Universitat Oberta de Catalunya

uoc.edu

Estudio sobre el malware Ransomware

Carlos Estrada Cola
Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
Instituto Nacional de Ciberseguridad (INCIBE)

Ángela María García Valdés
Víctor García Font

Diciembre de 2018

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

Copyright © 2019 Carlos Estrada Cola.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU Free Documentation License".

C) Copyright

Copyright © 2019 Carlos Estrada Cola.

Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Estudio sobre el malware Ransomware*
Nombre del autor:	*Carlos Estrada Cola*
Nombre del consultor/a:	*Ángela María García Valdés*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega:	12/2018
Titulación:	*Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)*
Área del Trabajo Final:	*Instituto Nacional de Ciberseguridad (INCIBE)*
Idioma del trabajo:	*Castellano*
Palabras clave	*ciberdelincuencia, malware, ransomware*

Resumen del Trabajo:

El uso de la informática está cambiando nuestra forma de vivir. La información almacenada en nuestros sistemas informáticos es un material muy valioso para nuestra sociedad altamente digitalizada.

Los cibercriminales saben que esta información es de vital importancia para las organizaciones. Una de las herramientas que utilizan hoy en día los ciberdelincuentes es un tipo de programa malicioso conocido como Ransomware, el cual secuestra la información almacenada en nuestros equipos informáticos para luego solicitar una compensación económica si se quiere recuperar.

Lo que se pretende con este trabajo es realizar un estudio sobre el malware Ransomware para cubrir la necesidad que poseen las organizaciones de proteger su información. Para ello se estudia las características de este programa malicioso, los tipos de ransomwares que existen, qué vectores de infección utiliza, sus modelos de negocio, qué respuesta da el Derecho ante esta amenaza y como ejemplo de ataque conocido se estudia el caso del ransomware WannaCry.

Abstract:

The use of information technology is changing the way we live. The information stored in our computer systems is a very valuable asset for our highly digitized society.

Cybercriminals know that this information is of vital importance to organizations. One of the tools used today by cybercriminals is a type of malicious program known as Ransomware, which hijacks the information stored in our computer equipment and after, an economic compensation is requested to recover it.

The aim of this work is to carry out a study on Ransomware malware to cover the need that organizations have to protect their information. To do this, we study the characteristics of this malicious program, the types of ransomware that exist, what vectors of infection it uses, its business models, how the law responds to this threat and, as an example of a known attack, the case of the WannaCry ransomware is studied.

Agradecimientos

A mi familia.

Índice

1. Introducción....1
  1.1 Contexto y justificación....1
  1.2 Objetivos....2
  1.3 Metodología....2
  1.4 Planificación del Trabajo....3
  1.5 Productos obtenidos....4
  1.6 Estructura del Trabajo Final de Máster....4
2. Estudio sobre el malware Ransomware....6
  2.1 Características del ransomware....6
    2.1.1 Definición....6
    2.1.2 Historia del ransomware....7
    2.1.3 Estado actual....9
    2.1.4 Futuro del ransomware....13
  2.2 Familias y variantes del ransomware....15
    2.2.1 Familias de ransomware....15
    2.2.2 Variantes de ransomware....16
  2.3 Vectores de infección más comunes....33
    2.3.1 Correos electrónicos maliciosos....33
    2.3.2 Páginas web infectadas....35
    2.3.3 Conexión de dispositivos periféricos....36
    2.3.4 Explotación de vulnerabilidades....37
    2.3.5 Descargas de ficheros en redes P2P o sitios web....37
  2.4 Modelos de negocio....38
    2.4.1 Motivación....38
    2.4.1 Modelo de negocio “tradicional”....39
    2.4.2 Ransomware-as-a-Service (RaaS)....41
  2.5 Medidas de seguridad....45
    2.5.1 Medidas de seguridad preventivas o activas....45
    2.5.2 Medidas de seguridad reactivas o pasivas....62
  2.7 Respuesta del Derecho ante el ransomware....73
    2.7.1 Tipificación Penal....73
    2.7.2 Cómo denunciar....78
  2.8 Caso: ataque WannaCry....79
    2.8.1 Antecedentes....79
    2.8.2 Ataque....81
    2.8.3 Impacto....82
    2.8.4 Contención....85
    2.8.5 Acusaciones....86
3. Conclusiones y trabajo futuro....88
  3.1 Conclusiones....88
  3.2 Objetivos cumplidos....89
  3.3 Trabajo futuro....90
4. Glosario....91
5. Bibliografía....94
6. Anexos....109
  Anexo I. Diagrama de Gantt....109

Lista de figuras

Figura 1: Archivos cifrados por un ransomware [3].....7
Figura 2:Comparativa del uso de tipos de ransomwares [6].....9
Figura 3: Número de equipos infectados por ransomware como mínimo una vez entre abril del 2016 y marzo del 2017 [9].....10
Figura 4: Número de teléfonos móviles infectados como mínimo una vez por ransomware entre abril del 2017 y marzo del 2018 [9].....10
Figura 5: Equipos infectados como mínimo una vez por cryptominers entre abril del 2016 y marzo del 2017 [9].....11
Figura 6: Equipos infectados como mínimo una vez por cryptominers entre abril del 2017 y marzo del 2018 [9].....11
Figura 7: Detecciones de cryptominers [11].....12
Figura 8: Precio del Bitcoin entre octubre del 2107 y octubre del 2018.....12
Figura 9: Familias de nuevos ransomwares entre 2015 y 2017 [10].....13
Figura 10: Nuevas variantes de ransomwares entre 2015 y 2017 [10].....13
Figura 11: Línea temporal de los ransomwares [64].....15
Figura 12: Mensaje de aviso del troyano AIDS [8].....17
Figura 13: Ficheros creados por el ransomware Archiveus [21].....17
Figura 14: Mensaje de que muestra GPGCoder después del cifrado[21].....18
Figura 15: Mensaje falso de la policía que del ransomware Reventon [19].....20
Figura 16: Mensaje que muestra Cryptolocker [68].....21
Figura 17: Mensaje que muestra Simplocker y archivos infectados [30].....22
Figura 18: Mensajes de muestra de Koler [32].....23
Figura 19: Mensajes de muestra de Synolocker [33].....23
Figura 20: Mensaje de TeslaCrypt [38].....25
Figura 21: Mensaje del ransomware Chimera [39].....25
Figura 22: Anuncio relacionado con el negocio de Tox [40].....26
Figura 23: Consola de configuración de Ransom32 [45].....27
Figura 24: Mensaje de rescate del ransomware Jigsaw [46].....28
Figura 25: Televisor bloqueado por el ransomware FLocker [49].....29
Figura 26: Mensaje de rescate del ransomware PopcornTime [50].....30
Figura 27: Mensaje de rescate de KimcilWare [54].....30
Figura 28: Ficheros cifrados por KimcilWare en servidor Web [54].....31
Figura 29: Mensaje de rescate del ransomware nRansom [56].....32
Figura 30: Correo electrónico con enlace malicioso de Correos [46].....33
Figura 31: Correo electrónico con enlace malicioso de Hacienda [58].....34
Figura 32: Correo electrónico con adjunto malicioso de Movistar [58].....34
Figura 33: Pantalla para actualizar Transmission a la versión 2.90 [42].....35
Figura 34: Muestra del disquete con el que se distribuía el troyano AIDS [7].. .36
Figura 35: Mensaje que que muestra Cryptowall [29].....40
Figura 36: Página web con las instrucciones del pago en Bitcoins [69].....40
Figura 37: Beneficio obtenido con el modelo de negocio tradicional [67].....41
Figura 38: Web que oferta el servicio RaaS Satán [72].....42
Figura 39: Formulario de suscripción al servicio de Satán [52].....43
Figura 40: Servicios adicionales que ofrece Satán [52].....43
Figura 41: Anuncio relacionado con el negocio de Petya y Mischa [47].....44

Figura 42: Consola principal de configuración de Karmen [77].....44
Figura 43: Ejemplo de segmentación de red [85].....48
Figura 44: Ejemplo de topología de red con firewall de perímetro [89].....51
Figura 45: Ejemplo de topología de red con IDS/IPS [92].....51
Figura 46: Ejemplo de topología de red con proxy web [93].....52
Figura 47: Pantalla principal de EMET [104].....60
Figura 48: Opción "Control de acceso a carpeta" de Windows 10 [105].....61
Figura 49: EternalBlue en Metasploit [126].....79
Figura 50: DoublePulsar en Metasploit [128].....80
Figura 51: Resultados parciales del escaneo de DoublePulsar [130].....80
Figura 52: Mensaje de rescate de WannaCry [131].....81
Figura 53: Direcciones IP afectadas en España [130].....82
Figura 54: Direcciones IP afectadas mundialmente [130].....82
Figura 55: Países afectados por WannaCry [132].....83
Figura 56: Correo de aviso de Telefónica [134].....84
Figura 57: Claves de CryptGenRandom [137].....85
Figura 58: Algoritmo AES de WannaCry [137].....86

1. Introducción

1.1 Contexto y justificación

La tecnología informática está cambiando nuestra vida cotidiana ya que nos facilita y permite controlar diversos aspectos y procedimientos de ésta. El uso de la informática se encuentra en diversas áreas como son, por ejemplo, la gestión de empresas, medicina, multimedia o industria. Todas estas áreas utilizan grandes cantidades de información almacenada en los equipos informáticos en forma de datos. Hoy en día, podemos encontrarnos cientos de tipos de ficheros almacenados en los ordenadores con información importante como son, por ejemplo: facturas, datos de salud, datos personales de clientes, planos de edificios o planos de material militar.

Esta información, estos datos, se ha convertido en un material muy valioso para nuestra sociedad. Por ejemplo, qué pasaría si una empresa de arquitectura pierde los planos de los edificios que tanto tiempo y dinero le han costado diseñar, qué ocurriría si en un hospital se extraviasen los informes de salud de su pacientes, qué sucedería si un banco perdiese todos o parte de los datos económicos de sus clientes o qué pasaría si una potabilizadora de agua no pudiese ejecutar sus procesos porque se han bloqueado sus sistemas industriales de control. La desaparición de esta información sería crítica tanto para la empresa como para la sociedad ya que puede conllevar perdidas económicas, de recursos e incluso puede causar daños hacia las personas.

Los ciberdelincuentes saben que esta información es de vital importancia para las organizaciones y que algunas de éstas estarían dispuestas a pagar por ella si se perdiese o cayese en malas manos. Una de las herramientas que utilizan hoy en día los ciberdelincuentes es un tipo de virus informático conocido como el Ransomware, el cual permite apoderarse de esta información para luego pedir una compensación económica si se quiere recuperar.

El Ransomware es un tema relevante porque actualmente es una de las amenazas más habituales utilizadas por los ciberdelincuentes y críticas para todas las organizaciones del mundo. Lo que se pretende con este trabajo es realizar un estudio sobre el malware Ransomware para cubrir la necesidad que poseen las organizaciones de proteger su información. El resultado que se pretende con este trabajo es conocer mejor este tipo de amenaza para concienciar a los usuarios y administradores de los sistemas informáticos de los riesgos, peligros y efectos derivados de esta amenaza tecnológica.

1.2 Objetivos

El objetivo principal de este trabajo final de máster es concienciar al lector de la amenaza que supone el malware Ransomware. Este objetivo se complementará junto con los siguientes objetivos:

- Comprender el concepto de Ransomware.
- Conocer los tipos de Ransomware que existen en la actualidad.
- Describir cómo infecta los sistemas informáticos.
- Conocer el modelo de negocio que se esconde detrás de las campañas de infección.
- Describir las técnicas que existen en la actualidad para detectar y mitigar su infección.
- Conocer las medidas legales que está adoptando la sociedad española para protegerse frente a esta amenaza
- Conocer el caso del ataque del Ransomware WannaCry.
- Exponer las conclusiones de este estudio.

1.3 Metodología

Para cumplir con los objetivos del presente trabajo se realiza una combinación de las metodologías de investigación exploratoria, descriptiva y explicativa tal y como se expone en los párrafos siguientes.

Para iniciar el estudio de este malware se utiliza una metodología exploratoria que permite conocer el Ransomware de una manera superficial para comenzar a familiarizarnos con este virus.

Posteriormente, se utiliza una metodología descriptiva que nos posibilita profundizar más en el estudio del Ransomware, ya que este método ayuda a poder definir, clasificar y conocer mejor su comportamiento. Además, mediante el uso de esta metodología también se puede estudiar las medidas de protección, tanto técnicas como legales, que existe actualmente en la sociedad española.

Para el estudio del ataque del Ransomware WannaCry se utilizará una metodología explicativa que permite, no solo describir este suceso, sino también buscar los motivos que llevaron a que grandes organizaciones se infectasen con este malware.

Entre las técnicas que se usan para hacer este trabajo se encuentra la investigación documental y la recolección de información procedente de numerosas fuentes como son artículos académicos de investigación, libros, noticias y páginas de Internet relacionadas con la seguridad de la información.

Esta estrategia de estudio que se sigue es la más apropiada porque permite al lector comenzar a entender los conceptos básicos y necesarios sobre el virus Ransomware para que, a medida que avanza su lectura, éste pueda entender la problemática que se encuentra detrás

de esta amenaza y, de esta forma, pueda reflexionar y concienciarse sobre los riesgos asociados que existen actualmente en los sistemas informáticos.

1.4 Planificación del Trabajo

La elaboración del estudio se compone de las siguientes fases principales:

1. **Planificación del proyecto**: en esta primera fase del trabajo se establece el contexto y la justificación de la importancia que tiene la realización de este estudio. Para ello se listan los objetivos, se describe la metodología y técnicas de investigación que se van a utilizar y se realiza una planificación temporal junto con la enumeración de los productos obtenidos que se entregará durante el periodo de realización de este proyecto.

2. **Investigación y documentación**: en esta segunda etapa del estudio se utilizan las técnicas de investigación documental y de recolección de información para ir completando cada uno de los apartados del estudio, en concreto, se investigan los puntos siguientes:
   I. Características del Ransomware.
   II. Familias y variantes del Ransomware.
   III. Vectores de infección más comunes.
   IV. Modelo de negocio.
   V. Medidas de seguridad.
   VI. Respuesta del Derecho ante el Ransomware.
   VII. Caso: ataque WannaCry.

3. **Conclusiones**: en esta fase se presentan las conclusiones obtenidas procedentes de la realización del estudio.

4. **Entrega**: en esta etapa se entrega en el aula virtual la memoria final del presente estudio.

5. **Preparación y realización del vídeo presentación**: en esta fase se toman decisiones sobre el diseño y la estructura del vídeo para, posteriormente, realizar la grabación de éste.

6. **Defensa**: esta etapa consiste en un periodo en el cual el tribunal realiza una serie de preguntas que se les da respuesta.

La plantificación temporal de este estudio definida mediante el diagrama de Gantt se puede ver en el Anexo I. Para la realización del Diagrama de Gantt se ha utilizado la herramienta online Tomsplanner[1].

1 Página web de la herramienta: https://www.tomsplanner.com

1.5 Productos obtenidos

A lo largo de la realización de este Trabajo Final de Máster se obtienen los siguientes entregables:

- **PEC 1**: este entregable consiste en la definición del plan de trabajo junto con su contexto y justificación, objetivos y metodología a seguir más una breve descripción de los productos entregables y un resumen del estudio. La fecha prevista para entregar esta producto es el día 8 de octubre de 2018.

- **PEC 2**: este producto consiste en entregar parte de la memoria final, en concreto se proporcionan desarrollados los siguientes puntos de la memoria:
  - Características del Ransomware.
  - Familias y variantes del Ransomware.
  - Vectores de infección más comunes.

  La fecha prevista para entregar esta PEC es el día 5 de noviembre de 2018.

- **PEC 3**: esta PEC consiste en entregar desarrollados los siguientes puntos de la memoria:
  - Modelo de negocio.
  - Medidas de seguridad.
  - Respuesta del Derecho ante el Ransomware.

  La fecha prevista para suministrar esta PEC es el día 3 de diciembre de 2018.

- **PEC 4**: este entregable es la memoria final con el desarrollo de los puntos restantes, en concreto:
  - Caso: ataque WannaCry.
  - Conclusiones.

  La fecha prevista para entregar este producto es el día 31 de diciembre de 2018.

- **PEC 5**: este entregable consiste en la presentación grabada en vídeo con la voz en off del autor del estudio. La fecha prevista para proporcionar este producto es el día 7 de enero de 2019.

1.6 Estructura del Trabajo Final de Máster

El siguiente capítulo de la memoria contiene el estudio sobre el malware Ransomware. Este capítulo esta subdividido en los siguientes puntos:

- **Características del Ransomware**: este punto enseña al lector la definición del programa malicioso para que entienda en qué consiste este tipo de virus informático junto con una breve historia del origen de este malware y cuál es el estado actual y futuro de las infecciones en el mundo.

- **Familias y variantes del Ransomware**: este apartado expone y describe las características de las familias y variantes más importantes del Ransomware que han existido hasta nuestros días.

- **Vectores de infección más comunes**: en esta parte se describe la forma y las vías en el que el virus accede e infecta los sistemas informáticos.

- **Modelo de negocio**: en este punto se enseña al lector cuál es la forma que tienen los ciberdelincuentes para lucrarse con el uso del Ransomware.

- **Medidas de seguridad**: esta sección muestra las formas que tienen los equipos informáticos para prevenir la infección del virus y cuáles son las medidas que se pueden adoptar para paliar su infección.

- **Respuesta del Derecho ante el Ransomware**: en este apartado se explica qué leyes y normativas existen actualmente en la sociedad española para protegerse frente a este tipo de amenazas.

- **Caso: ataque WannaCry**: en este punto se describe el conocido caso del Ransomware WannaCry que afectó a grandes empresas de todo el mundo en el año 2017.

- **Conclusiones**: este es el último apartado de la memoria y es donde se presentan las conclusiones alcanzadas procedentes del desarrollo del estudio.

2. Estudio sobre el malware Ransomware

2.1 Características del ransomware

El objetivo de este apartado del estudio es conocer qué es y en qué consiste el ransomware. Además se realiza un recorrido histórico de los principales ataques en el mundo relacionados con esta amenaza hasta el año 2018 y se analizará cuál es el estado actual de esta amenaza y qué futuro nos espera en relación a estos ataques. De esta forma el lector comienza a familiarizarse con este tipo de programa malicioso.

2.1.1 Definición

El termino ransomware proviene del inglés y éste se compone de la palabra *ransom* que significa secuestro y *ware* que es el acortamiento de la palabra inglesa *software* que significa programa. Otras opciones de éste termino en español son “programa de secuestro” o “secuestrador” y “programa de chantaje” o “chantajista" [1].

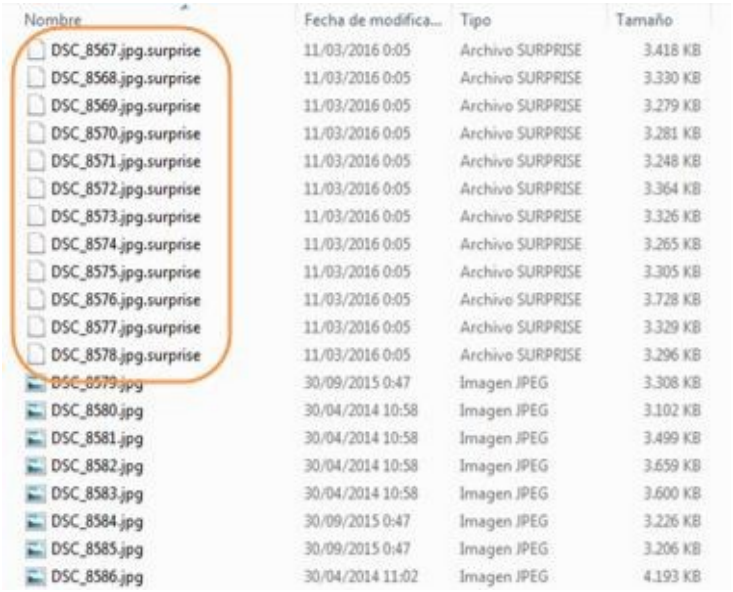
Un ransomware es un programa malicioso que impide el acceso a los ficheros almacenados en el equipo informático y/o al propio sistema informático para solicitar un rescate económico a la víctima si quiere recuperar este acceso [2] y de está forma ataca a uno de los pilares básicos de la seguridad, la disponibilidad de la información.

Las forma principal de ataque en las que el ransomware impide estos accesos son el uso de una clave de cifrado que solo conoce el ciberdelincuente creador del malware. En la figura 1 de la página siguiente se muestra una imagen de un directorio infectado con algunos de los archivos cifrados con la extensión “.surprise” y borrados los originales [3].

La principal motivación que lleva a que los *cibercriminales* utilicen esta forma de malware es la económica, ya que existen algunas campañas de ransomware que pueden superar los 6 millones de dólares [4].

Este tipo de ataques afecta a todos los sistemas operativos de los equipos informáticos, tanto de usuarios como de servidores, ya sean Windows, Linux o OSX e incluso a los sistemas operativos de los teléfonos móviles Android, Windows o iOS. No existe un sistema operativo que sea invulnerable, pero es importante remarcar que los sistemas más afectados son Windows y Android por ser los más utilizados [5].

Este tipo de programa malicioso puede afectar tanto a cualquier modelo de organización, ya sean empresas, gobiernos o infraestructuras críticas, hasta incluso usuarios con equipos domésticos [3].



Nombre	Fecha de modifica...	Tipo	Tamaño
DSC_8567.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.418 KB
DSC_8568.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.330 KB
DSC_8569.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.279 KB
DSC_8570.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.281 KB
DSC_8571.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.248 KB
DSC_8572.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.364 KB
DSC_8573.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.326 KB
DSC_8574.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.265 KB
DSC_8575.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.305 KB
DSC_8576.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.728 KB
DSC_8577.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.329 KB
DSC_8578.jpg.surprise	11/03/2016 0:05	Archivo SURPRISE	3.296 KB
DSC_8579.jpg	30/09/2015 0:47	Imagen JPEG	3.308 KB
DSC_8580.jpg	30/04/2014 10:58	Imagen JPEG	3.102 KB
DSC_8581.jpg	30/04/2014 10:58	Imagen JPEG	3.499 KB
DSC_8582.jpg	30/04/2014 10:58	Imagen JPEG	3.659 KB
DSC_8583.jpg	30/04/2014 10:58	Imagen JPEG	3.600 KB
DSC_8584.jpg	30/09/2015 0:47	Imagen JPEG	3.226 KB
DSC_8585.jpg	30/09/2015 0:47	Imagen JPEG	3.206 KB
DSC_8586.jpg	30/04/2014 11:02	Imagen JPEG	4.193 KB

Figura 1: Archivos cifrados por un ransomware [3].

Entre las consecuencias que tiene infectarse con este programa malicioso se encuentran [3]:

1. Posible pérdida permanente de la información importante guardada en los unidades de almacenamiento de los sistemas informáticos.

2. Interrumpir el flujo de trabajo de las organizaciones.

3. Perdidas económicas derivadas de la perdida de información y del tiempo empleado para restaurar los sistemas y ficheros afectados o incluso por pagar el rescate.

4. Perdida reputacional de la organización que puede hacer perder socios y/o clientes.

2.1.2 Historia del ransomware

El ransomware no es un programa malicioso reciente, podemos ver que éste ya lleva entre nosotros más de 28 años. El primer ransomware que se detectó fue el Troyano AIDS en 1989. En el punto "*2.2 Familias y variantes del ransomware"* se puede ver una descripción de cada uno de los ransomwares que han existido hasta nuestros días.

La historia del ransomware se puede dividir en las siguientes dos etapas dependiendo del tipo de infección que realice este malware [5]:

1. **Ransomware para bloquear el equipo**: en esta primera etapa este programa malicioso bloqueaba el acceso al sistema operativo del ordenador hasta que la víctima pagaba un rescate mediante el uso de un SMS que se enviaba a número de teléfono utilizado para realizar transferencias económicas [6].

   El uso del ransomware bloqueante era muy rentable hasta que los expertos en seguridad informática y las fuerzas policiales encontraron una forma de luchar contra esté problema atacando directamente a los pagos electrónicos que se efectuaban por teléfono. Los ciberdelincuentes vieron que este tipo de ataque pasó a tener mayor riesgo porque estos sistemas de pago podían ser rastreados por la policía y muchos de ellos comenzaron a ser detenidos y encarcelados [6].

2. **Ransomware para cifrar la información**: en esta segunda etapa, el tipo de ransomware que se hizo popular fue el de cifrado debido a la aparición de las criptomonedas, en especial del *bitcoin [6]*.

   Las *criptomonedas* (en inglés *cryptocurrency*) o *criptodivisas* son una forma de realizar transacciones económicas de manera digital utilizando técnicas criptográficas que permiten aumentar la seguridad de dichas transacciones. Entre las características de estas monedas se encuentran que eliminan a los agentes financieros, como por ejemplo los bancos, para realizar este tipo de transacciones y aumentando el anonimato del intercambio económico entre los usuarios de este tipo de monedas [7]. Este anonimato es el que utilizan los ciberdelincuentes para solicitar el rescate, ya que estos saben que es más difícil de rastrear el pago que realizan las víctimas.

   Los ciberdelincuentes saben que los archivos privados de los usuarios y de las empresas son únicos en su mayoría y que en el caso de perderlos éstos no pueden ser recuperados fácilmente. Ese es el motivo de utilizar técnicas de cifrado para bloquear el acceso al contenido de sus archivos con claves robustas y que a cambio se solicite una gran cantidad de dinero por recuperarse [5].

   Durante un tiempo, el uso de los ransomware cifradores no fue tan amplio como el de los bloqueadores. Según el análisis realizado por la empresa de seguridad informática Kaspersky Labs [6], en el año 2015 comenzó a incrementarse el uso de este tipo de ransomwares, tal y como se puede observar en la gráfica de la figura 2.

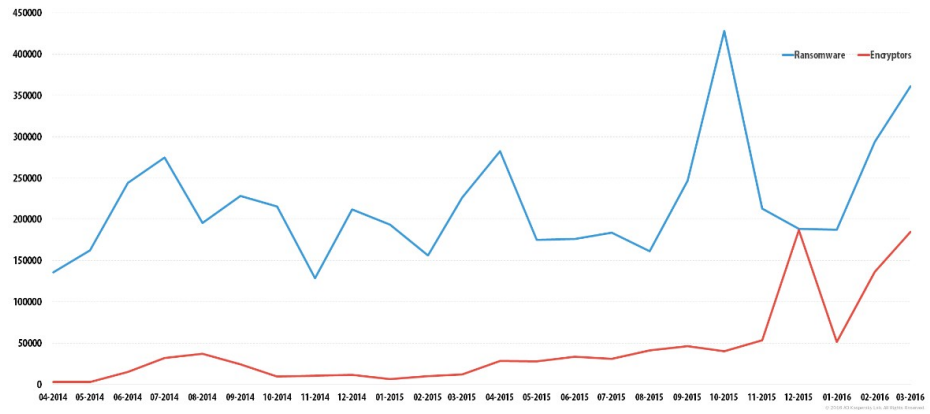


Figura 2:Comparativa del uso de tipos de ransomwares [6]. Imagen obtenida de Kaspersky Security Network [6].

2.1.3 Estado actual

Los primeros ransomwares eran simples con múltiples errores que permitían a los expertos en seguridad informática crear herramientas que descifrasen los archivos o desbloqueasen los equipos infectados. Con el paso del tiempo las amenazas comenzaron a ser más complejas y difíciles de desinfectar [2].

El ransomware habitualmente cifra la información de todas las unidades instaladas en el equipo, sean locales o mapeadas con otros equipos. La infección por el ransomware es más crítica cuando afecta a un servidor de archivos o al sistema encargado de realizar las copias de seguridad porque se cifrarán los ficheros originales y sus copias de seguridad [3].

En los primeros ransomwares los desarrolladores escribían su propio código de cifrado. En la actualidad, los ciberdelincuentes utilizan las librerías públicas de cifrado que poseen los algoritmos criptográficos, como AES o RSA, que incrementan la dificultad de descifrar los ficheros afectados y haciendo que los ataques sean más peligrosos y dañinos [2]. Con estas técnicas el cifrado realizado por este programa malicioso suele ser imposible de revertir porque se utilizan algoritmos de cifrado de clave simétrica y asimétrica y cada fichero se cifra con una clave diferente [3].

Otras diferencias que existen con los primeros ransomwares es que los vectores de infección se vuelven también más complejos porque estos utilizan campañas de *phishing dirigido* en vez de utilizar el envío de correo masivo que suele ser bloqueado por los *filtros antispam* de los *cortafuegos de correo* [2].

La cantidad de campañas de ataque relacionadas con el ransomware está reduciéndose en la actualidad, pero estos ataques están creciendo

en sofisticación. Hoy en día, los cibercriminales prefieren utilizar otro tipo de malware como son los *cryptominers* y/o los troyanos bancarios [9].

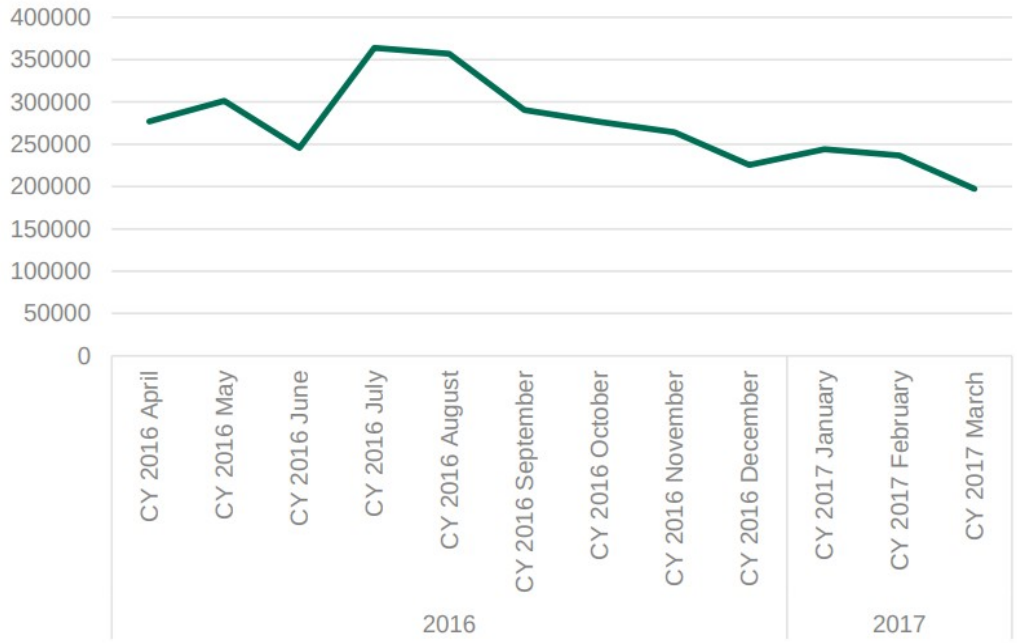


Figura 3: Número de equipos infectados por ransomware como mínimo una vez entre abril del 2016 y marzo del 2017 [9].

Según Karspersky Labs, el número de equipos infectados por el ransomware se ha reducido en un 30% entre los años 2016 y 2018 mientras que el uso de cryptominers ha aumentado en un 44,5% [10].

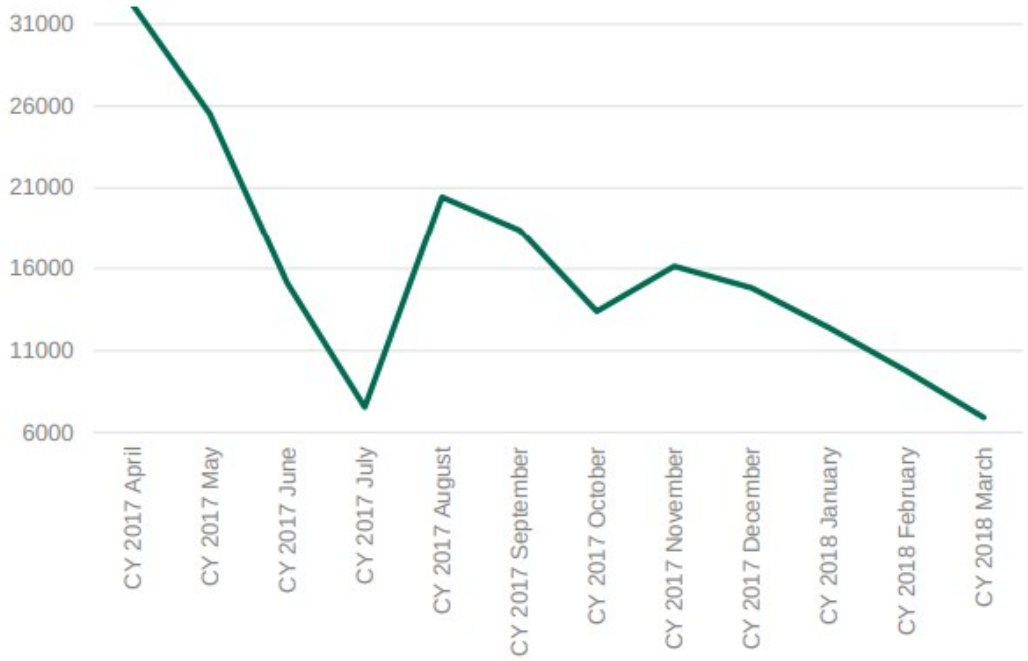


Figura 4: Número de teléfonos móviles infectados como mínimo una vez por ransomware entre abril del 2017 y marzo del 2018 [9].

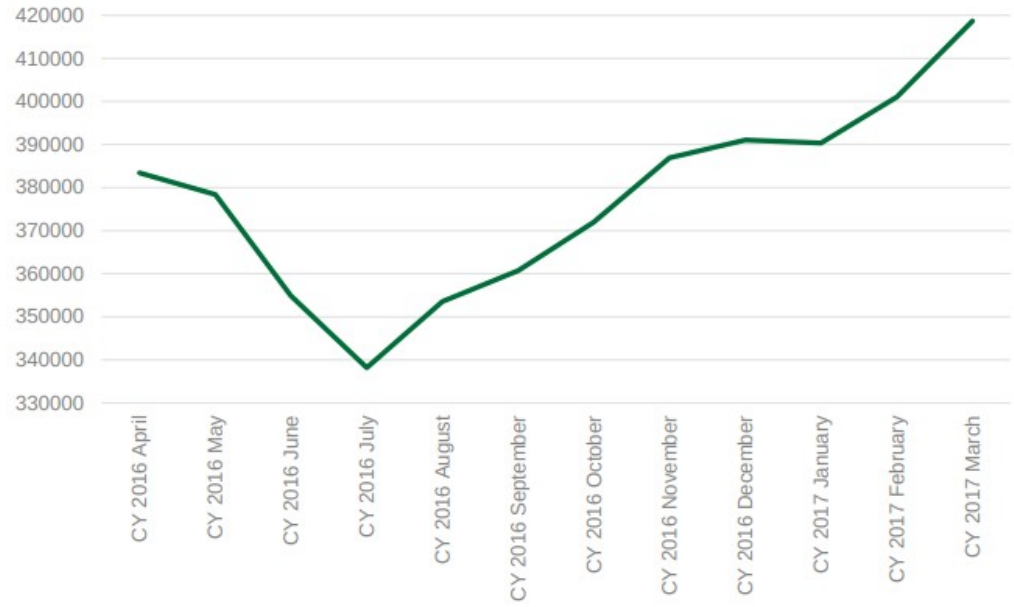


Figura 5: Equipos infectados como mínimo una vez por cryptominers entre abril del 2016 y marzo del 2017 [9].

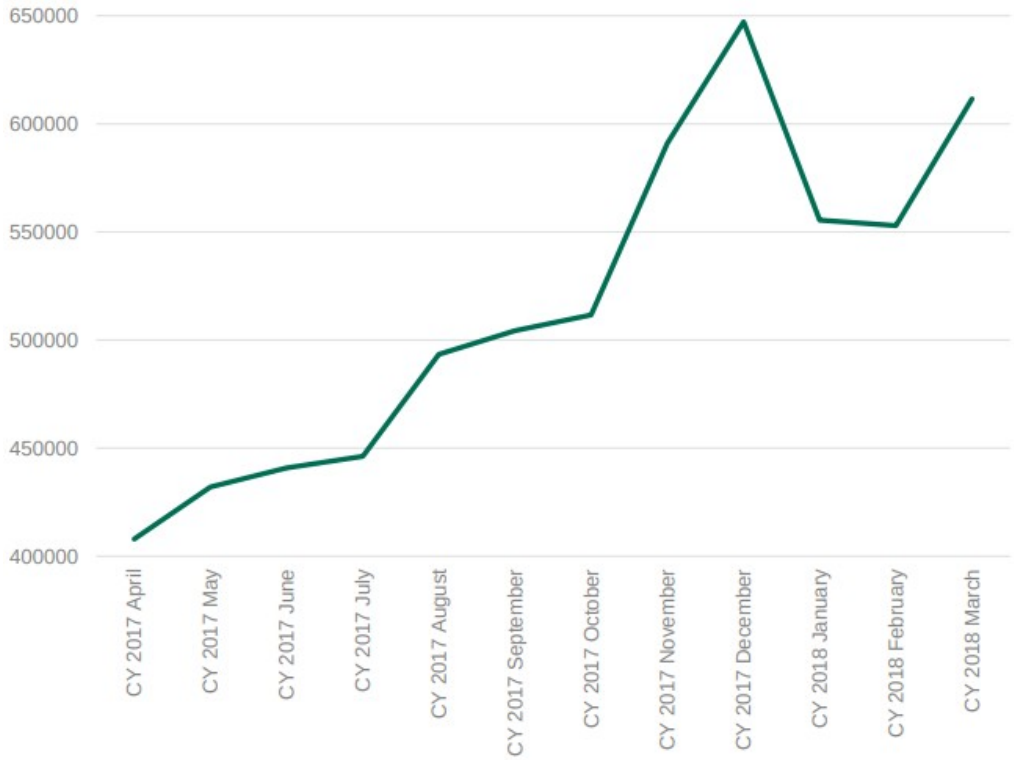


Figura 6: Equipos infectados como mínimo una vez por cryptominers entre abril del 2017 y marzo del 2018 [9].

Entre los factores que provocan que el uso del ransomware haya disminuido se encuentran que los usuarios cada vez están más concienciados y el aumento de la volatilidad de las criptomonedas, pero esto puede ser algo temporal, ya que un estudio realizado por la empresa de seguridad Malwarebytes revela que el uso de los cifradores

de monedas también se esta reduciendo [11], tal y como se puede observar en la siguiente gráfica.

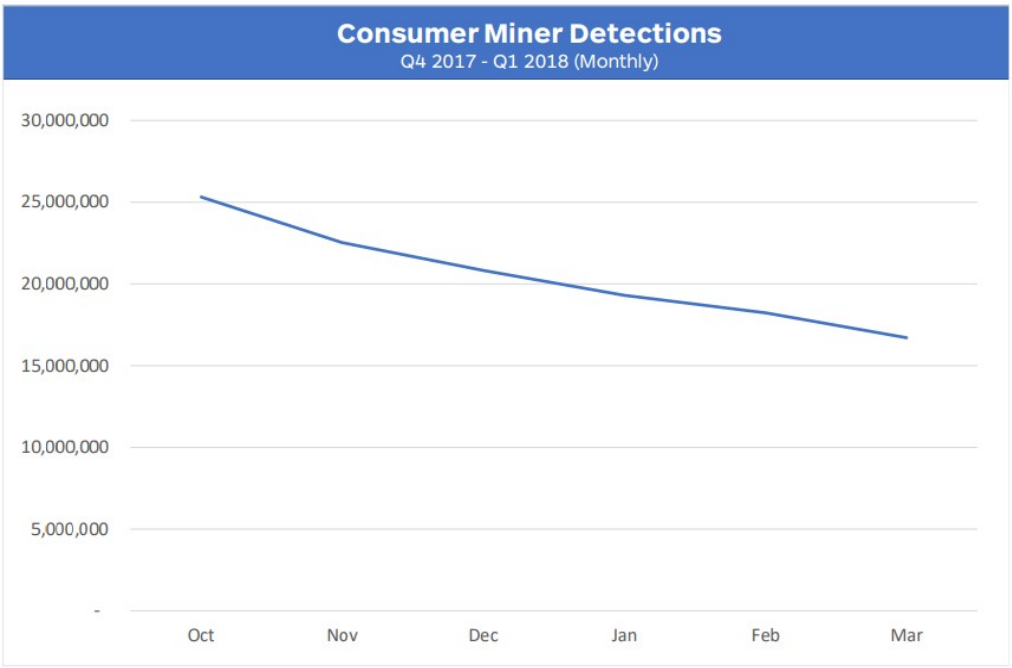


Figura 7: Detecciones de cryptominers [11].

Si comparamos el precio del Bitcoin y otras criptomonedas podemos ver que el precio de éstas se ha reducido en el año 2018, por lo que es posible que éste sea el factor que haya hecho que el uso de los crytominers se esté reduciendo [10].

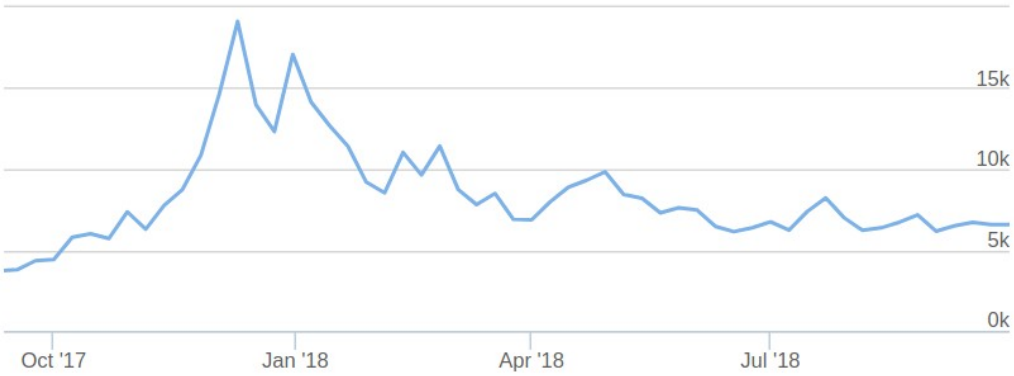


Figura 8: Precio del Bitcoin entre octubre del 2107 y octubre del 2018. Gráfica obtenida en el siguiente enlace del brocker Plus500: https://www.plus500.es/Instruments/BTCUSD

Según el informe "*2018 Internet Security Threat Report*" realizado por la empresa de seguridad Symantec, en el año 2017 el número de familias relacionadas con el ransomware se redujo un 71% mientras que su número de variantes se incremento un 46%. Esto datos dan a entender que las campañas de ransomware que estaban activas sacaban cada

vez más muestras, es decir, existen menos actores pero estos producen más variantes que antes [12].

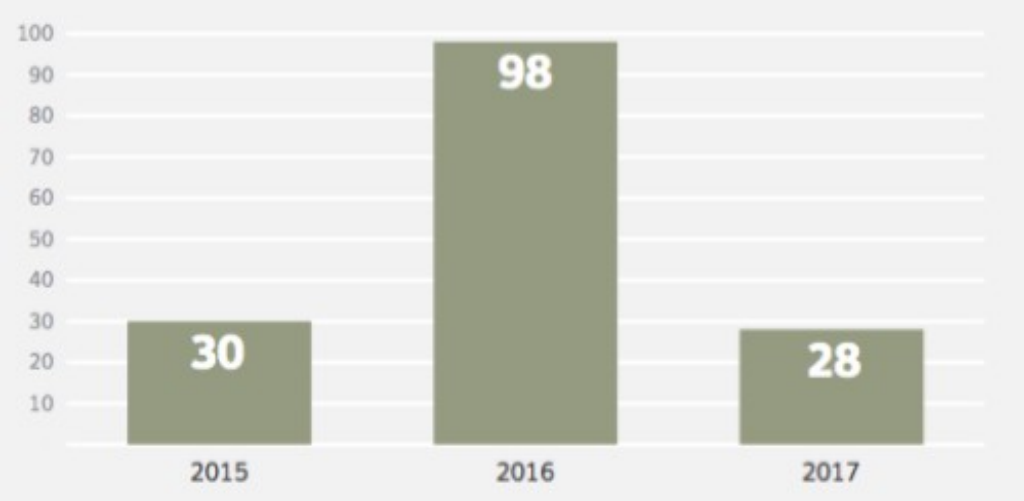


Figura 9: Familias de nuevos ransomwares entre 2015 y 2017 [10].

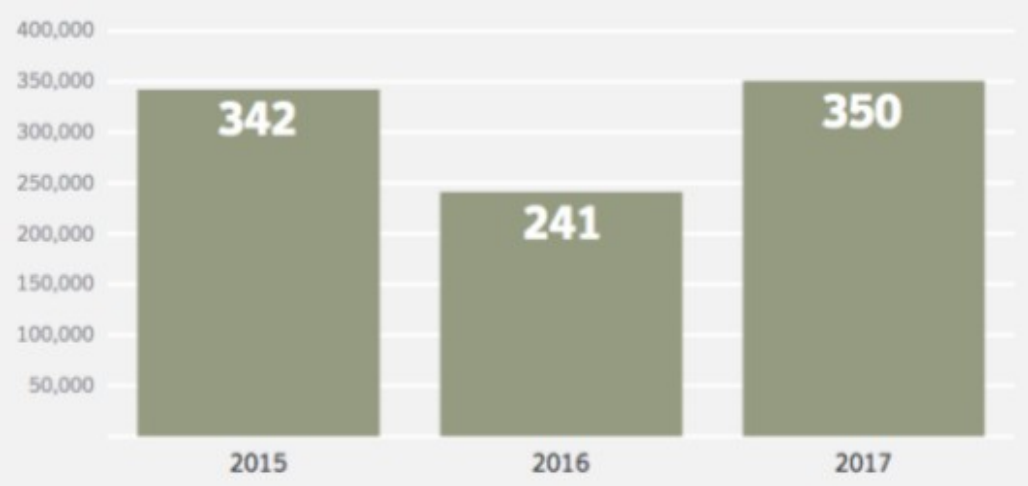


Figura 10: Nuevas variantes de ransomwares entre 2015 y 2017 [10].

Estos datos indican que es posible que el uso de los crytominers este disminuyendo y que los ciberdelincuentes vuelvan a utilizar el ransomware ya que estos ofrecen una forma de enriquecerse más rápida que los primeros [10].

2.1.4 Futuro del ransomware

En el año 2016, con el ransomware Cerber, los cibercriminales encuentran una nueva forma de negocio ofreciendo este programa malicioso como un servicio. Este servicio se conoce como RaaS, siglas del inglés que significan *Ransomware as a Service*. En estos momentos, cualquier ciberdelincuente con conocimientos básicos en informática que contrate este servicio puede realizar un ataque con este malware que afecte a múltiples organizaciones y/o usuarios en cualquier parte del

mundo [13]. Es posible que en el futuro se incremente esta modalidad de servicio porque los ciberdelincuentes encuentran un nicho de mercado nuevo ofreciendo ransomwares a personas sin conocimientos técnicos en la materia pero que quieren hacer daño.

Con el creciente aumento de la tecnología relacionada con los dispositivos *Internet of Things*, en adelante dispositivos IoT, es posible que los cibercriminales comiencen a encontrar un nuevo mercado con el uso de este programa malicioso. Pensemos que cada vez estamos conectando nuestras casas, coches o relojes a Internet y que el bloqueo del acceso a estos dispositivos puede hacer que paguemos los rescates que solicitan los ciberdelincuentes por afectar directamente a nuestra vida diaria [14]. Este tipo de ransomwares que afectan a los dispositivos IoT se conocen con el nombre de ROT, de las siglas en inglés *Ransomware of Things* o en español Ransomware de las Cosas.

Otro ataque preocupante es que existan nuevos objetivos relacionados con las infraestructuras críticas. En la conferencia de ciberseguridad RSA que tuvo lugar en el año 2017, Neil Jenkins, director de la oficina de administración del Departamento de Seguridad Nacional de los Estados Unidos, expuso su preocupación sobre que el ransomware empezase a apuntar a infraestructuras críticas pudiendo bloquear, por ejemplo, sistemas de control de empresas de agua. Además puso como ejemplo el ataque exitoso que se realizó a un hotel austriaco donde se bloquearon las tarjetas de acceso de las puertas del hotel [15].

2.2 Familias y variantes del ransomware

El ransomware, como herramienta de uso criminal, adopta multitud de formas. Hemos visto en el punto “2.1.2 Historia del ransomware” como este malware ha ido evolucionando y se ha ido modificando para ganar sofisticación y capacidad de destrucción. En la siguiente imagen, podemos ver una línea temporal que realizó la empresa de seguridad informática F-Secure en el año 2017 que muestra claramente como, a medida que pasa el tiempo, se ha ido expandiendo el número de variantes del ransomware.

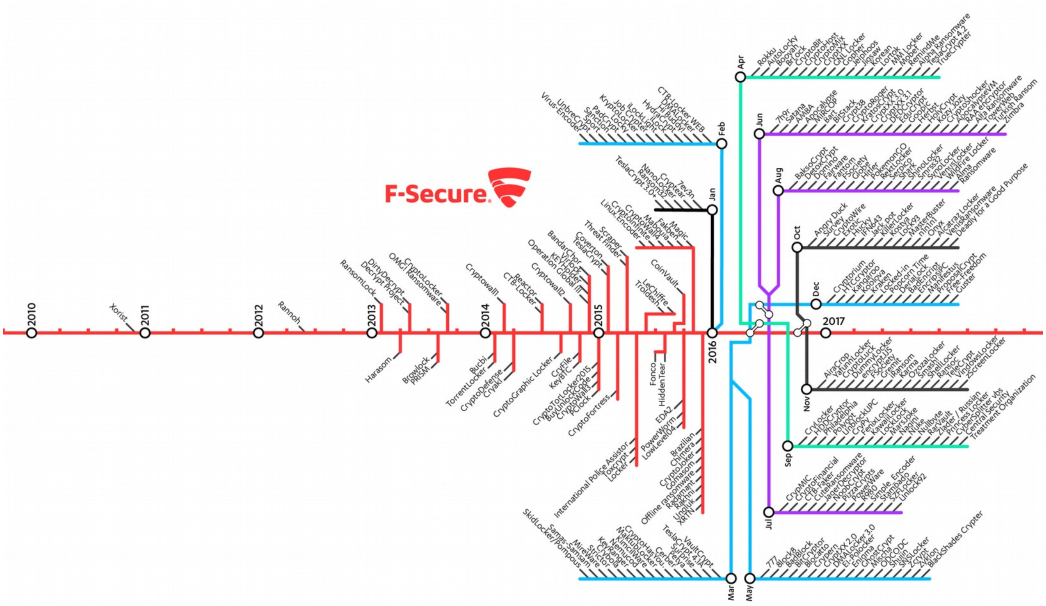


Figura 11: Línea temporal de los ransomwares [64].

En este apartado del estudio vemos las familias en las que se pueden agrupar los ransomwares y describimos, de todas las variantes que se han detectado, aquellas que por sus características o comportamiento se diferencian de los demás o introducían una nueva forma de actuar, de esta forma podemos conocer mejor cómo actúa este tipo de malware.

2.2.1 Familias de ransomware

Principalmente existen dos familias de ransomwares según la técnica que utilizan para impedir el acceso a los sistemas y extorsionar a sus víctimas:

1. **Ransomware *Lockscreen*** *[16]*: este tipo de ransomwares se caracterizan por vetar el acceso al equipo utilizando una pantalla de bloqueo, la cual imposibilita realizar cualquier actividad sobre el sistema. Esta pantalla suele mostrar un mensaje donde se le indica al usuario que ha sido infectado y se le pide el pago de una cantidad de dinero a cambio de recuperar el acceso.

Este tipo de ransomware no cifra los ficheros y la información se puede recuperar si se puede acceder al disco duro. Este programa malicioso suele utilizar técnicas de ingeniería social para engañar al usuario y hacer que éste pague.

2. **Ransomware *Criptolockers*** *[16]*: este tipo de programas maliciosos se diferencian de los anteriores porque en la infección se utilizan algoritmos de cifrado para impedir el acceso a los archivos almacenados en los equipos de los usuarios. Se suelen cifrar archivos ofimáticos y multimedia del equipo del usuario afectado. En este caso, solo conocen la clave de descifrado los cibercriminales y si la víctima quiere recuperar sus ficheros descifrándolos ha de pagarles una cantidad económica por el rescate.

   Cuando el proceso de cifrado de los ficheros termina, se le muestra al usuario una pantalla donde se le indica los pasos a seguir si quiere recuperar su información cifrada.

A continuación se describen las principales variantes de ransomware detectadas hasta nuestros días ordenadas de forma cronológica.

2.2.2 Variantes de ransomware

Troyano AIDS o PC Cyborg (1989)
El primer ataque del ransomware conocido ocurrió en 1989 en la industria médica. El doctor investigador del SIDA, Dr. Joseph Popp, distribuyó 20.000 disquetes en 90 países dirigidos a otros investigadores cuyo contenido supuestamente era un programa que media la probabilidad de que una persona se infectase con el SIDA, pero lo que realmente contenía era el troyano AIDS [17].

El troyano utilizaba una aplicación de encuestas que funcionaba como la víctima esperaba, pero en realidad, lo que se ejecutaba era el malware. Este troyano sustituía el script *Autoexe.bat* con código malicioso, el cual contaba el número de veces en el que el equipo arrancaba y, cuando llegaba a las 90 veces, el equipo de la víctima sufría el cifrado de datos y el bloqueo del equipo. Momento en el cual, se le mostraba al usuario un mensaje de rescate que indicaba el nombre de los archivos y directorios que se habían cifrado junto con la solicitud del pago de 189 dólares americanos si quería recuperar sus ficheros mediante la clave de descifrado. Esta pago por el rescate se realizaba enviando un cheque dirigido a la empresa falsa “PC Cyborg Corporation” que creó y que tenía una dirección postal en Panamá [17].

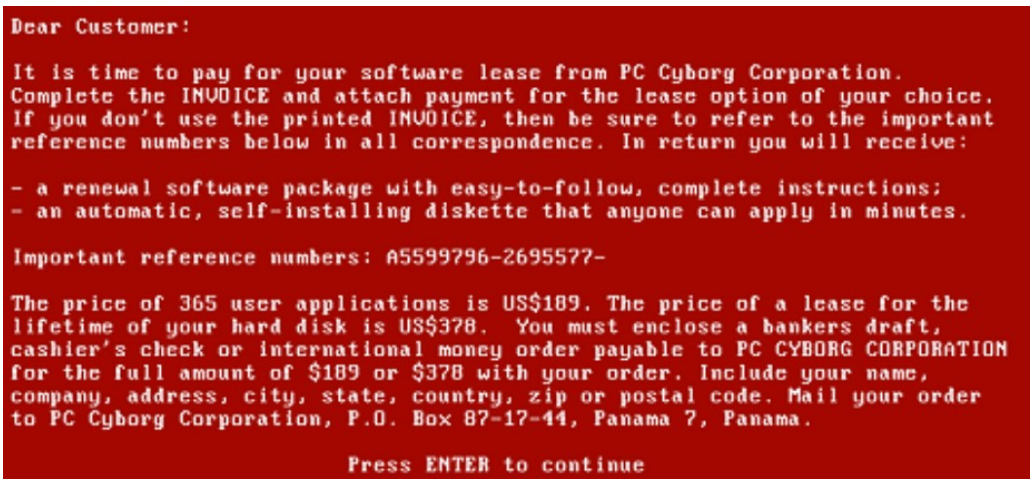


Figura 12: Mensaje de aviso del troyano AIDS [8].

No se conoce cuáles fueron las motivaciones exactas que llevaron al Dr. Joseph Popp a programar este troyano aunque, parece ser, que su motivación principal fue que le rechazaron para un puesto en la Organización Mundial de la Salud [18].

Este troyano tenía una serie de defectos en su programación. El troyano utilizaba una clave simétrica para cifrar el contenido de los archivos. La característica del cifrado simétrico es que se utiliza la misma clave en el proceso de cifrado que en el de descifrado y ésta se encontraba escrita en su propio código fuente, por lo que el cifrado de los ficheros era muy fácil de romper y surgieron múltiples herramientas que permitían recuperar los archivos [19].

Archievus (2005)

Después de más de una década apareció este ransomware cuya característica principal es que utilizaba cifrado RSA de 1024 bits. Archievus solo cifraba el contenido de la carpeta “Mis documentos” de Windows por ser el directorio configurado por defecto por la mayoría de usuarios para almacenar sus ficheros. Este ransomware dejaba un archivo de texto "INSTRUCTIONS HOW TO GET YOUR FILES BACK.txt" con las instrucciones para realizar el rescate. En este caso, los usuarios podían seguir utilizando el equipo [14].

Figura 13: Ficheros creados por el ransomware Archiveus [21].

Para recuperar los ficheros cifrados las víctimas tenían que acceder a una web y comprar una contraseña de 30 carácteres muy difícil de romper [14].

GPCoder (2005)
Este ransomware se detectó entre el año 2005 y junio del 2006 y fue uno de los primeros casos en los cuales se utilizó Internet para distribuirse. La infección consistía en cifrar con el algoritmo RSA de 1024 bits múltiples archivos con diferentes extensiones que se encuentran almacenados en los sistemas operativos Windows y, posteriormente, mostraba en la pantalla de inicio un mensaje que señalaba a un documento de texto ".txt" con los pasos a seguir para realizar el rescate [14].

Figura 14: Mensaje de que muestra GPGCoder después del cifrado[21].

Este malware utilizaba correos de phishing relacionados con una solicitud de trabajo. Estos correos tenían un adjunto que parecía una aplicación ayudar a encontrar trabajo pero en realidad engañaba a los usuarios e infectaba sus equipos [20].

Krotten (2005)
El ransomware Krotten se hacia pasar por un programa para generar códigos de recarga de los teléfonos móviles. Este programa estaba alojado en una página web rusa y se podía obtener de forma gratuita. Esta página engañaba a los usuarios indicándoles que el generador de claves estaba desarrollado por hackers ucranianos y que funcionaba al 100% para casi todos los proveedores de servicios de telefonía móvil de Ucrania. Cuando el usuario ejecutaba el programa generador de claves para recargar su teléfono móvil se ejecutaba el ransomware y se infectaba [23].

Cryzip (2006)
La característica principal de este ransomware es que utilizaba la compresión de ficheros utilizando archivos ZIP protegidos con contraseña. Los pasos que seguía este ransomware una vez infectaba el equipo son [22]:

1. Cuando este ransomware se ejecutaba buscaba múltiples extensiones de ficheros tanto en los discos duros del sistema como los discos “UNKNOWN” y en los CD-ROM.

2. Posteriormente creaba un fichero que seguía la estructura siguiente: *[Nombre de archivo cifrado]_CRYPT_.zip*.

3. Los archivos comprimidos los protegía con la contraseña "C:\ Program Files\Microsoft Visual Studio\VC98". Tiempo después se vio que la debilidad de este ransomware es que siempre utilizaba esta contraseña para cifrar [21].

4. Luego creaba el archivo de texto “AUTO_ZIP_REPORT.txt” que contenía las instrucciones para recuperar la clave de descifrado.

WinLock (2011)
Este ransomware fue el primero que marcó una nueva tendencia en la infección de los equipos ya que fue el primero que bloqueaba el equipo imposibilitando al usuario acceder a éste hasta que las víctimas comprasen la clave de desbloqueo [14]. Además, este mensaje engañaba a los usuarios indicando que tenía que volver a activar su clave de Windows y que para ello debían de llamar a un número de teléfono, supuestamente gratuito, para volver a activarlo. Este número de teléfono realmente era un número de tarificación especial cuyo pago iba destinado a las arcas de los cibercriminales [14].

Dorkbot (2011)
Dorkbot no solo cifraba los archivos del equipo infectado, sino que además hacia que el equipo pasase a formar parte de una *botnet* controlada mediante el uso del protocolo IRC (de las siglas en inglés *Internet Relay Chat*) el cual le permitía a los ciberdelincuentes poder realizar ataques de Denegación de Servicio, robar credenciales de algunas páginas web, utilizar el equipo para realizar ataques de phishing o incluso podía descargarse y ejecutar otros programas maliciosos en el equipo [24].

Este ransomware se propagaba utilizando múltiples canales como memorias extraíbles USB, redes sociales, SPAM y herramientas de chat como el *Messenger* o *Skype* [25].

Toda la actividad maliciosa que realizaba era transparente para los usuarios. Este ransomware estuvo activo durante cinco años [25].

Reveton (2012)
El ransomware Reventon tuvo mucho éxito y se propago por múltiples países. Debido al mensaje que mostraba también fue conocido como el "Virus de la policía".

Este ransomware bloqueaba el ordenador y luego engañaba a las víctimas con un mensaje falso de la policía del país al que pertenece que le indicaba que su equipo estaba siendo utilizado para actividades ilegales como descargar musica, programas piratas o poseer pornografía infantil y que por ello debían de pagar una multa como fianza. El pago se realizaba en una cuenta anónima de Paysafecarf o Ukash [26].

Para reforzar el engaño, el mensaje de advertencia mostraba datos del equipo infectado como su dirección IP, su país o la ciudad a la que pertenece [26].

Figura 15: Mensaje falso de la policía que del ransomware Reventon [19].

Cryptolocker (2013)
La característica principal de este ransomware y que los diferencia de los anteriores es que es el primero en utilizar Bitcoins como moneda de pago para solicitar los rescates [67].

Este ransomware engaña al usuario utilizando técnicas de ingeniería social. En concreto, el usuario recibe un correo electrónico de una empresa de correspondencia indicándole que tiene un paquete que no se le ha podido entregar y que para ello ha de pinchar sobre un enlace. En el momento que la víctima pincha, accede a un portal falso de una empresa de logística y desde este portal se descarga un fichero ZIP que contiene un falso documento PDF que en realidad es el malware. Cuando el usuario abre el PDF se infecta con el ransomware [27].

Una vez el ransomware se ha ejecutado y cifrado los ficheros del equipo, se le muestra al usuario una pantalla con las instrucciones del rescate y

dando un tiempo máximo para pagar antes de destruir la clave que permite descifrar los archivos [27].

Figura 16: Mensaje que muestra Cryptolocker [68].

El uso de CryptoLocker descendió cuando se puso fin a la *botnet Gameover Zeus* en 2014 [14].

CryptoWall (2014)
La característica principal de este ransomware y que los diferencia de los anteriores es que es el primero en utilizar la *red TOR* para solicitar los rescates [43].

CryptoWall es un ransomware bloqueador cuya vía de infección es el envío de un email malicioso que mediante un enlace se realiza la descarga del programa malicioso [29].

Este ransomware cifra los documentos del equipo del usuario con el algoritmo criptográfico RSA de 2048 bits y solicita un rescate de 500 $ por ellos [29]. Una vez cifrados los documentos, este malware crea los archivos DECRYPT_INSTRUCTION.txt, DECRYPT_INSTRUCTION.html y DECRYPT_INSTRUCTION.url en todas las carpetas donde haya actuado [29].

Se calcula que en el año 2015 los cibercriminales obtuvieron aproximadamente 325 millones de dolares con este programa malicioso [14].

SimplLocker (2014)
La característica principal de este ransomware es que es el primero que esta destinado a infectar dispositivos con el sistemas operativo Android. Cuando este ransomware infecta el dispositivo, escanea la tarjeta SD y

cifra todos los archivos de un cierto tipo para luego solicitar un rescate por ellos [30].

Al igual que el resto de ransomwares, éste muestra un mensaje en el terminal móvil escrito en ruso y solicitando el pago en monedas ucranianas, por lo que es muy probable que este ransomware estuviese dirigido a los habitantes de este país. De forma muy similar al ransomware Reventon, este mensaje utiliza ingeniería social para engañar a la víctima informándole que su dispositivo ha sido bloqueado por distribuir pornografía infantil, zoofilia y otras perversiones y que es necesario pagar 260 UAH (aproximadamente 18 Euros) si se desea desbloquear el dispositivo [30].

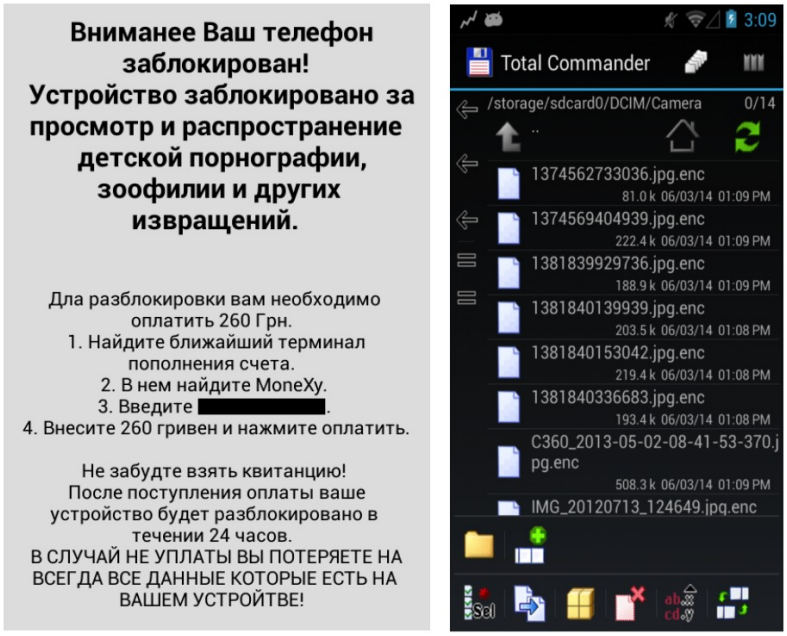


Figura 17: Mensaje que muestra Simplocker y archivos infectados [30]

Sypeng (2014)

Al igual que SimplLocker, es considerado uno de los primeros ransomware para dispositivos Android que bloqueaba las pantalla de los terminales. Este engañaba a los usuarios con un mensaje falso del FBI y solicitaba una cantidad económica de 200 dólares por el rescate. Este ransomware se propagaba mediante actualizaciones falsas de Adobe Flash [31].

Koler (2014)

Este ransomware también estaba pensado para infectar dispositivos Android. Koler fue el primer ransomware que utilizaba técnicas de malware del tipo *gusano informático* para infectar a otros dispositivos. La forma de propagarse que tenía era enviar mensajes personalizados a los contactos almacenados en el teléfono móvil infectado e intentaba engañar al resto de usuarios para que pinchasen en el enlace malicioso que se descargaba el ransomware [31].

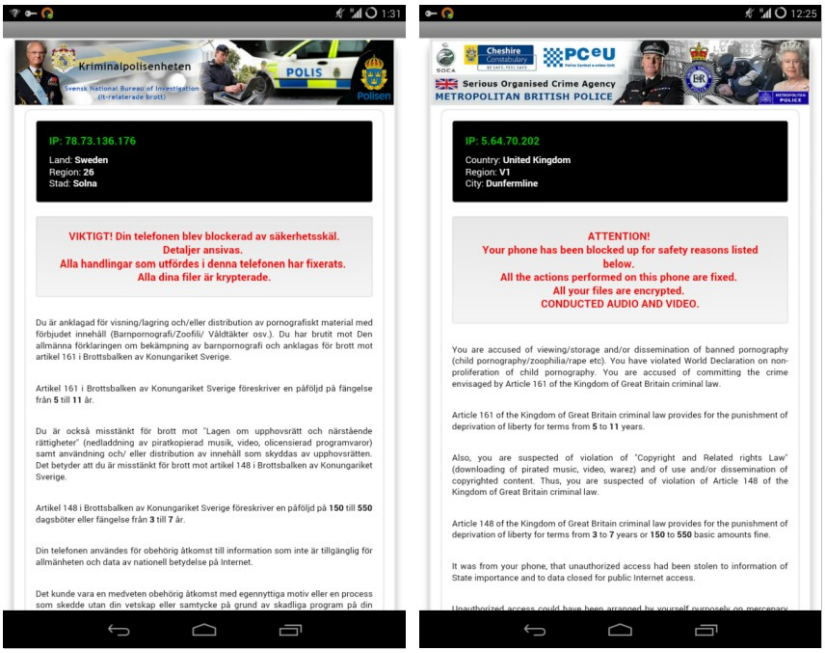


Figura 18: Mensajes de muestra de Koler [32]

Synolocker (2014)

La principal característica de este ransomware es que el destino de sus infecciones eras dispositivos NAS (de las siglas en inglés *Network Attached Storage*) de almacenamiento en red de la marca taiwanesa Synology Inc. Parece ser, que el malware aprovecha una vulnerabilidad del dispositivo que la fábrica Synology aún no ha corregido [33].

Este ransomware cifra cada uno de los archivos guardados en el NAS y modifica la página web de administración con un mensaje que solicita el pago del recate de 0.6 Bitcoins utilizando la red TOR [33].

Este programa malicioso también deshabilita el acceso al dispositivo utilizando *SSH* y *Telnet* [33].

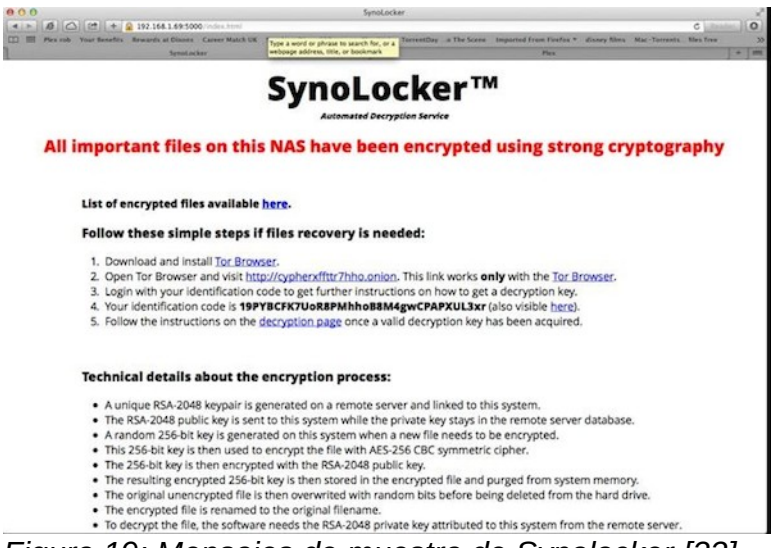


Figura 19: Mensajes de muestra de Synolocker [33]

Hidden Tear (2015)
Este ransomware se caracteriza porque es el primer ransomware de código libre y se distribuye solo para fines educativos. Este programa está desarrollado por el experto turco en seguridad informática Utku Sen [34].

Sus principales características son [34]:

1. Cifra los ficheros con el algoritmo AES.
2. Muestra un mensaje a la víctima cuando acaba con la infección.
3. Envía la clave de cifrado a un servidor remoto.
4. Genera un archivo de texto con las instrucciones del rescate.
5. No se conecta a la red TOR y no pide Bitcoins por el recate.
6. Se puede descargar desde el repositorio de código GitHub.

En el año 2016, la empresa Karspersky detectó que existían 24 variantes basadas en este ransomware. GitHub eliminó de su repositorio el código de este ransomware, pero muchos de los usuarios que se lo descargaron lo han vuelto a subir a la plataforma y es prácticamente imposible de eliminar [35].

Su creador se arrepiente de haber hecho público este malware y asegura que no tenía ninguna mala intención cuando lo creó [35].

Vaultcrypt (2015)
Este ransomware renombra los ficheros que cifra con la extensión ".vault" y deja una nota con las instrucciones de pago. Es un ransomware destinado principalmente a usuarios de Rusia porque el mensaje de solicitud del rescate está escrito en Ruso [36].

La forma de actuar de este ransomware es que el usuario recibe un correo con un adjunto que es un archivo JS que cuando el usuario lo abre, se ejecuta el ransomware en segundo plano. Posteriormente, Vaultcrypt escanea el equipo en busca de ficheros con una determina extensión y los cifra utilizando la herramienta de cifrado de código libre GnuPG con RSA de 2048 bits. Luego deja una nota de texto en formato ".txt" solicitando el rescate [36].

TeslaCrypt (2015)
Este ransomware se diferencia de los demás en que iba destinado a jugadores de PC, ya que para cifrar no buscaba archivos ofimáticos o multimedia como el resto de ransomwares, sino que buscaba archivos relacionados con los juegos como partidas guardadas, mapas o perfiles del jugador. Posteriormente, se detectó una versión que además buscaba archivos ofimáticos [37].

Una vez cifra los ficheros, muestra un mensaje solicitando en Bitcoins 500 dólares por la clave de descifrado. Según los analistas, comparte características con Cryptolocker pero parece que no pertenece a los

mismos cibercriminales por que la implementación del código no es la misma [37].

Figura 20: Mensaje de TeslaCrypt [38].

Chimera (2015)

Este ransomware se diferencia de los demás en que utiliza enlaces de Dropbox en los cuerpos de los correos electrónicos relacionados con campañas de phishing dirigido a trabajadores específicos con ofertas de trabajo personalizadas [39].

Una vez el usuario se descarga el programa malicioso, alojado en Dropbox y lo ejecuta, se cifran los archivos del equipo y de las unidades de red. Posteriormente, cuando el usuario reinicia el equipo se le muestra el mensaje de la figura 21.

Figura 21: Mensaje del ransomware Chimera [39].

Otra diferencia adicional de este ransomware es que si no se paga la cantidad solicitada para el rescate, los cibercriminales amenazan a las víctimas con publicar en Internet la información obtenida [39].

Tox (2015)
Tox es una herramienta que permite crear un ransomware "a medida" con tres sencillos pasos. Para crear este ransomware hay que acceder a una página web alojada en la *Deep Web* e indicar: la cantidad en Bitcoins que queremos pedir por el rescate, el mensaje y la dirección para realizar los pagos. Los ciberdelincuentes creadores de este malware se quedan un 30% de cada rescate que se lleve a cabo [40].

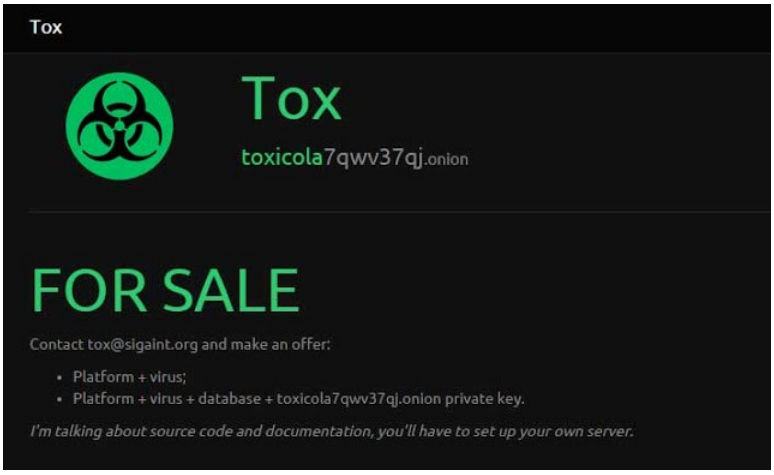


Figura 22: Anuncio relacionado con el negocio de Tox [40]

Este ransomware, una vez compilado, ocupa 2 MB y tiene una extensión ".src". Este malware cifra los programas usando el algoritmo AES y renombra los ficheros con la extensión ".toxcrypt" [40].

Linux.Encoder.1 (2015)
Este ransomware está considerado el primer ransomware cuyo objetivo son los sistemas operativos Linux. Este programa malicioso utiliza una vulnerabilidad existente en Magento que es un sistema de administración de tiendas virtuales [57].

Cuando este ransomware se ejecuta cifra determinados tipos de ficheros almacenados en el equipo, en las unidades de red y en la unidades montadas. Para el cifrado utiliza clave pública con los algoritmo AES y RSA, donde la clave privada se almacena en los servidores de control del programa malicioso [57].

Keranger (2016)
La característica de este ransomware es que es el primero que sale para dispositivos Mac. La distribución de este programa malicioso se realizaba mediante una distribución falsa del cliente Transmission de *BitTorrent* compatible con Mac OS X. Los cibercriminales comprometieron la página web oficial de ésta herramienta sustituyendo

el programa oficial por este ransomware. Todos los usuarios que se descargaron e instalaron Transmision v.2.90 se infectaron [41].

El comportamiento de este ransomware es similar al resto. Una vez infecta el dispositivo Mac busca los documentos del usuario, se conecta a sus *servidor de Command & Control* a través de la red Deep Web y muestra un mensaje para el rescate. Este ransomware utiliza el algoritmo de cifrado RSA de 2048 bits con clave asimétrica [41].

Locky (2016)
El vector de infección que tiene este ransomware es un correo malicioso con un documento Word o Excel que simula ser una factura pero en realidad lo que hace es ejecutar una macro que se descarga el ransomware y lo ejecuta cifrando así los archivos de la víctima y además les añade la extensión ".locky". Locky se diferencia de los demás ransomwares en que para difundirse utiliza archivos ofimáticos con macros en vez de utilizar directamente un archivo ejecutable que instala el malware [44].

Ransom32 (2016)
La diferencia principal que tiene este ransomware es que es el primero que está desarrollado en el lenguaje JavaScript, permitiendo afectar así a diferentes sistemas operativos. Además este ransomware se ofrece como un servicio, donde los cibercriminales, mediante una consola de configuración, se registran, configuran los parámetros del ransomware, como por ejemplo se bloqueante o la cantidad de Bitcoins que se solicita por el rescate, y posteriormente se descargan el programa malicioso personalizado para que lo distribuyan donde quieran. Los creadores de este ransomware cobran un 25% de los ingresos de sus clientes [45].

Figura 23: Consola de configuración de Ransom32 [45].

Jigsaw o BitcoinBlackmailer (2016)
Este ransomware debe su nombre a que usa la imagen del personaje Billy de las películas de terror Saw en el mensaje del rescate para causar aun más malestar en la víctima [46].

La característica que le diferencia de los demás es la forma en que extorsiona a las víctimas, ya que este malware borra los ficheros de forma exponencial cada hora en la que no se haya realizado el pago por el rescate. Después de 72 horas los elimina todos y si se intenta reiniciar el equipo o matar el proceso elimina 1.000 archivos. Además, existe una versión que amenaza con publicar la información en Internet [46].

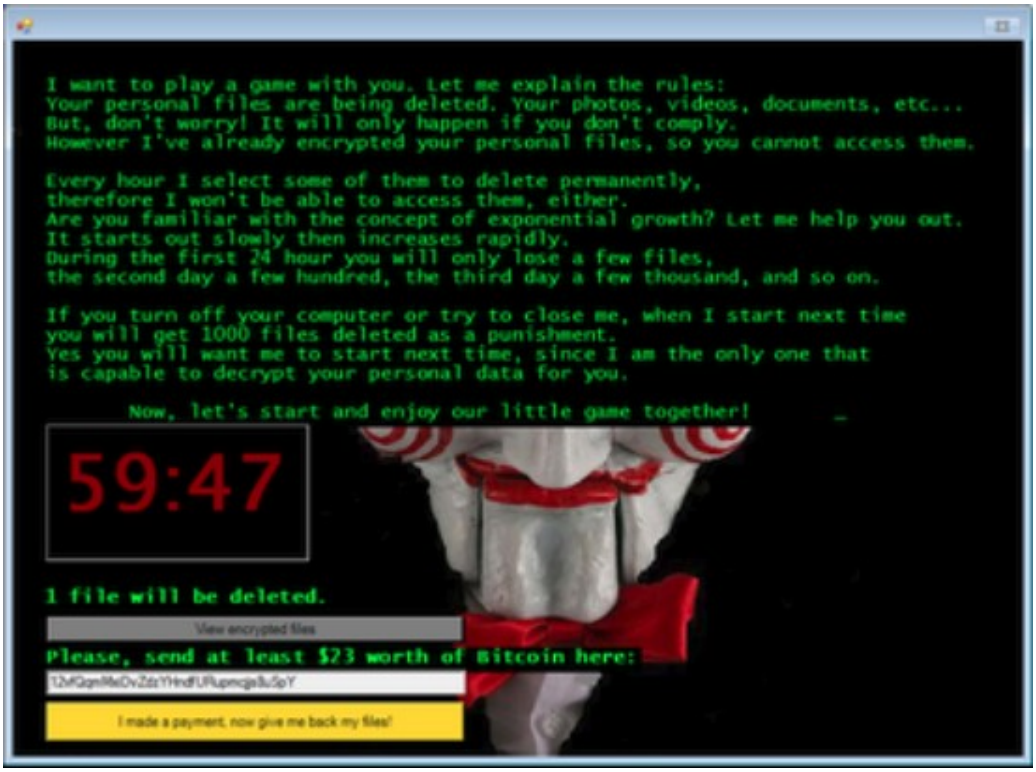


Figura 24: Mensaje de rescate del ransomware Jigsaw [46].

Petya y Mischa (2016)
La diferencia principal con el resto de ransomwares existentes hasta el momento es que éste, además de cifrar los archivos, se encarga de sobrescribir el Registro de Arranque Maestro (siglas en inglés MBR por su nombre *Master Boot Record*) cifrando la Tabla de Archivos Maestros (siglas en inglés MFT por su nombre *Master File Table*). Para consumar la infección, Petya necesita privilegios de administrador [47].

Para infectar a los sistemas, este ransomware utiliza Spear Phishing o Phishing Dirigido, ya que envía correos electrónicos personalizados y específicos a los departamentos de recursos humanos de las empresas que son objetivo de sus ataques. Estos correos tienen un enlace a Dropbox donde se supone que hay un currículum almacenado pero lo que contiene en realizad es el ransomware [47].

Otra diferencia con este ransomware es que utiliza un ransomware de respaldo, conocido como Mischa, para que si Petya, falla en la instalación y no consigue los privilegio necesarios, instalará Mischa que solo necesita privilegios de usuario cifrando así los archivos [47].

Frantic Locker o FLocker (2016)
Este ransomware es de especial interés porque además de poder bloquear dispositivos móviles Android es capaz de bloquear televisores "Smart TV" añadiendo así un nuevo objetivo para los ciberdelincuentes [48].

Este ransomware engaña al usuario haciéndose pasar por una aplicación que promete ver películas gratis. Una vez ha bloqueado el televisor, muestra un mensaje falso de la policía solicitando 500 dólares americanos por el rescate. A este ransomware también se le conoce como "Virus de la policía" por actuar de manera similar al ransomware Reveton [49].

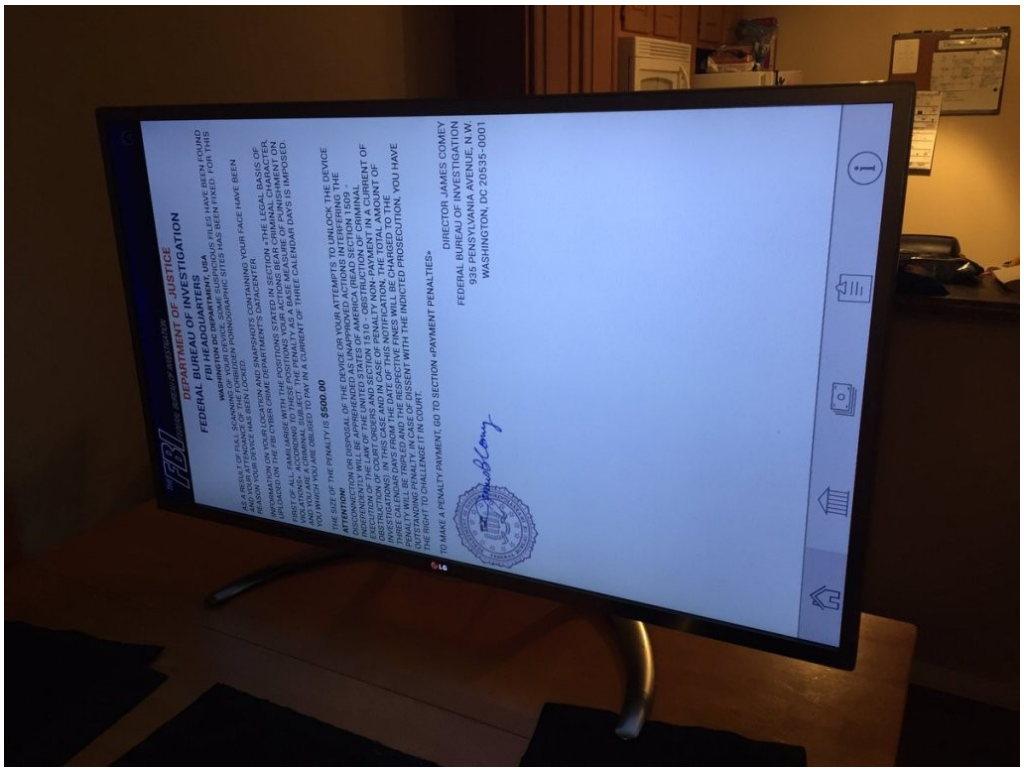


Figura 25: Televisor bloqueado por el ransomware FLocker [49].

PopcornTime (2016)
Este ransomware se diferencia en las opciones que da a la víctima para recuperar sus ficheros cifrados, ya que puede elegir entre pagar el rescate, mediante el pago de 1 Bitcoin, o proporcionarle personas a las que conoce para que sean infectadas enviándole un enlace malicioso. El mensaje de recate dice "Si dos o más personas instalan este archivo y pagan, descifraremos sus archivos de forma gratuita" [50].

Los creadores de este ransomware dicen que viven en la Siria devastada por la guerra y que el dinero del recate va destinado para pagar comida, medicinas y refugio para su gente. No hay forma de verificar si esta información es autentica [50].

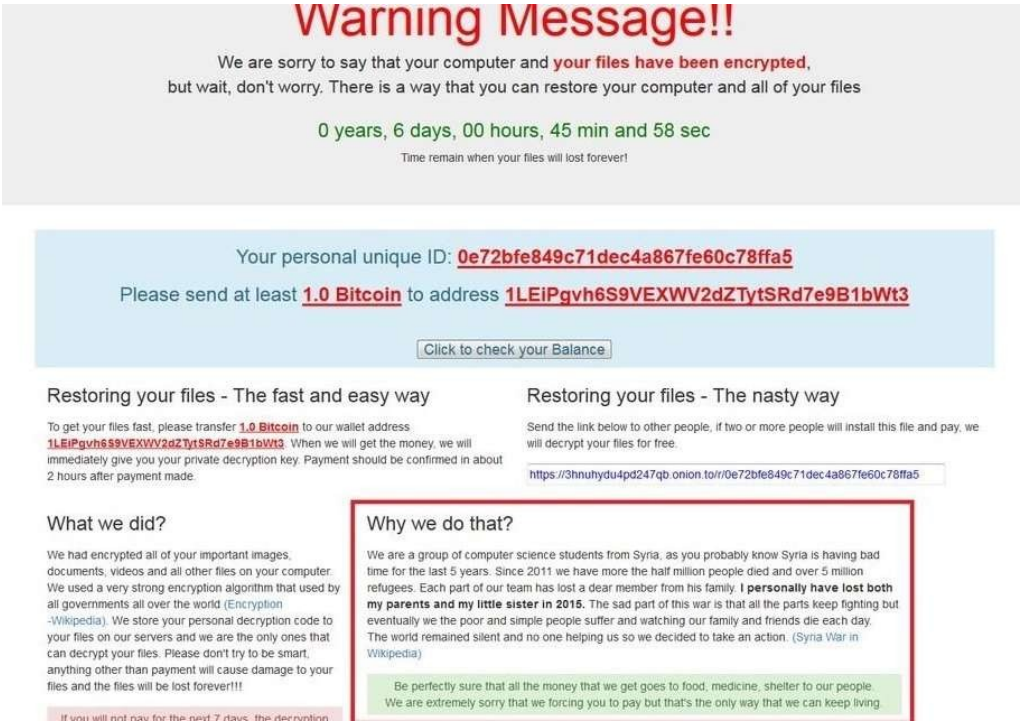


Figura 26: Mensaje de rescate del ransomware PopcornTime [50].

Kimcilware (2016)

La diferencia principal de este ransomware es que su objetivo no es cifrar equipos de usuario sino el de secuestrar servidores que alojan tiendas online. Los ciberdelincuentes buscan aprovecharse de de vulnerabilidades existentes en la plataforma Magento de creación de tiendas online o en el servidor que la aloja [53].

Este ransomware, una vez cifra el contenido de la tienda, añade a los ficheros afectados la extensión ".kimcilware" y crea su propio fichero "*index.html*" para que la página web siga funcionando [53].

Figura 27: Mensaje de rescate de KimcilWare [54].

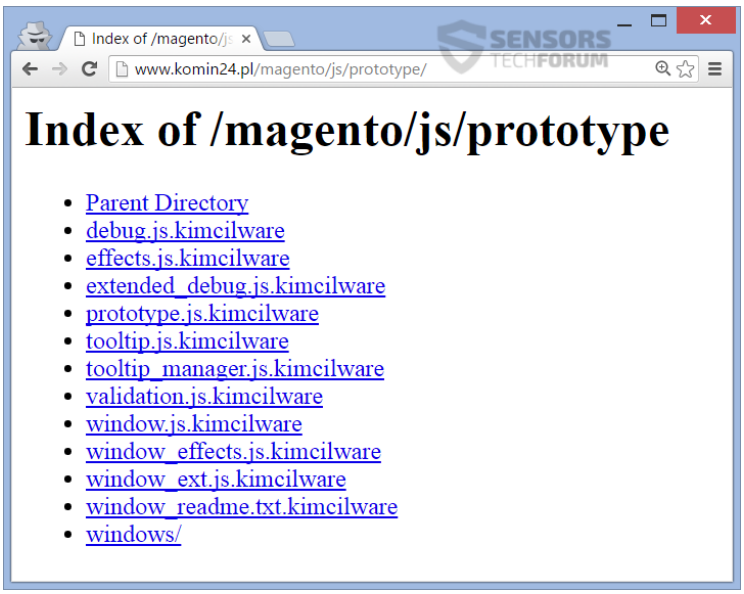


Figura 28: Ficheros cifrados por KimcilWare en servidor Web [54]

Cerber (2016)
Este ransomware utiliza pautas de comportamiento muy similares a las del resto de ransomwares, como por ejemplo que se propaga por el envio de correos fraudulentos, cifra los archivos del usuario y muestra un mensaje solicitando el rescate. Pero se ha decidido incluirlo en esta lista de variantes porque tiene una característica que lo diferencia de los demás y es que éste es capaz de emitir por los altavoces el mensaje en inglés: “¡Atención! ¡Atención! ¡Atención! ¡Sus documentos, fotos, bases de datos y otros archivos importantes se han cifrado!” [55].

WannaCry (2017)
Este ransomware se diferencia por el éxito de su ataque, ya que tuvo una afectación a escala mundial infectado aproximadamente a 141.000 equipos de múltiples empresas internacionales [51]. Este ransomware se estudia más a fondo en el apartado “2.8 Caso: Ataque WannaCry”.

Satanás (2017)
Este ransomware se diferencia de los demás en su modelo de negocio, ya que posiblemente sea el primero en ofrecer el servicio “Pago-por-uso” [52].

El servicio que ofrecen los desarrolladores de este ransomware incluye la creación de herramientas que ayudan a propagar su infección, como por ejemplo la creación de macros maliciosas para documentos ofimáticos o la creación de páginas web con aspectos inocente que cargue el ransomware [52]. Se profundiza más sobre el comportamiento de este ransomware en el apartado “2.4 Modelos de negocio”.

nRansom (2017)
Las diferencia de este ransomware con los demás es que no solicita dinero para rescatar los ficheros cifrados, sino que solicita son como

mínimo 10 fotos de la víctima desnuda. Estas fotos se envían a una dirección de correo electrónico y, una vez los cibercriminales verifican que las fotos pertenecen a la víctima y no están obtenidas de internet, le proporcionan, supuestamente, la contraseña de desbloqueo. El objetivo de este ataque es vender estas fotos en la Deep Web [56].

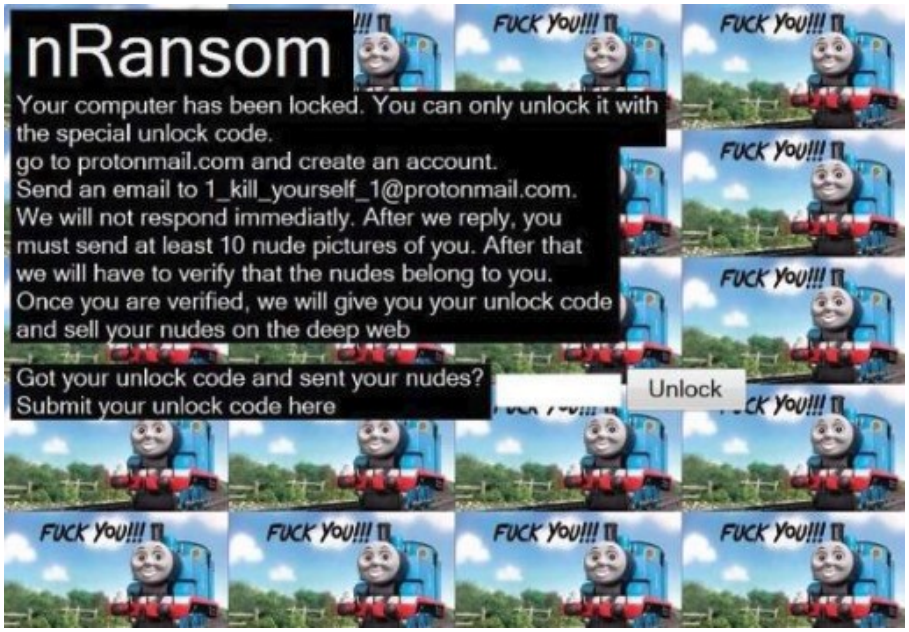


Figura 29: Mensaje de rescate del ransomware nRansom [56].

2.3 Vectores de infección más comunes

Un vector de infección es el camino que utiliza el malware, en este caso el ransomware, para tener acceso al sistema y para poder materializar la infección y consumar el ataque. Podríamos decir que es la forma en que los ransomwares se propagan.

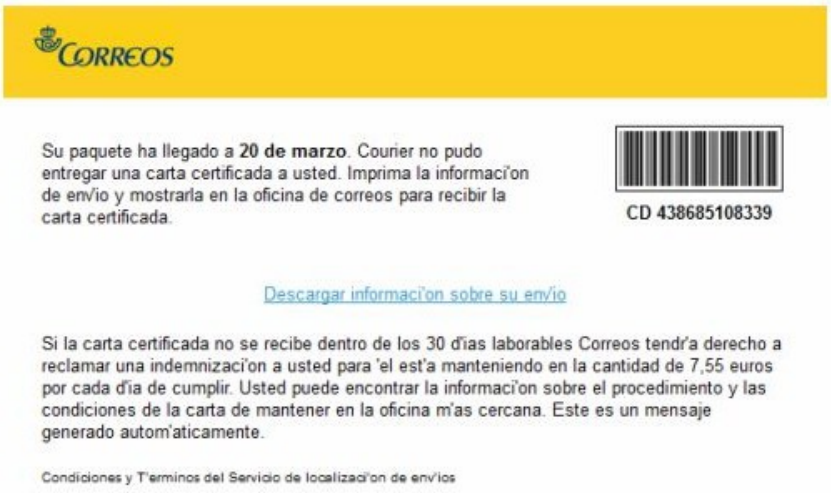
Los vectores de infección utilizados por los ransomware no difieren del resto de vectores que utilizan otros programas maliciosos como troyanos o virus.

Para que un ransomware infecte el equipo requiere la intervención del usuario para descargar y ejecutar el fichero malicioso, por ello los cibercriminales suelen utilizar la ingeniería social para engañarlos y lograr su propósito [16]. A continuación se describen los vectores de infección más comunes.

2.3.1 Correos electrónicos maliciosos

Este vector de propagación es uno de los más utilizados y consiste en que la víctima recibe un email falso que aparentemente procede de una empresa de logística conocida, entidad bancaria o de la administración pública de algún gobierno [16].

Estos correos suelen utilizar técnicas de *ingeniería social* para engañar al usuario y hacer que éste pinche sobre un enlace que se descarga así el ransomware o que descargue un fichero adjunto al correo que en realidad es el malware o es un documento ofimático con una macro encargada de realizar la descarga del programa y ejecutarlo [16]. Estos correos suelen enviarse mediante campañas de envío de correos masivos. A continuación se muestran ejemplos de correos fraudulentos con enlaces o adjuntos maliciosos.


CORREOS

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 438685108339

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Condiciones y T'erminos del Servicio de localizaci'on de env'ios

Figura 30: Correo electrónico con enlace malicioso de Correos [46].

Figura 31: Correo electrónico con enlace malicioso de Hacienda [58].

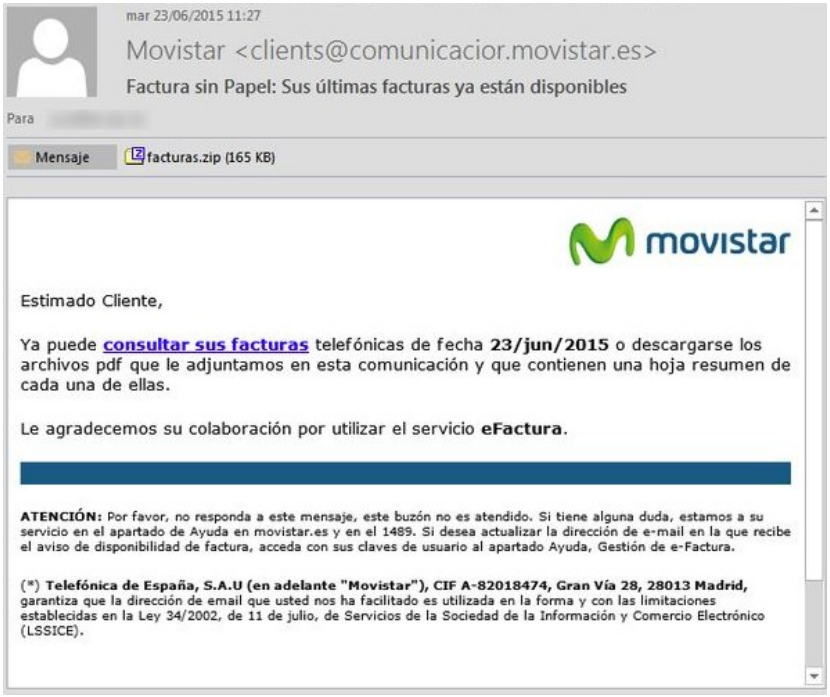


Figura 32: Correo electrónico con adjunto malicioso de Movistar [58].

Algunos ejemplos de troyanos que utilizan este método de infección son VaultCrypt, Criptolocker o Criptowall.

Para evitar este vector de propagación se recomienda no abrir los adjuntos ni pinchar sobre los enlaces de correos electrónicos que no esperemos o cuyo origen sea desconocido [16].

2.3.2 Páginas web infectadas

Otro método de propagación bastante común es visitar páginas web maliciosas o legitimas que han sido infectadas por los ciberdelincuentes para difundir el ransomware entre sus visitantes. Cuando la víctima visita estos sitios web se ejecuta a través del navegador un código malicioso o *payload* en el equipo del usuario que hace que se descargue el ransomware y se ejecute en su ordenador [59].

Otra forma habitual de infectar a los usuarios es que la página le redirecciona a otra web que tiene un *exploit kit*. Este Exploit kit es el que se encarga de detectar ciertas características de determinados componentes del sistema, como el tipo de navegador y su versión o el tipo de sistema operativo y su versión, y explota alguna vulnerabilidad asociado a las características encontradas para instalar el ransomware [60].

Un ejemplo de ransomware que utiliza este vector de infección es Keranger donde los cibercriminales comprometieron la página oficial del del cliente Transmission 2.90 de BitTorrent y lo sustituyeron por el malware, tal y como se ha visto en el punto “2.2.2 Variantes del ransomware”.

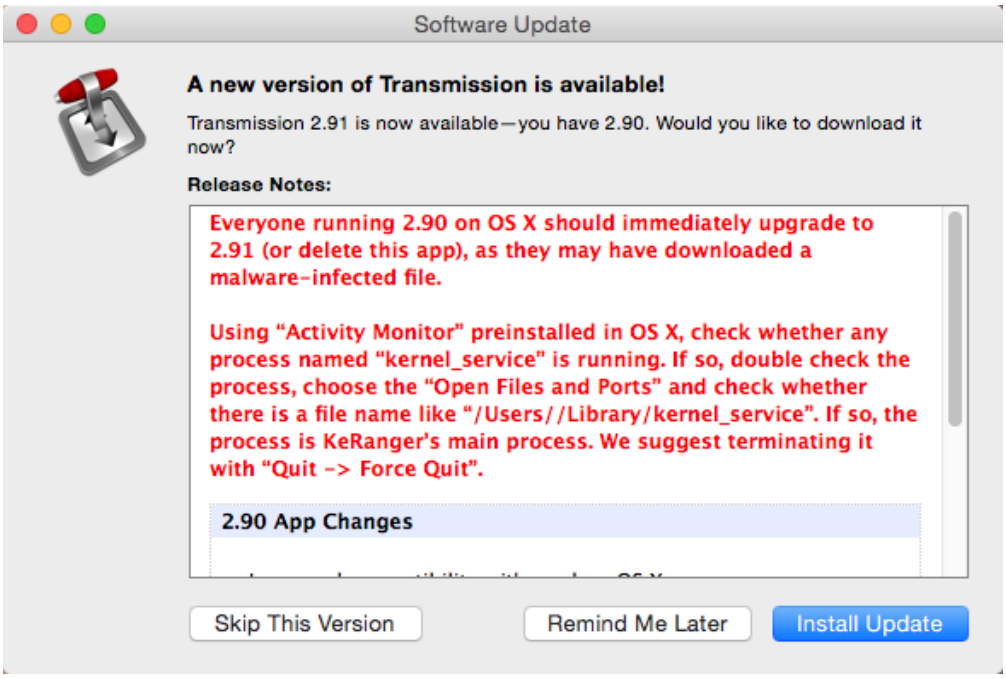


Figura 33: Pantalla para actualizar Transmission a la versión 2.90 [42].

Una recomendación es evitar visitar páginas web de contenido dudoso y hay que tener el navegador actualizado.

2.3.3 Conexión de dispositivos periféricos

Otra vía de infección posible es el de introducir en nuestro equipo un dispositivo periférico infectado con un ransomware, como una tarjeta de memoria SD de un teléfono móvil o una memoria USB.

Este tipo de dispositivos poseen el archivo “autorun.inf” y en el momento en el que el usuario lo conecta al equipo este archivo se ejecuta automáticamente y se activa el ransomware. Este fichero lo que hace es copiar el ransomware en el equipo y ejecutarlo, infectando así el equipo [61].

Otra forma en la que los usuarios se pueden infectar con este vector es mediante el uso de ingeniería social, haciéndoles creer que el programa que contiene este tipo de dispositivos periféricos es legítimo pero en realidad lo que hacen es ejecutar el programa malicioso. Un ejemplo que se ha visto en el punto “2.2.2 Variantes del ransomware” es el del ransomware AIDS, el cual utilizó disquetes para propagarse en 1989.

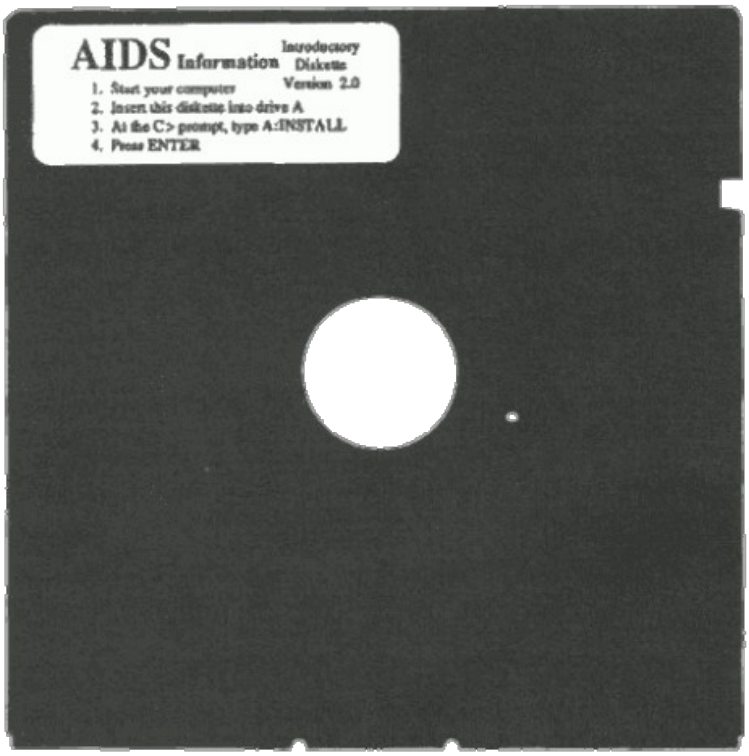


Figura 34: Muestra del disquete con el que se distribuía el troyano AIDS [7].

Para evitar este método de propagación se recomienda desactivar la ejecución automática de medios en Windows y asegurarse de que el origen del dispositivo externo que introducimos en el equipo es legítimo.

2.3.4 Explotación de vulnerabilidades

Un exploit es un programa que se aprovecha de un error de programación en la implementación del código de un sistema o de una aplicación para realizar acciones maliciosas, como por ejemplo tener acceso no autorizado a un equipo informático. Existen ransomwares que utilizan estos exploits para aprovecharse de las vulnerabilidades existentes y así poder acceder a un equipo e infectarlo [62].

Un ejemplo de ransomware que utilizaba esta técnica de propagación es WannaCry [51] que se aprovechaba de una vulnerabilidad existente en los sistemas operativo Windows, en concreto utilizaba un exploit conocido como Eternalblue que se aprovechaba de una vulnerabilidad existente en el protocolo SMB versión 1 usada para compartir determinados recursos entre los equipos. Esta vulnerabilidad está catalogada con el CVE-2017-0144 [63].

Para evitar este método de propagación se recomienda tener el sistema operativo y los programas actualizados a la última versión, ya que las actualizaciones suelen tener parches que corrigen las vulnerabilidades asociadas a los programas.

2.3.5 Descargas de ficheros en redes P2P o sitios web

Existen multitud de sitios web de descarga de ficheros o redes P2P (siglas del inglés *Peer-to-Peer*) para compartir ficheros donde un usuario se puede descargar programas piratas o herramientas, como *cracks,* para saltarse las licencias. Estos programas parecen que sean gratuitos pero no es así, ya que es posible que el usuario se infecte con un ransomware o cualquier otro tipo de programa malicioso. Además, estos programas pueden solicitar que se deshabilite el antivirus antes de instalarse, favoreciendo así la infección [16].

Para evitar infectar el equipo con este método de propagación se recomienda utilizar software original y que las descargas se hagan desde sitios oficiales y de confianza.

2.4 Modelos de negocio

Los ataques con ransomware cada vez son más sofisticados, tal y como hemos visto en el punto “2.2 Familias y variantes del ransomware”. Los cibercriminales se parecen cada vez más a las empresas que nos rodean, el negocio del ransomware es un negocio como cualquier otro que intenta maximizar sus ganancias y minimizar sus riesgos. A medida que los programas maliciosos pierden efectividad, surgen nuevas variantes que mejoran a las anteriores, parece que existe un ciclo de vida de desarrollo de software y hay cibercriminales que ofrecen el ransomware como un servicio en la nube, conocido como RaaS, similares a los del *SaaS* (de las siglas en inglés *Software as a Service*) [65].

En este punto se van a estudiar los modelos de negocio que se esconden detrás del ransomware y que permiten que éste sea un negocio lucrativo. En primer lugar vemos la motivación que hace que el ransomware sea una de las herramientas más lucrativas para los cibercriminales junto con las causas que ayudan a que su uso sea un negocio rentable. Posteriormente vemos los dos modelos de negocio principales, el que en este estudio se llama “el tradicional” y el que se ofrece como un servicio.

2.4.1 Motivación

Como cualquier negocio, la motivación principal para que los ciberdelincuentes utilicen el ransomware es la de ganar dinero. Existen una serie de causas que han ayudado a que este negocio sea más prospero para los cibercriminales por permitir reducir los costes, aumentar la rapidez de creación de campañas maliciosas y reducir los riesgos de que los cibercriminales sean capturados [66].

La primera causa es que crear un ransomware es fácil y accesible para la mayoría de cibercriminales, ya que no es necesario que éstos lo desarrollen, que sean expertos en criptología o que estén gastando recursos en su desarrollo, tan solo han de acceder a uno de los servicios ofertados por Internet de Ransomware como Servicio y comprar uno. La inversión para crear una campaña de ransomware es mínima [66].

La segunda causa es el surgimiento de las criptomonedas que ha permitido que los ciberdelincuentes soliciten de manera anónima el cobro por el rescate. Actualmente la mayoría de los ransomwares solicitan el pago en Bitcoins que no están asociados a una cuenta bancaria, por lo que rastrear esta actividad por la policía se vuelve más complicada [66].

La tercera y última causa es que la infraestructura necesaria para la utilización de este programa malicioso es flexible y rápida de desmontar.

En la actualidad la mayoría de ransomwares utilizan la Deep Web para mantener el anonimato y esto hace que se reduzcan las posibilidades de que puedan ser capturados por las Fuerzas y Cuerpos de Seguridad de los distintos países [66].

2.4.1 Modelo de negocio “tradicional”

En este estudio se le llama modelo de negocio tradicional al modelo que se está utilizando desde hace muchos años. Este modelo consiste en que los ciberdelincuentes extorsionan directamente a las víctimas solicitándoles, en la gran mayoría de casos, una cantidad económica pagada en criptomonedas.

En este punto del estudio se va a analizar el modelo de funcionamiento básico del ransomware, para ello se muestra como ejemplo el funcionamiento del ransomware Cryptowall, que nos permitirá ver cómo este modelo de negocio utiliza las tres causas vistas en el punto anterior para que sea un negocio rentable.

Las campañas de ransomware suelen llegar a las víctimas de diferentes formas, tal y como hemos visto en el punto “2.3 Vectores de infección más comunes” de la presente memoria. En nuestro ejemplo, Cryptowall llega a los usuarios mediante campañas de correos electrónicos que utilizan ingeniería social para engañar al usuario y haciendo que éste ejecute un archivo malicioso adjunto al correo o haga click sobre algún enlace que contiene malware [67] [68].

Cuando Cryptowall se ejecuta en el equipo del usuario, lo primero que hace es crear un directorio con nombre aleatorio, para evitar ser detectado por los antivirus, y oculto en el sistema para que el usuario no pueda verlo. En ese momento, Cryptowall envía un identificador al servidor Command & Control para identificar a la víctima y este servidor genera un par de claves públicas y privadas RSA de 2048 bits. Posteriormente el servidor envía la clave pública al ransomware instalado en el equipo de la víctima y además le envía una cuenta aleatoria de Bitcoins para que la víctima realice el pago por el rescate. Cuando el ransomware tiene la clave pública comienza el cifrado de los archivos y finaliza la infección mostrando un mensaje que solicita que la víctima se conecte a la Deep Web y que realice el pago en Bitcoins si quiere la clave privada almacenada en el servidor para descifrar los ficheros infectados [67] [68].

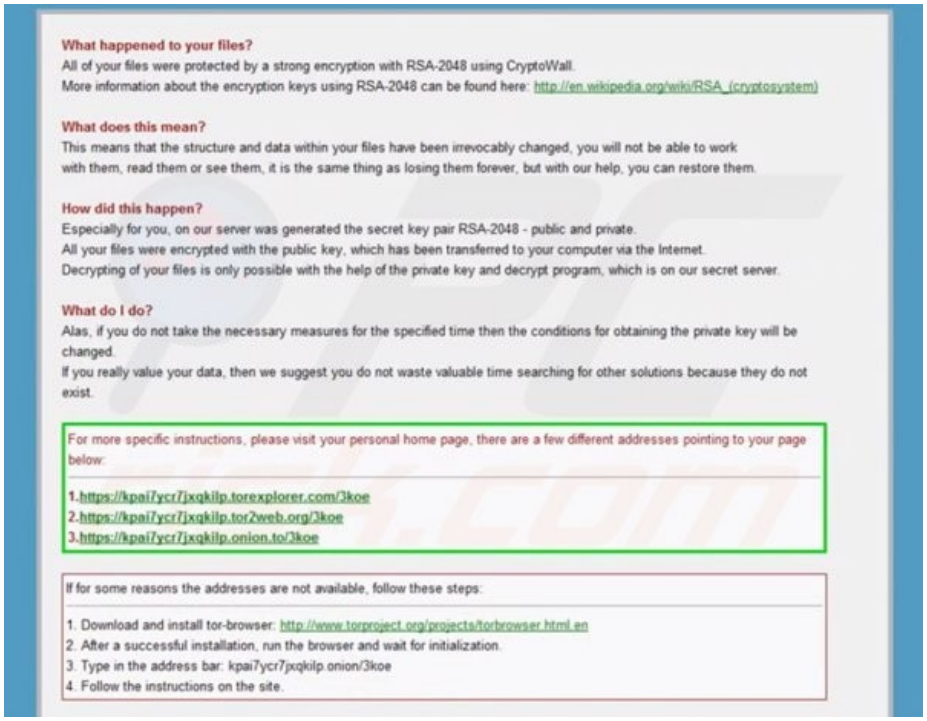


Figura 35: Mensaje que que muestra Cryptowall [29].

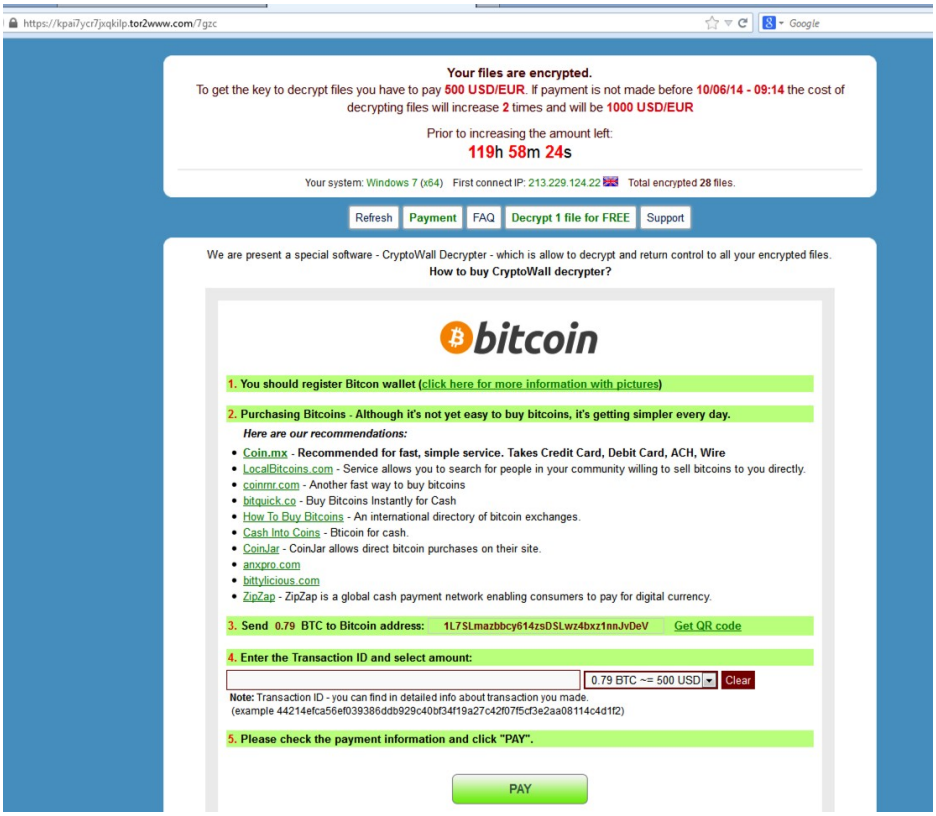


Figura 36: Página web con las instrucciones del pago en Bitcoins [69].

En este punto podemos ver que no es necesario que los cibercriminales que han desarrollado Cryptowall sean grandes expertos en criptografía, ya que utilizan el algoritmo de calve asimétrica RSA de 2048 bits que es

muy robusto y público, facilitando así el desarrollo de una herramienta eficaz y económica. Además, se observa que utilizan la Deep Web y una cuenta generada aleatoriamente para realizar el pago en Bitcoins, aumentando así el anonimato de los cibercriminales y dificultando la posible trazabilidad de la policía, por lo que el riesgo de ser capturados se reduce.

La tabla siguiente muestra el valor obtenido en dólares por los ransomwares que trabajan utilizando un modelo de negocio tradicional similar al de CryptoWall. Por las cifras, se puede observar como es un negocio bastante lucrativo para los cibercriminales.

Ransomware	**Rescate recibido en Bitcoin**	**Valor en dólares**	**Valor en euros**
CryptoWall	5.351,2329	2.220.909,12	1.804.055,58
CryptoLocker	1403,7548	449.274,97	364.948,30
DMA Locker	339,4591	178.162,77	144.722,51
WannaCry	47,1743	86.076,76	69.920,58
CryptoDefense	126,6960	63.859,49	51.873,38
NotPetya	4,0576	9.835,86	7.989,72
KeRanger	9,9990	4.173,12	3.389,85

Figura 37: Beneficio obtenido con el modelo de negocio tradicional [67].

2.4.2 Ransomware-as-a-Service (RaaS)

Este modelo de negocio está basado en el modelo de *Software-as-a-Service* (siglas SaaS en inglés) o, en español, Software como Servicio. El modelo SaaS es un modelo de distribución de software donde el servicio de mantenimiento, la operación diaria de soporte del software y los datos se gestionan en la nube, es decir en los servidores de la empresa que lo ofrece y no en los equipos del cliente [70]. El cliente accede a través de Internet a estos servicios que ha contratado. Las ventajas que ofrece este tipo de modelo de negocio son que permite reducir los costes, ya que el cliente no ha de poseer la infraestructura necesaria para almacenar los programas y la información y reduce el mantenimiento ya que no ha de realizar actualizaciones del software ni preocuparse de añadir nuevas funcionalidades porque de esto se encarga la empresa que ofrece este servicio.

Los cibercriminales han decidido adoptar este modelo de negocio con el ransomware y ofrecerlo a otros cibercriminales para que ahorren tiempo

y dinero si necesitan utilizar esta herramienta para su uso criminal. En este modelo los ciberdelincuentes que tienen poca experiencia pueden obtener un tipo de ransomware personalizado con poca inversión económica y sin mucha dificultad. Existen diferentes plataformas que ofrecen este tipo de modelo de negocio en la Deep Web, el cibercriminal que lo vea como una opción solo tiene que suscribirse, configurar su ransomware y pagar por el servicio [71].

Los ciberdelincuentes que ofrecen este tipo de negocio se encargan de desarrollar el código del ransomware y venderlo o alquilarlo. Además, utilizan un programa de afiliación destinado a otros cibercriminales para que estos sean los que realizan las campañas de ransomware. Los proveedores de este servicio proporcionan conocimientos técnicos, información de cómo se ha de lanzar el ataque e incluso una interfaz web donde se puede ver el estado y el éxito del ataque en tiempo real [71].

Los beneficios del ataque se reparten entre el proveedor del servicio, el desarrollador y los atacantes. Este modelo es interesante para los cibercriminales porque permite a los desarrolladores del ransomware ganar dinero de una forma rápida y a los clientes de este servicio les permite ahorrar tiempo y dinero en el desarrollo del código [71]. Ejemplos de ransomware que utilizan este modelo de negocio nos encontramos: Tox, Ransom32, Cerber, Frozr Locker, Satán, Petya, Mischa, RaasBerry, Atom, Hostman, Stampado o Filadelfia entre otros [71]. A continuación se muestran como ejemplo de uso de este modelo de negocio el ransomware Satán.

El servicio de Satán permite crear una muestra del ransomware y que el cliente se lo descargue de forma gratuita. Entre las opciones de configuración que ofrece este servicio se encuentran establecer el precio que se desee por el rescate, las condiciones del pago. El proveedor del servicio se encarga de cobrar los rescates en nombre del cliente y de proporcionar la herramienta de descifrado si las víctimas pagan [72]. Los proveedores de este ransomware se quedan con el 30% de los beneficios obtenidos por el cliente. Los precios de las tarifas varían dependiendo del número de equipos infectados y pagos que consiga el cliente [72].

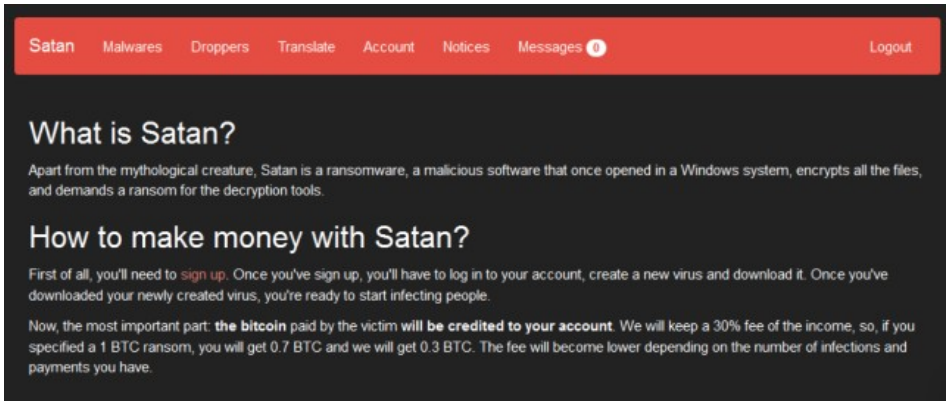


Figura 38: Web que oferta el servicio RaaS Satán [72].

Los clientes de este servicio han de rellenar un formulario para suscribirse al servicio y configurar el ransomware.

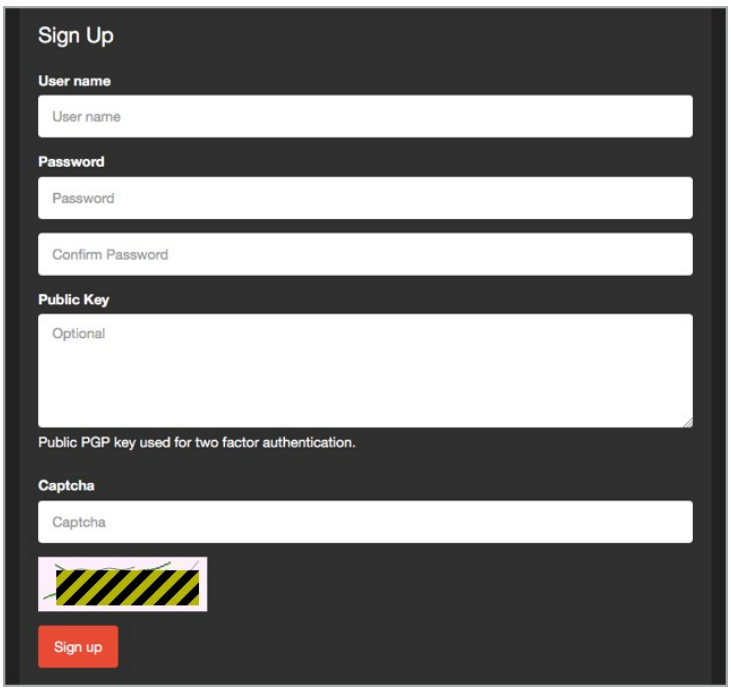


Figura 39: Formulario de suscripción al servicio de Satán [52].

Este servicio también ayuda a sus clientes a crear herramientas que faciliten la propagación del programa malicioso, como macros y scripts escritos en Powershell que se descargan el ransomware o páginas web que atraen a las víctimas para que se infecten [52].

Figura 40: Servicios adicionales que ofrece Satán [52].

Tal y como hemos visto,el modelo de negocio RaaS que sigue Satán se encontraría dentro del modelo “Pago por uso” (siglas en inglés *Pay-as-you-go*). Este modelo lo que busca es proveer al cliente solo la cantidad

de servicio que necesita cada vez [73]. El cliente de Satán se puede suscribir gratis al servicio y éste paga a medida que solicita más servicios de configuración [52]. Otro ejemplo de ransomware que sigue este modelo de negocio es Petya y Mischa.

Figura 41: Anuncio relacionado con el negocio de Petya y Mischa [47]

Además, el servicio que ofrece Satán sigue la filosofía de "*Do It Yourself*", siglas en inglés DIY, o en español "Hágalo usted mismo" que consiste en la fabricación de cosas por uno mismo, lo que permite ahorrar dinero, entretenerse y aprender a la vez [74]. En la Deep Web existen multitud de ransomwares que tiene esta filosofía y que ofrecen "Kits de bricolaje" para que los ciberdelincuentes se configuren su ransomware a su gusto [75]. Ejemplos de ransomwares que siguen está filosofía de creación con kits son Pletor, que su precio asciende a 5000 dólares [14] o Karmen, que pagas por el ransomware y el cliente que hace uso de él se queda con el 100% de los beneficios [76].

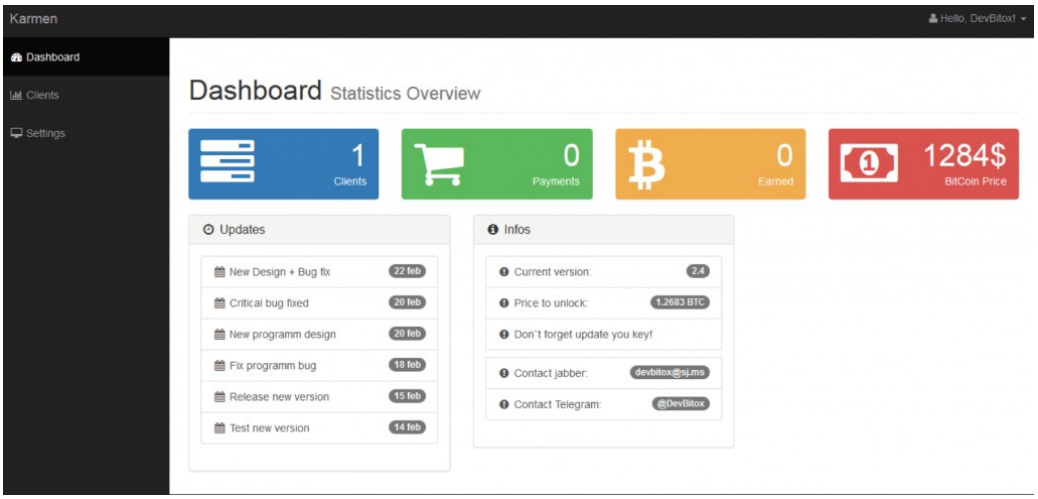


Figura 42: Consola principal de configuración de Karmen [77].

2.5 Medidas de seguridad

Los métodos para reducir los riesgos asociados a los ransomware pueden clasificarse en dos tipos:

1. **Medidas de prevención o activas**: el objetivo de este tipo de medidas es proteger y evitar la infección en los equipos informáticos [78]. Las medidas que se exponen en el presente estudio no son efectivas por si solas y hay que aplicarlas en conjunto como parte de una estrategia de seguridad. Cuantas más se apliquen más robusta será la seguridad del sistema y de la red perteneciente a la organización [3].

2. **Medidas de reacción o pasivas**: estas medidas tienen como objetivo disminuir los efectos causados por la infección del ransomware [78]. Entre las primeras acciones que realiza el ransomware una vez se ha producido la infección es cifrar los archivos del equipo, unidades de red y dispositivos periféricos conectados, como memorias USB o discos duros externos [95]. Seguramente seamos conscientes de que hemos sido infectados cuando se hayan cifrado los archivos y se nos muestre el mensaje de rescate, pero existe la posibilidad de que el ransomware no haya terminado el proceso de cifrado y que se puedan recuperar algunos de los archivos [95].

Los siguientes puntos describen cada una de estás medidas con más detalle.

2.5.1 Medidas de seguridad preventivas o activas

1. Realizar copias de seguridad periódicas
Esta es la principal medida que permite evitar perder la información que ha sido cifrada por el ransomware o evitar tener que pagar el rescate para recuperar los datos, ya que tan solo habría que recuperar los datos de la última copia de seguridad realizada [3].

Hay que tener en cuenta que muchos ransomwares tiene la capacidad de cifrar unidades de red, ficheros almacenados en la nube ,como por ejemplo en OneDrive y Dropbox, o dispositivos externos de almacenamiento. Es importarte que las copias de seguridad no sean accesibles desde la red corporativa y además no hay que tener siempre conectados los dispositivos externos de almacenamiento que poseen las copias de seguridad en el equipo y también hay que ser conscientes de que es muy probable que los archivos que se encuentran en la nube pueden ser infectados si estos están instalados como unidades de almacenamiento locales [79].

Para realizar las copias de seguridad se aconseja seguir las siguientes recomendaciones [80]:

- Realizar copias de seguridad periódicas de la información más importante en distintos dispositivos ya que si alguno de estos dispositivos es infectado o falla se pueda seguir accediendo a la información [80].

- Utilizar una aplicación de copias de seguridad fiable que no vaya a fallar en el proceso [80]. Por ejemplo, Windows ofrece la programar copias de seguridad periódicas de manera fácil desde la opción “Copias de Seguridad y Restauración” [79].

- Conocer las ventajas e inconvenientes del almacenamiento en la nube [79], ya que hay que tener en cuenta que es posible que el servicio que se ofrezca de almacenamiento sea menos seguro que tenerlo en nuestra organización.

- Almacenar la copias de seguridad cifradas porque pueden contener información sensible [79].

- Verificar periódicamente que el proceso de copia de seguridad y su recuperación funciona correctamente [3].

2. Concienciación y formación de los usuarios
Existe una frase que dice “*el eslabón más débil en la cadena de seguridad informática es el usuario*”.

En la seguridad informática no solo son importantes los procesos y la tecnología también son los usuarios del sistema por ser los que gestionan la información [81].

Ya hemos visto que el ransomware necesita la acción del usuario para que se ejecute cuando este llega al equipo por algún vector de infección más común, como un correo malicioso con apariencia inofensiva o una página web infectada. Para evitar que el usuario sea engañado hay que formarle y concienciarle en materia de ciberseguridad creando en la organización una cultura de seguridad que permite establecer las bases de la protección contra este tipo de amenazas [81].

3. Aplicar el principio de mínimo privilegios o LUA
Este principio consiste en reducir el impacto de la infección reduciendo los privilegios de la cuenta del usuario al mínimo necesario para que realice solo las tareas permitidas y necesarias para que desempeñe su labor. Este principio está relacionado con los diferentes perfiles o cuentas de usuario que se pueden crear en el sistema operativo [82].

Una recomendación sería la de tener configurada dos cuentas como mínimo:

- Cuenta de Administrador con privilegios de administración: esta cuenta puede gestionar el sistema y la instalación de software en el equipo. Se recomienda utilizar un seudónimo para no revelar la identidad de la misma [82]. Además, se recomienda acceder lo mínimo necesario con esta cuenta al equipo, ya que si un ransomware se ejecuta con privilegios de administración puede causar mucho más daño porque éste puede llegar a lugares que con otros permisos no podría acceder o desconectar medidas de seguridad como por ejemplo el antivirus.

- Cuenta de Usuario o Usuarios con privilegios mínimos: estas cuentas tiene permisos muy limitados, pueden realizar muy pocas modificaciones de configuración en el equipo y el acceso a los programas es muy restringido. Si un ransomware se ejecuta con esta cuenta se limita su rango de actuación, ya que por ejemplo no podrá desconectar las herramientas de seguridad del equipo. Muchos ransomware, como por ejemplo SamSam, utilizan técnicas de explotación de vulnerabilidades en el sistema para obtener privilegios de administración y así poder realizar las acciones que deseen [83].

La aplicación de este principio garantiza que el inicio de sesión se realiza con las cuentas de usuario con privilegios mínimos para que éste realice su trabajo diario reduciendo el uso de las credenciales de administración solo para tareas de mantenimiento del equipo y de los programas instalados [82].

4. Solución de Contraseña de Administrador Local (LAPS)
No existe constancia de que haya un ransomware que utilice como vector de infección la explotación de la vulnerabilidad de Windows “Pass the Hash” la cual se aprovecha de que la contraseña de Administrador Local sea común en muchos equipos de la organización [109].

LAPS es una solución de Microsoft que permite que la contraseña del Administrador Local sea generada de forma aleatoria y almacenada en Active Directory, además posee una serie de controles de acceso que ayudan a saber quién es el que ha solicitado dicha contraseña [109].

Este tipo de solución permiten poner ciertas barreras a los programas maliciosos que intentan moverse lateralmente por la red de la organización y, por lo tanto, se recomienda el uso de este tipo de herramientas [109].

5. Segmentación de la red informática
La segmentación de la red consiste en agrupar los activos de red, recursos y las aplicaciones de manera física y/o lógica en subredes o segmentos con el criterio de la relación de confianza entre ellos [84].

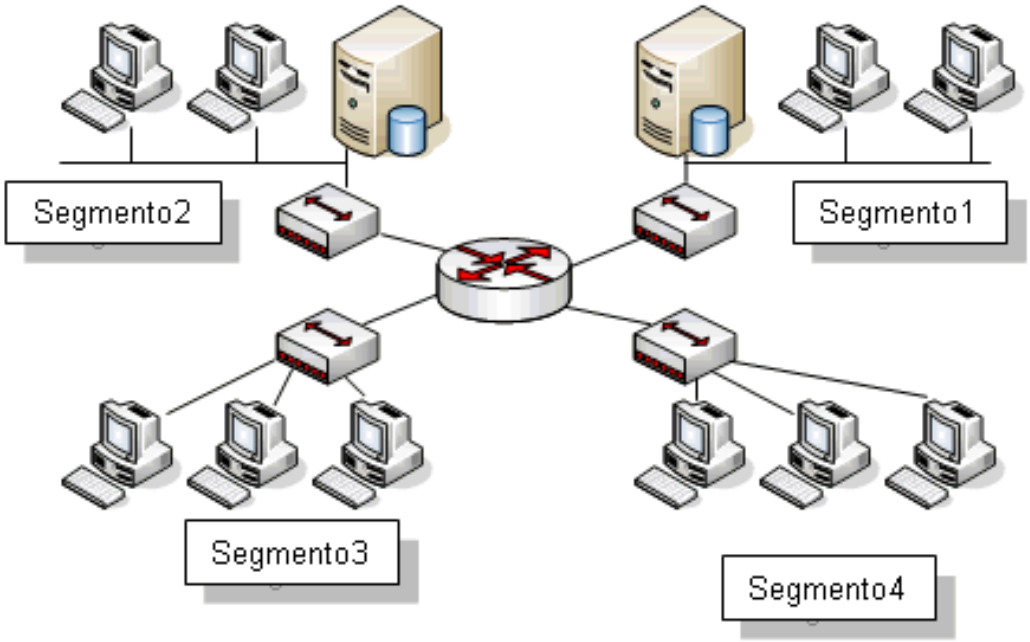


Figura 43: Ejemplo de segmentación de red [85].

Esta segmentación no evita el acceso del ransomware al sistema, pero si que limita su infección a otros equipos, haciendo que el programa malicioso quede contenido y aislado en el segmento de red que haya sido infectado y evitando que se propague por el resto de la organización [3].

6. Segmentación de red de Máquinas Virtuales

Hay que tener en cuenta que la segmentación de red vista en el punto anterior no cubre la comunicación existente entre las máquinas virtual que se encuentran dentro de un mismo servidor, ya que ésta tiene lugar en el plano posterior del servidor y no transversal de los equipos de la red que utilizan switches o routres para su comunicación [109].

Si la infraestructura de la organización se encuentra altamente virtualizada se recomienda utilizar tecnologías de segmentación de máquinas virtuales, como por ejemplo NSX de VMWare o HNV de Microsoft, para que las comunicaciones entre las máquinas virtuales estén controladas al mismo nivel que en la red física [109].

7. Revisar recursos compartidos y unidades de almacenamiento externos

Se recomienda realizar una revisión periódica de los recursos compartidos, como por ejemplo las unidades de disco, impresoras o carpetas, y de las unidades externas, como tarjetas de memoria o discos duros extraíbles, que se encuentran conectadas en los equipos para determinar si estos deben seguir compartidos [3].

Si se detecta que este tipo de recursos ya no se utilizan, se recomienda desconectarlos o deshabilitarlos para evitar que el ransomware se propague a otros equipos en el caso de que uno de ellos se infecte [3].

Además, también se recomienda restringir los privilegios de escritura para mitigar parcialmente el impacto de la infección [95].

8. Utilizar programas antivirus y herramientas anti-ransomware
Se recomienda utilizar varios antivirus en la organización, por ejemplo, podemos utilizar un antivirus en el firewall corporativo para analizar las comunicaciones, otro en el firewall de correo que analice los documentos adjuntos y otro en las estaciones de trabajo para analizar los programas que se descarguen los usuarios de Internet o que introduzcan en el equipo mediante dispositivos periféricos [3].

Además, también se recomienda que cada uno de los antivirus instalados sean de diferentes fabricantes, ya que es habitual que pasen un promedio de 48 horas entre que se detecta un nuevo ransomware y las fabricas de antivirus reaccionan ante él. Existen fabricantes de antivirus que pueden reaccionar antes que otros y por lo tanto se multiplican las probabilidades de detección en cada uno de los niveles [3].

También se recomienda que las soluciones antivirus que se elijan sean capaces de analizar el contenido de los ficheros comprimidos. Una limitación actual de los antivirus es que no pueden analizar el contenido de los ficheros comprimidos que son protegidos por contraseña [3].

Estos sistemas antivirus han de estar correctamente actualizados, tanto el propio antivirus como las firmas que permiten detectar el malware [3].

Muchos de estos antivirus ya poseen módulos Anti-Ransomware como la tecnología CryptoGuard de Sophos Intercept X [86] o Advanced Memory Scanner de ESSET [87] que bloquean los procesos que poseen un comportamiento sospechoso [95].

Otra medida adicional que se puede utilizar en los equipos es una Anti-Ransomware que permite reducir parcialmente el impacto producido por la infección parando parte del proceso de cifrado del ransomware. Algunas herramientas Anti-Ransomware [95], como por ejemplo Unlock ZeroLocker, permiten descifrar los ficheros infectados mediante fuerza bruta [88]. El funcionamiento de este tipo de herramientas es el siguiente:

1. Esta herramienta crea en las carpetas del usuario un fichero susceptible de ser cifrado. Ha este fichero se le conoce con el nombre de *honeyfiles*.

2. Esta herramienta monitoriza si el fichero *honeyfile* se modifica.

3. Si el fichero se modifica, la herramienta es capaz de detectar el proceso que lo ha modificado y hace una copia de él para intentar obtener la clave de cifrado y lo mata para que se detenga la infección.

4. Si el ransomware utiliza un algoritmo de cifrado de clave simétrica y la herramienta Anti-Ransomware ha obtenido esta clave se podrá recuperar los ficheros cifrados.

9. No ocultar las extensiones de los ficheros
El objetivo de esta medida es permitir identificar archivos ejecutables que se pueden hacer pasar por otro tipo de archivos, como documentos ofimáticos [95].

En los sistemas operativos Windows está configurado por defecto que se oculten las extensiones de los ficheros. Esto es un problema porque los ciberdelincuentes llaman a los archivos con doble extensión y con el icono de un programa legítimo para engañar al usuario y que éste lo ejecute [3]. Un ejemplo de nombres de programas maliciosos puede ser “factura.pdf.exe” o “Nomina.docx.scr”.

10. Inventario y control de aplicaciones
Se recomienda realizar un inventario periódico de las aplicaciones instaladas en la organización que permita tener una visibilidad completa de los programas que se se utilizan [3].

Este inventario permite detectar herramientas que no están autorizadas que pueden convertirse en un riesgo para la organización y además permite detectar software autorizado no actualizado que puede tener múltiples vulnerabilidades que pueden ser aprovechadas por un ransomware en su proceso de infección o propagación [3].

Además, también se recomienda utilizar programas de control de aplicaciones que permiten configurar qué software puede o no ejecutarse en los equipos de la organización basándose en la ruta, nombre, hash de la aplicación o en el usuario que la va a utilizar [3]. Estos programas pueden llegar a bloquear la ejecución de un ransomware, porque crean listas blancas de los programas que sí se pueden ejecutar [95]. Ejemplos de software de control de aplicaciones se encuentran Applocker de Microsoft, Bit9 Parity Suite [95], McAfee Application Control [95], Lumension Application Control [95] o la funcionalidad de controles de aplicaciones que poseen algunos antivirus como Panda, Sophos o Karspersky.

11. Uso de firewall
Se recomienda utilizar como mínimo un firewall en el perímetro de la organización para filtrar las conexiones entrantes y/o salientes de la red. Los firewalls actuales permiten crear listas blancas y listas negras de dominios, direcciones IP, puertos y aplicaciones para tener un control sobre el tráfico de la organización [3].

Como ya se ha visto en puntos anteriores, muchos ransomwares establecen una conexión con los servidores de Command & Control (C&C) para obtener la clave pública de cifrado antes de infectar los archivos. Si se posee un firewall que bloquea la conexión con el servidor

de C&C es posible que el ransomware que ha infectado un equipo no pueda cifrar los archivos [3]. También se recomienda realizar un filtrado del acceso a los nodos de la red de TOR, ya que muchos ransomwares utilizan está red como canal de comunicación con los servidores de C&C [3].

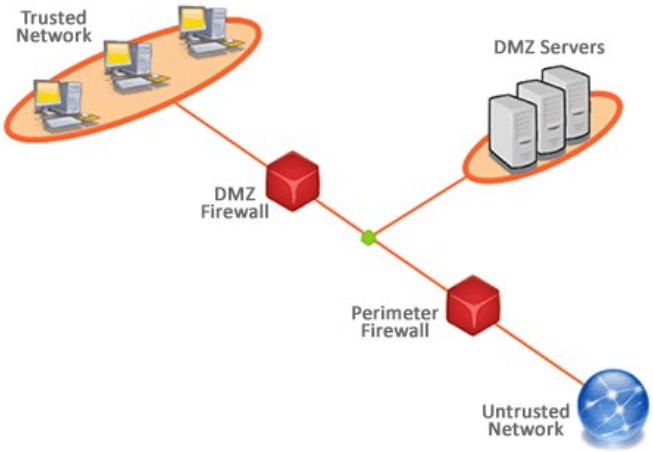


Figura 44: Ejemplo de topología de red con firewall de perímetro [89].

12. Uso de IDS/IPS

Un IDS o Sistema de Detección de Intrusos es un software que permite detectar en nuestra organización tráfico no deseado, como por ejemplo tráfico relacionado con el incumplimiento de políticas como puede ser el tráfico relacionado con chats, juegos, programas no permitidos o tráfico relacionado con programas maliciosos como el que generan los ransomwares. Un IPS o Sistema de Prevención de Intrusos es muy similar a un IDS pero es capaz de detectar y bloquear el tráfico no permitido [90].

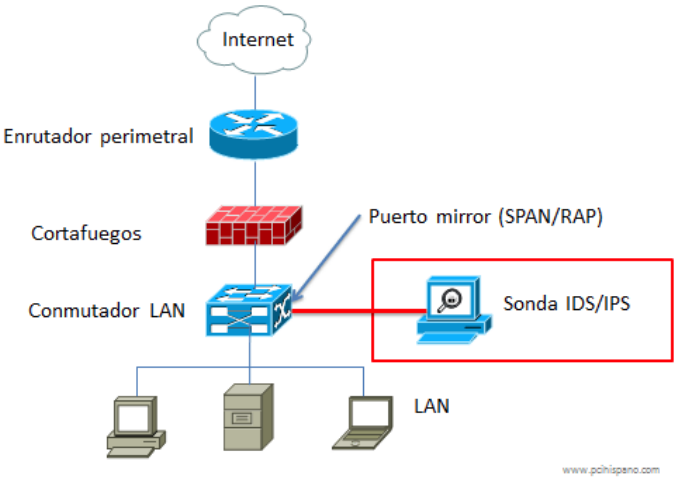


Figura 45: Ejemplo de topología de red con IDS/IPS [92].

Muchos firewall actuales conocidos como “de nueva generación” ya llevan incorporado módulos IPS que complementa su funcionamiento, un ejemplo son los del fabricante Check Point [91].

13. Uso de HIDS/HIPS

Un HIDS es un Sistema de Detección de Intrusos que se instala en un Host. Estos sistemas permite detectar anomalías que indican un riesgo potencial mediante la monitorización de las actividades que se realizan en el equipo o host. El funcionamiento de un HIDS es similar al de un IDS [110].

Un HIPS es un Sistema de Prevención de Intrusos que se instala en un Host y que funciona de manera similar a un HIDS pero éste es capaz de mitigar o bloquear los posibles intentos de ataque. Su funcionamiento sería equivalente al de un IPS para la red.

Estos sistemas pueden proporcionar información desde el comienza de un posible ataque o infección y por lo tanto se recomienda su instalación como mínimo en los equipos críticos de la organización [109].

14. Uso de un servidor proxy web

El proxy web es un elemento que interviene en la navegación web de los equipos informáticos a los servidores web que se encuentran en Internet permitiendo controlar el acceso a estos. Entre las funciones de un proxy web se encuentran el filtrado de webs maliciosas o no permitidas por la política de la organización.

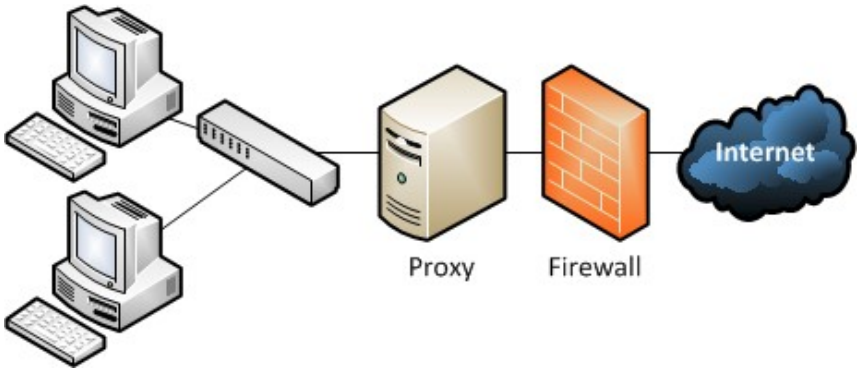


Figura 46: Ejemplo de topología de red con proxy web [93].

Se recomienda realizar la siguiente configuración en el proxy web de la organización para evitar ser infectados por un ransomware:

- Bloquear, si no afecta al negocio, tráfico procedente de Asia y países de Europa del Este, ya que muchos ransomwares proceden de estas zonas [3].

- Bloquear dominios catalogados como maliciosos y los relacionados con la red TOR. En internet existen listados con estos dominios y algunos fabricantes también lo proporcionan para que sus dispositivos actualicen su listado de dominios maliciosos de forma automática [3].

- Bloquear los siguientes Dominios de Nivel Superior (TLD), ya que según fuentes como Spamhaus o BlueCoat son sospechosos por naturaleza [109]:

Dominios de Nivel Superior (TLD)			
.accountant	.download	.party	.top
.biz	.gdn	.review	.trade
.click	.gq	.science	.win
.country	.kim	.stream	.zip
.cricket	.link	.tk	

Tabla 1: Dominios de Nivel Superior sospechosos [109].

- Realizar un filtrado de dominios por su categoría como por ejemplo las páginas web de pornografía, correo de publicidad no deseada, phishing o navegación anónima [3].

- Limitar el uso de correo no corporativo, como el acceso a Gmail o Hotmail; sitios web de almacenamiento en la nube, como Dropbox o Drive; y sitios de intercambio de ficheros, como Wetransfer, porque muchos ransomwares y otro tipo de programas maliciosos utilizan estos sitios como vector de infección [3].

15. Uso de filtros de correo

Los servidores de correo poseen una serie de filtros de correo que permiten bloquear SPAM o correo basura y analizar sus archivos adjuntos para buscar malware o eliminar direcciones URL maliciosas que contienen los cuerpo de los mensajes [3].

Se recomienda utilizar este tipo de filtro para evitar posibles infecciones por ransomware, ya que como hemos visto, uno de los principales vectores de infección es la recepción de correos maliciosos con adjunto o enlaces que permiten descargar el malware.

16. Uso de módulos de DLP

Las herramientas de Prevención de Perdida de Datos o DLP (siglas del inglés de *Data Loss Prevention*) permiten analizar los medios de entrada y salida de información como los correos electrónicos, páginas web y dispositivos periféricos de almacenamiento para evitar fugas de datos confidenciales y de esta forma cumplir con la normativa [94]. Muchos dispositivos como firewalls, proxies web o servidores de correo poseen módulos DLP [3].

Hemos visto que existen ransomwares que antes de cifrar la información del equipo son capaces de enviar los datos hacia sus servidores maliciosos para amenazar con publicarla en Internet en el caso de que la víctima no pague el rescate. Con este tipo de módulos DLP se puede detectar esta fuga de información y evitar que se haga realidad la amenaza de los ciberdelincuentes o detectar una posible infección y detenerla lo antes posible.

17. No permitir la ejecución de ficheros con extensiones peligrosas

Una de las técnicas que utilizan los ciberdelincuentes para engañar a los usuario y que ejecuten el ransomware es llamar a programas ejecutables maliciosos con nombres e iconos de programas legítimos como por ejemplo "Nomina_abril.ps1" en vez de "Nomina_abril.pdf"o "Factura_345678.bat" en lugar de "Factura_345678.doc". También hemos visto que algunos ransomwares se encuentran comprimidos en archivos tipo Zip o Rar.

Para evitar que se ejecuten este tipo de programas maliciosos se recomienda configurar los filtros de contenido que poseen los firewalls de última generación, servidores proxy web y los programas de control de aplicaciones para que no permitan que se ejecuten este tipo de ficheros por considerarse peligrosos [3]. En concreto se recomienda filtrar los ficheros que contengan las siguientes extensiones, el criterio de bloqueo depende de los administradores del sistema y de la política de la organización [108]:

Extensión	Tipo de Archivo	Extensión	Tipo de Archivo
.adp	Proyecto de Access (Microsoft)	.mshxml	Microsoft Shell
.app	Aplicación ejecutable	.msh1xml	Microsoft Shell
.asp	Página de Active Server	.msh2xml	Microsoft Shell
.bas	Código fuente en BASIC	.msi	Archivo de Windows Installer (Microsoft)
.bat	Procesamiento por lotes	.msp	Actualización de Windows Installer
.cer	Archivo de certificado de seguridad de Internet	.mst	Script de Windows SDK Setup Transform
.chm	Ayuda compilada en HTML	.ops	Archivo de configuración de perfil de Office
.cmd	Archivo de comando DOS CP/M, archivo de comandos para Windows NT	.osd	Aplicación virtualizada con Microsoft SoftGrid Sequencer
.cnt	Índice de archivo de ayuda	.pcd	Prueba Visual (Microsoft)
.com	Comando	.pif	Archivo de información de programa de Windows (Microsoft)
.crt	Archivo de certificado	.plg	Developer Studio Build Log
.csh	Script csh	.prf	Archivo de sistema de Windows
.der	Archivo de certificado codificado DER X509	.prg	Archivo de programa
.exe	Archivo ejecutable	.pst	Archivo de la libreta de direcciones de MS Exchange, archivo de la carpeta personal de Outlook (Microsoft)
.fxp	Fuente compilada de FoxPro (Microsoft)	.reg	Información de registro/clave para W95/98, archivo de datos

Extensión	Tipo de Archivo	Extensión	Tipo de Archivo
			del registro
.gadget	Gadget de Windows Vista	.scf	Comando de Windows Explore
.hlp	Archivo de ayuda de Windows	.scr	Salvapantallas de Windows
.hpj	Archivo de proyecto utilizado para crear el archivo de ayuda de Windows	.sct	Componente de Windows Script, pantalla Foxpro (Microsoft)
.hta	Aplicación de hipertexto	.shb	Acceso directo de Windows a un documento
.inf	Archivo de información o de configuración	.shs	Archivo de objeto de Shell Scrap
.ins	Configuración de comunicaciones de Internet de IIS (Microsoft)	.ps1	Windows PowerShell
.isp	Configuración del proveedor de servicios de Internet IIS (Microsoft)	.ps1xml	Windows PowerShell
.its	Conjunto de documentos de Internet, traducción de Internet	.ps2	Windows PowerShell
.js	Código fuente de JavaScript	.ps2xml	Windows PowerShell
.jse	Archivo codificado JScript	.psc1	Windows PowerShell
.ksh	Intérprete de comandos de UNIX	.psc2	Windows PowerShell
.lnk	Archivo de acceso directo de Windows	.tmp	Archivo/Carpeta tempora
.mad	Acceso directo a módulo de Access (Microsoft)	.url	Ubicación de Internet
.maf	Access (Microsoft)	.vb	Archivo VBScript o cualquier fuente de VisualBasic
.mag	Acceso directo a diagrama de Access (Microsoft)	.vbe	Archivo de proyecto de Visual Basic
.mam	Acceso directo a macro de Access (Microsoft)	.vbs	Archivo de secuencia de comandos VBScript, script de Visual Basic para aplicaciones
.maq	Acceso directo a consulta de Access (Microsoft)	.vsmacros	Proyecto macro basado en binario de Visual Studio .NET (Microsoft)
.mar	Acceso directo a informe de Access (Microsoft)	.vsw	Archivo de área de trabajo de Visio (Microsoft)
.mas	Acceso directo a procedimientos almacenados de Access (Microsoft)	.ws	Archivo de script (secuencia de comandos) de Windows
.mat	Acceso directo a tabla de Access (Microsoft)	.wsc	Componente de script de Windows
.mau	Unidad de archivos adjuntos	.wsf	Archivo de script (secuencia de comandos) de Windows

Extensión	Tipo de Archivo	Extensión	Tipo de Archivo
.mav	Acceso directo a vista de Access (Microsoft)	.wsh	Archivo de configuración de Windows Script Host
.maw	Página de acceso a datos de Access (Microsoft)	.xnk	Acceso directo a la carpeta pública de Exchange
.mda	Complemento de Access (Microsoft), MDA Access 2 Workgroup (Microsoft)	.ade	Archivo de audio ADC
.mdb	Aplicación de Access (Microsoft), MDB de base de datos de Access (Microsoft)	.cla	Archivo de clase Java
.mde	Archivo de base de datos MDE de Access (Microsof	.class	Archivo de clase Java
.mdt	Datos de complemento de Access (Microsoft)	.grp	Grupo de programas de Microsoft Widows
.mdw	Información del grupo de trabajo de Access (Microsoft)	.jar	Paquete de archivo comprimido para clases y datos de Java
.mdz	Plantilla de asistente de Access (Microsoft)	.mcf	Archivo MMS de Composer
.msc	Archivo de control del complemento de Microsoft Management Console (Microsoft)	.ocx	Archivo de control de ActiveX
.msh	Microsoft Shell	.pl	Código fuente del lenguaje de script Perl
.msh1	Microsoft Shell	.xbap	Paquete de aplicaciones Silverlight
.msh2	Microsoft Shell		

Tabla 2: Tipos de archivos que suelen ser amenazas [108].

18. Mantener actualizados el sistema operativo y las aplicaciones

Muchos ransomwares aprovechan vulnerabilidades existentes en los sistemas operativos y en las aplicaciones para acceder a los equipos y poder infectarlos.

Cuando se descubre una vulnerabilidad y se publica, los fabricantes de software la corrigen aplicando las oportunas actualizaciones de sus productos. Se recomienda mantener actualizados todos los programas y los sistemas operativos de la organización en sus últimas versiones [95] para corregir estas vulnerabilidades con sus correspondientes parches y reducir la probabilidad de ser infectado por un ransomware que las intente explotar.

19. Deshabilitar el escritorio remoto

Existen ransomwares, como por ejemplo el ransomware Surprise [96], que utilizan aplicaciones de escritorio remoto para infectar a sus víctimas como TeamViewer, VNC o el nativo de Windows con el protocolo RDP. Es muy común que estas aplicaciones posean vulnerabilidades o que posean contraseñas poco robustas [3].

Se recomienda tener deshabilitadas estas herramientas de acceso remoto a los equipos e implementar una VPN para que el acceso a la red corporativo se limite a unos pocos. Además, si es necesario la utilización del protocolo RDP, se recomienda que se use certificados digitales X.509 basados en PKI emitidos por una entidad de confianza. También es recomendable fortalecer la autenticación utilizando contraseña robustas y habilitando, si es posible, el doble factor de autenticación (2FA) [3].

20. No permitir la ejecución de archivos temporales

Existen una serie de archivos temporales utilizados por los instaladores y programas para realizar funciones propias. Si se trata de un sistema Windows, estos archivos temporales suelen ir ubicados en las carpetas temporales siguientes [3]:

- %AppData%\
- %LocalAppData%\
- %LocalAppData%\Temp\
- %ProgramData%\
- %Temp%\
- %userprofile%\
- %WinDir%\temp\
- %WinDir%\SysWow\

Es los sistemas Linux el directorio temporal es “/tmp” y en los equipos con sistema Mac OS el directorio es “~/Library/” [3].

Una de las características de los archivos temporales es que se eliminan una vez se ha cerrado la sesión o se ha reiniciado el equipo. Existen ransomwares y otros programas maliciosos que se ejecutan en las carpetas temporales para aprovechar esta característica y evitar así que se pueda recuperar el archivo ejecutable que ha infectado el equipo.

Se recomienda bloquear los permisos de ejecución en estas carpetas para que los programas maliciosos no puedan ejecutarse. Estos bloqueos se pueden realizar mediante el uso de políticas de Active Directory y añadir excepciones para aquellos programas que lo necesiten. Un ejemplo de rutas de carpetas temporales para bloquear sería [3]:

- %AppData%*.exe
- %AppData%**.exe
- %LocalAppData%*.exe
- %LocalAppData%**.exe
- %LocalAppData%\Temp*.zip*.exe
- %LocalAppData%\Temp\7z**.exe
- %LocalAppData%\Temp\Rar**.exe
- %LocalAppData%\Temp\wz**.exe
- %ProgramData%*.exe
- %Temp%*.exe
- %Temp%**.exe
- %userprofile%*.exe
- %WinDir%\temp*.exe

- %WinDir%\SysWow*.exe

21. Deshabilitar las macros y ActiveX

Como ya se ha visto anteriormente, una de las técnicas que utilizan los ciberdelincuentes para infectar a los equipos es enviar correos electrónicos con documentos ofimáticos maliciosos que se descargan el ransomware desde Internet. Estos documentos maliciosos contienen macros que se ejecutan automáticamente al abrirlos dando lugar a la descarga y ejecución del programa malicioso [3].

ActiveX es un entorno que permite definir componentes de software independientes del lenguaje de programación para que las aplicaciones puedan utilizarlos y complementar así su funcionalidad. Aplicaciones como Microsoft Office, Windows Media Player o Internet Explorer utilizan ActiveX [97].

Se recomienda deshabilitar las macros y ActiveX de los sistemas para que los documentos maliciosos no puedan realizar acciones malintencionadas. Además, también se recomienda no abrir documentos ofimáticos que se hayan recibido por un correo electrónico sospechoso o que no se estaba esperando [3].

22. Deshabilitar servicios de script y consolas

Existen campañas de ransomwares, como versiones de Locky (JS/Locky) o Nemucod (JS/Nemucod) que utilizan como vector de infección el uso de emails que contienen como adjunto un archivo comprimido en formato RAR o ZIP que almacenan un fichero Javascript que es el encargado de descargase y ejecutar el programa malicioso [98].

Se recomienda deshabilitar los programas del sistema operativo que abren y ejecutan los scripts. Un ejemplo de estos programas es la aplicación *Windows Based Script Host* (WSH). Además, también se recomienda deshabilitar las consolas de Microsoft Power Shell y el CMD de Windows porque la mayoría de los usuarios no la utilizan y así se evita que se puedan ejecutar ficheros con script como los archivos “.bat”, “.cmd” o “.ps1” [3].

23. Bloquear publicidad y ventanas emergentes

Una de las técnicas que utilizan los programas maliciosos es el *Malvertising*, término que viene de las palabras "malicious advertising" o publicidad maliciosa. Esta técnica consiste en esconder el ransomware en los espacio de publicidad de las páginas web. Estos anuncios maliciosos aprovechan las vulnerabilidades de los complementos o “plugins” que se encuentran instalados en el navegador para ejecutarse de forma automática e infectar el equipo [99].

Se recomienda instalar bloqueadores de publicidad, como pueden ser Adblock o Adblock Plus, y bloquear las ventanas emergentes en los

navegadores para evitar infectarse si se visitan páginas web infectadas o maliciosas [3].

24. Desconectar las conexiones inalámbricas

Hay que deshabilitar en los smartphones, tablets, notebooks y portátiles las conexiones inalámbricas, como las conexiones Wifi o Bluetooth, cuando no se vayan a utilizar, ya que éstas pueden ser aprovechadas por los ciberdelincuentes para instalar malware en el dispositivo si estos se conectan de forma automática a una red no confiable o peligrosa [3].

Un ejemplo de vulnerabilidad existente en las conexiones Bluetooth es la conocida como BlueBorne, que puede ser aprovechada por los ciberdelincuentes para infectar el dispositivo con programas maliciosos [100].

25. Desactivar Autorun/Autoplay

Autorun es la capacidad que tienen algunos sistemas operativos para ejecutar una acción, como ejemplo iniciar un programa, en el momento que se introduce un dispositivo extraíble en el equipo, como por ejemplo una memoria USB o un CD [101]. Desde que salió Windows Vista 2006 estas opciones se encuentran deshabilitadas por defecto, pero existen versiones anteriores de Windows que lo tienen activado [3].

Existe malware que se puede distribuir por dispositivos USB y que se aprovechan de la capacidad de ejecutarse automáticamente cuando se insertan en los equipos, por lo tanto se recomienda no activar estas funciones en los sistemas operativos [3].

26. Utilizar puertos no predeterminados

Existen herramientas, como por ejemplo Nmap, que permiten escanear los puertos abiertos que tiene los equipos y asociarlos a los servicios y sus versiones. Los ciberdelincuentes utilizan estas herramientas para encontrar vulnerabilidades asociadas a los servicios que están accesibles desde el exterior, explotarlas y obtener el control del equipo [95].

Un ejemplo de servicio que puede estar accesible a través del puerto TCP/3389 y UDP/3389 es el servicio de Escritorio Remoto de Windows (RDP). Como se ha visto en los apartados anteriores, existen ransomwares que se aprovechan de estos servicios para propagarse por la red e infectar a los sistemas.

Se recomienda modificar en los servicios los puertos preconfigurados por defecto para evitar ser infectados, en el caso de que un malware use una herramienta de escáner de puertos [95].

27. Establecer un máximo de intentos de acceso

Existen programas maliciosos, como los ransomwares Wallet y Dharma [102], que utilizan ataques de fuerza bruta dirigidos a los servicios de escritorio remoto que se encuentran expuestos a Internet.

Se recomienda configurar el acceso a los servicios con contraseña y con un número de intentos de acceso limitado para disminuir el éxito de este tipo de ataques y como consecuencia reducir las infecciones [95].

28. Soluciones que permitan mitigar exploits

Existen herramientas que evitan que se exploten vulnerabilidades de seguridad en los programas [95]. Un ejemplo de este tipo de herramientas es EMET de Microsoft para los sistemas operativos Windows.

EMET o *Enhanced Mitigation Experience Toolkit* permite aplicar medidas de seguridad de forma personalizada para prevenir la ejecución de código dañino y *exploits 0-day* [95]. Entre las medidas que se pueden seleccionar se encuentran:

- Data Execution Prevention (DEP).
- Structure Exception Handler Overwrite Protection (SEHOP).
- Address Space Layout Randomization (ASLR).
- Certificate Trust (Pinning).

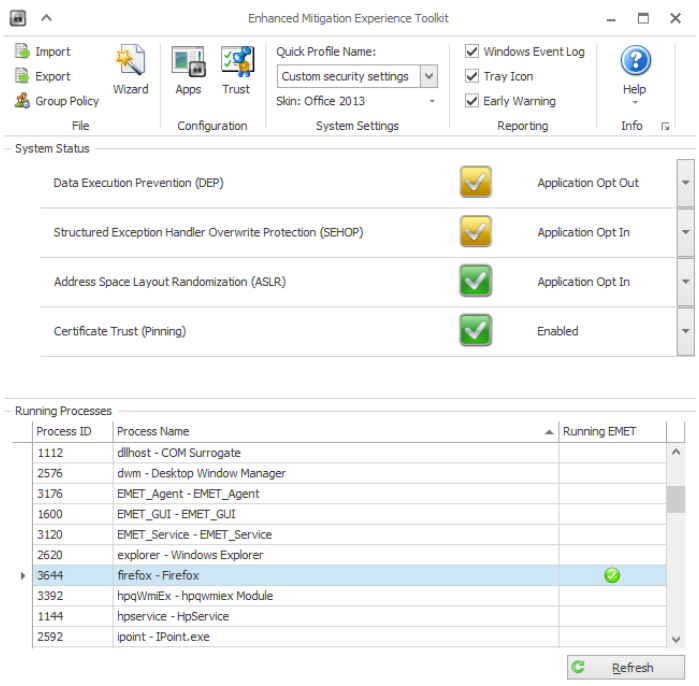


Figura 47: Pantalla principal de EMET [104].

Actualmente los sistemas operativos Windows 10 poseen características que mejoran o son equivalentes a la tecnología de EMET, como son:

- Device Guard: es una combinación de características que permiten bloquear en un equipo todas aquellas aplicaciones que no son de confianza [103].

- Control Flow Guard (CFG): este control permite analizar y descubrir la ubicación de las instrucciones de los programas compilados garantizando así que las instrucciones se ejecutan en

los lugares seguros y esperados y no en zonas de memoria donde no se deberían de ejecutar [103].

- AppLocker: esta función permite que no se ejecuten el uso de aplicaciones y programas no conocidos [103].

En párrafos anteriores se ha visto que existen ransomwares que explotan ciertas vulnerabilidades en los programas para infectar a los equipos, por lo que este tipo de herramientas ayudan a reducir su infección. Estas herramientas no sustituyen a los antivirus, sino que los complementan [95]. Se recomienda utilizar este tipo de herramientas en los equipos para añadir una capa adicional de seguridad.

29. Acceso controlado a carpetas en Windows 10

Windows 10 tiene la opción de establecer un control sobre qué aplicaciones pueden modificar determinadas carpetas. Esta funcionalidad es la que se conoce como “Control de Acceso a la carpeta” y se encuentra en las opciones de “Protección antivirus y contra amenazas” del “Centro de Seguridad de Windows Defender” [105].

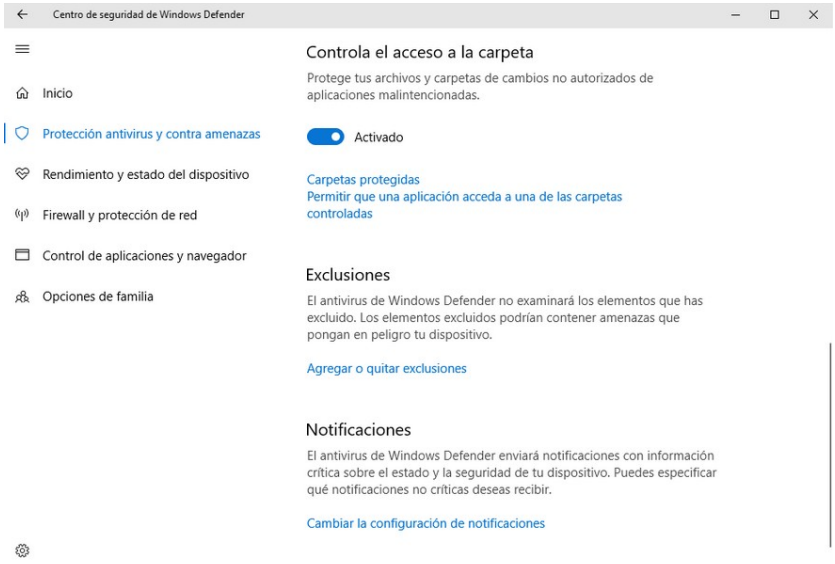


Figura 48: Opción "Control de acceso a carpeta" de Windows 10 [105].

Las carpetas que se establezcan como directorios protegidos no podrán ser modificadas por programas no autorizados. Se recomienda activar y configurar estas funcionalidades en los equipos para evitar que los ransomwares pueda cifrar su contenido [95].

30. Proteger el MBR

El MBR (siglas en inglés de *Master Boot Record*) es el Registro de Arranque Principal o Maestro de un sistema de almacenamiento como por ejemplo un disco duro. Este sistema de arranque se utiliza para iniciar el sistema operativo o para almacenar las tabla de particiones del sistema de almacenamiento [106].

El firmware para el arranque se encuentra en la memoria de solo lectura de la BIOS. La BIOS se ocupa de cargar y ejecutar el MBR, por lo que éste se ejecuta antes de que el sistema operativo sea cargado en el equipo [106]. Existen ransomwares, como por ejemplo Petya o Satán, que se encargan de explotar vulnerabilidades para modificar el MBR y poder controlar el equipo infectado [3].

Se recomienda utilizar herramientas que protejan el MBR para evitar que éste sea modificado. Un ejemplo de este tipo de herramientas es MBRFilter, herramienta de código libre de la empresa de seguridad Cisco, que hace que el Sector Principal sea de solo lectura [107].

31. Eliminar protocolos obsoletos

Ya se ha visto que existen ransomwares que pueden explotar vulnerabilidades asociada a los protocolos. Un ejemplo es el ransomware WannaCry que es capaz de explotar la vulnerabilidad CVE-2017-0144 asociada al protocolo SMBv1 para propagarse por la red.

En general, en las organizaciones se pueden encontrar protocolos obsoletos, como por ejemplo FTP, SMBv1 o Telnet, que ya no se utilizan y que deberían de ser sustituidos por sus versiones más recientes o deshabilitarlos si no son necesarios [3]. Se recomienda que los administradores de los sistemas de la organización detecten este tipo de protocolos y los deshabiliten si ya no son necesarios o los actualicen a las versiones más recientes para evitar que los programas maliciosos puedan aprovecharse de las vulnerabilidades existentes en estos.

2.5.2 Medidas de seguridad reactivas o pasivas

Aplicando las medidas preventivas del punto anterior reducimos la probabilidad de infectarnos con un ransomware. Aún así, cabe la posibilidad de que nos infectemos y, por lo tanto, hay que estar preparados para dar respuesta ante un incidente de una infección por un ransomware [109].

No es una buena práctica que la organización espere a que ocurra una infección con un ransomware u otro tipo de programa malicioso y/o incidente para empezar a pensar cómo se va a responder ante ello. Es importante que una organización tenga bien definido un Plan de Respuesta ante un Incidente, establecer el responsable de gestionar el incidente y qué acciones se llevarán a cabo en la fases que componen la respuesta ante un incidente como son las de preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas [109].

Una vez se tiene definido el Plan de Respuesta ante un Incidente es importante que se practique rutinariamente simulando un incidente para ver cómo responden las personas de la organización y a su vez adquirir la experiencia necesaria para actuar más rápido y mejor ante una posible infección. Se puede comenzar enviando campañas de emails

que contengan como adjunto un simulador de ransomware hacia los trabajadores de la organización. Ejemplo el simuladores de malware pueden ser RanSim, simulador de ransomware de la empresa KnowBe4 o el archivo de testigo EICAR [109].

A continuación se describen las fases de preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas que forman un Plan de Respuesta ante un Incidente para ayudar a los administradores de sistemas de las organizaciones a que estén preparados para actuar ante una posible infección.

1. Preparación
El objetivo de esta fase es preparar a la organización para que posea la capacidad de responder ante un incidente [112]. Esta fase es la más importante, ya que de ella dependerá que el equipo de seguridad responda correctamente ante un caso de análisis.

Un incidente puede ser desde un fallo en el suministro eléctrico o un error en el equipo, pasando por u ataque de un empleado que accede a información confidencial hasta un ataque por ransomware [111]. Esta estudio se va a centrar principalmente en los ataques por ransomware.

Los elementos más importantes que se han de tener preparados y definidos en esta fase son:

- Políticas: una política proporciona una serie de reglas y principios dentro de una organización. Permite orientar al equipo de seguridad para saber si se trata o no de un incidente [111]. Un ejemplo de política puede ser avisar a los usuarios que no pueden descargarse software sin el consentimiento de la organización y que si lo hacen se les podrá sancionar, con políticas como estás se puede evitar la infección por ransomware o en el caso de que ocurra el incidente se puede saber cuál era el programa malicioso que se descargó el usuario [111].

- Plan de Respuesta: el objetivo es definir una estrategia para gestionar el incidente. Los incidentes han de priorizarse teniendo en cuenta el impacto sobre el negocio [111].

- Comunicación: es importante conocer con quién hay que comunicarse, cuándo y cómo hay que comunicarse y el motivo del por qué hay que comunicarse. Es probable que si no existe una estrategia de comunicación el tiempo de respuesta ante un incidente se vea afectado ya que, por ejemplo nos podemos poner en contacto con las personas que no corresponde [111]. Se recomienda establecer un punto de contacto principal [112].

- Documentación: es importante tener bien documentado el incidente porque si se considera un acto delictivo se podrá presentar dicha documentación como evidencia ante un juez y

porque permite, en la fase de lecciones aprendidas, mejorar el conocimiento y la capacitación del equipo para resolver incidencias similares. La documentación ha de poseer todas las acciones realizadas por el equipo de seguridad para afrontar el incidente y responder a las cuestiones quién. qué, cuándo, donde, porqué y cómo [111].

- Equipo de seguridad: el equipo de seguridad ha de estar formado por técnicos especializados en diferentes disciplinas y que posean experiencia suficiente para analizar y gestionar de forma eficiente el incidente [112].

- Control de acceso: es importante que el equipo de seguridad tenga garantizados todos los accesos necesarios para poder gestionar el incidente y poder mitigarlo a tiempo [111].

- Herramientas: es importante poseer herramientas y recursos que aporten valor en la gestión del incidente. Ejemplo de este tipo de herramientas pueden ser herramientas antimalware, snifadores de tráfico de red o una lista de verificación de las acciones realizadas. Se recomienda poseer un conjunto de herramientas que estén dentro de una *Jump bag* para que estén accesibles de forma rápida en el momento del incidente. Esta Jump bag puede contener, por ejemplo, las siguientes herramientas [111]:

    - Documentación que será usada en el incidente como la lista de acciones o las plantillas de documentación que den respuesta a quién. qué, cuándo, donde, porqué y cómo.

    - Lista de miembros del equipo de seguridad y forma de contacto.

    - Discos USB para realizar imágenes forenses.

    - USB de arranque con actualizaciones de las firmas antimalware u otras herramientas que permitan dar respuesta ante el incidente.

    - Un portátil con herramientas forenses, herramientas antimalware y con acceso a internet por si hubiese que conectarse a internet para descargar más herramientas.

    - Cables de red o elementos hardware necesarios en un posible incidente, clonadoras de discos...

    - Una mochila que permita guardar adecuadamente todas las herramientas y que se guarde en un lugar seguro.

- Formación y/o entrenamiento: es necesario que el equipo esté bien preparado y posea una buena formación para que se

gestione de manera adecuada el incidente. Se recomienda realizar simulacros periódicos para que el equipo de seguridad esté bien preparado [111].

- Notificación: es importante definir un método para conocer cómo se va a notificar el incidente [112].

- Tiempo de respuesta: hay que definir un tiempo de respuesta para gestionar el incidente [112]. Este tiempo se puede utilizar como métrica para saber si el equipo de seguridad está mejorando o no en la respuesta ante incidentes.

- Métricas: hay que tener establecidos una serie de indicadores del incidente [112]. Ejemplo de indicadores pueden ser número de infecciones por ransomware mensuales, ataques bloqueados por el antivirus o número de correos maliciosos que no ha bloqueado el filtro de correo electrónico.

En esta fase se debe dar respuesta a las siguientes preguntas [112]:

- ¿Todos los miembros del equipo de seguridad conocen la política de seguridad de la organización?
- ¿Todos los miembros del equipo de seguridad saben con quién han de ponerse en contacto y la forma de hacerlo?
- ¿Todos los miembros del equipo de seguridad tienen acceso a la documentación necesaria para responder ante el incidente?
- ¿Todos los miembros del equipo de seguridad tienen acceso a las herramientas necesarias para responder ante el incidente?
- ¿Todos los miembros del equipo de seguridad han participado en los simulacros para mejorar sus competencias generales?

2. Identificación

El objetivo de esta fase es detectar desviaciones y un intento de ataque o infección por ransomware [112]. Detectar si el comportamiento que se ha desviado de la normalidad se trata de un incidente o no, es decir si realmente se trata de una infección por un ransomware un un falso positivo y además hay que determinar en esta fase el posible alcance de la infección [113].

Si se determina que es una infección, habrá que informar con la mayor brevedad posible al departamento de seguridad informática de la organización, CSIRT o CERT y/o INCIBE para que estos puedan recopilar la información necesaria y se vayan preparando los pasos siguientes [113]. Además, es posible que sea necesario contactar con la policía o con un asesor legal [113].

En esta fase hay que intentar reunir la mayor cantidad de evidencias posibles, hay que recopilar los hechos y analizarlos, para ello hay que apoyarse en diferentes fuentes de información presentes en la organización, realizar preguntas a los afectados y hay que documentar todas las evidencias por si fuese necesario presentarla en un juicio [111].

En esta fase se debe dar respuesta a las siguientes preguntas [112]:

- ¿Dónde tuvo lugar la infección por ransomware?
- ¿Quién y cómo descubrió la infección?
- ¿Existen otras áreas/departamentos afectados por el incidente? Si es así, ¿cuándo se dieron cuenta?
- ¿Cuál es el alcance de la infección?
- ¿Cómo afecta al negocio?
- ¿Qué valor poseen los sistemas afectados por la infección?
- ¿Se ha localizado el origen de la infección? Si es así, ¿dónde, cuándo y cómo?

En particular las preguntas que se realicen y documenten deben de ir enfocadas a contestar las cuestiones siguientes: Quién, Qué, Dónde, Por qué y Cómo [111].

Esta fase se divide en las siguientes pasos de actuación:

1. **Recopilación de información**: consiste en obtener información de las fuentes de datos como pueden ser los logs de los sistemas de seguridad, como por ejemplo de un SIEM, firewall, proxy, IPS, HIDS, o las alertas de los antivirus o errores del sistema. También pueden ser fuentes de información realizar una entrevista a los afectados para saber qué es lo que ha ocurrido.

   Para facilitar la recopilación de información se recomienda que la organización posea una política de retención de logs en la cuál se establezca dónde se van a almacenar de forma centralizada los logs y/o eventos y cuál va a ser el tiempo de retención de estos [112].

2. **Correlación de eventos**: una vez se haya recopilado toda la información posible habrá que determinar si se trata de una infección o no [112]. Habrá que tener en cuenta que los relojes de todos los sistemas estén sincronizados para poder realizar una linea temporal que ayude a realizar un análisis forense si éste fuese necesario. Además, también habrá que conocer cuál es el comportamiento normal de las redes, sistemas y programas de la organización para poder determinar si se trata de un comportamiento que se desvía de la normalidad, un incidente o una infección por ransomware.

   En esta fase la organización se puede apoyar en una Base de Conocimiento que posea la información necesaria para analizar el incidente, como puede ser un histórico de incidentes anteriores, procedimientos o contactos. El acceso a está Base de Conocimiento ha de ser la más rápido posible. También se recomienda poseer una Matriz de Diagnóstico que ayude a determinar qué tipo de incidente puede haber ocurrido ya que relaciona las categorías de los incidentes con sus sintamos asociados.

3. **Priorización de incidentes**: en el caso de múltiples infecciones o múltiples incidentes hay que dar prioridad a aquellos que impacten más en el negocio. Para ello hay que tener en cuenta la criticidad de los recursos afectados y número de usuario y/o procesos de negocio impactados.

4. **Declarar el incidente**: dependiendo del impacto que haya tenido la infección sobre el negocio se deben construir guías que describan la rapidez que ha de tener el equipo que de respuesta ante el incidente. En la declaración del incidente hay que dejar constancia de su categoría y criticidad teniendo en cuanta la base de conocimiento.

5. **Notificar el incidente**: la organización ha de notificar el incidente a la dirección y a las unidades de negocio afectadas para tener el apoyo necesario de éstas.

6. **Documentar la información recopilada**: todo paso que se realiza desde el momento en que se sospecha de un incidente ha de ser documentada hasta su resolución final. Hay que tener en cuenta la línea temporal de los eventos que se van recopilado. Además es necesario proteger la información recopilada del incidente restringiendo el acceso, tanto físico como lógico, de la documentación generada durante el proceso de respuesta.

Un ejemplo de esta fase podrá ser un usuario que contacta con el departamento de seguridad de la organización indicando que en su monitor se muestra un mensaje solicitando que pague por el rescate de sus datos o que ya no puede acceder a sus documentos informáticos porque se encuentran en una extensión extraña. Otro ejemplo relacionado con esta fase podría ser que se detecta tráfico sospechoso dirigido a un servidor de Command & Control relacionado con una campaña de ransomwares o que un usuario ha recibido un correo electrónico con un adjunto que posee la extensión “.pdf.exe”.

3. Contención

El objetivo principal de esta fase es impedir que la infección o el incidente afecte a otros recursos y reducir el impacto que puede tener sobre la organización [113]. Hay que limitar el daño causado y el que pueda causar la infección [111]. Esta fase se divide en las siguientes pasos de actuación:

1. **Contención a Corto Plazo**: el objetivo de este paso es limitar el daño tan pronto como sea posible para que el incidente no empeore la situación. En esta fase se pueden realizar, por ejemplo, las siguientes acciones:
   - Aislar el/los equipos infectados de la red [112].
   - Cambiar el equipo a otra VLAN [112].
   - Bloquear accesos a dominios o direcciones IP maliciosas.
   - Bloquear remitentes de correos maliciosos.

- Deshabilitar cuentas de usuarios que se han infectado o han sido comprometidas o cambiar sus contraseñas [113].

En esta fase se debe dar respuesta a las siguientes preguntas [111]:

- ¿El incidente puede ser aislado?
  - Si la respuesta es sí, hay que proceder a aislarlo.
  - Si la respuesta es no, hay que trabajar con los propietarios y/o administradores del sistema afectado para ver cómo se puede contener el problema.
- ¿Se han aislado todos los equipos afectados de los no afectados?
  - Si la respuesta es sí, continuar con paso de Realizar una imagen forense del sistema.
  - Si la respuesta es no, continuar aislando todos los sistemas afectados hasta que se hayan aislado por completo para prevenir que el impacto o la infección afecte a otros sistemas.

2. **Realizar una imagen forense del sistema**: antes de restaurar el sistema es necesario realizar una imagen forense de los equipos infectados o afectados por el incidente para tener una evidencia de que se ha producido un acto delictivo o para ver cómo funciona el sistema y cómo éste fue infectado o comprometido y de esta forma añadir conocimiento en la fase de lecciones aprendidas y evitar que vuelva a ocurrir el incidente [111]. Hay que realizar como mínimo 2 imágenes forenses que sean una copia bit a bit de la original de todos los sistemas de almacenamiento afectados [112], como puede ser por ejemplo la memoria RAM, el disco duro o cualquier dispositivo que haya podido ser la causa del incidente como una memoria USB u otro. Además, hay que obtener los *hashes* criptográficos de los originales [112] y de las copias para asegurarnos que son copias exactas de los originales y preservar la cadena de custodia si fuese necesario.

   En este paso se debe dar respuesta a las siguientes preguntas [111]:

   - ¿Se han realizado imágenes forenses de los sistemas afectados?
   - ¿Se tienen actualizados todos los comandos y toda la documentación desde el comienzo del incidente?
     - Si la respuesta es no, hay que documentar todas las acciones tan pronto como sea posible para asegurar que se guardan todas las evidencias y que se pueden utilizar en un juicio y/o se puede usar para la fase de lecciones aprendidas.
     - ¿Las copias forenses se han almacenado en un lugar seguro?
       - Si la respuesta es sí, continuar con el paso de la Contención a Largo Plazo.

- Si la respuesta es no, hay que guardar todas las imágenes forenses en un lugar seguro para evitar que éstas sean dañadas y/o manipuladas.

3. **Contención a Largo Plazo**: el objetivo de este paso es reparar el sistema temporalmente para permitir que se siga utilizando en producción si éste no puede mantenerse asilado de la red. En este paso hay que hacer que las operaciones de negocio continúen con normalidad y que el incidente no tenga un impacto adicional.

   En este paso se debe dar respuesta a las siguientes preguntas [111]:
   - ¿El sistema afectado puede seguir aislado de la red?
     - Si la respuesta es sí, continuar con la fase de Erradicación.
     - Si la respuesta es no, significa que el sistema ha de seguir en producción, entonces habrá que realizar acciones como por ejemplo: eliminar el ransomware, aplicar parches de seguridad en todos los equipos, modificar contraseñas comprometidas, eliminar cuentas que haya creado el programa malicioso, eliminar procesos maliciosos que contengan puertas traseras.

4. Erradicación

El objetivo de esta fase es eliminar, si es necesario, los elementos comprometidos y restaurar todos los activos afectados por la infección. En esta fase hay que continuar documentando todas las acciones realizadas para determinar el coste que ha habido en recursos personales y técnicos provocado por el impacto de la infección en la organización [111].

En esta fase hay que asegurarse que se elimina completamente el contenido malicioso de los sistemas afectados para garantizar que están completamente libres de toda posible infección y evitar una posible reinfección [111]. Durante esta fase, se pueden realizar las siguientes acciones:

- Restaurar en el sistema las imágenes de los discos que se crearon antes de que se colocase en producción y, posteriormente, instalarle parches de seguridad y deshabilitar los servicios que no se vayan a utilizar para evitar posibles ataques o infecciones [111].

- Restaurar el sistema con las copias de seguridad que se realizaron antes de que se infectasen [112].

- Escanear los equipos con los antivirus o cualquier otro programa similar para asegurarse que el sistema está libre de virus y utilizar, por ejemplo herramientas que limpien el registro de

Windows para buscar registros maliciosos que haya podido configurar el ransomware [111].

- Eliminar las cuentas que haya podido crear el ransomware y/o el atacante.

- Realizar un análisis de vulnerabilidades de la red para asegurarse que el sistema no puede volver a ser infectado por el ransomware y aplicar los parches de seguridad que las corrijan.

En esta etapa se debe dar respuesta a las siguientes preguntas [111]:

- ¿Es posible restaurar una copia de seguridad, reinstalar el sistema o aplicar parches de seguridad en los equipos afectados?
  - Si la respuesta es no, hay que reflexionar sobre el motivo.
- ¿Se han eliminado todos los programas maliciosos y otros mecanismos creados por los atacantes y se ha endurecido la protección de los sistemas afectados para evitar nuevas infecciones?
  - Si la respuesta es no, hay que explicar el motivo.

5. Recuperación

El objetivo de esta fase es restituir con cuidado los sistemas afectados por la infección al entorno de producción y asegurarnos que el incidente no vuelva a producirse. Es necesario verificar que los sistemas que se están colocando en producción están completamente libres de malware para ello hay que probarlos, monitorizarlos y validarlos [111].

En esta fase se tiene que tomar decisiones como las siguientes [111]:

- Fecha y hora para realizar los operaciones de restauración del sistema [111]. Esta decisión debe de tomarla el propietario del sistema afectado [112].

- ¿Qué acciones se van a realizar para verificar y probar que el sistema está libre de malware y que se encuentra el pleno rendimiento? [111] Como por ejemplo si se va a monitorizar las posibles cambios en la configuración, procesos maliciosos, puertas traseras creadas por el ransomware, modificación de cuentas de usuario, etc. [112].

- ¿Qué herramientas se van a utilizar para monitorizar y validar el correcto funcionamiento del sistema? [111] Como por ejemplo utilizar logs, IPS, HIPS, etc. [112].

- ¿Durante cuánto tiempo se va a estar haciendo el seguimiento del correcto funcionamiento?

En esta fase, hay que asegurarse que se dan respuesta a las siguientes cuestiones [111]:

- ¿Se han corregido todas la vulnerabilidades y se han aplicado medidas que fortalezcan la seguridad del sistema para evitar que vuelva a infectarse el equipo y posibles infecciones futuras?

- ¿Se ha fijado la fecha y la hora para restaurar en producción los sistemas afectados?

- ¿Qué herramientas se van a utilizar para monitorizar y validar la correcta restauración del sistema y que éste no vuelva a ser comprometido por el incidente ocurrido?

- ¿Cuanto tiempo se va a estar monitorizando que el sistema este correctamente y qué es lo que se va a monitorizar?

- Existen lecciones aprendidas o información y/o métricas previas del correcto funcionamiento del sistema que ayuden a comprobar que el sistema afectado se ha restaurado correctamente?

- ¿Pagar el rescate o no pagarlo? Se recomienda no pagar porque no hay una garantía de que los cibercriminales vayan a proporcionar la clave de descifrado, porque se contribuye con el cibercrimen y porque es posible que las empresas de ciberseguridad publiquen alguna herramienta que permita recuperar los ficheros cifrados o los equipos bloqueados [143].

6. Lecciones aprendidas

El objetivo de esta fase es terminar de documentar el incidente completándola con la documentación que no se pudo hacer mientras se gestionaba [111] y un hacer una reunión donde se realice un debate constructivo sobre las lecciones aprendidas [113] para responder a las preguntas qué, dónde, por qué y cómo. Con esta fase se aprende de los incidentes ocurridos dentro de la organización. Este aprendizaje permite mejorar las tareas del equipo de seguridad.

La documentación de las lecciones aprendidas permiten proporcionar un material de referencia en el caso de que en el futuro ocurra un incidente similar [111] y también proporciona un material de capacitación para las nuevas incorporaciones. Como mínimo, la documentación de esta fase ha de poseer la siguiente información:

- Momento en el que se detectó el incidente y quién lo detecto.
- Alcance del incidente.
- Acciones que se realizaron en la fase de contención y erradicación.
- Acciones realizadas durante la recuperación.
- Acciones y/o procedimientos que necesitan ser mejorados.

La documentación de está fase ha de poseer métricas que permitan medir el éxito del equipo de seguridad que ha gestionado el incidente.

Estas métricas pueden ser el número de incidentes atendidos y el tiempo dedicado a cada uno de los incidentes.

En esta fase, hay que asegurarse de que se dan respuesta a las siguientes preguntas [111]:

- ¿El incidente ha quedado completamente documentado?
  - Si la respuesta es sí, hacer un informe para la reunión.
  - Si la respuesta es no, terminar la documentación lo antes posible para que no se olvide ninguna acción que haga que el informe quede incompleto.
- ¿La documentación obtenida responde a las preguntas qué, dónde, por qué y cómo?
- ¿Se puede programar una reunión para realizar el debate sobre lo ocurrido en el incidente?
  - Si la respuesta es no, hay que explicar el motivo e intentar convocar otra reunión lo antes posible.
- En la reunión de las lecciones aprendidas:
  - ¿Se ha revisado el procedimiento de la respuesta ante incidentes con todos los miembros del equipo de seguridad?
  - ¿Se han comentado los errores cometidos en la gestión del incidente y se han propuesto mejoras?

7. Mejora continua

El objetivo de esta fase es actualizar los procedimientos, guías, políticas y métodos de trabajo para mejorar las deficiencias detectadas en la fase de lecciones aprendidas.

2.7 Respuesta del Derecho ante el ransomware

Los primeros ataques llevados a los tribunales relacionados con la informática fueron a comienzos de 1990 en Estados Unidos con el gusano Morris donde se condenó por un jurado federal al creador Robert Morris del gusano [105], éste lo creó con 23 años de edad mientras estudiaba en la Universidad de Cornell [114]. Esta fue la primera condena relacionada con un virus y castigada por la ley de fraudes informáticos de 1986 en Estados Unidos [115].

Los delitos informáticos o “ciberdelitos” son las actividades ilegales que utilizan sistemas informáticos como instrumento para cometer el acto delictivo y tienen como objetivo causar daños, provocar pérdidas o impedir el uso de un sistema informático [116]. Los Estados tipifican los ciberdelitos en sus correspondientes legislaciones, como es el caso de España, que lo tipifica en el Código Penal o en el caso de Estados Unidos que lo tipifica en sus leyes penales especificas. Además existen instrumentos internacionales como el Convenio sobre la Ciberdelincuencia adoptado el 23 de noviembre del 2001 en Budapest o las diversas directivas adoptadas por la Unión Europea [114].

Como hemos visto en los puntos anteriores, la infección por ransomware se puede catalogar como “ciberdelito”, ya que conlleva actos delictivos como por ejemplo el de secuestrar información privada, extorsionar al usuario para pedir un cantidad económica por el rescate de su información [117] o amenazar con publicar la información confidencial si no se paga el rescate. Todos estos delitos están cometidos por medio de un sistema informático.

Los ataques por ransomware son relativamente nuevos para el Derecho. El objetivo de este punto del estudio es conocer la regulación vigente que se encuentra tipificada en el Código Penal Español relacionada con este tipo de acto delictivo y cómo podemos denunciar si nos vemos afectados por uno de estos ataques.

2.7.1 Tipificación Penal

Un ataque por ransomware puede acumular varios tipos de delitos, cada uno con su responsabilidad penal. En términos generales, se puede decir que los cibercriminales que utilizan el ransomware como herramienta delictiva comenten los delitos de daño informático, de estafa, extorsión, amenaza, revelación de secretos y creación y/o pertenencia a una organización criminal entre otros.

En España existen dos sentencias de la Audiencia Nacional, sentencia del N.º 704/2016 del 3 de marzo del 2016 [144] y sentencia N.º 28/16 del 4 de julio del 2017 [145], relacionadas con el ransomware conocido como “el Virus de la Policía” que condenan a las ciberdelincuentes por

utilizar este programa malicioso para cometer delitos de blanqueo de capitales, organización criminal y al creador del virus se le castiga, además, por un delito de estafa utilizado como medio para realizar el delito de daños informáticos [118]. En concreto, se castigó a Alexander Krasnokutsky, líder de la organización criminal acusado de crear el virus a 6 años de prisión y al resto de integrantes se les castigó con penas que ascendían desde los 6 meses a los 3 años de prisión [121].

Hay que tener en cuenta que la legislación española afecta solo cuando los delitos se comenten en territorio español y que una de las dificultades que presentan los ataque por ransomware es que, gracias al uso de Internet, pueden provenir de una criminalidad transnacional [114] y por lo tanto nuestra legislación no les afecta, dificultando de esta forma la identificación y el castigo de los ciberdelincuentes.

1) Delito de Daños Informáticos

En la actualidad tenemos varios artículos en el Código Penal que describen los daños informáticos, en concreto, para los actos delictivos que comenten los cibercriminales con el ransomware se aplicarían los artículos 264, 264 bis y 264 ter dentro de la rúbrica “De los daños”. Para ver qué articulo es el que se le aplica a los cibercriminales hay que tener en cuenta cuál es el comportamiento del ransomware, ya que si su comportamiento es de la familia Criptolocker (cifra ficheros) se le aplicará el artículo 264, mientras que si es del tipo Lockscreen (bloquea el acceso al sistema) se le aplicará el artículo 264 bis [118].

En el artículo 264 podemos observar que la conducta delictiva de los cibercriminales que utilizan el ransomware encaja en este artículo porque el comportamiento del malware hace inaccesible los datos informáticos cuando cifra los documentos almacenados en el sistema. Cabe destacar que las penas se agravan si el acto delictivo se perpetua dentro de una organización criminal, si existe cifrado masivos de información; afecta a servicios públicos esenciales como por ejemplo un hospital; o afecta a la Seguridad de Estado o Unión Europea, como por ejemplo el Gobierno. El artículo 264 establece:

> ***“****Artículo 264 del Código Penal*
> *1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.*
>
> *2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:*
> 1. *Se hubiese cometido en el marco de una organización criminal.*
> 2. *Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.*

3. *El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.*
4. *Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.*
5. *El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter."*

En el estudio del artículo 264 bis se puede ver que se castiga a los cibercriminales que utilizan el ransomware cuando éste obstaculiza el funcionamiento del sistema. Además, las penas se agravan si el ransomware afecta al correcto funcionamiento de una organización, como puede ser una empresa, o a la Administración Pública. El artículo 264 bis dice:

> ***"****Artículo 264 bis del Código Penal*
> *1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:*
>
> *a) realizando alguna de las conductas a que se refiere el artículo anterior;*
> *b) introduciendo o transmitiendo datos; o*
> *c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.*
>
> *Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado. [...]"*

El articulo 264 ter es interesante porque castiga al creador del programa malicioso. Este artículo se aplicaría al programador del ransomware y a los cibercriminales que están detrás del modelo de negocio del Ransomware como Servicio porque proporcionan el malware a otros cibercriminales para que cometan los delitos de daños informáticos descritos en los artículos 264 y 264 bis. El artículo 264 ter establece:

> *"Artículo 264 ter del Código Penal*
> *Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente*

autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o
b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información [...]".

2) Delito de Estafa

El Código Penal establece que para que exista el delito de estafa ha de existir engaño [118] para que la víctima cometa un error y ánimo de lucro. El engaño por parte de los cibercriminales existe cuando estos utilizan técnicas de ingeniería social para confundir a la víctima haciendo que pinche un enlace que se descarga el ransomware o abriendo un adjunto que puede ser el malware.

"Artículo 248 del Código Penal
1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.
c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero."

3) Delito de Extorsión

Otro de los delitos que puede encajar en las conductas criminales asociadas al ransomware es el de extorsión porque puede obligar a la víctima, siempre que exista intimidación, a que dañe el patrimonio de la organización en la que trabaja [118].

"Artículo 243 del Código Penal
El que, con ánimo de lucro, obligare a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero, será castigado con la pena de prisión de uno a cinco años, sin perjuicio de las que pudieran imponerse por los actos de violencia física realizados."

4) Delito de Revelación de secretos

Estaríamos ante un delito de revelación de secretos [117] cuando los cibercriminales publican la información secuestrada sino se ha realizado el pago del rescate, tal cómo suelen exponer en sus mensajes de solicitud de pago. El artículo 197 del código penal establece lo siguiente:

> *"Artículo 197 del Código Penal*
> *1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses [...]"*

5) Delito de Amenazas

Cuando el ransomware amenaza a las víctimas con cometer el delito de revelación de secretos estaríamos ante un delito de amenazas. El articulo 169 del Código Penal establece que existe delito de amenaza cuando se amenaza a una persona con provocarle un mal que constituya delito y además, entre otras causas, se le exige una cantidad económica. A continuación se expone el contenido del artículo 169 del Código Penal:

> *"Artículo 169 del Código Penal*
> *El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado:*
>
> *1.º Con la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años.*
>
> *Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos.*
>
> *2.º Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional."*

6) Delito de Organización Criminal

Tal y como hemos visto en los modelos de negocio, es posible que detrás de la creación de las campañas de ransomware se encuentren

organizaciones criminales, ya que por una parte tendríamos a los creadores del programa malicioso, y por otra a los que lo difunden. Es difícil que los ransomware estén creados por una sola persona. Por eso es posible que otra de las conductas delictivas que se puedan incluir es la de crear y/o pertenecer a una organización criminal, tal y como expone el artículo 570 bis del Código Penal:

> *"Artículo 570 bis del Código Penal*
> *1. Quienes promovieren, constituyeren, organizaren, coordinaren o dirigieren una organización criminal serán castigados con la pena de prisión de cuatro a ocho años si aquélla tuviere por finalidad u objeto la comisión de delitos graves, y con la pena de prisión de tres a seis años en los demás casos; y quienes participaren activamente en la organización, formaren parte de ella o cooperaren económicamente o de cualquier otro modo con la misma serán castigados con las penas de prisión de dos a cinco años si tuviere como fin la comisión de delitos graves, y con la pena de prisión de uno a tres años en los demás casos.*
>
> *A los efectos de este Código se entiende por organización criminal la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos."*

2.7.2 Cómo denunciar

En el caso de que se sufra una infección por ransomware se recomienda denunciar el incidente para que se investigue el origen del delito y de está forma se puede colaborar para ayudar a que otras organizaciones prevengan la infección y se pueda capturar a los ciberdelincuentes [119].

En España se puede denunciar este tipo de actos delictivos en el Grupo de Delitos Telemáticos de la Guardia Civil y/o en la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional [119].

El Grupo de Delitos Telemáticos de la Guardia Civil indica en su página web que se pueden denunciar los delitos informáticos si se es víctima o testigo de uno. Para denunciar es necesaria la personificación del denunciante o su representante legal en un juzgado o centro policial para que acredite su identidad, conforme a los artículos 265 y 266 de la Ley de Enjuiciamiento Criminal. Esta denuncia dará lugar a un procedimiento judicial en el que el denunciante o su representante legal podrán ser citados para declarar y efectuar las reclamaciones previstas por la ley [119].

2.8 Caso: ataque WannaCry

La tarde del viernes 12 de mayo de 2017 tuvo lugar uno de los ataque de ransomware más grandes de la historia. El ransomware responsable de este ataque fue WannaCry, también conocido como WannaCryptor 2.0 o Wanna Decryptor que fue capaz de infectar a más de 230.000 equipos en más de 150 países. Para infectar los equipos WannaCry utilizaba como vector de infección una vulnerabilidad en la implementación del protocolo SMB de los sistemas operativos Windows [122]. A continuación se describe cómo ocurrió este ataque y sus consecuencias.

2.8.1 Antecedentes

El 14 de marzo de 2017 Microsoft publica la actualización de seguridad MS17-010 para corregir una vulnerabilidad presente en el protocolo SMB v1 que se utiliza para compartir recursos como archivos e impresoras entre los equipos [123]. Esta vulnerabilidad esta catalogada con el CVE-2017-0144 y afecta a los sistemas Microsoft Windows Vista SP2, Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1, Windows 10 Gold 1511 y 1607 y a Windows Server 2016. La característica de está vulnerabilidad es que permite a un atacante remoto ejecutar código arbitrario [124].

Dos meses después, el 8 de abril de 2017, el grupo de *Hackers malos* "The Sahdow Bokers" publica el exploit EternalBlue que se aprovecha de la vulnerabilidad expuesta en el párrafo anterior. Este grupo consiguió infiltrarse en los sistemas de la Agencia de Seguridad Nacional de Estados Unidos, conocida por sus siglas en inglés NSA, y robar un conjunto de herramientas entre las cuales se encontraba este exploit para luego publicarlo en el repositorio de código Github [125]. Este exploit se encuentra disponible en la conocida herramienta Metasploit.

```
msf exploit(ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of times to groom the kernel pool.
   GroomDelta          5                yes       The amount to increase the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times to retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject payload into.
   RHOST                                yes       The target address
   RPORT               445              yes       The target port (TCP)
   VerifyArch          true             yes       Check if remote architecture matches exploit Target.
   VerifyTarget        true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Figura 49: EternalBlue en Metasploit [126]

Por alguna razón desconocida, quizás falta de concienciación por parte de los usuarios y administradores de sistemas, muchos organizaciones

con Windows en sus equipos no aplicaron el parche de seguridad MS17-010 que corregía esta vulnerabilidad [122].

Otra de las herramientas que fue robada a la NSA por este grupo fue la puerta trasera DoublePulsar [127]. Esta puerta trasera permite dejar a los ciberdelincuentes vía libre al equipo afectado. A continuación se muestra parte del uso de este exploit en la herramienta Metasploit.

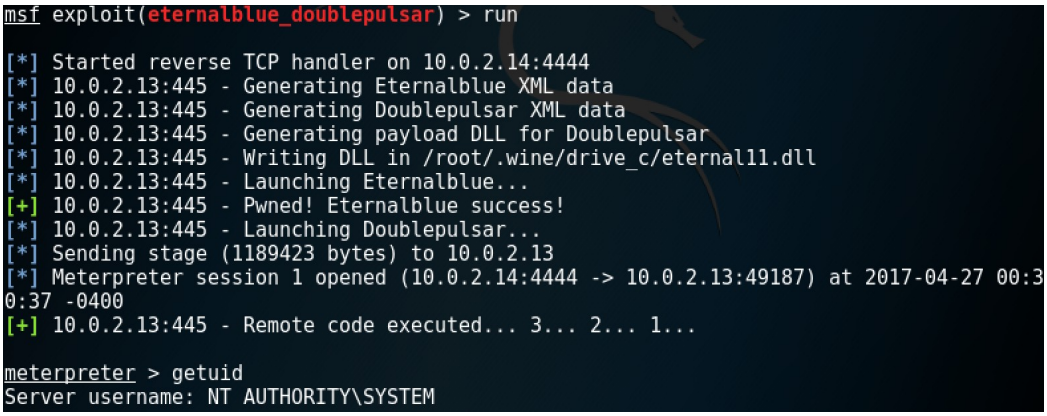


Figura 50: DoublePulsar en Metasploit [128]

En abril del mismo año, los expertos en seguridad detectan, gracias a los escaners de Internet, que más de 107.000 equipos en todo el mundo pueden ser vulnerables a DoublePulsar [129]

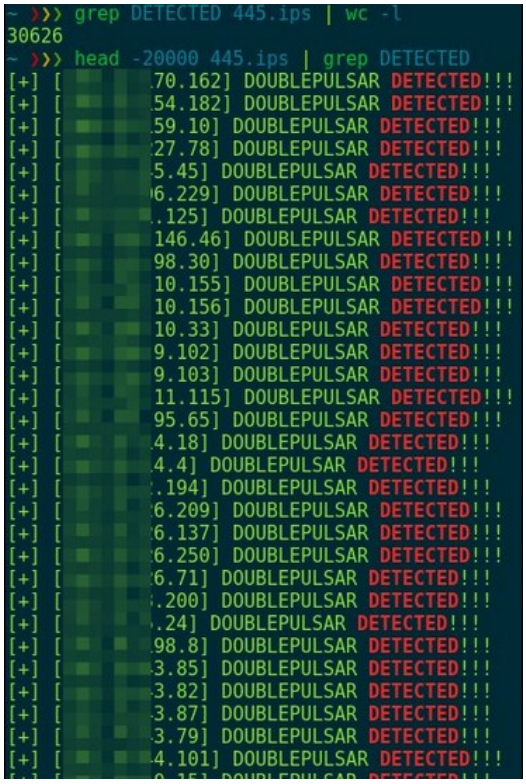


Figura 51: Resultados parciales del escaneo de DoublePulsar [130]

2.8.2 Ataque

La tarde del viernes 12 de mayo, WannaCry empezó a infectar múltiples equipos en el mundo. WannaCry utiliza el exploit EternalBlue y la puerta trasera DoublePulsar para infectar a los equipos y propagarse por los sistemas informáticos. Gracias a estos exploits este ransomware gana la capacidad de comportarse como los programas maliciosos de tipo gusano informático para poder escanear equipos que se encuentran en la red local al equipo afectado e infectar a otros equipos que se encuentran en su red [130].

La primera acción que utiliza WannaCry para infectar el equipo es utilizar el exploit EternalBlue para enviar un mensaje malicioso que permite explotar las vulnerabilidades de protocolo SMB de Windows del equipo si éste no posee instalado el parche MS17-010 que publicó Microsoft. Luego, utiliza el exploit DoublePulsar para dejar una puerta trasera que permita acceder al equipo [130].

Una vez WannaCry ha conseguido el control del equipo, éste se comporta como el resto de ransomwares, comienza a cifrar los ficheros del equipo infectado y posteriormente muestra un mensaje en el escritorio que informa al usuario que si quiere recuperar sus archivos cifrados ha de pagar 300 dólares en Bitcoins por ellos [130].

Figura 52: Mensaje de rescate de WannaCry [131].

El paso siguiente a la infección del equipo es comportarse como un gusano informático, para ello escanea toda la red en la que se encuentra el equipo infectado para buscar el puerto TCP/445 abierto y si los equipos de la red tienen instalados Windows y utilizan SMBv1 vulnerable entonces accede a ellos y los infecta, comprometiendo de esta forma a toda la red de la organización. Hay que tener en cuenta que este

ransomware no explota una *vulnerabilidad 0-day,* ya que Microsoft había publicado dos meses antes del ataque el parche que corregía dichas vulnerabilidades [130].

Cuando se produjo el ataque, muchas organizaciones en todo el mundo no habían instalado aún los parches que corregían las vulnerabilidades de Windows que explotaba WannaCry y se vieron afectados por la infección [122].

2.8.3 Impacto

El CERT de Seguridad e Industria (CERTSI) ha realizado un estudio de las direcciones IP afectadas por el ransomware WannaCry que permite valorar el impacto nacional y global entre los días 13 y 19 de mayo.

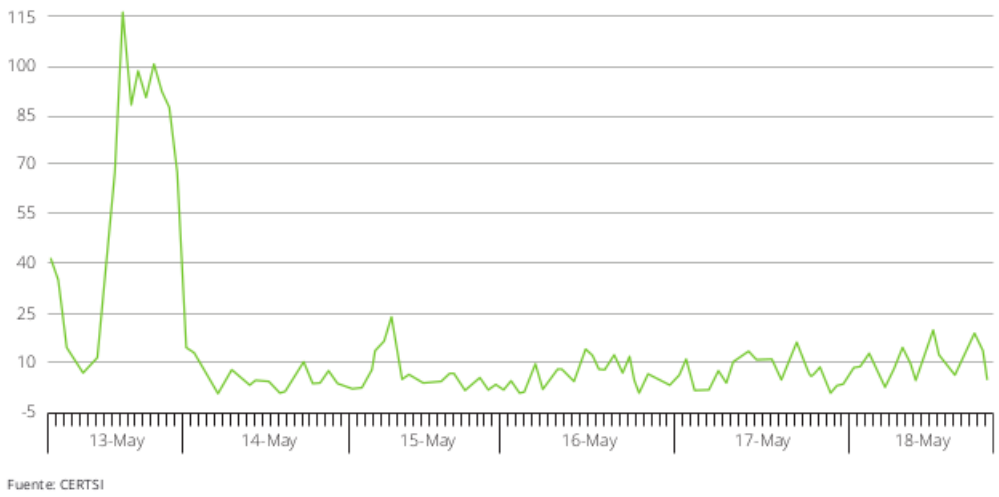


Figura 53: Direcciones IP afectadas en España [130].

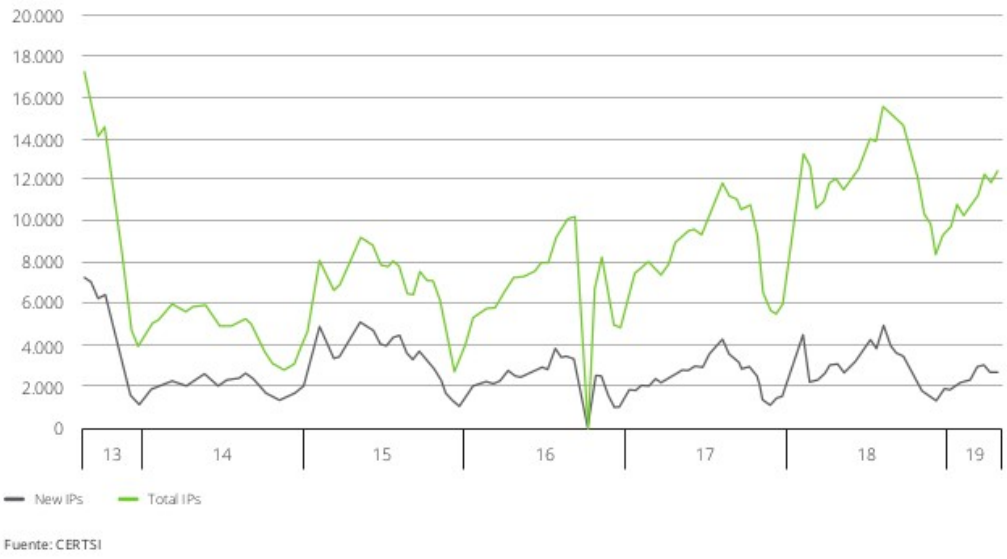


Figura 54: Direcciones IP afectadas mundialmente [130].

Según la Europol (Oficina Europea de Policía) este ataque no tiene precedentes en la historia informática, ya que se estima que, aproximadamente, fueron infectados 200.000 equipos en más de 150 países [122]. Este ataque ha afectado principalmente a países europeos y Rusia [132].

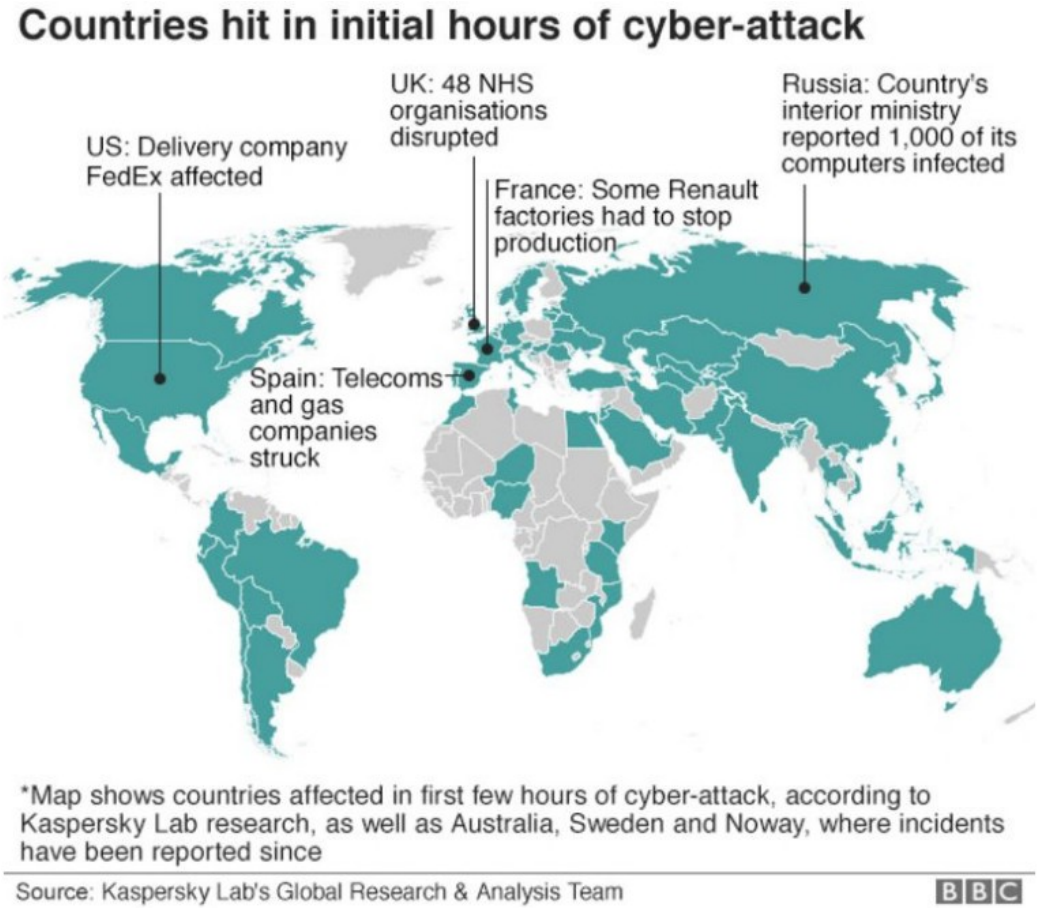


Figura 55: Países afectados por WannaCry [132].

Según el Servicio Nacional de la Salud de Reino Unido (NHS), más de 48 hospitales de este país fueron alcanzados por el ataque de este programa malicioso, dejando a hospitales y médicos sin acceso a los datos de los pacientes y obligando a cancelar las operaciones y las citas médicas [132].

Rusia ha sido el país que mas infecciones se han registrado. La infección de WannaCry afectó a sus bancos, a su red de ferrocarriles y a su red de telefonía móvil y a más de 1.000 equipos de su Ministerio de Interior [132]. También afectó a una planta de la empresa automovilística Nissan [133].

En EEUU, la firma de logística FedEx reconoció que el ataque fue efectivo sobre sus sistemas y como medida preventiva mantuvo sus equipos desconectados hasta el lunes 15 de mayo del 2017 [133].

La principal operadora de comunicaciones portuguesa, Portugal Telecom, también admitió que fue afectada por el programa malicioso.

En Italia infectó a un laboratorio de computación universitario y en Suecia a una autoridad local [132]. En Alemania afectó principalmente a la red de ferrocarriles estatales [132]. En Francia perjudicó a la empresa de automóviles Renault, la cual se vio obligada a parar la producción en varios lugares [132].

En Asia afectó a múltiples colegios en China , y a bastantes hospitales en Indonesia y Corea del Sur [132].

En España el ransomware logró infectar a la empresa de telecomunicaciones Telefónica, y a empresas de servicios públicos como Iberdrola y Gas Natural [132]. Otras grandes empresas como Vodafone, Capgemini o Everis también pudieron haber sido afectadas por el ransomware. El CNPIC (Centro Nacional para la Protección de las Infraestructuras Críticas) y el INCIBE confirmaron que parece ser que no hubo más de diez empresas españolas afectadas por el ataque [133]. Ante esta situación muchas organizaciones solicitaron a sus trabajadores que apagasen sus equipos como medida preventiva ante una posible infección [133].

Figura 56: Correo de aviso de Telefónica [134].

2.8.4 Contención

Mientras el ataque con WannaCry estaba infectado a múltiples sistemas en todo el mundo, un joven investigador informático del Reino Unido de 22 años, Marcus Hutchins, conocido en la redes sociales bajo el seudónimo MalwareTech logró encontrar un “botón de apagado” mientras analizaba el programa malicioso que permitió detener la infección masiva de éste ransomware [122].

Los cibercriminales creadores del ransomware implementaron un dominio oculto [136] en el código de WannaCry que no estaba registrado y éste lo utilizaba para decidir si cifraba o no el equipo. Si WannaCry no se conectaba al dominio entonces infectaba el equipo, si lograba conectarse entonces se detenía y no cifrada los ficheros [135]. Marcus Hutchins se dio cuenta de que si registraba el dominio relacionado con WannaCry siempre recibiría respuesta y por lo tanto se detendría la infección [135]. El día 12 de mayo de 2017 a las 17:08 UTC Marcus compró el dominio por 10,69 dólares, aproximadamente 10 euros, y redirigió las peticiones de WannaCry a un servidor de Los Ángeles [136] cesando de esta forma el ataque [135].

Paralelamente, Microsoft publicó una declaración que recomendaba a todos los usuarios de Windows que instalasen la actualización MS17-010 para corregir la vulnerabilidad que explotaba WannaCry. Además, también corrigió está vulnerabilidad para los sistemas Windows que ya no tenían mantenimiento como Windows XP, Windows 8 y Windows Server 2003 [122].

El 16 de mayo de 2017 con ayuda de la ingeniería inversa, investigadores de la Universidad College de Londres consiguieron obtener la herramienta PayBreak. Esta herramienta permite obtener las claves de sesión únicas que utiliza WannaCry para el cifrado. WannaCry utiliza su propia función de cifrado AES-128-CBC. Paybreak se configura para enlazar funciones arbitrarias, incluida la función AES personalizada de WannaCry, y registrar los parámetros que se le han pasado como la clave. Para ello se conecta a la función de Windows CryptGenRandom, para crear nuevas claves de sesión única que utiliza WannaCry y la mayoría de ransomwares y está herramienta permite interceptar las claves y guardarlas a la salida de la función [137].

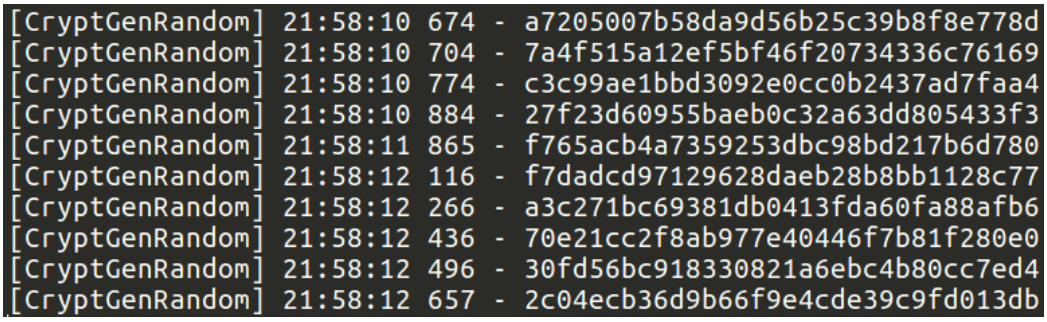
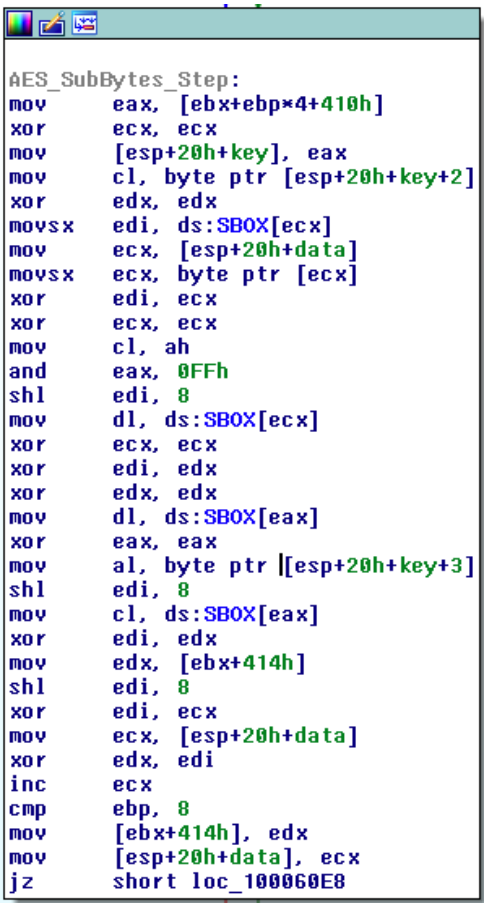


Figura 57: Claves de CryptGenRandom [137].

Para recuperar los archivos tan solo hay que probar cada una de las claves de sesión únicas que se han generado con los archivos cifrados por WannaCry hasta que se descifren todos los ficheros. Descifrar aproximadamente 1000 archivos cuesta unos 94 minutos [137].



```
AES_SubBytes_Step:
mov     eax, [ebx+ebp*4+410h]
xor     ecx, ecx
mov     [esp+20h+key], eax
mov     cl, byte ptr [esp+20h+key+2]
xor     edx, edx
movsx   edi, ds:SBOX[ecx]
mov     ecx, [esp+20h+data]
movsx   ecx, byte ptr [ecx]
xor     edi, ecx
xor     ecx, ecx
mov     cl, ah
and     eax, 0FFh
shl     edi, 8
mov     dl, ds:SBOX[ecx]
xor     ecx, ecx
xor     edi, edx
xor     edx, edx
mov     dl, ds:SBOX[eax]
xor     eax, eax
mov     al, byte ptr [esp+20h+key+3]
shl     edi, 8
mov     cl, ds:SBOX[eax]
xor     edi, edx
mov     edx, [ebx+414h]
shl     edi, 8
xor     edi, ecx
mov     ecx, [esp+20h+data]
xor     edx, edi
inc     ecx
cmp     ebp, 8
mov     [ebx+414h], edx
mov     [esp+20h+data], ecx
jz      short loc_100060E8
```

Figura 58: Algoritmo AES de WannaCry [137].

2.8.5 Acusaciones

El Departamento de Justicia de Estados Unidos acusó al programador Pak Jin Kyok de Corea del Norte y a la empresa Chosun Expo Joint Venture como responsables del ataque con WannaCry. Además, también se le atribuye al programador Pak Jin Kyok el ataque que tuvo lugar en 2014 a la empresa Sony Pictures y el ataque al Banco Central de Bangladesh en 2016. Estados Unidos alegó que el responsable actuó “en nombre del Gobierno de Corea del Norte o del Partido de los Trabajadores de Corea” [138].

El 24 de noviembre de 2014 la empresa Sony Pictures Entertainment Inc. sufrió uno de los ciberataques más grandes dirigidos a una empresa de Estado Unidos. El ataque consistió en paralizar los sistemas informáticos de la empresa y en filtrar grandes cantidades de datos como 12.000 correos electrónicos y registros financieros de la industria

de Hollywood. Se estima que los daños económicos fueron aproximadamente de 200 millones de dólares [139]. En febrero de 2016 el Banco Central de Bangladesh sufrió otro de los ataques informáticos más grandes de la historia que consistió en el robo de 81 millones de dolares [140] aprovechándose de una serie de vulnerabilidades que tienen los sistemas de mensajería que utilizan los bancos [141].

Pak Jin Kyok formaba parte del grupo de hackers malos llamado Lazarus Group [138]. No se conoce mucho sobre los miembros de Lazarous Group porque su identidad es anónima, pero si que se sabe que trabajan en grupo y que es posible que esté relacionados con Corea del Norte aunque esto puede ser un intento de engaño, ya que los autores de estos ciberataques pueden estar dejando pistas falsas para que se señale a Corea del Norte como presuntos culpables. Lazarous Group utiliza ataques sofisticados para intentar conseguir el mayor beneficio posible. Según Karspersky Lab, que ha estado investigando este tipo de ataques financieros, dicen que su forma de trabajar es infiltrarse en el banco accediendo a un único equipo para después de estar varias semanas en su interior, estudiar el entorno del banco y robar su dinero. El objetivo de este grupo de hackers malos no solo son los bancos, sino que también se encuentran, entre otros, negocios de criptomonedas y casinos [142].

3. Conclusiones y trabajo futuro

En este último capítulo se recopilan las conclusiones obtenidas tras el desarrollo de este estudio, los objetivos cumplidos y el posible trabajo futuro que puede surgir desde el punto actual.

3.1 Conclusiones

El ransomware es una amenaza para todos los sistemas informáticos. Este programa malicioso va a estar entre nosotros unos cuantos años más y es por ello que debemos de estar preparados para evitar que nuestros equipos sean infectados. La precaución y educación en seguridad informática es clave para protegernos de los ataques por ransomware.

Las múltiples variantes del ransomware, cada vez más distintas, llevan a éste a una nueva etapa con nuevos objetivos y nuevas formas de actuar con múltiples vectores de infección. Los ataque por ransomware son cada vez más sofisticados y estos evolucionan siguiendo el incremento del uso de las nuevas tecnologías.

Los cibercriminales ofrecen nuevos modelos de negocio que permiten facilitar el uso de este malware como herramienta de extorsión. Estos nuevos modelos de negocio ayudan a que los ataques por ransomware sean un negocio lucrativo para los cibercriminales, ya que permiten, gracias al uso de Internet, atacar a cualquier sistema del mundo y reducir el riesgo de ser capturados.

Se debe de poner la mayor cantidad posible de medidas preventivas para evitar el éxito de los ataques por ransomware, aunque la implementación de éstas no garantiza que los sistemas no puedan ser infectados y es por ello que hay que adoptar medidas reactivas que nos permitan responder con la mayor brevedad posible si nuestros equipos son comprometidos.

El Estado de Derecho intenta combatir y erradicar el impacto social y económico que tienen los ataques por ransomware mediante la aplicación de leyes Estatales e Internacionales que castigan a los cibercriminales que comenten múltiples delitos con el uso de este programa malicioso. Hay que denunciar para colaborar con la sociedad y reducir el daño que genera la infección por ransomware en nuestra sociedad.

El ataque mundial con el ransomware WannaCry demuestra lo vulnerable que es la sociedad digital en la que vivimos ante los ciberataques y además demuestra que es necesario que las organizaciones se tomen muy en serio la seguridad informática.

3.2 Objetivos cumplidos

Después del desarrollo del presente estudio se ha logrado cumplir con los siguientes objetivos:

- Comprender el concepto de ransomware: este objetivo se logra exponiendo las características que posee el ransomware, para ello se define qué es este programa malicioso y se estudia su origen, su estado actual y su futuro. Para conseguir este objetivo se ha utilizado una metodología exploratoria que ofrecer al lector un primer acercamiento al problema, ya que con esta metodología se proporciona un conocimiento de las características principales que posee el ransomware.

- Conocer los tipos de ransomware que existen en la actualidad: la consecución de este objetivo se alcanza definiendo las familias en las que se agrupa este malware y describiendo, de todas las variantes detectadas, aquellas que por sus características o comportamiento se diferencian de las demás o introducen una nueva forma de actuar. Este objetivo se alcanza con la aplicación de una metodología descriptiva, ya que con el conocimiento de las diferentes familias y variantes del ransomware se ha podido definir las diferentes formas de actuar que tiene este programa malicioso.

- Describir cómo infecta los sistemas informáticos: este objetivo se consigue mostrando los vectores de infección más comunes que utiliza el ransomware para introducirse en los sistemas informáticos. Para lograr este objetivo se utiliza una metodología descriptiva que nos permite explicar cómo este malware alcanza a los equipos para luego infectarlos.

- Conocer el modelo de negocio que se esconde detrás de las campañas de infección: este objetivo se logra conociendo cómo funciona el modelo de negocio Ransomware como Servicio y el modelo tradicional. Se continua con el uso de la metodología descriptiva para lograr este objetivo, ya que se describen los dos modelos de negocio que se esconden con el uso de este programa malicioso.

- Describir las técnicas que existen en la actualidad para detectar y mitigar su infección: este objetivo se alcanza exponiendo las medidas de seguridad, tanto preventivas como reactivas, que se pueden aplicar en los sistemas informáticos y en las organizaciones de todo el mundo. Para conseguir este objetivo se utiliza una metodología descriptiva que permite analizar los procesos que se pueden llevar a cabo para proteger los sistemas y reaccionar ante una infección.

- Conocer las medidas legales que está adoptando la sociedad española para protegerse frente a esta amenaza: para lograr este objetivo se ha realizado un recorrido por los principales artículos del Código Penal Español que castigan las conductas delictivas que conlleva la utilización del ransomware y se explica cómo denunciar en el caso de nuestros equipos se infecten por esta amenaza. Se continua el uso de una metodología descriptiva para lograr este objetivo que nos permite analizar el Código Penal Español y encontrar aquellos artículos que están relacionados con las conductas delictivas asociadas al ransomware.

- Conocer el caso del ataque del ransomware WannaCry: este objetivo se consigue exponiendo las causas que ayudan a que el ataque tenga lugar y describiendo en qué consiste el ataque, qué impacto tuvo y cómo se detuvo la infección mundial. Para lograr este objetivo se aplica una metodología explicativa que permite explicar qué condiciones provocaron que el ataque se llevará a cabo, cómo fue el ataque y quienes son los responsables de éste.

Este estudio permite concienciar al lector de la amenaza que supone el malware ransomware porque utiliza un lenguaje simple que permite, además, este estudio colabora en la reducción y prevención de las infecciones por ransomware ayudando de esta forma a cubrir la necesidad de proteger su información que poseen las organizaciones.

3.3 Trabajo futuro

A continuación se presentan unas lineas de trabajo que pueden surgir a partir del presente estudio:

- Creación de un curso formativo destinado a administradores de sistemas y al público en general que ayude fortalecer la seguridad de su infraestructura informática.

- Complementar el estudio mediante el análisis estático del código que implementa un ransomware.

- Realizar un seguimiento de la evolución de los ataques que surgen y posibles nuevas formas de actuar que pueda adquirir el ransomware.

4. Glosario

Autoexe.bat: es un archivo que poseen los sistemas operativos Windows que permite ejecutar de forma automática determinados comandos cuando se inicia el sistema.

BitTorrent: es un protocolo utilizado para intercambiar archivos entre los usuarios utilizando Internet y una red del tipo Peer-to-Peer.

Botnet: es un conjunto de equipos informáticos que están infectados y que son controlados de forma remota por los cibercriminales para cometer sus delitos.

Cibercriminales: sinónimo de ciberdelincuentes.

Ciberdelincuentes: son las personas que utilizan internet y la informática para cometer delitos.

Cortafuegos de correo: son dispositivos o programas que poseen un conjunto de herramientas, como por ejemplo filtros anti-spam o antivirus, que evitan que lleguen los correos maliciosos a sus destinatarios finales.

Cryptominers: es un tipo de malware cuya función principal es minar criptomonedas para que los ciberdelincuentes obtengan un beneficio económico.

Deep Web: ver definición de Red TOR.

Dropbox: es un servicio de almacenamiento de ficheros que se ofrece en Internet y que pertenece a la empresa Dropbox Inc. [147].

Exploit kit: es una herramienta que permite aprovecharse de una vulnerabilidad en los programas para que estos se comporten de una determinada forma. Suelen se utilizados por los programas maliciosos y por los ciberdelincuentes para obtener el control de los equipos.

Exploits 0-day: una vulnerabilidad existente en un programa y que no ha sido revisada por los fabricantes o por expertos en la materia para corregirla mediante un parche de seguridad se suele conocer como vulnerabilidad 0-day. Un Exploit 0-day es un programa que se aprovecha de este tipo de vulnerabilidades.

Filtros anti-spam: estos filtros los suelen poseer los servidores y dispositivos que analizan el correo para evitar que le lleguen al usuario final los correos electrónicos no deseados, como por ejemplos los que se utilizan en campañas de publicidad no deseada o abusiva.

Gameover Zeus: es una botnet relacionada con el troyano bancario Zeus que se utilizaba para robar las credenciales a los usuarios.

Gusano informático: es un programa malicioso cuya propiedad principal es que es capaz de hacer una copia de si mismo para contagiar a otros equipos.

Hash: es una función o algoritmo que tiene como entrada una serie de datos y como salida una serie de caracteres de longitud fija, es decir permite convertir los datos de entrada en una serie de caracteres. Si uno de los datos de las serie de datos que se tiene como entrada cambia, el resultado de la salida de la función hash será diferente.

Index.html: es el archivo por defecto que se muestra cuando se accede a un dominio de una página web.

Ingeniería social: es una técnica que utiliza la manipulación de las personas para obtener información confidencial de éstas como por ejemplo contraseñas de acceso a un equipo.

Internet of Things: este término hace referencia a la conexión de diferentes objetos cotidianos, como la cafetera o el televisor, a Internet para que ganen funcionalidades.

Jump bag: es una mochila que posee diferentes herramientas, como un equipo portátil, cables o herramientas forenses, que se utiliza para dar una respuesta rápida a un incidente.

Malware: proviene de la combinación de las palabras inglesas malicious y software, es decir son los programas maliciosos como por ejemplo los virus, los troyanos o, como en el caso de este estudio, el ransomware.

Messenger: programa propiedad de Microsoft que sirve para enviar mensajes que dejó de utilizarse en 2005 y que fue sustituido por el programa Skype [146].

Network Attached Storage (NAS): son dispositivos de almacenamiento en red que permiten compartid unidades de almacenamiento, como por ejemplo discos duros, entre diferentes usuarios para que estos compartan sus ficheros.

Payload: es la parte de un programa que se encarga de hacer daño al equipo. Un ejemplo de payload sería la parte del programa que posee un troyano que permite que se conecta con el servidor del Comand & Control de una Botnet.

Peer-to-Peer: es un tipo de red de ordenadores en las que todos los equipos actúan como clientes y servidores de forma simultánea [148].

Phishing: es una técnica que utilizan los cibercriminales que consiste en suplantar la identidad de una persona y/o empresa mediante el uso de un correo falso para engañar a los usuarios y hacer que estos sean víctimas de un fraude, inducirles a que pinchen sobre un enlace

malicioso o que se descarguen un adjunto que en realidad es un malware.

Phishing dirigido: es un phishing que esta dirigido a una persona o grupo de personas determinado y que suele estar más elaborado para aumentar las probabilidades del éxito del ataque.

Red TOR: es una red de comunicaciones que permite mantener el anonimato a nivel de red (a nivel de dirección IP), también se le conoce como Deep Web o Darknet.

Registro de Arranque Maestro (MBR): es el primer sector de un dispositivo de almacenamiento de datos. Por ejemplo, en los discos duros instalados en los equipos es el primer sector que se utiliza para iniciar el sistema operativo.

SSH: es un protocolo de comunicaciones que permite a los usuarios conectarse en remoto a un equipo. Suele tener asociado el puerto TCP/22.

SaaS: es un modelo de negocio de distribución de software donde el servicio de mantenimiento, la operación diaria de soporte del software y los datos se gestionan en Internet, es decir en los servidores de la empresa que lo ofrece y no en los equipos del cliente.

Servidor de Command & Control: son los servidores de los ciberdelincuentes que permiten controlar los programas maliciosos o las botnets de forma remota.

Skype: programa propiedad de Microsoft para enviar mensajes de texto y realizar videoconferencias.

Tabla de Archivos Maestros (MFT): es una tabla que contienen un directorio centralizado de todos los archivos que se encuentran en un dispositivo del almacenamiento y que permite saber dónde se encuentran almacenados los archivos.

Telnet: es un programa que permite a los usuarios conectarse un equipo en remoto.

Vulnerabilidad 0-day: ver definición de Exploit 0-day.

Windows Based Script Host (WSH): es un entorno que se encuentra en el sistema operativo Windows que se utiliza para ejecutar scripts o programas sencillos.

5. Bibliografía

[1] Fundéu BBVA (2017). P*rograma maligno, mejor que malware*. Recuperado el 6 de octubre de 2018, de
https://www.fundeu.es/recomendacion/programa-maligno-mejor-malware/

[2] Nate Lord (2018). *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*. Recuperado el 6 de octubre de 2018, de
https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#1

[3] Cristian Borghello, Marcelo Temperini, Mauro Gioino, Nicolás Gustavo, Bruna Matías Sequeira ,Maximiliano Macedo & Walter Heffel (2018). *Guía para evitar infecciones de RANSOMWARE*. Recuperado el 6 de octubre de 2018, de
https://www.owasp.org/images/b/b0/Owasp-guia-evitar-ransomware_es.pdf

[4] Andrew Brandt (2018). *SophosLabs releases SamSam ransomware report*. Recuperado el 6 de octubre de 2018, de
https://news.sophos.com/en-us/2018/07/31/sophoslabs-releases-samsam-ransomware-report/

[5] Samuel Fernandez (2018). *El ransomware en móviles también existe: qué es, cómo evitarlo y cómo librarte de él*. Recuperado el 6 de octubre de 2018, de
https://www.xatakamovil.com/seguridad/el-ransomware-en-moviles-tambien-existe-que-es-como-evitarlo-y-como-librarte-de-el

[6] Alex Drozhzhin (2016). *Historia y evolución del ransomware: datos y cifras*. Recuperado el 6 de octubre de 2018, de
https://latam.kaspersky.com/blog/ransomware-blocker-to-cryptor/7295/

[7] Wikipedia (2018). *Criptomoneda*. Recuperado el 6 de octubre de 2018, de
https://es.wikipedia.org/wiki/Criptomoneda

[8] Kaspersky Lab (2016). *KSN Report: PC ransomware in 2014-2016*. Recuperado el 6 de octubre de 2018, de
https://securelist.com/pc-ransomware-in-2014-2016/75145/

[9] Kaspersky Lab (2018) *KSN Report: Ransomware and malicious cryptominers 2016-2018*. Recuperado el 7 de octubre de 2018, de
https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf

[10] The Barkly Team (2018). *Must-Know Ransomware Statistics 2018*. Recuperado el 7 de octubre de 2018, de
https://blog.barkly.com/ransomware-statistics-2018

[11] Malwarebytes Lab (2018). *Cybercrime tactics and techniques: Q1 2018*. Recuperado el 7 de octubre de 2018, de
https://www.malwarebytes.com/pdf/white-papers/CTNT-Q1-2018.pdf

[12] Symantec (2018). 2018 *Internet Security Threat Repor*t. Recuperado el 7 de octubre de 2018, de
https://www.symantec.com/security-center/threat-report

[13] Danny Palmer (2016). *Ransomware-as-a-service allows wannabe hackers to cash-in on cyber extortion*. Recuperado el 7 de octubre de 2018, de
https://www.zdnet.com/article/ransomware-as-a-service-for-allows-wannabe-hackers-to-cash-in-on-cyber-extortion/

[14] Guy Fawkes (s.f). *Historia de la amenaza conocida como Ransomware: pasado, presente y futuro*. Recuperado el 7 de octubre de 2018, de
https://es.vpnmentor.com/blog/historia-de-la-amenaza-conocida-como-ransomware-pasado-presente-y-futuro/

[15] Michael Kan (2017). *Experts worried about ransomware hitting critical infrastructure*. Recuperado el 7 de octubre de 2018, de
https://www.csoonline.com/article/3169584/security/experts-worried-about-ransomware-hitting-critical-infrastructure.html

[16] Eset (s.f.). *Guía de Ransomware*. Recuperado el 7 de octubre de 2018, de
https://www.welivesecurity.com/wp-content/uploads/2017/10/guia-ransomware-eset.pdf

[17] Bryan Lee (2017) Palo Alto Networks Santa Clara, CA, USA. *Ransomware: Unlocking the lucrative criminal business model*. Recuperado el 6 de octubre de 2018, de
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/ransomware-report

[18] Gaspar Sánchez (2016). *Ciberataques en los hospitales: Cuando los infectados son los ordenadores*. Recuperado el 6 de octubre de 2018, de
https://desayunoconfotones.org/2016/05/19/cuando-los-infectados-en-el-hospital-son-los-ordenadores/

[19] David Perez (2017). *Historia del ransomware: desde Cryptolocker hasta WannaCry*. Recuperado el 6 de octubre de 2018, de

https://omicrono.elespanol.com/2017/11/historia-del-ransomware/

[20] KonwBe64 (s.f). *GPcode Ransomware*. Recuperado el 7 de octubre de 2018, de
https://www.knowbe4.com/gpcode

[21] David Cantón (2013). *RANSOMWARE II: Malware de cifrado*. Recuperado el 7 de octubre de 2018, de
https://www.incibe-cert.es/blog/ransomware-de-cifrado

[22] Rodney Andres (2007). *Trojan.Cryzip*. Recuperado el 8 de octubre de 2018, de
https://www.symantec.com/security-center/writeup/2006-031314-5208-99

[23] Alexander Gostev (2005). *Krotten source traced – for the moment*. Recuperado el 8 de octubre de 2018, de
https://securelist.com/krotten-source-traced-for-the-moment/30086/

[24] Pablo Ramos (2012). *Dorkbot: infección de dispositivos USB y propagación en redes sociales*. Recuperado el 8 de octubre de 2018, de
https://www.welivesecurity.com/la-es/2012/01/27/dorkbot-infeccion-dispositivos-usb-redes-sociales/

[25] Esset (2016). *Dorkbot, 5 años después de la primera detección en Latinoamérica*. Recuperado el 8 de octubre de 2018, de
https://www.welivesecurity.com/la-es/2016/04/21/dorkbot-despues-primera-deteccion/

[26] Wikipedia (2018). *Ransomware*. Recuperado el 8 de octubre de 2018, de
https://es.wikipedia.org/wiki/Ransomware#Reveton

[27] Panda Security (2015). *CryptoLocker: Qué es y cómo evitarlo.* Recuperado el 7 de octubre de 2018, de
https://www.pandasecurity.com/spain/mediacenter/malware/cryptolocker/

[28] Panda Security (2014). *¡Ataque masivo a través de CryptoLocker! ¡No pinches en un email de Correos.* Recuperado el 8 de octubre de 2018, de
https://www.pandasecurity.com/spain/mediacenter/noticias/ataque-masivo-traves-de-cryptolocker-pinches-en-un-email-de-correos/

[29] Pcrisk (2017). *Virus CryptoWall*. Recuperado el 9 de octubre de 2018, de
https://www.pcrisk.es/guias-de-desinfeccion/7401-cryptowall-virus

[30] Robert Lipovsky (2014). *Análisis de Simplocker, primer ransomware para Android activado en TOR*. Recuperado el 9 de octubre de 2018, de https://www.welivesecurity.com/la-es/2014/06/04/analisis-primer-ransomware-android-activado-tor/

[31] Ryan Francis (2016). *The history of ransomware*. Recuperado el 9 de octubre de 2018, de https://www.csoonline.com/article/3095956/data-breach/the-history-of-ransomware.html

[32] Bogdan Botezatu (2014). Reveton/IcePol Ransomware Moves to Android. Recuperado el 9 de octubre de 2018, de https://labs.bitdefender.com/2014/05/reveton-icepol-ransomware-moves-to-android/

[33] KonwBe64 (s.f). *GPcode SynoLocker*. Recuperado el 9 de octubre de 2018, de https://www.knowbe4.com/synolocker

[34] Rubén Velasco (2015). *Hidden Tear, el primer ransomware de código abierto con fines educativos*. Recuperado el 9 de octubre de 2018, de https://www.redeszone.net/2015/08/19/hidden-tear-el-primer-ransomware-de-codigo-abierto-con-fines-educativos/

[35] Rubén Velasco (2016). *Hidden Tear, el ransomware de código abierto, ya cuenta con 24 variantes maliciosas*. Recuperado el 9 de octubre de 2018, de https://www.redeszone.net/2016/02/05/hidden-tear-el-ransomware-de-codigo-abierto-ya-cuenta-con-24-variantes-maliciosas/

[36] Vinransomware (s.f.). *Vault crypt Ransomware*. Recuperado el 10 de octubre de 2018, de http://www.vinransomware.com/vault-crypt-ransomware

[37] 360 Total Security (2016). *¿Qué es el ransomware TeslaCrypt y cómo borrarlo?* Recuperado el 10 de octubre de 2018, de https://blog.360totalsecurity.com/es/borrar-ransomware-teslacrypt/

[38] Sophos (2016). The current state of ransomware: TeslaCrypt. Recuperado el 10 de octubre de 2018, de https://news.sophos.com/en-us/2016/01/06/the-current-state-of-ransomware-teslacrypt/

[39] KonwBe64 (s.f). *Chimera Ransomware*. Recuperado el 10 de octubre de 2018, de https://www.knowbe4.com/chimera-ransomware

[40] El-brujo (2015). *El creador del ransmoware Tox decide vender su negocio de creación de malware.* Recuperado el 11 de octubre de 2018, de
https://blog.elhacker.net/2015/06/el-creador-del-ransmoware-tox-decide-poner-a-la-venta-su-negocio-creacion.html

[41] David Balaban (2016). *History and Evolution of Mac Ransomware*. Recuperado el 11 de octubre de 2018, de
https://www.informationsecuritybuzz.com/articles/history-evolution-mac-ransomware/

[42] Peter Stancik (2016). *KeRanger: nuevo ransomware para Mac se propaga vía Transmission*. Recuperado el 11 de octubre de 2018, de
https://www.welivesecurity.com/la-es/2016/03/07/keranger-ransomware-mac-transmission/

[43] Serge Malenkovich (2014). *Un Nuevo Ransomware Que Utiliza la Red TOR Busca Eclipsar a CryptoLocker*. Recuperado el 11 de octubre de 2018, de
https://latam.kaspersky.com/blog/un-nuevo-ransomware-que-utiliza-la-red-tor-busca-eclipsar-a-cryptolocker/3576/

[44] Wikipedia (2016). *Locky*. Recuperado el 11 de octubre de 2018, de
https://es.wikipedia.org/wiki/Locky

[45] Pcrisk (2017). *Virus criptográfico Ransom32.* Recuperado el 11 de octubre de 2018, de
https://www.pcrisk.es/guias-de-desinfeccion/8162-ransom32-ransomware

[46].Wikipedia (2018). *Jigsaw (ransomware)*. Recuperado el 13 de octubre de 2018, de
https://en.wikipedia.org/wiki/Jigsaw_(ransomware)

[47] KonwBe64 (s.f). *Petya Ransomware*. Recuperado el 13 de octubre de 2018, de
https://www.knowbe4.com/petya-ransomware

[48] Echo Duan (2016). *FLocker Mobile Ransomware Crosses to Smart TV*. Recuperado el 13 de octubre de 2018, de
https://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/

[49] Pierluigi *Paganini (2017). It has happened again, ransomware infected an LG Smart TV*. Recuperado el 13 de octubre de 2018, de
http://securityaffairs.co/wordpress/54991/malware/lg-smart-tv-ransomware.html

[50] Panda (2017). *A New Ransomware Is Testing Our Morality*. Recuperado el 13 de octubre de 2018, de

https://www.pandasecurity.com/mediacenter/malware/popcorn-ransomware-morality/

[51] Wikipedia (2017). *WannaCry*. Recuperado el 12 de octubre de 2018, de
https://es.wikipedia.org/wiki/WannaCry

[52] Paul Ducklin (2017). *Satanás ransomware: nombre antiguo, nuevo modelo de negocio*. Recuperado el 12 de octubre de 2018, de
https://nakedsecurity.sophos.com/es/2017/03/07/satan-ransomware-old-name-new-business-model/

[53] Rubén Velasco (2016). *KimcilWare, un nuevo ransomware enfocado a secuestrar tiendas online*. Recuperado el 13 de octubre de 2018, de
https://www.redeszone.net/2016/03/30/kimcilware-nuevo-ransomware-enfocado-secuestrar-tiendas-online/

[54] Berta Bilbao (2016). *Ransomware KimcilWare golpea sitios Magento*. Recuperado el 13 de octubre de 2018, de
https://sensorstechforum.com/es/kimcilware-ransomware-hits-magento-sites/

[55] Masaki Suenaga (2016). *Ransom.Cerber*. Recuperado el 13 de octubre de 2018, de
https://www.symantec.com/security-center/writeup/2016-030408-0817-99

[56] Mundo Deportivo (2017). *Un nuevo virus informático pide como rescate fotos de desnudos*. Recuperado el 13 de octubre de 2018, de
https://www.mundodeportivo.com/elotromundo/tecnologia/20170928/431591325585/nuevo-virus-informatico-pide-rescate-fotos-desnudos-ciberataque-ransomware.html

[57] Wikipedia (2018). *Linux.Encoder.1*. Recuperado el 13 de octubre de 2018, de
https://en.wikipedia.org/wiki/Linux.Encoder.1

[58] Vilatec Information Technologies (s.f.). *Virus Correo, Hacienda y Telefónica (ransomware)*. Recuperado el 12 de octubre de 2018, de
https://www.vilatec.com/virus-correo-hacienda-y-telefonica-ransomware/

[59] Infodasa Asesores Informáticos (2016). RANSOMWARE: Métodos de infección, protección y recuperación. Recuperado el 12 de octubre de 2018, de
www.infodasa.com/web/newsDetails.php?id_section=115&id=91

[60] Daniel Cid (2015). *Malware en WordPress – Actualización de la Campaña VisitorTracke.* Recuperado el 12 de octubre de 2018, de

https://blog.sucuri.net/espanol/2015/09/malware-en-wordpress-actualizacion-de-la-campana-visitortracker.html

[61] Norfipc (s.f.). Como evitar las infecciones y trasmisiones de virus a través del USB. Recuperado el 12 de octubre de 2018, de
https://norfipc.com/articulos/infecciones-virus-usb.html

[62] Miguel Ángel Mendoza (2015). *Exploits en empresas: ¿cómo afectan el funcionamiento normal?* Recuperado el 12 de octubre de 2018, de
https://www.welivesecurity.com/la-es/2015/03/27/como-afectan-exploits-a-las-empresas/

[63] Wikipedia (2017). *EternalBlue*. Recuperado el 12 de octubre de 2018, de
https://es.wikipedia.org/wiki/EternalBlue

[64] Sean Sullivan (2017). *Ransomware Timeline: 2010 – 2017*. Recuperado el 12 de octubre de 2018, de
https://labsblog.f-secure.com/2017/04/18/ransomware-timeline-2010-2017/

[65] Hewlett Packard Enterprise (2016). *The Business of Hacking*. Recuperado el 14 de octubre de 2018, de
http://static.politico.com/b9/55/4e3ce4cc41d88401e264dcacc35c/hpe-security-research-business-of-hacking-may-2016.pdf

[66] G DATA Software AG (2017). Ransomware. Recuperado el 13 de octubre de 2018, de
https://file.gdatasoftware.com/web/es/documents/techpaper/G_DATA_TechPaper_Ransomware_ES.pdf

[67] Benedikt Luft (s.f.). *El lucrativo alcance de los ataques 'ransomware' en Bitcoin*. Recuperado el 13 de octubre de 2018, de
https://www.technologyreview.es/s/10173/el-lucrativo-alcance-de-los-ataques-ransomware-en-bitcoin

[68] Rubén Velasco (2013). *Funcionamiento interno del ransomware Cryptolocker*. Recuperado el 14 de octubre de 2018, de
https://www.redeszone.net/2013/10/30/funcionamiento-interno-del-ransomware-cryptolocker/

[69] John Leyden (2014). *KER-CHING! CryptoWall ransomware scam rakes in $1 MEEELLION*. Recuperado el 14 de octubre de 2018, de
https://www.theregister.co.uk/2014/08/29/cryptowall_analysis/

[70] Wikipedia (2018). Software como servicio. Recuperado el 14 de octubre de 2018, de
https://es.wikipedia.org/wiki/Software_como_servicio

[71] Autores de Tripwire Guest (2018). *Ransomware-as-a-Service (RaaS): Cómo funciona*. Recuperado el 14 de octubre de 2018, de https://www.tripwire.com/state-of-security/security-data-protection/ransomware-service-raas-works/

[72] Bill Brenner (2017). *5 kits de ransomware como servicio (RaaS) - SophosLabs investiga*. Recuperado el 14 de octubre de 2018, de https://nakedsecurity.sophos.com/2017/12/13/5-ransomware-as-a-service-raas-kits-sophoslabs-investigates/

[73] DIGIWORKS (s.f). *Modelos de negocio que pueden ayudar a tu empresa.* Recuperado el 15 de octubre de 2018, de https://www.digiworks.es/modelos-de-negocio-que-pueden-ayudar-a-tu-empresa/

[74] Wikipedia (2018). *Hágalo usted mismo*. Recuperado el 15 de octubre de 2018, de https://es.wikipedia.org/wiki/H%C3%A1galo_usted_mismo

[75] Bruno (2018). *DIY Ransomware Kits Accessible on the Dark Web.* Recuperado el 15 de octubre de 2018, de https://darkwebnews.com/dark-web/ransomware-diy-kits/

[76] Tom Spring (2017). Low-Cost Ransomware Service Discovered. Recuperado el 15 de octubre de 2018, de https://threatpost.com/low-cost-ransomware-service-discovered/125017/

[77] Catalin Cimpanu (2017). *New Karmen Ransomware-as-a-Service Advertised on Hacking Forums*. Recuperado el 20 de octubre de 2018, de https://www.bleepingcomputer.com/news/security/new-karmen-ransomware-as-a-service-advertised-on-hacking-forums/

[78] David & José Ángel (2008). *1-Seguridad activa y pasiva*. Recuperado el 20 de octubre de 2018, de http://david-jose.blogspot.com/2008/12/bitdefender-antivirus-2009-kaspersky.html

[79] Oficina de Seguridad del Internauta (s.f.). *Haz copias de seguridad y cifra tus datos*. Recuperado el 20 de octubre de 2018, de https://www.osi.es/es/copias-de-seguridad-cifrado

[81] INCIBE (s.f). *Desarrollar cultura en seguridad*. Recuperado el 20 de octubre de 2018, de https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad

[82] Miguel A. Perez (2014). *Qué es el Principio de Mínimo Privilegio y cómo puede salvar tu ordenador.* Recuperado el 20 de octubre de 2018, de
https://blogthinkbig.com/principio-de-minimo-privilegio

[83] Sophos (2018). *SamSam: The (almost) $6 million ransomware*. Recuperado el 20 de octubre de 2018, de
https://nakedsecurity.sophos.com/2018/07/31/samsam-the-almost-6-million-ransomware/

[84] León Blaustein (2014). *¿Cómo ayuda la segmentación de la red a proteger la red empresarial?* Recuperado el 20 de octubre de 2018, de
https://searchdatacenter.techtarget.com/es/consejo/Como-ayuda-la-segmentacion-de-la-red-a-proteger-la-red-empresarial

[85] Alianza Winex Paraguay (2017). *Segmentación y Direccionamiento IP*. Recuperado el 20 de octubre de 2018, de
http://www.winex.com.py/2017/03/05/segmentacion-y-direccionamiento-ip/

[86] Sophos (s.f.). *Detenga el ransomware con Sophos Intercept X*. Recuperado el 20 de octubre de 2018, de
https://www.sophos.com/es-es/lp/ransomware.aspx

[87] ESSET (s.f). *Advanced Memory Scanner*. Recuperado el 20 de octubre de 2018, de
https://help.eset.com/eis/11/en-US/technology_ams.html

[88] Vínsula (s.f.). *Unlock ZeroLocker*. Recuperado el 20 de octubre de 2018, de
http://vinsula.com/security-tools/unlock-zerolocker/

[89] Anónimo (s.f). *Implantación de técnicas de acceso remoto*. Recuperado el 21 de octubre de 2018, de
https://zubiri-sad-03.webcindario.com/

[90] Alejandro (2017). Funcionamiento de IDS, IPS y UTM ¿Qué es cada cosa? Recuperado el 21 de octubre de 2018, de
https://protegermipc.net/2017/03/16/funcionamiento-de-ids-ips-y-utm-que-es-cada-cosa/comment-page-1/

[91] Check Point (2017). *Software blade architecture*. Recuperado el 21 de octubre de 2018, de
https://www.checkpoint.com/downloads/product-related/brochure/Software-Blades-Architecture.pdf

[92] David Acosta (2014). *Controles Técnicos de PCI DSS parte V: Sistemas de detección/prevención de intrusiones (IDS/IPS).* Recuperado el 21 de octubre de 2018, de

https://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-v-sistemas-de-deteccionprevencion-de-intrusiones-idsips/

[93] ZAZ informática (s.f). *Servidor Proxy*. Recuperado el 21 de octubre de 2018, de
http://www.zazinformatica.com.br/category/sem-categoria/#

[94] IREO (s.f). *DLP (Data Loss Prevention)*. Recuperado el 21 de octubre de 2018, de
https://www.ireo.com/soluciones/seguridad/dlp-data-loss-prevention?doing_wp_cron=1540113677.7831959724426269531250

[95] Centro Criptológico Nacional (2018). *CCN-CERT IA 11/18 Medidas de seguridad contra ransomware.* Recuperado el 29 de octubre de 2018, de
https://www.ccn-cert.cni.es/pdf/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

[96] Segu-Info (2016). *Surprise, nuevo ransomware propagado por TeamViewer*. Recuperado el 29 de octubre de 2018, de
https://blog.segu-info.com.ar/2016/03/surprise-nuevo-ransomware-propagado-por.html

[97] Wikipedia (2018). *ActiveX*. Recuperado el 30 de octubre de 2018, de
https://es.wikipedia.org/wiki/ActiveX

[98] Segu-Info (2016). *Cómo evitar infectarse con archivos JS adjuntos y ransomware.* Recuperado el 30 de octubre de 2018, de
https://blog.segu-info.com.ar/2016/03/como-evitar-infectarse-con-archivos-js.html

[99] Oficina de Seguridad del Internauta (2015). *¿Sabes lo que es el malvertising y cómo estar protegido frente a él?.* Recuperado el 30 de octubre de 2018, de
https://www.osi.es/es/actualidad/blog/2015/05/08/sabes-lo-que-es-el-malvertising-y-como-estar-protegido-frente-el

[100] Armis (s.f.). *The Attack Vector "BlueBorne" Exposes Almost Every Connected Device*. Recuperado el 31 de octubre de 2018, de
https://armis.com/blueborne/

[101] Wikipedia (2018). *Autorun.* Recuperado el 31 de octubre de 2018, de
https://es.wikipedia.org/wiki/Autorun

[102] Cert-py (s.f). *Distribución de ransomware mediante ataques de fuerza bruta a RDP*. Recuperado el 1 de noviembre de 2018, de
https://www.cert.gov.py/index.php/noticias/distribucion-de-ransomware-mediante-ataques-de-fuerza-bruta-rdp

[103] Swiat (2016). *Enhanced Mitigation Experience Toolkit (EMET) version 5.5 is now available.* Recuperado el 1 de noviembre de 2018, de https://blogs.technet.microsoft.com/srd/2016/02/02/enhanced-mitigation-experience-toolkit-emet-version-5-5-is-now-available/

[104] Anónimo (s.f.). *Microsoft EMET 5.5 review - The goodness abides.* Recuperado el 1 de noviembre de 2018, de https://www.dedoimedo.com/computers/windows-emet-v5-5.html

[105] Alex Monrás (2017). *Cómo habilitar el 'Acceso controlado a carpetas' en Windows 10 Fall Creators Update*. Recuperado el 1 de noviembre de 2018, de https://www.dominiogeek.com/como-habilitar-el-acceso-controlado-a-carpetas-en-windows-10-fall-creators-update/

[106] Wikipedia (2018). *Registro de arranque principal*. Recuperado el 1 de noviembre de 2018, de https://es.wikipedia.org/wiki/Registro_de_arranque_principal

[107] Rubén Velasco (2016). *MBRFilter, la herramienta de Cisco para protegernos del malware del MBR*. Recuperado el 1 de noviembre de 2018, de https://www.redeszone.net/2016/10/20/mbrfilter-la-herramienta-cisco-protegernos-del-malware-del-mbr/

[108] Symantec (2018). *Tipos de archivos y extensiones que son vectores de amenazas comunes en archivos adjuntos de correo electrónico.* Recuperado el 3 de noviembre de 2018, de https://support.symantec.com/es_ES/article.INFO3768.html

[109] Christopher M. Frenz & Christian L. Diaz (s.f.). *Guia contra ataques Ransomware*. Recuperado el 4 de noviembre de 2018, de https://www.owasp.org/images/3/39/Guia_Contra_Ransomware.pdf

[110] Wikipedia (2018). *Host-based intrusion detection system.* Recuperado el 4 de noviembre de 2018, de https://es.wikipedia.org/wiki/Host-based_intrusion_detection_system

[111] Patrick Kral (2011). *Incident Handler's Handbook*. Recuperado el 5 de noviembre de 2018, de http://gauss.ececs.uc.edu/Courses/c6055/pdf/incident-handlers-handbook-33901.pdf

[112] Joaquín Louzao, Gerardo Geis & Gabriel Silva. *Gestión de Incidentes - Análisis Forense*. Recuperado el 5 de noviembre de 2018, de ftp://public.dhe.ibm.com/la/documents/imc/la/uy/news/events/networking12/files/15_IBM_-_Gestion_de_Incidentes_-

_Analisis_Forense_-_Joaquin_Louzao_Gerardo_Geis_Gabriel_Silva.pdf

[113] INCIBE (s.f.) *¿Estáis preparados? Cuestionario inicial de respuesta a incidentes*. Recuperado el 5 de noviembre de 2018, de https://www.incibe.es/sites/default/files/contenidos/JuegoRol/juegorol_cuestionarioinicialrespuestaincidentes.pdf

[114] Moisés Barrio (2017). *La respuesta del Derecho ante los ciberataques*. Recuperado el 10 de noviembre de 2018 de https://blogs.elconfidencial.com/tecnologia/tribuna/2017-05-14/ciberataque-respuesta-del-derecho_1382252/

[115] Wikipedia (2018). *Gusano Morris*. Recuperado el 10 de noviembre de 2018 de https://es.wikipedia.org/wiki/Gusano_Morris

[116] Wikipedia (2018). *Delito informático*. Recuperado el 10 de noviembre de 2018 de https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

[117] Miriam Guardiola (2017). *Ciberataques : ¿cómo se regulan los nuevos peligros del siglo XXI?* Recuperado el 10 de noviembre de 2018 de http://www.legaltoday.com/practica-juridica/penal/penal/ciberataques-como-se-regulan-los-nuevos-peligros-del-siglo-xxi

[118] David Maeztu (2017). *Tipificación penal del ransomware*. Recuperado el 10 de noviembre de 2018 de https://www.derechoynormas.com/2017/05/tipificacion-penal-del-ramsomware.html

[119] INCIBE (s.f.). *Servicio AntiRansomware.* Recuperado el 10 de noviembre de 2018 de https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

[120] Grupo de Delitos Telemáticos Unidad Central Operativa Guardia Civil (s.f.). *Denunciar el delito*. Recuperado el 10 de noviembre de 2018 de https://www.gdt.guardiacivil.es/webgdt/pinformar.php

[121] David Valero (2016). *La justicia española condena a 6 años de cárcel al creador del "virus de la policía"*. Recuperado el 10 de noviembre de 2018 de https://www.adslzone.net/2016/02/29/la-audiencia-nacional-condena-a-6-anos-al-creador-del-virus-de-la-policia/

[122] Wikipedia (2018). *Ataques ransomware WannaCry.* Recuperado el 18 de noviembre de 2018 de

https://es.wikipedia.org/wiki/Ataques_ransomware_WannaCry

[123] Microsoft (2017). *MS17-010*. Recuperado el 18 de noviembre de 2018 de
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

[124] Common Vulnerabilities Exposures (2017). *CVE-2017-0144*. Recuperado el 18 de noviembre de 2018 de
https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144

[125] Andres Galeano (2017), *Usando el exploit eternalblue de la NSA*. Recuperado el 18 de noviembre de 2018 de
https://backtrackacademy.com/articulo/ms17-010-eternalblue-doublepulsar

[126] Seguridad Ofensiva Telinsec S.L. (2018). *Windows embedded vulnerable al exploit DoublePulsar*. Recuperado el 18 de noviembre de 2018 de
https://www.telinsec.com/windows_embedded_vulnerable_a_doublepulsar.html

[127] Wikipedia (2018). *DoublePulsar.* Recuperado el 18 de noviembre de 2018 de
https://en.wikipedia.org/wiki/DoublePulsar

[128] Andrés Checa (2017). *¡Hackea Windows con Kali, Metasploit y FuzzBunch!* Recuperado el 18 de noviembre de 2018 de
https://medium.com/@acheca/hackea-windows-con-kali-metasploit-y-fuzzbunch-f3d6a4153050

[129] Dan Doodin (2017). *10,000 Windows computers may be infected by advanced NSA backdoor.* Recuperado el 18 de noviembre de 2018 de
https://arstechnica.com/information-technology/2017/04/10000-windows-computers-may-be-infected-by-advanced-nsa-backdoor/

[130] Rubén Frieiro Barros, Pablo Pérez San-José & Xabier Pascual Villanueva (2017). *¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?* Recuperado el 18 de noviembre de 2018 de
http://perspectivas.deloitte.com/hubfs/Campanas/WannaCry/Deloitte-ES-informe-WannaCry.pdf

[131] Yúbal FM (2017). *Crece la preocupación por la llegada de un WannaCry sin 'kill-switch': así puedes protegerte*. Recuperado el 19 de noviembre de 2018 de
https://www.xataka.com/seguridad/wannacry-vuelve-sin-el-kill-switch-que-permite-desactivarlo-asi-puedes-protegerte

[132] BBC News (2017). *Cyber-attack: Europol says it was unprecedented in scale.* Recuperado el 19 de noviembre de 2018 de
https://www.bbc.com/news/world-europe-39907965

[133] Manuel Ángel Méndez (2017). *Así fue el primer ciberataque masivo que ha paralizado el mundo*. Recuperado el 19 de noviembre de 2018 de
https://www.elconfidencial.com/tecnologia/2017-05-13/ransomware-wannacry-ciberataque-hackeo-ciberseguridad-telefonica_1381986/

[134] FayerWayer (2017) *Telefónica España, Chile y Argentina sufren hackeo, piden rescate en Bitcoins.* Recuperado el 20 de noviembre de 2018 de
https://www.fayerwayer.com/2017/05/telefonica-espana-sufrio-importante-ataque-de-ransomware/

[135] Wikipedia(2018). *WannaCry*. Recuperado el 21 de noviembre de 2018 de
https://es.wikipedia.org/wiki/WannaCry

[136] Mundo Deportivo (2017) *Este es Marcus Hutchins, el hacker que frenó el ciberataque con tan solo 10 euros*. Recuperado el 21 de noviembre de 2018 de
https://www.mundodeportivo.com/elotromundo/actualidad/20170516/422620537910/marcus-hutchins-hacker-frenar-ciberataque-virus.html

[137] Eugene Kolo (2017). *PayBreak able to defeat WannaCry/WannaCryptor ransomware.* Recuperado el 23 de noviembre de 2018 de
https://www.benthamsgaze.org/2017/05/16/paybreak-able-to-defeat-wannacrywannacryptor-ransomware/

[138] Antonia Laborde (2018). *EE UU acusa al hacker norcoreano detrás del ciberataque 'WannaCry' y el de Sony*. Recuperado el 24 de noviembre de 2018 de
https://elpais.com/internacional/2018/09/06/actualidad/1536257762_840433.html

[139] Wikipedia (2017). *Ciberataque a Sony Pictures de 2014.* Recuperado el 24 de noviembre de 2018 de
https://es.wikipedia.org/wiki/Ciberataque_a_Sony_Pictures_de_2014

[140] AFP – Diario ABC (2018). *EE.UU. acusa a un hacker norcoreano de ser el autor de los ciberataques más importantes en los últimos años.* Recuperado el 24 de noviembre de 2018 de

https://www.abc.es/tecnologia/redes/abci-eeuu-acusa-corea-norte-ciberataques-mas-importantes-ultimos-anos-201809071848_noticia.html

[141] Diario El Periódico (2017). *El mayor ciberatraco del mundo tuvo topos en el banco*. Recuperado el 24 de noviembre de 2018 de
https://www.elperiodico.com/es/sociedad/20161230/el-mayor-ciberatraco-del-mundo-tuvo-topos-en-el-banco-5696007

[142] David Pérez (2017). *Quienes son Lazarus, los hackers de Corea del Norte denunciados por EEUU*. Recuperado el 24 de noviembre de 2018 de
https://omicrono.elespanol.com/2017/12/lazarus-group-hackers-de-corea-del-norte/

[143] Shanan Carney (2017). *Ransomware: 3 motivos por los que NUNCA deberías pagar el rescate*. Recuperado el 25 de noviembre de 2018 de
https://blog.avast.com/es/ransomware-3-motivos-por-los-que-nunca-deberias-pagar-el-rescate

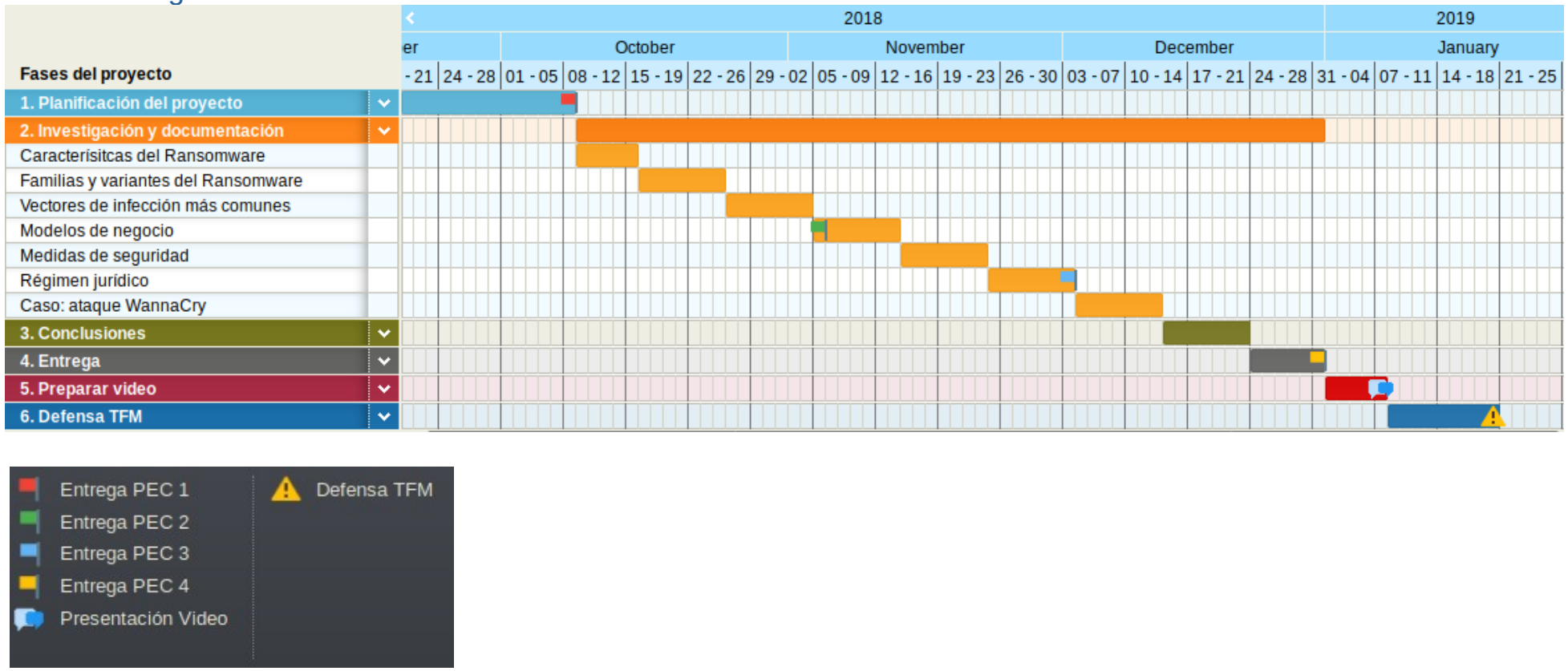
[144] Asociación Nacional Afectados Internet y Nuevas Tecnologías (2016). *Sentencia virus de la policía*. Recuperado el 25 de noviembre de 2018 de
https://issuu.com/asociacionnacionalafectadosinternet/docs/sentencia_virus?workerAddress=ec2-54-196-189-55.compute-1.amazonaws.com

[145] Audiencia Nacional Sala de lo Penal (2016). *Sentencia 28/16*. Recuperado el 25 de noviembre de 2018 de
http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7736507&links=&optimize=20160714&publicinterface=true

[146] Wikipedia (2018). *MSN Messenger*. Recuperado el 30 de noviembre de 2018 de
https://es.wikipedia.org/wiki/MSN_Messenger

[147] Wikipedia (2018). *Dropbox*. Recuperado el 30 de noviembre de 2018 de
https://es.wikipedia.org/wiki/Dropbox

[148] Wikipedia (2018). *Peer-to-peer*. Recuperado el 30 de noviembre de 2018 de
https://es.wikipedia.org/wiki/Peer-to-peer

6. Anexos

Anexo I. Diagrama de Gantt