Cibercrimen: Ransomwares

Nombre Estudiante: Armando Antonio Nieto Hernández
Plan de Estudios del Estudiante: Máster Interuniversitario de Seguridad de las Tecnologías de la Información y las Comunicaciones (MISTIC)
Área del trabajo final: Hacking

Nombre Consultora: Angela María García Valdés
Nombre Profesor responsable de la asignatura: Victor Garcia Font

1/06/2020


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

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Cibercrimen: Ransomwares*
Nombre del autor:	*Armando Antonio Nieto Hernández*
Nombre del consultora:	*Angela María García Valdés*
Nombre del PRA:	*Victor Garcia Font*
Fecha de entrega (mm/aaaa):	06/2020
Titulación:	*Máster Interuniversitario de Seguridad de las Tecnologías de la Información y las Comunicaciones*
Área del Trabajo Final:	*Hacking*
Idioma del trabajo:	***Español***
Palabras clave	*malware, ransomware, secuestro de información.*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

Durante los primeros meses del 2020, ha quedado de manifiesto la evolución e importancia de los recursos que plantea la Sociedad Digital para la implementación del concepto de "Continuidad del Negocio" a distancia en organizaciones y también para el establecimiento de nuevas formas de comunicación entre personas. Sin embargo, paralelo a este desarrollo tecnológico, se ha dado el surgimiento y evolución de una modalidad de ciberataque conocido como Ransomware, letal para las víctimas y lucrativa para ciberdelincuentes.

El siguiente Trabajo de Fin de Máster presenta, en primer lugar, una clasificación con algunos ejemplos de ataques Ransomware conocidos desde sus inicios y de cómo éstos han transcendido de plataforma, tipos de dispositivos, estrategias de infección, funciones, formas de obtener dinero y maneras de coaccionar a la víctima para que realice el pago por el rescate.

En segundo lugar, se propone una estrategia de prevención de ataques tipo Ransomware separada en capas para reducir su posibilidad de éxito. Un ataque efectivo supone pérdidas que pueden alcanzar miles de Euros o Dólares, sin mencionar el impacto negativo en la imagen de la víctima.

En tercer lugar, se exponen algunas estrategias legales y su impacto, en el caso particular de El Salvador, Latinoamérica y Europa; realizando una breve exposición de cómo ha madurado el marco jurídico en cada contexto.

En cuarto lugar, se presentan 3 soluciones informáticas de empresas de antivirus en respuesta a esta problemática. Por último, se realiza la exposición de Ransoware Ryuk, su vector de infección, funcionamiento y evolución.

Abstract (in English, 250 words or less):

During the first months of 2020, the evolution and importance of the resources proposed by the Digital Society has been showed for the implementation of the concept of "Business Continuity", for teleworking in organizations and also for the establishment of new forms of communication between people. However, simultaneously to this technological development, there has been given the emergence and evolution of a cyber attack known as Ransomware, lethal for victims and profitable for cybercriminals.

The following Project shows, first of all, a classification with some examples of Ransomware attacks known since their inception and how they have finded different ways to expand to platforms, types of devices, infection strategies, functions, ways to obtain money and force the victim to make the ransom payment.

Secondly, a layered Ransomware-type attack prevention strategy is proposed to reduce their chance of success. An effective attack can reach losses in thousands of Euros or Dollars, regardless of the negative impact on the image of the victim.

Thirdly, some legal strategies and their impact are exposed, in the particular case of El Salvador, Latin America and Europe; giving a brief presentation of how the legal framework has matured in each context.

Fourthly, 3 computer solutions from antivirus companies are presented in response to this problem. Finally, the exposition of Ransoware Ryuk, its vector of infection, functioning and evolution, is carried out.

Índice

Lista de Figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Los ataques mediante ransomware no son una novedad, el primer indicio de este tipo sucedió en el año de 1989 durante una convención de la Organización Mundial de la Salud sobre el tema del SIDA, su vector de infección, en aquel entonces, era por medio de diskettes y su funcionamiento, en líneas generales, era el secuestro de los archivos (cifrándolos) en los terminales infectados a cambio de solicitar un rescate que consistía en el envío de cierta cantidad de dinero a una determinada cuenta bancaria para la entrega de la clave que revertiera el cifrado, posteriormente surgieron herramientas que lograban romper el algoritmo implementado y de esta forma evitar así el pago exigido por el ciberdelincuente.

Con el surgimiento de nuevas tecnologías gracias a las cuales diferentes tipos de dispositivos se conectan entre sí, más el auge de Internet, esta forma de ataque también ha logrado evolucionar a tal punto que para su distribución ya no se requiere de un medio físico que se deba intercambiar entre usuarios, sino mas bien se realiza por medio de la red, lo cual acelera su propagación, se emplean algoritmos de cifrado más robustos difíciles de romper, su objetivo ha dejado de ser una plataforma en específico.

Por un lado, características como las mencionadas han convertido a esta amenaza en una de las principales durante los últimos años, ocasionando graves pérdidas de información no solo personal, sino también empresarial, siendo más grave en este último ámbito debido a diferentes legislaciones que se han establecido y que penalizan fuertemente la vulneración de la protección sobre datos personales. Por otro lado, se ha sabido de casos en el que algunas compañías han tenido que cerrar debido a que no lograron recuperarse de las consecuencias sufridas por este tipo de ataques.

Por todo lo anterior, se presentan como resultado de esta investigación algunos de los diferentes tipos de ransomware que se han conocido hasta el momento, su vector de infección, así como la mitigación de los daños y más importante su prevención como la mejor alternativa para evitar los estragos económicos y de imagen que pudiera causar este tipo de ataque.

1.2 Objetivos del Trabajo

El objetivo general del TFM consiste en exponer la evolución y diferentes medios de propagación del malware ransomware que permita definir estrategias para prevenir y mitigar las consecuencias de este tipo de ciberataque.

Además del objetivo general, los objetivos específicos más relevantes que se plantean conseguir al término de esta investigación son los siguientes:

- Ejemplificar diversas técnicas de propagación de ransomware para secuestro de información.
- Enumerar recomendaciones que contribuyan a la prevención de un ataque exitoso.
- Mostrar el modelo de negocio de este tipo de malware.
- Identificar las consecuencias legales de este tipo de ataque.
- Presentar un caso notable de una campaña de ransomware.

1.3 Enfoque y método seguido

Para cubrir los objetivos del presente TFM, se realiza una combinación de las metodologías de investigación descriptiva y explicativa según se expone a continuación:
En primer lugar, una metodología descriptiva posibilita realizar un estudio detallado del fenómeno del ransomware como lo es su evolución, sus diferentes vectores de ataque y comportamiento, gracias a esto es posible ir definiendo algunas medidas de protección frente a este tipo de ataque.
En segundo lugar, se utiliza una metodología explicativa que permite realizar una descripción más profunda en especial sobre las consecuencias económicas y legales.
Lo anterior se realizará mediante la recolección de información de diferentes fuentes como lo son artículos de investigación académica, libros, noticias, blogs, entre otros, relacionados con la temática.

1.4 Planificación del Trabajo

La elaboración del TFM requiere las siguientes tareas:

1. Planificación: en esta etapa se establecerá el contexto de la investigación justificando su desarrollo, los objetivos y la metodología para alcanzarlos, además se presentará la temporalización de la misma, identificando los productos que se entregarán a su finalización.
2. Desarrollo de la investigación: consiste en realizar toda la investigación documental de diferentes fuentes para dar respuesta a cada una de las siguientes interrogantes:
   a) ¿Qué tipos de malware de ransomware existen?
   b) ¿Cómo operan?
   c) ¿Qué vector de infección utilizan?
   d) ¿Cómo controla el operador el material cifrado y los depósitos de dinero?
   e) ¿Cómo obtiene el dinero el operador (blanqueo de dinero?
   f) ¿Cómo es posible mitigar el impacto?
   g) ¿Qué se está haciendo a nivel legal? ¿y las compañías antivirus?

h) Seleccionar y explicar algún caso notable de una campaña de ransomware.

3. Elaboración de las conclusiones: se presentan las conclusiones obtenidas.
4. Elaboración de otros productos para la entrega: preparación de un vídeo y presentación que contribuyan a la revisión/evaluación de la memoria final.
5. Entrega: se realiza la entrega de todos los productos obtenidos durante el desarrollo de la investigación mediante la herramienta del aula virtual.
6. Defensa: consiste en brindar respuesta a las posibles interrogantes planteadas por el tribunal responsable de la evaluación del TFM.

La planificación temporal se representa mediante un diagrama de Gantt, el cual puede consultarse en el Anexo I.

1.5 Breve sumario de productos obtenidos

Durante la elaboración del presente TFM se obtienen los siguientes entregables:

- PEC 1: consiste en la entrega del plan de trabajo que incluye el contexto y la justificación de la investigación, la metodología a implementar, la previsión temporal y una breve revisión del estado del arte. La fecha prevista para su entrega es el 03/03/2020.
- PEC 2: consite en una entrega parcial de la investigación que abarca la definición y características del ransomware, los tipos y la forma de operar de cada uno. La fecha prevista para su entrega es el 31/03/2020.
- PEC 3: es una entrega parcial que involucra los vectores de infección, el modelo de negocios, estrategias de prevención y medidas de recuperación de desastres, impactos legales y acciones de empresas de antivirus. La fecha prevista para su entrega es el 28/04/2020.
- PEC 4: consiste en preparar el caso de estudio para luego realizar una compilación de todo el trabajo desarrollado en la memoria final, complementándola con la presentación y un vídeo para la respectiva evaluación por parte del tribunal. La fecha prevista para su entrega es el 02/06/2020.

1.6 Breve descripción de los otros capítulos de la memoria

- Capítulo 2: Presenta una breve descripción del estado del arte, se han identificado 3 investigaciones realizadas en la UOC cuya temática se encuentra realacionada con el contenido del presente TFM, a nivel general son bastante similares en cuanto a contenido, la idea es tener un punto de partida evitando de esta forma repetir el trabajo que ya ha sido previamiente realizado. Se incluyen otras fuentes de consulta.

- Capítulo 3: En primer lugar, se desarrolla la temática de la investigación, se inicia con la presentación y descripción de la forma de operar del ransomware. En segundo lugar, se realiza una clasificación de esta variante de malware en base a su alcance, forma de operar, plataforma objetivo, modelo de negocio, estrategias de prevención/mitigación, acciones e impactos legales, así como una breve mención del actuar de las casas comerciales de algunos antivirus reconocidos.
- Capítulo 4: Presenta un caso de notable de una campaña de ransomware, en este caso se ha seleccionado el malware Ryuk, se presentan sus atencedentes, describe como funciona y la evolución que éste ha tenido, también el cómo los ciberdelincuentes han mejorado sus técnicas de ataque que les permite crear herramientas más sofisticadas cada día.

2. Estado del arte

El análisis del estado del arte se basa en investigaciones previas sobre el tema seleccionado. Dentro de la UOC se tienen las siguientes:

1. Arnaltes Navarro, M. (2018). *Ransomware*. Máster Interuniversitario de Seguridad de las Tecnologías de la Información y las Comunicaciones. Universitat Oberta de Catalunya.
   Tomado de: http://hdl.handle.net/10609/72608.
   Lo interesante de esta investigación es que selecciona 6 muestras de ransomware muy conocidas por los estragos que causaron en su momento, realiza un análisis de sus características generales, procesos de infección y algoritmo de cifrado, así como también la posibilidad de efectuar un proceso de desinfección exitosa.
   Adicionalmente, también presentan algunas recomendaciones de prevención y reacción frente a este tipo de ataques, más un estudio de la legislación española junto con la europea en lo relativo al ransomware a la fecha de su elaboración.
2. Estrada Cola, C. (2018). *Estudio sobre el malware Ransomware. Máster Interuniversitario de Seguridad de las Tecnologías de la Información y las Comunicaciones*. Universitat Oberta de Catalunya.
   Tomado de: http://hdl.handle.net/10609/89025.
   Este trabajo presenta los orígenes de la definición del término ransomware, sus variantes, sus diferentes vectores de infección y modelo de negocio hasta el 2018. Su caso de estudio es el ya muy conocido Wanacry del 2017.
   Su objetivo principal es hacer conciencia del tipo de amenaza que representa este malware, brindando técnicas para detectar y mitigar su infección.
3. Quilez Garrido, A. (2018). *Latest Ransomware trends targeting IoT*. Máster Universitario de Seguridad de las Tecnologías de la Información y las Comunicaciones. Universitat Oberta de Catalunya.
   Tomado de: http://hdl.handle.net/10609/81833.
   Se realiza un estudio de 6 muestras de ransomware, se orienta a los ataques que pueden sufrir los dispositivos IoT debido al gran auge que estos han tenido en los últimos años. Además, presenta una simulación en un entorno controlado sobre un ataque de Cryptolocker. Sobre sus conclusiones se pueden encontrar algunas recomendaciones para la prevención de este tipo de ataque

Las dos primeras investigaciones tienen muchos elementos en común ya que ambas presentan una definición y diferentes tipos de ransomware, proporcionan recomendaciones para prevención y realizan un análisis sobre las posibilidades de recuperación ante este tipo de desastre; referente a la tercera investigación, aunque mantiene ciertas

coincidentas respecto a las primeras, esta última no contempla una sección sobre el estado actual de la legislación al momento de su elaboración o de su modelo de negocio

Las 3 investigaciones consultadas fueron realizadas en el 2018, sin embargo, en el 2020 se ha contemplado una variante en la forma de operar de algunos ataques, ya que no solamente amenazan con el cifrado de los datos, sino también con la divulgación de la información muchas veces de carácter personal, privada y sensible a nivel empresarial, diversas legislaciones también han evolucionado en lo referente a esta amenaza cibernética.

Fuera de la UOC se puede encontrar una buena cantidad de información referente al concepto de ransomware, así como diferentes clasificaciones, recomendaciones de prevención y acciones a tomar en caso de desastres, se presentan algunos ejemplos:

1. INCIBE. (2017). Ransomware: una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad.
   Tomado de:
   https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario.
   Es una guía para empresas que inicia con la presentación del concepto de ransomware, vectores de infección y los tipos mas conocidos, además, presenta pautas de cómo protegerse, planes de acción en caso de infección y recomendación para una prevención a futuro luego de un incidente.
2. O'Gorman, G. and McDonald, G., 2012. Ransomware: A Growing Menace. [ebook] Disponible en:
   <https://vxug.fakedoma.in/papers/ransomware-growing-menace-12-en.pdf> [Consultado el 28 Marzo de 2020].
   Es una descripción del concepto de ransomware y de cómo éste utiliza la imagen de Organizaciones de seguridad, reconocidas incluso a nivel internacional, para coaccionar a la víctima e inducirla a que efectúe el pago exigido para el desbloqueo de la información, también se presenta el avance que dicha amenaza tuvo en el 2011 a lo largo del continente Europeo, Canadá y Estados Unidos.
3. Kolodenker, E., Koch, W., Stringhini, G. and Egele, M., 2017. Paybreak: Defense Against Cryptographic Ransomware. [ebook] Disponible en:
   <https://dl.acm.org/doi/abs/10.1145/3052973.3053035>
   [Consultado el 28 Marzo de 2020].
   Con esta investigación se concluye que algunas de las primeras amenzas de ransomware que se conocieron tenían el fallo en aplicar de forma incorrecta algoritmos criptográficos, como es de esperarse los ciberdelincuentes han ido mejorando el desarrollo de nuevas amenazas haciéndolas más sofisticadas, a raíz de ello, también se hace mención a que muchas de las herramientas utilizadas para contrarrestrar la amezana son de tipo reactivo, es decir, hasta que el usuario ha sido infectado. Como respuesta a esta situación, se propone un mecanismo conocido como PayBreak, es una medida preventiva contra el

ransomware para mantener seguros los archivos de las posibles víctimas. PayBreak esta basado en una encriptación segura de archivos híbrida donde se usan claves de sesión simétricas en la computadora del usuario. PayBreak observa el uso de estas claves, las mantiene almacenadas y, por lo tanto, puede descifrar archivos que de otro modo solo serían recuperables pagando el rescate. Como resultado, se evaluó PayBreak en 107 muestras de ransomware y se demostrós una recuperación con éxito del daño causado por doce familias diferentes de ransomware.

Como se ha mencionado, el término ransomware no es nuevo, sin embargo, gracias al avance de la tecnología misma, han surgido nuevas herramientas criptográficas con el propósito de contribuir a la seguridad de la información, mismas que lamentablemente han sido utilizadas para obtener un beneficio económico de forma ilegal secuentrando datos y/o equipos para exigir un rescate que no ofrece ninguna garantía de recuperación del acceso o el control.

Paralelo a lo anterior, se ha visto una evolución en el que ya no se trata solo de una amenaza contra una plataforma en específico, se han realizado ataques a plafaformas Linux, Mac, plafaformas móbiles e incluso la misma nube no escapa de ello.

Existen muchos estudios que han retomado este fenómeno, sin mencionar, las noticias que salen con frecuencia sobre nuevas amenazas de esta clase de malware.

Se retoma una clasificación breve de las amenzas que se han conocido, así como la inclusión de las últimas relacionadas a este tema para constatar su evolución.

3. Ransomwares

3.1 Definición.

Empezamos definiendo un «malware» como un software desarrollado con fines maliciosos que busca alterar el comportamiento habitual de un equipo sin el consentimiento/conocimiento del usuario de manera intencional. La palabra «ransomware» es la unión de dos palabras que provienen del inglés, una es «ransom» que significa «rescate» y la otra «ware» que hace referencia a un «programa informático», de ahí que también se le conozca con el nombre de «el malware del rescate» y consiste en restringir el acesso al sistema y parte de los archivos en un terminal mediante la aplicación de algoritmos criptográficos a cambio de exigir el pago de una cantidad de dinero para poder recuperar dicho control.

3.2 Caraterísticas.

El ransomware es un tipo de malware, por lo que hereda algunas de sus características siendo la principal la denonimada «persistencia» es decir, que no importa las veces que se reinicie un sistema infectado, el software malicioso siempre mantendrá su actividad mantiendo el bloqueo total o parcial del mismo.
El canal de infección, al igual que otros tipos de malware puede ser vía correo electrónico, sitios web comprometidos, aplicaciones maliciosas camuflajadas en archivos adjuntos, entre otros. Una vez comprometido el primer dispositivo, este busca expandirse al resto dentro de una misma red, similar a como lo haría un gusano informático (Worm).
La diferencia principal con otro tipo de amenazas es el secuestro del sistema junto con los datos de usuario (utilizando algoritmos critográficos) a cambio de exisigir un rescate para el desbloquedo de los mismos o para evitar su divulgación en Internet.

3.3 Tipos y forma de operar de cada uno.

Desde sus orígenes han surgido diferentes tipos de ransomware los cuales han ido evolucionando en su forma de operar con el paso del tiempo, se mencionan los tipos más representativos:

3.3.1 ScreenLocker.

Este tipo de ransomware es de los menos sofisticados, puesto que es probable que utilice cifrado de archivos o no; su característica más relevante es que bloquea el acceso al sistema, impidiendo que se haga uso normal del mismo gracias a una pantalla de bloqueo hasta que se pague el rescate para supuestamente obtener nuevamente dicho acceso.
Entre algunos ejemplos de este tipo se tienen:

1. BlueScreen
2. Koktrom
3. Kovter
4. LockScreen
5. Reveton
6. Tobfy
7. Urausy
8. Weelsof
9. Winlock

3.3.2 Browser ransomware.

Esta clase de ransomware no es muy popular si se compara contra otros tipos, tal como su nombre lo indica, consiste en obstaculizar el uso normal de un navegador web mediante mensajes pop-up codificados en su mayoría con Javascript. Para solventar este tipo de inconvenientes se recomienda la instalacion de algún complemento que bloquee el tipo de mensajes pop-up.
Lo peligroso de esta clase de ataque es que dependiendo de la complejidad con la cual han sido desarrollados, algunos son capaces de desviar el tráfico hacia otra red, como por ejemplo Tor, ejecutar rutinas que pueden interactuar con servicios de comunicación sobre Internet y/o redes sociales, robo de identidades, entre otras.
Algunos ejemplos son:

1. Brolo
2. Browlock
3. Krypterade
4. Ransoc

3.3.3 Crypto ransomware.

Esta forma de ataque es una de las más conocidas, pues consiste en restringir el acceso a los archivos del usuario mediante técnicas de cifrado en un terminal, advirtiendo dicha acción mediante una pantalla de bloqueo en la cual se solicita un pago a cambio de la liberación del acceso. A diferencia de otros ataques, es tal el bloqueo sobre el acceso a los archivos que, en algunos casos, ni siquiera se toma la molestia en ocultarse (característica general del malware) entre los archivos del sistema, su vector de infección puede ser correo electrónico, aplicaciones de mensajería instantánea, descargas automáticas, entre otros.
Algunos ejemplos destacables de este tipo son:

1. Cerber: valiéndose de estrategias de phishing su objetivo principal era Office 365.
2. Crysis: su objetivo son unidades de almacenamiento fijas, extraíbles o en red.
3. Cryptolocker: ransomware que heredaba las características de un troyano, su objetivo son sistemas operativos basados en Windows.

4. CryptoWall: puede decirse que es el sucesor de Cryptolocker luego de su caída. Conocido también bajo los nombres de Cryptobit, CryptoDefense, CryptoWall 2.0, CryptoWall 3.0, entre otros.
5. CTB-Locker: igual de peligroso que los anteriores, cuya principal diferencia es que implementaba el algoritmo de cifrado RSA-2048, lo cual hacía prácticamente imposible la recuperación de los archivos cifrados a no ser que se efectuara el pago del rescate, alternativa que tampoco era una garantía 100% de recuperación de la información.
6. Jigsaw: este tipo de ransomware no solamente cifraba los archivos, sino que también los eliminaba de forma progresiva dentro de un plazo establecido por los ciberdelincuentes, generalmente 72 horas.
7. KeRanger: orientado para infectar sistemas Mac OS X, por lo general en su mayoría de esta clase de ataque había sido enfocado a sistemas Windows.
8. LeChiffre: su característica principal es que necesitaba ser ejecutado de forma local en el equipo infectado, esto se hace por medio de técnicas de penetración que realizan los atancantes en terminales débilmente protegidos.
9. Locky: para su ataque era necesaria la ejecución de macros, cuando estas se encuentraban habilitadas, hace uso del cifrado AES para secuestrar los datos.
10. TeslaCrypt: similar a Locky con la diferencia de que éste último explotaba una vulnerabilidad en Adobe.
11. TorrentLocker: similar a CryptoLocker pero utilizando como vector el correo electrónico, su característica es que no solamente se encargaba de cifrar los archivos en el equipo infectado, sino también, accedía a la libreta de contactos de correo electrónico del mismo para enviarse y de esta forma expandir su infección.
12. Zcryptor: considerado como un híbrido entre un Crypto ransomware y un gusano por su forma en cómo se distribuye mediante unidades externas y unidades flash.

3.3.4 Ransomware orientado a una infraestructura específica.

Hasta el momento se han visto amenazas que han proliferado contra una plataforma específica, sin embargo, también han existido otras variantes cuyo objetivo ha sido una estructura específica o un recurso determinado:

1. MongoDB Apocalypse: fue un ataque realizado por un grupo de hackers a finales del 2016 cuyo objetivo eran servidores de base de datos MongoDB, aprovechándose de la falta de contraseña para el usuario Administrador en dichos servidores, se encargaron de bloquear el servidor de base de datos dejando una nota de pago a cambio del desbloqueo de dicho recurso. El primer grupo de hackers responsable de esta acción fue el denominado Harak1r1, se estima que

durante los primeros dos meses del 2017 resultaron afectados un grupo aproximado de 28,000 servidores.

2. Erebus: Hasta el momento, la mayoría de los ataques de ransomware se enfocaban a la plataforma Windows, sin embargo, el objetivo de esta amenaza eran servidores web basados en Linux. Sus primeras versiones utilizaban un algoritmo criptográfico RSA-2048, añadiendo la extensión «.ecrypt» a los archivos de usuario y dejando las notas YOUR_FILES_HAS_BEEN_ENCRYPTED.txt y YOUR_FILES_HAS_BEEN_ENCRYPTED.html con indicaciones de lo sucedido más la forma de realizar el pago, una de las empresas que mas afectada se vió fue NAYANA, proveedora de hosting en Corea del Sur, que al final terminó cediendo al pago de 1 millón de dólares por el rescate.
3. Rex: este ataque perpetrado por el grupo de hackers identificado como Armada Collective, explotaba vulnerabilidades de los gestores de contenido Drupal, WordPress y Magento. Poseía características de troyano, capaz de ejecutar ataques DDoS y de convertir un servidor Linux en minero de bitcoins.
4. KillDisk: una variante del malware original del mismo nombre, cuya función principal es la de borrar el disco duro, esta variante, además de realizar tal acción dejaba una nota de rescate para engañar a la víctima de que efecutando el pago recibiría nuevamente el acceso a sus archivos personales, de ahí que también sea conocimo como un «falso» ransomware.
5. Fairware: otra variante de amenaza para servidores Linux, consiste en borrar la carpeta pública del servidor web no sin antes realizar una copia de éstos en un equipo propiedad de los ciberdelincuentes vía FTP. Se exige el pago a cambio de no hacer públicos dichos archivos.
6. Kimcilware: el objetivo de esta amenaza eran las tienas en linea, en especial las basadas en Magento, al momente de crifrar los datos en el servidor, se añadía la extensión «.kimcilware» y generaba su propia página index con las indicaciones para poder efectuar el pago del rescate.

3.3.5 Boot ransomware.

Tal como su nombre lo indica, este tipo de ataque tiene entre sus objetivos bloquear el sector de arranque conocido también como Master Boot Record (MBR) imposibilitando el arranque del sistema operativo y mostrando el mensaje de advertencia exigiendo el pago en su lugar para, en teoría, recurar el acceso. Entre algunos ejemplos se tienen los siguientes:

1. Petya: este ataque cifra diferentes archivos de usuario, pero además, también altera la tabla maestra de archivos (MFT) e imposibilita el arranque del Sistema Operativo. Para actuar también necesitaba de la ayuda de otro troyano conocidomo

como Mischa. Surgió apróximadamente en Marzo 2016 afectando a diferentes empresas especialmente de Ucrania y Rusia. Casi un año después de su primera aparición, Marzo del 2017 surgió una nueva versión con algunas variantes denominada PetrWrap.

2. Mebroot: esta amenza aparte de cifrar los archivos del equipo infectado y afectar el MBR para imposibilitar el acceso al mismo desde antes del arranque del Sistema Operativo, también crea una puerta tracera, backdoor, mediante las cual los atancantes ganan acceso total al sistema de la víctima e incluso poder controlarlo de forma remota. Sus primeras apariciones se remontan desde el 2008.
3. Satana: actúa de forma similar a Petya, con la diferencia que tanto el cifrado y el bloqueo al arranque del sistema lo realiza por sí mismo, sin la ayuda de otro tipo de código malicioso; otra proncipal diferencia es que en lugar de bloquear la MFT, este bloqueaba el MBR.

3.3.6 Ransomware para la nube.

Durante los últimos años existe la tendencia de mantener el almacenamiento en la nube a tenerlo todo en forma local en un único equipo, esto es así debido a muchas ventajas que este esquema proporciona, por ejemplo el hecho de poder trabajar de forma remota desde cualquier lugar que cuente con conexión a Internet, almacenar todo tipo de archivos, gestión de copias de seguridad, entre otros. Sin embargo, paralelo a este avance, los ataques tipo ransomware también han ido mejorándose para mal de muchos; erróneamente se ha pensado que el almacenamiento en la nube es una solución para contrarrestar los ataques de ransomware, nada más lejano de la realidad, pues bajo este esquema, lo que se genera es potenciar el riesgo de un contagio a muchos más dispositivos, pues al final, estamos hablando de un disco duro más, solo que virtual. Se presentan algunos ejemplos de este tipo:

1. Sodin: conocido también como Sodinokibi o Revil, esta amenaza explotaba la vulnerabilidad catalogada como CVE-2019-2725 que permitía la ejecución remota de comandos en Oracle WebLogic Server sin necesidad de especificar credenciales de usuario. Para elevar la complejedidad de este ataque, Sodin hacía uso de un esquema híbrido para el cifrado de los archivos. El contenido del archivo es cifrado mediante el algoritmo salsa20, y las claves con un algoritmo asimétrico de curva elíptica. Gracias a la vulnerabilidad mencionada, los atancantes lograban cargar un «dropper» (Software que permite la instalación otro tipo de malware) con el que posteriormente se instalaba el ransomware Sodin.

2. RansomCloud O365: tal como lo indica su nombre, es un ranwomware diseñado para atacar plataformas que trabajan con Office 365.

Con esta clase de ataque, surge un nuevo término denominado «RansomCloud» el cual hereda todas las característica del ransomware tradicional con la diferencia de que busca explotar vulnerabilidades de los servicios que se prestan en la nube.

3.3.7 Ransomware para smartphones.

Los ataques que se han comentado anteriormente han sido dirigidos de forma muy particular, en su mayoría, a plataformas Windows, sin embargo, ningún sistema operativo es 100% seguro (simplementen unos pueden llegar a ofrecer mejor protección que otros), muestra de ello es que se tienen amenazas que han sido descubiertas para plataforma Mac y Linux, sin embargo, debido al auge que han tenido desde hace algunos años atrás, los teléfonos inteligentes y tabletas no se han quedado atrás, algunos ejemplos son los siguientes:

1. Hackeado por Oleg Pliss: en el 2014 muchos usuarios de iPhone, especialmente de Autralia, recibieron a primera hora una notificación con una pantalla de bloqueo con el siguiente mensaje: *Hackeado por Oleg Pliss. Para desbloquearlo TIENES que mandar un bono de 100 euros de uno de estos (Moneypack/Ukash/PaySafeCard) a helplock@gmx.com Te envío código 2618911226*. Se presume que la infiltración se realizó a partir del servicio de iCloud, los atacantes habían logrado comprometer diferens ID’s de Apple mediante técnicas de phishing y de esta manera lograron tener acceso a los dispositivos de los usuarios descargándoles el malware.
2. Fallo en Safari: en el 2017, los atancates aprovechaban una vulnerabilidad en Safari mediante desplegaban pop-up en cientos de páginas web de manera que el navegador quedaba inutilizado, las páginas que se deplegaban presentaban un mensaje con información de organizaciones de seguridad, exigiendo el pago de una cantidad específica en forma de tarjeta de regalo de iTunes cuyo código debía ser enviado por SMS. La solución a este caso era tan simple como eliminar el historial del navegador.
3. DoubleLocker: ocurrió en el 2017, esta amenaza se distribuía principalmente como un falso Adobe Flash Player, una vez el atque se efectuaba de manera exitosa, se modificaba el PIN del dispositivo por un valor aleatorio que no se almacenaba en ningún lado, ni siquiera el ciberdelicuente sabía cuál era (pero éste último si sabía cómo modificarlo de forma remota), utilizaba el algoritmo basado en AES para cifrar los archivos adicionándoles la extensión «.cryeye». Para liberarse de esta amaneza, estaba la opción de pagar el rescate (un método para nada

recomendado) o restaurar el terminal a sus valores de fábrica lo que implica la pérdida de toda la información personal almacenada en el teléfono.

4. Android/Filecoder.C: en Julio de 2019 se dió a conocer este ataque orientado a Android, se distribuía por medio de mensajes de texto con enlaces maliciosos. Su forma de operar era un poco más elaborada que otras, puesto que luego de infectar el equipo de la víctima, accedía a la lista de contactos para poder enviarse en el mismo idioma del terminal comprometido e incluso incorporaba el nombre de la persona en el mensaje a quien iba dirigido el ataque para ser más convincente, sumado a lo anterior, también cifraba los datos.
5. CovidLock: lamentablemente los ciberdelicuentes, aprovechando la pandemia que ha paralizado al mundo a principios de 2020, realizan la infección mediante la visita a un sitio fraudulento en el que se invita a la victima a que instale una App para Android que supuestamente ofrece información en tiempo real sobre el Covid-19 tales como gráficos y zonas geográficas en las que se ha dado un mayor impacto de la pandemia. Una vez se realiza la instalación de la App, el usuario es obligado a modificar su contraseña de desbloqueo del dispositivo, luego de realizar este cambio, se le presenta al usuario una pantalla de bloqueo con una nota de rescate exigiendo 100 USD en Bitcoin dentro de un plazo de 48 horas, de lo contrario toda la información personal será eliminada y a la vez hecha pública.

3.3.8 Ransomware para IoT (RoT).

Los ataques de ransomware se han extendido de plataforma en plataforma, han llegado a los smartphones, han logrado trascender hasta la nube secuestrando datos, sin embargo, alguien podría pensar que por lo general los dispositivos IoT al no almacenar datos de usuario éstos podrían quedar fuera del radar de los ciberdelincuentes, sin duda alguna se trata de un pensamiento muy errado puesto que lo que se limitaría en este caso es el acceso al control total del disposito o incluso el acceso a la red en la cual éstos se encuentran. Imaginemos que un ataque de esta clase pudiera evitar las entradas o salidas a una Smart House, detener un automóvil, manipular la electricidad en un cuarto, controlar la temperatura dentro de una habitación, un sin fin de posibilidades las cuales son un verdadero incentivo para exigir montos de dinero elevados a cambio de la liberación del recurso tecnológico. Se debe tomar en cuenta que estos dispositivos al final cuentan con sistemas operativos muy conocidos y adaptados, con una conexión permanente a Internet, además, el tema de la seguridad en IoT no es algo que haya progresado de la misma forma en cómo lo ha

hecho en el caso de los sistemas para servidores, desktop's o smartphones.

3.4 Vectores de infección.

Los vectores de infección no difieren mucho del malware tradicional, de hecho, existen diferentes formas de lograr que un ataque sea exitoso, prácticamente cualquier dispositivo se encuentra expuesto (servidores, equipos de usuario, teléfonos inteligentes, dispositivos IoT, servicios en la nube). En la sección anterior se presentaban algunos ejemplos de cada tipo de amenzas y, en algunos casos, la forma en cómo realizaban con éxito su infeccción. Se presentan a continuación los vectores de ataque más conocidos hasta el momento:

1. Adjuntos en correo electrónico: el ataque se dispara cuando un usuario abre un archivo adjunto con contenido malicioso.
2. Enlaces embedidos en documentos: probablemente el archivo como tal no represente mucho riesgo, para no levantar sospecha, sin embargo, dentro de su contenido existen enlaces a los cuales si el usuario hace clic provoca que se dispare el ataque.
3. Enlaces en el cuerpo del correo electrónico: similar a la anterior, con la diferencia de que no se incorpora un archivo adjunto sino que el enlace se encuentra directamente en el cuerpo del correo.
4. Descarga de archivos: este ataque se ejecuta por medio de archivos que el usuario descarga (software, pdf, entre otros).
5. Sitios web comprometidos: usuarios que navegan o son enviados a sitios web para que su equipo sea analizado, mediante *Exploit Kits*, para la posterior descarga del ransomware.
6. Unidades de almacenamiento externas: generamente dispositivos de almacenamiento USB, discos duros o unidades de red comprometidas.
7. Exploit Kits: son herramientas desarrolladas para determinar vulnerabilidades en un equipo del usuario, sin que éste lo perciba, para poder explotarlas y de esta forma hacerle llegar el ransomware. Se presentan algunos de éstos recursos maliciosos:
    1. Angler: uno de los primeros conocidos, en el 2013, utilizado para identificar y explorar vulnerabilidades es Adobe Flash Player, Internet Explorer, Microsoft Silverlight, Java, y ActiveX, utiliza técnicas sofisticadas para saltarse medidas de detección y prevención tradicionanes como antivirus y virtualización. Se ha utilizado para distribuir el siguiente ransomware: CryptoWall 4.0, CryptXXX, HydraCrypt, Locky, TeslaCryp.
    2. Bizarro Sundown: ha logrado explotar una falla de corrupción de memoria de Internet Explorer y vulnerabilidad de desbordamiento de memoria en Adobe Flash Player; también se ha realizado una variante de este ataque denomida GreenFlash Sundown la cual consistía en hacer redirecciones mediante URL que aparentaban ser legítimas. Se ha utilizado para distribuir diferentes variantes de Locky.

3. Fallout: identificado a finales de 2018, explotaba las vulnerabilidades CVE-2018-4878 y CVE-2018-8174 por medio de las cuales distribuía el ransomware GandCrab.
4. Neutrino: descubierto en 2012, explotaba vulnerabilidades en todas las versiones de Java hasta la versión 7 update 11, así como también vulnerabilidades entoncradas en Flash. Entre las amenzas que distribuía se tiene a PizzaCrypts y también variantes de ransomware Bandarchor y CrypMIC.
5. Nuclear: detectado en el año 2009, se aprovechaba de vulnerabilidades en Active X, Flash, Internet Explorer, Java, PDF, y Silverlight. Permitía la intrusión de diversos malware y ransomware como CryptoWall 4.0.
6. RIG: uno de los mas activos desde Febrero de 2015, en sus diferentes versiones ha logrado inyectar diferentes clases de amenazas, aprovechando también las vulnerabilidades CVE-2015-5119 y CVE-2015-5122. Entre el ransomware que ha distribuido se encuentra Radamant y CryptoBit.

8. Equipos débilmente protegidos: este vector esta más relacionado con las políticas de seguridad débilmente implementadas por los responsables de TI, utilizando configuraciones y contraseñas por defecto o simples. Los ciberdelincuentes buscan este tipo de fallas para lograr explotarlas e inyectar de esta manera su código malicioso.

3.5 Modelo de negocios.

A nivel general existen dos maneras por medio de las cuales el atacante obtiene el pago exigido por el rescate:

1. El ciberdelincuente posee información sensible que incluso puede dañar la imágen de la víctima si esta es hecha pública, esto puede generar que la víctima guarde silencio en algunos casos, lo que facilita que ésta se vea obligada a pagar el rescate exigido.
2. El cibercriminal brinda instrucciones a la víctima sobre cómo realizar el pago mediante transferencias bancarias de dinero o criptomoneda a cuentas en bancos ubicadas en países con leyes de secreto bancario estrictas, lo que provoca que éstas no se puedan identificar.

En ambos casos el anonimato juega un papel muy importante, una forma de garantizarlo en la red es la navegación de forma anómina que ofrece la Deep Web a la cual se puede acceder gracias al navegador Tor, lo que contribuye a que dicha modalidad de secuestro de información digital sea muy lucatriva.

Ransomware como servicio (RaaS):

Ataques como el de Wanacry fueron muy mediáticos y dejaron al descubierto para muchos la forma en cómo éste opera, gracias a esto, comenzaron a surgir algunas medidas de prevención para reducir la

efectividad de este tipo de ataques, lo que ha provocado que la forma de «hacer negocio» pueda evolucionar adoptando modelos por suscripción, similiar a como lo hacen servicios legalmente establecidos como Netflix, Spotify, Youtube, entre otros. A este modelo de negocio de le conoce con el nombre de Ransomware-as-a-Service (RaaS), dentro de este esquema se desarrollan conjuntos de herramientas o kits de ransomware fáciles de utilizar por personas sin conocimientos técnicos especializados quienes son los responsables de realizar los ataques contra objetivos bien determinados; básicamente se tienen dos figuras:

1. Autor o autores del kit ransomware: son los responsables de crear, mantener y mejorar los kit de ransomware, así como de promocionar su uso en la «deep web». El autor o autores son desarrolladores con conocimientos técnicos preferentemente en el área de criptografía en informática.
2. Comprador o suscriptor (afiliado): persona sin conocimientos técnicos avanzanos que se encarga de distribuir el ransomware adquirido mediante el servicio de suscripción, como se ha visto anteriormente, existen diferentes vectores de infección que pueden utilizarse. Muchas veces este agente tiene acceso a un *panel de administración*, similar al de una suscripción legal, para llevar un mejor control de sus infecciones y sus ganancias.

Bajo esta dinámica, cuántas más infecciones logren realizarse con éxito mayores serán las ganancias, lo que garantiza el desarrollo de nuevas funciones y continuidad de esta actividad ilícita. Algunos ejemplos de este tipo son:

1. Satan: ofrece una interfaz profesional que le permite al usuario llevar una gestión de las infecciones y el dinero recaudado a partir de éstas, incluso brinda recomendaciones sobre cómo realizar la infección. Su uso es gratuito, pero se debe pagar un 30% de cada ganancia ilícita a los desarrolladores.
2. Philadelphia: uno de los servicios más sofisticados, no es un servicio de suscripción propiamende dicho, se puede realizar una compra directamente por el valor $389 (en Bitcoins), a cambio, se obtiene un acceso de por vida gracias al cual podrá «gozar» de diferentes características de malware, acceso a las últimas versiones, soporte técnico, entre otros. A diferencia de otros esquemas, no necesita distribuir las ganancias con el operador RaaS.
3. MacRansom: en este RaaS, el 30% de las ganancias ilícitas es para los afiliados, mientras que el resto es para los desarrolladores, su característica particular es que el malware que se ofrece está especialmente dirigido a equipos MacOS.
4. Stampado: conocido como la primera versión de Philadelphia, permite ejecutar campañas de infección en un corto tiempo. Dentro de este RaaS, es posible obtener un kit por un precio de $39.

5. RaaSberry: le permite al cliente o suscriptor mantener el 100% de las ganacias ilegales, ofrece diferentes planes de pago desde un costo inicial de $60. Entre las ventajas que se ofrecen son: soporte técnico, compatibilidad con diferentes sistemas operativos, entre otros.
6. Frozr Locker: es una de las soluciones más caras de RaaS, pues su costo es de $1,262.00, se puede usar idefinidamente sin la necesidad de actualizar la suscripción, permite personalizar formas de pagos, mensajes, decifradores, entre otros.

3.6 Estrategias de prevención.

Se proponen los siguientes puntos para la prevención no solo de ranwomware (pues no es la única amenaza que existe):

1. Establecer una política de seguridad a nivel de TI: se establecen los lineamientos y procedimientos a seguir por parte del equipo de TI para reducción de riesgos informáticos, entre los puntos que más se pueden destacar estan:
    1. Características y clasificación de la información, lo que permitirá identificar entre otras cosas, cuáles son los datos más sensibles de una organización y obviamente aplicar políticas de seguridad más estrictas en este tipo de datos.
    2. Identificar a los responsables de la información, así como el nivel de acceso que poseerá cada uno.
    3. Gestión de usuarios y políticas de contraseña.
    4. Políticas de antivirus, uso de los recursos tecnológicos proporcionados por la organización, uso de aplicaciones e Internet.
    5. Gestión de endpoints y servidores.
    6. Programación de auditorías de seguridad informática.
    7. Capacitaciones de personal para identificar posibles amenazas como por ejemplo, correos electrónicos, archivos adjuntos, archivos con «doble extensión», no navegar en sitios de dudosa credibilidad o hacer uso no adecuado de los equipos que les han sido confiados.
2. Seguridad física y del entorno: cómo se controlará el acceso a los terminales, servidores y otros equipos que sostienen el funcionamiento y la seguridad de la red telemática. En ese apartado se involucra a todas aquellas medidas no virtuales para prevención de intrusiones.
3. Defesan perimetral: involucra todos los elementos necesarios para establecer una barrera de seguidad entre la red exterior (comúnmente Internet) y la red interna de la organización, entre estos elementos se destacan:
    1. Routers de frontera: es necesaria una adecuada configuración de éstos equipos, según necesidades de la organización.
    2. Firewall: se definen e implementan las reglas para restringir el tráfico no deseado, autorizar comunicaciones, además,

permiten establecer canales cifrados, mejor conocidos como VPN’s.

3. Sistemas de detección de intrusos: estos elementos permiten detectar tráfico sospechoso, acceso no autorizado a un equipo, servicios que se encuentran habilidatos y que podrían no ser imprescindibles, además, son un apoyo para la realización de auditorías.
4. Creación de VPN’s: son canales seguros que se establecen para obtener acceso a un recurso dentro de la red de la organización por medio de Internet.
5. Definir y preparar Host Bastion.
6. Segmentación de red según el tamaño y necesidades de la organización, también se recomienda la inclusión de una zona desmilitarizada (DMZ).

4. Protección de la red Interna: esta parte va de la mano con el punto de seguridad perimetral pues se complementa con la implementación de:
    1. Cortafuegos personales.
    2. Licencias de antivirus auténticas y actualizadas constantemente.
    3. Listas de acceso a redes virtuales, cuando aplique.
    4. Herramientas antispyware.
    5. Configuración de sistemas operativos.
    6. Implementar herramientas de cifrado de contenido.
5. Protección de aplicaciones: todo lo relacionado a la autenticación y autorización sobre el uso de aplicaciones.
6. Protección de datos: involucra todas las medidas que conllevan a la protección de datos de la organización, se debe tener un cuidado especial con la legislación del país en el que se procesa y almacena dicha información, ya que de no cumplirla, se pueden acarrear desde una amonestación hasta la imposición de multas y cierre. Establecer estrategias de respaldo de información utilizando equipos NAS y/o servicios en la nube que se actualicen con una periocidad que reduzca la pérdida de información en caso de incidentes.
7. Protección de equipos: se recomienda aplicar lo que se conoce como «hardening» para la puesta en producción no solo de servidores, sino también de equipos destinados a usuarios finales, realizar actualizaciones de los mismos, mostrar siempre la extensión de todos los archivos, entre otros.

3.7 Medidas para recuperación de desastres.

Ante un ataque realizado, lo que se debe hacer en primer lugar es aislar el equipo (desconectando la red y medios extraíbles de almacenamiento). En segundo lugar, conservar la calma y evitar a toda costa realizar el pago por dicho rescate. Por último, tratar de identificar cuál ha sido el vector de ataque para reducir la posibilidad de que más equipos sufran el mismo incidente y tomar las debidas acciones de

prevención. Se presentan algunos escenarios de cómo proceder frente a alguna infección:

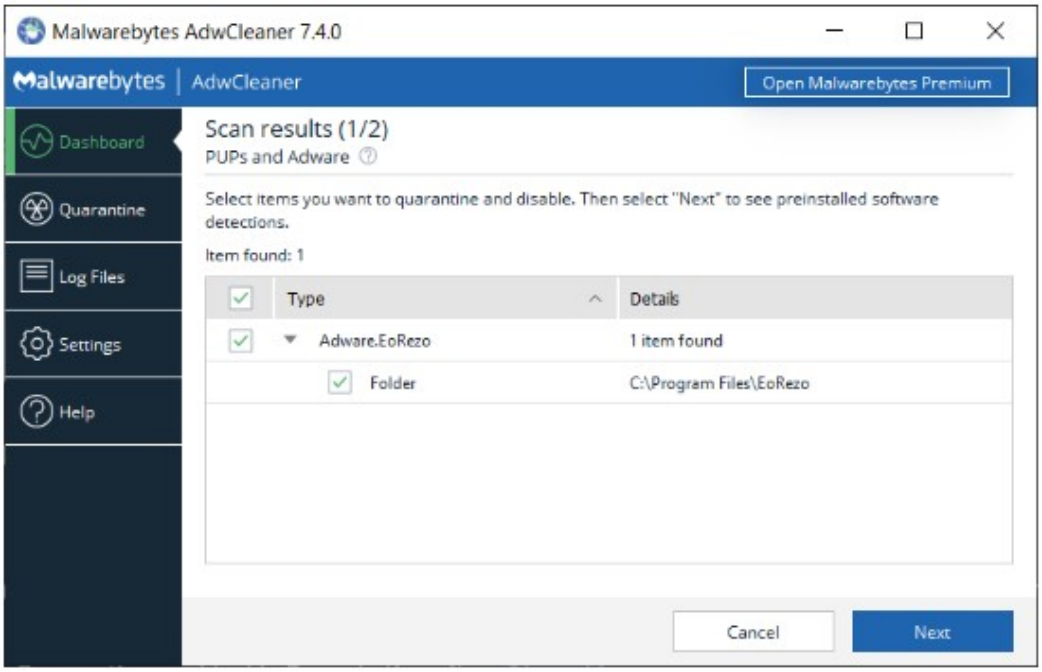
Hacer uso de la copia de respaldo:

Como se ha mencionado, una medida de prevención es mantener las copias de respaldo actualizadas, pues frente a esta eventualidad, hacer uso del respectivo y último backup realizado para recuperar el máximo de información posible, previamente se recomienda hacer una reinstalación del sistema operativo para eliminar cualquier rastro del malware que pudiera quedar oculto en el sistema. Al final de dicho proceso, secularizar el equipo para la prevención de futuros ataques exitosos.

Tratar de descifrar la información:

De no ser viable el escenario anterior, lo primero que debe hacer es eliminar el ransomware con alguna solución antivirus o antimalware cuya base de datos se encuentre actualizada. Una buena alternativa sería Malwarebytes[1]:

Figura 1: Pantalla principal de Malwarebytes



Lo segundo, tratar de descifrar los archivos encriptados, esta es la parte más crucial, pues no se tiene certeza de qué tanto porcentaje de información se podrá recuperar, se presentan dos soluciones que podrían ayudar en este sentido:

1 https://es.malwarebytes.com/

id-ransomware
Url: https://id-ransomware.malwarehunterteam.com/

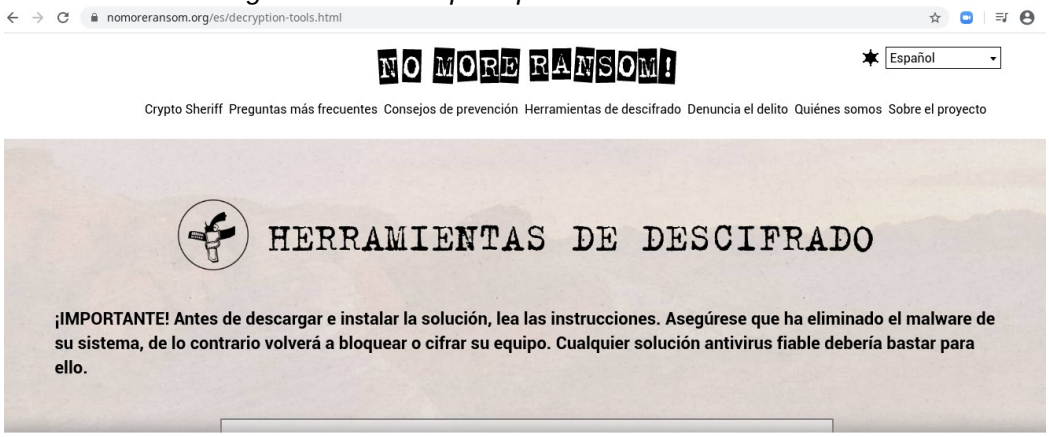
Este software servirá para identificar el tipo de ransomware que ha realizado el ataque, existen dos vías: cargando el archivo de la nota de rescate ó cargar uno de los archivos que han sido cifrados. El archivo que se cargue será analizado con la base de datos de la mencionada herramienta para su identificación, una búsqueda positiva indica que existe una forma conocida para realizar el descifrado y se redireccionará al recurso encontrado para hacerlo. Una búsqueda negativa indica que aún no existe ningún método para revertir el cifrado, la información será analizada por expertos en malware para identificar futuras infecciones o en el mejor de los casos, encontrar un método para revertir el resultado de algoritmo criptográfico implementado.

Figura 2: Pantalla principal de id-ransomware

No more ransom!
Url: https://www.nomoreransom.org/es/decryption-tools.html

Este sitio presenta diferentes recomendaciones para prevernir un ataque de ransomware, lo más importante, es que también ofrece un conjunto de herramientas de descifrado desarrolladas gracias a que el código malicioso poseía un bug o que se conozca su clave pública.

Figura 3: Pantalla principal de No more ransom!



Sobre Smarphones:

El método a seguir no sería muy diferente al descrito anteriormente, en el caso de los teléfonos inteligentes es posible restaurarlo a sus valores de fábrica (perdiendo todos los datos de usuario en el camino) y recuperar la información desde un respaldo que se tenga en una nube. Es de comentar también que si se opta por una desinfección, Malwarebytes también ofrece versiones para Android e IOS. Aunque todavía queda el problema de los archivos cifrados.

Sobre dispositivos IOT:

Este es el escenario más complicado, puesto que las medidas comentadas anteriormente no son aplicables a esta situación, en su mayoría los dispositivos IOT no reciben actualizaciones que pudieran cubrir vulnerabilidades en los sistemas operativos de éstos y como agravante, el tema de la seguridad en este tipo de recursos tecnológicos no avanza al mismo ritmo que en otros escenarios, por lo que se desconoce de algún método de recuperación al momento de ser víctima de un ataque de esta clase.

Sobre el ransomware para la Nube:

En ese caso como se tienen multitud de servicios en la nube, lo recomendado es conctactar con el soporte técnico del servicio contratado para obtener la respectiva guía de cuál es la mejor forma de proceder frente a una situación como ésta.

Como se dijo anterioremente, lo mejor es la prevención, ya que no hay una garantía de recuperación del 100% de la información cifrada, sumado a que existen diferentes variantes de cada amenaza que va saliendo a la luz y cada vez son más sofisticadas que lo que dificulta el descrifrado.

3.8 Impactos legales.

Sobre aspectos legales existen diferentes proporciones de avance en temas de seguridad informática, diversas legislaciones hacen referencia a la protección de los datos y a las penalidades en caso de su respetiva vulneración. En lo referente a los ataques de ransomware, se visualizan delitos como los siguientes: suplantación de identidad, alteración ilegal de un sistema informático, denegación de servicio, acceso no autorizado a datos personales, divulgación de información no autorizada y extorción. Se presentan 3 escenarios de ejemplos:

Legislación sobre ciberseguridad en El Salvador:

En el 2016 se aprobó la *Ley Especial contra los Delitos Informáticos y Conexos*[2] la cual establece los siguientes delitos que pudieran considerarse frente a un ataque ransomware:

1. *Acceso indebido a los programas informáticos o datos informáticos*, según el *Artículo 5*, será sancionado con prisión de 2 a 4 años. Como se ha visto, algunos tipos de ransomware se han activado de forma remota, lo que conlleva a realizar un acceso no autorizado en el sistema operativo; por presentar un ejemplo.
2. *Interferencia del sistema informático*, según el *Artículo 6*, será sancionado con prisión de 3 a 6 años, el malware por definición altera el funcionamiento normal de un equipo informático.
3. *Daños a sistemas informáticos*, según el *Artículo 7*, será sancionado con prisión de 3 a 5 años el que inhabilite un sistema informáctio. Como se ha dejado en claro, un ransomware impide que el dispositivo se continúe ejecutando.
4. *Posesión de equipos o prestación de servicios para la vulneración de la seguridad*, según el *Artículo 8*, será sancionado con prisión de 3 a 5 años la prestación de servicios cuyo objetivo sea la vulneración de un sistema informático, en este caso se puede considerar la modalidad de ataques conocida como RaaS.
5. *Violación de la seguridad del sistema*, según el *Artículo 9*, será sancionado con prisión de 3 a 6 años la persona que vulnere la seguridad de un sistema informático sin la debida autorización. Acá se puede incluir la figura de la persona que realiza el ataque, no necesariamiente que sea el autor del ransomware, tal como ocurre en RaaS.
6. *Estafa informática*, según el *Artículo 10*, será sancionado con prisión de 2 a 5 años la persona que busque generar un beneficio personal como resultado de una operación ilegal, en otras palabras la extorción que caracteriza la forma de operar de un ransomware.
7. *Fraude informático*, según el *Artículo 11*, será sancionado con prisión de 3 a 6 años la persona que introduzca instrucciones fraudulentas en un sistema informático para lograr un beneficio

2 https://www.asamblea.gob.sv/decretos/details/2688

personal. Contextualizando, es la persona que logra intrudicir el malware al sistema informático de la víctima.

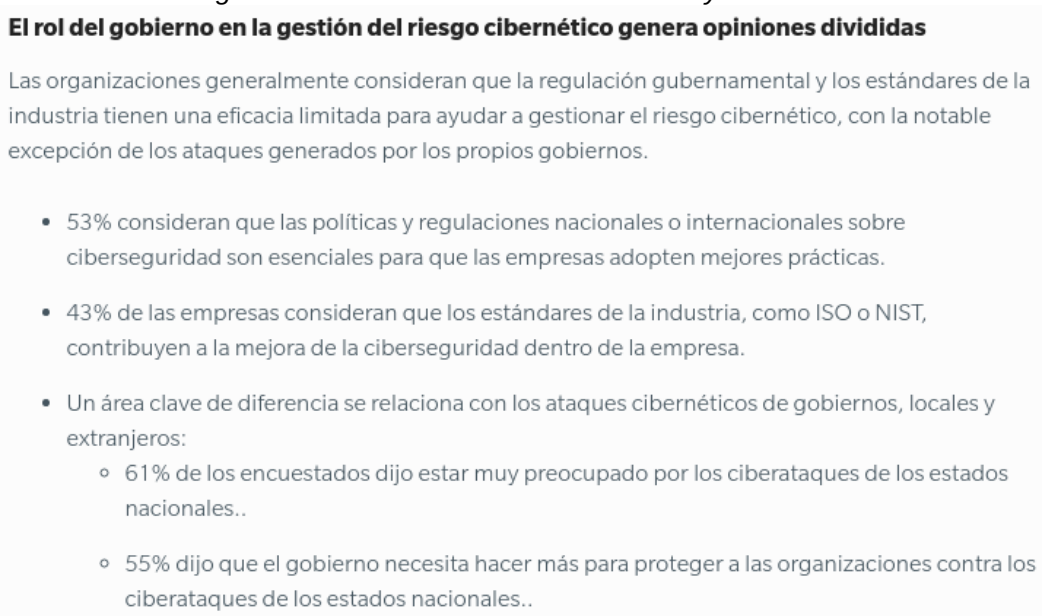
8. *Espionaje informático*, según el *Artículo 12*, será sancionado con prisión de 6 a 10 años la persona que obtenga acceso no autorizado a información catalogada como confidencial, muchas veces durante un ataque de ransomware, antes de procederse al cifrado, se tiene acceso no autorizado a datos confidenciales que gestiona la víctima.
9. *Hurto por medios informáticos*, según el *Artículo 13*, será sancionado con prisión de 2 a 5 años la persona que se apodere de bienes tangibles o intangibles de caracter personal o patrimonial, lo cual se cumple al establecer un bloqueo al terminal infectado, de esta forma quitándole el control del mismo a su legítimo dueño.
10. *Técnicas de denegación de servicio*, según el *Artículo 14*, será sancionado con prisión de 3 a 5 años la persona que provoque la denegación de un servicio informático, un ejemplo bastante claro son los ataques de ransomware realizados a servidores web.
11. *Alteración, daño a la integridad y disponibilidad de los datos*, según el *Artículo 19*, será sancionado con prisión de 3 a 6 años la persona que altere o duplique la disponibilidad de la información de forma no autorizada, ya sea que ésta se encuentre moviendo en un medio de transmisión o almacenada en algún dispositivo para tal fin. Los ataques de ransomware no solamente cifran y bloquean los datos, sino que también, en algunas ocasiones, se hacen copias ilegales de toda la información a servidores bajo control del ciberdelincuente.
12. *Hurto de identidad*, según el *Artículo 22*, será sancionado con prisión de 5 a 8 años el que realice la suplantancación de identidad con el objetivo de proceder a una extorción.
13. *Divulgación no Autorizada*, según el *Artículo 23*, será sancionado con prisión de 5 a 8 años el que sin autorización divulgue información contenida en algún medio de almacenamiento, últimamente las amenazas de ransomware no solamente realizan el cifrado, sino que, el pago se exige a cambio de no divulgar en Internet la información secuestrada.
14. *Revelación indebida de datos o información de carácter personal*, según el *Artículo 23*, será sancionado con prisión de 3 a 5 años la persona que divulgue información obtenida gracias a medios fraudulentos para su divulgación, esto incluye material sexual explícito todo con ánimos de lucrarse.

Aunque ya se cuenta con una ley, se ha difundido muy poco; aun no forma parte del plan de estudios de muchas carreras relacionadas con TI; tampoco existe una forma en la que las autoridades como policía, fiscalía y jueces trabajen en conjunto para su aplicación; sin duda son retos a superar en un futuro dentro del marco jurídico salvadoreño.

Sobre la legislación en América Latina:

Una encuesta realizada por Marsh y Microsoft titulada «Percepción del riesgo cibernético en Latinoamérica 2019[3]» muestra que las organizaciones han tomado mayor conciencia sobre los riesgos informáticos que existen y sobre de todo del alcance que pudieran llegar a tener. Sin embargo, resulta de vital importancia que dicha preocupación y acciones particulares se vean reforzadas con el apoyo de legislaciones promovidas por los gobiernos de diferentes países:

Figura 4: Resultados de encuesta Marsh y Microsoft



Cada Estado ha tomado la iniciativa de crear por cuenta propia regulaciones que contribuyan a perseguir el ciberdelito en mayor o menor medida, es decir, cada uno tiene su propio avance en este ámbito legal, algo que hay que reconocer, es que gracias a Internet, las fronteras que delimitan a los países no existen, por lo que habrá que trabajar bastante en una homologación de los esfuerzos que cada país realiza.

<u>Sobre la legislación en Europa:</u>

La legislación Europea lleva más de una década en su evolución, lo que la constituye en una legislación, robusta, depurada, restrictiva e implacable al momento de considerar los ciberdelitos, es un modelo a seguir por el resto países fuera del espacio europeo. la Unión Europea (UE) ha comprendido que la nueva era digital ofrece nuevas posibilidades de crecimiento y expansión pero a la vez conlleva un nicho para la ejecución de delitos informáticos, sumado a eso, ha comprendido también que Internet sobrepasa las fronteras físicas de sus Estados

3 https://www.marsh.com/uy/es/insights/research/marsh-microsoft-encuesta-percepcion-riesgo-cibernetico-2019.html

Miembros y para hacer frente a las ciberamenazas es necesario realizar acciones transversales para contrarrestarlas.
Dado el escenario anterior, se ha creado el «Reglamento Europeo 2019/881[4]» que pretende ser un marco legal vertebral a nivel de Europa al que todos sus Estados Miembros puedan acogerse, se busca abarcar distintos ámbitos como por ejemplo:

1. Contrarrestar la delincuencia organizada.
2. Trabajar en su política exterior.
3. Establecer las bases para una ciberdefensa.

Un ente que juega un rol bastante activo e importante es *La Agencia Europea para la Ciberseguridad (ENISA)*, entre sus actividades más destacables están:

1. Brindar un ambiente de cooperación entre gobiernos, instituciones y organismos de la Unión Europea.
2. Elaboración y ejecución de prácticas de ciberseguridad.
3. Presentación de informes sobre la situación actual de la UE en materia de ciberseguridad.
4. Impulsar normas y certificaciones de ciberseguridad.

Tal como se mencionó antes, las actividades y esfuerzos en la lucha contra la ciberdelincuencia en general, por parte de la UE, es un referente para el resto de naciones.

3.9 Acciones de empresas de antivirus.

Las grandes empresas de antivirus realizan investigaciones de forma permanente para ofrecer la mejor protección posible contra este tipo de amenazas. Se presentan algunos ejemplos:

1. ESET: ofrecen lo que ellos mismos denominan una protección multicapas para la prevención de ataques tipo ransomware:
   1. Escudo contra Ransomware.
   2. Protección de ataques contra la red.
   3. Sistema de protección contra malware en la nube.
   4. Detecciones ADN.

   Más información al respuesto se puede consultar en: https://www.eset.com/es/ransomware-empresas/#

2. Bitdefender: Bitdefender Labs realiza un seguimiento y análsis de las amenazas actuales y las posibles a futuro, prestándole especial atención al ransomware debido a los estragos que puede llegar a causar. Al igual que ESET, Bitdefender por medio de su solución GravityZone ofrece protección multicapas para proporcionar prevención, detección y reparación.

4 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Más información al respuesto se puede consultar en:
https://www.bitdefender.es/business/cyber-threats-solutions/anti-ransomware.html#why-bitdefender

3. Kaspersky: ofrecen deiferentes soluciones, uno de sus principales productos es su antivirus que bloquea diferentes clases de malware: virus, ransomware, spyware, cryptolockers, malware de la minería de criptomonedas, entre otros.

   Más información al respuesto se puede consultar en:
   https://latam.kaspersky.com/antivirus

4. Sophos: ofrece difentes soluciones para Windows, Mac y Linux, dentro de las cuáles también se encuentra la detección del ransomware de archivos y el ransomware de discos utilizado en los ataques wiper que manipulan el registro de arranque maestro

   Más información al respuesto se puede consultar en:
   https://www.tecnozero.com/antivirus-y-anti-ransomware/

Se han presentado unos pocos ejemplos sobre soluciones comerciales de antivirus, muchas de ellas proclamándose como la mejor solución del mercado para protección y eliminación de ransomware, sin embargo, es de recalcar que los ciberdelincuentes siempre van a la vanguardia, mejorando sus técnicas de infección y depurando de mejor forma sus códigos maliciosos lo que supone un gran reto para todos los equipos de investigación de ciberseguridad de las casas comerciales.

Existe una investigación realizada por Safebreach Labs[5] (un grupo élite de investigadores en seguridad ofensiva) durante la cual después de probar tres importantes soluciones anti-ransomware ofrecidas por proveedores de ciberseguridad, ninguna de las tres logró detener los ataques.

Esto indica que mientras los equipos de investigación de las casas comerciales de antivirus buscan y analizan nuevas amenazas, los ciberdelincuentes ya están trabajando o ya cuentan con nuevas estrategias de infección capaz de saltarse los antivirus.

Ciertamente contar con una solución completa de antivirus reduce un poco la efectividad de un ataque pero ninguna es capaz de ofrecer una protección del 100% de esta clase de amenaza. La mejor apuesta siempre es adoptar medidas de prevención como las que se describe en el apartado 3.6.

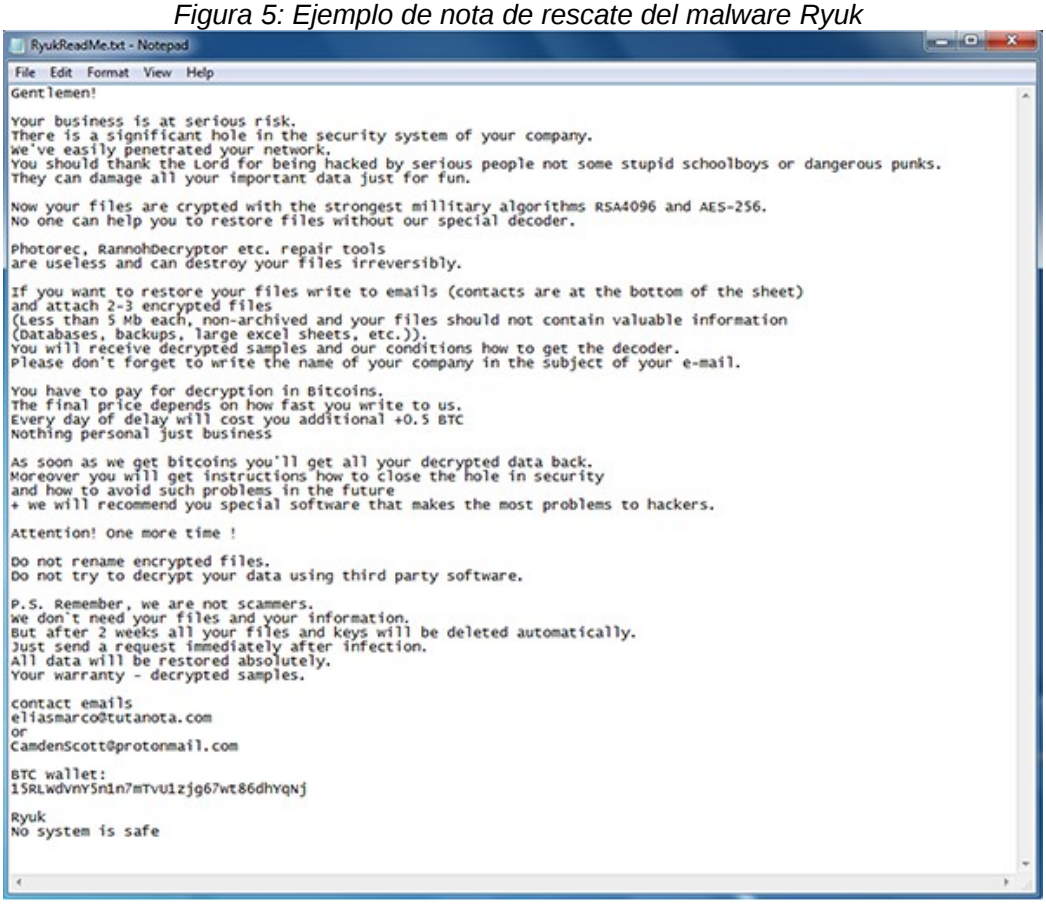
5 https://safebreach.com/Post/EFS-Ransomware

4. Caso Notable de Campaña de Ransomware: Ryuk Ransomware:

4.1 Antecedentes:

A finales del 2018, algunas organizaciones reportaban de que les era imposible tener acceso a sus equipos e información pues estos se encontraban cifrados y al mismo tiempo, al iniciar el Sistema Operativo, se mostraba una nota de rescate como la siguiente:

Figura 5: Ejemplo de nota de rescate del malware Ryuk



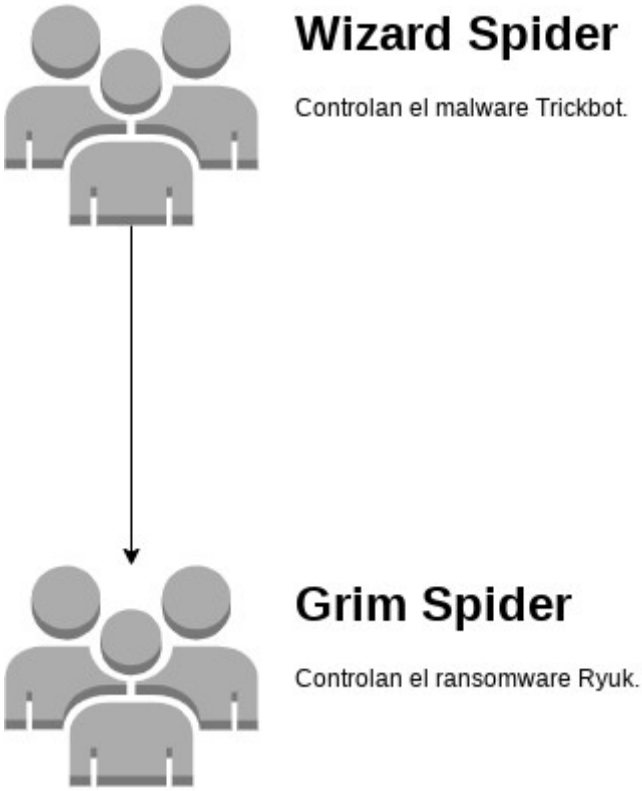
Era una evidencia bastante clara de que habían sido víctimas de uno de los ataques informáticos más letales de los últimos años, el Ransomware.

Corporaciones como la Cadena SER y otras emisoras de Prisa Radio, el Ayuntamiento de Jerez, direfentes instituciones hospitalarias, instalaciones de la Guardia Costera en Estados Unidos, entre otros, se han visto fuertemente golpeadas en sus operaciones por ataques de esta clase posterior al ya muy recordado Wannacry.

4.2 ¿Quiénes esaban tras este ataque?

Ryuk está soportado por el grupo de ciberdelincuentes conocido como Grim Spider, el cual es una célula de otro grupo conocido como Wizard Spider:

Figura 6: Grupo que mantiene Ryuk



En sus inicios esta campaña se encontraba relacionada con otras familias de malware, especialmente los troyanos bancarios Emotet y Trickbot, aunque no se descarta que podría ser distribuido por otros malwares. La campaña Emotet - TrickBot – Ryuk resultaba efectiva debido a sus componentes:

1. Emotet: es un troyano bancario modular detectado por primera vez en 2014, y aunque tiene sus propias funcionalidades maliciosas, se ha utilizado cada vez más como un medio para la distribuición de otros troyanos. Opera por medio de campañas de Spam vía correo electrónico con archivos ajuntos que incorporan las macros maliciosas y generando persistencia.
2. TrickBot: este es otro troyano bancario que era descargado gracias a Emotet en el equipo infectado. Empleaba técnicas de manipulación del navegador para facilitar el robo de datos con el objetivo de acceder a las diversas cuentas en línea de las víctimas para permitir un mayor fraude y generar ingresos

financieros para los operadores y moverse de forma lateral por medio de la red de la organización, explotando también la vulnerabilidad de Eternalblue.

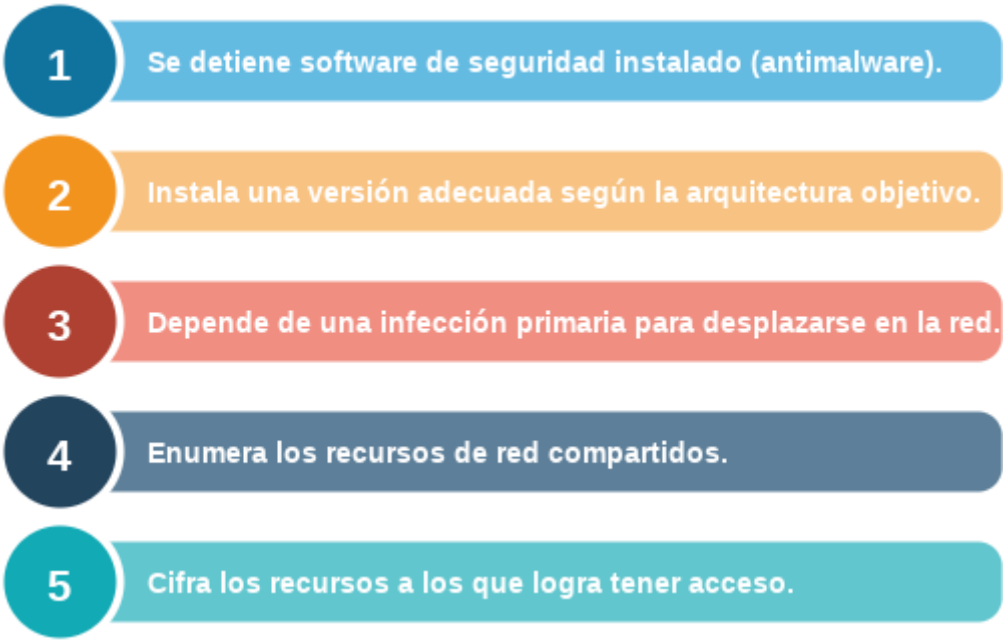
3. Ryuk: una vez se tenga la suficiente información de los equipos infectados gracias a TrickBot, se procede a la descarga del ransomware que se encargaba de cifrar los archivos, bloquear el sistema y presentar la nota de rescate.

Según una investigación realizada por EDSI Trend[6], la combinación de las 3 amenzas anteriores tiene como objetivo principal la efectividad, un factor que contribuye fuertemente a esto es que Emotet implementa técnicas de Inteligencia Artificial para efectuar el robo de cadenas de correos electrónicos y listas de contactos, haciendo que los mensajes fraudulentos sean bastante realistas. Una vez estando dentro de la red, se utiliza TrickBot para descrubrir la mayor cantidad de vulnerabilidades en diferentes terminales para finalizar con la implantanción de Ryuk.

4.3 ¿Cómo funciona Ryuk?

Una infección, en sus inicios, de Ryuk se puede resumir en los siguientes pasos:

Figura 7: Infección de Ryuk en sus inicios.



Todos los archivos no ejecutables son cifrados (utilizando RSA-2048 y AES-256) y modifican su nombre adicionando la extensión de archivo «.ryk». Se coloca una nota de rescate en cada carpeta procesada con el nombre RyukReadMe (.html o .txt).

6 https://www.youtube.com/watch?v=CRCL9zma_ac

4.4 Evolución de Ryuk:

Uno de los aspectos que hacen de este malware una verdadera amaneza es que ha evolucionado al punto de poder utilizar la función Wake-on-Lan que prácticamente le permite «encender una computadora apagada» por medio de la red.

Wake-on-Lan (WoL) es un protocolo gracias al cual muchos administradores de sistemas pueden encender un equipo de forma remota para poder realizar cualquier tarea de mantenimiento o incluso actualizaciones dentro de una organización, la ventaja es que dichas tareas las pueden realizar en horas no laborales de los usuarios. El detalle de cómo trabaja este protocolo se encuentra fuera del alcance de esta investigación, pero a nivel general se puede decir que todas las operaciones de este encendido se realizan a nivel de capa 2 del modelo OSI, consiste en enviar un «paquete mágico» que inicia su trama con la dirección física FF-FF-FF-FF-FF-FF seguida de 16 veces la dirección MAC del equipo.

En primer lugar, Ryuk realiza una scaneo de la tabla ARP del dispositivo, esto para encontrar direcciones IP y MAC que se encuentren relacionadas. En segundo lugar, determina si dichas entradas forman parte de las subredes «10.», «172.16.» y «192.168», si encuentra coincidencia, entonces el «paquete mágico» es enviado. En tercer lugar, si el proceso de encendido remoto es exitoso se intentantán montar los dispositivos compartidos. Para finalizar, se continúa con el proceso de cifrado de archivos.

Esta característica supone un alto riesgo para cualquer organización víctima de este tipo de ataque.

Una de las recomendaciones para reducir el impacto es asegurarse de que esta actividad se realice dentro de la red LAN de la organización, de ser necesario, trabajarlo desde afuera, lo más recomendable es hacer uso de una VPN para realizar todas las operaciones.

5. Conclusiones y trabajo a futuro.

En este capítulo se presentan las conclusiones del trabajo de investigación realizado, las lecciones aprendidas, el cumplimiento de los objetivos planteados, los resultados de la metodología seguida y el posible trabajo a seguir en un futuro desde el punto actual.

5.1 Conclusiones.

El Ransomware es una de las amenzas más peligrosas hoy en día, no solamente para las organizaciones, sino también para usuarios finales, se ha demostrado que desde sus primeras apariciones ha ido evolucionando utilizando técnicas de infección y algorimos de cifrado cada más complejos. Lamentablemente esta evolución se ha dado en mayor medida gracias a que también es una de las actividades más rentables para los ciberdelincuentes y mientras esta realidad no cambie, será difícil detener su evolución como amenza cibernética.

Hoy en día puede encontrarse que este tipo de malware utiliza métodos tradicionales de infección como lo es la suplantanción de identidad, archivos adjuntos malicios y navegación en sitios web comprometidos hasta el uso de Inteligencia Artificial para garantizar la efectivad de una infección. Es por esta razón y de suma importancia la adopción de medidas de prevención, aunque se debe aclarar que el contar con un buen esquema preventivo tampoco es garantía para evitar el éxito de un ataque. Es por ello que también es importante elaborar un plan de reacción frente a este tipo de ameza adecuado al entorno en el que se implemente.

El hecho de contar con una solución de antivirus actualizada tampoco debe brindar esa falsa sensación de estar protegido ante cualquier amenaza, pues como se ha planteado, los grupos criminales evolucionan más rápido en su forma de operar y crear amenzas que los laboratorios de investigación de ciberseguridad de las casa comerciales de antivirus en crear y mejorar soluciones para la seguridad informática.

Ninguna plataforma es inmune a este tipo de ataques, ciertamente Microsoft Windows ha sido una de las más embestidas, pero una tecnología mientras más utilizada es, mayor riesgo posee de recibir todo tipo de incidentes; a la fecha se han realizado vulneraciones contra plataformas Linux, MAC, teléfonos inteligentes, servicios en la nube y dispositivos IoT, siendo éste último el más agravante, puesto que el tema de la ciberseguridad no ha logrado avanzar al mismo ritmo que en otros contexto tecnológicos.

Ciertamente se han realizado importantes avances en materia legal para perseguir y penalizar el ciberdelito a nivel general, dentro de las cuales se encierran las actividades que promueven el uso de Ransomware, sin embargo, hace falta impulsar un esfuerzo mundial para homologar una

legislación que se adapte al marco jurídico de la mayor cantidad de países posibles ya que Internet sobrepasa las fronteras físicas.

5.2 Cumplimiento de objetivos planteados.

El objetivo general del trabajo planteado es: exponer la evolución y diferentes medios de propagación del malware ransomware que permita definir estrategias para prevenir y mitigar las consecuencias de este tipo de ciberataque. Para cumplir este objetivo, se ha realizado una combinación de investigación descriptiva y explicativa que consiste en la consulta de diferentes fuentes sobre el problema tratado, exponiendo de esta forma las características y evolución de esta amenaza, así como también se ha realizado una propuesta de estrategias de prevención y reacción a este tipo de incidentes.

Adicionalmente, se ha contado con los siguientes objetivos específicos:

1. *Ejemplificar diversas técnicas de propagación de ransomware para secuestro de información*. Se presenta al lector los métodos utilizados para realizar y propagar de forma exitosa un ataque tipo Ransomware los cuáles van desde los ya conocidos durante años atrás, hasta el uso de técnicas de Ingeniería Social e Inteligencia Artificial.
2. *Enumerar recomendaciones que contribuyan a la prevención de un ataque exitoso*. Se ha propuesto una estructura de prevención en capas para reducir el alcance y posibilidad de éxito de un ataque.
3. *Mostrar el modelo de negocio de este tipo de malware*. El surgimiento de RaaS deja en evidencia que lo que inició como una serie de ataques aislados de secuestro de información, hoy en dia se ha convertido en un modelo de negocio rentable con características similares a las de los servicios legítimos.
4. *Identificar las consecuencias legales de este tipo de ataque*. Se han presentado al lector tres escenarios que ejemplifican los esfuerzos en materia judicial para la persecución y castigo de ciberdelitos.
5. *Presentar un caso notable de una campaña de ransomware*. Se ha presentado el caso de la campaña del ransomware Ryuk, su efectividad gracias a la combinación con otros tipos de malware y su evolución.

5.3 Sobre la planitifación y metodología seguida.

Ciertamente el combinar una metodología de investigación descriptiva y explicativa ha permitido realizar la consulta de diferentes fuentes de información, recursos mulimedia incluídos, sobre ciberseguridad; cumpliendo de esta forma con los objetivos planteados al inicio de la investigación. Posiblemente una oportunidad de mejora al trabajo realizado en el presente TFM sea la elaboración de un laboratorio experimental para realizar un análisis más profundo a nivel técnico sobre

el comportamiento y recuperación de un ataque Ransomware, lo cual también se encuentra documentado en otras investigaciones de esta clase (consúltese la sección Estado del Arte).

5.4 Trabajo a futuro.

A continuación se presentan algunas líneas de trabajo que no se han logrado explorar en el presente TFM pero que se pueden desarrollar desde el punto actual:

1. Realizar un análisis técnico detallado del código fuente de un Ransomware reciente.
2. Elborar una guía de capacitación para realizar conciencia en los empleados de una organización en la prevención de Ransomware.
3. Desarrollar una formación para profesionales de TI que fortalezcan sus habilidadtes de prevención y reacción frente a esta clase de amenaza.
4. Realizar un seguimiento a la evolución de las técnicas de infección y funciones de futuras amenzas tipo Ransomware.

6. Glosario

1. **Algoritmo:** secuencia de pasos lógicos para resolver un problema o realizar una actividad específica, es la base sobre el que se desarrolla cualquier tipo de software.
2. **Almacenamiento en la nube:** también conocido como «cloud storage» es un servicio para almacenar información en una red de servidores soportado por algún proveedor de tecnología, al que tiene acceso comunmente por Internet desde diferentes lugares.
3. **Android:** sistema operativo móvil propiedad de Google presente en la gran mayoría teléfonos inteligentes y tablets.
4. **App:** aplicación que se instala sobre un sistema operativo para extender las funciones que éste ofrece al usuario.
5. **Backdoor:** conocido también como «puerta trasera» y forma parte del código fuente de un software para saltarse las medidas de seguridad que implementa el algoritmo con el que ha sido desarrollado.
6. **Bitcoin:** solución informática utilizada como crytomoneda, utilizada como alternativa para realizar pagos en efectivo y/o tarjetas de crédito por la prestación de servicios.
7. **Cibercriminal:** persona que explota vulnerabilidades en redes informáticas, sistemas opertivos y demás aplicaciones para cometer acciones ilegales.
8. **Ciberdelicuente:** sinónimo de Cibercriminal.
9. **Ciberdelito:** acción que realiza un Cibercrimina para obtener un beneficio particular.
10. **Ciberseguridad:** es la rama de las Tecnologías de Información y las Comunicaciones que se encarga de la protección de los datos frente a ciberdelitos.
11. **Criptomoneda:** conocida también como Criptodivisa o Criptoactivo, es un recurso electrónico para realizar pagos por la prestación de servicios.
12. **Deep Web:** denominada también como Internet Profunda, Internet Invisible o Internet Oculta; básicamente es la parte de Internet que no indexa en las búsquedas que realizan navegadores tradicionales como Google Chrome, Microsoft Edge, Mozilla Firefox, entre otros. Para tener acceso a ella se utilizan herramientas especiales como el navegador Tor.
13. **Desktop:** computadora de escritorio designada como herramienta de trabajo para usuario final.
14. **Dirección IP:** es un identificador lógico y jerárquico que se asigna a una interfaz de red.
15. **Dirección MAC:** es un identificador único y físico que se asigna a una interfaz de red.
16. **DMZ:** llamada también como «zona desmilitarizada», es una red local ubicada entre una red externa, por lo general Internet, y la red interna de una organización. Dentro de una DMZ se colocan todos los recursos tecnológicos que proveen servicios accesibles desde la red externa.

17. **Dropper:** es un software malicios que se utiliza para inyectar otro tipo de malware en el sistema infectado por el primero.
18. **Exploit Kits:** conjunto de herramientas (código fuente, secuencias de comandos o software) para explotar vulnerabilidades no reconodicas o que no han sido parchadas en un sistema informático.
19. **Hacker:** es un profesional de la informática con conocimientos técnicos especializados en las áreas de desarrollo de software, redes, etc. capaz de encontrar vulnerabilidades en sistemas o redes de computadoras. Es de aclarar que un hacker no es un ciberdelincuente.
20. **IOS:** sistema operativo móvil propiedad de Apple desarrollados para su gama de dispositivos.
21. **Itunes:** servicio de contenido multimedia proporcionado por Apple para su gama de dispostivos.
22. **Linux:** es un término corto para referenciar al sistema operativo libre más utilizado en el mercado conocido como GNU/Linux, correctamente Linux es el Kernel o Código Fuente del sistema operativo ya mencionado.
23. **Master Boot Record (MBR):** es el registro de arranque principal o registro maestro en el primer sector de un dispositivo de almacenamiento basado en particiones lógicas; almacena la información de dichas particiones y se encarga de iniciar el Sistema Operativo instalado.
24. **MongoDB:** gestor de base de datos NoSQL utilizado en gran parte de servicios que se ofrecen en una red de computadoras.
25. **Office 365:** es una presentación del paquete de oficina Microsoft Office en modaliad de arrendamiento renovable por lo general de forma anual.
26. **Pop-up:** es una ventana emergente que se muestra en un navegador web mientras se navega por Internet, generalmente utilizada para mostrar publicidad.
27. **RaaS:** es un modelo de negocio ilegal utilizado por personas sin conocimientos técnicos especializados para que puedan adquirir y lanzar ataques de Ransomware. Esto modelo adopta muchas características del SaaS que sí es un esquema legal.
28. **SaaS:** es un servicio por medio del cual se pone a disposición del usuario el software que éste requiere, se encuentra soportado sobre la nube (red de computadoras) del proveedor y la forma de hacer uso de este servicio es por medio de Internet.
29. **Safari:** es un navegador web desarrollado por Apple especialmente para ser utilizado en sus dispositivos, aunque también existe una versión para Windows.
30. **Sistema Operativo:** es el software principal instalado en un dispositivo encargado de gestionar todos los recursos de hardware y software del mismo.
31. **Smart House:** es un hogar cuya gestión de electrodomésticos, iluminación, audio, vídeo y otras características se pueden contrarlar prácticamente desde un teléfono inteligente, el objetivo de todo esto es la comodidad de los habitantes del hogar.

32. **SMS:** es un servicio para telefonía móvil para el envío de mensajes cortos utilizando la red telefónica a la que se encuentra conectado el dispositivo.
33. **Tabla ARP:** es un registro que posee cada terminal conectado a una red informáctica y se utilza para relacionar las direcciones IP’s con direcciones MAC’s conocidas.
34. **Tabla maestra de archivos (MFT):** es un registro que almacena información sobre todos los archivos acerca de los archivos que se encuentran almacenados en un disco duro,
35. **Vector de ataque:** es un método que utiliza un ciberdelincuente para realizar un ataque a un sistema informático.
36. **VPN:** es una red privada virtual que permite que la extensión de una red local, perteneciente a una organización, a través de una red pública, por lo general Internet.
37. **Wake-on-Lan:** es un protocolo utilizado en el campo de redes informáticas para encender un equipo de forma remota.
38. **Windows:** es el sistema operativo comercial perteneciente a Microsoft con mayor difusión en el mercado.

7. Bibliografía

Mohanta, A., Hahad, M. and Velmurugan, K., Preventing Ransomware, Packt Publishing Ltd, Birmingham, 2018

Significado de Ransomware.
https://www.significados.com/ransomware
Fecha de consulta: 06/03/2020

El ransomware Ransoc que bloquea el escritorio saquea archivos locales y perfiles de redes sociales.
https://www.proofpoint.com/es/threat-insight/post/ransoc-desktop-locking-ransomware-ransacks-local-files-social-media-profiles
Fecha de consulta: 24/03/2020

Conocer los tipos de Ransomware más habituales.
https://www.infotecnika.com/common-types-of-ransomware/
Fecha de consulta: 24/03/2020

New hacker groups join the MongoDB Apocalypse, ask for a ransom in exchange for the data.
https://cyware.com/news/new-hacker-groups-join-the-mongodb-apocalypse-ask-for-a-ransom-in-exchange-for-the-data-c837aa67
Fecha de consulta: 25/03/2020

Remove Erebus ransomware / virus (Removal Instructions) - Mar 2020 update.
https://www.2-spyware.com/remove-erebus-ransomware-virus.html
Fecha de consulta: 25/03/2020

Nayana cede ante el ransomware y paga un millón de dólares de “rescate”.
http://www.zonavirus.com/noticias/2017/nayana-cede-ante-el-ransomware-y-paga-un-millon-de-dolares-de-rescate.asp
Fecha de consulta: 25/03/2020

Alerta ante multivirus ‘Rex Linux’: ransomware, ataques DDoS y minería bitcoin.
https://www.criptonoticias.com/seguridad-bitcoin/alerta-multivirus-rex-linux-ransomware-ataques-ddos-mineria-bitcoin/
Fecha de consulta: 25/03/2020

KillDisk, un falso ransomware, empieza a golpear con fuerza
https://www.redeszone.net/2018/01/16/killdisk-falso-ransomware-empieza-golpear-fuerza/
Fecha de consulta: 25/03/2020

Fairware ransomware Ataques servidores Linux.

https://sensorstechforum.com/es/fairware-ransomware-attacks-linux-servers/
Fecha de consulta: 25/03/2020

KimcilWare, un nuevo ransomware enfocado a secuestrar tiendas online.
https://www.redeszone.net/2016/03/30/kimcilware-nuevo-ransomware-enfocado-secuestrar-tiendas-online/
Fecha de consulta: 25/03/2020

Un nuevo ransomware como WannaCry vuelve a atacar de forma global.
https://www.pandasecurity.com/spain/mediacenter/malware/petya-ataque-ransomware/
Fecha de consulta: 25/03/2020

Satana: ransomware que cifra archivos y MBR
https://www.ccn-cert.cni.es/en/gestion-de-incidentes/lucia/23-noticias/3939-satana-ransomware-que-cifra-archivos-y-mbr.html
Fecha de consulta: 25/03/2020

Sodin, el ransomware que se aprovecha de los MSP
https://unaaldia.hispasec.com/2019/08/sodin-el-ransomware-que-se-aprovecha-de-los-msp.html
Fecha de consulta: 26/03/2020

Oracle Security Alert Advisory - CVE-2019-2725
https://www.oracle.com/security-alerts/alert-cve-2019-2725.html
Fecha de consulta: 26/03/2020

Informe RansomCloud O365
https://www.elevenpaths.com/es/nuevo-whitepaper-ransomcloud-o365/index.html
Fecha de consulta: 26/03/2020

Los usuarios de Apple, víctimas de malware de ransomware
https://www.kaspersky.es/blog/ransomware-afecta-ios-osx/3534/
Fecha de consulta: 27/03/2020

'Ransomware' en tu iPhone, o por qué debes actualizar ahora a la última versión de iOS
https://www.elconfidencial.com/tecnologia/2017-03-28/ransomware-iphone-ios-seguridad-pornografia-movil_1356766/
Fecha de consulta: 27/03/2020

DoubleLocker
https://malware.wikia.org/wiki/DoubleLocker
Fecha de consulta: 27/03/2020

Nuevo ciberataque: llega por SMS y secuestra archivos del celular
https://www.infobae.com/america/tecno/2019/08/02/nuevo-ciberataque-llega-por-sms-y-secuestra-archivos-del-celular/

Fecha de consulta: 27/03/2020

APP de seguimiento del Covid-19 instala ransomware en su Smartphone; tenga cuidado.
https://noticiasseguridad.com/malware-virus/app-de-seguimiento-del-covid-19-instala-ransomware-en-su-smartphone-tenga-cuidado/
Fecha de consulta: 27/03/2020

Ransomware and the Internet of Things.
https://www.cyberdefensemagazine.com/ransomware-and-the-internet-of-things/
Fecha de consulta: 28/03/2020

Ransomware: 10 formas en las que puede comportarse al infectar un sistema.
https://www.welivesecurity.com/la-es/2018/05/29/formas-ransomware-puede-comportar-al-infectar-sistema/
Fecha de consulta: 28/03/2020

¿Qué es el ransomware?
http://www.consisa.com/index.php/es/que-es-el-ransomware/
Fecha de consulta: 01/04/2020

Explot Kits
https://www.cyber.nj.gov/threat-profiles/exploit-kits
Fecha de consulta: 01/04/2020

Ransomware como servicio: comercialización de ransomware
https://www.linkedin.com/pulse/ransomware-como-servicio-comercializaci%C3%B3n-de-andrew-sanaev/
Fecha de consulta: 06/04/2020

Ransomware as a Service (RaaS) – A Contemporary Mal du siècle?
https://heimdalsecurity.com/blog/ransomware-as-a-service/
Fecha de consulta: 06/04/2020

Elementos básicos de la seguridad perimetral
https://www.monografias.com/trabajos106/elementos-basicos-seguridad-perimetral/elementos-basicos-seguridad-perimetral.shtml
Fecha de consulta: 07/04/2020

Seguridad en la Red interna
https://guardnet.wordpress.com/2011/06/09/seguridad-en-la-red-interna/
Fecha de consulta: 07/04/2020

Identifica el ransomware y si es posible recuperar tus datos www.informaticovitoria.com
https://www.youtube.com/watch?v=gF5lIn84am8
Fecha de consulta: 07/04/2020

¿Cómo recuperar archivos encriptados por Ransomware?
https://velorciosgroup.com/recuperar-archivos-encriptados-por-ransomware/
Fecha de consulta: 07/04/2020

FIRMA INVITADA. El futuro del 'ransomware': la puerta de tu casa cerrada por un virus
https://retina.elpais.com/retina/2019/10/14/tendencias/1571030270_022377.html
Fecha de consulta: 07/04/2020

Los Delitos Cibernéticos en El Salvador
https://garciabodan.com/los-delitos-ciberneticos-en-el-salvador/
Fecha de consulta: 08/04/2020

Análisis de Ley de Delitos Informáticos y conexos de El Salvador
https://es.slideshare.net/ulselsalvador/anlisis-de-ley-de-delitos-informticos-de-el-salvador
Fecha de consulta: 08/04/2020

La nueva ley de Seguridad Cibernética de la Unión Europea
https://www.viafirma.com/blog-xnoccio/es/ley-seguridad-cibernetica-union-europea/
Fecha de consulta: 08/04/2020

Ciberseguridad en Europa: normas más estrictas y mejor protección
https://www.consilium.europa.eu/es/policies/cybersecurity/
Fecha de consulta: 08/04/2020

El antivirus no te protege del ransomware
https://www.redeszone.net/noticias/seguridad/problemas-seguridad-antivirus-ransomware/
Fecha de consulta: 08/04/2020

Ryuk Ransomware
https://www.youtube.com/watch?v=CRCL9zma_ac
Fecha de consulta: 18/04/2020

2019. *Advisory: Ryuk Ransomware Targeting Organisations Globally*. National Cyber Security Centre.

Curso virtual: Ransomware | Prevención y respuesta a incidentes.
URL: https://www.udemy.com/course/ransomware-prevencion-y-respuesta-a-incidentes/

8. Anexos

Anexo I: Diagrama de Gantt.