es posible porque no elimina el virus es por ellos que no se recomienda hacerlas.
- Como conclusión la única forma de recuperar los archivos cuando está afectado por este malware es por medio de la copia de seguridad que se debe hacer diariamente porque hasta al momento no hay software que puedan recuperar los archivos o la opción de pagar, pero como ya se ha mencionado antes esta no es recomendada hacerse.

5.2.5. Mapa conceptual de las buenas practicas



6. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

- A lo largo de esta investigación se evidencio como el Ransom paso de ser un simple virus a una de las más grandes amenaza informática a nivel mundial, donde solo hay un beneficio económico para los delincuentes, las técnicas de infección cada día son más sofisticadas lo que conlleva a más perdidas de datos sensibles de los sistemas de información. Debido a los últimos ataques y a la magnitud de daño provocado ha hecho que las empresas de seguridad informática innoven los protocolos de seguridad para ayudar a mitigar estos daños.
- También se puede concluir que el termino ransomware ya es conocido por muchas personas, pero no por esto se toman las medidas preventivas para evitar ser parte de un ataque. En la investigación se pudo descubrir que las personas piensan que sus computadores o celulares están eximidos de un ataque, que solo sucede a empresas grandes, ignorando los riesgos que están expuesto todos los usuarios que tengan acceso a un dispositivo electrónico como son los computadores y móviles.
- En algunas páginas de internet salen muchos programas, herramientas y formas en las que indican que es posible eliminar alguno de los malware, pero como se puede evidenciar y concluir en esta investigación, no es posible eliminar este tipo de malware, es por ello por lo que se recomienda siempre tener una copia de seguridad de sus datos.
- Se sugiere seguir los protocolos de seguridad, las recomendaciones de expertos y las buenas prácticas para reducir o evitar el impacto de un ataque ransomware.
- Como trabajo futuro se propone buscar métodos de análisis criptográficos, que permitan romper estos cifrados para eliminar esta amenaza y quitarles este negocio a los ciberdelincuentes. También continuar en la profundización en el análisis de esta temática, tomando como base este trabajo, dado que la limitación de tiempo y el alcance no permitieron hallar métodos de solución efectivos para evitar la infección. Además se debe capacitar la concientización de todos los usuarios de tener una copia de seguridad, que por ahora es el único método de protección ante este malware.

REFERENCIAS

Abrams, (2016), Desencriptado: Alpha ransomware acepta tarjetas de regalo de iTunes como pago, recuperado de, https://www.bleepingcomputer.com/news/security/decrypted-alpha-ransomware-accepts-itunes-gift-cards-as-payment/, accedido el día 06/09/2017

Abrams, (2016), Nuevo alma Locker ransomware siendo distribuido a través del kit de explotación de Rig, Recuperado de https://www.bleepingcomputer.com/news/security/new-alma-locker-ransomware-being-distributed-via-the-rig-exploit-kit/, accedido el día 06/09/2017

Agudo, (2015), El malware de 2015 resumido en nueve cifras, recuperado de, http://www.malavida.com/es/analisis/el-malware-de-2015-resumido-en-nueve-cifras-005831, accedido el día 06/09/2017

Alejandro, (2016), ransomware locky: propagación, protección y recuperación, recuperado de https://protegermipc.net/2016/04/12/ransomware-locky-propagacion-proteccion-y-recuperacion/, accedido el día 07/09/2017.

Arteaga, (2017), El autor del ransomware Petya original publica la clave de descifrado, Recuperado de, http://computerhoy.com/noticias/software/autor-del-ransomware-petya-original-publica-clave-descifrado-64755 , accedido el día 06/09/2017

Berr,(2017), "WannaCry" ransomware attack losses could reach $4 billion, recuperado de, http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/, accedido el día 06/09/2017

Bilbao, (2015), Retire SimpleLocker ransomware Para Android o PC, recuperado de, https://sensorstechforum.com/es/remove-simplelocker-ransomware-for-android-or-pc/, accedido el día 06/09/2017

Bilbao, (2016), Retire Petya ransomware - Misión Imposible (Actualización – Virus encontrado descifrado, recuperado de, https://sensorstechforum.com/es/remove-petya-ransomware-mission-impossible/, accedido el día 06/09/2017

bleepingcomputer (2014), CTB-Locker y Critroni Ransomware Guía de información y preguntas frecuentes, recuperado de, https://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomware-information#ctb_locker, accedido el día 06/09/2017

Bisson, (2016), las 10 principales tendencias del ransomware en 2016, Recuperado de, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/top-10-ransomware-strains-2016/, accedido el día 06/09/2017

Cabaj & Mazurczyk, (2016), Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall, IEEE Network, vol.30, Pag 14-20, accedido el día 06/09/2017

Cabaj, Gregorczyk & Mazurczyk (2016), Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics, arxiv.org, Pag 1-14, accedido el día 06/09/2017

Campos, (2011), El algoritmo de Diffie-Hellman recuperado de, http://www.javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/, accedido el día 06/09/2017

Carlos, Chua y Rodwin, (2015), Virlock infecta archivos y se reinstala después de eliminado, recuperado de, https://www.seguridad.unam.mx/historico/noticia/index.html-noti=2181, accedido el día 06/09/2017

Comunic, (S.F), ¿Qué es Magento?, recuperado de, http://www.comunic-art.com/magento/tiendas-online-magento.html, accedido el día 06/09/2017

Ccm, (2017), Introducción a la seguridad informática, recuperado de, http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica, accedido el día 06/09/2017

Conceptodefinicion, (S.F), Definición de criptografía, recuperado de, http://conceptodefinicion.de/criptografia/, accedido el día 06/09/2017

conceptodefinicion.de, (S.F), definición de criptografía, recuperado de, http://conceptodefinicion.de/criptografia/82/, accedido el día 07/09/2017.

Contreras,flores & otros, (S.F), algoritmo RC5, recuperado de, http://profesores.fi-b.unam.mx/jaqui/Algoritmo%20RC5.pdf, accedido el día 07/09/2017.

Córdoba, (2016), RSA: Cómo funciona este algoritmo de cifrado, recuperado de, https://juncotic.com/rsa-como-funciona-este-algoritmo/, accedido el día 06/09/2017

Cox, (2017), Kidnappers Around the World Want Their Ransoms Paid in Bitcoin, Recuperado de, https://motherboard.vice.com/en_us/article/zmvn44/kidnappers-around-the-world-want-their-ransoms-paid-in-bitcoin, accedido el día 06/09/2017

Crespo, (2016), Lockdroid, un ransomware al que es vulnerable el 67% de los equipos Android, Recuperado de, https://www.redeszone.net/2016/01/28/lockdroid-un-ransomware-al-que-es-vulnerable-el-67-de-los-equipos-android/, accedido el día 06/09/2017

Dc.uba.ar (S.F), criptografía hasting, Recuperado de http://www-2.dc.uba.ar/materias/crip/docs/HASHING.pdf, accedido el dia 10/10/2017

Definición de, (S.F), Seguridad informática, Recuperado de http://definicion.de/seguridad-informatica/, accedido el día 06/09/2017

DeLuz,2010), Criptografía: Algoritmos de cifrado de clave simétrica, Recuperado de, , https://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/, accedido el día 06/09/2017

Drozhzhin, (2015), Ransomware TeslaCrypt 2.0: más fuerte y más peligroso, Recuperado de, https://latam.kaspersky.com/blog/teslacrypt-20-ransomware/5771/, accedido el día 06/09/2017

Drozhzhind, (2016). Historia y evolución del ransomware: datos y cifras, Recuperado de, https://blog.kaspersky.es/ransomware-blocker-to-cryptor/8526/, accedido el día 06/09/2017

Ducklin, (2016), "Locky" ransomware: Lo que usted necesita saber, recuperado de, https://nakedsecurity.sophos.com/es/2016/02/17/locky-ransomware-what-you-need-to-know/, accedido el día 06/09/2017

Ecured, (S.F), sistema informático, Recuperado de https://www.ecured.cu/Sistema_inform%C3%A1tico, accedido el día 06/09/2017

Ecured, (S.F), RC4, recuperado de, https://www.ecured.cu/RC4, accedido el día 07/09/2017.

Enigmasoftware, (S.F), CryptoDefense, Recuperado de, https: //www.knowbe4.com/cryptodefense-ransomware., accedido el día 06/09/2017

Esposito, (2016), Surge un descifrador de Petya gracias a un bug en el ransomware, Recuperado de https://www.kaspersky.es/blog/petya-decryptor/8091/, accedido el día 06/09/2017

Es.ccm, (2017), Introducción a la seguridad informática, recuperado de, http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica, accedido el día 06/09/2017

Es.easyremovemalware, (2016), Directrices eficaces para eliminar KimcilWare Ransomware virus desde el PC, recuperado de, http://es.easyremovemalware.com/directrices-eficaces-para-eliminar-kimcilware-ransomware-virus-desde-el-pc, accedido el día 06/09/2017

es.pcmalwareremoval, (2017), Eliminar Wannacry Ransomware: Guía completa de eliminación, recuperado de, http://es.pcmalwareremoval.com/blog/eliminar-wannacry-ransomware-guia-completa-de-eliminacion, accedido el día 06/09/2017

Esteban, (2016), Realizando Ingeniería inversa a ransomware, recuperado de, https://backtrackacademy.com/articulo/realizando-ingenieria-inversa-a-ransomware

Etienne & Léveillé, (2015), CryptoFortress imita a TorrentLocker, pero es un ransomware diferente, Recuperado de, https://www.welivesecurity.com/la-es/2015/03/11/cryptofortress-imita-torrentlocker-ransomware-diferente/, accedido el día 06/09/2017

Etienne & Léveillé, (2016), Novedades de TorrentLocker: el ransomware criptográfico sigue activo Recuperado de https://www.welivesecurity.com/la-es/2016/09/01/torrentlocker-ransomware-criptografico-activo/, accedido el día 06/09/2017

Ferri, (2013), Qué es Tor y cómo funciona, recuperado de, https://articulos.softonic.com/que-es-tor-uso-seguridad-y-alternativas, accedido el día 06/09/2017

Fortune, (2017), Global Shipping Giant Maersk Is Reeling From the Ransomware Fallout, recuperado de, http://fortune.com/2017/06/29/petya-goldeneye-maersk-ransomware-effects/, accedido el día 06/09/2017

García, (2011), Algoritmo de Cifrado Xor, recuperado de, http://garciac-gaby.blogspot.com.co/2011/06/algoritmo-de-encriptacion-xor.htm, accedido el día 06/09/2017l

GoldSparrow, (2016), Pokemon GO Ransomware, recuperado de, https://www.enigmasoftware.com/pokemongoransomware-removal/, accedido el día 06/09/2017

GoldSparrow, (SF), Anubis Ransomware, recuperado de, https://www.enigmasoftware.com/anubisransomware-removal/, accedido el día 06/09/2017

Gutierrez, (2013), Tipos de criptografía: simétrica, asimétrica e hibrida, Recuperado de, https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida, accedido el día 06/09/2017

Gutierrez, (2016), Nuevas variantes de ransomware en evolución constante, Recuperado de, https://www.welivesecurity.com/la-es/2016/07/08/variantes-de-ransomware-evolucion/, accedido el día 06/09/2017

Gutierrez, (2013), ¿Qué son y para qué sirven el hash?: funciones de resumen y firmas digitales Recuperado de, https://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales, accedido el día 11/10/2017

Gross, (2017), Study finds that 30% of SMES lack an incident response plan https://www.breachsecurenow.com/blog/, accedido el día 06/09/2017

Hampton & Baig, (2015), Ransomware: Emergence of the cyber-extortion menace, conferencia de Edith Cowan University Research Online, Pag 47-56, accedido el día 06/09/2017

Hasherezade, (2016), Maktub Locker, recuperado de https://blog.malwarebytes.com/threat-analysis/2016/03/maktub-locker-beautiful-and-dangerous/, accedido el día 06/09/2017

Hasherezade, (2016), DMA Locker es otro ransomware que apareció a principios de este año, recuperado de, https://blog.malwarebytes.com/threat-analysis/2016/02/dma-locker-a-new-ransomware-but-no-reason-to-panic/, accedido el día 06/09/2017

Hasherezade, (2016), Inside Chimera ransomware – el primer ' doxingware ' en Wild, recuperado de, https://blog.malwarebytes.com/threat-analysis/2015/12/inside-chimera-ransomware-the-first-doxingware-in-wild/, accedido el día 06/09/2017

Henley & Solon, (2017), 'Petya' ransomware attack strikes companies across Europe and US Recuperado de, https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe, accedido el día 06/09/2017

Hernández, (2017), Así funciona Wanna Decryptor, el ransomware que ha atacado a Telefónica, Recuperado de, https://www.tutecnomundo.com/asi-funciona-wanna-decryptor-ransomware-ha-atacado-telefonica,accedido el día 06/09/2017

Herzog & Bal, (2015), Great Crypto Failures Check Point Software Technologies, Pag 1-15, accedido el día 06/09/2017

Infonasa, (S. F), Ransomware: métodos de infección, protección y recuperación, recuperado de, http://www.infodasa.com/web/newsDetails.php?id_section=115&id=91 , accedido el día 17/10/2017

Kessem & Barlow, (2016), Ransomware Report: Top Security Threat Expected to Continue Rising in 2017, Recuperado de, https://securityintelligence.com/ransomware-top-security-threat-expected-to-continue-rising-in-2017/, accedido el día 06/09/2017

Kiguolis, (2015), Radamant ransomware, ¿Cómo eliminar? (Guía de desinstalación), recuperado de, http://losvirus.es/radamant-ransomware/, accedido el día 06/09/2017

Kiguolis, (2016), El virus ransomware Jigsaw. ¿Cómo eliminar? (Guía de desinstalación de), recuperado de, http://losvirus.es/el-virus-ransomware-jigsaw/, accedido el día 06/09/2017

Kiguolis, (2017), Cerber virus. How to remove? (Uninstall guide), Recuperado de http://www.2-spyware.com/remove-cerber-virus.html, accedido el día 06/09/2017

knowbe4, (S.F), CryptoDefense ransomware, Recuperado de https://www.knowbe4.com/cryptodefense-ransomware, accedido el día 06/09/2017

Llorca, (2016), CryptoWall, Locky y Cerber; Este es el ransomware más popular. ¿Cómo evitarlo, Recuperado de https://www.genbeta.com/a-fondo/cryptowall-locky-y-cerber-este-es-el-ramsomware-mas-popular-como-evitarlo, accedido el día 06/09/2017

McAfee, (2016), HydraCrypt Variante de Ransomware Distribuido por Angler Exploit Kit, recuperado de,(2016), recuperado de, https://securingtomorrow.mcafee.com/mcafee-labs/hydracrypt-variant-of-ransomware-distributed-by-angler-exploit-kit/, accedido el día 06/09/2017

Majauskas, (S.F), TeslaCrypt Cómo eliminarlo Recuperado, http://www.malwarerid.com/malwares/teslacrypt //, accedido el día 07/09/2017

Malwarerid, (S.F), PokemonGO ransomware - ¿Cómo eliminarlo? recuperado de, http://www.malwarerid.com/malwares/pokemongo-ransomware, accedido el día 07/09/2017

Medina, (2009), En criptografía, MD5 (Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits recuperado de, http://seguridadredesmedina.blogspot.com.co/2009/10/md5-definicion-y-aplicaciones.html, accedido el día 07/09/2017

Medina, (2015), El criptoanálisis es el arte de descifrar comunicaciones encriptadas, Recuperado de, http://alexandra8-2.blogspot.com.co/2015/08/el-criptoanalisis-es-el-arte-de.html, accedido el día 07/09/2017

Mendez & Villabrille, (2016), El reto de los virus Polyransom el desafio de los virus de Polirransomo, recuperado de, http://www.informaticahabana.cu/sites/default/files/ponencias/SEG06.pdf, accedido el día 07/09/2017

Monika, Zavarsky, Lindskog, (2016). Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization. ScienceDirect, vol.94, Pag 465-472, accedido el día 07/09/2017

Muñoz, (2014), ¿Qué es Bitcoin? ¿Cómo funciona? ¿Dónde se compran?, recuperado de, http://computerhoy.com/noticias/internet/que-es-bitcoin-como-funciona-donde-compran-5389, accedido el día 07/09/2017

Nath & Jyoti (2006), Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics, citeseerx.ist.psu.edu, Pag 1-6, accedido el día 07/09/2017

Noticias de seguridad Informática,(2017), como evitar ser víctimas de ransomware, Recuperado de http://noticiasseguridad.com/malware-virus/como-evitar-ser-victimas-de-ransomware/, accedido el día 07/09/2017

Nyxbone, (SF), Análisis de malware / Base de datos, recuperado de, http://www.nyxbone.com/mdb.html, accedido el día 07/09/2017

Orfila, (2016), Cómo sobrevivir a una infección de ransomware, recuperado de, http://www.cromo.com.uy/como-sobrevivir-una-infeccion-ransomware-n913595, accedido el día 07/09/2017

Pagnotta, (2016), Locky, un nuevo ransomware ya presente en Latinoamérica, recuperado de, https://www.welivesecurity.com/la-es/2016/02/19/locky-nuevo-ransomware-latinoamerica/, accedido el día 07/09/2017

Pastor, (2017) Así funciona, el ransomware que se ha usado en el ciberataque a Telefónica, Recuperado de, https://www.xataka.com/seguridad/wanna-decryptor-asi-funciona-el-supuesto-ransomware-que-se-ha-usado-en-el-ciberataque-a-telefonica, accedido el día 07/09/2017

Pastor, (2017), NotPetya: así actúa el nuevo ransomware que está causando el cso, recuperado de, https://www.xataka.com/seguridad/notpetya-asi-actua-el-nuevo-ransomware-que-esta-causando-el-caos-y-asi-puedes-detener-su-avance, accedido el día 07/09/2017

Peeva, (2017), Quitar el virus troyano Zeus (actualización de agosto 2017), Recuperado de, https://sensorstechforum.com/es/remove-zeus-trojan-virus/, accedido el día 07/09/2017

Peñas, (1995), que es la criptografia, raco.cattp, Vol 6, Pag 6-8, accedido el día 07/09/2017

Perez, (2015), Cuál es la diferencia: Malware, virus, gusanos, spyware, troyanos y ransomware, recuperado de, http://computerhoy.com/listas/software/cual-es-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etc-35163, accedido el día 07/09/2017

Perez, (2016), El ransomware no sólo ataca al ordenador, esta desagradable forma de malware es cada vez más sofisticado y común también en el mundo de los móviles, Recuperado de, https://blog.avast.com/es/la-evolución-del-ransomware-movil, accedido el día 07/09/2017

Preukschat, (2014), Por qué se utiliza Criptografía de Curva Elíptica en Bitcoin, recuperado de, https://www.oroyfinanzas.com/2014/01/criptografia-curva-eliptica-bitcoin-por-que-utiliza-ecdsa/, accedido el día 07/09/2017

Pulzo, (2017), ¿Qué hacer si es víctima del poderoso ciberataque mundial?, recuperado de, http://www.pulzo.com/tecnologia/como-defenderse-ciberataque-masivo/PP267385, accedido el día 07/09/2017

Reaqta, (2016), Ransomware Bandarchor sigue activo, recuperado de, https://reaqta.com/2016/03/bandarchor-ransomware-still-active/, accedido el día 07/09/2017

Raúl Armando Ramos Morocho, Enrique Gallegos Mosquera. (2016). infección con ransomware en el servidor de base de datos del sistema onsystec. 3c tecnología, vol.5 – nº 4, 14 pg, accedido el día 07/09/2017

Redyseguridad.fi-p.unam.mx, (2017), DSA (Digital Signature Algorithm) ,recuperado de http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/5-criptografia-asimetrica-o-de-clave-publica/56-firmas-digitales/562-dsa-digital-signature-algorithm, accedido el día 07/09/2017.

Roth, Bart, Gillespie, Rivero, Gallagher, Hahn, Mosh, (SF), Descripción de ransomware, recuperado de, http://www.nyxbone.com/malware/RansomwareOverview.html, accedido el día 07/09/2017

Rus, (2013), Qué es Tor y cómo se utiliza, recuperado de, https://rootear.com/seguridad/que-es-tor, accedido el día 07/09/2017

Segu.info, (S.F), criptologia, Recuperado de, http://www.segu-info.com.ar/criptologia/criptologia.htm, accedido el día 07/09/2017

Sensorstechforum, (2017), quitar el virus troyano zeus, recuperado de, https://sensorstechforum.com/es/remove-zeus-trojan-virus/, accedido el día 07/09/2017

Snow, (2017), El ransomware Petya se “come” tu disco duro, recuperado de, https://www.kaspersky.es/blog/petya-ransomware/8044/, accedido el día 07/09/2017.

Show, (2017), Petya.A Ransomware Don't Encrypt Files, recuperado de, https://www.youtube.com/watch?v=bNqgFW4Wj2M, accedido el día 07/09/2017

Show, (2017), WannaCrypt0r Ransomware (download link + removal), recuperado https://www.youtube.com/watch?v=4BGxbwSG9Bg, accedido el día 07/09/2017

Splinters, (2017), Virus de Samsam ransomware. ¿Cómo quitar? (Guía de desinstalación), recuperado de, http://www.2-spyware.com/remove-samsam-ransomware-virus.html, accedido el día 07/09/2017

Ssl247, (S.F) ¿Qué son RSA, DSA y ECC?, recuperado de, https://www.ssl247.es/certificats-ssl/rsa-dsa-ecc, accedido el día 07/09/2017

Techdatatsmex, (2017), La evolución del ransomware móvil, recuperado de, http://techdatatsmex.blogspot.com.co/, accedido el día 07/09/2017

tecnologia-facil, (2015), ¿Qué es P2P?, recuperado de, http://tecnologia-facil.com/que-es/que-es-p2p/, accedido el día 07/09/2017

ticbeat, (2017), Los 9 tipos de ransomware más habituales, Recuperado de, http://www.ticbeat.com/seguridad/los-9-tipos-de-ransomware-mas-habituales/2/, accedido el día 07/09/2017

trendmicro, (2017), Ransomware Recap: The Week of WannaCry, Recuperado de https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-the-week-of-wannacry, accedido el día 07/09/2017

trendmicro, (2017), Erebus Linux Ransomware: Impact to Servers and Countermeasures https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/erebus-linux-ransomware-impact-to-servers-and-countermeasures, accedido el día 07/09/2017

Ugr, (S.F) El cifrado de Cesar, Recuperado de, http://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/02a04.htm, accedido el día 07/09/2017

Valdez & Sconzo, (2016), Alerta de amenazas: "PowerWare", nuevo Ransomware escrito en PowerShell, se dirige a organizaciones a través de Microsoft Word, recuperado de, https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word/, accedido el día 07/09/2017

Velasco, (2016), KimcilWare, un nuevo ransomware enfocado a secuestrar tiendas online, recuperado de https://www.redeszone.net/2016/03/30/kimcilware-nuevo-ransomware-enfocado-secuestrar-tiendas-online/, accedido el día 07/09/2017

Vencislav Krustev, (2016), Eliminar 8lock8 ransomware y descifrar archivos 8lock8 de forma gratuita, recuperado de, https://sensorstechforum.com/remove-8lock8-ransomware-decrypt-8lock8-files-free/, accedido el día 07/09/2017

Webtriplex, (2017), Que es y cómo protegerse de un ataque de diccionario, recuperado de, http://webtriplex.com/vernoticias.php?Id=81&ti=Que-es-y-como-protegerse-de-un-Ataque-de-Diccionario&pageNum_listado=2&totalRows_listado=122, accedido el día 07/09/2017

Zetter, (2016), Why Hospitals Are the Perfect Targets for Ransomware, recuperado de, https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/, accedido el día 07/09/2017

FIRMA ESTUDIANTES Lina castañeda

Deisy Mosquera

FIRMA ASESOR Rdo correcciones entrega informe final. 25/10/201

FECHA ENTREGA: _____

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO ACEPTADO CON MODIFICACIONES _____

ACTA NO. _____

FECHA ENTREGA:

FIRMA CONSEJO DE FACULTAD _____

ACTA NO. _____

FECHA ENTREGA: