Proyecto Trabajo Final de Graduación

Ingeniería en Software

Proyecto de Investigación Aplicada (PIA)

Seguridad Informática: virus ransomware, el Secuestro virtual de datos es Posible

Medina Carranza, Facundo Martin

SOF00346

Fecha: 06/12/17

Tutora: Ing. Adriana Pérez

Dedicatoria

A los que me apoyaron en este arduo camino, a mi esposa Giuliana y a mi hijo Renzo que son mi inspiración. A mis padres que me acompañaron y a mi tía Silvia que *me tiró una soga* en el tramo final. Solo resta decir: Gracias a todos los que me bendijeron.

Resumen

El presente Trabajo Final de Grado se enfoca en el estudio del malware[1] llamado ransomware[2]. Para ello se utilizaron las siguientes herramientas de investigación: entrevista, observación, búsqueda de información bibliográfica y documental, pruebas y análisis del ransomware.

El objetivo fue determinar cómo ransomware se infiltra en las empresas, estudiando las técnicas utilizadas por los ciberdelicuentes.

La primera parte del trabajo se enfoca en explicar qué es el ransomware, su historia, las diferentes versiones, sus características generales, su propósito y estadísticas de los ataques que realizó a usuarios y empresas.

En la segunda parte se incluye una breve reflexión sobre algunas organizaciones que podrían ser víctimas del ransomware.

Por otro lado, en la tercera parte se profundiza sobre las medidas de seguridad que debería tener mínimamente la empresa u organización para reducir los riesgos de infección de cualquier malware.

Como medida para entender mejor el funcionamiento del ransomware, se estudiaron dos versiones: Hidden Tear y Eda2. Éstos fueron lanzados como código abierto por el experto de seguridad Utkusen, para lo cual se procedió a un análisis del código y su funcionamiento por medio de una máquina virtual.

[1] Código malicioso que intenta infiltrarse o dañar una computadora.
[2] Software que secuestra los archivos y pide un rescate por una suma de dinero.

Para finalizar, se realizaron entrevistas a diferentes organizaciones radicadas en la Ciudad de Córdoba: Municipalidad de Córdoba, Globant, La Lacteo, Tarjeta Naranja y Sanatorio Allende. Estas entrevistas tienen como finalidad conocer la preparación en cuanto a seguridad informática se refiere, y si además el ransomware las afectó.

Con la recopilación de información y análisis del ransomware, se realizó el trabajo final en el cual se obtuvieron conclusiones que cumplen con el objetivo propuesto.

Con el avance exponencial que existe en la Informática, se sugiere continuar investigando este tema, ya que no solo el secuestro de datos está en riesgo, sino también el de objetos tecnológicos que tengan conexión a Internet.

Palabras clave: Ransomware, Seguridad, Datos, Empresa, Pérdida de información

Abstract

This work focusses on the study of the malware called “ransomware”. To carry on this study, certain investigation tolls were used: interview, observation, bibliographic and documentary information searching, tests and analysis on the ransomware.

The objective is to determine how ransomware infiltrates into the companies through the study of the techniques used by cybercriminals.

The first part of this work is devoted to the explanation of what is the ransomware, its history, the different versions, its general characteristics, its purpose and some statistics of the attacks made to users and companies.

The second part includes a brief reflection about some organizations as potential victims of ransomware.

The third part deals with security measures that companies or organizations should consider to minimize infection risks by any kind of malware.

So as to better understand the ransomware’s functioning, two versions will be studied: “Hidden Tear” and “Eda2”, both known as open codes by the security expert Utkusen. A code analysis and a study of its functioning will be implemented by a virtual machine.

To conclude, several interviews were carried out to local organizations from the city of Córdoba: Municipalidad de Córdoba, Globant, La Lacteo, Tarjeta Naranja and Sanatorio Allende. These interviews’ goals were to know about their informatic security measures and to know if they have been affected by the ransomware.

Based on the information and analysis of the ransomware, the final work was achieved, by which conclusions were obtained, meeting the proposed goal.

Because of the exponential information technology progress, it is suggested to continue investigating the topic in depth, since not only the data is at risk of a hijack, but also the technologic objects connected on the Internet.

Keywords: Ransomware, Security, Data, Organizations, Information loss.

Tabla de contenido

Tabla de figuras

Tablas

Seguridad Informática: virus ransomware, el secuestro de datos es posible

1. Introducción - Marco de referencia institucional

En el mundo globalizado de hoy, el crecimiento exponencial de Internet y de las redes de comunicación han contribuido a guardar la información ya no en papel, sino en archivos digitales, por lo que usuarios de computadoras o celulares inteligentes, y empresas al estar conectados en la Red de Redes pueden sufrir ataques a sus datos. De ahí surge la importancia de la Seguridad Informática para colocar un muro a estos ataques y proteger tales datos.

La Seguridad, como nos indican Buecker et al. en su libro *IBM Security Solutions Architecture for Network, Server, and Endpoint* está focalizada en la Confidencialidad, la Integridad y la Disponibilidad. La Confidencialidad es proteger el acceso de los datos para que solo puedan leerlas personas autorizadas, la Integridad es el cuidar que los datos los modifique solo la gente autorizada, y la Disponibilidad es que los datos estén accesibles para la gente autorizada en todo momento. Si se sostienen estos requisitos cumplimos con la Seguridad Informática, pero ¿qué pasa cuando un usuario con autorización para entrar a esos datos, recibe un correo con un archivo malicioso y lo ejecuta?, toda la seguridad que implementamos, todo el presupuesto que gastamos para tener esa seguridad en un segundo se desvanecen (p 128).

Como plantea Fabián Portantier en *Seguridad Informática* (2012, p. 29) no se puede llegar a la perfección, pero con una mejora continua en la seguridad, al menos se debe intentar ser casi infalible, por lo que el proceso nunca termina y siempre hay algo para mejorar. En esta dirección el objetivo de este trabajo final es conocer en profundidad el virus ransomware, su historia,

funcionamiento y cómo evolucionó en tan corto tiempo, a tal punto de que es uno de los más usados por los ciberdelicuentes.

Esta investigación se realizó en la Ciudad de Córdoba, recolectando información bibliográfica de textos escritos e Internet sobre Seguridad Informática, a la vez que se ejecutaron pruebas de muestras de ransomware y se entrevistó a informantes clave de distintas empresas de la Ciudad sobre esta problemática.

1.1 Antecedentes

En el siguiente apartado se optó por describir algunos trabajos llevados a cabo en diferentes regiones geográficas que abordan, de distintas formas, la problemática de los sistemas de detección de virus y la seguridad en los sistemas informáticos. Dichos estudios se consideran relevantes y significativos para el proyecto de aplicación profesional que se desarrolla.

Cabe destacar que no se incluyen antecedentes de nuestro contexto, porque del rastreo bibliográfico realizado se puede afirmar que son escasos los estudios realizados, o al menos publicados.

La investigación titulada *Cryptovirology*[3]*: Extortion-Based Security Threats and Countermeasures* (Adam Young, 1996) llevada a cabo por Adam Young y Moti Yung, investigadores de seguridad informática estadunidenses, revela cómo la criptografía en malas podía ser un arma muy peligrosa. Definen al **Cryptovirus** como la utilización de la criptografía aplicada en un virus de computadora. En la primera parte de la investigación advierte cómo un programa malicioso puede sobrevivir en el anfitrión, como una Computadora o Servidor, sin ser detectado, para posteriormente realizar cambios en el sistema. En la segunda parte, se dan

[3] Cryptovirology: Virus criptográfico, en donde se utiliza la criptografía en un virus informático.

ejemplos de ataques criptográficos, en los que el autor del virus posee la clave privada y se demuestra que de esa forma pueden encriptar los archivos para extorsionar a las personas. Esta fue una de las primeras investigaciones sobre este fenómeno informático, cuando aún no existía el nombre ransomware.

Otra de las investigaciones que se realizó sobre ransomware fue presentada en una revista de investigación del Instituto Tecnológico de Mérida, México titulada *Origen y Evolución del Cryptovirus Ransomware* (Martinez-García & Moo Medina, 2016). En este caso, se explica el origen del ransomware y su evolución en el tiempo, cómo funciona y el crecimiento de ataques de este tipo en el último tiempo. Enfatizan sobre la problemática que puede traer a las empresas e instituciones que no tomen medidas para proteger sus datos, ya que luego de perdidos asumen la verdadera dimensión del daño producido. También advierten que los usuarios deben ser educados sobre este tema para minimizar los riesgos de ser infectados.

Exponen al ransomware como un servicio que ofrecen los ciberdelicuentes, para que cualquier usuario sin necesidad de que tengan conocimientos de programación, pueda infectar a otros sistemas pidiendo un rescate por los archivos secuestrados. Con este mecanismo ganan tanto el afiliado del servicio como el creador de éste.

Una investigación también muy interesante se presenta en una revista de la India de Ciencia y Tecnología titulada *Ransomware Digital Extortion: A Rising New Age Threat* (Akashdeep Bhardwaj, 2016), en la que se presenta al ransomware explicando qué es y cómo se propaga, pero además recopila soluciones para contrarrestar el malware. Proponen un ambiente de detección de malware en la nube con tres diferentes ambientes de análisis, con lo que, según la investigación, se consigue detectar más rápido el malware. El malware cuando es detectado ya

no puede ingresar a otros huéspedes que tengan esta solución instalada, ya que por medio de la utilización de la nube como medio de comunicación y recopilación de información se evita su propagación.

Ransomware (del inglés ransom: rescate y ware: equipo) es un malware conocido desde 2011 que secuestra el equipo informático por medio de artilugios como bloqueo de pantalla o encriptamiento de archivos por medio de la criptografía. Uno de los primeros métodos que utilizó este código malicioso es mostrar en la pantalla del equipo infectado un mensaje engañoso, en el que argumenta que es la policía del país donde se encuentra el equipo, y alega que el usuario había ingresado en páginas de pornografía infantil o alguna otra página con contenido vergonzoso para la persona. El usuario no puede eliminar el mensaje, ya que la computadora está bloqueada y le advierten que, si no paga una suma de dinero en 24 horas, le borran el disco duro. Por eso, las primeras variantes informadas de este virus llamado en ese entonces "El virus de la policía" (Brulez, 2011) datan de marzo de 2011 según reportes de Kasperky Labs provenientes de la Policía alemana.

Posteriormente en el año 2012, fueron surgiendo variantes como Locked y SGAE con nuevas características como encriptación de los archivos.

En el año 2014, aparecieron nuevos ransomware como CryptoDefense, CryptoLocker y Cryptowall, este último es el más potente de los tres que, en su versión Cryptowall 3.0 según El Confidencial en su artículo *Como el Ransomware se esta convirtiendo en la mayor amenaza de Internet*, consiguió alrededor de 325 millones de dólares en rescate y estiman que la versión 4.0 conseguirá mucho más (Ferrer, 2015).

Finalmente, resulta significativo destacar que el año 2016 ha sido definido por la mayoría de los expertos en seguridad como el “Año del ransomware” trayendo muchas dificultades y conflictos a usuarios y empresas, y a su vez muchos beneficios a los atacantes.

1.2 Descripción del área problemática

El ransomware afecta a cualquier computadora, servidor o celular inteligente en el mundo. Esto ocurre tan solo con ejecutar algún archivo que puede ser enviado por protocolo IRC (Internet Relay Chat), correo electrónico, redes peer to peer (red entre pares), grupos de noticias, entre otros.

Esta problemática viene aumentando cada año según Kaspersky Lab, uno de los proveedores más importantes en el mundo de protección TI. Entre 2014 y 2015 hubo 131,111 ataques de ransomware, en cambio entre 2015 y 2016 hubo 718,536 ataques (SecureList, 2016) por lo que se quintuplicaron los números de ataques, infectando tanto a computadoras personales como a las de empresas de todo tipo. El circuito planteado se completa exigiendo dinero para recuperar los datos encriptados, en donde muchas veces a pesar de pagar el rescate no recuperan los datos, ocasionando el posterior formateo de la computadora y perdiendo toda la información de la misma.

1.3 Formulación de la problemática

¿Cuáles son los factores por los que el ransomware penetra en la seguridad de las empresas?

1.4 Justificación

Este trabajo final de grado se realiza con el objeto de estudiar al ransomware para aportar conocimiento sobre este malware que actualmente está en expansión, y dirigiendo cada vez más

sus ataques a empresas y áreas gubernamentales, las que podrían sufrir cifrado de sus archivos, y la posterior pérdida de datos.

Las empresas recopilan los datos necesarios para funcionar. Éstos deben estar protegidos de toda amenaza interna o externa, manteniéndolos confidenciales, íntegros y disponibles (Buecker, A. et al., 2012). Dentro de la información almacenada por las empresas puede haber datos personales (de clientes, empleados), que en Argentina están protegidos por la ley Nº25.236 llamada "Protección de los datos personales", y en su artículo 9º expresa que cualquier persona que tenga algún archivo de datos personales debe asegurar que no sea adulterado o perdido, por lo tanto las empresas no pueden permitir que los archivos que contengan datos personales sean encriptados por un ransomware (Nación, 2000).

Las empresas deben informarse y asignar recursos para implementar las medidas de seguridad necesarias, pero como dice Portantier (2012, p. 17) no existe una organización donde su objetivo principal sea la seguridad informática.

Este trabajo pretende dar a conocer el funcionamiento del ransomware, cómo se infiltra en las organizaciones y qué medidas de seguridad informática se deben tener en cuenta.

Investigarlo exhaustivamente servirá para identificar posibles patrones de comportamiento, y de este modo poder ayudar a su detección temprana. Es mucho más fácil y eficaz prevenir que reparar los daños ocasionados.

1.5 Objetivo general

Analizar los efectos del virus ransomware en las empresas realizando recopilación bibliográfica de su surgimiento, métodos utilizados y evolución del malware en el tiempo.

Además, obtener opiniones y experiencias entrevistando a informantes clave y concluir con pruebas de código de forma estática y dinámica para conocer y evaluar su comportamiento.

1.6 Objetivos específicos

Describir las manifestaciones del virus ransomware en organizaciones de la Ciudad de Córdoba.

Identificar las distintas versiones y funcionamiento del ransomware.

Enumerar las distintas soluciones para recuperar los archivos infectados.

Evaluar el impacto de cómo ransomware afecta a empresas y organizaciones.

2. Marco teórico

2.1 Presentación

La presente investigación se centrará en el análisis del virus ransomware y sus efectos socioeconómicos. Al concepto de malware Buecker, A. et al. lo define como un programa o macro malicioso que puede ser ejecutado en la mayoría de las computadoras (2012, p. 129). El ransomware por lo tanto es un programa malicioso que infecta a los archivos, principalmente a los documentos de procesadores de texto u hojas de cálculo.

Las empresas han cambiado drásticamente la forma en que almacenan la información pasando del guardar copias en papel a los archivos de computadora, por lo que para asegurar que no se pierdan, deben destinar tanto recursos materiales como personal y tiempo. En esta dirección Fabián Martínez Portantier, un experto en seguridad informática, nos dice “no es tan importante

la cantidad de recursos que invertimos, sino que debemos considerar la inteligencia con la cual implementamos dichas medidas" (2012, p. 17).

Cabe destacar que cuando un usuario corporativo abre un archivo ejecutable con este virus puede infectar a toda una empresa y a más de 400.000 archivos, como el caso de la Institución Ferial de Madrid (IFEMA) y que fue informado por medios como el diario El País (Barroso, 2015). A pesar de que las empresas habían advertido de estos mails enviados "supuestamente" por CORREOS (Empresa de Correo Española), bastó con que un solo usuario desinformado ejecute el archivo, infectando a la mayor parte de la empresa.

Resulta interesante interrogarse sobre: ¿Por qué los antivirus no pueden detener el ataque? Evan Davidson, Vicepresidente de Ventas, EMEA, en Cylance, una empresa estadounidense de Ciberseguridad, nos explica que los antivirus ya no resultan suficientes, con tantas mutaciones de virus, y se requiere estar por demás infectado para protegerte (Pizarro, 2016). Esto lo explica de este modo porque los antivirus buscan patrones similares para detectar los programas maliciosos, pero cuando mutan muchas veces no se los puede detectar, y se ejecutan en la computadora causando grandes inconvenientes.

Entonces, para que las empresas no estén tan vulnerables, una de las primeras medidas es la capacitación del personal para que verifiquen antes los archivos recibidos, de este modo, transformarlos como si fueras un investigador que tienes que verificar la fuente. En esta dirección, como explica Portantier (Seguridad Informatica por Fabian Portantier, 2012, pág. 21), la NSA(Agencia de Seguridad Nacional de Estados Unidos) existe una estrategia de enfoque por capas, en que la capa externa es la capacitación del personal, la capa media son las políticas y procedimientos de seguridad, y la capa interna es la seguridad física. En lo cual si una capa falla

existe otra para detectar la amenaza, y si todas las capas fallan se debe tener un respaldo para recuperarse de dichos ataques.

El problema radica cuando no se tiene un respaldo de los datos, y las empresas poseen datos tan importantes como para estar obligadas a pagar el rescate que se les solicita, a pesar de que advierten que por esto el negocio para los hackers es tan lucrativo, aunque muchas otras no tienen el dinero para costearlo. Tal es así que un experto en seguridad informática, Yago Jesús, autor de Anti-Ransom, comentó "Hice esta herramienta cuando vi la desesperación que genera ese tipo de amenaza. Encontrarte a toda una mujer de 4x años, llorando y diciendo que, o recuperaba sus datos, o cerraba una empresa con varios empleados, me impactó bastante" (Ferrer, 2015, https://goo.gl/Byg5vi).

Encontrar a estos denominados ciberdelicuentes no es una tarea fácil, sobre todo cuando dejaron de utilizar transferencias bancarias, como sí lo hizo el grupo de hackers ucranianos que fue atrapado por la policía de España en 2013 (Policía Nacional, 2013, https://goo.gl/FGR5Ef) gracias a que rastrearon las transferencias bancarias que realizaron las víctimas. Esto fue rápidamente aprendido por los hackers, y en cambio, ahora la moneda que solicitan se llama bitcoin, que es una moneda virtual que tiene un valor aproximado de USD 917 cada uno. Operan con diversas herramientas como el mezclador de direcciones que, como explican en Bitcoin.org, cuando se envían los bitcoins anónimamente a un destinatario, el mezclador lo desvía hacia una billetera compartida, para luego enviar al destinatario otras monedas diferentes que contenía la billetera, así cortar cualquier relación entre el emisor y destinatario (Majamalu, 2012). A la vez que utilizan la red TOR, una red que permite no revelar la identidad de los usuarios, es decir, su IP, ya que los mensajes están protegidos por diferentes capas de encriptación. Este mensaje encriptado viaja por una red de nodos, en la cual en cada comunicación cambia el camino, por lo

que hace mucho más complicado el rastreo de los atacantes. Resulta contradictorio e irónico saber que, por un malware, alguien puede ser infectado para pedirle dinero, y por otro, detectar esa situación. Un ejemplo de lo planteado es el malware que utilizó el experto en Ciberseguridad Matt Edman (O'Neill, 2016) para encontrar la IP de los usuarios de la red TOR, y dejar al descubierto a los ciberdelicuentes. Esto demuestra que siempre se encuentran nuevas formas de reproducir este circuito entre el ataque y su detección.

Como se observa, este malware puede provocar mucho daño al punto de hacer quebrar una empresa, por lo que, en el mundo de la Seguridad Informática, toma cada vez más trascendencia buscar formas para detectarlo. Al punto que la empresa Cylance por medio del Director de ventas Lloyd Webb dice “mientras que 2015 fue el año de las mega intrusiones, como Sony y Ashley Madison, 2016 es el año del ransomware, que se está convirtiendo en una actividad altamente lucrativa para los cibercriminales” (Pizarro, 2016, https://goo.gl/ApFdNm).

Cabe destacar que varios expertos en el campo de la informática plantean que cuestiones más complejas y negativas podrían estar por llegar, ya que como afirma Florián Manuel Pérez Sánchez “el día que opten por cifrar documentos de CAD/CAM o código fuentes de aplicaciones o código ya compilado y en ejecución, los efectos pueden ser catastróficos” (Florián Manuel Pérez Sánchez, 2015, https://goo.gl/dbUWqA).

2.2 Desarrollo del marco teórico

A partir de las decisiones teóricas metodológicas planteadas en los apartados siguientes y con la intencionalidad de profundizar la información, es que a continuación se desarrollarán nociones centrales alrededor del tema objeto de este trabajo final.

El recorrido incluye tres ejes temáticos:

El primer eje está relacionado con ransomware, sus característicos modos de funcionamiento, tipos, posibles vías de contagio, la historia de surgimiento, y las estadísticas de ataque del ransomware.

Luego, como segundo eje de contenido, se incluye una breve reflexión sobre algunas organizaciones que podrían ser víctimas del ransomware, en particular las vinculadas al servicio de Salud por la relevancia que cumplen en la sociedad.

Finalmente, como tercer eje, se plantean cuestiones alrededor de los sistemas de seguridad, y también de prevención en relación al malware.

3. Metodología

La metodología hace referencia al conjunto de métodos, tareas, habilidades, conocimientos y tareas, utilizados para lograr los objetivos planteados. En este apartado se mencionarán todas las herramientas metodológicas que se utilizarán en esta investigación.

3.1 Paradigma metodológico

En el presente trabajo se desarrolla una indagación de corte descriptiva que utiliza una metodología combinada. Por un lado, se recupera bibliografía (especialmente publicaciones respecto al problema definido) donde también se recuperan algunos datos estadísticos, por el otro, se diseñan y suministran entrevistas a informantes clave al fin de recuperar sentidos y significados, que no tienen una pretensión de muestra estadística sino más bien la posibilidad de recuperar las voces de protagonistas desde su propio lugar de trabajo. Además, desde el punto de vista técnico se incluyen pruebas de ejecución y su análisis a la manera de una experimentación y observación de los resultados obtenidos.

3.2 Carácter y diseño de la investigación

La investigación utilizará la lógica inductiva de forma de experimentación y observación del comportamiento del ransomware sobre todo en las empresas y usuarios, buscando patrones similares de los distintos tipos, y así poder hacer una descripción del virus y cómo afecta a las distintas organizaciones.

3.3 Fuentes de información

La fuente primaria será la lectura de registros escritos como libros, revista científicas, o fuentes confiables, además de empresas de seguridad que contienen estadísticas de ataques de ransomware, ya que no se cuenta con una organización que nuclee las estadísticas de ataques de malware. La secundaria será entrevistas a personal de seguridad informática de empresas y/o organizaciones de la Ciudad de Córdoba, también se utilizará la observación y prueba controlada del virus como funciona y su estructura interna.

Ficha técnica

Tipo de investigación	Descriptiva
Metodología	Cualitativa
Técnicas de investigación	Entrevista, Observación
Instrumento	Cuestionario de Entrevistas, Fichas de Observación
Población/ Corpus de análisis	Varones y Mujeres que trabajen en la parte de seguridad de empresas
Muestra/ Recorte del corpus	5 empleados de seguridad de empresas erradicadas en Córdoba
Criterio muestral	No Probabilístico.

4. Qué es un ransomware

El ransomware es un tipo de malware o programa infeccioso que al ejecutarse se infiltra en el sistema, y empaqueta los archivos para encriptarlos, luego elimina los archivos originales, haciendo imposible acceder a ellos, a menos que se pague un rescate (Buecker, A. et al., 2011).

Ahora bien, el interrogante es acerca de cómo funciona, y para aproximar algunas respuestas recuperamos lo que describe la revista científica *Indian Jornal of Science and Technology*, respecto a que existen dos grandes tipos de ransomware: los bloqueadores y los cifradores (Akashdeep Bhardwaj, 2016).

Uno de ellos es el denominado Lock screen (bloquea pantalla): Su función es bloquear la pantalla sin poder realizar ninguna acción, el Lock screen al infectar la máquina presenta en la pantalla del monitor un mensaje intimidatorio de la policía local, interpol o FBI (como en la Figura 1) dependiendo de la ubicación de la computadora.

Figura 1. Mensaje engañoso de ransomware. **(Security, 2013)**.

Exige un pago para desbloquearla, y advierte que si la computadora es desconectada no podrá volver a arrancar. Lo positivo de este tipo de ataque es que el ransomware no encripta los archivos, y se puede recuperar la información del disco duro, aunque se debe formatear e instalar el sistema operativo nuevamente. Por lo cual, el impacto de este tipo de versión es bajo, a menos que el usuario (por desconocimiento y miedo) haga el pago solicitado.

Respecto al clasificado como Cifrador: Su funcionamiento es parecido al "bloqueador". Según lo que dice Emiliano Piscitelli en *Ransomware: Qué es y cómo funciona el secuestro digital* (2015), generalmente lo primero que realiza es instalarse en alguna carpeta (como Mis Documentos) con un nombre aleatorio, para luego crear en el registro de Windows una entrada por si el equipo se apaga, y así cuando vuelve a encender se active nuevamente el ransomware. Al activarse, intenta comunicarse con los servidores de Comando y Control (C&C) que como explica Command Five (Command and Control in the Fifth Domain, 2012), organización de servicios y tecnologías de la información, son servidores que utilizan los hackers para controlar los malware, en general estos servidores son botnets[4], por lo que dificulta el rastreo del atacante y así puede mantener su anonimato. La mayoría de los ransomware al conectarse con el servidor C&C, solicitan las claves de cifrado, una "Pública" y otra "Privada", en el que utiliza algún algoritmo de cifrado como el RSA de 2048 bits (Emiliano Piscitelli, 2015). Con la clave pública empaqueta los archivos importantes encriptándolos, borrando luego los archivos originales. Además, si la computadora se encuentra en una red local con unidades mapeadas (carpetas guardadas en otro equipo que son copiadas para un acceso más rápido) u otros dispositivos externos (disco duro externo, usb) hasta los archivos de la nube (Dropbox, Google Drive) pueden sufrir también la encriptación de los datos, por lo que no se recomienda guardar las copias de

[4] Robots informáticos que se ejecutan de manera autónoma y automática en máquinas infectadas en forma remota.

respaldo en dichas unidades. Si el cifrado tuvo éxito, la única forma de recupero de los archivos es obteniendo la clave privada que se encuentra en el servidor C&C. Al finalizar el trabajo el ransomware crea unos archivos en diferentes formatos (.pdf, .txt, .doc) con un mensaje pidiendo un pago para recuperar los archivos.

4.1 ¿Cuáles son las vías de contagio?

El Centro Criptológico Nacional de España explica que existen muchas vías de contagio, una de las más comunes es por medio del correo electrónico, en donde utilizan técnicas de ingeniería social como se ve en la figura 2.

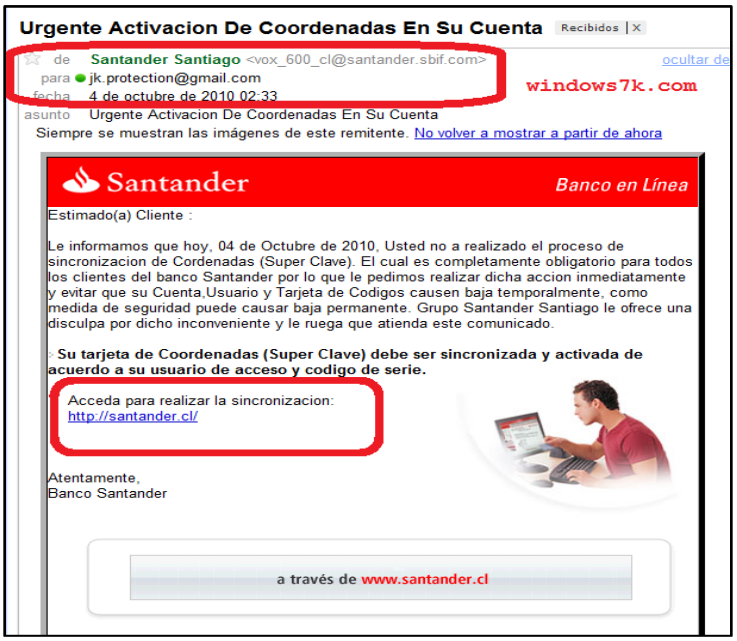


Figura 2. Email engañoso usando ingeniería social. (Windows 7k, 2010).

Intentan engañar al usuario para que descargue un archivo adjunto, o como en este caso utilizando el phising o suplantación de identidad, en donde el pescador (phiser) se hace pasar por alguna compañía conocida utilizando logotipos y un mensaje bastante creíble para que la víctima ingrese a una URL. Esa URL lo redirige a un sitio web fraudulento, muy parecido al verdadero,

para robar información como el usuario o contraseña (Centro Criptológico Nacional, 2016). Según lo que detalla Emiliano Piscitelli, experto de seguridad, uno de los más eficaces ataques para infectar de ransomware a las empresas es enviar un correo con un asunto como currículum o búsqueda de trabajo (que puede ser enviado por ejemplo a un departamento de recursos humanos de una empresa), que contiene un archivo adjunto con doble extensión como "curriculum.pdf.exe" para que luzca como un documento pdf. Lo anterior sucede porque Windows tiene pre activado el ocultamiento de la extensión, y entonces el usuario vería al archivo como "curriculum.pdf", pero en realidad es un ejecutable que al activarlo comienza a correr el malware por la computadora (Emiliano Piscitelli, 2015), infectándola para que luego aparezca un mensaje que informa que los datos personales han sido encriptados, como muestra la figura 3.

Figura 3. Mensaje de CryptoLocker pidiendo el pago para rescatar los archivos del dispositivo (Piscitelli, 2015).

Otro medio de contagio, utilizado por los ciberdelicuentes, son los web exploit kits, que, como también detalla el CCN-CERT, son herramientas que buscan vulnerabilidades en el sistema, sobre todo en los navegadores y programas que utilizan Adobe Reader, Java o Adobe Flash Player, que al lograr atacar y tomar el control de la computadora pueden instalar por ejemplo un ransomware (Centro Criptológico Nacional, 2016).

También existen formas de contagio en la que el culpable no es el empleado de la empresa, sino como nos indica el reporte de F-Secure (State of Cyber Security, 2017, pág. 22) las empresas al estar constantemente compitiendo e intentando innovar, buscan maneras más rápidas de llegar a los objetivos, por lo que muchas veces contratan servicios de consultores externos para implementar mejoras, los cuales tienen acceso total al sistema y pueden ocasionar una vulnerabilidad. Un ejemplo de lo anterior es si se infecta la computadora del consultor que está conectado a la red de la empresa, el ransomware se puede expandir a través de ella. Otra amenaza que puede ocasionar el uso de empresas tercerizadas es cuando se implementan sistemas o aplicaciones con backdoor[5] como nos dicen Chris Wysopal y Chris Eng (Static Detection of Application Backdoors, 2007) en su artículo en que se refiere al backdoor, y lo clasifica en 3 categorías:

1. System backdoors: en los que el atacante crea el sistema de backdoor cuando consigue entrar al sistema por medio de una vulnerabilidad o ingeniería social, con esto logra que, a pesar de que la misma es reparada, pueda ingresar de todos modos al sistema.
2. Aplication backdoors: es una versión legítima del programa, pero que ha sido modificado para no tener que pasar por los mecanismos de seguridad, y así el operador

[5] Significa “puerta trasera”.

del sistema pueda ingresar más rápido, aunque pueda comprometer al sistema ya que cualquier hacker logrará descubrirlo y utilizarlo.

3. Crypto backdoors: a un sistema de encriptación como RSA, se le coloca una vulnerabilidad para que, al vender el programa con el sistema de encriptación, el creador de ese programa pueda leer los mensajes encriptados a pesar de no tener la clave secreta.

5. Historia del ransomware

Luego de aproximarnos a la noción de ransomware, sus características y a las posibles vías de contagio, resulta importante contextualizar y plantear una breve historización sobre su surgimiento y desarrollo.

El ransomware se hace conocido por la sociedad en 2011, con la aparición del famoso "Virus de la Policía", pero no es el primero en aparecer, ya que en 1989 según Gazet (2010) hubo un envío masivo de discos flexibles de 3 ½ por correo postal, que contenían "supuestamente" información que podría ayudar a encontrar una cura contra una enfermedad. Al utilizar esta ingeniería social, el atacante conseguía infectar la computadora y luego de 90 reinicios, el virus cifraba los archivos y aplicaciones dejándolos inutilizables. Solo se visualizaba en la pantalla el archivo de licencia que solicitaba el pago para rescatar los archivos y aplicaciones por medio de un cheque a nombre de "Pc Cyborg Corporation", aunque todavía no existía la palabra "ransomware", este malware llamado "AIDS info disk" o "PC Cyborg Trojan" fue el primer antecedente.

A principios de la década del 90 apareció otro malware que realizaba acciones parecidas a los ransomware actuales, éste se llamaba Virus del Casino que como explica la empresa ESET

(2015) si la computadora estaba infectada, en una determinada fecha el virus se activaba y copiaba la tabla de asignación de archivos[6] en la memoria RAM[7] para luego borrar la tabla de asignación, y luego invitaba a jugar a una máquina de tragamonedas en la pantalla en la que daba 5 oportunidades y, si el usuario no ganaba, borraba la tabla FAT de la memoria RAM haciendo perder todos los archivos y obligando a reinstalar el sistema operativo.

Otro llamado One Half (ESET, 2014) surgió en 1994 en donde cifraba la primera parte de los sectores del disco rígido logrando que no pudiera arrancar la máquina.

Los piratas informáticos de los 90 como cuenta Merce Molist Ferrer (Hackstory, 2012, pág. 40), buscaban como conectarse a la red de redes utilizando sobretodo ingeniería social para luego entrar a cualquier universidad o empresa, e investigar los sistemas operativos para conseguir nuevos conocimientos, pero nunca con una intencionalidad o mentalidad delictiva. Un ejemplo de que los "Hackers" de esa época solo buscaban conocimiento y prestigio al crear estos virus es que lo consideraban como un arte, como si pintaran un Picasso o un Rembrandt les ponían sus propias firmas a los virus y los publicaban en la web (Ferrer, Hackstory, 2012, pág. 83), en forma de revista donde publicaban artículos con códigos de virus. Por lo expresado, muchas veces les costaba que los atraparan por publicar virus que utilizaban personas que solo les interesaba hacer daño.

Con el cambio de siglo hubo grandes avances en la tecnología y en la informatización en un mundo cada vez más globalizado, esto hizo que paulatinamente el Estado, los bancos y las empresas hayan "volcado sus procesos de negocio netamente a los sistemas de información"

[6] Índice donde señala que en que parte del disco duro comienza y termina un archivo creado por Windows para MS-DOS (https://es.wikipedia.org/wiki/Tabla_de_asignaci%C3%B3n_de_archivos).
[7] Memoria volátil que guarda información para poder acceder más rápido, cuando se apaga el ordenador al ser volátil se borra todo lo que tenía guardado.

(Portantier, 2012, pág. 26). Este fenómeno trajo cambios, como explica Portantier, antes se guardaba la información en formato papel para luego leerlo, copiarlo o destruirlo, y ahora la información son bits (0 y 1) guardados en distintos tipos de almacenamiento como memorias USB, discos duros, etc. que generalmente están conectados a la red de redes.

En una época donde cualquier persona puede ingresar a internet y conseguir información, como los "Hackers", esto también es aprovechado por los ciberdelicuentes que utilizan cualquier medio para atacar a las empresas e ingresar a sus sistemas, y así conseguir réditos económicos. Los organismos, al verse afectados por los ataques tuvieron y tienen que invertir en productos y servicios de seguridad informática para protegerse de estos ataques. Muchas empresas deben haber tenido en cuenta el lema de Sun Tzu que dice: "Siempre mantén a tus amigos cerca, pero aún más cerca a tus enemigos" (El Arte de la Guerra, 500 A.C.). En esta dirección, algunas empresas implementaron la contratación de ex "Hackers" como Kevin Mitnick (Portantier, 2012, pág. 18) para aprender de ellos, entender cómo piensan y actúan, para así encontrar las amenazas y vulnerabilidades del sistema, resultando esto una gran estrategia para comprender mejor cómo defenderse.

Estos cambios que implementaron las empresas en seguridad lograron que no fuera tan sencillo que un ciberdelicuente pueda infiltrarse en el sistema, por lo que muchos de estos formaron grupos de delincuencia informática para conseguir sus fines que eran sobre todo el dinero (F-Secure, 2017, pág. 33). Estos grupos comenzaron a crear nuevos malware para robar información desde números de tarjeta de crédito, claves de usuarios, hasta datos financieros de las empresas más importantes.

La aparición del malware llamado ransomware según fuentes periodísticas surgió en marzo del 2011 en Alemania llamado el "Virus de la Policía" (CUERPO NACIONAL DE POLICÍA, 2013, https://goo.gl/WoLcR9). Fue creado por un grupo de ciberdelicuentes ucranianos. Esta primera versión de ransomware enviaba un mensaje engañoso que suplantaba la identidad de la policía del país donde se encontraba la computadora infectada, a lo que intimaba a realizar un pago a pena de ser encarcelado por supuestas acciones ilícitas realizadas en la computadora (pornografía infantil, chats comprometedores). Esta metodología fue extendiéndose por toda Europa y en Latinoamérica surgió por primera vez en Argentina en octubre del 2011 y en EEUU en agosto de 2012. Según Florián Manuel Pérez Sánchez (2015) (Ciberseguridad: Ransomware, parte I - El negocio del secuestro digital., 2015) este "Virus de la Policía" hizo eco en los medios de comunicación sobre todo europeos que lograron hacer conocer a la sociedad como el primer caso de ransomware.

Existen controversias en relación al surgimiento del virus, las empresas de seguridad no están de acuerdo en la aparición de cada versión de ransomware, por ejemplo en la figura 4 Symantec (Internet Security Threat Report Volume 21, 2016, pág. 59) muestra en su cronología de descubrimientos del ransomware que el primero que surgió fue el llamado Gpcoder en 2005 que es del tipo cifrador, pero no fue tan efectivo y difundido como el virus Reventon o "Virus de la Policía".

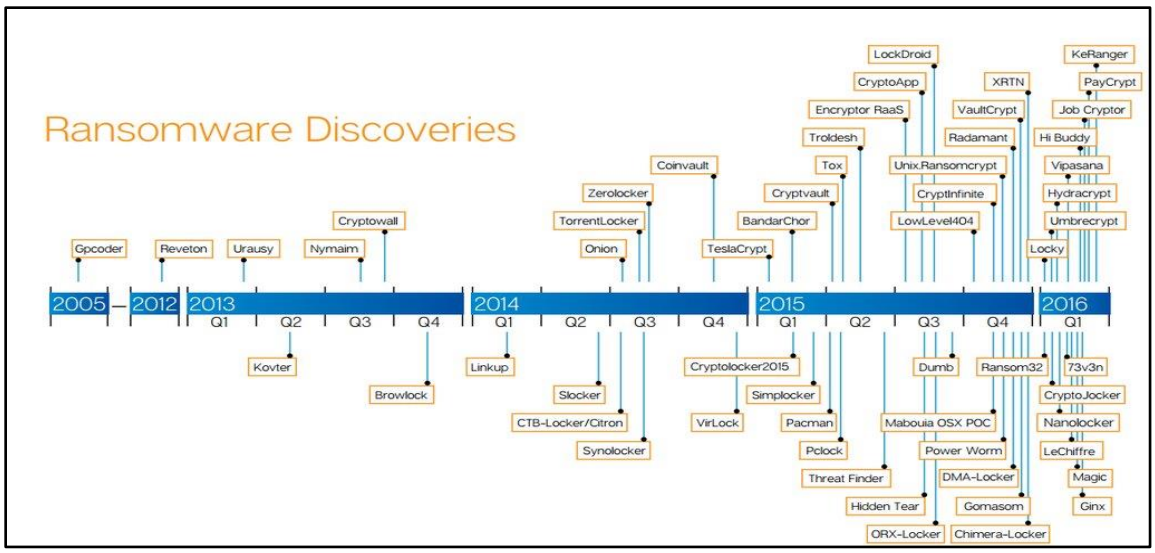


Figura 4. Descubrimientos de ransomware por Empresa Symantec (Internet Security Threat Report Volume 21, 2016, pág. 59).

Por lo contrario, en la figura 5 se advierte que la Empresa EndGame toma como primer ransomware a ransomlock que surge entre 2012 y 2013.

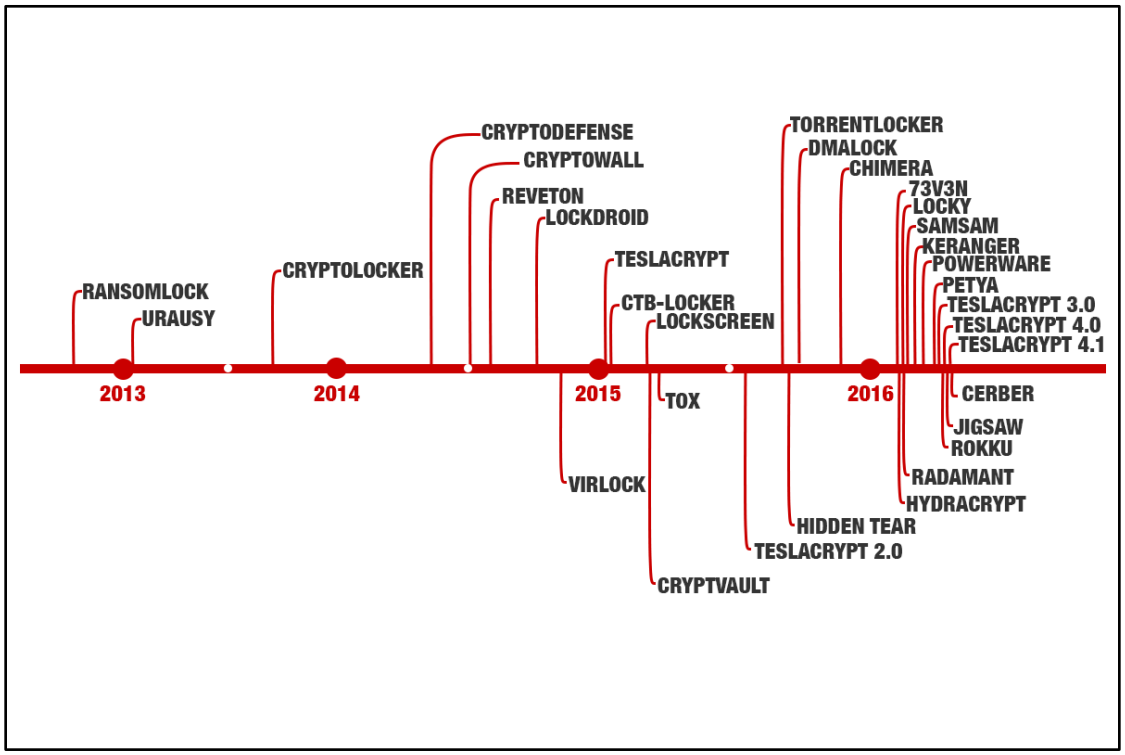


Figura 5. Historia del ransomware por Empresa de Seguridad EndGame (Rousseau & Mager, 2016).

Por último, en la figura 6 se puede observar que la empresa F-Secure afirma que el primero fue Rannoh entre 2012 y 2013 y que a principios de 2013 aparece Ransomlock. Esto muestra la falta de un organismo central de Ciberseguridad que defina las apariciones de los virus, por lo que cada empresa de seguridad expone su propia experiencia.

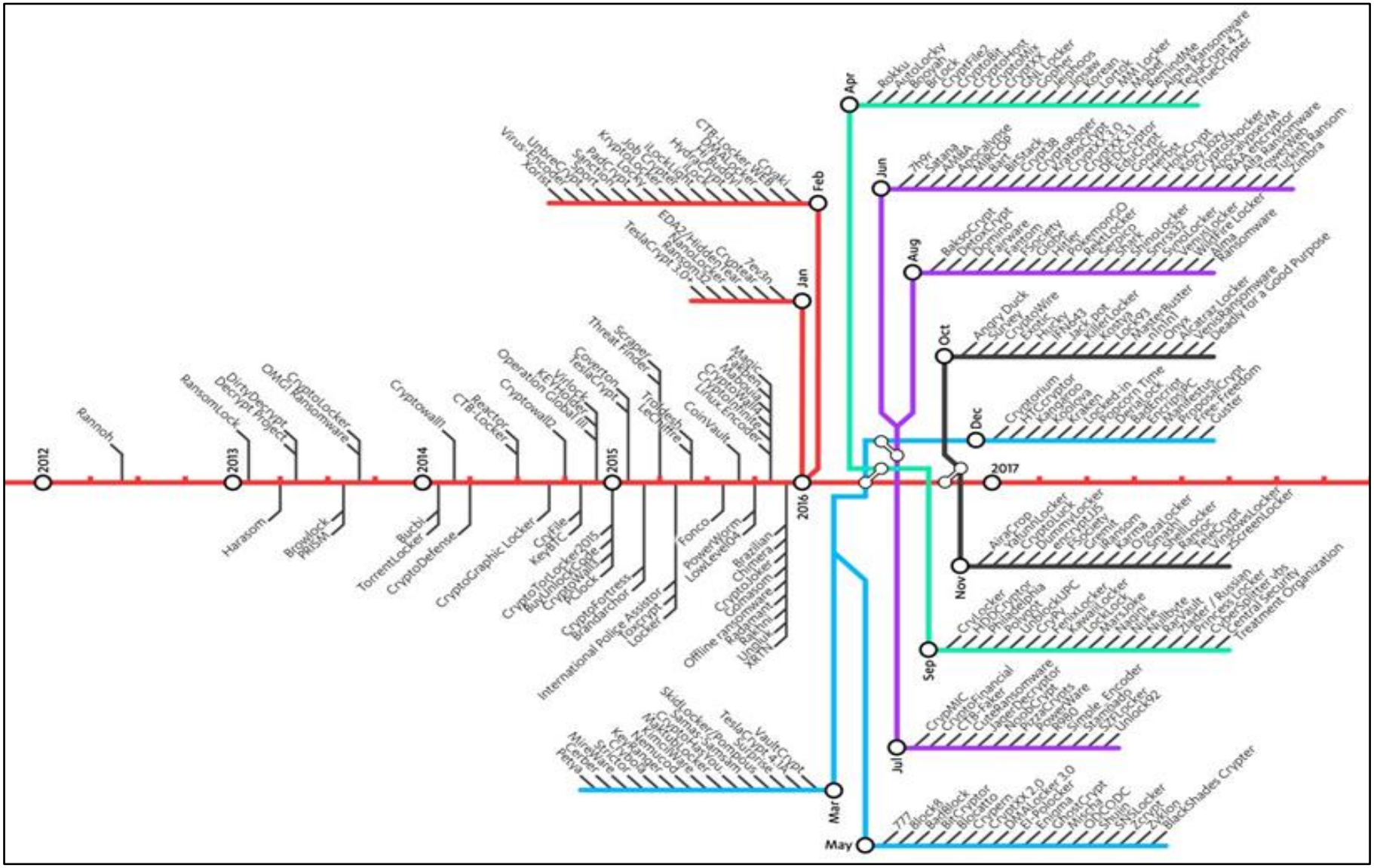


Figura 6. Mapa del Metro del ransomware de la Empresa F-Secure **(State of Cyber Security, 2017, pág. 41)**.

Continuando con la historización, cabe destacar que en el año 2013, después del éxito que tuvo el "Virus de la Policía", otros grupos de hackers comenzaron a desarrollar nuevos ransomware mutándolos para no ser detectados por los antivirus y sofisticando los procesos, según un informe de F-Secure (State of Cyber Security, 2017, pág. 41) el auge de los ransomware cifradores fue gracias a la aparición del llamado CryptoLocker que cifra los archivos con una clave pública RSA-2048 en donde éstos son casi irrecuperables, por tanto pagar el rescate y esperar la clave de recuperación (nadie asegura que envíen la clave después de pagar) era la forma de recuperarlos, y gracias al éxito que tuvo es que "definió el modelo de negocio y proveyó la oportunidad" para que muchos otros atacantes vean lo lucrativo que puede ser este tipo de malware.

Desde ese momento grupos de ciberdelicuentes comenzaron a crear nuevos tipos de ransomware cifradores, tal es así que fue creciendo exponencialmente año a año las nuevas familias de ransomware. Por ejemplo, F-Secure en su informe (State of Cyber Security, 2017, pág. 41) nos muestra que en 2013 había 8 nuevas familias, en 2014 encontraron 15 nuevas familias, en 2015 35 familias y en 2016 193 nuevas familias por lo que se advierte que el negocio de cifrar archivos es bastante redituable económicamente.

6. Clasificación de ransomware

Se puede afirmar que ransomware se ha expandido a lo largo de los años, a causa de que muchas personas y empresas pagan el rescate de sus archivos que son únicos e irremplazables, y los ciberdelicuentes, al ver un negocio tan rentable, han creado diferentes formas de ransomware.

Se pueden diferenciar, como aclara Wojciech Mazurczyk, en dos grandes tipos: locker[8] y crypto[9].

6.1 Locker

Este tipo de ransomware por lo general solo intenta asustar al usuario por medio de algún mensaje de pago, pero sin encriptar los archivos. Entre los más famosos de este tipo de ransomware de lock screen se encuentra el WinLock que en sus primeras versiones afectó a más de 10.000 usuarios en Rusia, Ucrania, Bielorrusia y Moldavia. Según el Instituto Nacional de Ciberseguridad de España S.A., este malware bloquea el acceso a la computadora infectada y solicita el envío de un SMS Premium para desbloquearlo (Cantón, 2014). Otro es el ya mencionado "Virus de la Policía" o Reventón que sigue activo, como explica el medio Computer Hoy (Ramírez, 2016). Existe una variante para celulares que se ha extendido a 31 países del mundo y, obviamente, sigue habiendo variantes para PC. Locker engaña mayormente a usuarios de PC inexpertos, quienes ante la amenaza y el desconocimiento pagan el rescate de la PC. Se debe saber que este tipo de ransomware no afecta los archivos sino al sistema operativo, el problema se soluciona con un respaldo de los datos y luego un formateo, aunque es un poco engorroso y se pierde tiempo, al menos no se debe pagar para recuperar los datos.

El virus de la Policía fue tan famoso por sus ataques, que en Europa los medios de comunicación le dieron un espacio concientizando de no pagar el rescate e informaron cómo podían realizar el desbloqueo de la PC.

[8] Bloqueador: bloquea la pantalla y no deja realizar ninguna acción.
[9] Cifrador: encripta los archivos.

6.2 Cryptovirus[10]

Como afirma la investigación de Adam Young y Moti Yung, la criptografía permite guardar información de forma segura, y realizar comunicaciones privadas entre el emisor y el receptor, pero los ciberdelicuentes encontraron la forma de usar esto para sus propios fines. Utilizaron la misma metodología que con el tipo de ransomware locker, pero al ejecutarse en la máquina infectada, primero encriptan los archivos por medio de la criptografía, y luego envían el mensaje intimidatorio.

6.2.1 CryptoLocker[11]

El CryptoLocker fue creado por un ruso llamado Evgeniy Bogachev, que es el cibercriminal más buscado por el FBI (como dato anecdótico, ofrecen 3 millones de dólares por su paradero, la cifra más alta para atrapar a un Ciberdelicuente, según la BBC (2015). Es buscado también por estar involucrado en otro malware llamado GamerOver Zeus en el que captura cuentas bancarias con los datos de ID y contraseña.

El ransomware bloqueador es redituable pero no tanto como el cifrador, y con la llegada del CryptoLocker en 2013 y el éxito que obtuvo en un solo mes, como nos dice The Guardian (Ferguson, 2013), hubo 1 millón de computadoras infectadas por CryptoLocker. Este virus aprovechaba que los antivirus todavía no tenían información de estos nuevos malwares y los hackers los iban mutando.

El CryptoLocker, en su primera versión, cifraba los archivos usando una clave RSA en los que, como dice el experto en seguridad Gavin O`Gorman, nadie en el mundo podría desencriptar

[10] Cryptovirus: Utilizar la criptografía en virus, en este caso encriptando archivos de computadora.
[11] Cryptolocker: Una versión de ransomware que utiliza la criptografía para encriptar los archivos de computadora.

esa clave y se plantea que harían falta más de 30 años para concretarlo (2013). Los archivos que "secuestra" son desde documentos de Word y Excel, pasando por imágenes y fotos hasta archivos de Autocad, por lo que los usuarios atacados, que no habían hecho un respaldo de los datos, si querían recuperar sus valiosos archivos solo quedaba pagar USD 300 o € 300 en bitcoins antes de que pasen 72 o 95 horas, y arriesgarse a que los hackers envíen la clave para descifrar los archivos. De esta experiencia se describe que, si no pagan en ese lapso de tiempo, las víctimas podían perder sus archivos, en cuanto los ciberdelicuentes cumplan con la amenaza de eliminar la clave privada del servidor. Según Symantec (Ferguson, 2013) el 3% de los perjudicados pagó para recuperar los datos sin saber si en verdad esto sucedería. El gran dilema reside en qué tan importantes son esos datos para las víctimas. Si no se pagara a los hackers, estos dejarían de utilizar estos métodos, en cambio como se ve en las estadísticas en el punto 0 cada año se incrementa más este tipo de ataque, lo que da a entender que muchas víctimas pagan.

Suponiendo la siguiente situación de que una víctima de ransomware no quiso pagar el rescate de sus archivos por X causa, pero luego se arrepiente ya que hay algún documento o foto importante que desea recuperar. El tiempo para pagar el rescate de los archivos se acabó, por lo que la víctima pierde toda esperanza de recuperar sus archivos. Aquí surge la perspicacia de los creadores del Cryptolocker para lanzar un nuevo servicio. Este consiste en que las víctimas del ransomware envían algún archivo encriptado a una dirección provista por los ciberdelicuentes y pagan 10 bitcoins (en 2013 eran USD 2300), que es 10 veces más que la primera extorsión, luego los ciberdelicuentes entregan la clave privada para recuperar los archivos. La amenaza de los ciberdelicuentes de destruir la clave en 72 horas es falsa, por lo que afirma Constantin (2013) puede que los cibercriminales no hayan destruido la clave como habían amenazado, ya que es

muy difícil descifrar la clave privada. Se necesitarían muchas computadoras por muchos años procesando la información para recuperar la clave.

Respecto al funcionamiento del Cryptolocker como explica Lawrence Abrams (2014) se guarda con un nombre aleatorio en la carpeta del superusuario (root), es decir, que este archivo va a tener todos los privilegios de escritura sobre el sistema operativo. Las carpetas de superusuario donde se guarda la información están en la ruta %AppData o %LocalAppData. Luego, modifica el registro de arranque de la computadora:

KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker

KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker_<version_number>"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker_<version_number"

Como se aprecia en el código este ransomware ha sido creado para el Sistema Operativo Windows.

Al realizar la modificación del registro de arranque hace que el malware se active apenas inicia la computadora. En el registro también hay un asterisco (*) después de la palabra RunOnce, que al correr el modo seguro hace que también se active el CryptoLocker.

Además de este cambio de registro, el malware secuestra los archivos con extensión .EXE, que son los archivos ejecutables utilizados para lanzar una aplicación, por lo que cuando se ejecuta una aplicación, el ransomware borra el volumen de copias ocultas (shadow volumen copies), logrando que no se puedan restaurar los archivos a como estaban anteriormente. Al hacer clic en un ejecutable, se realiza el siguiente comando:

```
"C:\Windows\SYsWOW64\cmd.exe" /C

"C:\Windows\Sysnative\vssadmin.exe" Delete Shadows /All /Quiet
```

La primera línea llama al Símbolo de Sistema (Command prompt), y la segunda utiliza el administrador de volumen de copias ocultas para eliminarlas, y no poder recuperar los archivos a un estado anterior.

Como muestra el informe de Abrams, el secuestro de la extensión .EXE en el registro aparece de una forma parecida a esta:

```
[HKEY_CLASSES_ROOT\.exe]
@=" Myjiaabodehhltdr "
"Content Type"="application/x-msdownload"

[HKEY_CLASSES_ROOT\.exe\PersistentHandler]
@="{098f2470-bae0-11cd-b579-08002b30bfeb}"

[HKEY_CLASSES_ROOT\Myjiaabodehhltdr]
```

[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\DefaultIcon]

@="%1"

[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\shell]

[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\shell\open]

[HKEY_CLASSES_ROOT\Myjiaabodehhltdr\shell\open\command]

@="\"C:\\Users\\User\\AppData\\Local\\Rlatviomorjzlefba.exe\" - \"%1\" %*"

Lo que realiza es llamar al ejecutable .exe con un nombre aleatorio como “Myjiaabodehhltdr” para bloquear la utilización de software de detección de virus.

Al eliminar el volumen de restauración de Windows, CryptoLocker intenta comunicarse con los servidores C&C de los atacantes, utilizando un algoritmo de generación de dominio (DGA) que es la forma en que los ciberdelicuentes cambian los dominios para no ser encontrados. Si en la búsqueda la computadora es apagada, la comunicación se pierde, pero cuando se inicia nuevamente, el malware buscará algún servidor C&C, por lo que la única forma de que no encuentre un servidor es que la computadora no tenga acceso a Internet. Cuando CryptoLocker logra comunicarse solicita una clave pública para encriptar los archivos, y luego la guarda en el registro HKEY_CURRENT_USER\Software\Cryptolocker_0388, pero la manera de descifrar los archivos es por medio de la clave privada que está resguardada en el servidor C&C del atacante. Al terminar de encriptar los distintos tipos de archivos, se crea un mensaje que explica cómo rescatar los datos por una suma considerable que varía entre USD 100 a USD 300. Para realizar el pago, aunque no se recomienda hacerlo, los ciberdelicuentes ponen a disposición unas

direcciones de cuenta de BitCoins, por el cual consiguen dificultar el rastreo del dinero, y así quedar impunes.

6.3 Estadísticas de ataques del ransomware

Según las estadísticas que provee Kapersky Labs (SecureList, 2016) de los usuarios que utilizan su producto en el período de abril 2014-marzo 2015 los encriptadores que más se detectaron fueron Cryptowall, Cryalk, Scatter, Mor, CTB-Locker, Torrent Locker, Fury, Lortok, Aura y Shade, se realizaron 101.568 ataques en todo el mundo, un 77,48% de todos los ataques de malware.

En el período de abril 2015-marzo 2016 (figura 7) solo tres ransomware ocupan el 79,21% de los ataques y esos son Tesla Crypt con el 48,81%, CTB-Locker con el 21,61% y Scatter con 8,66%.

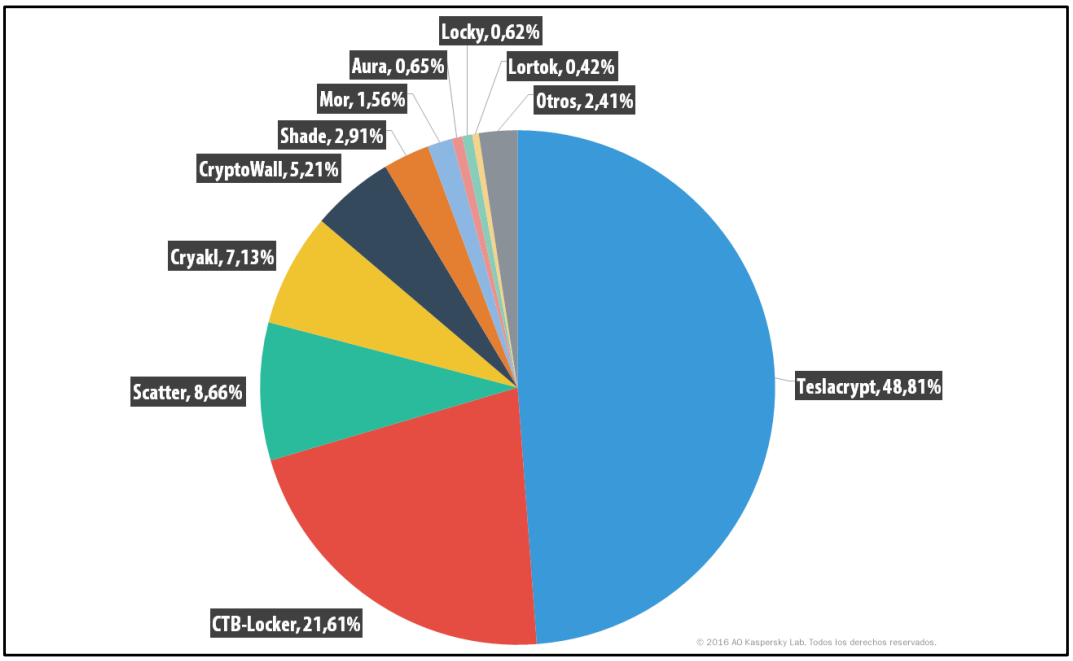


Figura 7. Porcentaje de ataques de ransomware en los usuarios desde abril 2015 a marzo 2016 (SecureList, 2016).

Otro dato interesante es que, el porcentaje de ataques a usuarios corporativos subió un 6% entre períodos, alcanzando 13,13 %, estos datos llevan a pensar que los ciberdelicuentes tienen en la mira a las empresas. Este creciente negocio del Ransomware se ve reflejado en la creación de nuevos tipos de este malware, en 2015 la empresa de seguridad Symantec (2016) (Symantec, Ransomware and Businesses 2016, 2016) encontró 100 nuevas familias. Sumado a lo explicado por Martinez-Garcia & Moo Medina, los grupos de cibercriminales comienzan a utilizarlo para vender los servicios y kits de ransomware a cualquier usuario malintencionado (2016). Se puede ver un mensaje de venta de kits de ransomware en la figura 8.

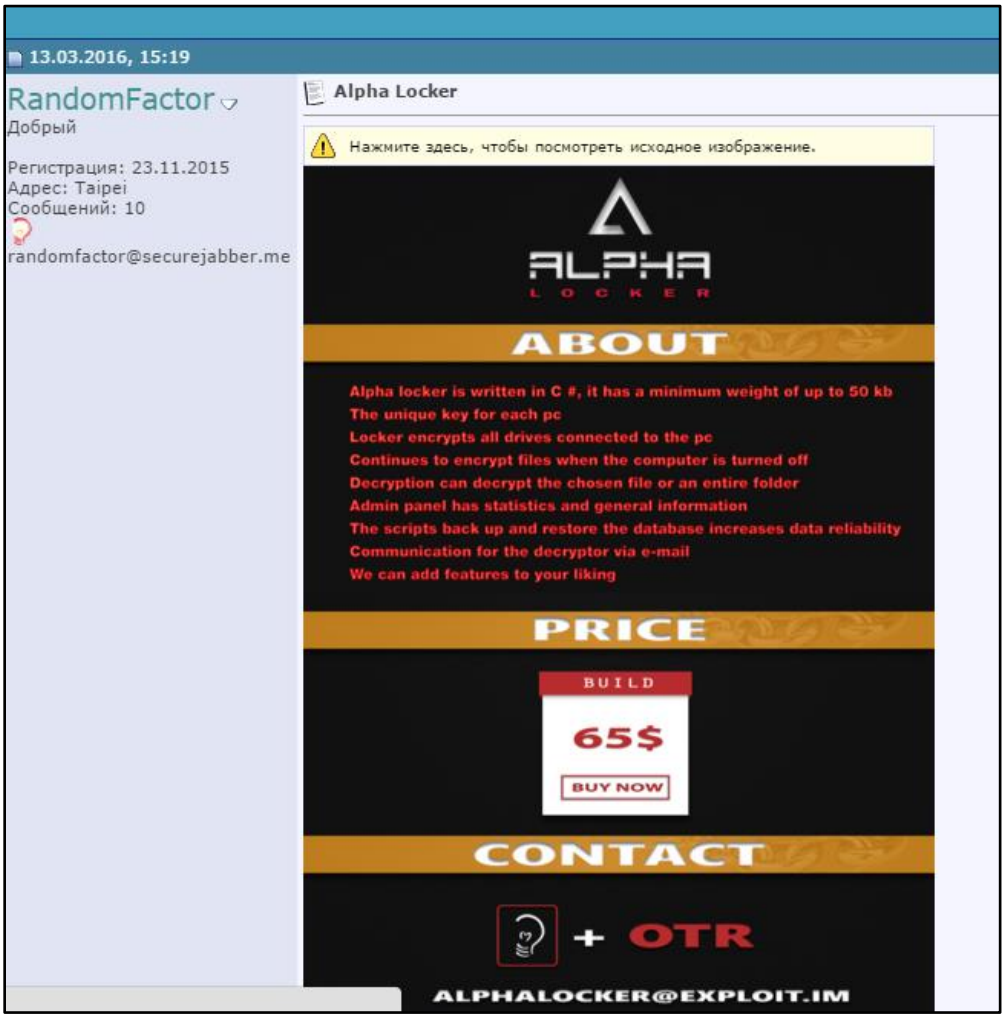


Figura 8. Anuncio en un foro de hacking de venta de servicio de ransomware (Cruz, 2016).

El comprador del kit consigue un virus listo para utilizar con una interfaz muy simple, como se ve en la figura 9, donde puede diseminar el virus y obtener cuantiosas sumas de dinero, en el cual un porcentaje va al usuario del kit y otro al grupo criminal que lo proveyó.

Figura 9. Interfaz de AlphaLocker (Cruz, 2016).

Por su parte, IBM realizó un estudio (IBM Study: Businesses More likely to Pay Ransomware than Consumers, 2016) en el que más del 50% de los usuarios no pagaría por rescatar sus datos, y en el caso de que sí lo hiciera, sería un máximo de USD 100. Pero se ve en el estudio que la parte emotiva juega su papel, ya que el 55% de los usuarios que son padres pagarían para recuperar sus datos, y los que no son padres un 39% lo haría. Con respecto a las empresas, un 70% de los ejecutivos paga para recuperar los archivos, y de ese porcentaje, 50% pagaría alrededor de USD 10.000 y un 20% alrededor de USD 40.000, con estos datos se puede observar que las empresas pagan un monto mayor de rescate que los usuarios comunes dando cuenta así

porque los ciberdelicuentes han centrado sus objetivos en ellas. Las organizaciones más afectadas según Symantec (Ransomware and Businesses 2016, 2016, pág. 8) son las de servicio (38%) y manufactura (17%) como se ve en la figura 10, aunque no tienen claro porque estos sectores son más atacados. Una de las teorías es que al tener que utilizar más servicios de Internet están más expuestos a ataques que los demás sectores.

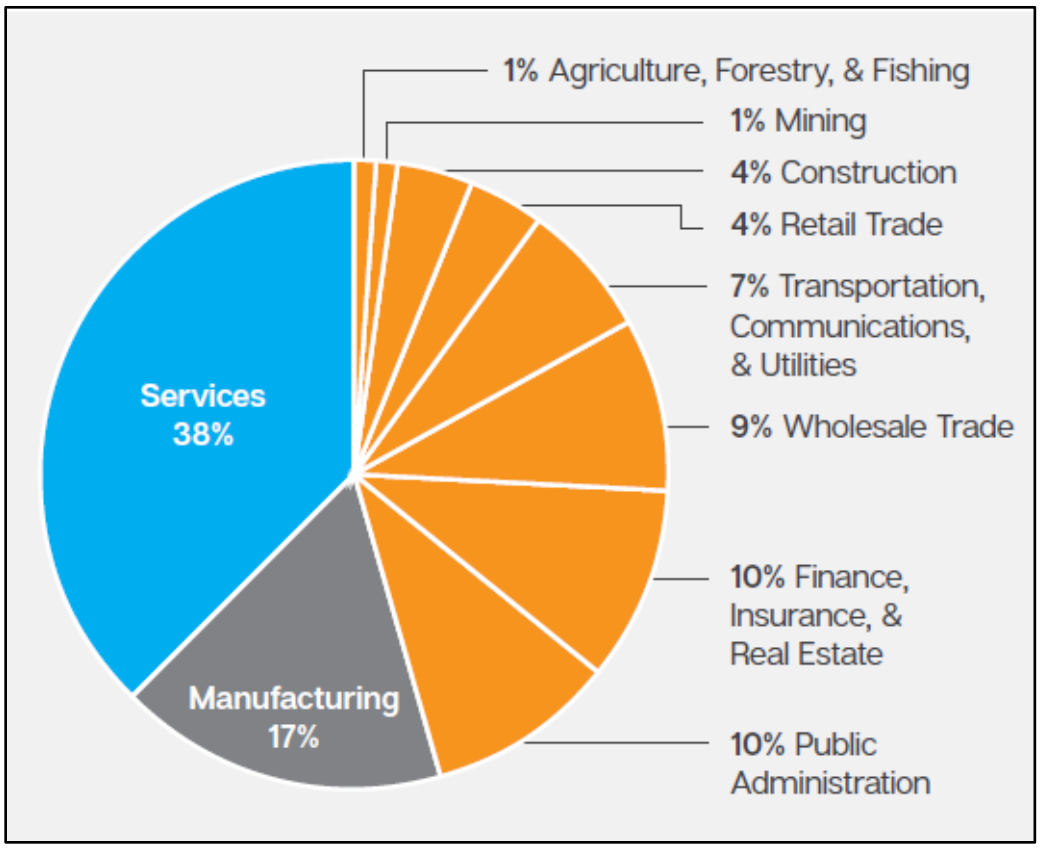


Figura 10. Porcentaje de sectores organizacionales afectados por el ransomware. (Symantec, Ransomware and Businesses 2016, 2016).

6.4 Organizaciones relacionadas a la salud

Los hospitales brindan servicios esenciales para la salud de la población y son lugares donde está en juego la vida y la muerte de las personas. Los médicos necesitan la información de sus

pacientes para diagnosticarlos o hacer cualquier tipo de intervención, pero ¿qué pasa cuando los datos son secuestrados?

Según un informe de McAfee (Labs, 2016) los cibercriminales ven como un objetivo accesible atacar los hospitales, ya que cuentan con sistemas obsoletos de muchos años, que no tienen nuevas actualizaciones de seguridad. Esto generalmente sucede con los equipos antiguos, que no permiten instalar sistemas operativos actuales por falta de requerimientos, y deja una brecha de seguridad muy grande. Lo anterior tiene otro agravante respecto a que el personal del hospital no está instruido en los problemas de seguridad informáticos, y regularmente abren correos que infectan el sistema del hospital.

Cuando un empleado del Hospital ejecuta el ransomware, éste elimina los volúmenes guardados por Windows para que no se pueda recuperar el sistema a un estado anterior. Posteriormente, se comunica con los C&C para obtener la clave pública y encriptar los datos, pero lo más grave es que algunos dispositivos médicos también pueden quedar afectados y fuera de funcionamiento, pudiendo a su vez ocasionar pérdidas humanas.

Como dice Vásquez (2016) al principio el ransomware atacaba a las personas, luego comenzó con las empresas y en los últimos años son los hospitales donde los cibercriminales han fijado su objetivo, ya que la pérdida de datos de los pacientes y el no funcionamiento de los dispositivos médicos es algo crítico. Por eso, según Health Alliance, en el 2016 el 18% de los hospitales de EEUU fueron afectados por ransomware, y el 50% de ellos se sospecha que siguen infectados con el virus.

El caso más resonante de infección en un hospital fue en Los Ángeles, en el Hollywood Presbyterian Medical Center. El periódico Los Ángeles Times (Winton, 2016) informó que el

ataque fue el 5 de febrero de 2016 y estuvieron 10 días con el sistema infectado, hasta que finalmente se pagó el rescate por una suma de 40 bitcoins, que en ese momento equivalía aproximadamente a USD 17.000. El jefe ejecutivo del Hospital, Allen Stefanek, afirmó que la forma más rápida y eficaz que tuvieron para recuperar los datos fue pagar al criminal, a pesar de que recomiendan no hacerlo ya que no se asegura que envíen la clave.

Otro caso ocurrido en un hospital de Kansas da una clara muestra de por qué no hay que pagar a los cibercriminales, ya que fomentan la permanencia de estas prácticas extorsivas y con el agravante de que pueden no enviar la clave para desencriptar los archivos. Como informa en su blog Trend Micro, una empresa que desarrolla software de seguridad, el hospital de cardiología de Kansas, en Wichita, fue atacado por el ransomware locky el 18 de mayo de 2016. La directiva decidió pagar el rescate, pero los delincuentes no desencriptaron todos los archivos, por eso solicitaron más dinero por los faltantes. Por lo que la directiva reflexionó que no era inteligente repetir el comportamiento que resultó fallido y decidió no pagar el segundo rescate.

Es realmente preocupante que los hospitales, que son instituciones sociales que cumplen una función sanitaria tan importante, no puedan atender a los pacientes por haber sido atacados por un ransomware, como sucedió el día 29 de marzo de 2016 en el MedStar Southern Maryland Hospital Center. Como cuenta el Washington Post (Cox, 2016) tuvieron que derivar a los pacientes, sin dar ninguna explicación, a sus viviendas por la caída del sistema. De esta situación nadie hubiera conocido lo que pasaba si no fuera por los mismos empleados que informaron por las redes sociales, mostrando la carta de pedido de rescate por 45 bitcoins, es decir, USD 19.000. Ese día, enfermeras y doctores tuvieron que utilizar el fax y formularios en papel que eran menos comprensibles (con letra poco clara y papel de fax poco legible) que el formato digital, y una práctica inusual. Pero lo más alarmante fue que la Base de Datos no podía ser utilizada, por lo

tanto, esa falta de información vital del paciente pudo ocasionar un mal diagnóstico, y poner en juego su vida.

6.5 Cómo funciona locky, considerado la pesadilla de los hospitales

Generalmente, el ransomware locky, como explica Abrams (The Locky Ransomware Encrypts Local Files and Unmapped Network Shares, 2016), se distribuye por email adjuntando un documento Word (como se ve en la figura 11), en este documento el delincuente agrega una macro. Una macro es una serie de instrucciones que se ejecutan en un programa, en este caso Microsoft Word, en el que esas instrucciones podrían realizar cambios peligrosos en el equipo. Por lo que Windows siempre aconseja, por seguridad, tener deshabilitadas las macros, ya que pueden tener código malicioso.

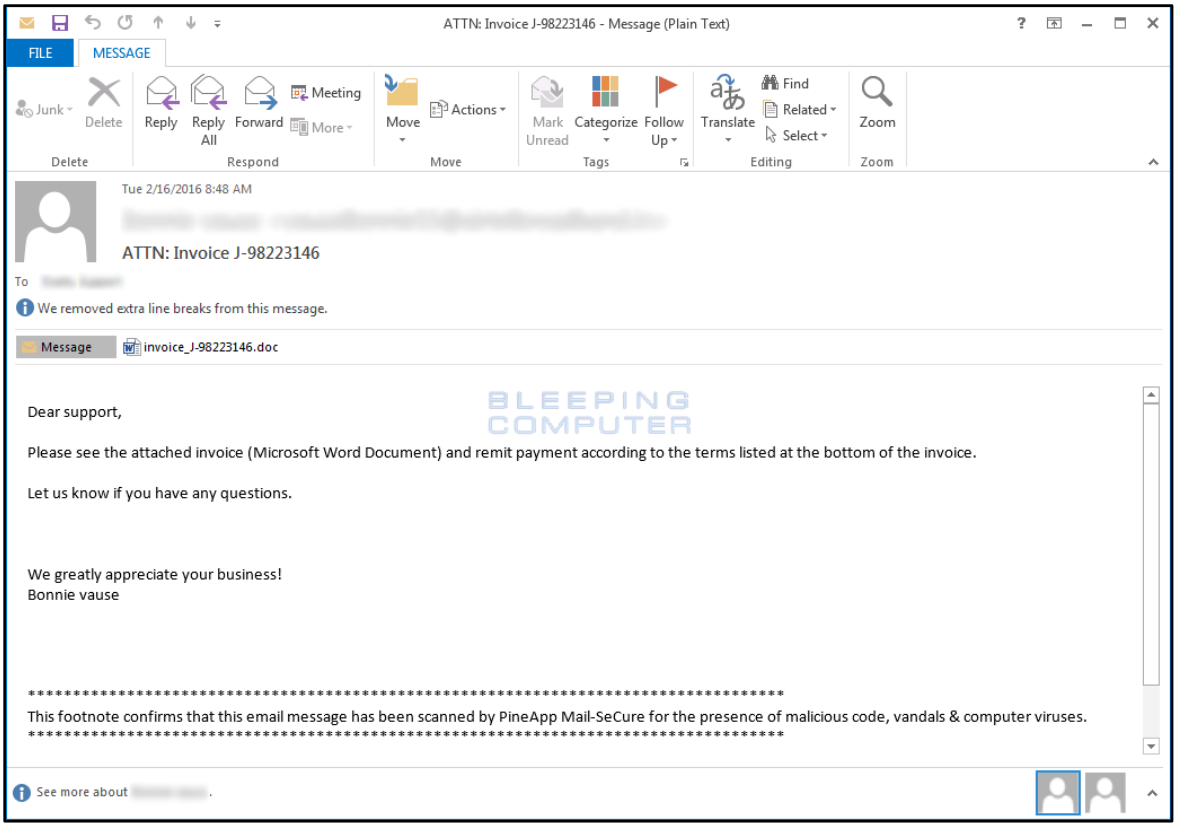


Figura 11. Email enviado por el Ransomware Locky (Abrams, The Locky Ransomware Encrypts Local Files and Unmapped Network Shares, 2016).

Al abrir el documento Word, el cibercriminal escribió como título “activa la macro si los datos codificados son incorrectos” como se muestra en la figura 12, y luego de esto, hay un texto indescifrable por lo que un usuario sin conocimientos sobre el tema podría activar la macro. Esto seguramente sucedió en los hospitales atacados, donde cualquier enfermera o doctor pudo haber activado la macro sin pensar en lo que pudiera ocasionar.

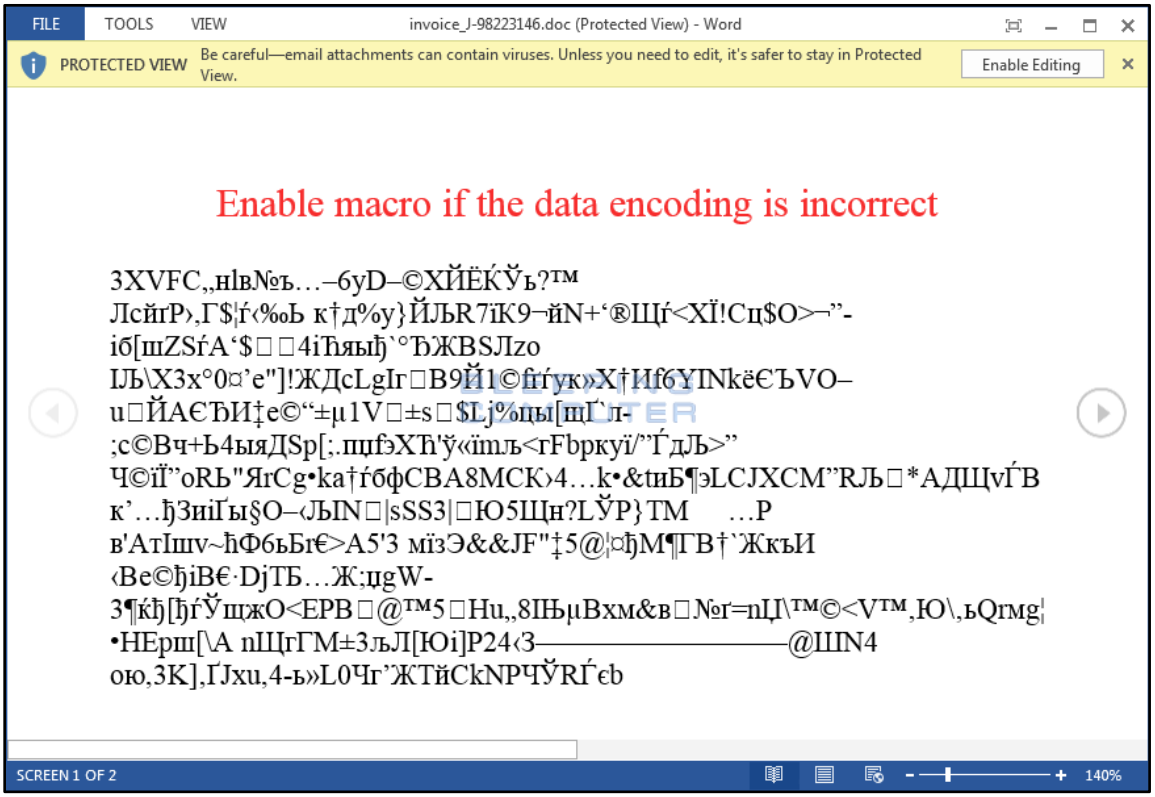


Figura 12. Documento de Word con macro malicioso (Abrams, The Locky Ransomware Encrypts Local Files and Unmapped Network Shares, 2016).

Al ejecutar la macro (se puede ver el código en figura 13) el malware busca el servidor C&C y descarga un archivo que se guarda en la carpeta %Temp%.

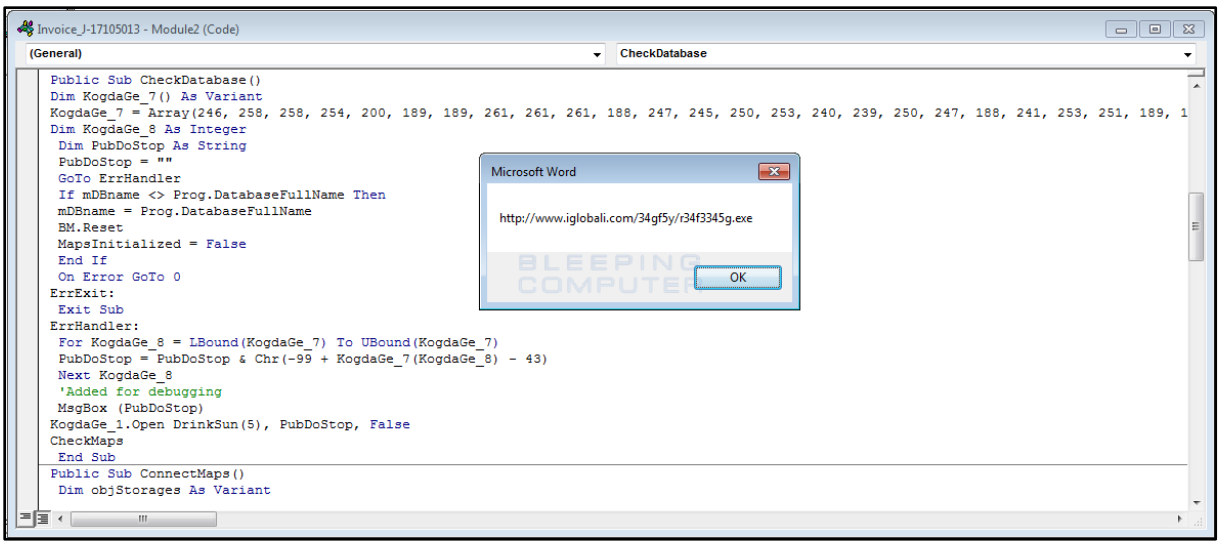


Figura 13. Código de la macro maliciosa (Abrams, The Locky Ransomware Encrypts Local Files and Unmapped Network Shares, 2016).

Este archivo contiene el ransomware locky, que se ejecuta encriptando los archivos de la computadora de los discos locales, y también los mapeados en la red, como sucedía con los otros tipos de ransomware, pero locky además encripta las redes compartidas, aunque no hayan sido mapeadas localmente. Por eso, como política de seguridad, se deben otorgar los permisos esenciales y preferentemente que sean de solo lectura. A los archivos encriptados locky se les asigna un ID único de 16 números hexadecimales que siguen el siguiente formato **[id_unico][identificador].locky**, el **id_unico** es el ID único hexadecimal, y el identificador también es un código hexadecimal diferente para cada archivo.

Locky luego de realizar su trabajo de encriptamiento, crea la nota de pedido de rescate (ver figura 14) ubicándolas en el escritorio, y en las carpetas donde encripta los archivos con el nombre **_Locky_recover_instructions.txt**, en la cual se explica qué ha pasado con los archivos y dónde puede realizar el pago de rescate.

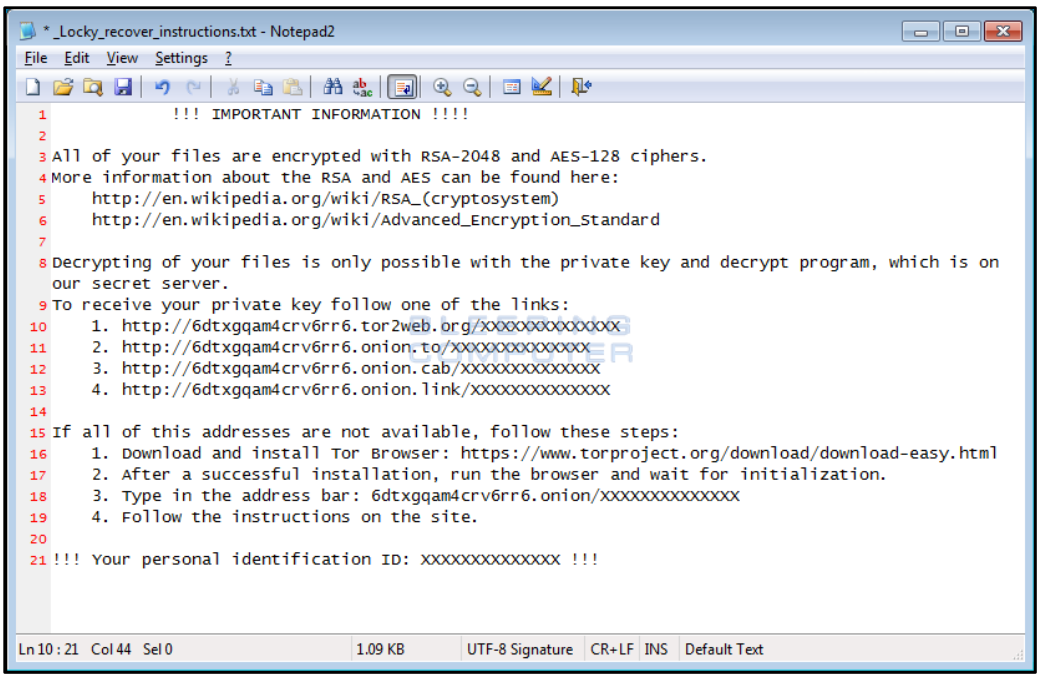


Figura 14. Nota de rescate del malware locky (Abrams, The Locky Ransomware Encrypts Local Files and Unmapped Network Shares, 2016).

Además, por si el usuario no se percató de las notas de rescate, realiza un cambio en la imagen de fondo de pantalla con las mismas instrucciones (ver figura 15) que las notas de rescate llamado **_Locky_recover_instructions.bmp**.

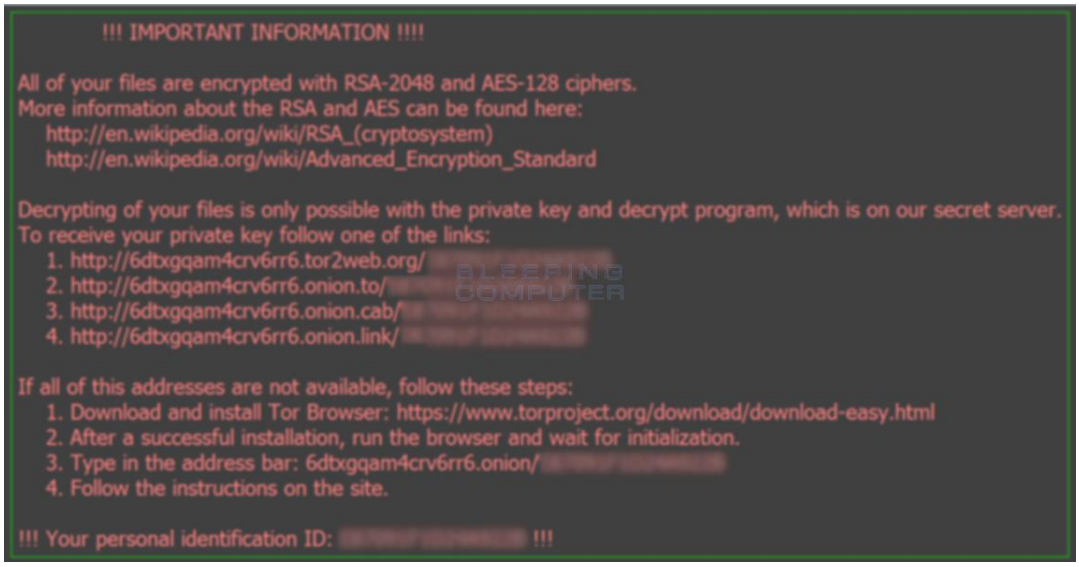


Figura 15. Fondo de pantalla del locky (Abrams, The Locky Ransomware Encrypts Local Files and Unmapped Network Shares, 2016).

Locky se guarda en el registro de Windows en las siguientes llaves:

- HKCU\Software\Locky\id
- HKCU\Software\Locky\pubkey
- HKCU\Software\Locky\paytext
- HKCU\Software\Locky\completed

En la llave id se guarda el ID único de la computadora atacada, en la llave **pubkey** la clave RSA pública que no sirve para desencriptar, ya que la criptografía es asimétrica y se necesita la clave privada para desencriptar los archivos. Por último, la llave **completed** aparece cuando se pudieron encriptar todos los archivos.

7. No más secuestro

A causa del crecimiento de ataques de ransomware se ha creado un portal llamado NO MORE RANSOM creado por la National High Tech Crime Unit de los Países Bajos (policía que investiga crímenes hechos en la red), el European Cybercrime Centre de Europol, Kaspersky Labs e Intel Security/McAfee.

Este proyecto, como se ve en su página web (figura 16), realizado por estas cuatro organizaciones, tiene el aval de muchas otras organizaciones de Seguridad, y también de las que combaten el cibercrimen. Intenta concientizar al usuario de las formas de prevención contra el ransomware y, llegado el caso de ser infectado, darle herramientas para no tener que pagar el rescate, evitando que se financie a estos criminales y fomenten el uso de estos métodos.

Figura 16. Captura de pantalla extraída de la página web https://www.nomoreransom.org/es/about-

En la página de inicio del portal (RANSOM, 2016) hay una ingeniosa frase "¿NECESITAS AYUDA para desbloquear tu vida digital sin pagar el rescate a tus atacantes?" como muestra la figura 17, aludiendo, de este modo, a los documentos guardados, que seguro ocupan una gran parte de la vida de las personas como fotos familiares, documentos del trabajo u otras cosas personales que nadie quiere perder. Además, que advierte que pagar el rescate no garantiza la solución.

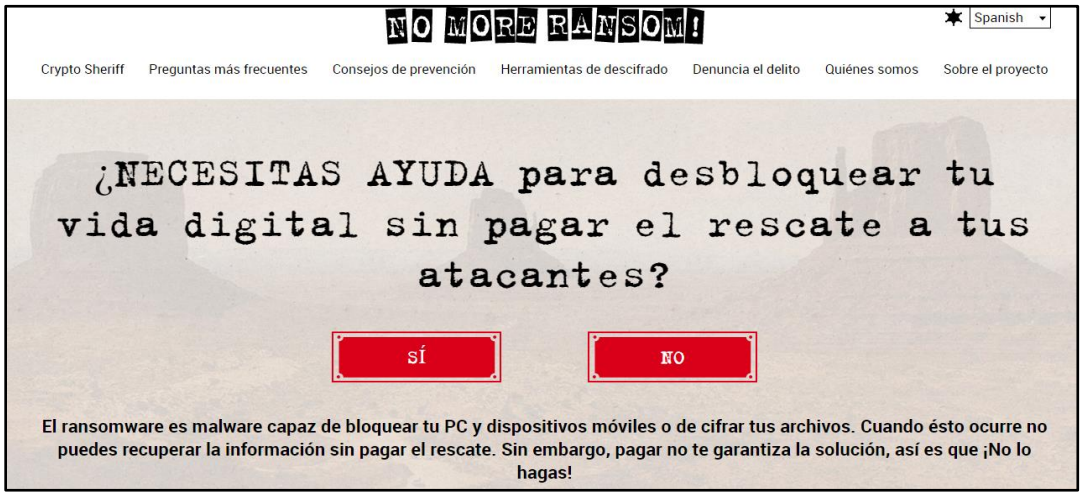


Figura 17. Captura de pantalla extraída de la página web https://www.nomoreransom.org/es/index.html

Al cliquear en SI, la web redirecciona a otra página con el título Crypto Sheriff (ver figura 18) en donde se puede enviar uno o dos archivos, más la nota de rescate para así definir de qué ransomware se trata y ayudar a desencriptar los archivos.

Figura 18. Captura de pantalla extraída de la página web https://www.nomoreransom.org/es/ crypto-sheriff.php

En algunos casos, pueden tener la solución de desencriptación como muestran en la página: "La batalla para estas amenazas de ransomware han terminado". En otros casos ayuda a descubrir el ataque de nuevos ransomware e investigar por medio de ingeniería inversa o algún otro método como desencriptar los archivos.

8. Formas de prevención

Luego del recorrido anterior y para cerrar el desarrollo, resulta conveniente plantear algunas formas de prevención de los ataques de ransomware. Se presentan numerosas y variadas formas de protección que resultan significativas para el usuario y las organizaciones.

Para lograr la protección contra éstos es importante una buena prevención, para así no perder las fotos, archivos o cualquier otra información que se guarda en la computadora y sea de valor

para los usuarios, por eso se deben seguir una serie de medidas como recomienda el Centro Criptológico Nacional de España (Informe de Amenazas - CCN-CERT IA-01/16 - MEDIDAS DE SEGURIDAD CONTRA RANSOMWARE, 2016):

1- Copias de respaldo periódicos

Se deben realizar copias de los datos que se consideren importantes en medios externos (USB, Disco Externo, memoria SD, etc.) e intentar no abrir ningún archivo desconocido mientras se realiza la copia, ya que puede ser un ransomware y también puede atacar al respaldo. Luego se expulsa y se mantiene aislado hasta que se lo necesite nuevamente.

2- Mantener sistema actualizado

Dejar el sistema operativo sin actualizar con los últimos parches de seguridad es un error muy grave y deja una brecha de seguridad considerable, como pasó con el Ransomware Wanna Cry en que empresas como Telefónica no tenían actualizado el Sistema Operativo Windows y pudieron ingresar e infectarlos. También se debe actualizar cualquier otro programa como los navegadores, Java, antivirus, etc.

3- Defensas bien preparadas

Actualizar todas las firmas de virus en el antivirus, para que encuentre cualquier tipo (nuevo o mutación de uno antiguo) que haya en la Red, además, es importante tener bien configurado el firewall (cortafuegos) para que bloquee cualquier acceso no autorizado.

4- Sistema antispam

El sistema antispam logra bloquear el correo masivo que lo utilizan generalmente para publicidad y también para enviar virus, por lo que este sistema filtra esos correos para que no lleguen al usuario final.

5- Políticas de seguridad en el sistema para impedir ejecución de ficheros

El ransomware se ejecuta en directorios como App Data y Local App Data por lo que el Centro Criptológico Nacional (CCN) advierte que se deberían impedir la ejecución de archivos en las carpetas donde generalmente éste se ejecuta.

6- Bloquear el tráfico entre la máquina y el servidor C&C

Mediante herramientas de identificación de intrusos como el IDS (Sistema de Detección de Intrusos) o el IPS (Sistema de Prevención de Intrusos) se debería bloquear la comunicación entre la máquina infectada y el servidor de comando y control, así no podría obtener la clave pública para realizar el encriptado.

7- Establecer una defensa en profundidad

La defensa en profundidad del Sistema de Información como dice la DCSSI (La defensa en profundidad aplicada a los sistemas de información, 2004, pág. 19) defiende un bien específico con varias barreras de defensa, en el que la caída de una barrera no debe ser en vano, ya que debe conseguir información de lo que está atacando al sistema para luego encontrar formas de repeler el ataque. En este sentido, mientras más preciado es el bien las defensas deben ser mayores y cada barrera debe contener diferentes técnicas o procedimientos.

8- No utilizar cuentas con privilegio de administrador

Los usuarios por ningún motivo deben tener privilegios de administrador, para que así el ataque del ransomware sea menos efectivo.

9- Mantener listas de control de acceso para las unidades mapeadas en red

Como el ransomware ataca a toda unidad conectada a la máquina infectada para mitigar el impacto se recomienda restringir el acceso de escritura en las unidades mapeadas.

10- Bloquear JavaScript en el navegador

Para que los atacantes no tomen control del ordenador e infecten con ransomware, se deben utilizar un bloqueador de Javascript para que no se ejecuten script dañinos.

11- Mostrar extensiones de los archivos

En Windows, por defecto, las extensiones de archivos están desactivadas, se debe activar la opción de mostrar extensiones de archivos así se puede detectar que el archivo es un ejecutable y no un archivo Word, Excel o Pdf como usualmente engañan a los usuarios.

12- Instalar Anti Ransom

Esta herramienta monitoriza las carpetas donde están los archivos "dulces" que atacan los ransomware y cuando intenta cifrar algún archivo trata de bloquear el proceso. Además, por medio de un volcado de memoria el Anti Ransom investiga lo que realizó el proceso que utilizaba el ransomware para encontrar la clave de cifrado.

13- Utilizar máquinas virtuales

La mayoría de los ransomware tienen técnicas anti-debug (esto es para que no puedan depurar el código para analizarlo) y anti-virtualización (para utilizarlo para pruebas y ver el comportamiento del virus) por eso se recomienda utilizar máquinas virtuales así se evita que el malware actúe.

9. Hidden Tear y EDA2

En este capítulo se analizarán dos códigos de ransomware llamados Hidden Tear y EDA2 provistos por un experto en seguridad, para comprender mejor su funcionamiento y encontrar posibles formas de detección o mitigación.

9.1 Open Source de Ransomware

Antes de analizar la estructura de estos dos ransomware, el Hidden Tear y el EDA2, hay que hacer una reflexión de lo que uno comparte en la Red, ya que hay muchas cosas interesantes que se comparten como Open Source[12] que ayudan a muchos desarrolladores a reutilizar códigos que han escrito otros desarrolladores, pero se debe ser responsable y pensar lo que se comparte, por todo lo que venimos planteando de la existencia de prácticas delictivas en relación a lo informático.

Hidden Tear fue el primer ransomware de código abierto que fue publicado en GitHub, por el usuario Utkusen que según su blog (Sen, About, 2017) es un turco experto en seguridad y programador. Este código diseñado por Utku Sen cuando lo compartió en GitHub en su momento tuvo bastante repercusión, ya que aducía que era con fines educativos, a pesar de que fue cuestionado en las redes por diversos expertos, porque dejaba un código de malware para que cualquier persona pueda estudiarlo y utilizarlo para fines tanto éticos como antiéticos. Luego, se retractó y eliminó el código de su repositorio (https://github.com/utkusen/hidden-tear) pero ya el daño estaba hecho. Según Kaspersky (Wiel, 2016) en febrero de 2016 analizaron la muestra de la clase Trojan.Ransom.MSIL.Tear del código de Hidden Tear en la que encontraron 24 muestras adicionales, entonces gracias al Open Source (código abierto) se habían creado 24 variantes de este ransomware. Utku Sen, además de Hidden Tear, público el EDA2 (Sen, eda2 – a new era of open source ransomware, 2015) otro ransomware más sofisticado que Hidden Tear con encriptación asimétrica, con un generador de número aleatorio y que se comunica con un servidor C&C. Obviamente que fue más criticado por este segundo código abierto más poderoso,

[12] Open source o código abierto, son programas que se comparten entre programadores para modificarlos, estudiarlos o cualquier cosa que desees hacer con ellos.

a pesar de que aducía que era muy apropiado para educar y hacer ataques simulados en las compañías.

Como cuenta John Snow (Ded Cryptor: un ambicioso ransomware creado a partir de código abierto, 2016), Utku Sen suponía que podía haber gente que usara su código para otros fines que no eran los educativos, por esto introdujo en su código puertas traseras por las cuales podía obtener la dirección de los servidores, donde se alojaban las claves privadas y dárselas a las víctimas, aunque estas víctimas tenían que saber que este ransomware venía de un código abierto y que debían pedir las claves a Utku Sen.

Hubo dos variantes de los ransomware creados por Utku Sen que se hicieron conocidos, primero el Ransomware Magic, en el cual los creadores habían alojado las claves privadas en un servidor gratuito. Al ser denunciado que ese servidor estaba siendo usado de forma ilegal la empresa que prestaba el servicio eliminó la cuenta del delincuente con todos los archivos que tenía dentro, por lo cual Utku Sen no pudo recuperar las claves para desencriptar los archivos de las víctimas. El otro ransomware como dice Snow (Ded Cryptor: un ambicioso ransomware creado a partir de código abierto, 2016) fue un estilo "Frankenstein", ya que fue creado gracias al Open Source, en donde los desarrolladores tomaron porciones de código de varias fuentes sobre todo de las proporcionadas por Utku Sen para crear el Ded Cryptor, un ransomware que hasta la fecha del artículo de Snow no se podían descifrar los archivos.

Antes de entrar en los análisis de los dos ransomware de código abierto es necesario aclarar que no se publicará el código completo, pero se puede pedir el CD de este Trabajo Final de Grado en el estará el código completo, para fines educativos de los estudiantes de la Universidad.

9.2 Análisis de Hidden Tear

Análisis estático[13]

El código de Hidden Tear se puede observar con Visual Studio para un análisis estático de éste, en App.config está la configuración del ransomware en la cual se observa hasta qué versión de Framework soporta, ya que cada sistema Windows corre hasta una versión de Framework. Por ejemplo Windows XP solo soporta hasta el .Net Framework4.0 (https://msdn.microsoft.com/es-es/library/8z6watww(v=vs.110).aspx) como se ve en la figura 19, por lo que si se deja por defecto daría un error de que no es una aplicación Win 32 válida.

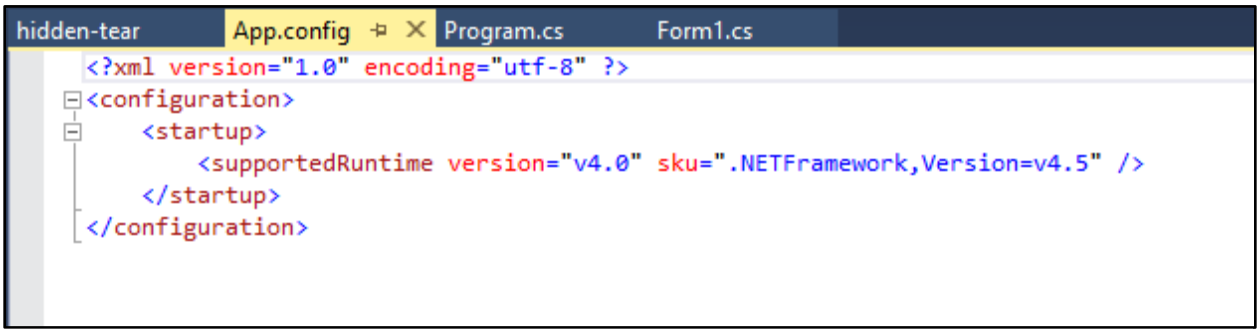


Figura 19. Código de Hidden Tear, carpeta App.config.

Después en el Form1.cs[Design] se puede observar, como en la figura 20, cómo está diseñado para que parezca un archivo PDF y así engañar a la víctima.

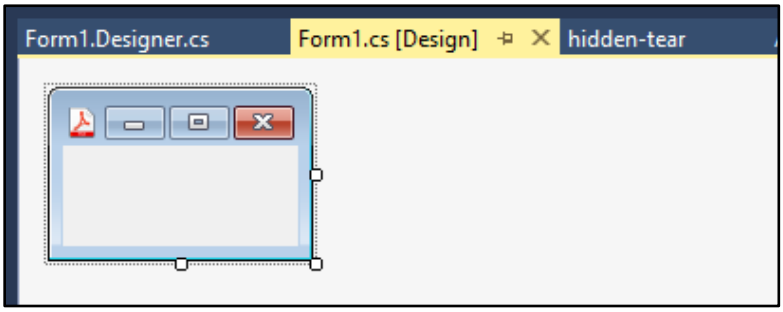


Figura 20. Diseño de Hidden Tear para que luzca como un archivo

[13] Es el análisis de una aplicación sin ejecutarla.

En la parte principal del Hidden Tear al principio de la función se observan las variables en las que está el targetURL, que contiene la dirección donde se van a enviar los datos que recolecte el malware de la máquina infectada. Ellos son el usuario de Windows (userName), el nombre de la computadora (computerName) y la dirección de la carpeta usuario (userDir) (ver figura 21).

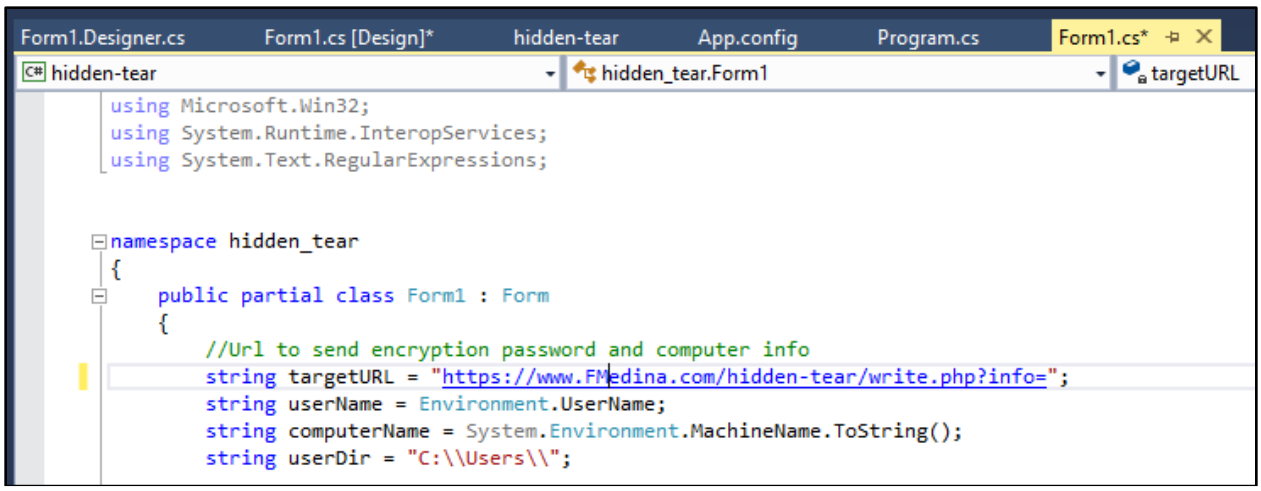


Figura 21. Datos que captura el malware para enviar a la dirección targetURL

Para que el malware pueda enviar la información se debe tener configurada el archivo write.php en el servidor (como se muestra en figura 22), donde se alojarán las claves privadas para desencriptar los archivos.

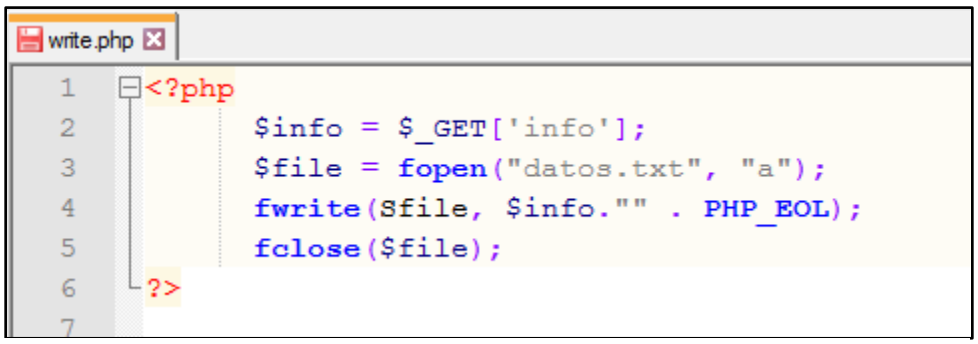


Figura 22. Archivo php que debe estar alojado en el servidor.

En el archivo write.php se encuentra la variable *$info* en donde va a recibir los datos que envían desde la máquina infectada, en la segunda línea se designa a la variable *$file* como

puntero del archivo datos.txt que debe estar ubicado en el mismo lugar que esta el archivo write.php en el servidor, y el "a" al final de la línea le da permiso de escritura. Luego, con el *fwrite* escribe en el archivo datos.txt los datos de la computadora, usuario y clave privada al terminar cierra el puntero al archivo.

El algoritmo de encriptación que utiliza Hidden Tear es el AES, este estándar fue publicado en el Federal Information Proccesing Standards Publication 197 (FIPS PUBS 197) por la National Institute of Standards and Technology (NITS) (Advanced Encryption Standard FIPS PUBS 197, 2001). Este algoritmo es un bloque de cifrado simétrico que puede encriptar y desencriptar información. Por lo que puede utilizar llaves de cifrado de 128, 192 y 256 bits para encriptar y desencriptar bloques de datos de 128 bits.

Hay 5 modos de operación confidenciales para utilizar en algoritmos cifrado como publica NITS (Division & Laboratory, 2001) el que se utiliza en el Hidden Tear es el CBC (Cipher Block Chaining) en el cual lo que hace primero es buscar el primer bloque de texto sin cifrar y la combina con un vector de inicialización (IV). Esta operación solo se hace en el primer bloque, luego realiza un "encadenamiento" de operaciones por el cual el primer bloque cifrado opera con el segundo bloque sin cifrar. Al cifrar el segundo bloque se combina con el tercer bloque sin cifrar y así sucesivamente hasta terminar con todos los bloques. Con esta técnica, si se alterara un solo bloque cifrado, no se podría desencriptar el archivo y quedaría corrupto para siempre.

Como se puede ver en el código de la figura 23, utiliza un tamaño de llave (AES.KeySize) de 256 bits por la que se tardarían décadas en descifrar, y como dice el Standard de AES se debe utilizar un bloque de 128 bits, luego crea una variable llave (var key) que la utiliza para crear la

llave AES de cifrado y la variable de inicialización para el modo de operación CBC que lo define en el AES.Mode.

```
AES.KeySize = 256;
AES.BlockSize = 128;

var key = new Rfc2898DeriveBytes(passwordBytes, saltBytes, 1000);
AES.Key = key.GetBytes(AES.KeySize / 8);
AES.IV = key.GetBytes(AES.BlockSize / 8);

AES.Mode = CipherMode.CBC;
```

Figura 23. Parte de código de Hidden Tear usando algoritmo AES y modo de operación CBC.

La clase void startAction es la que inicia al correr el malware y llama a las otras funciones del código.

Lo que realiza en esta secuencia de pasos (figura 24) es crear una contraseña de 15 caracteres con la función CreatePass(), eligiendo de forma aleatoria las letras minúsculas, mayúsculas, números y símbolos y la guarda en la variable *password*.

```
public void startAction()
{
    string password = CreatePassword(15);
    string path = "\\Desktop\\test";
    string startPath = userDir + userName + path;
    SendPassword(password);
    encryptDirectory(startPath,password);
    messageCreator();
    password = null;
    System.Windows.Forms.Application.Exit();
}
```

Figura 24. Parte de código de Hidden Tear en la que inicia el programa.

En la segunda línea de la función se crea la variable *path* con la dirección de la carpeta a la cual se van a encriptar los archivos, en este caso es en la carpeta test que está ubicado en el escritorio de la víctima. A lo que esa variable *path* se concatena con la dirección y nombre de usuario, que se había guardado al principio del código. La variable *password* que fue creada se envía por medio de la función SendPassword() agregando las variables computerName y userName hacia el servidor al archivo write,php.

En la función encryptDirectory() primero se define qué extensiones de archivos se van a encriptar como archivos de fotos o dibujo (.jpg, .png, .dwg, etc.) o de oficina (.xls, .doc, etc.). Luego busca los archivos a encriptar en la carpeta designada y en las subcarpetas. Para encriptar cada archivo llama a la función EncryptFile() en la que usa el tipo de dato byte[] y convierte el archivo en bytes. También realiza lo mismo con la contraseña por lo que la codifica para que quede guardada en bytes. Posteriormente, a esa contraseña la encripta con una función hash SHA256 para que no se pueda descifrar. Por último, utiliza la función AES_Encrypt() para encriptar el archivo con la contraseña hasheada, luego guarda el archivo encriptado con la extensión .locked.

Al terminar de encriptar todo llama a la función messageCreator() que es la que crea un mensaje amenazador en la que solicita realizar un pago en bitcoins para recuperar los archivos.

Luego borra la contraseña creada y finaliza el malware habiendo logrado su cometido.

Análisis dinámico[14]

Para realizar las pruebas de ejecución del ransomware se creó un entorno de pruebas por medio de Virtualbox (Virtualbox.org, 2017, https://goo.gl/DBZGho) que es un software que

[14] Es el análisis de una aplicación cuando está en ejecución.

permite virtualizar distintos sistemas operativos. Para lo anterior, se crearon tres computadoras que estuvieran en red de manera virtual con las características que se muestran en la tabla 1.

Tabla 1. *Características de las máquinas virtuales*

Máquina Virtual	Sistema Operativo	IP
Principal	Windows 8.1	172.16.1.2
Secundaria 1	Windows Xp	172.16.1.1
Secundaria 2	Ubuntu 17.04	172.16.1.3

Las características que se eligieron para las máquinas virtuales.

Las pruebas se hicieron en la máquina principal con Windows 8.1, ésta tenía dos adaptadores de red. El primero de ellos se utilizó para comunicarse con las otras máquinas virtuales, y por medio de esta red interna, se compartieron las carpetas mapeando las unidades. El segundo adaptador se comunicó al exterior con el servidor.

En la primera prueba se cambió el código de Hidden Tear en la función starAction (figura 24) en la variable startPath para que recorra todo el disco duro, pero se detuvo la encriptación mostrando un mensaje de error explicando que la aplicación no encripta los archivos que tienen permisos de administrador. Por ello, se probó modificando el startPath para que ataque la unidad mapeada Y: que era la carpeta compartida de Ubuntu, pero nuevamente apareció un mensaje de error que advertía que no se podía acceder a los archivos de solo lectura, como se muestra en la figura 25.

Figura 25. Captura de error en máquina virtual por acceso no autorizado a un archivo de solo lectura.

Ante esta situación, se modificó el código de Hidden Tear y se agregó una excepción para que omita los archivos con privilegios de administrador y de solo lectura. Se procedió a correr nuevamente el malware, logrando así encriptar todos los archivos que no tienen privilegios de administrador y de solo lectura. La encriptación de los archivos de la máquina principal y de la unidad mapeada Y: se realizó sin inconvenientes, como se muestran en figura 26, y 27.

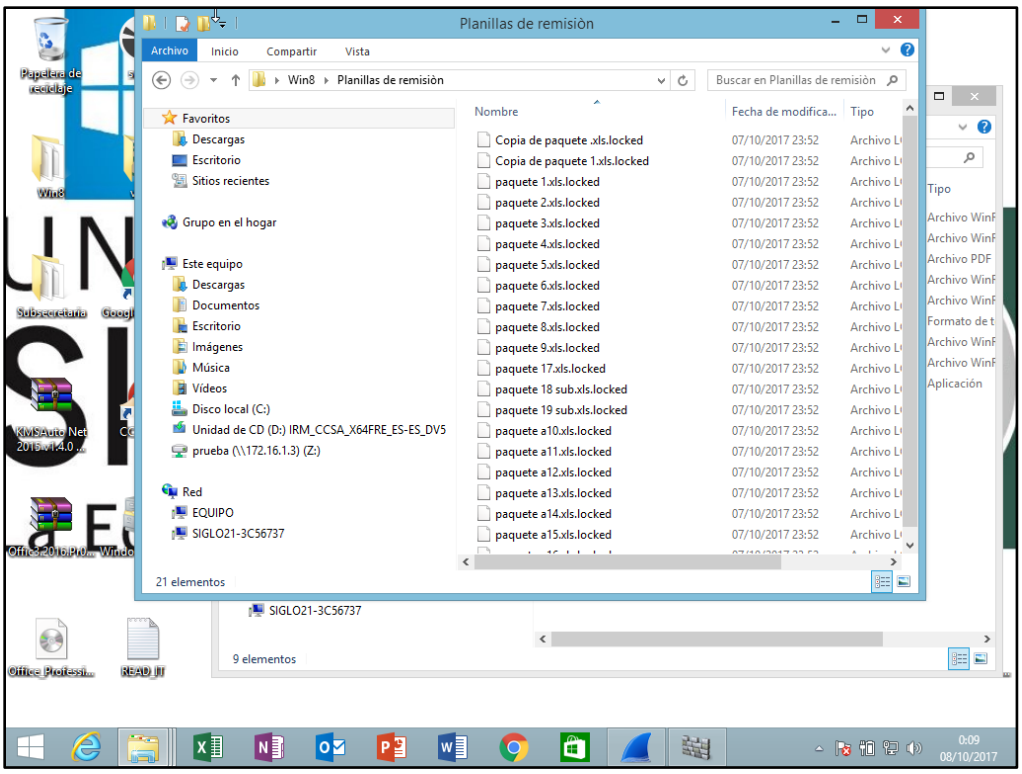


Figura 26. Captura de pantalla de carpeta de máquina principal encriptada.

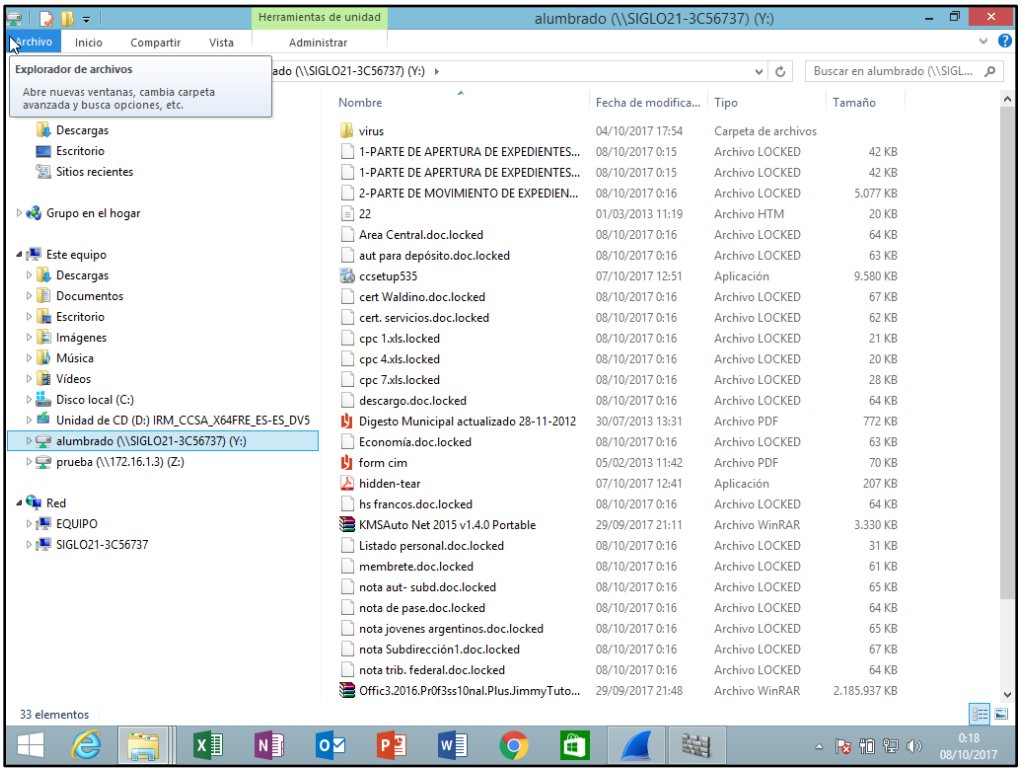


Figura 27. Captura de pantalla unidad mapeada Y: máquina con Windows XP.

Pero en la unidad Z: donde esta mapeada una carpeta de Ubuntu no se logró la encriptación ya que contaba con permisos de solo lectura, como se puede apreciar en la figura 28.

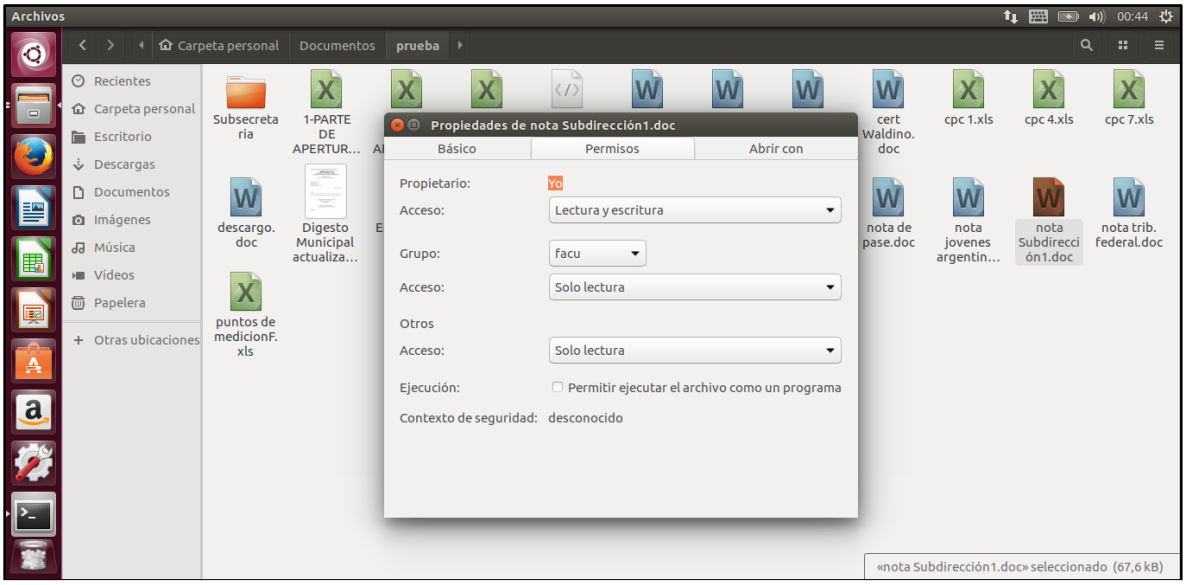


Figura 28. Captura de pantalla propiedades de la carpeta compartida de Ubuntu.

En cuanto se cambiaron los permisos de la carpeta del Sistema Operativo Ubuntu y se permitió la escritura de los archivos, al correr nuevamente Hidden Tear, se logró encriptar también la unidad mapeada. Ante esta situación se puede observar que al compartir los archivos esto no incide en qué sistema operativo se encuentre la carpeta original, ya que para comunicarse entre sistemas operativos se utiliza un protocolo de comunicación. Por lógica se puede decir que, al compartir carpetas y darle permisos a un usuario de lectura y escritura, éste puede modificar los archivos y cambiar la extensión. Por consiguiente, como se advirtió anteriormente, un malware es un programa con instrucciones. Estas operaciones pasan desapercibidas para cualquier antivirus ya que son las que comúnmente puede realizar cualquier usuario.

Al ejecutar el malware, se monitorearon las acciones que realizaba Hidden Tear, por medio de un programa llamado Process Monitor, como se puede ver en la figura 29. En él se observó que

realizaba la lectura de los archivos (Operation: ReadFile), cuando encontraba un archivo del tipo especificado (.doc, .xlsx, .pdf., .jpg) lo modificaba, escribiendo sobre éste (Operation: WriteFile) utilizando la criptografia. Al finalizar cambia, la extensión del archivo (Operation: SetRenameInformationFile).

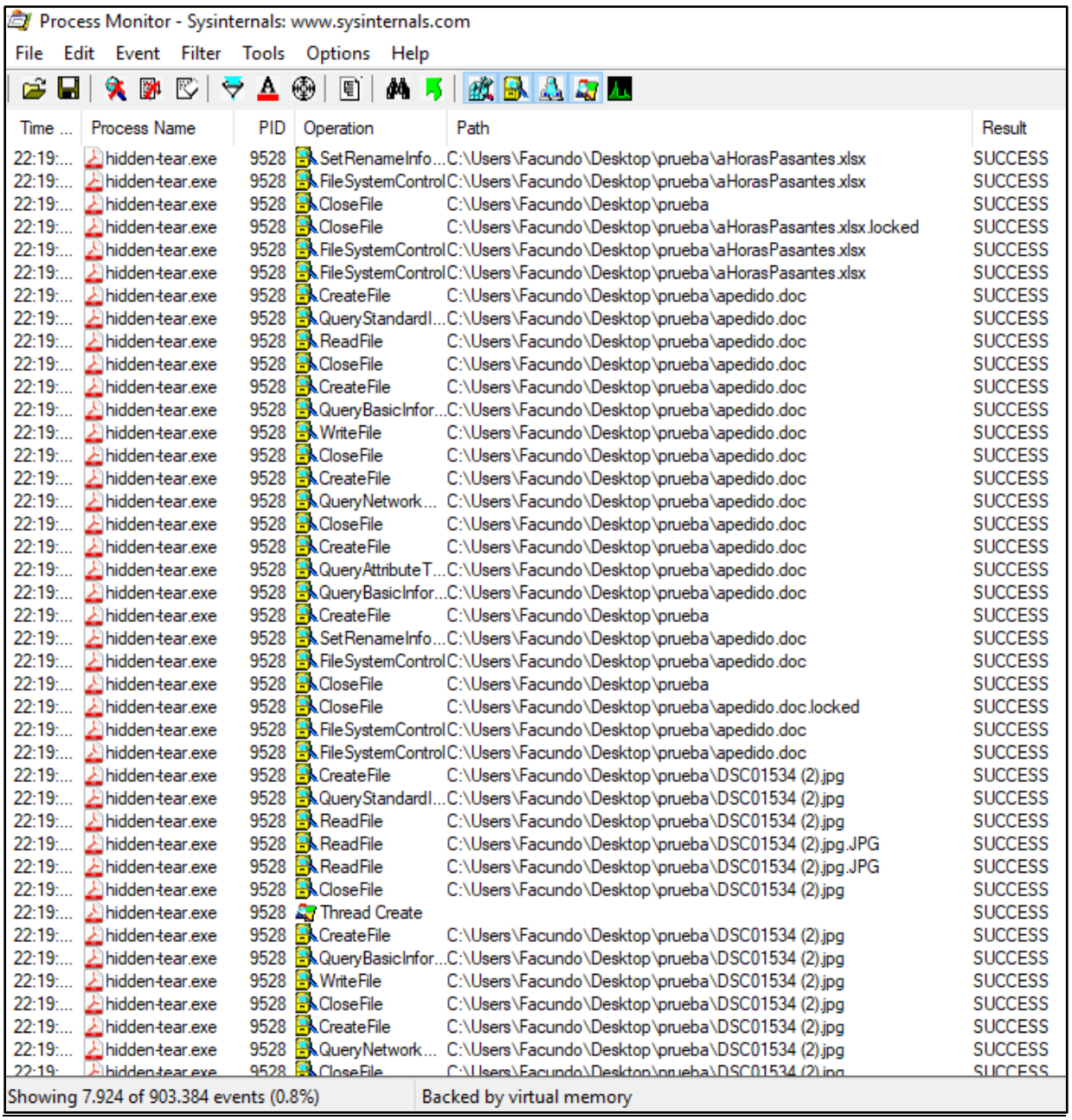


Figura 29. Captura de la actividad del Hidden Tear.

Continuando con el análisis del ransomware, se analizaron los protocolos que circularon por la red mientras estaba en ejecución. En la figura 30 se puede observar cómo busca el servidor con IP 31.170.164.206, para, luego de haberse comunicado, enviar la petición GET del protocolo HTTP que permite las transferencias de información por toda la red.

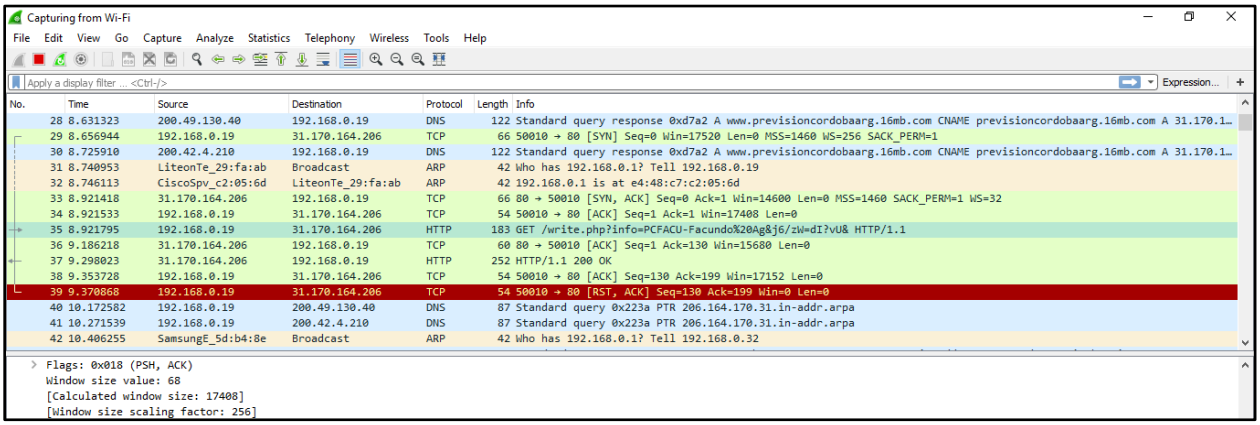


Figura 30. Captura de Wireshark cuando Hidden Tear se comunicaba con el servidor.

Esta petición solicita el recurso que se encuentra en el archivo write.php y a su vez envía información sobre el nombre del equipo, el usuario y la contraseña utilizada para encriptar los archivos, como se ve en el detalle de la figura 31. Luego, el servidor confirma la información recibida dando por concluida la comunicación.

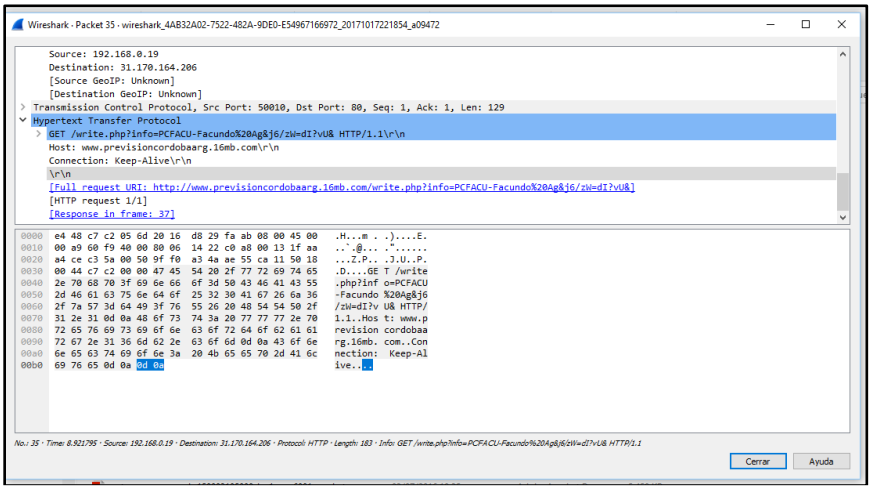


Figura 31. Captura del detalle del protocolo HTTP enviando la información de la computadora.

En cuanto a la comunicación con la red interna se puede apreciar en la figura 32 cómo se utiliza el protocolo SMB para enviarse peticiones entre la máquina infectada y las computadoras con carpetas compartidas, en las que el proceso del ransomware pide información de los archivos que están almacenadas en ellas.

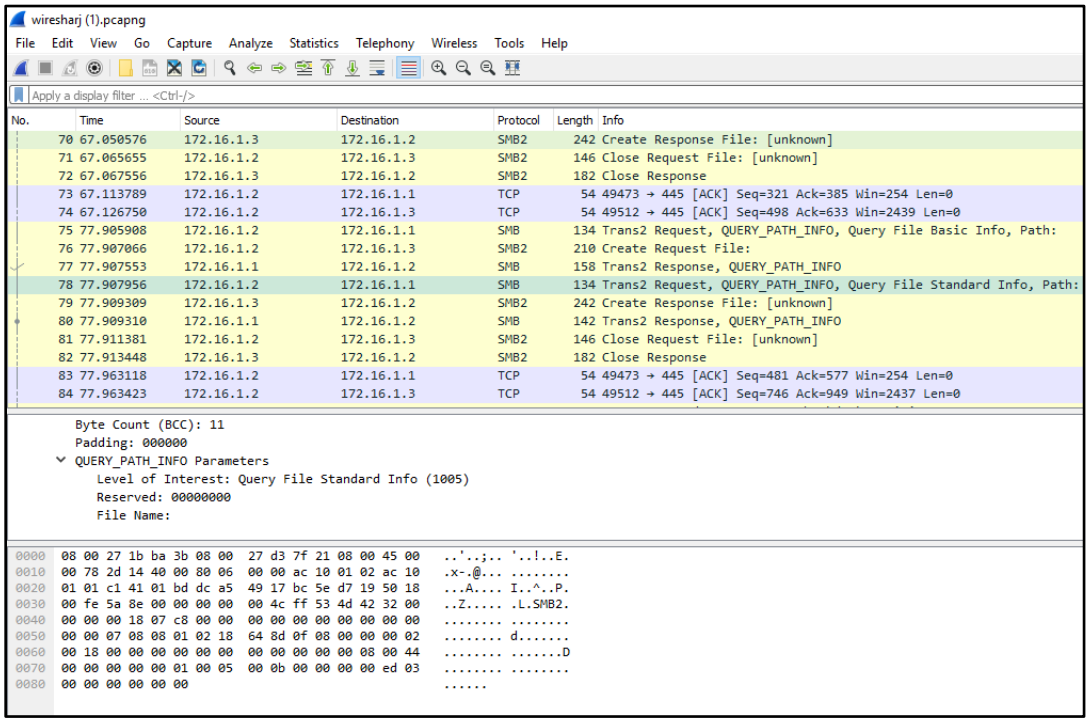


Figura 32. Peticiones por medio del protocolo SMB entre las computadoras de la red interna.

Al obtener acceso a los archivos, los modifica y cambia su extensión, como se observa en la figura 33.

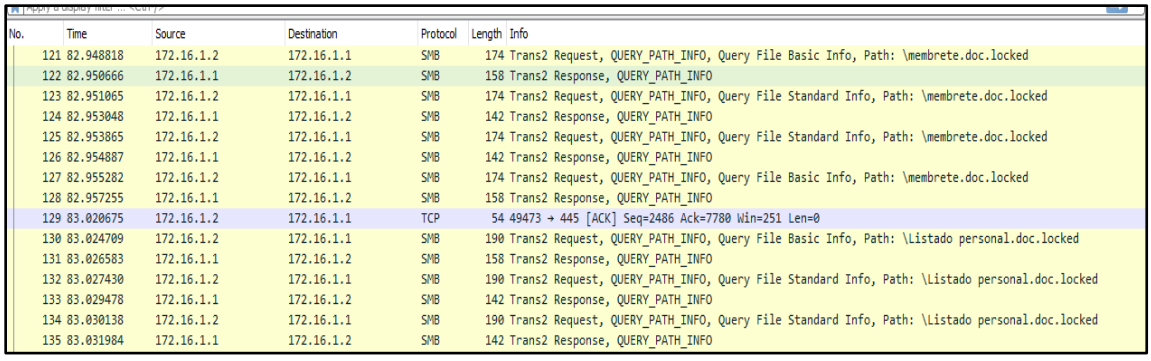


Figura 33. Modificación de la extensión del archivo en las computadoras con unidades mapeadas.

Para finalizar este análisis, se tuvo en cuenta que estos tipos de ransomware buscan archivos con extensiones específicas como .jpg que son imágenes, .doc documentos de Word, etc. Por lo que se modificaron algunas extensiones, como por ejemplo a .jpg como .JPG, y a .doc como .word, como se muestra en la figura 34.

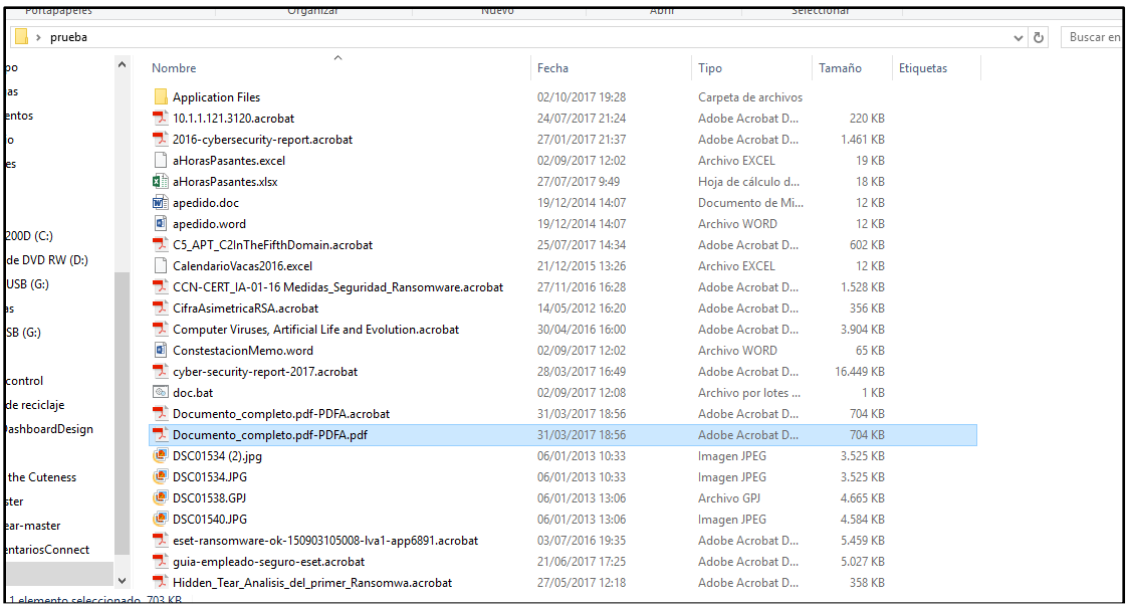
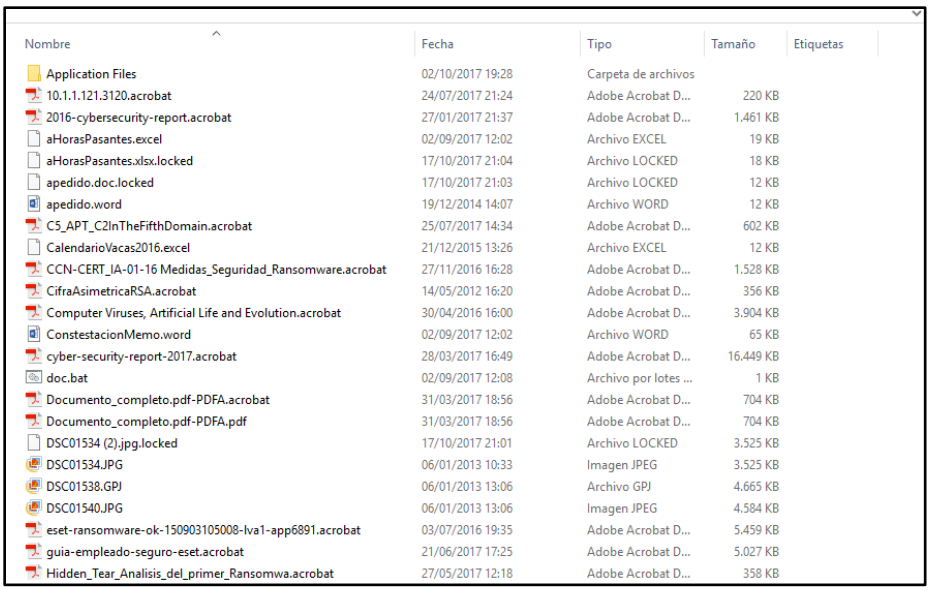


Figura 34. Carpeta de prueba con extensiones de archivo modificados

Al ejecutar el malware, se obtuvieron los siguientes resultados (figura 35), los archivos con extensión .doc, .xlsx y .jpg fueron encriptados y modificada su extensión con .locked. En cambio, los modificados .word, .acrobat, .excel, .JPG no fueron encriptados y se pudieron utilizar, al elegir la aplicación correspondiente para su uso.



Nombre	Fecha	Tipo	Tamaño	Etiquetas
Application Files	02/10/2017 19:28	Carpeta de archivos		
10.1.1.121.3120.acrobat	24/07/2017 21:24	Adobe Acrobat D...	220 KB	
2016-cybersecurity-report.acrobat	27/01/2017 21:37	Adobe Acrobat D...	1.461 KB	
aHorasPasantes.excel	02/09/2017 12:02	Archivo EXCEL	19 KB	
aHorasPasantes.xlsx.locked	17/10/2017 21:04	Archivo LOCKED	18 KB	
apedido.doc.locked	17/10/2017 21:03	Archivo LOCKED	12 KB	
apedido.word	19/12/2014 14:07	Archivo WORD	12 KB	
C5_APT_C2InTheFifthDomain.acrobat	25/07/2017 14:34	Adobe Acrobat D...	602 KB	
CalendarioVacas2016.excel	21/12/2015 13:26	Archivo EXCEL	12 KB	
CCN-CERT_IA-01-16 Medidas_Seguridad_Ransomware.acrobat	27/11/2016 16:28	Adobe Acrobat D...	1.528 KB	
CifraAsimetricaRSA.acrobat	14/05/2012 16:20	Adobe Acrobat D...	356 KB	
Computer Viruses, Artificial Life and Evolution.acrobat	30/04/2016 16:00	Adobe Acrobat D...	3.904 KB	
ConstestacionMemo.word	02/09/2017 12:02	Archivo WORD	65 KB	
cyber-security-report-2017.acrobat	28/03/2017 16:49	Adobe Acrobat D...	16.449 KB	
doc.bat	02/09/2017 12:08	Archivo por lotes ...	1 KB	
Documento_completo.pdf-PDFA.acrobat	31/03/2017 18:56	Adobe Acrobat D...	704 KB	
Documento_completo.pdf-PDFA.pdf	31/03/2017 18:56	Adobe Acrobat D...	704 KB	
DSC01534 (2).jpg.locked	17/10/2017 21:01	Archivo LOCKED	3.525 KB	
DSC01534.JPG	06/01/2013 10:33	Imagen JPEG	3.525 KB	
DSC01538.GPJ	06/01/2013 13:06	Archivo GPJ	4.665 KB	
DSC01540.JPG	06/01/2013 13:06	Imagen JPEG	4.584 KB	
eset-ransomware-ok-150903105008-lva1-app6891.acrobat	03/07/2016 19:35	Adobe Acrobat D...	5.459 KB	
guia-empleado-seguro-eset.acrobat	21/06/2017 17:25	Adobe Acrobat D...	5.027 KB	
Hidden_Tear_Analisis_del_primer_Ransomwa.acrobat	27/05/2017 12:18	Adobe Acrobat D...	358 KB	

Figura 35. Carpeta de prueba luego de ejecutar Hidden Tear

9.3 Análisis de EDA2

El segundo ransomware creado por Utku Sen tiene la misma base que el Hidden Tear, pero el EDA2 tiene nuevas funcionalidades.

La primera diferencia con Hidden Tear es la carpeta WebPanel, que al entrar se pueden observar los archivos PHP y la librería para con esto tener un servidor C&C que gestione todas las infecciones.

Análisis estático

Cuando pasamos al proyecto de EDA2, muchas funciones son las mismas que se utilizaron en Hidden Tear por lo cual, en este análisis, se explicarán solamente las funciones que se modificaron y las nuevas que se agregaron al EDA2.

Al utilizar el Servidor C&C se modificaron algunas variables, como se ve en la figura 36 a generatorUrl y a keySaveUrl que apuntan a los archivos que contiene el servidor. Además de

utilizar una clave con el algoritmo AES, como hace el Hidden Tear le agrega una llave RSA de 2048 bits de longitud para proteger la clave privada y la pública, para luego enviar la clave pública a la máquina infectada, y guardar la clave privada en el servidor.

```
namespace eda2
{
    public partial class Form1 : Form
    {
        [DllImport("user32.dll", CharSet = CharSet.Auto)]
        private static extern Int32 SystemParametersInfo(UInt32 action, UInt32 uParam, String vParam, UInt32 winIni);
        private static bool OAEP = false; //Optimal Asymmetric Encryption Padding
        const int keySize = 2048; //key size for RSA algorithm
        string publicKey;
        string encryptedPassword; //AES key encrypted with RSA public key
        string userName = Environment.UserName;
        string computerName = System.Environment.MachineName.ToString();
        string userDir = "C:\\Users\\";
        string generatorUrl = "http://www.example.com/panel/createkeys.php"; //creates public key
        string keySaveUrl = "http://www.example.com/panel/savekey.php"; //saves encrypted key to database
        string backgroundImageUrl = "https://i.imgur.com/5iVZ4gf.jpg"; //desktop background picture
        string aesPassword;
```

Figura 36. Primera parte del código EDA2.

Tiene una función getPublicKey() por medio de la cual la máquina infectada con EDA2 se comunica con el servidor a través de un POST (mensaje HTTP) enviándole como parámetros el nombre del usuario y nombre de la computadora; el servidor Web al recibir la información le contesta con la clave pública RSA y guarda la clave Privada RSA. El ransomware crea una clave AES igual a como hace Hidden Tear e infecta los archivos en las carpetas definidas, después, esa clave AES la encripta por medio de la clave pública y se la envía al servidor Web para protegerla de cualquier intercepción, ya que necesitarían la clave privada para poder desencriptar los archivos. Este método se llama Criptografía Hibrida, utiliza de manera combinada Criptografía Simétrica (Clave AES) para cifrar los archivos y Criptografía Asimétrica (Clave Publica RSA y Clave Privada RSA) para proteger la clave que cifró los archivos.

Por último, se agrega una imagen que se coloca como protector de pantalla en la máquina infectada apenas termina de encriptar los archivos.

Análisis dinámico

En la ejecución del EDA2 se observó que los procesos de modificación eran similares a Hidden Tear (figura 37) en el que solo cambia el nombre del proceso.

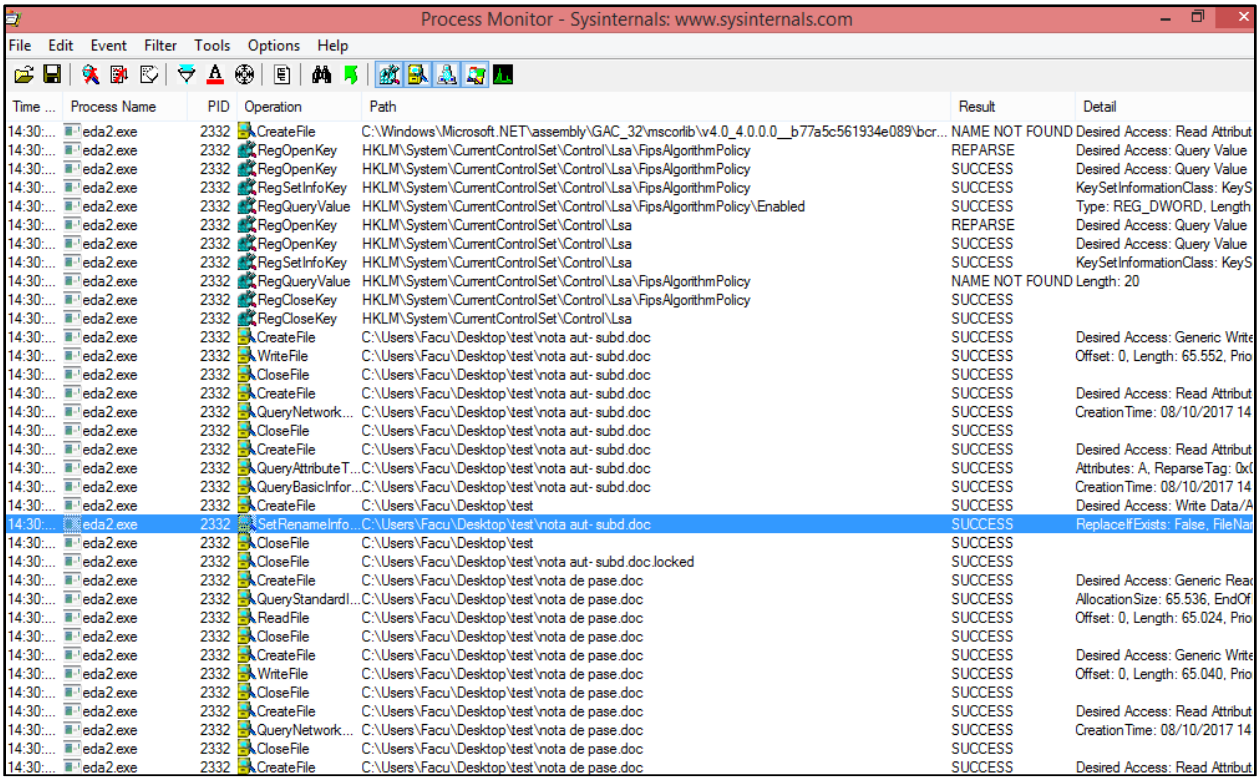


Figura 37. Procesos del ransomware EDA2.

Por tanto, para probar la comunicación de EDA2 con el servidor, se debió crear una tabla en una Base de Datos que tenía estos campos: id, nombre de equipo(pcname), usuario(username), clave privada(privatekey) y clave AES encriptada(aesencrypted). En la primera prueba de ejecución se observó que en las tablas se mostraban todos los datos excepto la clave AES, esto se debió a que el código de la clase savekey.php actualiza la tabla buscando el número de id, y el campo id en este caso era null(vacío) por lo que no encontraba el campo donde actualizar. Ante esta situación, se modificó agregando el atributo auto-incremental, y al agregar una nueva fila en este campo id, se incrementa en uno. Resuelto esto, otro error encontrado es que, al repetirse el

nombre del equipo, la base de datos busca la primera coincidencia en forma ascendente en la que modifica el campo aesencrypted dando un nuevo valor, y dejando inutilizable la desencriptación para todos los campos con nombre de equipo repetido (figura 38).

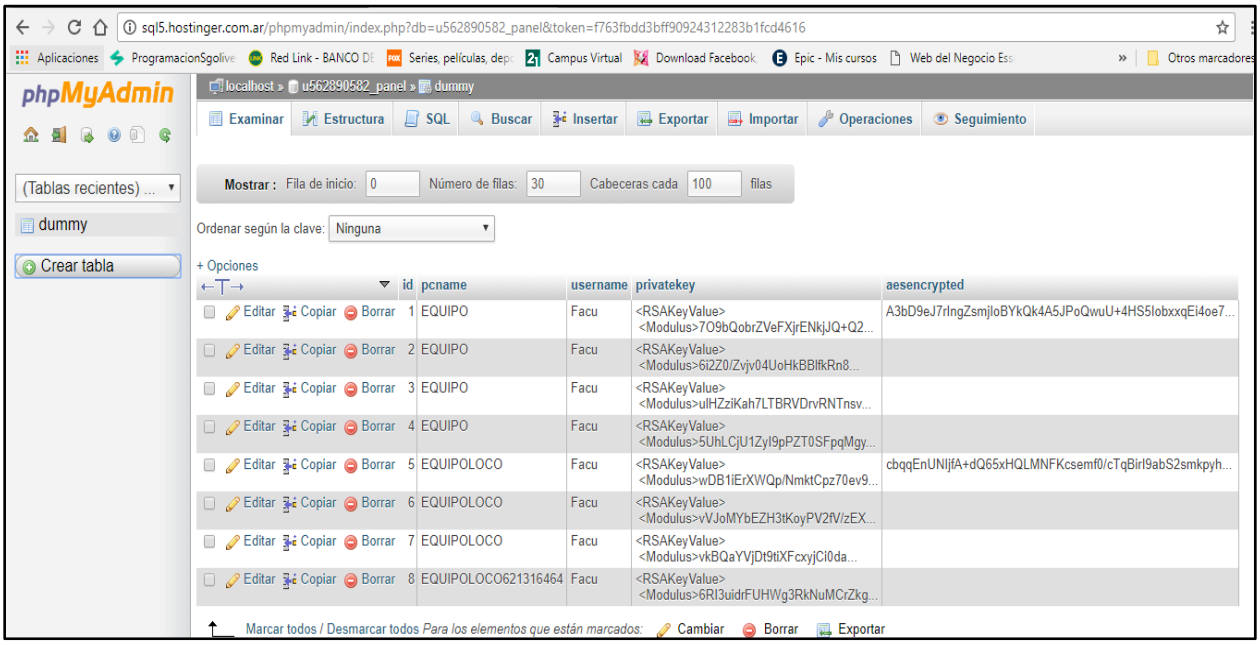


Figura 38. Tabla dummy con los datos obtenidos.

Ante la situación planteada se podrían dar dos soluciones, una es ordenar el id en forma descendente para que busque el último campo de nombre de equipo. Otra opción es buscar el nombre de equipo con el campo aesdecrypted vacio (null), para así asegurarse de no modificar una fila erróneamente.

En cuanto a la comunicación de la máquina infectada con el servidor C&C se puede ver detalladamente cómo se comunica por medio del protocolo TCP, para luego enviar una petición POST con la información del usuario y nombre del equipo a lo que solicita la clave pública (Figura 39), que posteriormente el servidor le envía.

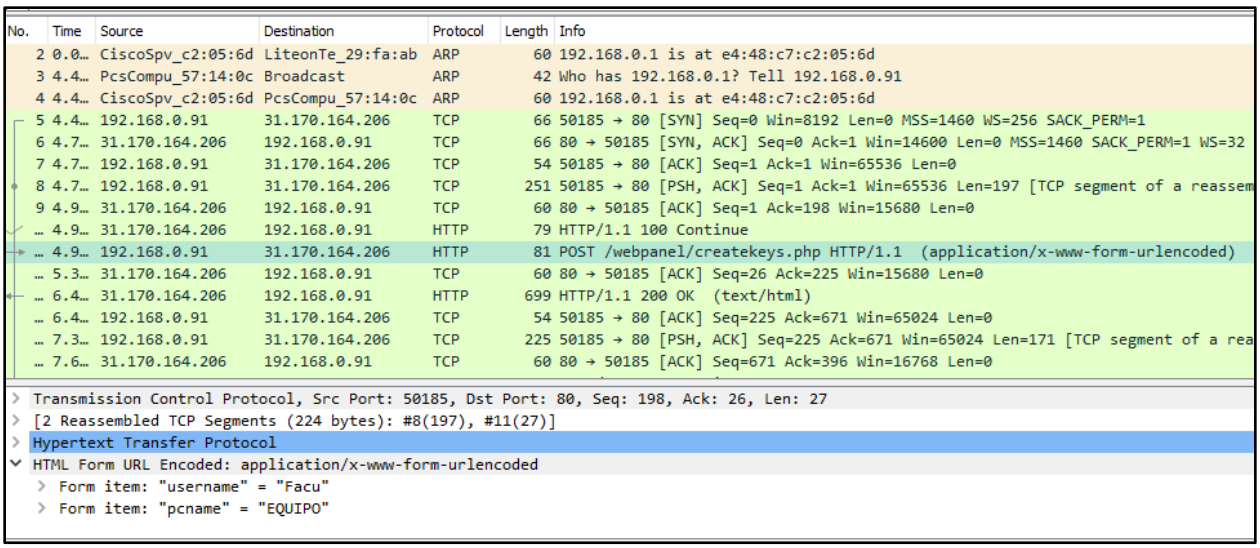


Figura 39. Comunicación de EDA2 con el servidor solicitando clave pública.

Al recibir la clave pública, EDA2 encripta la contraseña y envía otro POST al servidor con la contraseña y el nombre del equipo, como se ve en la figura 40.

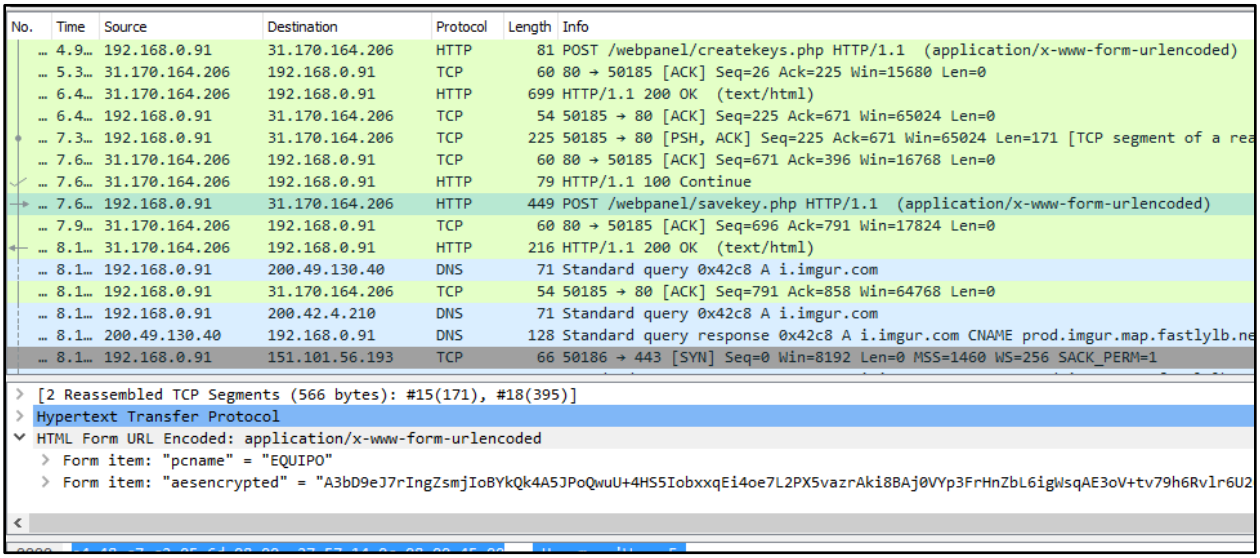


Figura 40. Comunicación de EDA2 con el servidor guardando la clave AES encriptada.

Luego, solicita la imagen que cambiará el fondo de la pantalla advirtiendo que fueron encriptados los archivos.

En cuanto al Panel Web para ver la información de las computadoras infectadas y las claves, se debe ingresar con usuario y contraseña, y luego se puede ver (figura 4)1 la tabla con los datos de las computadoras infectadas y al final el botón Decipher. Al tocar dicho botón ejecuta el desencriptador que utiliza la clave privada (privatekey) y la llave AES para conseguir la contraseña que se utilizó para encriptar los archivos de la máquina infectada.

Figura 41. Panel con la info de la computadora infectada.

10. Análisis de las entrevistas a personal de seguridad de empresas

En el diseño metodológico del presente trabajo se anticipaba que, como fuentes secundarias de indagación, se implementarían entrevistas a informantes claves (anexo 1), definidos a partir de su tarea como personal de seguridad informática de empresas y organizaciones de la Ciudad de Córdoba.

Las entrevistas se organizaron alrededor de ejes temáticos que se configuraron a partir de la exploración bibliográfica ya desarrollada. Se indagó acerca de las medidas de seguridad con las que contaba la organización, en particular resultaba significativo recuperar si poseían sistemas de detección de prevención, políticas de seguridad y sitios de contingencias.

Por otra parte, se intentó rastrear si en las organizaciones de pertenencia de los entrevistados se reconocían ataques de ransomware y qué medidas y herramientas de solución implementaron.

De manera indirecta, se tuvo la intencionalidad de advertir el nivel de información que poseían sobre ransomware y las formas de prevención y recuperación del sistema.

Cabe destacar que resultó complejo acceder a la concreción de las entrevistas y la actitud de reserva fue la predominante en los sujetos entrevistados. Lo anterior se acentuó particularmente en las organizaciones que brindan un servicio de salud.

Los entrevistados pertenecen a Organizaciones y/o empresas tanto privadas como públicas, radicadas en la ciudad de Córdoba: Globant, La Lacteo, Tarjeta Naranja, Sanatorio Allende y Municipalidad de Córdoba.

Los informantes entrevistados expresaron tener un buen sistema de Back Up que es muy importante para proteger los datos, pero también se advierte que no hay un plan general de seguridad informática, sino más bien cada empresa tiene su propia forma de protegerse de los ataques. Luego de repasar las entrevistas se decidió preguntar si tenían capacitación en seguridad informática y si utilizaban alguna metodología o norma, aunque solo respondieron algunos de los entrevistados.

Respecto a lo anterior, resulta muy interesante lo que indica Martin Bono, empleado en seguridad de la Empresa La Lacteo, sobre las políticas de seguridad de la empresa, que restringen los permisos de administrador y también inhabilitan el uso de pen drive para asegurarse que no entre ningún virus por ese medio. Otra medida efectiva es el cuidado respecto a cómo ingresan los usuarios en el que está sectorizado el sistema de archivos, por lo que si se infecta una máquina solo infecta el área a la que pertenece el usuario. Lo que sí resulta

preocupante es que la Empresa La Lacteo tenga el correo tercerizado, ya que, como explica F-Secure (State of Cyber Security, 2017, pág. 20). Cada parte o sector tercerizado que tenga la empresa incrementa la superficie de ataque por lo que esa decisión que tomaron no es muy recomendable. Otro punto importante es que tienen el Antivirus centralizado para monitorear y actualizar todas las terminales de la empresa, por lo que no hay que esperar que el usuario actualice el antivirus en la terminal. Esto puede ocasionar que no estén las firmas de virus actualizadas y pueda ingresar alguno nuevo.

Por otro lado, respecto a la empresa La Lacteo, según lo expresado por Bono, no realizaron capacitaciones y tampoco siguen ninguna norma, lo que puede aumentar los riesgos de infección, situación que es evitada porque hay personal que se capacita de manera autónoma y por decisión personal.

Por su parte, la empresa Tarjeta Naranja sigue un plan de seguridad estandarizado como la ISO 27001, que es un Sistema de Gestión de la Seguridad de la Información, además que se complementa con la ISO 27005, que es una guía para la gestión del riesgo de la seguridad de la información. Muy importante es la decisión de mantener los sitios de contingencia en otros lugares para respaldar los datos de cualquier catástrofe que pueda ocurrir, y el uso de herramientas como IPS y DLP para detectar intrusos en la red, ya que manejan valiosa información financiera de los clientes.

En cuanto a los dos ataques de ransomware que sufrió la empresa Tarjeta Naranja, se advierte que la seguridad falló poniendo en riesgo los datos personales y financieros de los clientes. Se puede plantear como hipótesis que el sistema quedó desconectado hasta que se pudo realizar la recuperación mediante el Back up, que seguro trajo problemas en todos los departamentos de la

empresa y con los clientes que no pudieron utilizar la tarjeta en los comercios adheridos. También se pone en duda si es verosímil que se recuperó toda la información, y se entiende que decir lo contrario, en el contexto de una entrevista, se percibe como perjudicial para la empresa.

En cuanto a medidas implementadas luego de los ataques mencionados, mejoraron las barreras defensivas para evitar uno próximo, también es muy valorable la concientización que realizan a los usuarios de la empresa.

En la entrevista realizada al informante perteneciente al Sanatorio Allende se puede observar una buena infraestructura en seguridad, pero igualmente tuvieron ataques de ransomware que aseguran que no se perdieron archivos críticos ya que contaban con backup de ellos. A pesar de que se podrían haber perdido datos personales o de otra índole, el Sanatorio no consideró esos datos como importantes, por lo que no pagaron el rescate. Respecto a lo anterior se considera que, si bien no eran archivos críticos, igual pudo ser información importante que en un futuro se pueda necesitar. Del acontecimiento anterior se extrae como positivo que gracias a que en su infraestructura tiene configurada las redes separadas por sectores, y además están monitoreadas constantemente lograron que el ransomware no se esparza a todas las máquinas de la institución, operando esto como prevención de un problema mayor.

El entrevistado perteneciente a Globant explica sobre su experiencia en seguridad en la organización en la cual utilizan servidores centralizados que guardan la información, y si las terminales son infectadas con algún malware que ocasiona pérdida de información, pueden recuperarla con estos servidores, aunque no asegura que los datos puedan haber sido robados y utilizados con fines negativos. Otro punto que señala es que utilizan servidores Linux en los que no vio casos de ataque, pero hay ransomware que atacan estos servidores como el Erebus, por lo

que no hay que tener una mirada superficial sobre su seguridad. Un punto importante es que brindan capacitación en seguridad para los agentes que no tienen conocimientos en el tema, y cuentan con la certificación ISO 27001, que es un estándar para la seguridad de la información.

Por último, el entrevistado perteneciente a una institución pública, señala que en la Municipalidad de Córdoba tienen filtrado de spam y malware, aunque de todos modos tuvieron un incidente con un virus en el que el filtrado de malware no funcionó, por ser un virus nuevo del que no se tenían datos. Esto generalmente se llama vulnerabilidad del día 0, que son vulnerabilidades desconocidas que explotan los ciberdelicuentes para llegar a su objetivo. Al tener servidores de backups aislados de la red, el malware no puede ingresar, a menos que una persona interna lo ingrese por su cuenta. Lo que tiene en contra esto es que el backup se hacer por las noches, por lo que un ataque podría desaparecer información de un día entero. En cuanto a que no tienen backups de las terminales, los archivos que tenga el usuario en Word o Excel pueden ser atacados por un ransomware, y a menos que el usuario realice respaldos diarios de sus archivos, ocasiona la pérdida de la información que contenía la computadora.

11.Conclusiones

Tras el análisis del ransomware en el presente trabajo, se pudo afirmar que la principal causa de infección por este malware es por medio de la acción de un usuario que ejecuta el archivo en que los antivirus no logran detectar primero debido a las distintas mutaciones del virus. En segundo lugar, como se observó en el análisis dinámico los procesos que realiza son acciones comunes que pueden ser hechas por cualquier usuario o proceso.

Ante esta situación y luego de las pruebas realizadas, surge el interrogante de cómo realizar una detección temprana de este malware antes de que encripte todos los archivos. Como se

observó en el análisis dinámico, la ejecución del ransomware modificaba los archivos, al ser esta acción comúnmente usada por cualquier proceso, no sería óptimo detenerlo pidiendo confirmación de estar realizando modificaciones. Sí sería motivo de prueba para futuras investigaciones la detección del cambio de extensión de un archivo, que es una acción muy rara vez utilizada, para luego detener el proceso y se verifique que el usuario esté realizado la modificación. Si se confirma que el usuario no cambió la extensión se debería detener el proceso, y a su vez advertir al usuario y a la empresa que puede existir un malware en la computadora.

Otro punto que se pudo dilucidar es que, si los archivos tienen privilegios de administrador o son de solo lectura, y la máquina donde corre el ransomware es un usuario sin privilegios, estos tipos de archivos no podrán ser encriptados, ya que necesitaría romper de algún modo los privilegios u obtener la clave del administrador. En las unidades mapeadas se debe tener especial cuidado, ya que podrían infectar a todo el sistema, por lo que es recomendable que para modificar un archivo se pida permiso de administrador o usuario y contraseña, y de esta manera evitar el encriptamiento.

Para finalizar con lo que dejó el análisis del código y ejecución del ransomware, una práctica que podría ayudar a la prevención es cambiar las extensiones de los archivos por otros que sean inexistentes en el uso computacional. Un ejemplo de lo anterior, sería que para documentos Word en Windows, en vez de usar la extensión .doc, utilizar la extensión .document, ya que, como se vio en el análisis, primero buscan la extensión y luego modifican el archivo. Una empresa podría implementar esto y configurar qué aplicación debe abrir cada extensión. Puede que implementarlo sea costoso, pero quizás para archivos críticos sea una buena solución.

Luego del recorrido realizado por la bibliografía especializada y recuperando las expresiones de protagonistas pertenecientes a las organizaciones se advirtió la importancia de profundizar la concientización y formación sobre las amenazas que existen en Internet como Phising, malware o Ingeniería Social.

Existen múltiples versiones de ransomware, pero por lo general utilizan el mismo mecanismo de propagación que consiste en el envío de un archivo ejecutable por algún canal de comunicación. Lo que primero deberían hacer los sistemas operativos es mostrar toda la extensión del archivo, para así detectar que no es un Word o PDF sino un ejecutable (.exe), que seguramente es un virus camuflado. Otra medida de prevención que podría realizar la organización es el filtrado del correo de tipos de archivo como .exe, .zip o .rar aunque esta medida puede que genere animosidad en los usuarios y busquen formas de poder recibirlos, también se debe tener en cuenta que mejoraría mucho la seguridad.

Se considera que uno de los aportes de lo indagado es haber profundizado en cuanto al funcionamiento de las distintas versiones de ransomware del tipo cifrador y donde se pudo determinar que siguen un patrón de funcionamiento muy similar:

- Clave de X bits,
- Encriptamiento de archivos (algunas versiones encriptan el disco duro),
- Pedido de dinero (generalmente en bitcoins) para rescatar archivos.

Las diferencias radican en las mejoras que le pueden agregar al ransomware:

- Servidor C&C (Servidor de Comando y Control) su función es dar instrucciones a las maquinas infectadas con malwares para luego recibir información de estas.

- Clave hibrida.
- Detección de ejecución en máquina virtual.
- Propagación del virus por la red y en unidades mapeadas.

En cuanto al objetivo de encontrar las soluciones para recuperar los archivos, se debe aclarar que si el código malicioso está bien hecho y tiene una clave de 2048 bits o más habría que esperar años para descifrar la clave privada o que haya computadoras con un poder de procesamiento mayúsculo. Por lo contrario, si hay errores en el código o han dejado algún backdoor en donde se pueden recuperar las claves, muchos expertos en seguridad han conseguido y han puesto a disposición distintas herramientas de recuperación.

En los casos que no se puedan recuperar los archivos, se debe tener en cuenta primero que, como se observó, al pagar el rescate se financia estas prácticas extorsivas, segundo que el envío de la clave para desencriptar los archivos depende de los ciberdelicuentes, que, si está mal implementado el código, aunque tengan predisposición para enviar la clave, no lo podrán hacer.

Con el análisis sobre las empresas y las estadísticas recolectadas, se puede afirmar que los cibercriminales están redirigiendo el ransomware hacia organizaciones, sobre todo de servicios como hospitales en donde la información es crítica. Cada organización debe realizar su plan de seguridad y tomar medidas preventivas para cualquier tipo de ataque, y en definitiva, no se debe simplificar la problemática de la Seguridad de la Información.

De lo recabado en las entrevistas es llamativo como son escasas las herramientas técnicas y conceptuales que implementan las organizaciones o las empresas en relación a la capacitación de los sujetos a cargo de la seguridad informática. En relación a esto, parecería que las instancias de

capacitación o de recepción de la información se resuelven más individualmente y como una opción del técnico a cargo. Las nuevas tecnologías tienen un avance constante como también las nuevas formas de atacarlas, por lo que se debe concientizar a las empresas en la importancia de destinar recursos a la seguridad informática. En tanto que los organismos estatales competentes deberían controlar que las empresas y organizaciones cumplan la ley de Protección de los Datos Personales.

Sobre evaluar el impacto que realiza el ransomware en las organizaciones, se pudo observar por medio de las entrevistas y la información recabada que el impacto va a depender del rubro que tenga la empresa. Si se trata de una empresa que brinda servicios de salud como el Sanatorio Allende el impacto es muy grande, aunque se cuente con respaldo de datos, la recuperación puede tardar horas valiosas y perjudicar un paciente. En la entrevista realizada a este sanatorio se constató que tuvieron pérdida de información, pero no lo consideraron importante. Esto no debe minimizarse en sus posibles efectos, especialmente en un sanatorio donde toda información de la salud de una persona es valiosa. El impacto que puede ocasionar en una empresa financiera como Tarjeta Naranja es importante, en cuanto a las pérdidas monetarias que pueden presentarse si el sistema está detenido y los comercios no pueden realizar las transacciones. La pérdida más importante es la credibilidad que puede tener la empresa si extravían los datos personales de sus clientes, y el costo que conlleva su recuperación. En otras empresas con otro rubro como el de alimentación o de gobierno el costo es menor, ya que la detención del sistema no origina tantas complicaciones, pero si lo ocasionaría si no se tiene respaldo de los datos con la consecuente pérdida total de la información.

Se debe tener en cuenta en futuras investigaciones no solo el secuestro de datos, sino que con el avance del Internet de las Cosas (IoT), en donde cada vez más artefactos están conectados

(auto, televisor, heladera, cámaras, micrófono, GPS, sensores de movimiento, de calor), en un tiempo no muy lejano el secuestro de las cosas materiales va a ocurrir y los ciberdelicuentes usarán eso a su favor.

Este panorama a su vez se complejiza ya que con backup no se soluciona el problema, sino que hay que mejorar la seguridad de los dispositivos y concientizar al usuario común de los riesgos de no mantener un buen uso de la tecnología.

Algunas de las soluciones para combatir el virus estudiado, que se desprenden del análisis de este trabajo y que está relacionado con nuestro campo profesional a desarrollar en las organizaciones y/o empresas:

- Elaboración de un Plan de Seguridad Informática,
- Concientización para formar un empleado seguro,
- Formación para la elaboración de un Plan de Prevención,
- Asesorar para una infraestructura de red dividida por sectores,
- Instalación de software que detecte intrusos en la red,
- Backup de los datos,
- Implementar unas buenas barreras de defensa con artilugios como Firewall, servidores proxy, VPN, honeypot[15].

[15] Tarro de miel en donde su función es atraer ataques de ciberdelicuentes en un ambiente seguro para estudiar sus formas de ataque.

Finalmente, es importante destacar la importancia de realizar conjuntamente con los procesos de indagación teórica, el análisis también desde las prácticas y experiencias que llevan a cabo los sujetos a cargo de la seguridad informática. Es posible detectar demandas que las organizaciones sociales tienen sobre el campo profesional de la Ingeniería en Software, y de esta manera poder realizar propuestas de avances situadas en las estructuras informáticas existentes y la creación de nuevas propuestas.

Bibliografía

Abrams, L. (2013 de octubre de 2014). *CryptoLocker Ransomware Information Guide and FAQ.* Recuperado el 5 de abril de 2017, de Bleeping Computer: https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

Abrams, L. (16 de febrero de 2016). *The Locky Ransomware Encrypts Local Files and Unmapped Network Shares.* Recuperado el 12 de mayo de 2017, de Bleeping Computer: https://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/

Adam Young, M. Y. (1996). Cryptovirology: Extorsion-Based Security Threats and Countermeasures . *IEEE Computer Society Press*, 129-141.

Akashdeep Bhardwaj, V. A. (2016). Ransomware Digital Extortion: A Rising New Age Threat. *Indian Journal of Science and Technology*, 1-5.

Axel Buecker, Kent Browne, Louis Foss, Jaco Jacobs, Vladimir Jeremic, Carsten Lorenz, Craig Stabler, Joris Van Herzele. (2011). *IBM Security Solutions Architecture for Network, Server, and Endpoint.* IBM RedBoooks.

Barroso, J. (13 de abril de 2015). *Unos Hackers bloquean 400.000 archivos de Ifema*. Recuperado el 25 de septiembre de 2016, de El Pais, Madrid: http://ccaa.elpais.com/ccaa/2015/03/13/madrid/1426272342_374007.html

BBC Mundo. (25 de febrero de 2015). *El ruso por el que el FBI ofrece la mayor recompensa por un hacker.* Recuperado el 2 de abril de 2017, de BBC: http://www.bbc.com/mundo/noticias/2015/02/150225_tecnologia_cibercriminal_bogachev_ruso_amv

Brulez, N. (24 de marzo de 2011). *Secure List*. Recuperado el 10 de octubre de 2016, de https://securelist.com/blog/incidents/29781/ransomware-fake-federal-german-police-bka-notice/

Cantón, D. (2 de enero de 2014). *Instituto de Ciberseguridad de España S.A.* Recuperado el 3 de noviembre de 2016, de Ransomware III: Variante Lock Screen: https://www.certsi.es/blog/ransomware-lock-screen

Centro Criptológico Nacional (España) (1 de enero de 2016). *Informe de Amenazas - CCN-CERT IA-01/16 - MEDIDAS DE SEGURIDAD CONTRA RANSOMWARE.* Recuperado el 12 de noviembre de 2016, de CCN-CERT: https://www.ccn-cert.cni.es/informes/informes-ccn-

cert-publicos/1384-ccn-cert-ia-01-16-medidas-de-seguridad-contra-ransomware/file.html

Chris Wysopal, C. E. (21 de enero de 2007). *Static Detection of Application Backdoors.* Obtenido de Veracode Inc: https://www.veracode.com/sites/default/files/Resources/Whitepapers/static-detection-of-backdoors-1.0.pdf

Command Five Pty Ltd. (5 de febrero de 2012). *Command and Control in the Fifth Domain.* Recuperado el 24 de febrero de 2017, de Command Five: http://www.commandfive.com

Constantin, L. (4 de noviembre de 2013). *CryptoLocker creators try to extort even more money from victims with new service.* Recuperado el 2 de abril de 2017, de PCWorld: http://www.pcworld.com/article/2060640/cryptolocker-creators-try-to-extort-even-more-money-from-victims-with-new-service.html

Cox, J. W. (29 de marzo de 2016). *MedStar Health turns away patients after likely ransomware cyberattack.* Recuperado el 12 de mayo de 2017, de The Washigton Post: https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html?utm_term=.c392dac1302c

Cruz, C. d. (6 de mayo de 2016). *FayerWayer.* Recuperado el 3 de agosto de 2017, de AlphaLocker es un Ransomware que se vende como Software: https://www.fayerwayer.com/2016/05/alphalocker-es-un-ransomware-que-se-vende-como-software/

Cuerpo Nacional de Policía (España) (27 de septiembre de 2013). *Desarticulada la rama económica responsable del "virus de la Policía"*. Recuperado el 10 de enero de 2017, de Cuerpo Nacional de Policia España: https://www.policia.es/prensa/20130927_1.html

DCSSI, C. (19 de julio de 2004). *La defensa en profundidad aplicada a los sistemas de información.* Recuperado el 22 de mayo de 2017, de Agence nationale de la sécurité des systèmes d'information: https://www.ssi.gouv.fr/archive/es/confianza/documents/methods/mementodep-V1.1_es.pdf

Division, C. S., & Laboratory, I. T. (5 de diciembre de 2001). *Recommendation for Block Cipher Modes of Operation.* Recuperado el 27 de mayo de 2017, de National Institute of

Standards and Technology: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

ESET. (4 de noviembre de 2014). *Infografía: 28 años de historia del malware.* Recuperado el 2 de junio de 2017, de Welivesecurity: https://www.welivesecurity.com/la-es/2014/11/04/infografia-historia-malware/

ESET. (2015). *Ransomware, Historia de una molesta amenaza.* Madrid: ESET. Recuperado el 12 de Octubre de 2016

Ferguson, D. (19 de octubre de 2013). *CryptoLocker attacks that hold your computer to ransom.* Recuperado el 2 de abril de 2017, de The Guardian: https://www.theguardian.com/money/2013/oct/19/cryptolocker-attacks-computer-ransomeware

Ferrer, M. M. (1 de junio de 2012). *Hackstory.* Recuperado el 27 de julio de 2017, de https://hackstory.es/: https://hackstory.es/ebook/Hackstory%20-%20Merce%20Molist%20Ferrer.pdf

Ferrer, M. M. (14 de diciembre de 2015). *Como el Ransomware se esta convirtiendo en la mayor amenaza de Internet.* Recuperado el 15 de noviembre de 2016, de El Confidencial: http://www.elconfidencial.com/tecnologia/2015-12-14/como-el-ransomware-se-esta-convirtiendo-en-la-mayor-amenaza-en-internet_1119003/

F-Secure. (2017). *State of Cyber Security.* Helsinki, Finlandia: F-Secure Corporation.

Gazet, A. (1 de febrero de 2010). Comparative analysis of various ransomware virii. *Journal of Computer Virology and Hacking Techniques*, págs. 77-90. Recuperado el 10 de febrero de 2017.

IBM. (14 de diciembre de 2016). *IBM Study: Businesses More likely to Pay Ransomware than Consumers.* Obtenido de IBM Security: http://www-03.ibm.com/press/us/en/pressrelease/51230.wss

Labs, M. (2016). *Informe de McAfee Labs sobre amenazas.* Madrid: McAfee. Recuperado el 5 de mayo de 2017.

Majamalu. (11 de julio de 2012). *Transacciones Bitcoin completamente anónimas, gracias a Blockchain.info*. Recuperado el 15 de noviembre de 2016, de ElBitcoin.org: http://elbitcoin.org/transacciones-bitcoin-completamente-anonimas-gracias-a-blockchain-info/

Martinez-García, H. A., & Moo Medina, M. (2016). Origen y evolución del cryptovirus ransomware. *Revista del Centro de Graduados e Investigación Tecnológico de Mérida*, 5.

Micro, T. (30 de mayo de 2016). *Hospital de Kansas Es Atacado por Ransomware y Doblemente Extorsionado.* Recuperado el 12 de mayo de 2017, de Blog Trend Micro: http://blog.la.trendmicro.com/hospital-de-kansas-es-atacado-por-ransomware-y-doblemente-extorsionado/#.WRWnyNI1_IU

Ministerio de Justicia y Derechos Humanos de la Nación Argentina (2000). *PROTECCION DE LOS DATOS PERSONALES - Ley 25.326.* Buenos Aires: Congreso de la Nación.

O'Neill, P. H. (27 de abril de 2016). *Former Tor developer created malware for the FBI to hack Tor users*. Recuperado el 06 de enero de 2017, de Daily Dot: http://www.dailydot.com/layer8/government-contractor-tor-malware/

Piscitelli, E. (27 de mayo de 2015). Ransomware: Que es y como funciona el secuestro digital. (D. S.A., Ed.) *USERS*, 40. Recuperado el 19 de enero de 2017, de http://www.redusers.com/noticias/ransomware-que-es-y-como-funciona-el-secuestro-digital/

Pizarro, H. (29 de abril de 2016). *Cylance realiza la primera presentacion mundial de neutralizacion de ransomware en tiempo real.* Recuperado el 28 de noviembre de 2016, de Diario TI: http://diarioti.com/cylance-realiza-la-primera-presentacion-mundial-de-neutralizacion-de-ransomware-en-tiempo-real/97458

Portantier, F. (2012). *Seguridad Informatica por Fabian Portantier.* Buenos Aires: Fox Andina.

Ramírez, T. (29 de mayo de 2016). *Cómo eliminar el virus de la Policía de tu móvil o PC.* Recuperado el 1 de abril de 2017, de Computer Hoy: http://computerhoy.com/noticias/software/como-eliminar-virus-policia-tu-movil-pc-43065

Ransom, N. M. (1 de julio de 2016). *NO MORE RANSOM*. Obtenido de NO MORE RANSOM: https://www.nomoreransom.org/es/index.html

Rousseau, A., & Mager, M. (20 de abril de 2016). *Your package has been successfully encripted: Teslacrypt 4.1 and the Malware attack chain.* Recuperado el 20 de febrero de 2017, de EndGame: https://www.endgame.com/blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack-chain

Sánchez, F. M. (20 de mayo de 2015). *Ciberseguridad: Ransomware, parte I - El negocio del secuestro digital.* Recuperado el 21 de septiembre de 2016, de Cantabria TIC: http://www.cantabriatic.com/ciberseguridad-ramsonware-parte-i/

SecureList. (22 de Junio de 2016). Recuperado el 5 de Noviembre de 2016, de Kaspersky Lab: https://securelist.com/analysis/publications/75145/pc-ransomware-in-2014-2016/

Security, P. (15 de noviembre de 2013). *Panda Security*. Recuperado el 20 de Noviembre de 2016, de ¿Que es un ransomware?: http://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-ransomware/

Sen, U. (18 de octubre de 2015). *eda2 – a new era of open source ransomware.* Recuperado el 23 de mayo de 2017, de Utkusen: https://www.utkusen.com/blog/eda2-a-new-era-of-open-source-ransomware.html

Sen, U. (22 de mayo de 2017). *About*. Recuperado el 22 de mayo de 2017, de Utkusen: https://www.utkusen.com/en/about.html

Snow, J. (7 de julio de 2016). *Ded Cryptor: un ambicioso ransomware creado a partir de código abierto.* Recuperado el 23 de mayo de 2017, de Kaspersky Lab: https://blog.kaspersky.es/ded-cryptor-ransomware/8621/

Symantec. (2016). *Internet Security Threat Report Volume 21.* Mountain View, CA 94043 USA: Symantec Corporation World Headquarters. Recuperado el 29 de marzo de 2017, de https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Symantec. (2016). *Ransomware and Businesses 2016.* Mountain View, CA 94043 USA: Symantec Corporation World Headquarters.

Technology, N. I. (26 de noviembre de 2001). *Advanced Encryption Standard FIPS PUBS 197.* Recuperado el 27 de mayo de 2017, de National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Tzu, S. (500 A.C.). *El Arte de la Guerra.* China.

Vásquez, E. C. (16 de octubre de 2016). *McAfee.* Recuperado el 25 de abril de 2017, de Ransomware en hospitales, una infección difícil de curar: https://securingtomorrow.mcafee.com/languages/espanol/ransomware-en-hospitales-una-infeccion-dificil-de-curar/

Wiel, J. V. (2 de febrero de 2016). *Hidden tear and its spin offs.* Recuperado el 22 de mayo de 2017, de SecureList: https://securelist.com/blog/research/73565/hidden-tear-and-its-spin-offs/

Windows 7k. (4 de octubre de 2010). *Email Falso del Banco Santander.* Recuperado el 22 de enero de 2017, de Windows 7k: http://www.windows7k.com/email-falso-del-banco-santander-phishing/

Winton, R. (18 de febrero de 2016). *Los Angeles Times.* Recuperado el 10 de mayo de 2017, de Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating: http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Anexo I

Modelo de entrevista

1. A grandes rasgos ¿qué medidas de seguridad tiene tu empresa? ¿Usan proxys, tienen servidor con manejo de correo no deseado (Spam), las redes entre departamentos están separadas, tienen Sistema de detección de intrusos o de prevención de intrusos? ¿Políticas de seguridad? ¿Sitios de contingencias?
2. En tu empresa ¿tuviste algún ataque de ransomware?
3. ¿Cómo lo solucionaron?
4. Tienen un buen sistema de recupero de datos (backup) ¿cada cuánto tiempo lo realizan? ¿El backup está guardado en un dispositivo externo a la red de la Empresa?
5. ¿Cuánto tardan en recuperar la información de los backups después de haber sufrido un ataque?
6. ¿Han sufrido ataques de otros tipos de malware? ¿Cuales?
7. ¿Dan capacitación sobre seguridad informática?
8. ¿Utilizan alguna metodología, norma o estándar de seguridad informática?

Entrevista 1

Nombre: Víctor Ocanto

Puesto: Teach Leader Equipo SER

Empresa: Globant

1. A grandes rasgos ¿qué medidas de seguridad tiene tu empresa? ¿Usan proxys, tienen servidor con manejo de correo no deseado (Spam), las redes entre departamentos están

separadas, tienen Sistema de detección de intrusos o de prevención de intrusos? ¿Políticas de seguridad? ¿Sitios de contingencias?

Bueno, en general la seguridad se forma utilizando múltiples capas, desde la estación de trabajo que usan hasta las redes. Por ejemplo, utilizan Mac OS o Linux, ahí ya tenemos una buena protección, si se usa Windows se suele deshabilitar los USB o la instalación de software por medio de políticas de Active Directory. Mayormente las empresas suelen utilizar Active Directory para el manejo de credenciales y políticas, mail, evitar el spam, autorización y autenticación centralizada e incluyen un proxy transparente que filtra determinado tráfico saliente y todo lo entrante por medio de firewalls. Suele haber un área de networking que se encarga de mantener los Firewall, la división entre departamentos se suele hacer con VLANs y a su vez ACLs que permiten la comunicación solo algunos puertos e IPs entre servidores o servidores/clientes. En una empresa tipo no suele haber sistema de detección de intrusos porque es algo laborioso de tener actualizado debido al dinamismo de las empresas, en cambio apuestan más a evitar intrusos, si ya está adentro la empresa es vulnerable. Se suele exponer lo menos posible hacia afuera. En el caso del acceso remoto a la empresa se suele utilizar una VPN con un encriptado de RSA de 2048 bit como minino y con Two-factor authentication.

2. En tu empresa ¿tuviste algún ataque de ransomware?

No vi un tipo de ataque de estos en ninguna empresa en la que trabajé, no a cambio de dinero.

3. ¿Cómo lo solucionaron?

He visto casos en que los usuarios perdieron la contraseña de encriptamiento del disco duro de la computadora, que puede ser un caso similar a los ransomware que encriptan el disco. En este

caso la gente de Soporte Técnico suele reinstalar el sistema operativo sin darle mayor importancia, ya que por lo general utilizan formas de trabajo centralizado donde la información del empleado está en un servidor central y resguardado.

4. Tienen un buen sistema de recupero de datos (backup) ¿cada cuánto tiempo lo realizan? ¿El backup está guardado en un dispositivo externo a la red de la Empresa?

El tema de backup varía mucho dependiendo de las actividades de la empresa. A nivel usuario, el empleado tiene la responsabilidad de hacer su backup diario o semanal dependiendo de su volumen de trabajo. Por ejemplo, en IBM teníamos una herramienta que hacía un backup automático de perfil de usuario con sus archivos semanalmente y estaba en un servidor centralizado que a su vez tenía un backup en un Storage especializado para backup. La restauración era bastante simple, por medio del cliente instalado en la workstation el empleado podía restaurar el backup en el día. Con respecto al backup de aplicaciones o servidores como emails, hoy en día se suele utilizar un almacenamiento en la nube, por ejemplo, S3 de Amazon que permite almacenar datos en sus servidores, eso es fiable y barato para la empresa, porque puede tener un backup externo a la empresa.

5. ¿Cuánto tardan en recuperar la información de los backups después de haber sufrido un ataque?

Dependiendo del tipo de ataque, por lo general si es a empleados, luego de la instalación nueva del sistema operativo, en el mismo día pueda tener la información. Si el ataque es a una base de datos, puede tardar dos o tres días, dependiendo de la cantidad de información. Nunca vi

en persona un caso de ataque a servidores con pérdida de información, porque por lo general están muy protegidos, no muchas personas tienen acceso, son Linux/Unix y además están replicados, si borras algo en cuestión de horas se sincronizan. El único caso que vi fue de alguien que cometió un error y borro 1.5TB en una base de datos, en ese caso tardo casi una semana en restaurar el backup.

6. ¿Han sufrido ataques de otros tipos de malware? ¿Cuales?

Dos veces hubo ataques en una empresa donde trabajé, una fue un malware que se distribuía por USB, los empleados se pasaban información e infectaban las máquinas que usaban Windows. Otro fue un malware que se distribuía solo por red por medio de emails, en ese caso la gente de networking inhabilitaba las direcciones MAC de red para que los equipos no puedan conectarse a la red hasta que no sean verificados.

7. ¿Dan capacitación sobre seguridad informática?

Suele haber capacitaciones internas de seguridad informática para quienes no tiene un rol puramente técnico como PM, RRHH, etc. Para los Developers, SysAdmins, DevOps no suele haber porque esos conocimientos son parte de las entrevistas, así que por lo general quien ingresa ya sabe lo básico de eso.

8. ¿Utilizan alguna metodología, norma o estándar de seguridad informática?

Si, utilizamos certificación ISO 27000 para lo que se desarrolla en la oficina.

Entrevista 2

Nombre: Martin Bono

Puesto: Jefe de Sistemas

Empresa: La Lacteo

1. A grandes rasgos ¿qué medidas de seguridad tiene tu empresa? ¿Usan proxys, tienen servidor con manejo de correo no deseado (Spam), las redes entre departamentos están separadas, tienen Sistema de detección de intrusos o de prevención de intrusos? ¿Políticas de seguridad? ¿Sitios de contingencias?

La primera barrera en seguridad al exterior era un Router Cisco 1811, el cual tenía configurado un proxy que gestionaba peticiones algunos puertos que se accedían a recursos internos de la empresa, por ejemplo, Servidores de datos, Servidor de aplicación o base de datos. El acceso externo se hacía desde terminal server, una VPN a través del sistema VPN Client Cisco y/o una VPN del server.

Por otro lado, teníamos instalado una plataforma antivirus Eset Nod32, la cual era gestionada desde un servidor y desde el mismo distribuíamos cada cliente. Esto nos permitía actualizar desde un solo lugar (desde el servidor) a cada PC/Notebook de la empresa y dicha plataforma también nos permitía tener un monitoreo de cada PC/Notebook el cual nos notificaba si la misma habría recibido algún "ataque" o problema de seguridad.

Con respecto a Políticas de Seguridad, además de la plataforma de antivirus, por medio del sistema de gestión de usuarios de Windows Server "Active Directory" establecíamos reglas destinadas a la seguridad Física y Lógica, por ejemplo:

a. No permitíamos que el usuario de cada PC/Notebook tenga privilegios de "Administrador"

b. No permitíamos que el usuario de cada PC/Notebook ingrese un Pen Drive a la misma.

c. Cada usuario tenía un perfil y permiso y solo accedía archivo del Servidor de Archivos que le correspondiese. Por ejemplo, las carpetas/archivos del área de Recursos Humanos solo accedían los usuarios de Recursos Humanos y la Gerencia de la empresa. De esa manera establecíamos la división de áreas en el acceso a la información.

d. Las contraseñas de los usuarios de cada PC/Notebook tenía una regla de "n" cantidad de caracteres y combinación de letras y números.

e. Con respecto a los usuarios del Sistema ERP (Tango Gestión), cada usuario tenía su perfil de acceso y edición de acuerdo a las responsabilidades del mismo.

El correo de la empresa estaba tercerizado, por lo que no nos preocupábamos con el correo no deseado.

Con respecto a contingencias, teníamos un servidor respaldo para el Servidor de Datos y para el Servidor de Aplicaciones y Base de Datos, el último tenía un sistema en RAID 1 a través de dos discos.

Por otro lado, teníamos instalada sistemas de monitoreo de Red y Equipo llamadas Nagios y Kerios, los cuales nos permitía ayudar a revisar comportamientos en ambos lados.

2. En tu empresa ¿tuviste algún ataque de ransomware?

Nunca tuvimos ataques ransomware

3. ¿Cómo lo solucionaron?

---

4. Tienen un buen sistema de recupero de datos (backup) ¿cada cuánto tiempo lo realizan? ¿El Backup está guardado en un dispositivo externo a la red de la Empresa?

Sí, hacíamos Backup del servidor de archivo todos los días y de la base de datos del ERP y sus satélites todas las semanas. El mismo se hacía por medio del sistema de Windows NetBackup y por medio de Cintas de 200/400 Gb. El soporte de las unidades de cintas era Ultrium LTO. Por otro lado, por políticas de Backup, guardábamos una cinta por mes en una caja fuerte en el exterior del piso donde estaba el datacenter.

5. ¿Cuánto tardan en recuperar la información de los backups después de haber sufrido un ataque?

Nunca tuvimos que hacerlo por un ataque, pero si hicimos un par de pruebas con el servidor de respaldo y para recuperar los archivos de dichas cintas y se demoraba entre 2 y 4 horas. Para el caso del RAID, nunca hicimos pruebas, pero si levantamos bases de datos en otros servidores para tener alternativas de acceso a la información en caso de algún problema de seguridad o soporte técnico.

6. ¿Han sufrido ataques de otros tipos de malware? ¿Cuales?

El mayor problema de seguridad que tuvimos fue un ataque a la central telefónica. Teníamos instalada una Central Asterisk modelo TrixBox, la cual estaba expuesta a internet para poder realizar llamadas por internet a usuarios que estén fuera de país y tuvimos un ataque que generaba llamadas a todos lados del mundo. Nos dimos cuanta al día siguiente, porque entre

otras cosas nos comunicamos con Telecom que nos advirtió del tema y, por otro lado, por medio del Sistema Nagios que monitoreaba el tráfico de red, se veían comportamientos fuera de lo común. Se solucionó desconectado la central de internet. Ese mes...la cuenta de teléfono vino un poco más elevada de lo normal.

7. ¿Dan capacitación sobre seguridad informática?

En la empresa donde estaba, no dieron capacitación en seguridad informática. Las hice por mi cuenta (Especialidad en Seguridad y Peritaje Informático - 2009).

8. ¿Utilizan alguna metodología, norma o estándar de seguridad informática?

No seguimos ninguna Norma o Estándar.

Entrevista 3

Nombre: Ana Torres del Santo

Puesto: CISO

Empresa: Tarjeta Naranja

1. A grandes rasgos ¿qué medidas de seguridad tiene tu empresa? ¿Usan proxys, tienen servidor con manejo de correo no deseado (Spam), las redes entre departamentos están separadas, tienen Sistema de detección de intrusos o de prevención de intrusos? ¿Políticas de seguridad? ¿Sitios de contingencias?

Naranja cuenta con una gestión integrada para el gobierno de la seguridad. Existe un área de seguridad alineada a la ISO 27001. Contamos con un enfoque basado en riegos ISO 27005.

Tenemos una política de seguridad que refleja la intención de la dirección en temas de seguridad y un plan director anual.

Contamos con equipos Firewall de primera marca para proteger la red interna de intrusiones no debidas.

También tenemos otras herramientas de seguridad como IPS (prevención de intrusiones) DLP (FUGA DE INFORMACION), equipos proxy, antivirus, centralizadores de logs y herramientas propias de Ciberseguridad y seguridad defensiva.

Naranja cuenta con sitios se contingencia entre las empresas de todo el grupo.

El área está formada por profesionales certificados y bajo un programa de actualización anual.

2. En tu empresa ¿tuviste algún ataque de ransomware?

En noviembre de 2015 tuvimos al menos 2 infecciones de bajo impacto. A partir de allí incorporamos herramientas específicas que nos permitieron pasar 2016 y hasta la fecha sin otras infecciones.

3. ¿Cómo lo solucionaron?

En lo inmediato se recuperaron los datos de los usuarios del backup.

Se implementaron herramientas específicas. Se está alerta a las vulnerabilidades de día Zero.

A su vez como el usuario es el eslabón más débil de la cadena, contamos con un esquema agresivo de concientización en estos temas.

4. Tienen un buen sistema de recupero de datos (backup) ¿cada cuánto tiempo lo realizan? ¿El Backup está guardado en un dispositivo externo a la red de la Empresa?

Naranja cuenta con una política de resguardo en función a las buenas practicas COBIT y las normativas del Banco Central; Com. A 4609.0

El esquema actual consta de backup diarios, semanales y mensuales que se almacenan fuera de la empresa. En función a la necesidad del negocio existen para casos puntuales copias a disco y réplicas online.

5. ¿Cuánto tardan en recuperar la información de los backups después de haber sufrido un ataque?

Dependiendo el tipo de información, entre 10 minutos y 6 horas.

6. ¿Han sufrido ataques de otros tipos de malware? ¿Cuáles?

Como toda la industria financiera estamos sufriendo algunos casos de phishing.

Para estos casos en Naranja cuenta con un plan de concientización para titulares, comercios y público interno.

Entrevista 4

Nombre: Ing. M. Teresa Lozada

Puesto: Jefa de Sistemas

Empresa: Sanatorio Allende

1. A grandes rasgos ¿qué medidas de seguridad tiene tu empresa? ¿Usan proxys, tienen servidor con manejo de correo no deseado (Spam), las redes entre departamentos están separadas, tienen Sistema de detección de intrusos o de prevención de intrusos? ¿Políticas de seguridad? ¿Sitios de contingencias?

Utilizamos unos Gateways de red marca Fortinet. Tenemos en total 4 (2 por sitio) Fortigate 500D para Nueva Córdoba y 300D para la sede Cerro. Anteriormente teníamos un proxy, pero luego, gracias a la implementación de los equipos Fortinet lo sacamos.

Por otro lado, tenemos implementadas VLANs en toda la red, por lo que efectivamente tenemos separadas las redes.

Con respecto al manejo de SPAMs, tenemos implementado un servidor de Correo Zimbra, que maneja sus propias Black List. Igualmente, desde el Fortigate filtramos los correos que contienen virus, eliminando el riesgo de infectarnos por ransomware

Con respecto a la detección de intrusos, tenemos centralizado el acceso a nuestra red por los equipos Fortinet. Y tenemos desactivado desde fuera de nuestra red todos los protocolos de acceso remoto (team viewer, etc.) por lo que si alguien quiere conectarse remotamente lo tiene que hacer si o si por VPN. Estos accesos si los tenemos monitorizados.

Con respecto al sitio de contingencia, tenemos 2 data centers (uno por sitio) que estamos este año terminando un proyecto de dejar absolutamente todos los servidores duplicados. (Hoy en día tenemos la mitad)

2. En tu empresa ¿tuviste algún ataque de ransomware?

Tuvimos ataques, pero al contar con VLANs y fileserver por área (y contamos con Back Up de estos fileservers diarios) los daños fueron locales a las PC en las que abrieron el virus. No tuvo gran impacto

3. ¿Cómo lo solucionaron?

No lo solucionamos. Se perdieron los archivos (no compramos el desencriptador). Pero como mencione anteriormente, tenemos BackUp de los archivos críticos.

4. Tienen un buen sistema de recupero de datos (backup) ¿cada cuánto tiempo lo realizan? ¿El Backup está guardado en un dispositivo externo a la red de la Empresa?

Realizamos diariamente los BackUp de servidores/fileserver. Con respecto a la base de Datos, la tenemos en HDR duplicada, por lo que tenemos duplicada la información.

Con respecto a donde guardamos las copias de BackUp, actualmente lo hacemos en disco. Pero tenemos el proyecto de compra de una librería de Cintas para poder tener de manera externa una copia mensual.

5. ¿Cuánto tardan en recuperar la información de los backups después de haber sufrido un ataque?

Como máximo una hora

6. ¿Han sufrido ataques de otros tipos de malware? ¿Cuales?

No

Entrevista 5

Nombre: Alejandro Gómez

Puesto: Jefa de Seguridad Informática

Empresa: Municipalidad de Córdoba

1. A grandes rasgos ¿qué medidas de seguridad tiene tu empresa? ¿Usan proxys, tienen servidor con manejo de correo no deseado (Spam), las redes entre departamentos están separadas, tienen Sistema de detección de intrusos o de prevención de intrusos? ¿Políticas de seguridad? ¿Sitios de contingencias?

Tenemos firewall corporativo. El acceso a internet se da solo a través de un proxy con filtrado de malware. El servidor de correo también tiene filtrado de spam y malware. Las redes están separadas de acuerdo a la ubicación geográfica, no internamente en el mismo edificio.

Utilizamos IDSs como medidas reactivas y se hacen escaneos de seguridad como medidas proactivas.

2. En tu empresa ¿tuviste algún ataque de ransomware?

No tuvimos ningún reporte de ransomware

3. ¿Cómo lo solucionaron?

4. Tienen un buen sistema de recupero de datos (backup) ¿cada cuánto tiempo lo realizan? ¿El Backup está guardado en un dispositivo externo a la red de la Empresa?

Hay backups en línea, clusters, duplicación de bases de datos y backup periódicos todas las noches. Aunque no de las terminales de cada empleado. Solo de los sistemas que presta la municipalidad.

Los servidores de backup están aislados de la red.

5. ¿Cuánto tardan en recuperar la información de los backups después de haber sufrido un ataque?

No hemos sufrido ataques, pero si incidentes de hardware. Depende siempre de la cantidad de datos a restaurar. Normalmente el servidor de reemplazo con servicios instalados está listo en un par de horas. Luego lo que demore la cantidad de datos, que puede variar de minutos a días.

6. ¿Han sufrido ataques de otros tipos de malware? ¿Cuáles?

Virus. En 2009 tuvimos una infección generalizada debido a un virus que el antivirus todavía no detectaba. Hubo que tomarse el trabajo de reinstalar todas las computadoras clientes.

7. ¿Dan capacitación sobre seguridad informática?

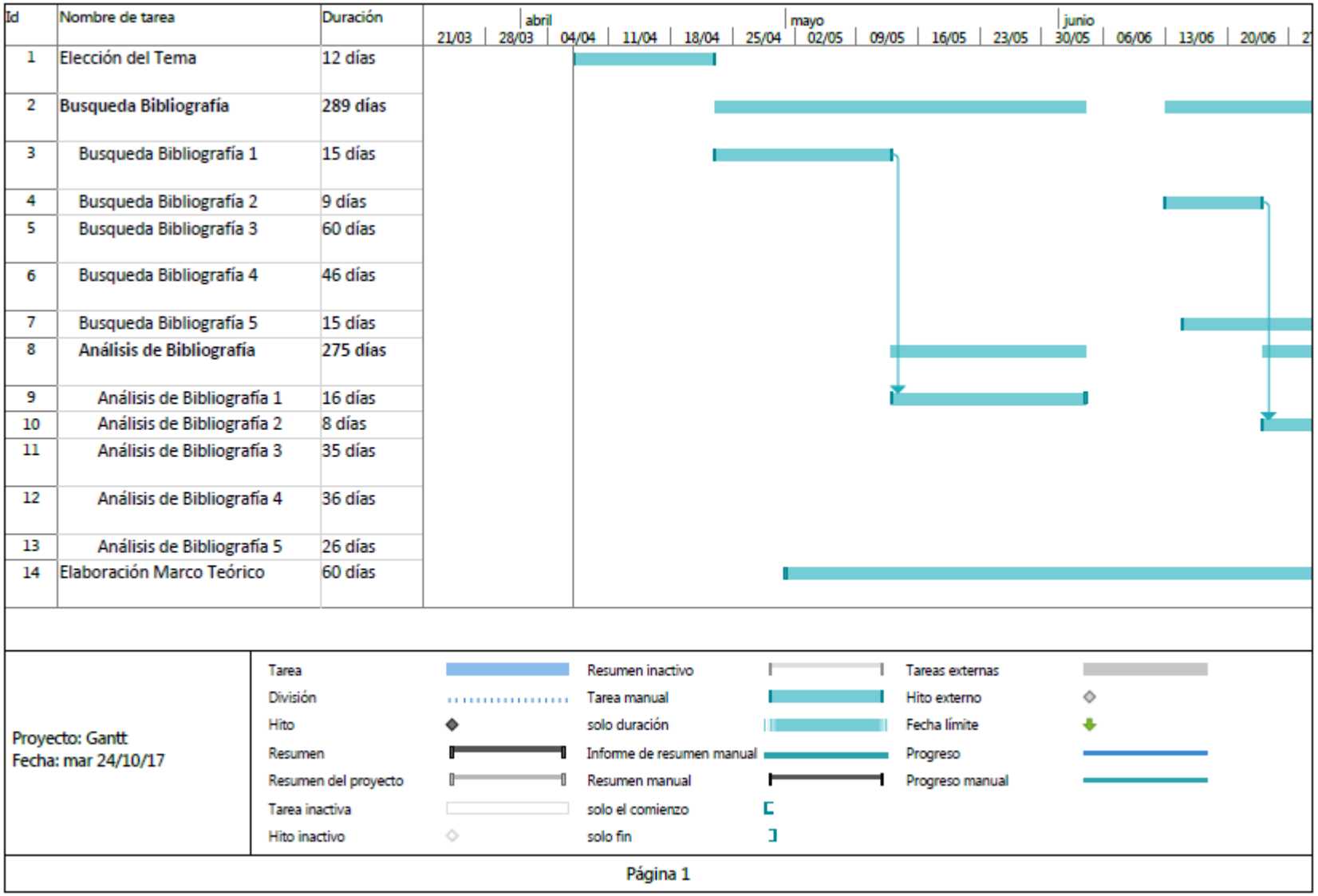
No, no hemos tenido hasta ahora ninguna capacitación en seguridad.

8. ¿Utilizan alguna metodología, norma o estándar de seguridad informática?

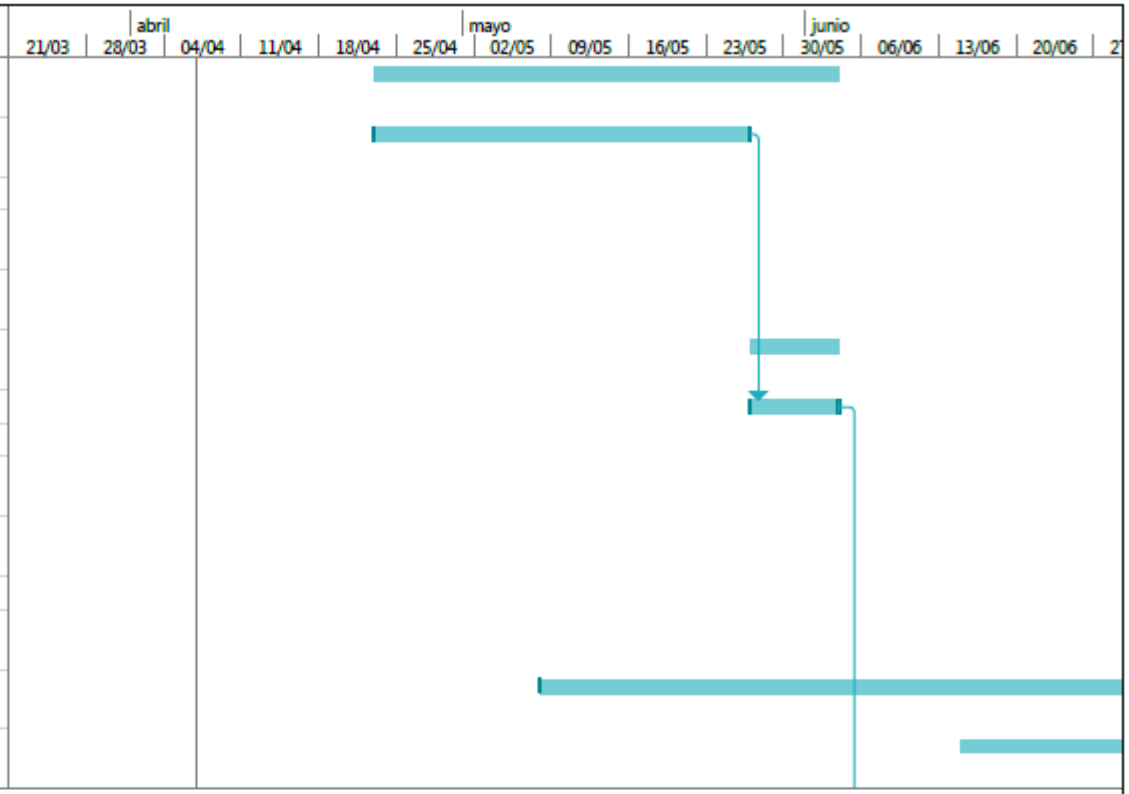
Las metodologías las vamos armando nosotros sobre la marcha.

Anexo II

Diagrama de Gantt



Id	Nombre de tarea	Duración
15	Recolección de datos	375 días
16	Recolección de datos 1	25 días
17	Recolección de datos 2	7 días
18	Recolección de datos 3	66 días
19	Recolección de datos 4	34 días
20	Análisis de datos	351 días
21	Análisis de datos 1	6 días
22	Análisis de datos 2	9 días
23	Análisis de datos 3	24 días
24	Análisis de datos 4	50 días
25	Pruebas de Ransomware	178 días
26	Analisis dinámico y estático del Ransomware	123 días
27	Redacción de TFG	120 días
28	Revisión y correccion TFG	352 días

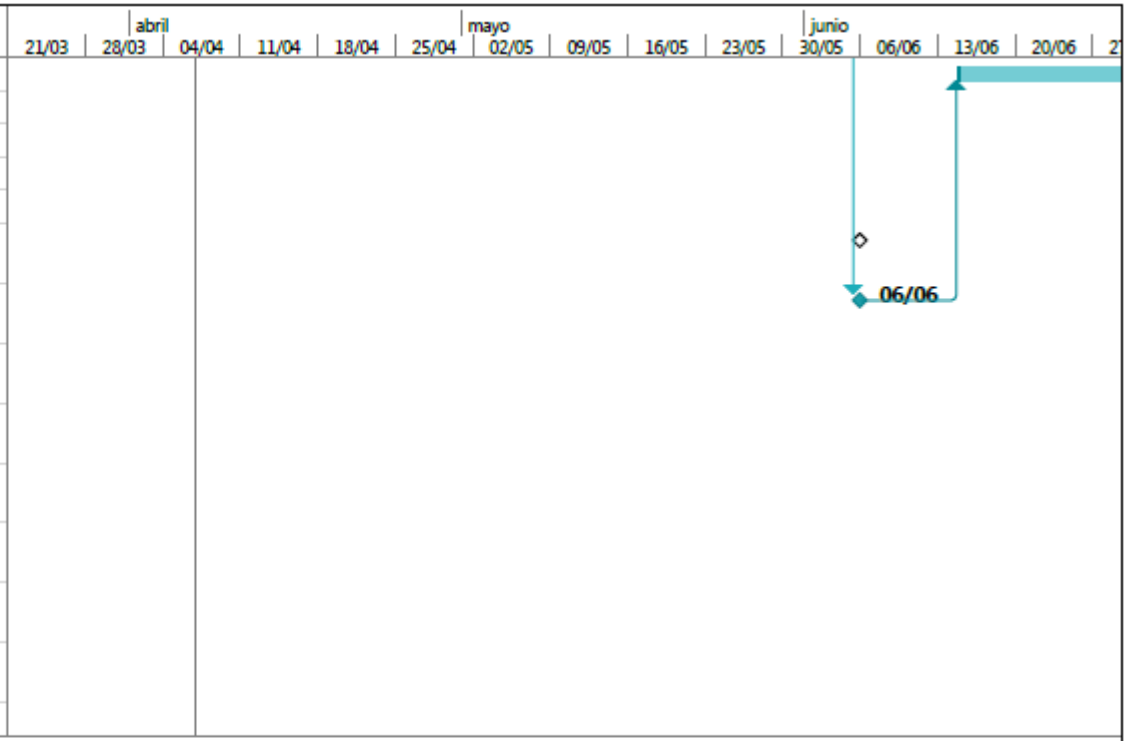


Proyecto: Gantt
Fecha: mar 24/10/17

Tarea	Resumen inactivo	Tareas externas
División	Tarea manual	Hito externo
Hito	solo duración	Fecha límite
Resumen	Informe de resumen manual	Progreso
Resumen del proyecto	Resumen manual	Progreso manual
Tarea inactiva	solo el comienzo	
Hito inactivo	solo fin	

Página 2

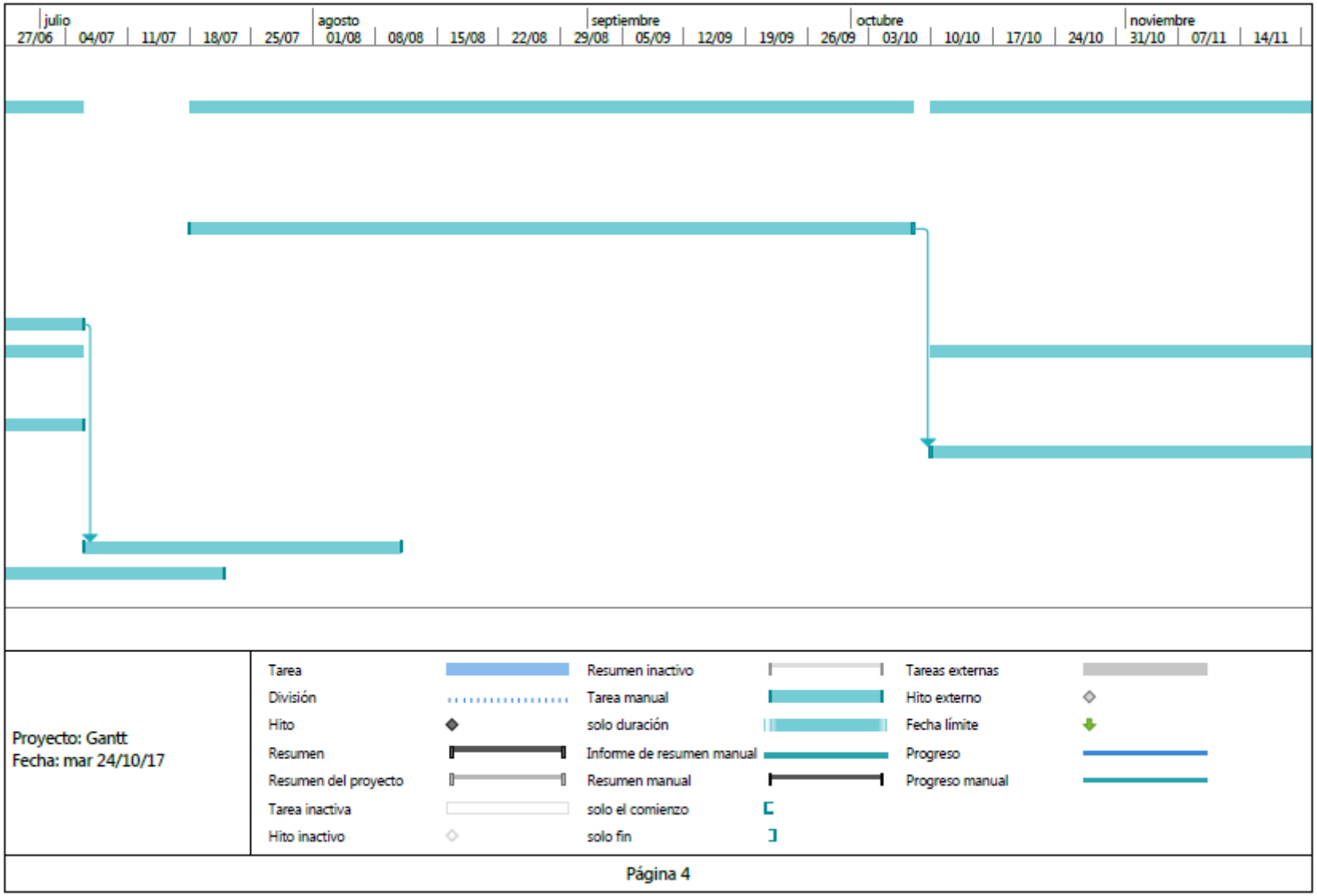
Id	Nombre de tarea	Duración
29	Revisión y correccíon TFG 1	17 días
30	Revisión y correccíon TFG 2	102 días
31	Revisión y correccíon TFG 3	132 días
32	Revisión y correccíon TFG 4	52 días
33	Revisión y correccíon TFG 5	45 días
34	Entrega de TFG para corrección	359 días
35	Entrega de TFG para corrección 1	0 días
36	Entrega de TFG para corrección 2	0 días
37	Entrega de TFG para corrección 3	0 días
38	Entrega de TFG para corrección 4	0 días
39	Entrega de TFG para corrección 5	0 días
40	Entrega de TFG para corrección 6	0 días
41	Entrega de TFG para corrección 7	
42	Tutoría	111 días

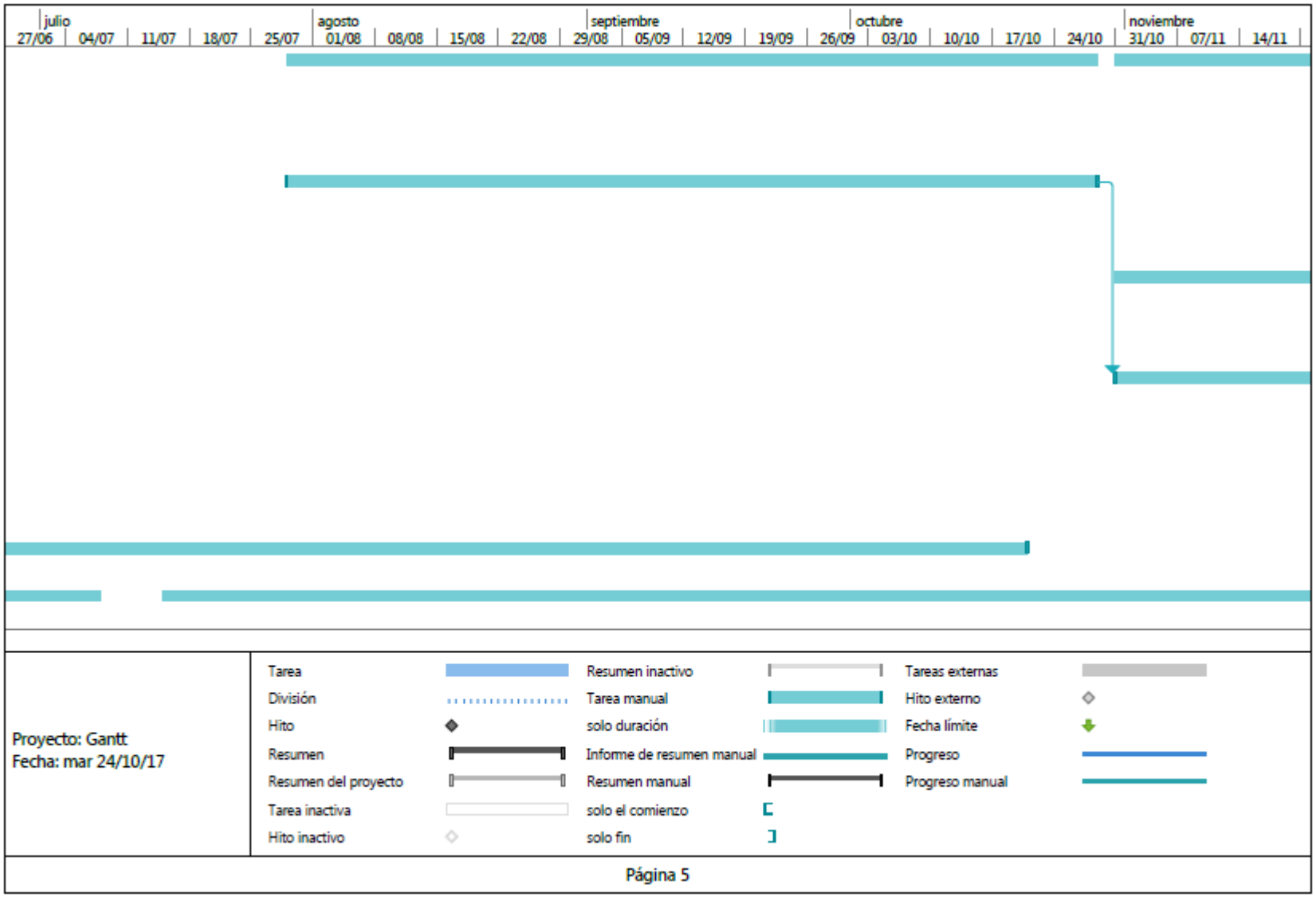


Proyecto: Gantt
Fecha: mar 24/10/17

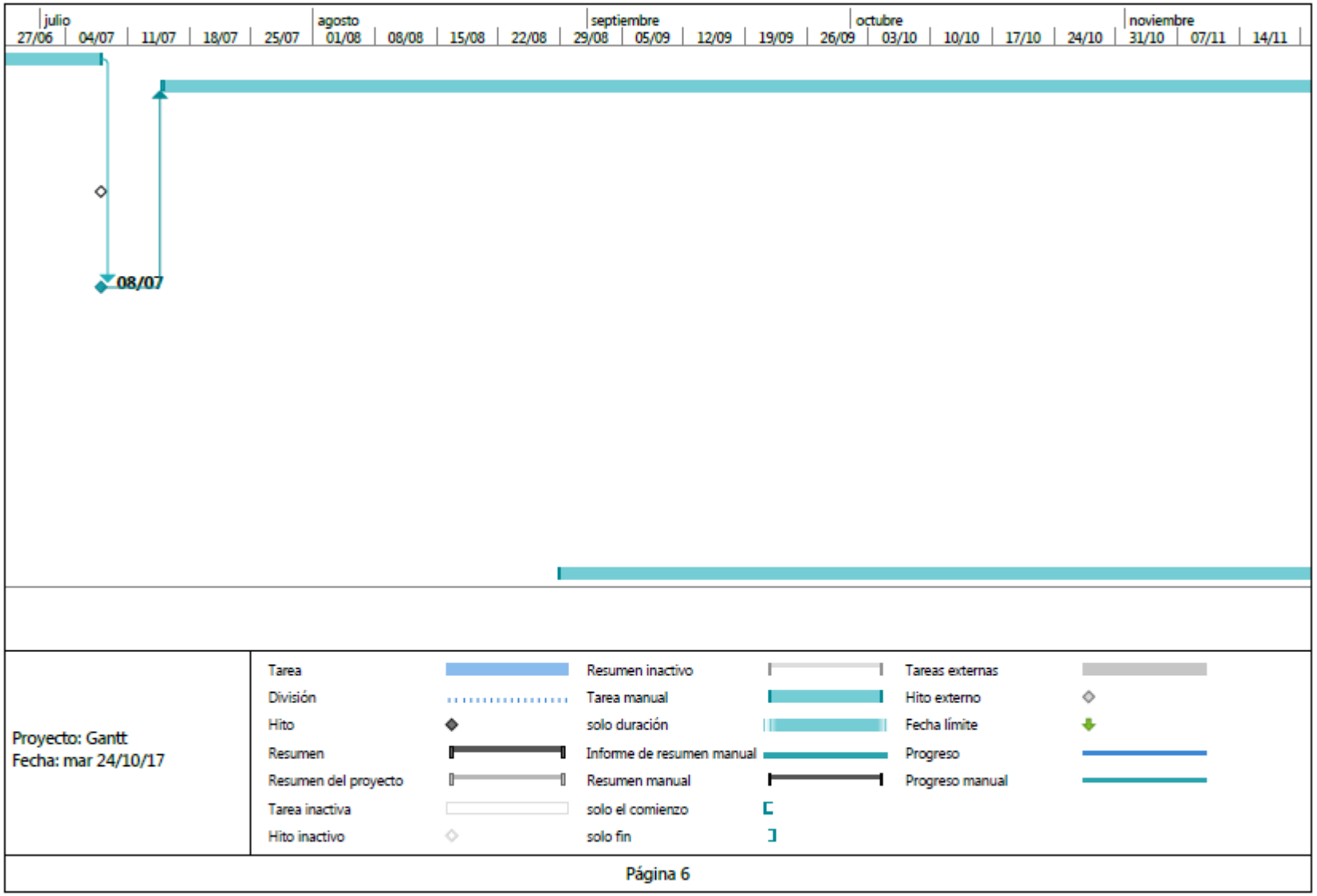
Tarea		Resumen inactivo		Tareas externas	
División		Tarea manual		Hito externo	
Hito		solo duración		Fecha límite	
Resumen		Informe de resumen manual		Progreso	
Resumen del proyecto		Resumen manual		Progreso manual	
Tarea inactiva		solo el comienzo			
Hito inactivo		solo fin			

Página 3

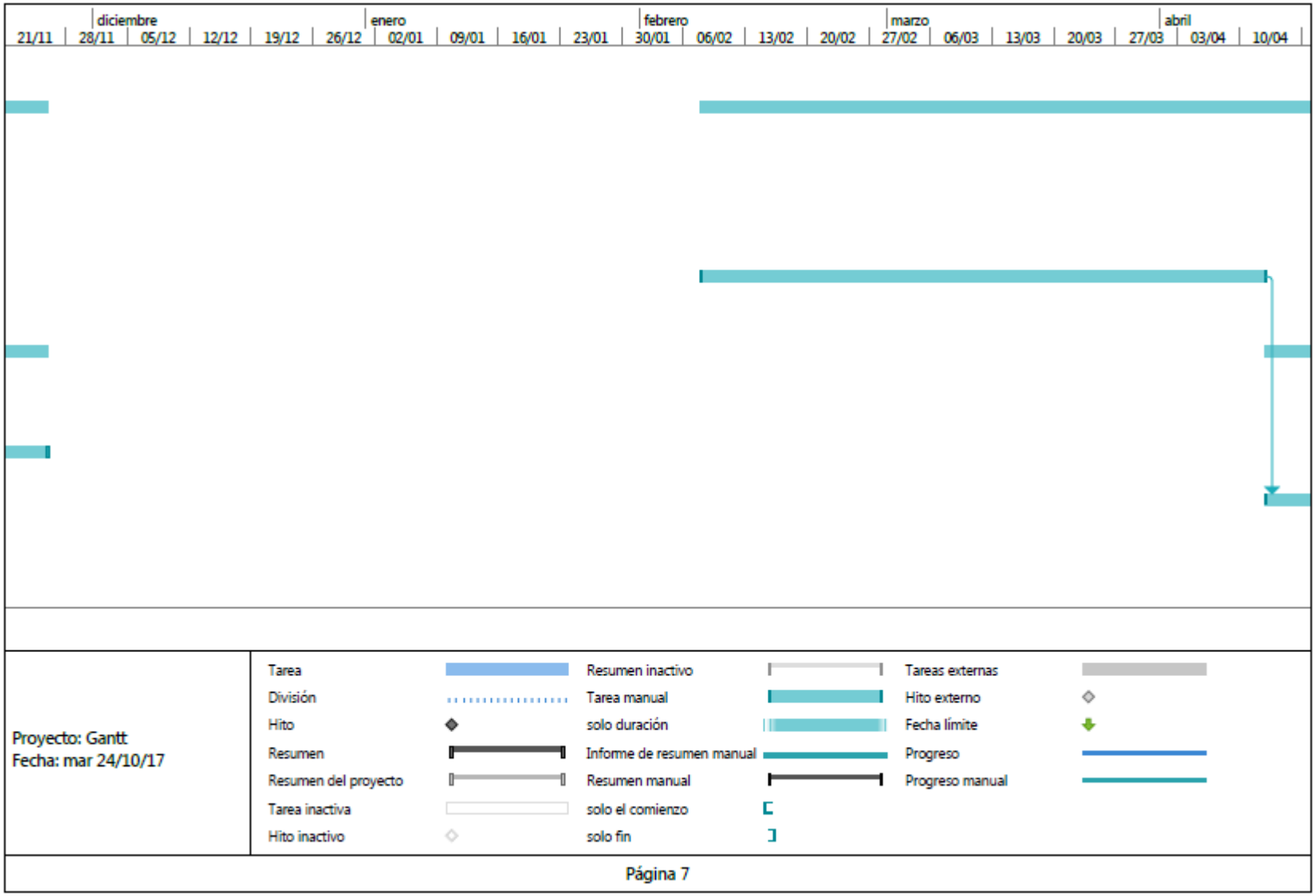

julio
agosto
septiembre
octubre
noviembre
27/06
04/07
11/07
18/07
25/07
01/08
08/08
15/08
22/08
29/08
05/09
12/09
19/09
26/09
03/10
10/10
17/10
24/10
31/10
07/11
14/11
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual
Página 4

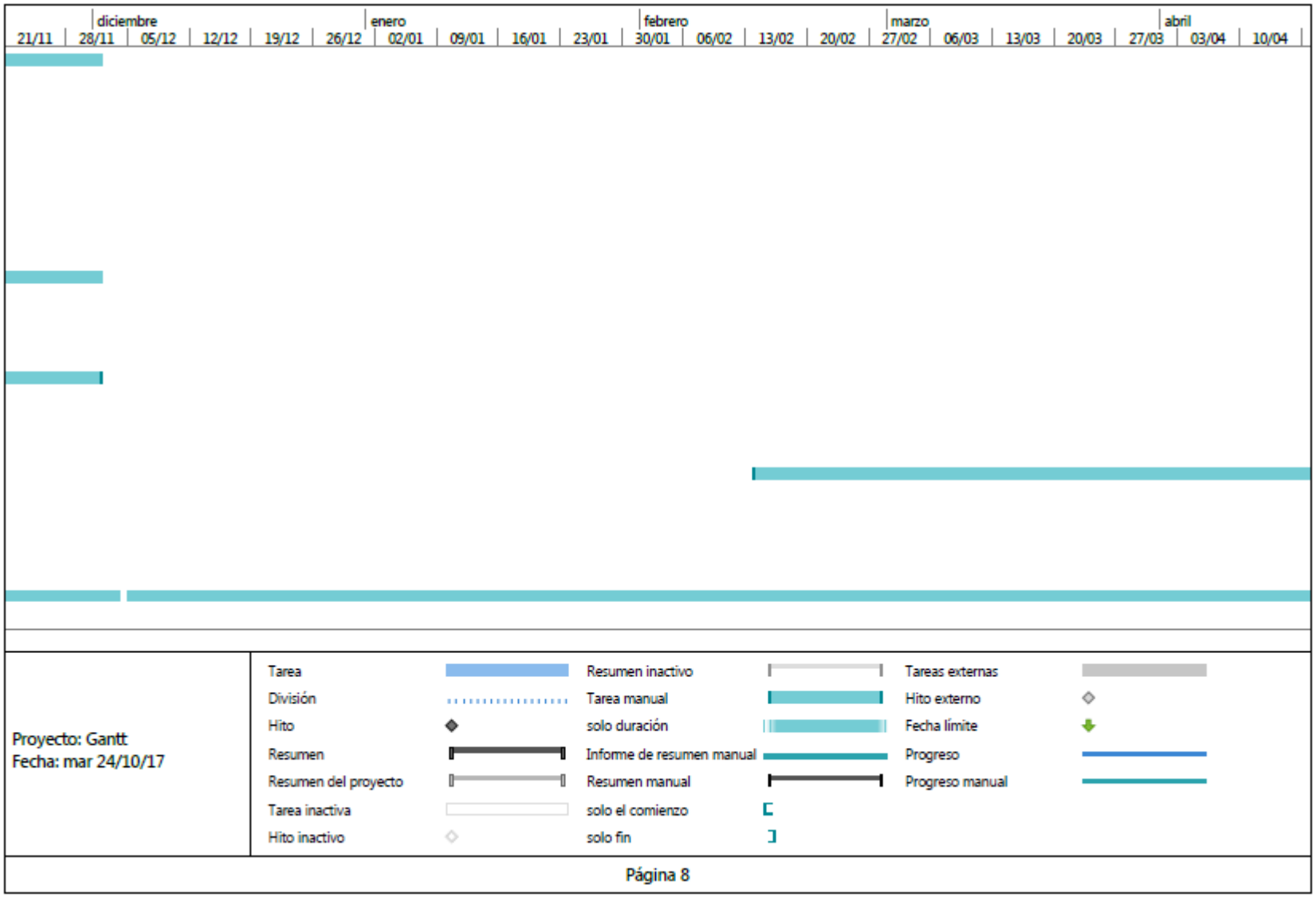

julio
agosto
septiembre
octubre
noviembre
27/06
04/07
11/07
18/07
25/07
01/08
08/08
15/08
22/08
29/08
05/09
12/09
19/09
26/09
03/10
10/10
17/10
24/10
31/10
07/11
14/11
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual

Página 5

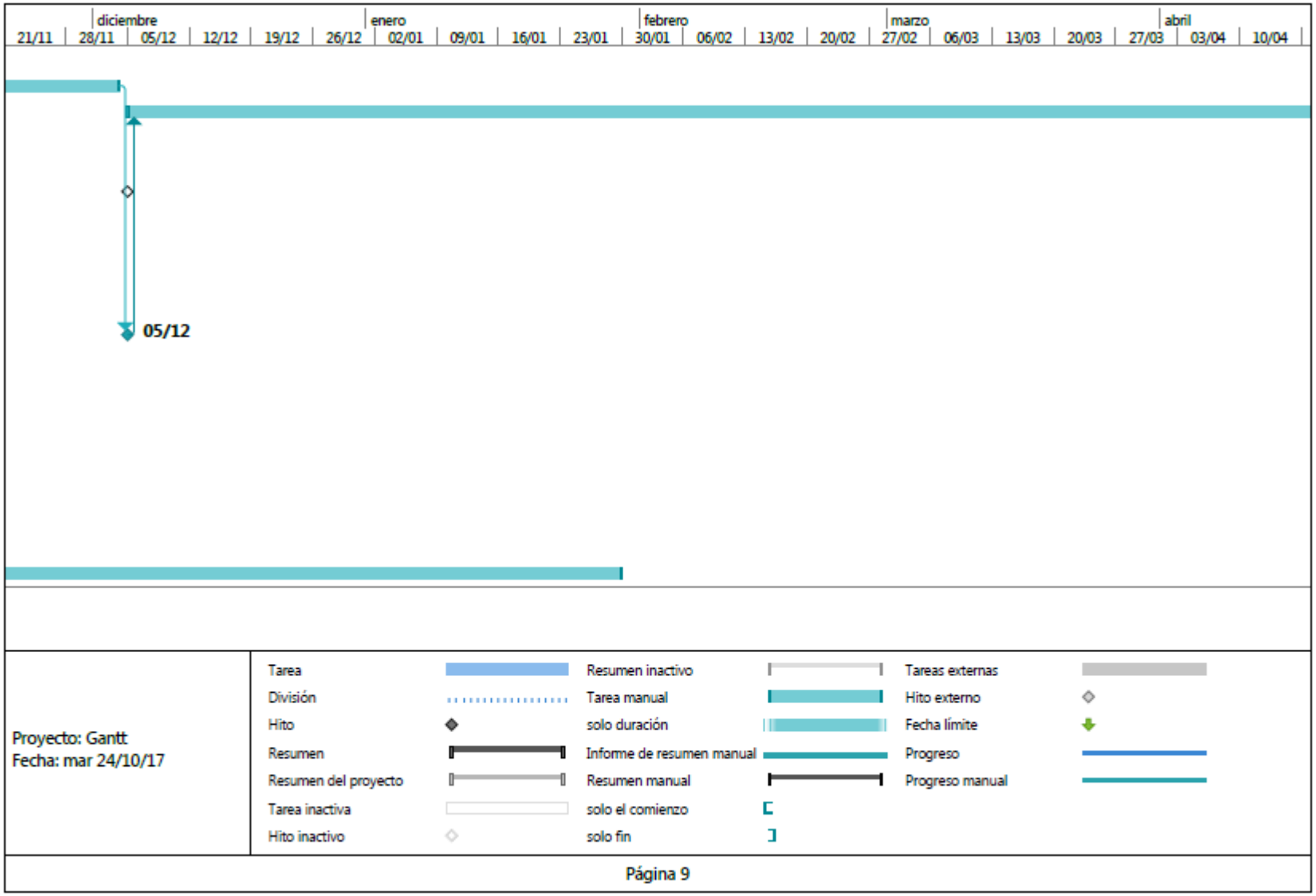

julio
agosto
septiembre
octubre
noviembre
27/06
04/07
11/07
18/07
25/07
01/08
08/08
15/08
22/08
29/08
05/09
12/09
19/09
26/09
03/10
10/10
17/10
24/10
31/10
07/11
14/11
08/07
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual

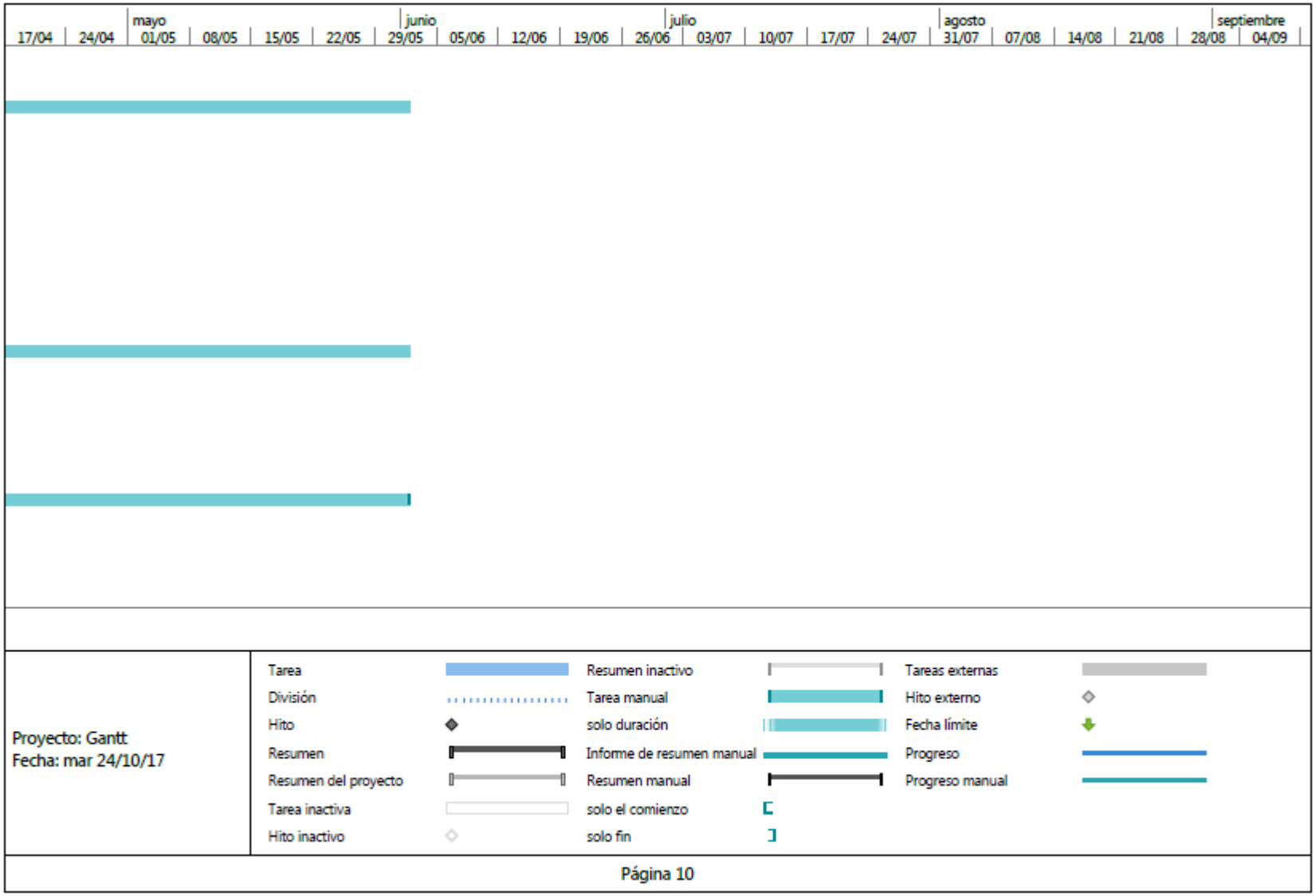
Página 6

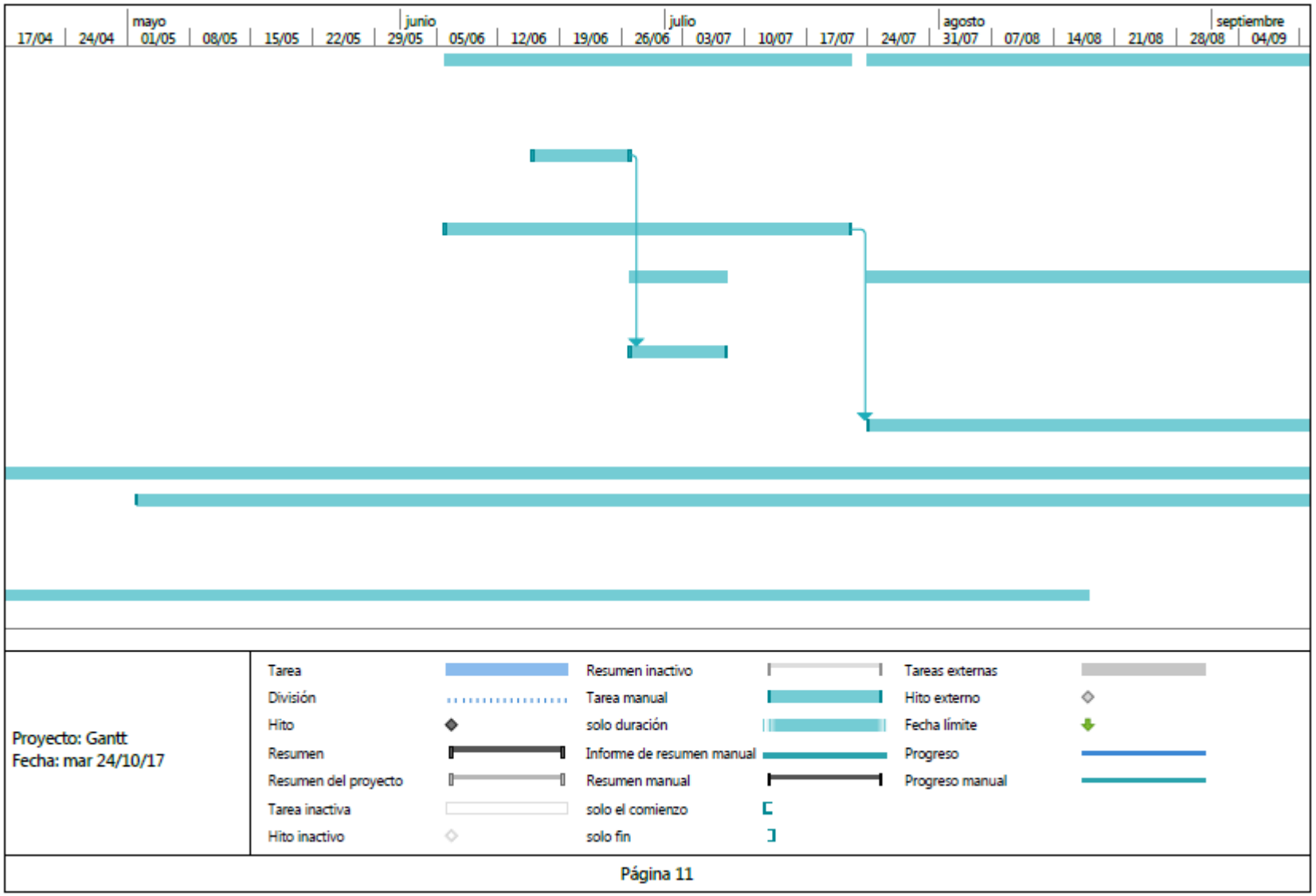

diciembre
enero
febrero
marzo
abril
21/11
28/11
05/12
12/12
19/12
26/12
02/01
09/01
16/01
23/01
30/01
06/02
13/02
20/02
27/02
06/03
13/03
20/03
27/03
03/04
10/04
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual
Página 7


diciembre
enero
febrero
marzo
abril
21/11
28/11
05/12
12/12
19/12
26/12
02/01
09/01
16/01
23/01
30/01
06/02
13/02
20/02
27/02
06/03
13/03
20/03
27/03
03/04
10/04
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual

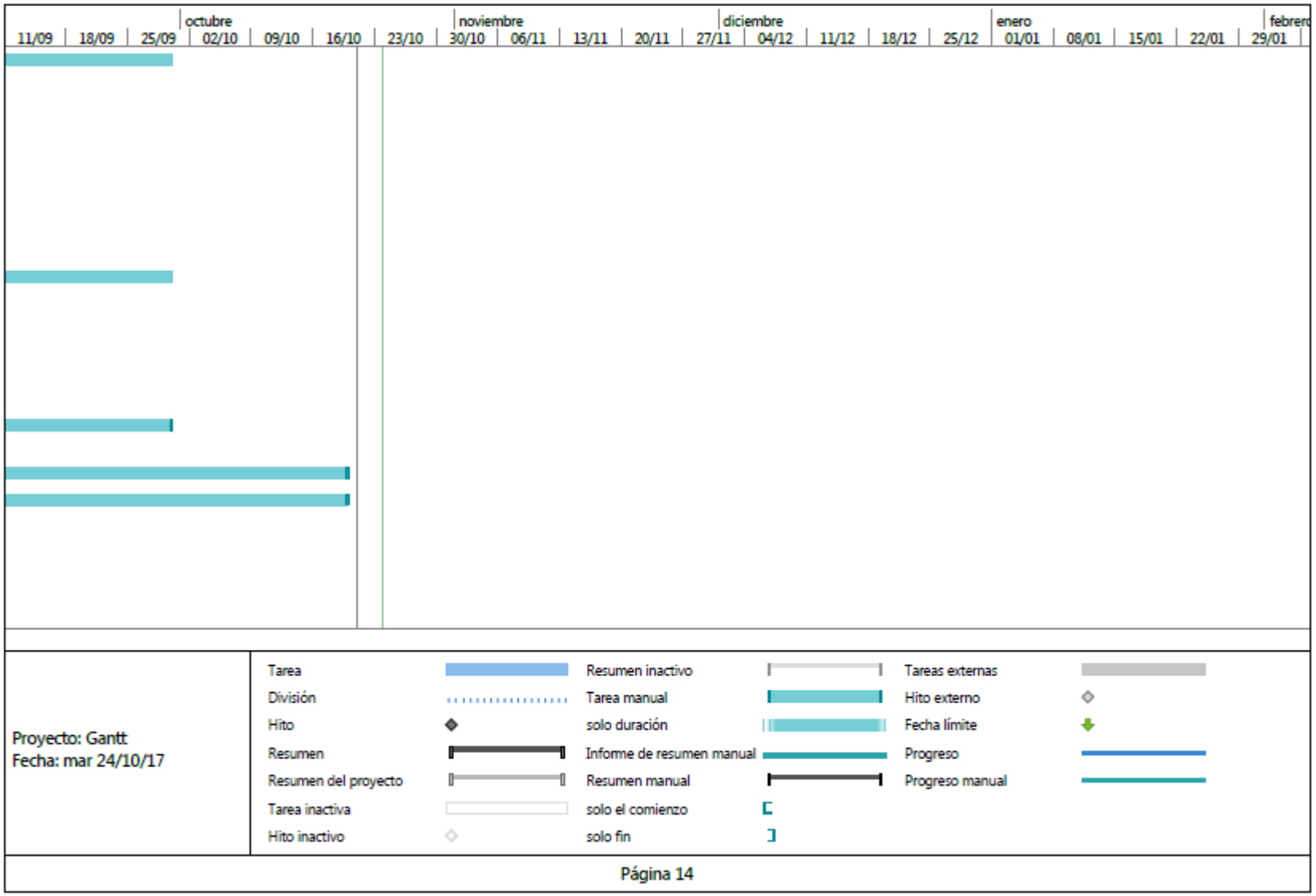
Página 8

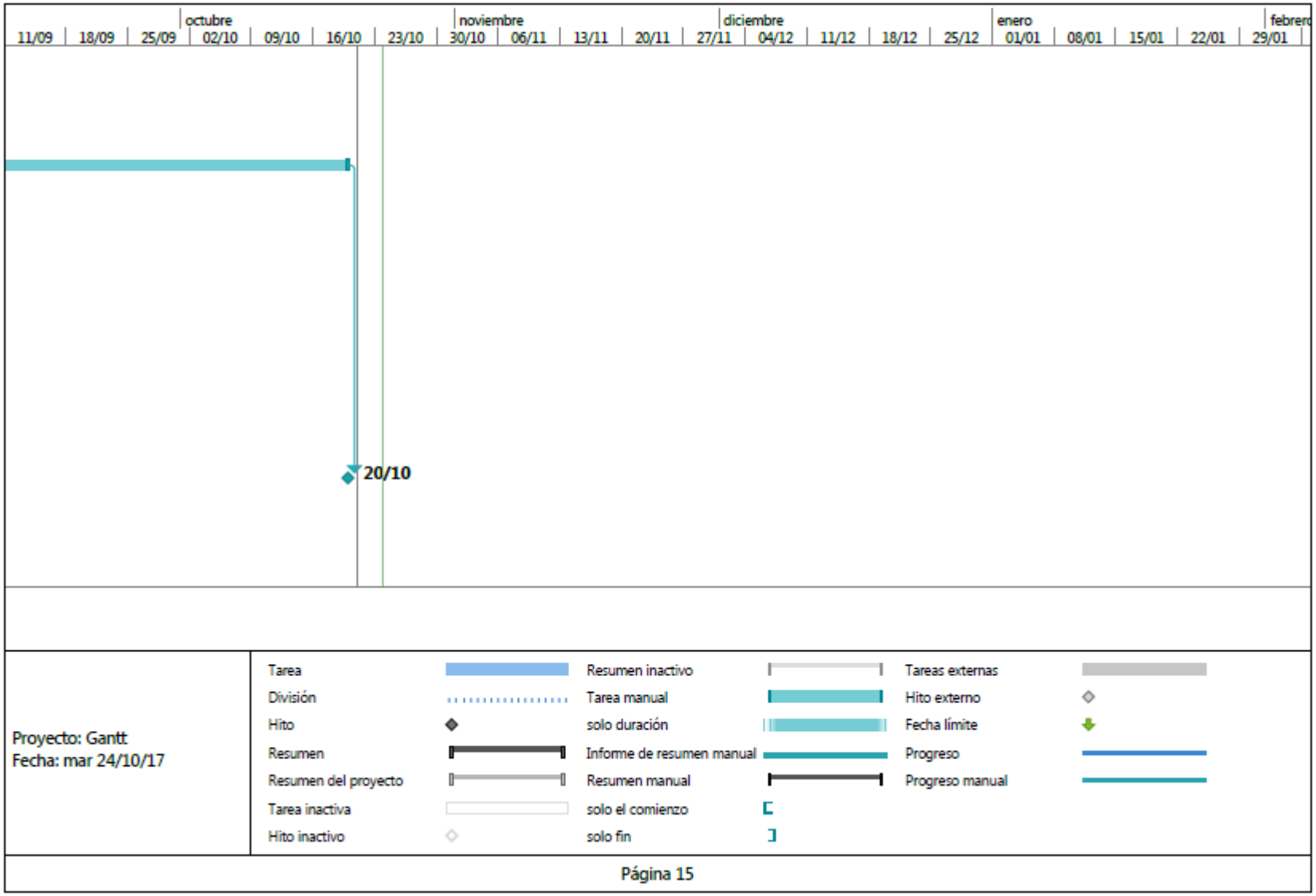

diciembre
enero
febrero
marzo
abril
21/11
28/11
05/12
12/12
19/12
26/12
02/01
09/01
16/01
23/01
30/01
06/02
13/02
20/02
27/02
06/03
13/03
20/03
27/03
03/04
10/04
05/12
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual


mayo
junio
julio
agosto
septiembre
17/04
24/04
01/05
08/05
15/05
22/05
29/05
05/06
12/06
19/06
26/06
03/07
10/07
17/07
24/07
31/07
07/08
14/08
21/08
28/08
04/09
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual


mayo
junio
julio
agosto
septiembre
17/04
24/04
01/05
08/05
15/05
22/05
29/05
05/06
12/06
19/06
26/06
03/07
10/07
17/07
24/07
31/07
07/08
14/08
21/08
28/08
04/09
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual


17/04
24/04
mayo
01/05
08/05
15/05
22/05
junio
29/05
05/06
12/06
19/06
julio
26/06
03/07
10/07
17/07
24/07
agosto
31/07
07/08
14/08
21/08
septiembre
28/08
04/09
07/06
18/08
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual


octubre
noviembre
diciembre
enero
febrero
11/09
18/09
25/09
02/10
09/10
16/10
23/10
30/10
06/11
13/11
20/11
27/11
04/12
11/12
18/12
25/12
01/01
08/01
15/01
22/01
29/01
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual


octubre
noviembre
diciembre
enero
11/09
18/09
25/09
02/10
09/10
16/10
23/10
30/10
06/11
13/11
20/11
27/11
04/12
11/12
18/12
25/12
01/01
08/01
15/01
22/01
29/01
20/10
Proyecto: Gantt
Fecha: mar 24/10/17
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual

ANEXO E – FORMULARIO DESCRIPTIVO DEL TRABAJO FINAL DE GRADUACION

AUTORIZACIÓN PARA PUBLICAR Y DIFUNDIRTESIS DE POSGRADO O GRADOA LA UNIVERIDAD SIGLO 21

Por la presente, autorizo a la Universidad Siglo21 a difundir en su página web o bien a través de su campus virtual mi trabajo de Tesis según los datos que detallo a continuación, a los fines que la misma pueda ser leída por los visitantes de dicha página web y/o el cuerpo docente y/o alumnos de la Institución:

Autor-tesista *(apellido/s y nombre/s completos)*	Medina Carranza Facundo Martin
DNI *(del autor-tesista)*	31.901.759
Título y subtítulo *(completos de la Tesis)*	Seguridad Informática: Virus Ransomware, el secuestro virtual de datos es posible.
Correo electrónico *(del autor-tesista)*	medinafacundom@gmail.com
Unidad Académica *(donde se presentó la obra)*	Universidad Siglo 21
Datos de edición: *Lugar, editor, fecha e ISBN (para el caso de tesis ya publicadas), depósito en el Registro Nacional de Propiedad Intelectual y autorización de la Editorial (en el caso que corresponda).*	Córdoba, Medina Carranza Facundo Martin, 5 de diciembre de 2017

Otorgo expreso consentimiento para que la copia electrónica de mi Tesis sea publicada en la página web y/o el campus virtual de la Universidad Siglo 21 según el siguiente detalle:

Texto completo de la Tesis *(Marcar SI/NO)*[1]	SI
Publicación parcial *(Informar que capítulos se publicarán)*	

Otorgo expreso consentimiento para que la versión electrónica de este libro sea publicada en la en la página web y/o el campus virtual de la Universidad Siglo 21.

Lugar Fecha: Córdoba, 6 de Diciembre de 2017

Firma autor-tesista **Aclaración autor-tesista**

Esta Secretaría/Departamento de Grado/Posgrado de la Unidad Académica: _____certifica que la tesis adjunta es la aprobada y registrada en esta dependencia.

Firma Autoridad Aclaración Autoridad

Sello de la Secretaría/Departamento de Posgrado

[1] Advertencia: Se informa al autor/tesista que es conveniente publicar en la Biblioteca Digital las obras intelectuales editadas e inscriptas en el INPI para asegurar la plena protección de sus derechos intelectuales (Ley 11.723) y propiedad industrial (Ley 22.362 y Dec. 6673/63. Se recomienda la NO publicación de aquellas tesis que desarrollan un invento patentable, modelo de utilidad y diseño industrial que no ha sido registrado en el INPI, a los fines de preservar la novedad de la creación.