Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Criptografía maliciosa: Ransomware

Autor: Ing. Matías Ezequiel Sena

Tutor de Trabajo Final: Dr. Pedro Hecht

Año de presentación: 2018

Cohorte: 2017

DECLARACIÓN JURADA

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Nombres y Apellidos: Matías Ezequiel Sena

Número de documento: 36.729.304

RESUMEN

El presente trabajo final de la Especialización en Seguridad Informática realiza un estudio crítico de información respecto del ransomware criptográfico. Si bien la criptografía es una herramienta poderosa empleada por individuos particulares y organizaciones, también puede usarse indebidamente con fines maliciosos. El ransomware criptográfico es una categoría de software malicioso que cifra los archivos de una computadora y solicita el pago de un rescate para recuperarlos.

La investigación realizada involucra la recopilación y análisis de información referente a: los antecedentes del uso de criptografía malintencionada; cómo ha surgido el nacimiento de ransomware; los tipos y familias más importantes que se han desarrollado desde sus comienzos hasta la actualidad, considerando algoritmos de cifrado, forma de pago de rescate y plataformas afectadas; los vectores de ataque utilizados por estos cibercriminales y las estrategias que se pueden adoptar para defenderse del ransomware, considerando aquellas que son proactivas y reactivas.

Palabras clave

Ransomware, Criptografía, Malware, Software malicioso.

TABLA DE CONTENIDOS

INTRODUCCIÓN

Uno de los principales riesgos y preocupaciones latentes en la actualidad referidos a la seguridad informática es el software malicioso. Con el objetivo de dañar ordenadores, se han desarrollado diversos tipos de *malware* tales como virus, troyanos y gusanos. Si bien estos tipos y otros han sido definidos en el pasado, actualmente hay individuos y organizaciones dedicadas a crear nuevas variantes de estos malware aprovechando nuevas fallas en el software de las aplicaciones y/o sistemas operativos para obtener rédito. Es por ello por lo que es necesario mantenerse a la vanguardia de los softwares malintencionados lanzados e identificar estrategias para proteger los ordenadores y, en particular, la información valiosa que contienen.

Ransomware ha sido uno de los softwares maliciosos que ha cobrado relevancia en los últimos años. A diferencia del resto, si bien daña los ordenadores de las víctimas, el objetivo principal es obtener dinero luego de la infección. Para lograr esto, utiliza criptografía para cifrar archivos y deja a la víctima en una situación de que, si quiere recuperar el acceso a su información, necesita pagar un rescate. La criptografía ha sido pensada y utilizada para fines defensivos, el cifrado de archivos permite garantizar la confidencialidad de estos. Ya sea con algoritmos de criptografía simétrica o asimétrica, aquel individuo que no posea la clave para desencriptar no podrá ver la información. No obstante, en este caso es empleada para fines ofensivos ya que, gracias a los métodos criptográficos, puede extorsionar a sus víctimas.

Ante esta problemática, este trabajo de investigación tiene por objetivo desarrollar y exponer el nacimiento del ransomware criptográfico, su evolución, cifrado e impacto en la seguridad ofensiva y defensiva, a fin de comprender el objeto de estudio. En este trabajo no se publica nada que no se haya descubierto antes. El principal aporte de este es recopilar historias y detalles técnicos de una bibliografía variada para tener una visión y comprensión integral de una de las principales amenazas informáticas que existen hoy. Se espera que sirva como una primera lectura para que futuras investigaciones profundicen en alguno de los puntos tratados.

Este documento se encuentra estructurado en cinco capítulos. En el primero, se trata de los antecedentes del uso de criptografía para fines maliciosos, haciendo un breve recorrido de una rama dedicada a su investigación hasta el nacimiento de ransomware. Luego, el segundo capítulo describe los vectores de ataque que son utilizados por el ransomware para llegar e infectar los ordenadores de las víctimas. Las familias de ransomware más destacadas que han sido desarrolladas en la historia hasta el 2018 son detalladas en el tercer capítulo, considerando los algoritmos de encripción utilizados y las nuevas tecnologías que han ido incorporando las nuevas variantes. En los capítulos cuatro y cinco, se exponen estrategias y herramientas de defensa que se pueden adoptar para evitar (preventivas) o recuperarse (reactivas) de un ataque de ransomware, tanto aquellas que pueden ser implementadas en una organización entera como las que pueden ser instauradas en un ordenador individual. Finalmente, se establecen las conclusiones obtenidas a lo largo del desarrollo de este trabajo.

CAPÍTULO 1. Antecedentes de criptografía maliciosa

A lo largo de la historia, la criptografía ha ido evolucionando y variando, incluyendo diversos avances tecnológicos, nuevos algoritmos desarrollados e implementados y diferentes aplicaciones y rubros en la cual se ha identificado que la criptografía puede aportar su utilidad y potencial. En esta sección no se desarrolla la criptografía tradicionalmente conocida, sino que se hace foco en el nacimiento de la aplicación de la criptografía para fines dañinos o maliciosos.

1.1. Criptovirología

Desde sus comienzos, la criptografía ha sido pensada y utilizada como un mecanismo de defensa, en el cual los usuarios pueden gozar de aspectos como autenticidad, privacidad y seguridad. Actualmente, es posible detectar que estas funcionalidades de la criptografía, tanto simétrica como asimétrica, aún siguen siendo de gran utilidad en los sistemas informáticos. Si se requiere encriptar los archivos de todo el disco de un ordenador, la primera solución que se puede optar es el uso de un algoritmo de criptografía simétrica como AES (*Advanced Encryption Standard*). Por otro lado, si se necesita enviar un archivo mediante correo electrónico a otra persona sin que nadie en la red pueda interceptar y tener acceso a ese archivo, una solución posible es implementando un algoritmo de criptografía asimétrica como RSA (Rivest–Shamir–Adleman).

Sin embargo, durante todos estos años de existencia de la criptografía, se han encontrado otras aplicaciones que no necesariamente buscan defender el sistema informático. Se ha desarrollado una rama en la informática que tiene el objetivo de estudiar el uso de criptografía para crear software malicioso, la cual es conocida como criptovirología.

Los ataques estudiados por la criptovirología involucran la utilización en conjunto de técnicas de criptografía y malware conocidos tales como virus y troyanos. De esta manera, la criptografía es mucho más vista como una herramienta adicional para los desarrolladores de malware para mejorar las capacidades de sus desarrollos, antes que un malware en sí misma.

Entre los objetivos ofensivos para los que la criptografía “maliciosa” es útil, se encuentran: el control de acceso sobre los datos del ordenador infectado; extorsión; fuga de información; robo de información sensible y ocultamiento de claves y estructura del malware [1]. Muchas de estas ideas que se fueron extendiendo a lo largo de las investigaciones de la criptovirología sirvieron de base para el origen de ransomware.

1.2. Nacimiento del Ransomware

Del inglés *ransom* que significa rescate y “ware” que hace referencia a software, el ransomware es un software malicioso que infecta un ordenador, restringe el acceso a los archivos afectados y pide un rescate al usuario para quitar la restricción. El ransomware se nutre de las funcionalidades y beneficios que brinda la criptografía, no con fines de defensa sino con fines ofensivos, más precisamente de extorsión. Además del ransomware criptográfico (o *crypto-ransomware*), el cual es el foco de esta tesis, existe el *locker ransomware* que no utiliza criptografía debido a que no encripta archivos, sino que sólo bloquea el acceso a los datos o archivos del ordenador infectado hasta que se pague el rescate.

Se considera que el primer malware de este tipo fue lanzado en 1989, sin necesidad de la masividad que hoy tiene Internet para ser expandido, el cual será tratado en una sección posterior. Sin embargo, la explosión de ransomware comenzó a partir del año 2005 con Gpcode, que también será tratado.

A comparación de otros malwares, el ransomware tiene un objetivo claro y conciso: infectar para obtener dinero a cambio. La víctima del ransomware, que puede ser un usuario aislado o una organización entera, sufre daños económicos y financieros tras ocurrir una infección. No solo es afectado por el pago que tiene que realizar para recuperar su información encriptada, sino que también puede tener otras consecuencias negativas colaterales tales como el tiempo de baja de servicio o la pérdida de reputación. En 2017, el ransomware costó a las empresas un total de 5 billones de dólares considerando el ataque en su completitud, no sólo el

precio del rescate. Esto marcó un pico en el impacto causado por un ransomware en la historia, más aún si lo comparamos con los años 2016 (costos alrededor de 1 billón de dólares) y 2015 (costos alrededor de 325 millones de dólares) [2]. Durante el transcurso de estos años, la estrategia de los desarrolladores de ransomware también ha cambiado en cuanto a los precios de los rescates. En 2016, con el objetivo de extraer más rédito de las víctimas, se empezaron a utilizar estrategias como el aumento del precio del rescate a medida del paso del tiempo, buscando adicionalmente presionar para que se efectúe la transacción. El año siguiente, las demandas de rescate disminuyeron abruptamente (más de la mitad), lo cual demuestra que se ha buscado pedir menos dinero, pero abarcar y afectar a muchos más usuarios [3]. Estos valores son resumidos y expuestos en la siguiente tabla:

Impacto	2015	2016	2017
Costo total para las empresas (en dólares)	325 millones	1 billón	5 billones
Precio de rescate (en dólares)	293	1077	522

Tabla 1: Resumen de costos financieros debido a ataques de ransomware

Con respecto a su evolución hasta la actualidad, el ransomware ha experimentado variaciones respecto a su forma de expandirse, algoritmos de encripción utilizados, estructuras, entre otras características. Sin embargo, hay dos acontecimientos que han influenciado notablemente el curso que han tomado las familias de ransomware y que siguen presentes en las variantes que se lanzan actualmente.

1.2.1. Internet profunda

Del inglés *deep web*, la llamada internet profunda, oculta o invisible es el contenido de la *World Wide Web* que no está indexada por los motores de búsqueda estándar como Google o Yahoo. Es una parte de internet que se distingue por el anonimato, formado por conexiones *peer-to-peer* que permiten a los usuarios compartir archivos directamente. Si bien pueden

llevarse a cabo las mismas tareas que en la web tradicional, es un lugar propicio para llevar a cabo actividades ilegales y criminales. Es aquí donde aparece la conexión entre el ransomware y la deep web, aprovechando el beneficio del anonimato.

El proyecto TOR (The Onion Router) permite a los usuarios no sólo navegar la internet profunda de manera anónima, sino también crear servicios ocultos como servidores SSH o páginas web [4]. Aunque existen otras redes ocultas en la deep web, TOR es una de las tres más grandes y es la más utilizada por los desarrolladores de ransomware. De esta manera, utilizando sitios alojados en TOR, se ha solucionado el problema del cobro del rescate de las víctimas. Los desarrolladores han aprovechado la internet profunda para crear sus sitios de pagos, sin necesidad de informar a las víctimas una cuenta en particular (algunos se han visto obligados a utilizar los servicios de e-Gold o Liberty Reserve cuando esta alternativa no existía) que permiten que sea posible el rastreo y la determinación de quién es el responsable del ransomware.

1.2.2. Criptomoneda

Del inglés *cryptocurrency*, una criptomoneda es un medio digital descentralizado de intercambio que confirma transacciones financieras mediante pruebas criptográficas. A diferencia de otras monedas, ofrece tres características que la hacen atractiva: protección contra ataques de doble gasto (transacciones que buscan gastar el mismo dinero dos veces); independencia de la autoridad central y anonimato limitado por la cantidad total de unidades que tiene la criptomoneda en cuestión. Particularmente esta última característica probablemente ha sido la causante de que desarrolladores de ransomware hayan optado por utilizar cuentas de criptomonedas para recibir el pago de los rescates de sus víctimas, sin necesidad de revelar información sobre ellos. El anonimato también está garantizado en la creación de una cuenta y una misma persona puede tener muchas, ya que es recomendado que una cuenta sea utilizada sólo para una transacción. Estas cuentas consisten en una combinación de una clave privada y una dirección de la cuenta misma, y no hay manera de identificar al dueño de ella a partir de los datos de la cuenta [5].

Se han generado distintas criptomonedas con alguna variación en su estructura o comportamiento, pero siguiendo los lineamientos antes mencionados. Sin embargo, la más elegida empleada por ransomware es **Bitcoin** [6], una de las más utilizada a nivel mundial y la primera en haber empezado a operar. El uso en conjunto de sitios web alojados en la deep web vía TOR y cuentas de criptomonedas ha sido la combinación perfecta para los creadores de ransomware para cobrar los rescates sin que se conozca su identidad. En una sección posterior se tratarán familias de ransomware que utilizaban otros medios de pagos antes de que existiera Bitcoin, familias que hacen uso de Bitcoin y una familia en particular que optó por otra criptomoneda llamada **Dash** [7].

CAPÍTULO 2. Vectores de ataque

Existen diferentes maneras en que el atacante puede lograr que el ransomware infecte a los usuarios [8]. Los métodos predominantes y más utilizados para distribuir este tipo de software malicioso serán explicados en esta sección.

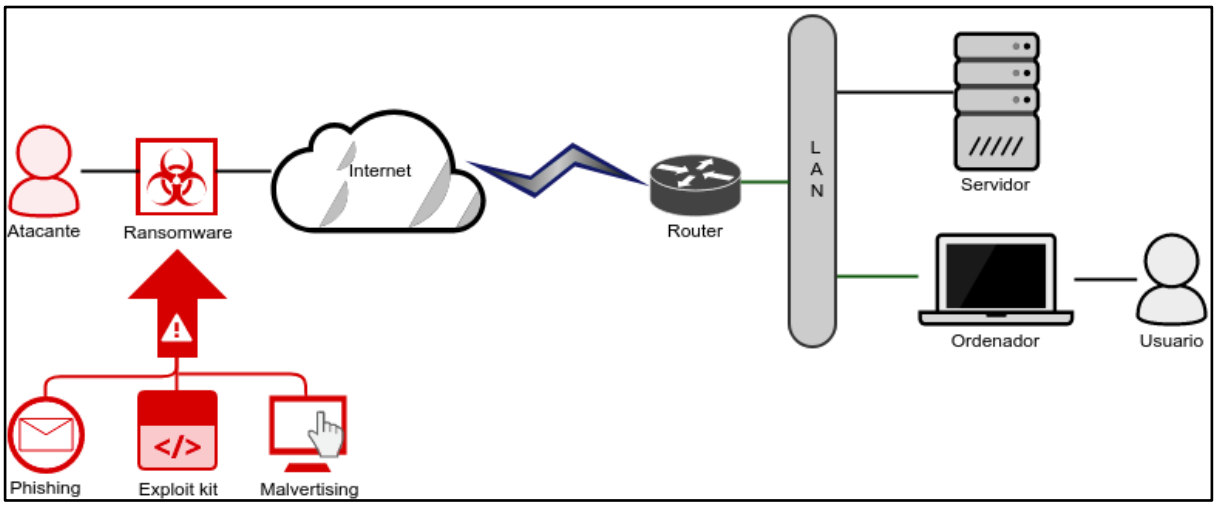


Imagen 1: Vectores de ataque

2.1. Phishing

Mediante *phishing* (o suplantación de identidad), el atacante envía un correo electrónico de aspecto inocente con el objetivo de esconder el software malicioso, incluido como archivo adjunto o en un sitio cuyo enlace está presente en el mensaje. La infección puede ocurrir si el usuario: abre el archivo adjunto malicioso que instala el ransomware; abre el adjunto malicioso que inicia una descarga y luego instala el ransomware o ingresa al enlace del mensaje que apunta al ransomware.

2.2. Exploit kit

El atacante utiliza herramientas que aprovechan las vulnerabilidades de seguridad que se encuentran sin arreglar en una aplicación o sistema operativo para instalar malware. La infección puede ocurrir meramente debido a la presencia de una vulnerabilidad, no requiere acción alguna de los usuarios. Este método es aún más efectivo si las vulnerabilidades que

son explotadas son de “día cero” (*zero-day*), debido a que cualquier ordenador que posea el software en cuestión será vulnerable y permeable.

2.3. Malvertising

Utilizando *malvertising* (o publicidad maliciosa), el atacante coloca anuncios maliciosos a través de sitios web de confianza con gran cantidad de visitantes. La infección puede ocurrir si el usuario: hace clic en el anuncio malicioso provocando la descarga del ransomware o simplemente accede y carga la página web que aloja el anuncio, sin necesidad de interactuar.

CAPÍTULO 3. Familias ransomware

En esta sección se presentan en detalle ransomwares que han sido importantes debido a sus características y/o funcionalidades que incluyeron y que se destacan entre tantos otros que se lanzaron en la historia desde 1989. Para cada año en que se ha lanzado un ransomware, se ha seleccionado el más relevante y el que más ha aportado en la evolución de un malware que aún sigue latente y con el que ciberdelincuentes siguen sacando provecho y dinero con su desarrollo. Debido a que la esencia del ransomware es la misma desde sus comienzos, en cada subsección se ahondará en las características que más los diferencian del resto o de sus antecesores. Algunos ransomwares repiten lo implementado por otros y en términos de esta sección, aquellas características ya explicadas en su antecesor no serán repetidos. Adicionalmente, con respecto al ransomware más exponente de la historia que fue lanzado en 2017, se aportan más detalles en cuanto al análisis dinámico que se ha realizado de su comportamiento al momento de una infección. También cabe aclarar que en esta sección y en la completitud de esta tesis se ha hecho foco en ransomwares criptográficos, aquellos que encriptan los archivos de los ordenadores de las víctimas y no los que no hacen uso de la criptografía como los que sólo bloquean la pantalla.

3.1. 1989 | AIDS Trojan

La primera gran manifestación de ransomware se remonta a 1989, con el AIDS Trojan, también llamado PC Cyborg. Si bien el término ransomware se ha comenzado a utilizar años posteriores, este programa tenía la diferencia de encriptar archivos y pedir un rescate.

3.1.1. Propagación

Debido a que pocas personas utilizaban computadoras personales, que Internet no era como lo conocemos hoy y era útil sólo para expertos de ciencia y tecnología, AIDS Trojan no tuvo tanto éxito, comparado al impacto causado por sus sucesores. Este troyano fue distribuido a través de

disquetes. Joseph Popp, investigador sobre el SIDA y creador del programa, distribuyó 20.000 disquetes a asistentes en una conferencia sobre SIDA.

3.1.2. Modo de operación

Al colocar el disquete, se le proporcionaba al usuario información sobre riesgos de contraer SIDA. Sin embargo, adicionalmente a esto, el troyano encriptaba el disco duro de la víctima después de 90 reinicios. El programa contaba las veces que se inició el sistema y al alcanzar este número de reinicios, ocultaba los directorios y encriptaba los nombres de los archivos de la unidad C. Esto era realizado con criptografía simétrica simple, aunque no se conoce el algoritmo exacto. En la siguiente captura de pantalla, se muestra el mensaje que recibían las víctimas que insertaron el disquete:

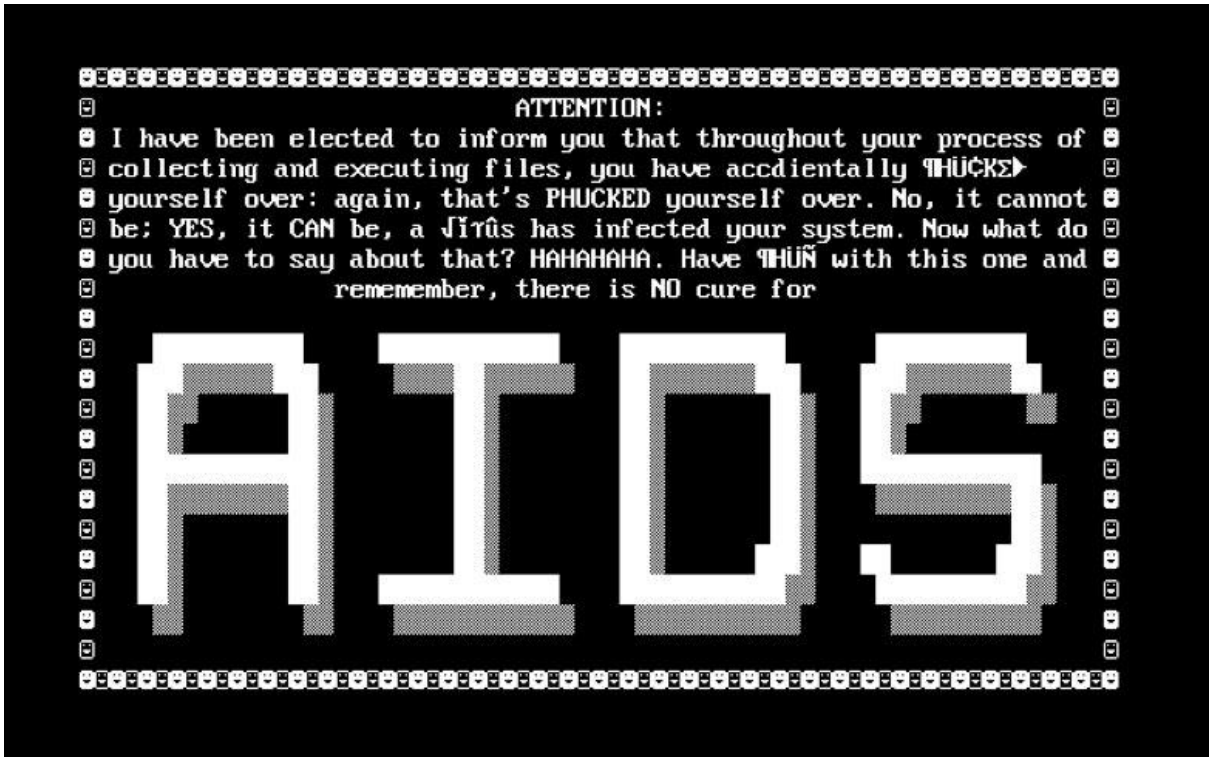


Imagen 2: Mensaje de AIDS Trojan. Fuente: KnowBe4

Al finalizar la encripción y dejar el sistema inutilizable, se le informa a la víctima que debe pagar una "tarifa de licencia" para recibir la clave para descifrar, extrapolable al pago del rescate de los ransomware propiamente dichos.

La simplicidad del algoritmo de encripción, llevó al lanzamiento de programas y/o herramientas de remediación, los cuales desencriptaban los archivos infectados. Estos permitieron que las víctimas que no pagaron la tarifa puedan eliminar el troyano de sus ordenadores y recuperar sus archivos [9].

3.2. 2005 | Gpcoder

El siguiente registro de la existencia de un ransomware, posterior a AIDS Trojan, toma lugar más de una década después con el descubrimiento de Gpcoder. Es un troyano que encripta archivos en sistemas Windows utilizando, en sus primeras variantes, criptografía simétrica.

3.2.1. Propagación

La principal forma de propagación de Gpcoder es mediante phishing o adjuntos en mensajes de correo electrónico. Fue de los primeros ransomware en distribuirse mediante lo llamado *spear-phishing*, que hace referencia a mensajes de correo electrónico dirigidos a una persona o un grupo de personas en particular dentro de una organización, tales como un departamento. Así, las víctimas pueden creer que el mensaje proviene de una fuente confiable.

3.2.2. Modo de operación

Una vez ejecutado, Gpcoder escanea tanto las unidades locales como las remotas en busca de archivos con algunas extensiones en particular. Para garantizar su persistencia, crea una entrada de registro en el sistema para que se ejecute cada vez que Windows inicia.

En sus inicios, este ransomware realizaba la encripción con un algoritmo personalizado de criptografía simétrica, el cual fue fácil de analizar y descifrar. Debido a esto, surgieron nuevas variantes de esta familia de ransomware, dando lugar a Gpcoder con otros algoritmos de encripción simétrica hasta que se llegó a una versión más fuerte usando RSA de 1024

bits y AES de 256 bits. Esta última variante fue el primer ransomware en utilizar criptografía asimétrica, más específicamente el algoritmo RSA [10].

Como consecuencia de la encripción, los archivos se tornan inaccesibles para la víctima. En la siguiente captura de pantalla, se muestra el archivo que el malware deja en el ordenador con las instrucciones para el rescate:

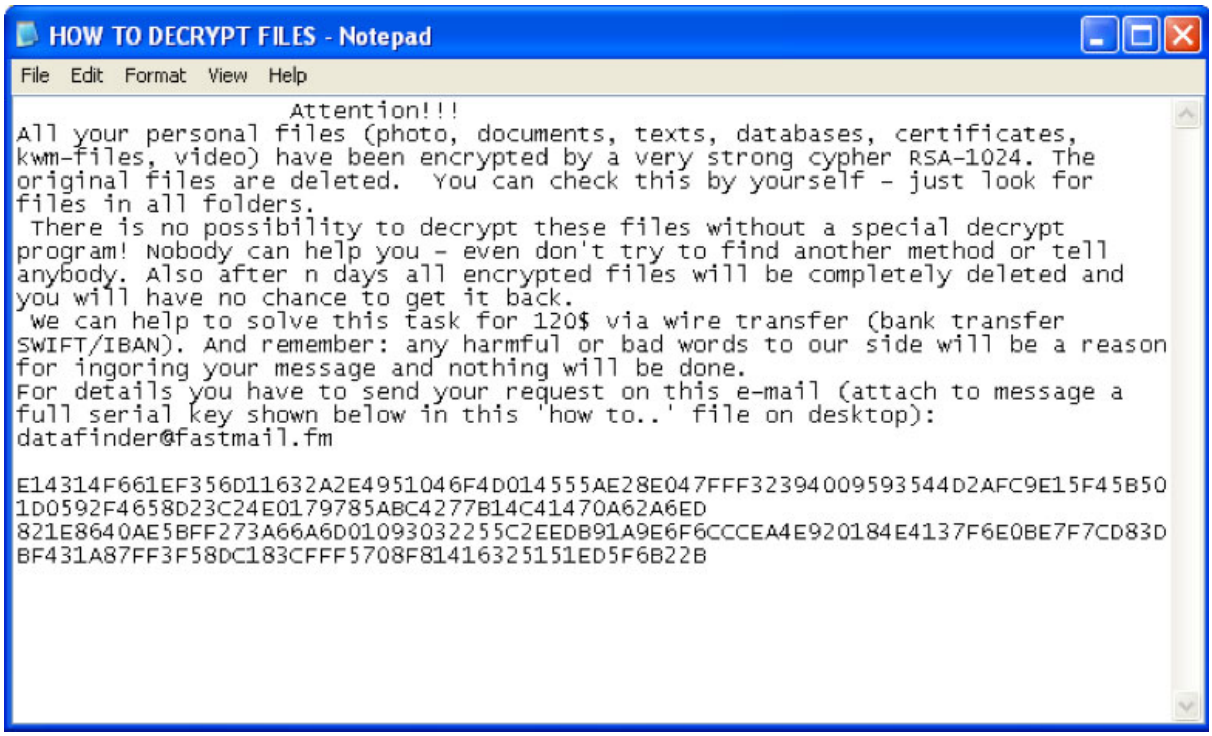


Imagen 3: Instrucciones de Gpcoder para recuperar archivos. Fuente: KnowBe4

Para el pago del rescate, la víctima debía contactarse con los desarrolladores mediante la cuenta de correo electrónico proporcionada en las instrucciones y debía abonar a una cuenta de e-Gold o Liberty Reserve, ambos servicios de moneda digital que han cerrado y no brindan más sus servicios.

Aquellas víctimas de Gpcoder que tenían archivos infectados no tenían otra alternativa que el pago del rescate mediante los mecanismos antes mencionados. No se ha encontrado una solución para el descifrado directo de archivos que funcione correctamente [11].

3.3. 2006 | Archiveus

Un año después, surgió el descubrimiento de Archiveus, un troyano que “protegía” los archivos de la víctima con una contraseña. A diferencia de un ransomware como conocemos hoy, en vez de pagar un rescate, la víctima debía comprar algo en sitios web específicos para recuperar sus archivos.

3.3.1. Propagación

Archiveus utilizaba descargas de archivos gratuitos o adjuntos vía correo electrónico. Adicionalmente, podía ocultarse en sitios webs o archivos particulares.

3.3.2. Modo de operación

Al ser descargado y ejecutado, el troyano escaneaba y encriptaba todos los archivos encontrados en el directorio “Mis documentos” de Windows. Copiaba el contenido de los archivos a un archivo propio creado por el ransomware. Posteriormente, eliminaba los archivos originales y pedía un rescate para restaurarlos. Si bien el ordenador seguía funcionando correctamente, normalmente los usuarios utilizaban este directorio para almacenar sus documentos más necesarios tales como planillas de cálculo. Por lo tanto, las víctimas podían utilizar otras funcionalidades, pero los archivos que más les importaba quedaban inaccesibles [12]. En la siguiente captura de pantalla, se muestra la ventana lanzada por Archiveus cuando el usuario quería acceder a un archivo infectado:

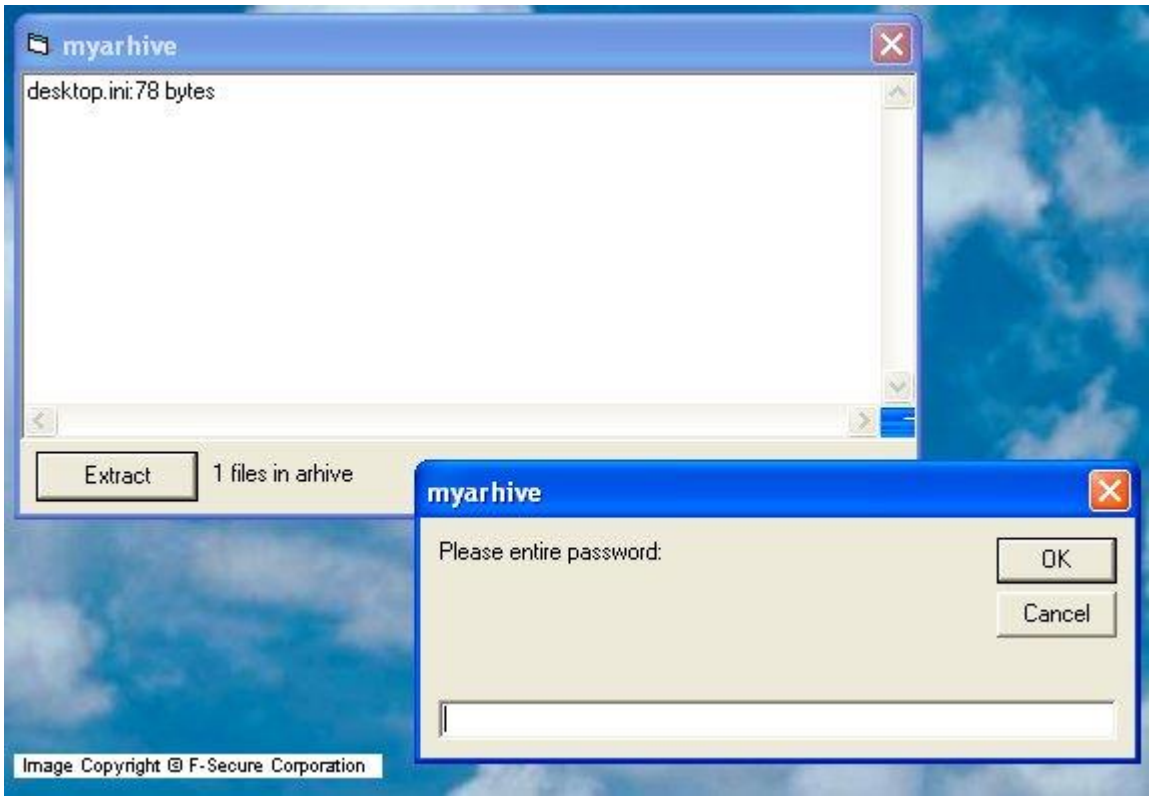


Imagen 4: Mensaje de Archiveus al abrir un archivo infectado. Fuente: F-Secure

Para la encripción, utilizaba RSA de 1024 bits, el cual es un algoritmo seguro. Sin embargo, la contraseña no era única para cada víctima y en esto radica la causa por la que Archiveus ha llegado a su fin. La obtención de la clave de 30 dígitos para desencriptar sólo era posible si la víctima hacía compras a vendedores específicos en Internet.

El análisis en profundidad de este malware llevó a que investigadores descubran que la contraseña para recuperar los archivos estaba contenida en el código de este. Actualmente, esta contraseña es pública para que cualquier víctima afectada tenga la posibilidad de recuperarse de la infección [13].

3.4. 2013 | CryptoLocker

Luego de Archiveus, el siguiente ransomware que se ha destacado fue recién en 2013 con CryptoLocker, el cual encriptaba archivos en ordenadores Windows. Causando un fuerte impacto afectando a un gran número de víctimas alrededor del mundo, este malware ha sido el primero

en utilizar dos estrategias que han sido adoptadas por la mayoría de sus sucesores.

Por un lado, un hecho importante fue la creación de la criptomoneda y sistema de pago Bitcoin en 2009. Esto abrió una puerta para que desarrolladores de ransomware tengan a disposición un método anónimo de extorsión para recibir el pago de los rescates. Así, ya no es necesario exponerse con cuentas de e-Gold o Liberty Reserve como requerían en 2005 si querían exigir un pago, ahora con TOR y Bitcoin esto es un problema solucionado.

La segunda estrategia es la combinación de algoritmos de encripción para el cifrado. No basta con elegir criptografía simétrica o asimétrica. A partir de este año, los desarrolladores de este tipo de malware entendieron que, para tener un mecanismo robusto, era más beneficioso combinar algoritmos de encripción simétrica para encriptar archivos y asimétrica para la comunicación con el servidor.

3.4.1. Propagación

Para propagarse y llegar a más usuarios, CryptoLocker se escondía en archivos adjuntos en correo electrónico o a través de descargas de sitios web afectados a través de una *botnet* llamada GameOver ZeuS, la cual robaba credenciales bancarias y distribuía este ransomware [14]. Esta botnet no sólo permitía infectar muchos usuarios, sino también operaba como servidor C&C (*Command-and-Control*) para CryptoLocker, lo cual en principio era útil para su operación, pero posteriormente, fue una de las causas de la caída de este importante ransomware.

3.4.2. Modo de operación

Al ejecutarse CryptoLocker, buscaba conectarse con el servidor C&C que tiene asignado para obtener la clave pública RSA de 2048 bits con la cual iba a encriptar. Luego, escaneaba los discos locales y unidades de redes en busca archivos con ciertas extensiones en particular, las cuales fueron ampliadas en nuevas variantes de CryptoLocker para afectar aún más el ordenador de la víctima. Cada archivo era encriptado con una clave única AES de 256 bits, dejándolo asentado en el registro de Windows.

Finalizado el proceso de encripción, el ransomware muestra un mensaje con el aviso a la víctima. En la siguiente imagen, se muestra las instrucciones brindadas por CryptoLocker para que las víctimas paguen el rescate para recuperar sus archivos:

Imagen 5: Instrucciones de CryptoLocker para el pago de rescate. Fuente: Avast

El mecanismo de encripción utilizado por este malware es seguro, ya que resulta prácticamente imposible obtener la clave privada RSA que sirve para obtener las claves simétricas. Sin embargo, han ocurrido dos hechos que debilitaron a CryptoLocker y que lo han llevado a su desuso. En primer lugar, la dependencia mencionada anteriormente que tenía el malware con la botnet terminó causando daños catastróficos al funcionamiento de este, especialmente en 2014 cuando gran parte de GameOver ZeuS fue desactivada por una operación del Departamento de Justicia de Estados Unidos. Además, en el mismo año, una empresa de seguridad creó una herramienta para desencriptar archivos infectados por CryptoLocker, luego

de haber realizado un ataque de hackeo y obtener todas las claves utilizadas para anteriores encripciones [15].

3.5. 2014 | CryptoWall

CryptoWall es un programa ransomware de tipo troyano que fue descubierto en 2014, siendo uno de los más destacados del año. Está destinado a encriptar archivos de todas las versiones de Windows, incluyendo Windows XP, Windows Vista, Windows 7 y Windows 8. A diferencia de los expuestos anteriormente, este ransomware sigue aún vigente y no se ha encontrado forma de recuperar los archivos infectados evitando el pago a los ciberdelincuentes.

3.5.1. Propagación

Este ransomware se distribuye de diferentes maneras. La más utilizada es mediante campañas de spam vía correo electrónico, en donde se incluyen adjuntos maliciosos. Cuando la víctima descomprime o ejecuta el archivo que pretenden ser facturas u otras comunicaciones comerciales, ocurre la infección de CryptoWall. Adicionalmente a esta alternativa, otros malwares ya instalados en la computadora víctima pueden descargar archivos e infiltrar CryptoWall, Por último, puede ser distribuido también mediante *exploit kits*, específicamente kits que se aprovechan de las siguientes vulnerabilidades: Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability (CVE-2012-0507); Adobe Flash Player Buffer Overflow Vulnerability (CVE-2014-0515) y Adobe Flash Player and AIR Unspecified Heap Based Buffer Overflow Vulnerability (CVE-2014-0556) [16].

3.5.2. Modo de operación

Una vez que CryptoWall ha sido ejecutado en el ordenador de la víctima, escanea las unidades locales, extraíbles y recursos compartidos de red buscando archivos de datos a cifrar. Posteriormente, elimina todas las

copias Shadow Volume para evitar que los archivos encriptados sean recuperados.

Los desarrolladores de este ransomware crearon un sitio web TOR llamado CryptoWall Decryption Service para que las víctimas paguen el rescate. En cada carpeta donde se cifró un archivo, se crean tres archivos con las instrucciones para llevarlo a cabo. En la siguiente captura de pantalla, se muestran las instrucciones que este ransomware expone al usuario afectado con el aviso de lo ocurrido y la demanda del pago del rescate:

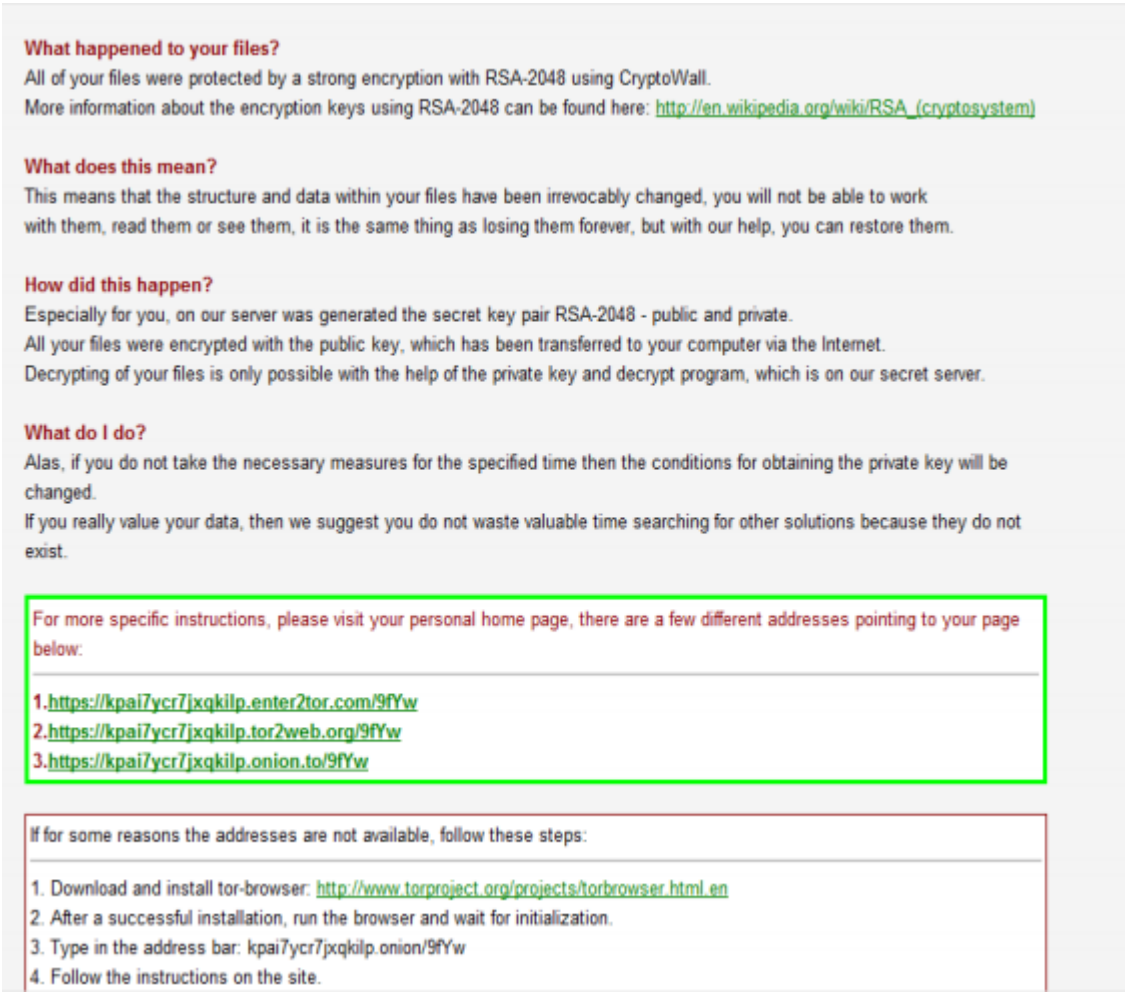


Imagen 6: Mensaje de CryptoWall. Fuente: McAfee Labs

Este ransomware utiliza dos algoritmos de cifrado: AES y RSA. Por un lado, genera una clave AES de 256 bits para cifrar los archivos. Esta clave es cifrada con la clave pública única RSA creada por los desarrolladores y

que se encuentra en el ejecutable malicioso. Así, la clave AES cifrada con RSA es transmitida al servidor de C&C, evitando que viaje en texto plano y que alguien la pueda obtener. La única manera de recuperar la clave AES es teniendo la clave privada de RSA asociada a la clave pública, perteneciente a los desarrolladores del malware (no viaja por la red ni tampoco se encuentra en el archivo utilizado para infectar) [17].

Hasta el momento, no se ha encontrado manera de recuperar la clave privada para descifrar los archivos afectados por CryptoWall. La única manera de recuperarlos es mediante el pago del rescate en CryptoWall Decryption Service.

3.6. 2015 | TeslaCrypt

Uno de los ransomware más destacados descubiertos en 2015 y que será resaltado en esta sección es TeslaCrypt. Fue un troyano que encripta archivos de datos en Windows, especialmente los utilizados para videojuegos populares como Minecraft o World of Warcraft. Si bien utilizaba algoritmos criptográficos estándar que garantizaban un alto nivel de seguridad, este ransomware ha llegado a su fin por otro factor que se será tratado en esta subsección.

3.6.1. Propagación

Este ransomware infectaba a las víctimas principalmente mediante exploit kits, Angler (en sus comienzos) aprovechando una vulnerabilidad en una versión desactualizada de Flash player, Sweet Orange y Nuclear EKs. También podía ser distribuido mediante campañas de spam o sitios web comprometidos.

3.6.2. Modo de operación

Tras su ejecución, TeslaCrypt exploraba las unidades buscando archivos con extensiones en particular, los abría, leía y cifraba. Para garantizar su persistencia, eliminaba las copias Shadow Volume.

Una vez encriptados los archivos, colocaba dos archivos en la computadora de la víctima: uno de texto plano y uno en HTML indicando las instrucciones para recibir la clave de descifrado. El pago del rescate debía llevarse a cabo a través de un sitio web ubicado en TOR, para el cual cada instancia de TeslaCrypt poseía su dirección Bitcoin.

Existieron variantes de TeslaCrypt. En sus inicios, investigadores de Cisco descubrieron que sólo utilizaba cifrado simétrico con AES, a pesar de que el ransomware afirmaba encriptar con algoritmos asimétricos. Posteriores versiones incorporaron el algoritmo de encripción RSA-2048 [18].

En el año 2016, TeslaCrypt sorprendentemente llegó a final. Los desarrolladores dejaron cerrar su “proyecto” y publicaron la clave maestra para descifrar los archivos infectados. Por lo tanto, cualquier ordenador que fue víctima de este ransomware puede recuperar su información de manera gratuita, sin necesidad de pagar un rescate [19]. En la siguiente captura de pantalla, se muestra el mensaje de los desarrolladores con la clave maestra en su sitio de pago:

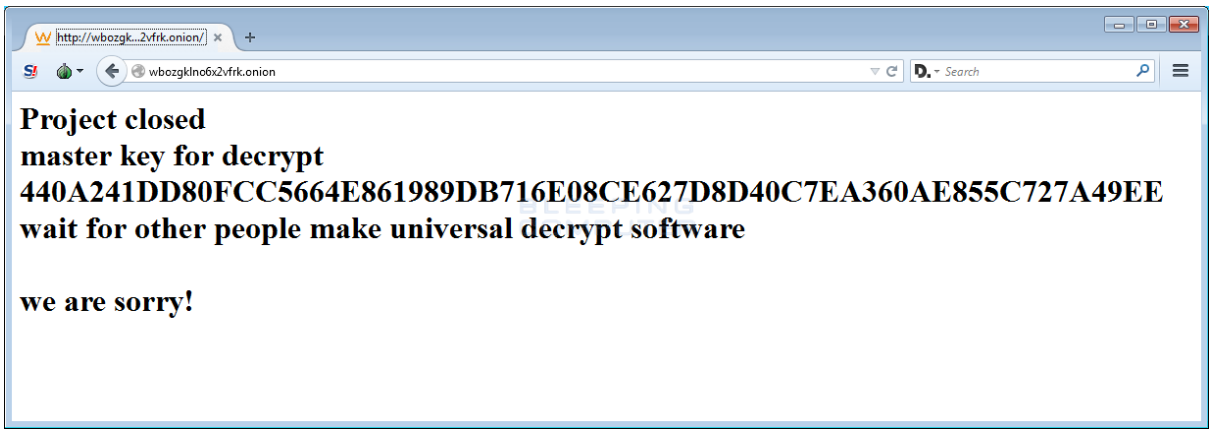


Imagen 7: Sitio de pago que muestra la clave maestra de descifrado. Fuente: Bleeping Computer

3.7. 2016 | Locky

En 2016, Internet se vio sacudida por infecciones causadas por el troyano Locky. Es un ransomware que encripta archivos en Windows y, a diferencia de sus antecesores, obtiene estadísticas de sus víctimas con el

aparente objetivo de determinar valores a los archivos cifrados y pedir rescates de manera individual. Si bien ha infectado a una gran cantidad de ordenadores alrededor del mundo, ganó popularidad luego de atacar importantes hospitales de Estados Unidos.

3.7.1. Propagación

La principal fuente de propagación de Locky es mediante campañas "agresivas" de phishing y spam. En primera instancia, este ransomware se distribuía mediante documentos maliciosos adjuntos de formato Microsoft Word, Microsoft Excel, que incluían macros con scripts ofuscados Visual Basic Script (VBS). En la siguiente captura de pantalla, se muestra un ejemplo de estos mensajes de correo electrónico, engañando a la víctima de que eran enviados por grandes y reconocidas empresas:

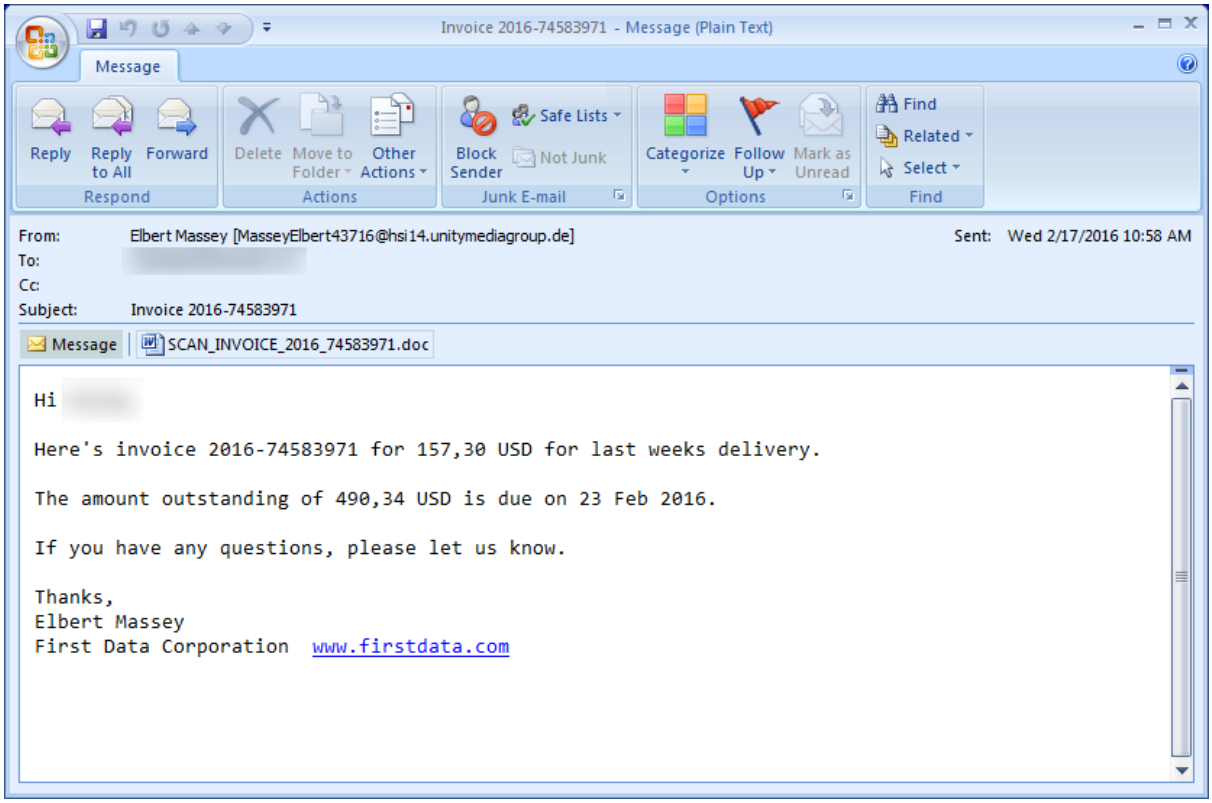


Imagen 8: Campaña de spam de Locky. Fuente: Kaspersky

Las nuevas variantes de Locky, han optado por utilizar archivos de formato .ZIP, en lugar de los documentos mencionados anteriormente,

incorporando un programa de descarga de JavaScript ofuscado para permitir a Locky ingresar al ordenador [20].

3.7.2. Modo de operación

Cuando Locky es ejecutado por primera vez, se contacta con el servidor C&C para avisar que ha ocurrido la infección. Es por ello por lo que el ransomware no puede encriptar si el dispositivo se encuentra desconectado de Internet. Al recibir la clave pública RSA de 2048 bits del servidor, comienza a buscar archivos de ciertas extensiones y en ciertas unidades. Para cada archivo, se genera una nueva clave aleatoria de 128 bits y cifra los contenidos del archivo con el algoritmo AES.

Al finalizar la encripción, muestra el aviso y pedido de rescate a la víctima. Se detallan las instrucciones, cuyo diseño ha sido cambiado a medida que Locky fue evolucionado. Una vez abonado el rescate, el descifrador se puede encontrar en cuatro distintos sitios en TOR [21].

Hasta el momento, no se ha encontrado manera de desencriptar los archivos afectados por Locky. Debido a que la generación del par de claves pública y privada de RSA utilizadas para la infección ocurre en el servidor C&C, es imposible la desencripción de forma manual.

3.8. 2017 | WannaCry

Sin dudas, WannaCry fue el ransomware que causó más impacto a nivel mundial no sólo del año 2017, sino de la historia de este tipo de malwares. Ha tenido repercusión no sólo en el ambiente de la informática, sino también en diarios y canales de televisión al haber afectado alrededor de 200.000 ordenadores en 150 países, incluyendo como objetivos empresas, universidades y hospitales.

A comparación de sus antepasados, WannaCry adoptó una nueva estrategia que lo hizo sumamente agresivo y le permitió alcanzar muchísimas más víctimas que si hubiera seguido los patrones anteriores. Desde este año en adelante, no sólo se siguió hablando de ransomware, sino que también se comenzó a hablar de *cryptoworm*. Estos nuevos

ransomwares combinaron la auto-propagación de los gusanos informáticos (del inglés *worms*) y el uso de la criptografía para encriptar archivos y pedir el pago de un rescate. Por lo tanto, estas nuevas familias no se satisfacen sólo con secuestrar la información del ordenador de la víctima, además intentan afectar y conseguir nuevas víctimas a través de la red a la cual está conectado el ordenador infectado [22]. En el caso de WannaCry en particular, está compuesto por dos módulos: módulo worm y módulo ransomware.

3.8.1. Propagación

Al igual que en los ransomware mencionados previamente, uno de los medios de propagación de WannaCry era mediante adjuntos en mensajes de correo electrónico. Sin embargo, la masiva infección a tantas víctimas en los diversos países no fue resultado de la descarga de un adjunto en los ordenadores afectados. Este ransomware se propagó principalmente al aprovechar vulnerabilidades presentes en todos los sistemas operativos Windows que no estaban actualizados con los últimos parches de seguridad. Gracias al exploit EternalBlue, desarrollado por la NSA (Agencia de Seguridad Nacional de Estados Unidos) y filtrado por el grupo de hackers Shadow Brokers, explotaba las siguientes vulnerabilidades en el protocolo de Microsoft Server Message Block (SMB): Microsoft Windows SMB Server Remote Code Execution Vulnerability (CVE-2017-0144) y Microsoft Windows SMB Server Remote Code Execution Vulnerability (CVE-2017-0145). Durante su explotación, utilizaba un *backdoor* llamado DoublePulsar con el objetivo de copiarse, instalarse y ejecutarse a sí mismo. Por último, WannaCry buscaba otras computadoras vulnerables e intentaba dispersarse automáticamente a cualquiera que encontraba.

3.8.2. Modo de operación

Una vez que el módulo worm arriba a destino, intenta colocar en el ordenador el módulo ransomware. Este segundo módulo primero enumeraba los discos existentes en el ordenador, como pueden ser unidades locales, extraíbles y de red. Luego, escaneaba en busca de archivos con determinada extensión, asociados a aplicaciones, bases de datos, archivos

comprimidos y de multimedia. En la siguiente captura de pantalla, se muestra el aviso que hacía WannaCry a sus víctimas, incluyendo un contador que indicaba el tiempo restante antes que el precio del rescate sea aumentado:

Imagen 9: Mensaje de WannaCry. Fuente: Secureworks

Para lograr esto, se generaba aleatoriamente una clave AES de 128 bits para cada uno de los archivos que quería infectar y encriptar. Adicionalmente, generaba un par de claves RSA de 2048 bits para cada encripción, la cual era a su vez encriptada con una clave pública RSA que tenía incorporada el módulo. La clave RSA generada era utilizada para encriptar las claves AES.

A WannaCry no le bastaba sólo con encriptar el sistema de la víctima. Además, se ejecutaba la rutina de propagación, mediante el cual el módulo worm escaneaba direcciones IP (direcciones pertenecientes a la misma subred del ordenador comprometido y direcciones generadas aleatoriamente) en busca de poder replicarse y conseguir nuevas víctimas.

Debido al nivel de los algoritmos y la seguridad ofrecida por la criptografía utilizada en este ransomware, no se han desarrollado herramientas para desencriptar archivos infectados y evitar el pago del rescate. La única manera que tienen las víctimas de WannaCry para desinfectar su sistema es a través del pago a los desarrolladores del malware [23].

3.8.3. Análisis dinámico

Para llevar a cabo el análisis del comportamiento de WannaCry, se tomó una captura de malware que tiene publicada el proyecto **Stratosphere IPS** [24], la cual contiene el tráfico interceptado en una computadora normal que fue infectada remotamente con WannaCry. La variante del ransomware utilizado como muestra tiene un valor de hash SHA1 de 3b669778698972c402f7c149fc844d0ddb3a00e8. El ambiente de prueba consiste en dos ordenadores con Windows conectadas en la misma red, una de las cuales fue infectada previamente con WannaCry. La siguiente imagen ilustra y detalla el ambiente mencionado:

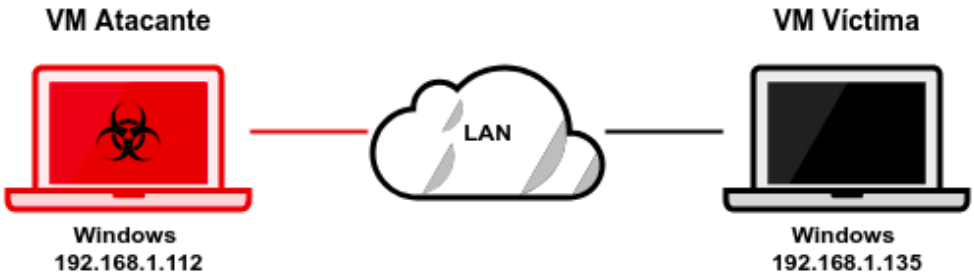
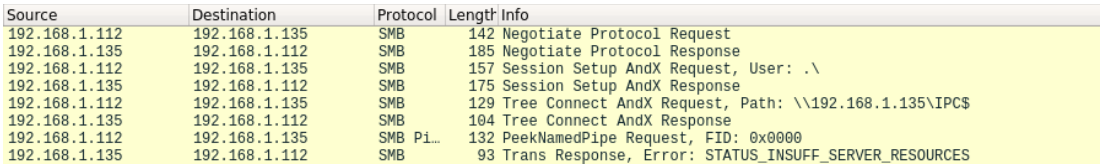


Imagen 10: Ambiente utilizado para el análisis dinámico de WannaCry

Del tráfico analizado, se pudieron identificar diferentes etapas que el malware lleva adelante para lograr la infección [25]. El primer paso consiste en detectar si el parche de Microsoft MS17-010 fue aplicado, el cual arregla las vulnerabilidades en el protocolo SMB antes mencionadas. Para eso, WannaCry se conecta al IPC$ del ordenador, que se utiliza para navegar y establecer conexiones TCP/IP, y envía un paquete del tipo *SMB_COM_TRANSACTION* con el FID (“FileID”) en 0. En caso de que el código de respuesta de error sea

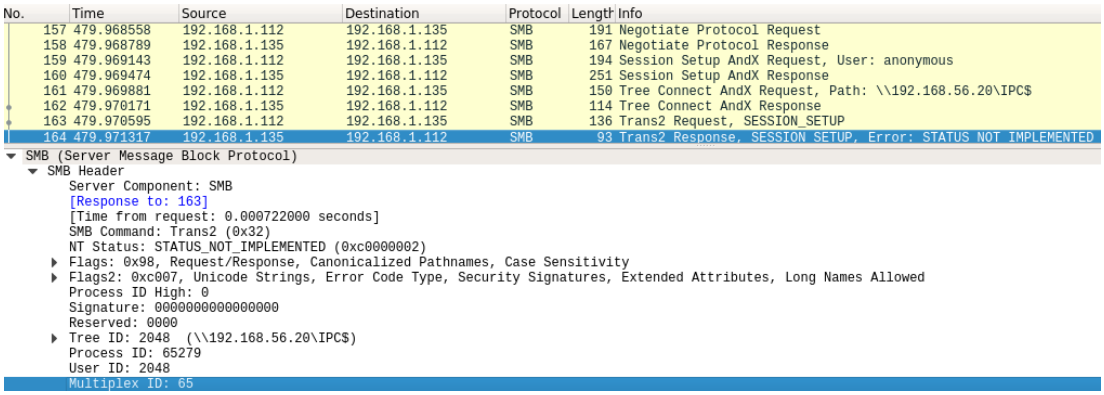
STATUS_INSUFF_SERVER_RESOURCES, tal como lo muestra la siguiente imagen, significa que el ordenador es vulnerable y la ejecución remota de código es posible.



Source	Destination	Protocol	Length	Info
192.168.1.112	192.168.1.135	SMB	142	Negotiate Protocol Request
192.168.1.135	192.168.1.112	SMB	185	Negotiate Protocol Response
192.168.1.112	192.168.1.135	SMB	157	Session Setup AndX Request, User: .\
192.168.1.135	192.168.1.112	SMB	175	Session Setup AndX Response
192.168.1.112	192.168.1.135	SMB	129	Tree Connect AndX Request, Path: \\192.168.1.135\IPC$
192.168.1.135	192.168.1.112	SMB	104	Tree Connect AndX Response
192.168.1.112	192.168.1.135	SMB Pi…	132	PeekNamedPipe Request, FID: 0x0000
192.168.1.135	192.168.1.112	SMB	93	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES

Imagen 11: Paquetes de detección de la instalación del parche de seguridad

Posteriormente, WannaCry busca detectar la presencia del backdoor DoublePulsar. Establece una sesión SMB y se conecta al IPC$. Le envía un paquete del tipo *SMB_COM_TRANSACTION2* que sirve para chequear si ya se encuentra implantado el backdoor. En caso afirmativo, el valor de "Multiplex ID" contenido en la respuesta será 81. Por el contrario, si "Multiplex ID" es 65, significa que el ordenador no ha sido infectado aún. En el caso analizado, DoublePulsar no estaba instalado y el paquete que lo indica se expone en la siguiente imagen:



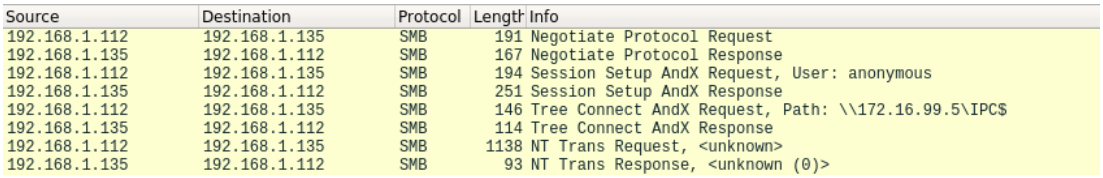
No.	Time	Source	Destination	Protocol	Length	Info
157	479.968558	192.168.1.112	192.168.1.135	SMB	191	Negotiate Protocol Request
158	479.968789	192.168.1.135	192.168.1.112	SMB	167	Negotiate Protocol Response
159	479.969143	192.168.1.112	192.168.1.135	SMB	194	Session Setup AndX Request, User: anonymous
160	479.969474	192.168.1.135	192.168.1.112	SMB	251	Session Setup AndX Response
161	479.969881	192.168.1.112	192.168.1.135	SMB	150	Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
162	479.970171	192.168.1.135	192.168.1.112	SMB	114	Tree Connect AndX Response
163	479.970595	192.168.1.112	192.168.1.135	SMB	136	Trans2 Request, SESSION_SETUP
164	479.971317	192.168.1.135	192.168.1.112	SMB	93	Trans2 Response, SESSION SETUP, Error: STATUS NOT IMPLEMENTED

```
▾ SMB (Server Message Block Protocol)
  ▾ SMB Header
      Server Component: SMB
      [Response to: 163]
      [Time from request: 0.000722000 seconds]
      SMB Command: Trans2 (0x32)
      NT Status: STATUS_NOT_IMPLEMENTED (0xc0000002)
    ▸ Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity
    ▸ Flags2: 0xc007, Unicode Strings, Error Code Type, Security Signatures, Extended Attributes, Long Names Allowed
      Process ID High: 0
      Signature: 0000000000000000
      Reserved: 0000
    ▸ Tree ID: 2048  (\\192.168.56.20\IPC$)
      Process ID: 65279
      User ID: 2048
      Multiplex ID: 65
```

Imagen 12: Paquetes de detección de la presencia del backdoor DoublePulsar

Si el ordenador es vulnerable pero no se encuentra DoublePulsar, el ransomware entra en una tercera etapa donde ejecuta el exploit EternalBlue que tiene incorporado para instalar el backdoor. Utiliza paquetes de tipo *SMB_COM_NT_TRANSACT* y paquetes *SMB_COM_TRANSACTION2_SECONDARY* que contienen el *shellcode* (conjunto de órdenes programadas y trasladadas a *opcodes*). Los paquetes

mostrados en la siguiente imagen corresponden a la actividad del ransomware en esta etapa:



Source	Destination	Protocol	Length	Info
192.168.1.112	192.168.1.135	SMB	191	Negotiate Protocol Request
192.168.1.135	192.168.1.112	SMB	167	Negotiate Protocol Response
192.168.1.112	192.168.1.135	SMB	194	Session Setup AndX Request, User: anonymous
192.168.1.135	192.168.1.112	SMB	251	Session Setup AndX Response
192.168.1.112	192.168.1.135	SMB	146	Tree Connect AndX Request, Path: \\172.16.99.5\IPC$
192.168.1.135	192.168.1.112	SMB	114	Tree Connect AndX Response
192.168.1.112	192.168.1.135	SMB	1138	NT Trans Request, <unknown>
192.168.1.135	192.168.1.112	SMB	93	NT Trans Response, <unknown (0)>

Imagen 13: Paquetes de implantación del backdoor DoublePulsar

La última etapa corresponde a la principal de todo el proceso de infección y es llevado a cabo mediante instrucciones de DoublePulsar [26]. WannaCry envía instrucciones de “ping”, el cual es ocultado en el campo “Timeout” del paquete, para asegurarse que el backdoor está instalado en el sistema objetivo. Este paquete explicado se evidencia en la siguiente imagen:

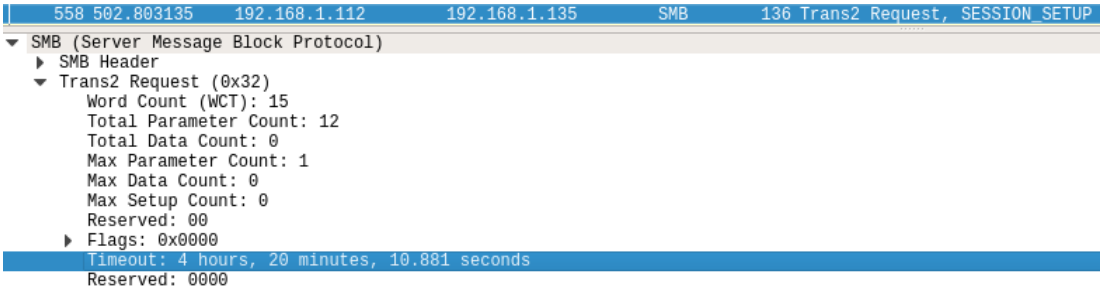


Imagen 14: Paquete de la instrucción ping oculto en el campo “Timeout”

El ordenador infectado contesta al comando ping indicando 81 en el campo “Multiplex ID” y en “Signature” envía la plataforma afectada (en este caso x86 por empezar con 0x00) concatenado con una clave XOR de 4 bytes que será utilizada para la encripción del payload de los próximos paquetes. La siguiente imagen corresponde a la captura del paquete con la respuesta de la víctima:

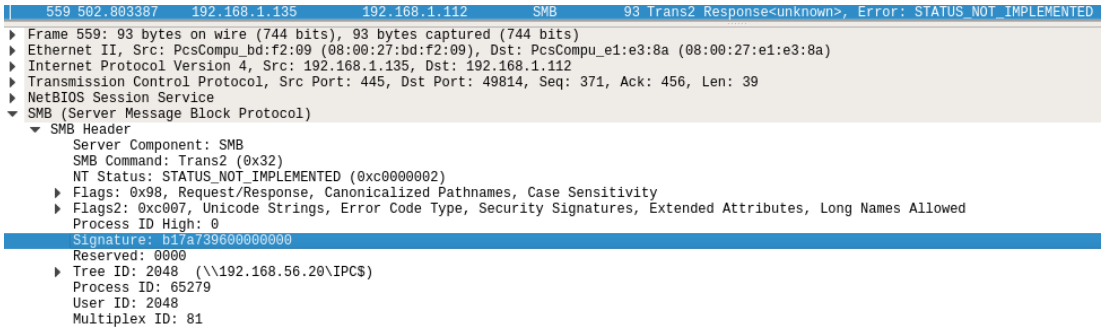


Imagen 15: Paquete con información oculta en los campos "Multiplex ID" y "Signature"

Por último, el ransomware envía el comando "exec" de DoublePulsar que desencadena la infección utilizando nuevamente el campo "Timeout". En este caso, contiene el valor 0x001a8925 correspondiente al comando "exec", a diferencia del anterior comando ("ping") que tiene el valor 0x00ee3401.

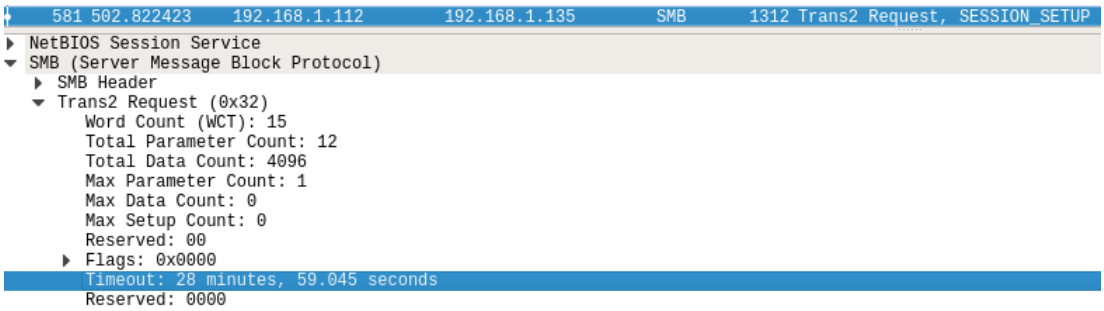


Imagen 16: Paquete de la instrucción exec oculto en el campo "Timeout"

Una vez finalizado el proceso de infección, el ordenador víctima enviará una respuesta, utilizando una vez más el campo "Multiplex ID". Cuando este campo es devuelto con valor 82, WannaCry ha terminado su actividad. En la siguiente imagen se muestra el paquete de finalización, el cual tuvo lugar 30 minutos después del primer paquete correspondiente al comienzo de la infección analizada:

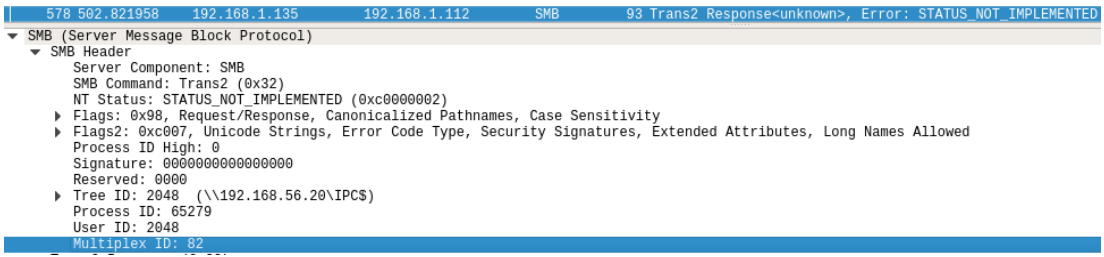


Imagen 17: Paquete de finalización de la infección de WannaCry

3.9. 2018 | GandCrab

Al igual que en los últimos años, durante 2018 se han lanzado un gran número de nuevas variantes y familias de ransomware. En esta sección, GandCrab es el que será destacado, ransomware que encripta archivos en sistemas operativos Windows. Si bien tiene muchos puntos en común con los anteriores malwares que se han mencionado, hay algunas otras características relevantes que podrían marcar el camino de los próximos ransomware que se están o serán desarrollados.

GandCrab tiene la particularidad de requerir que el pago sea realizado mediante criptomoneda, pero no con Bitcoin como los anteriores, sino Dash. Es probable que los desarrolladores de este malware han tomado esta decisión debido a que Dash favorece aún más el anonimato y es muy complejo de rastrear. De todas maneras, posteriores variantes incluyeron el método de pago con Bitcoin.

Adicionalmente, GandCrab es un ejemplo actual de que no siempre las organizaciones cibercriminales ganan. Un grupo de empresas e investigadores se han juntado para batallar contra este ransomware y han desarrollado una herramienta, la cual será tratada a continuación.

3.9.1. Propagación

GandCrab puede ser distribuido mediante adjuntos en mensajes de correo electrónico, utilizando documentos encriptados de Microsoft Word, scripts en VBA (Visual Basic for Applications) o Javascript [27]. Sin embargo, la mayor propagación la logró mediante exploit kits: RIG, Magnitude y uno que es mucho menos común y se creía desaparecido llamado Grandsoft.

3.9.2. Modo de operación

Después de desempacar el binario, GandCrab comienza su trabajo. Realiza un proceso de inicialización y se conecta con el servidor C&C. Esta conexión se realiza de manera encriptada, pero curiosamente, la encripción de la misma es llevada a cabo con una *hard-coded key*. Esto significa, que la

comunicación entre el servidor de C&C y el malware una vez que ha llegado a un objetivo es encriptada con la misma clave. Esto fue modificado en posteriores variantes que los desarrolladores fueron lanzando de esta familia de ransomware.

Posteriormente, genera el par de clave pública y privada RSA para cada víctima, la cual se utilizará para encriptar la clave AES de 256 bits que se usa para cifrar los archivos. Al cifrar, el malware omite el cifrado de ciertos archivos con determinados nombres y pertenecientes a determinados directorios. Finalmente, en cada directorio infectado deja una nota de rescate y demanda su pago en Dash. En la siguiente captura de pantalla, se muestra el aviso de GandCrab una vez terminado el proceso de encripción:

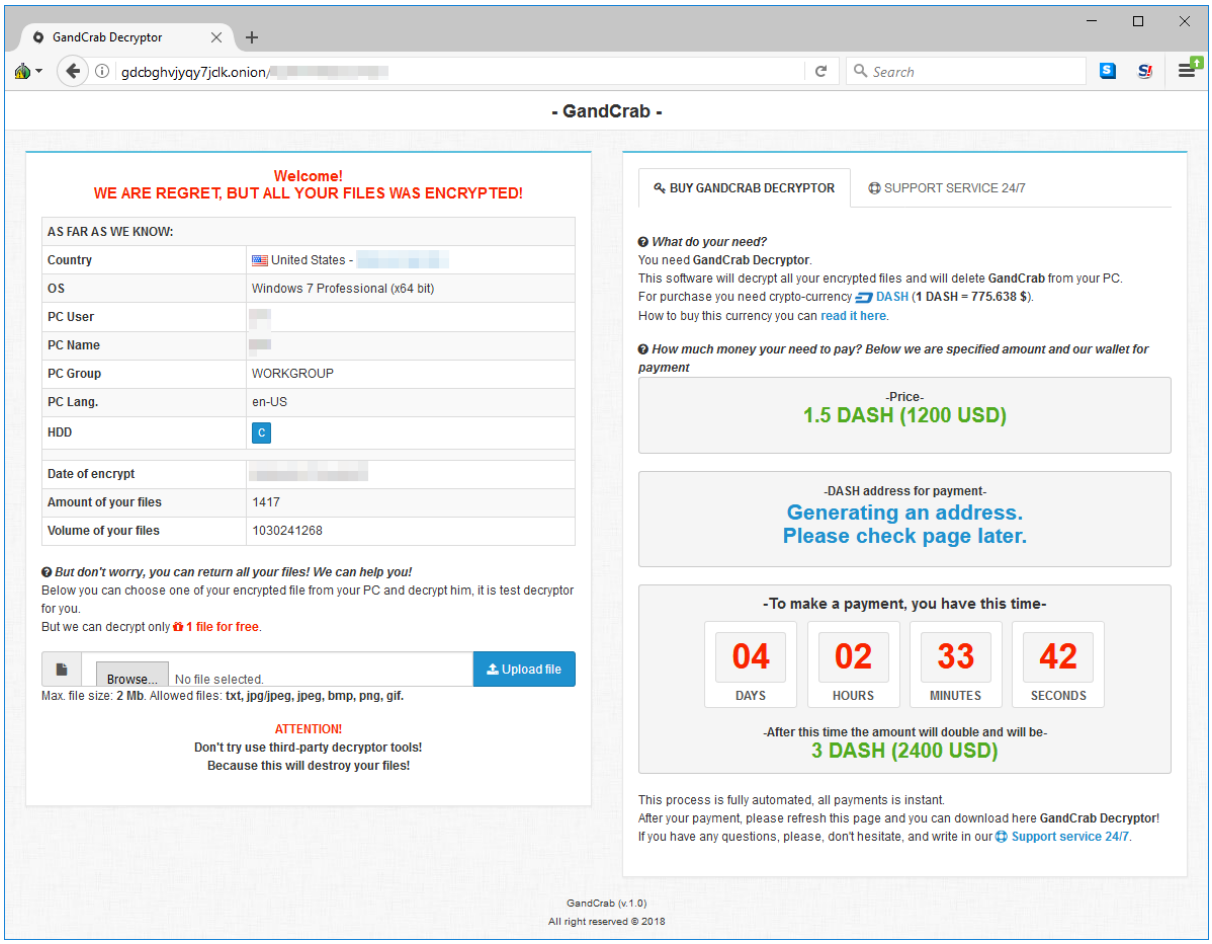


Imagen 18: Instrucciones de GandCrab para el pago de rescate. Fuente: Malwarebytes

Al igual que cualquier software, en el desarrollo de malwares también aplican las buenas y las malas prácticas, es decir, lo que sí hay que hacer y

lo que no para lograr un buen programa de computadora. Una de las malas prácticas es el *hard-code* mencionado previamente, que consiste en la incrustación de datos directamente en el código fuente. Además, GandCrab tenía un error en su código, lo cual es posible en el mundo del software y es conocido en inglés como *bug*. Estos errores pueden desencadenar un resultado indeseado en el mismo. En particular, este ransomware tiene un error de programación que deja las claves en memoria. Esto fue descubierto y aprovechado por un grupo conformado por una empresa antimalware, Europol y la policía de Rumania. Como resultado, realizaron una publicación en **NoMoreRansom** [28], haciendo pública una herramienta que permite a víctimas de GandCrab desencriptar y recuperar sus archivos infectados [29]. Esta organización y su iniciativa será tratada posteriormente en esta tesis. Debido a estos errores citados y mejoras que los desarrolladores encontraron para hacer más efectivo su ransomware, han sido lanzadas nuevas variantes que incluyen nuevos mecanismos de encripción (como la incorporación de Salsa20 para mejorar la *performance*), capacidades para detectar si está corriendo en una máquina virtual, entre otros. Es por ello, que la lucha contra GandCrab aún sigue latente. Continuamente se pueden encontrar nuevos hallazgos por parte de las empresas interesadas en abatir el ransomware y nuevas funcionalidades por parte de los desarrolladores de este.

3.10. Resumen comparativo

Luego de describir los ransomwares más destacados en la historia, es interesante compilar todo lo expuesto, lo cual nos puede ayudar a identificar la evolución que ha tenido este tipo de malware y los cambios que fueron implementados por sus desarrolladores. En la siguiente tabla, se muestra un resumen y una comparación entre los ransomware explicados:

Ransomware	Fecha de descubrimiento	Tipo	Plataforma afectada	Algoritmo de cifrado
AIDS Trojan	Diciembre 1989	Troyano	MS-DOS	Personalizado
GPCoder	Mayo 2005	Troyano	Microsoft	Personalizado

Archiveus	Mayo 2006	Troyano	Microsoft	RSA
CryptoLocker	Septiembre 2013	Troyano	Microsoft	RSA + AES
CryptoWall	Junio 2014	Troyano	Microsoft	RSA + AES
TeslaCrypt	Febrero 2015	Troyano	Microsoft	RSA + AES
Locky	Febrero 2016	Troyano	Microsoft	RSA + AES
WannaCry	Mayo 2017	Troyano Gusano	Microsoft	RSA + AES
GandCrab	Enero 2018	Troyano	Microsoft	RSA + AES

Tabla 2: Resumen comparativo de familias de ransomware

Es fácil de reconocer que todos los ransomwares expuestos son de tipo troyano y que a partir de 2017 esta tendencia pudo haber cambiado, al haber ransomwares más robustos que están conformados por un módulo de encripción y un módulo gusano. Antes del 2017, era una monotonía de ransomwares troyanos. Esto tiene sentido si nos remitimos al modo de propagación necesario para que un ransomware infecte un ordenador. Se presenta ante la víctima como un programa legítimo, como puede ser en el adjunto de un mensaje de correo electrónico que busca engañarlo para que el usuario lo descargue y ejecute. La incorporación de capacidades de un gusano informático en el mismo ransomware, permite que, una vez infectado un ordenador, se propague de computadora a computadora consiguiendo nuevas víctimas en la misma red.

Analizando las plataformas afectadas, se puede identificar que todos los ransomwares de esta sección afectan a sistemas operativos Windows (o Microsoft Disk Operating System debido a la época). Esto muestra el interés de los desarrolladores de ransomwares, cuyo objetivo es infectar a la mayor cantidad de ordenadores posibles o que su ataque sea lo más masivo posible. A nivel mundial, el liderazgo de Windows es incontestable. La gran mayoría de los ordenadores utilizan Windows y esto lo hace más propenso a que los desarrolladores pongan su ojo en ellos y estén más expuestos a ataques de ransomware. Sin embargo, esto no quiere decir que no hay ransomwares que afecten otras plataformas. Existen ransomwares que afectan a macOS o Linux, pero no llegan a tener tanta relevancia o protagonismo como los que afectan a Windows, que impactan a miles de ordenadores a nivel mundial.

Con respecto a los algoritmos de cifrado, en sus comienzos se utilizaron algoritmos criptográficos simétricos los cuales siguen siendo los más elegidos para encriptar los archivos en el ordenador de la víctima. Sin embargo, se puede apreciar un cambio en el algoritmo seleccionado, optando por algoritmos estándar que sean públicamente conocidos y que, por consecuencia, garantizan seguridad. Aquellos que eligen algoritmos personalizados, es probable que esa seguridad por oscuridad sea quebrada luego de su análisis como ha ocurrido con GPCoder en sus inicios. Luego, los desarrolladores de ransomware han incorporado criptografía asimétrica particularmente para que la comunicación entre el malware y el servidor C&C esté cifrada y evitar fugas de información.

CAPÍTULO 4. Estrategias de defensa proactiva

En esta sección se presentan las acciones que pueden llevarse a cabo previo a que el ransomware haya infectado el ordenador, red y/o sistema. El objetivo de las estrategias proactivas es que el administrador de seguridad o usuario final se encuentre con un nivel de protección que permita evitar los ataques de este tipo de código malicioso. Es importante destacar que las técnicas que pueden emplearse para proteger la información del Ransomware no se limitan a las expuestas a continuación.

4.1. Red segura

Asegurar la red en la que se encuentran los servidores y ordenadores de usuarios finales es una de las principales medidas que se deben tomar en la batalla contra el ransomware. Mediante una red segura, no sólo es posible evitar que los dispositivos sean afectados por el código malicioso en primera instancia, sino también evita que se expanda la infección en caso de ya haber ingresado a la misma.

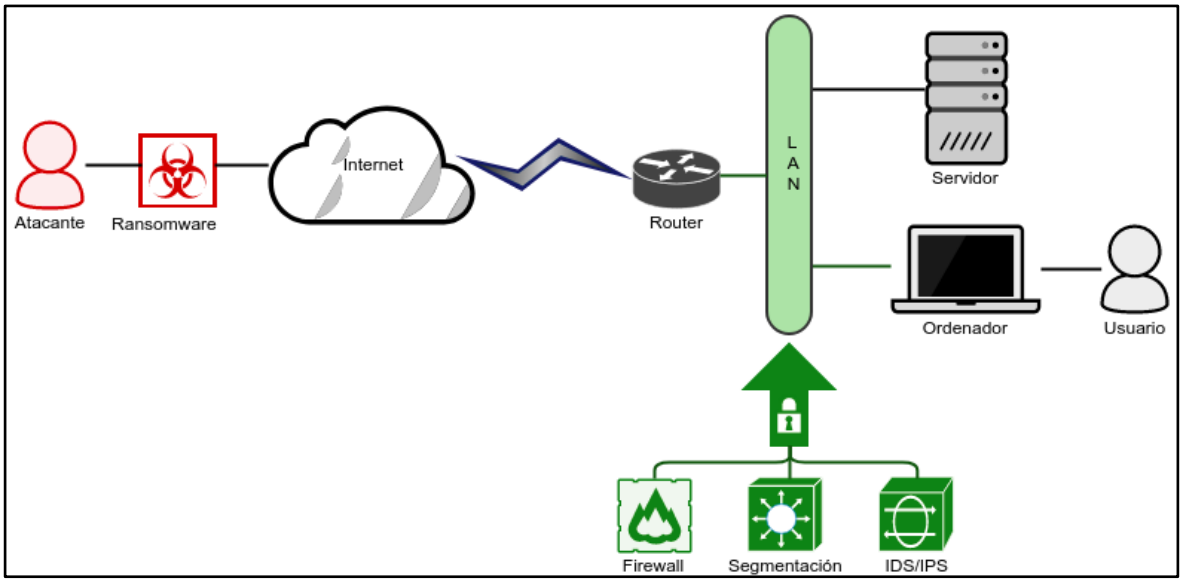


Imagen 19: Estrategias proactivas mediante Red segura

4.1.1. Firewall

Un cortafuegos (del inglés *firewall*) es un dispositivo configurado para permitir, limitar, cifrar y/o descifrar el tráfico entre diferentes ámbitos. Puede ser utilizado para el filtrado de tráfico entrante (controla las comunicaciones desde el exterior a la red) y tráfico saliente (controla las comunicaciones desde la red hacia equipos externos).

Es menos probable que la red sea objetivo de un malware si un firewall es restrictivo en cuanto a las comunicaciones que tienen los ordenadores con entidades externas. En caso de que la red esté afectada por ransomware, un filtro de salida adecuado hará que el ordenador, una vez infectado, no pueda comunicarse con el atacante [30]. Adicionalmente a estas medidas, un Firewall de siguiente generación (del inglés *Next Generation Firewall*) puede brindar mayor protección, debido a las funciones extra comparadas con un firewall tradicional, como el análisis de malware.

4.1.2. Sistema de detección y prevención de intrusiones

Un sistema de detección de intrusos (IDS, del inglés *Intrusion Detection System*) es un dispositivo que monitorea eventos que ocurren en la red en busca de incidentes, violaciones o amenazas a las políticas de seguridad. Es idéntico a un sistema de prevención de intrusos (IPS, del inglés *Intrusion Prevention Systems*), a diferencia que este último al detectar un incidente, lo detiene. Si bien no nacieron con el objetivo de detectar malware, los más recientes ofrecen funciones de detección de exploits.

Pueden utilizarse para alertar si se realizan intentos de comunicación con direcciones IP maliciosas, tales como centros de comando y control para *botnets* y sitios de generación de claves para ransomware. Adicionalmente, ayudan a identificar un sistema dentro de la organización que está intentando infectar a otros sistemas, evitando su expansión [30].

4.1.3. Segmentación

La segmentación de una red consiste en dividirla en subredes a través de VLANs y ACLs (*Access control lists*) que controlan el tráfico con el objetivo de mejorar el rendimiento, disminuyendo la cantidad de ordenadores conectados a cada subred. Ante un ataque de ransomware, la segmentación no evita que sea satisfactorio, pero ayuda a garantizar que una infección

afecte sólo en el segmento de red en el que se encuentra el ordenador comprometido y no permite que se extienda por toda la red [30], particularmente en ransomwares que tienen un módulo worm incluido.

4.2. Software de seguridad

Existen en el mercado una gran variedad de programas, aplicaciones y herramientas comerciales y de código abierto que son de utilidad para proteger los ordenadores y servidores de ataques de Ransomware. Las posibles soluciones que se plantean en este apartado se focalizan en software libre y gratuito.

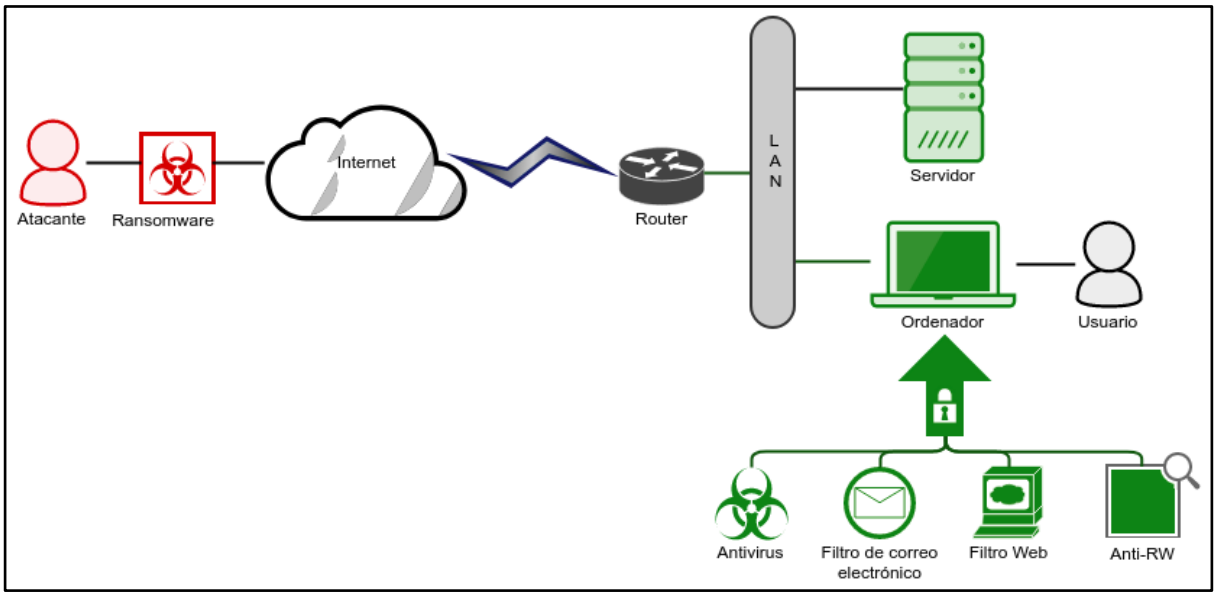


Imagen 20: Estrategias proactivas mediante Software de seguridad

4.2.1. Antivirus

Un antivirus es un programa cuyo objetivo es detectar y/o eliminar virus, gusanos y otros tipos de códigos maliciosos. Utiliza tres tecnologías para la detección en un ordenador: coincidencia de firma (se mantiene una base de datos de firmas, con la cual detecta un virus si el código analizado coincide con una de las entradas almacenadas); heurística (se utiliza una base de datos de firmas de comportamiento de virus, con la cual detecta un virus si la rutina del código analizado coincide con una firma almacenada) y suma de comprobación de integridad (se calcula el *checksum* de los

archivos “limpios” y los utiliza para detectar la posible presencia de virus ante un cambio de *checksum* de los mismos). Si bien las últimas dos tecnologías pueden causar falsos positivos en la detección, el uso de firmas sólo detecta malware que haya sido identificado previamente y necesita que los usuarios actualicen periódicamente la base de datos de virus [31].

Ante un ataque de ransomware, un antivirus puede ser utilizado para proteger a los usuarios. Ofrece la posibilidad de evitar que el usuario sea víctima gracias a la detección del código, mediante cualquiera de las tecnologías mencionadas previamente.

Clam AntiVirus [32] es un antivirus que ofrece protección tanto para ordenadores personales como para servidores. Ofrece diversas utilidades de línea de comandos e incorpora una base de datos con firmas para virus no polimórficos (en formato de cadena simple) y para virus polimórficos (en formato de expresión regular). ClamAV realiza la detección principalmente mediante el uso de una variante del algoritmo Aho-Corasick y una versión optimizada del algoritmo Boyer-Moore [33].

4.2.2. Filtro de correo electrónico

Un filtro de correo electrónico (*email filter* en inglés) es un tipo de programa que procesa los correos electrónicos para organizarlos según criterios específicos. El filtro puede operar en el tráfico de correo electrónico entrante y saliente. El filtrado de correo entrante implica el escaneo de mensajes de Internet dirigidos a los usuarios protegidos por el programa. Por otro lado, el filtrado de correo saliente implica el análisis de mensajes de correo electrónico de los usuarios protegidos, antes de que se envíen mensajes potencialmente dañinos a otras personas. Existen distintos tipos de filtros disponibles, según la revisión y los criterios aplicados: de contenido (revisan el contenido de los mensajes); de encabezado (revisan el encabezado de los mensajes); basados en listas negras (bloquean mensajes que provienen de *spammers* conocidos); basados en reglas (bloquean mensajes según criterios definidos por el usuario); de permiso (requieren que el emisor del mensaje esté pre-aprobado) [34].

Una de las formas en que el ransomware afecta es mediante correo electrónico. Engañando al usuario, el atacante logra que se descargue un

archivo adjunto en el ordenador de la víctima. Como defensa, el filtro de correo electrónico puede utilizarse para descartar los mensajes entrantes. Su objetivo es escanear y poner en cuarentena aquellos con documentos, archivos ejecutables y archivos comprimidos maliciosos, antes que sean abiertos por los usuarios protegidos.

SpamAssassin [35] es uno de los programas de filtrado de correo electrónico que se puede utilizar para defender a los usuarios ante el ransomware. Esta herramienta informa que un mensaje es no deseado (*spam*) debido a que posee un puntaje alto, luego de comparar el contenido del mensaje con un conjunto de reglas. Se puede utilizar junto al servidor de correo para filtrar automáticamente el correo de un sitio o directamente ejecutado por usuarios en su propio buzón, integrándose con varios programas de correo como Outlook. Sus principales características son: comparación de encabezados y frases; filtrado bayesiano; direcciones según *whitelists* y *blacklists*; sistema de reputación del remitente; bases de datos colaborativas de identificación de spam; listas de bloqueo de DNS (RBLs, del inglés *Realtime Blackhole List*) [36].

4.2.3. Filtro Web

Un filtro web (*web filter* en inglés) es un programa capaz de evitar que usuarios accedan a sitios web que contienen código malicioso. Este filtro verifica el origen o el contenido de una página contra un conjunto de reglas proporcionadas por el proveedor o el usuario que instaló el programa. Provee diferentes modalidades: detección pasiva, bloqueo pasivo, detección activa o bloqueo activo [37].

Debido a que la manera más común de expansión del ransomware es mediante archivos adjuntos que son descargados por los usuarios inintencionalmente, el filtro web puede ser utilizado como defensa ante el criptovirus. Evita que los usuarios visualicen y por ende accedan a páginas o publicidades que poseen software infectado.

Adblock Plus [38] es un programa de filtrado web que puede ser utilizado para defender a los usuarios del ransomware. Esta aplicación ofrece extensiones para ser incluidas en los navegadores web como Google Chrome, permitiendo al usuario configurar para bloquear u ocultar anuncios.

Este filtrado se basa en reglas de filtro conformadas por expresiones regulares, las cuales permiten reducir el tráfico de red gracias a la evasión de objetos relacionados con anuncios no deseados [39].

4.2.4. Software anti-ransomware

Debido al gran crecimiento de familias de ransomware y la ocurrencia de ataques masivos en el último tiempo, se han desarrollado programas especializados que tienen como objetivo proteger a los usuarios de este tipo de software malicioso proactivamente, para evitar el daño o cifrado de los archivos. La detección de estas herramientas está basada en heurísticas, lo cual permite detectar ataques *zero-day*. Adicionalmente, incorporan otros métodos de defensa como la comparación de la suma de verificación (utilizar el *checksum* para saber si un archivo fue encriptado o no) y/o la predicción de comportamiento (asumir que está ocurriendo un ataque según la cantidad de archivos cambiados en un intervalo de tiempo) [40].

Malwarebytes Endpoint Security [41] incorpora una capa especial de protección anti-ransomware, la cual realiza un seguimiento de toda la actividad. Una vez que dispone de pruebas para determinar la presencia de ransomware, bloquea la infección y lo almacena en cuarentena antes de que logre afectar o encriptar los archivos. Protege a los usuarios ante amenazas conocidas (por ejemplo, CryptoWall) y ante amenazas de nuevas familias aún no descubiertas.

4.3. Actualizaciones

Uno de los puntos de entrada del ransomware es a través de un sistema operativo o una aplicación que se encuentra desactualizado y con alguna vulnerabilidad de seguridad. Es por ello por lo que la actualización continua del software utilizado e instalación de parches de seguridad se convierte en un hábito primordial para defenderse de este tipo de malware. La actualización es necesaria tanto para el sistema operativo como para el browser instalado, Microsoft Word, Java, Shockwave, Flash y Adobe Reader. Con el objetivo de facilitar la tarea de administradores de seguridad o

usuarios finales, los distintos proveedores de software están tendiendo a proveer una herramienta de auto-actualizador [42].

Si bien no existen muchos de este tipo, en el caso de ransomware que utiliza kits de explotación con exploits *zero-day*, la estrategia de defensa de actualizaciones no brinda protección. El software malicioso explota una vulnerabilidad de seguridad para la cual no existe un parche que la arregle.

4.4. Copia de seguridad

Una copia de seguridad (*backup*) es un duplicado de información, la cual incluye documentos, carpetas y todo objeto que se haya seleccionado del ordenador al momento de copiar. La copia permite recuperar la información original en casos en que se pierda la misma o no se encuentre disponible debido a: fallos de software o programación; problemas en el hardware; catástrofes (como incendio o inundación); infección por software malicioso (virus; ransomware); entre otros. Para esto, es importante que se almacene la copia de seguridad en un lugar seguro, preferiblemente en un lugar diferente y separado (lógica y físicamente). De lo contrario, un mismo problema que afecte a la información original afectará a la duplicada, dejando sin efecto esta medida de protección [43].

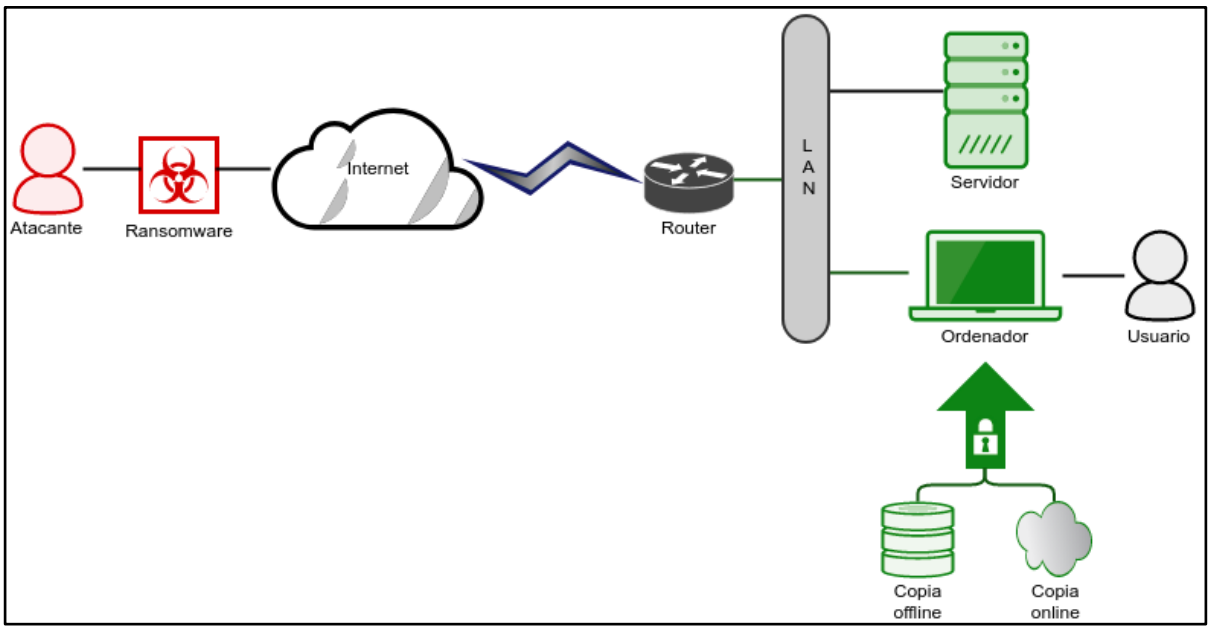


Imagen 21: Estrategias proactivas mediante Copias de seguridad

El ransomware atenta sobre la disponibilidad de la información, por lo que su objetivo es bloquear el acceso a los archivos de la víctima. Contar con copias de seguridad de estos archivos se torna en una metodología de defensa para evitar la efectiva pérdida de la información.

4.4.1. Online

Una copia de seguridad en línea (*online*) es aquella que se almacena en sistemas basados en la nube. La información es resguardada por un servidor que está conectado a Internet, por lo que es necesario una conexión a Internet activa para copiar. Permite un acceso a los datos de manera sencilla, rápida y desde cualquier ubicación con conexión a Internet.

Duplicati [44] es un cliente de copia de seguridad que puede ser utilizado para defender a los usuarios del Ransomware. Esta aplicación admite una variedad de proveedores de almacenamiento basados en la nube, tales como Amazon S3 y OneDrive. Además, ofrece funciones de encriptación, compresión y duplicación, control de versiones y copias de seguridad incrementales.

4.4.2. Offline

Una copia de seguridad fuera de línea (*offline*) es aquella que se almacena en un medio físico de hardware como discos duros externos o DVDs. El proceso de copia es sencillo, rápido y queda a salvo de cualquier ataque cibernético que pueden sufrir las redes o servicios conectados a Internet.

Rsync [45] es uno de los programas que se puede utilizar para defender a los usuarios del ransomware. Esta aplicación permite sincronizar archivos y directorios desde una ubicación a otra, minimizando la transferencia de datos (ahorrando tiempo y ancho de banda). En un ordenador puede sincronizar archivos de manera eficiente con una copia de seguridad en un disco duro externo. Adicionalmente, mediante administradores de procesos en segundo plano, se pueden llevar a cabo tareas como la duplicación mediante Rsync de manera encriptada y automatizada entre un host y un servidor central [46].

4.5. Concientización

Todo lo que necesita el ransomware para ingresar e infectar a un ordenador, red y/o sistema es que un usuario ejecute un archivo adjunto malicioso. Si bien existe la frase popularmente conocida que los usuarios son parte del eslabón más débil de la seguridad, mediante la concientización, se pueden convertir en la primera línea de defensa ante el ataque de un criptovirus.

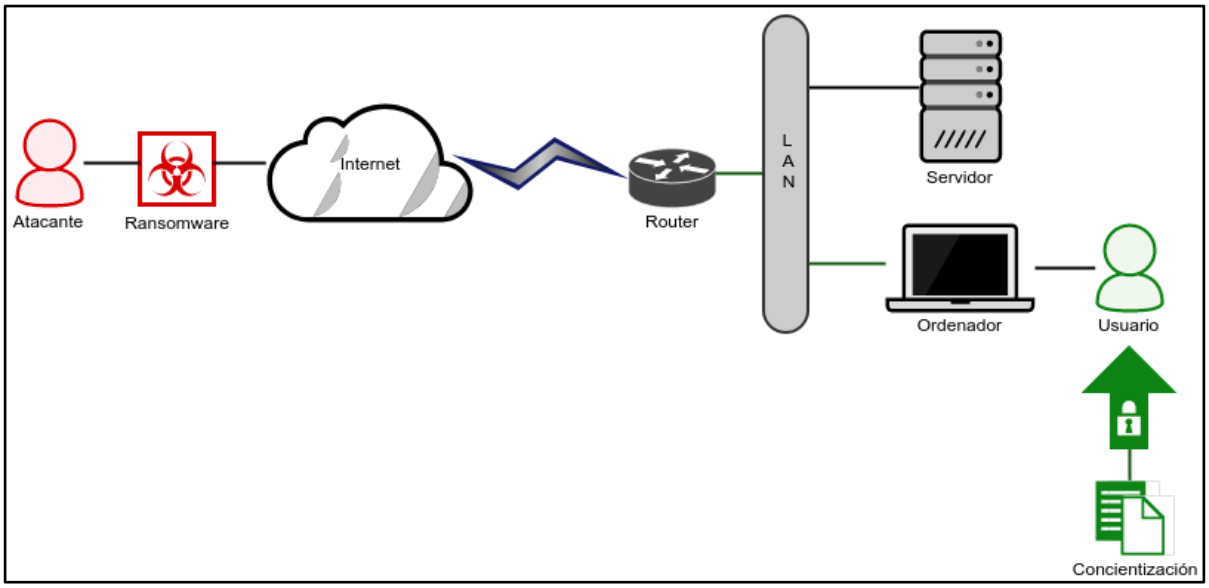


Imagen 22: Estrategia proactiva mediante Concientización

La capacitación, concientización y educación sobre qué es el ransomware, sus vectores de ataques e impacto que causa a los usuarios y a la organización harán que las personas entiendan que su comportamiento puede afectar a sus clientes, a su compañía y/o a ellos mismos. Permite que los usuarios tomen conciencia e incorporen medidas para protegerse, por ejemplo, evitando abrir archivos adjuntos inesperados de fuentes desconocidas [47].

CAPÍTULO 5. Estrategias de defensa reactivas

En esta sección se presentan las acciones que pueden llevarse a cabo una vez que el ransomware ha infectado el ordenador, red y/o sistema. El objetivo de las estrategias reactivas es que el usuario final recupere los archivos que han sido encriptados. El pago del rescate está fuera de análisis y no es considerado como una salida recomendable debido a dos motivos fundamentales: pagar fomenta este tipo de crímenes y no hay garantía de que los archivos sean descifrados luego de haber pagado.

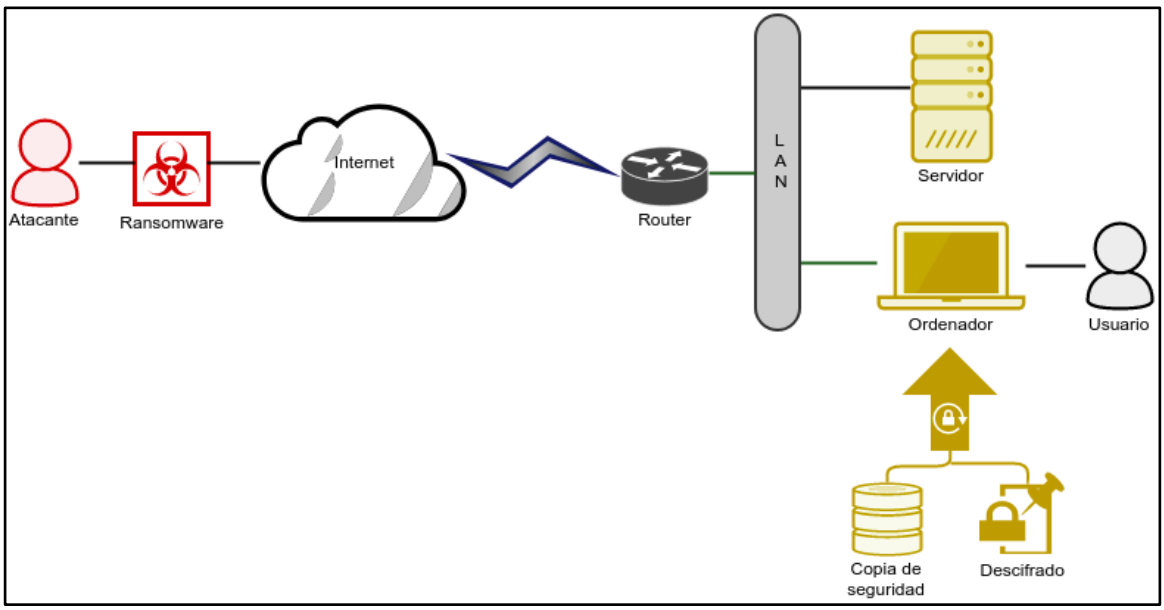


Imagen 23: Estrategias reactivas

5.1. Copias de seguridad

En caso de que se haya utilizado la estrategia proactiva de las copias de seguridad, al ser víctima de un ataque de ransomware, es posible restaurar los duplicados. La mayoría de las familias de este tipo de software malicioso están diseñadas para no ser destructivas, ya que deben permitir que luego del pago del rescate, se restaure el sistema. Esto hace que un ordenador infectado pueda restaurarse fácilmente desde una copia de seguridad [48]. El proceso de restauración de la copia dependerá del método (online u offline) y la herramienta utilizada para su ejecución.

5.2. Descifrado

Las compañías de antivirus ofrecen herramientas de descifrado de archivos infectados por ransomware de manera gratuita. Si bien es poco lo que se puede hacer cuando un criptovirus ha ingresado a nuestro ordenador o red (sin copias de seguridad disponibles), a veces es posible recuperar el acceso a los archivos encriptados gracias a estas herramientas. Son capaces de romper el cifrado debido a que los autores del malware cometieron un error de implementación, decidieron detener su distribución y lanzar una llave maestra, entre otros. La gran mutación y lanzamiento de nuevas familias de ransomware lleva a que este tipo de herramientas se encuentre en continuo desarrollo [49].

NoMoreRansom es un proyecto creado por las fuerzas y cuerpos de seguridad y las compañías tecnológicas de seguridad que tiene como objetivo ayudar a las víctimas del ransomware a recuperar la información encriptada, sin tener que pagar el rescate. Ofrece un conjunto de herramientas de descifrado categorizadas por la familia de ransomware que solucionan. Los programas disponibles han sido desarrollados por las compañías de seguridad de la información que son parte del proyecto [50].

CONCLUSIONES

El Ransomware es un software malicioso al que nos encontramos expuestos diariamente. Es una amenaza que ha crecido abruptamente en el último tiempo, por lo cual, requiere su respectiva atención y entendimiento del riesgo tanto por parte de administradores de seguridad como de usuarios finales. A continuación, se detallan las principales conclusiones obtenidas:

- Los cibercriminales se actualizan continuamente: Se ha explicado el impacto que tuvo el surgimiento de la deep web, TOR y las criptomonedas en las nuevas familias de ransomware. Los desarrolladores de este tipo de malware han aprovechado los beneficios que ofrecen estas nuevas tecnologías lanzadas, particularmente el anonimato, para potenciar sus ransomwares. Esto demuestra que los individuos y organizaciones que están detrás se encuentran a la vanguardia, evaluando qué nuevas características o funcionalidades pueden incorporar que les garantice mayor masividad o anonimato.
- Solo se necesita un clic para que el ransomware ingrese a la organización: Se han mencionado las distintas maneras en que el atacante puede lograr que el ransomware infecte a los usuarios. Si bien cuando el malware utiliza un exploit kit no se le puede atribuir mucha responsabilidad a la víctima, en el resto de los casos, los cuales corresponden a la mayoría de las infecciones, se dan debido a que un usuario ha hecho clic en un anuncio o ha descargado un archivo a partir de un phishing. Si se trata de un ordenador aislado, ese clic o acceso desencadena sólo la encripción de archivos que residen en ese ordenador. No obstante, cuando esto ocurre en un ordenador que es parte de una red corporativa, puede provocar una infección masiva de todos los ordenadores, siempre y cuando el ransomware sea capaz de replicarse.
- El software popular es el principal objetivo de ataque: Se han detallado ransomwares que han sido importantes debido a sus características y/o funcionalidades lanzados desde 1989 hasta la actualidad. En el recorrido de cada año hasta 2018, todos los

ransomwares más destacados afectan ordenadores con sistema operativo Windows, el cual es el más elegido por los usuarios a nivel mundial. Aunque esto no significa que existen ransomware sólo para Windows (de hecho, existen familias que afectan a otros sistemas operativos), muestra la tendencia y el principal objetivo de los desarrolladores de ransomware. Buscan afectar la mayor cantidad de usuarios posibles para que el impacto del ransomware sea masivo y sacar mejor rédito económico.

- No existe la panacea universal contra el ransomware: Se han presentado diferentes estrategias de defensa que pueden ser implementadas para proteger la información. Es importante resaltar que no existe una única medida que garantice efectivamente la protección frente al ransomware, sino que la seguridad se logra utilizando una combinación de las tácticas y herramientas mencionadas. Es recomendable establecer una seguridad por capas, incrementando la seguridad en la red (a través de la segmentación y dispositivos como IDS); ordenadores y servidores (con software de seguridad como anti-ransomware, mecanismos de actualización continua y copias de respaldo) y usuarios finales (mediante planes de concientización).

BIBLIOGRAFÍA

[1] A. Young and M. Yung, "Cryptovirology: extortion-based security threats and countermeasures," in *Proceedings 1996 IEEE Symposium on Security and Privacy*, Oakland, 1996.

[2] S. Morgan, "Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017," Cybersecurity Ventures, 18 Mayo 2017. [Online]. Available: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/. [Accessed 13 Octubre 2018].

[3] Symantec, "Internet Security Threat Report," Marzo 2018. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf. [Accessed 4 Octubre 2018].

[4] L. Orsolini, D. Papanti, F. Schifano and J. Corkery, "An insight into the deep web; why it matters for addiction psychiatry?," Human Psychopharmacology: Human and Experimental, 2017.

[5] J. Lansky, "Possible State Approaches to Cryptocurrencies," Journal of Systems Integration, 2018.

[6] Bitcoin Project, "Bitcoin - Open source P2P money," 2018. [Online]. Available: https://bitcoin.org/en. [Accessed 30 Marzo 2018].

[7] The Dash Network, "Dash Official Website," 2018. [Online]. Available: https://www.dash.org. [Accessed 25 Septiembre 2018].

[8] D. O'Brien, "Ransomware and Businesses 2016," Symantec Corporation, Mountain View, USA, 2016.

[9] E. Wilding, Ed."The authoritative international publication on computer virus prevention, recognition and removal," *Virus bulletin,* 1990.

[10] D. Nazarov and O. Emelyanova, "Blackmailer: the story of Gpcode," Kaspersky Lab, 26 June 2006. [Online]. Available: https://securelist.com/blackmailer-the-story-of-gpcode/36089. [Accessed 16 June 2018].

[11] M. James, "The evolution of Ransomware," ESET, [Online]. Available: http://www.infosecurityeurope.com/__novadocuments/89024?v=635703301368700000. [Accessed 20 June 2018].

[12] E. Vanderburg, "The evolution of a cybercrime: A timeline of ransomware advances," Carbonite, 28 Agosto 2017. [Online]. Available: https://www.carbonite.com/blog/article/2017/08/the-evolution-of-a-cybercrime-a-timeline-of-ransomware-advances. [Accessed 26 Junio 2018].

[13] F-Secure Labs, "MayArchive.B Description," 2006. [Online]. Available: https://www.f-secure.com/v-descs/mayarchive_b.shtml. [Accessed 3 Julio 2018].

[14] KnowBe4, "Gameover Zeus (GOZ)," [Online]. Available: https://www.knowbe4.com/gameover-zeus. [Accessed 23 Julio 2018].

[15] Avast, "CryptoLocker ransomware - what it is and how to protect your PC," [Online]. Available: https://www.avast.com/c-cryptolocker. [Accessed 2 Agosto 2018].

[16] Symantec, "Ransom.Cryptowall," 2014. [Online]. Available: https://www.symantec.com/security-center/writeup/2014-061923-2824-99. [Accessed 12 Agosto 2018].

[17] McAfee Labs, "Threat Advisory: Ransom Cryptowall," 22 Junio 2018. [Online]. Available: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25480/en_US/McAfee_Labs_Threat_Advisory-Ransom_Cryptowall.pdf. [Accessed 23 Agosto 2018].

[18] Dell SecureWorks Counter Threat Unit Threat Intelligence, "TeslaCrypt Ransomware Threat Analysis," 12 Mayo 2015. [Online]. Available: https://www.secureworks.com/research/teslacrypt-ransomware-threat-analysis. [Accessed 1 Septiembre 2018].

[19] L. Abrams, "TeslaCrypt shuts down and Releases Master Decryption Key," BleepingComputer, 18 Mayo 2016. [Online]. Available: https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/. [Accessed 17 Junio 2018].

[20] Avast Threat intelligence team, "A closer look at the Locky ransomware," 10 Marzo 2016. [Online]. Available: https://blog.avast.com/a-closer-look-at-the-locky-ransomware. [Accessed 3 Septiembre 2018].

[21] F. Sinitsyn, "Locky: the encryptor taking the world by storm," 6 Abril 2016. [Online]. Available: https://securelist.com/locky-the-encryptor-taking-the-world-by-storm/74398. [Accessed 12 Septiembre 2018].

[22] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 5, pp. 1938-1940, 2017.

[23] SecureWorks Counter Threat Unit, "WCry Ransomware Analysis," 18 Mayo 2017. [Online]. Available: https://www.secureworks.com/research/wcry-ransomware-analysis. [Accessed 29 Agosto 2018].

[24] "Stratosphere IPS," 2018. [Online]. Available: https://www.stratosphereips.org. [Accessed 14 Octubre 2018].

[25] The Cylance Threat Research Team, "Threat Spotlight: Inside the WannaCry Attack," 6 Junio 2017. [Online]. Available: https://threatvector.cylance.com/en_us/home/threat-spotlight-inside-the-wannacry-attack.html. [Accessed 20 Octubre 2018].

[26] D.-Y. Kao and S.-C. Hsiao, "The dynamic analysis of WannaCry

ransomware," in *International Conference on Advanced Communications Technology*, Chuncheon-si Gangwon-do, 2018.

[27] T. Boczan, "The Evolution of Gandcrab Ransomware," 5 Junio 2018. [Online]. Available: https://www.vmray.com/cyber-security-blog/gandcrab-ransomware-evolution-analysis/. [Accessed 23 Septiembre 2018].

[28] "No More Ransom project," 2017. [Online]. Available: https://www.nomoreransom.org. [Accessed 3 Octubre 2017].

[29] Malwarebytes Labs, "GandCrab ransomware distributed by RIG and GrandSoft exploit kits," 30 Enero 2018. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits. [Accessed 23 Septiembre 2018].

[30] C. Frenz and C. Diaz, "Anti-Ransomware Guide," OWASP, 2016.

[31] J. Castelli, "Choosing your anti-virus software," SANS Institute, 2002.

[32] "ClamAV - Open source antivirus engine," 2017. [Online]. Available: https://www.clamav.net. [Accessed 25 Septiembre 2017].

[33] G. Vasiliadis and S. Ioannidis, "GrAVity: A Massively Parallel Antivirus Engine," Creta, Grecia, 2010.

[34] G. V. Cormack, "Email Spam Filtering: A Systematic Review," *Foundations and Trends in Information Retrieval,* vol. 1, no. 4, pp. 335-455, 2008.

[35] The Apache Software Foundation, "Apache SpamAssassin," Apache, 2017. [Online]. Available: https://spamassassin.apache.org. [Accessed 20 Septiembre 2017].

[36] A. Schwartz, The Open Source Solution to SPAM, O'Reilly Media, 2009.

[37] R. Alvey, "The Art of Web Filtering," SANS Institute, 2004.

[38] Eyeo, "Adblock Plus - Surf the web without annoying ads," 2017. [Online]. Available: https://adblockplus.org. [Accessed 22 Octubre 2017].

[39] E. Pujol, O. Hohlfeld and A. Feldmann, "Annoyed Users: Ads and Ad-Block Usage in the Wild," in *IMC '15 Proceedings of the 2015 Internet Measurement Conference*, Tokio, 2015.

[40] E. Kolodenker, W. Koch, G. Stringhini and M. Egele, "PayBreak: Defense Against Cryptographic Ransomware," in *ASIA CCS '17 Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi, 2017.

[41] Malwarebytes, "Malwarebytes Endpoint Security vs. Ransomware," Santa Clara, 2016.

[42] KeepItSafe, "Understanding and Preventing Ransomware Attacks," 2016.

[43] ESET LA, "Guía de Ransomware," 2017.

[44] "Duplicati 2.0 - Free backup software," 2017. [Online]. Available:

https://www.duplicati.com. [Accessed 7 Octubre 2017].

[45] W. Davison, "Rsync - Open source utility," 2017. [Online]. Available: https://rsync.samba.org. [Accessed 4 Noviembre 2017].

[46] BackupAssist, "File Protection using Rsync," 2016.

[47] X. Luo and Q. Liao, "Awareness Education as the Key to Ransomware Prevention," *Information Systems Security,* vol. 16, no. 4, pp. 195-202, Julio 2007.

[48] A. Liska and T. Gallo, Ransomware: Defending Against Digital Extortion, O'Reilly Media, 2016, p. 190.

[49] N. Shah and M. Farik, "Ransomware - Threats, Vulnerabilities and Recommendations," *International Journal of Scientific & Technology Research,* vol. 6, no. 6, pp. 307-309, Junio 2017.

[50] F-Secure, "Ransomware: How to predict, prevent, detect & respond," 2016.