Articles

Análisis y técnicas de prevención ante ataques ransomware

Analysis and prevention techniques for ransomware attacks

Dustyn Zamora Baidal*
Anthony Triviño*
Puris Cáceres Amilkar Yudier*
Zhuma Mera Rodrigo Emilio*
Byron Oviedo Bayas*

REVISTA TECNOLÓGICA
ciencia y educación
Edwards Deming

ISSN: 2600-5867

Editado por: Tecnológico Superior Corporativo Edwards Deming
Enero - Julio Vol. 5 - 1 - 2021
https://revista-edwardsdeming.com/index.php/es
e-ISSN: 2576-0971
Recibido: 09 Marzo 2020
Aprobado: 09 Diciembre, 2020
Pag 109-122

RESUMEN

El presente proyecto de investigación está enfocado al análisis de los ataques ransomware y las formas para contrarrestarlo. Los ransomware son un tipo de malware que encriptan datos dejándolos inaccesibles y para desencriptarlos los ciberatacantes piden un rescate, generalmente económico. El proyecto consta de 4 partes y se plantea primero, realizar una recopilación de estudios con relación a los ataques ransomware usando el meta-análisis. Posteriormente se conocen los ransomwares más comunes y las características de los ataques por localidad, tipo de empresas, economía y software. En esta parte se detalla estadísticamente el impacto del ransomware a nivel global. En tercera parte se realiza un ataque ransomware WannaCry considerado el más común, simulado en una

* Ingeniero en Telemática de la Universidad Técnica Estatal de Quevedo, dustyn.zamora2016@uteq.edu.ec, ORCID: https://orcid.org/0000-0002-8127-004X

* Ingeniero en Telemática de la Universidad Técnica Estatal de Quevedo, anthony.triviño2016@uteq.edu.ec, ORCID: https://orcid.org/0000-0002-2888-4210

* PhD Docente Investigador en la Universidad Técnica Estatal de Quevedo, Ecuador. apuris@uteq.edu.ec ORCID: https://orcid.org/0000-0002-7288-7451

* MsC, Docente y Coordinador de Carrera en la Universidad Técnica Estatal de Quevedo, Ecuador. ezhuma@uteq.edu.ec. ORCID: https://orcid.org/0000-0002-3086-1413

* PhD en Tecnologías de la Información y Comunicación. Profesor Titular y Director de Investigación de la Universidad Técnica Estatal de Quevedo, Ecuador. E-mail: boviedo41@uteq.edu.ec. ORCID: https://orcid.org/0000-0002-5366-5917

Articles
Revista tecnológica ciencia y educación Edwards Deming
ISSN: 2600-5867

máquina virtual, también se detalla el proceso de infección y encriptación de los datos.

Palabras clave: ransomware, ciberseguridad, meta-análisis, simulación, compendio.

ABSTRACT

This research project is focused on the analysis of ransomware attacks and ways to counteract it. Ransomware is a type of malware that encrypts data making it inaccessible and to decrypt it the cyberattackers pay a ransom, usually economic. The project consists of 4 parts and it is proposed first to carry out a compilation of studies related to ransomware attacks using meta-analysis. Subsequently, the most common ransomwares and the characteristics of the attacks by location, type of companies, economy and software are known. In this part, the impact of ransomware at a global level is statistically detailed. In the third part, a WannaCry ransomware attack, considered the most common, is simulated in a virtual machine, and the infection and data encryption process is also detailed.

Keywords: ransomware, cybersecurity, meta-analysis, simulation, compendium

INTRODUCCIÓN

En el año 2020 con la aparición del Coronavirus el internet se ha convertido en nuestro mejor aliado, con el distanciamiento social se han necesitado varias alternativas para poder retomar las actividades de manera normal.

La ciberseguridad ha incrementado su nivel de interés para la sociedad en la última década, debido a los frecuentes ataques informáticos que llegan a colapsar plataformas gubernamentales, con trágicas consecuencias (Zambrano, 2019).

Los hackers buscan constantemente grietas en las defensas que se colocan como protección; si la empresa opta por renunciar a la seguridad de la red informática, puede dañar gravemente su reputación y hacer vulnerable su red, datos y aplicaciones (Zambrano, 2019). La seguridad en Internet debería ser una prioridad para cualquier empresa u organización con presencia en el medio digital.

La mayoría de las personas desconocen qué tan vulnerable es la información que envían a través de internet o que tienen almacenada en sus ordenadores, dispositivos móviles y servicios en la nube. Esto se debe al desconocimiento, falta de información y poco interés en la seguridad informática.

Es de conocimiento que la mayoría de las personas naturales ajenas a las tecnologías no se preocupan por su seguridad y la de sus archivos, pero, no solo ellas son afectadas por los ciberataques, nadie está completamente a salvo.

En esta época digital donde la mayor cantidad de información está en internet es de suponer que gracias a los avances tecnológicos la seguridad debería ser totalmente efectiva, pero el panorama es completamente diferente, cada día se realizan ataques cibernéticos ransomware de tipo scareware atracando a empresas o cualquier persona que sea vista como un blanco viable para los ciberdelincuentes haciendo que en muchas ocasiones el afectado pierda su información.

No se necesita ser un ingeniero en informática ni tener un profundo conocimiento en el tema para hacer ataques ransomware. En la Dark Web existen "paquetes" de ransomware como servicio (RaaS). El software viene listo para su uso, con manuales de funcionamiento e incluso videos instructivos, es similar a adquirir un programa cualquiera como los servicios Office 365 de Microsoft, en los pagos generalmente se usan criptomonedas como bitcoins casi imposibles de rastrear.

Algunas medidas preventivas ayudarían a que las personas reconozcan cuando son atacados por ransomware y si es posible recuperar la información sin necesidad de dar dinero.

Existen varios tipos y formas de realizar ataques ransomware por esta razón es necesario un estudio que detalle los diferentes tipos de ataques y sus técnicas de operación, además especificar algunos procedimientos de mitigación, prevención y recuperación de la información afectada.

Es necesario que las personas tengan algo de conocimiento sobre seguridad informática y de esta manera evitar que sean víctimas.

Realizando un estudio de los países que han sido más propensos en los últimos años al ransomware, conoceremos en qué mercados se han ido estableciendo los atacantes, también el profundizar en el por qué el 2020 se ha incrementado el malware ransomware con respecto a años anteriores y cuáles son los países con la menor seguridad en sus sistemas.

Es necesario conocer cuáles son los ambientes favoritos de los ciberdelincuentes para tener mayor cuidado. Para ello determinaremos el software al que prefieren atacar y cuáles son sus motivos, por ejemplo 0 days, fallos de seguridad o vulnerabilidades en el sistema, así sabremos por donde se mueven los atacantes que podrían ser páginas webs, aplicaciones de escritorio, aplicaciones móviles, etc.

Con toda la información obtenida tendremos las bases para iniciar el testeo y simulación de ataques ransomware. Haciendo pruebas de campo obtendremos conocimiento del modus operandi y las técnicas que utilizan los ciberdelincuentes para adentrarnos en su campo, experimentando en primera persona cómo es ser víctima y cómo es llevarlo a cabo ataques de ransomware.

De todo lo aprendido anteriormente y los análisis realizados se desarrollará un compendio o guía de buenas prácticas, que recopilen tips, métodos, procesos y software

Articles
Revista tecnológica ciencia y educación Edwards Deming
ISSN: 2600-5867

de apoyo para hacerle frente a los piratas informáticos mismo que será publicado para conocimiento de las personas.

El Ransomware es la palabra o término utilizado a todo tipo de software malicioso que tiene como objetivo controlar un sistema o apropiarse de los datos, y que exige al propietario una remuneración de un rescate para el proceso de liberación. La función de este software es cifrar los documentos con una clave única que cuando el usuario provea la recompensa se la proporcionará (Romero, 2018).

RANSOMWARE DE BLOQUEO

Este tipo de ransomware impide que la persona afectada acceda a su propio dispositivo, es decir, el usuario no tiene control sobre su sistema o dispositivo hasta que el pago del rescate se haya realizado (Skulason, 1990).

En muchas ocasiones este tipo de atraques permite una breve manipulación del teclado, con el único fin de que mediante el periférico se realice el pago. En este tipo de ataques los ciberdelincuentes utilizan técnicas de ingeniería social para que la víctima realice el pago (Skulason, 1990).

- LOOCKSCREEN

El ransomware Lockscreen en Windows ha utilizado varios temas en el pasado. Algunos ejemplos anteriores incluían pantallas de bloqueo que aparecían como pantalla azul de la muerte (BSOD) o un mensaje de activación de Windows. Mientras de vez en cuando detectamos varios temas nuevos en la pantalla de bloqueo, el que se repite con mayor frecuencia en los últimos años es el ransomware policial. Reveton es una de las familias más conocidas de este tipo (Ferbrache, 1992.).

RANSOMWARE DE CIFRADO

El ransomware de cifrado evita que el usuario tenga acceso a los archivos o datos, también es conocido como "Data Locker" o casillero de datos, este tipo de malware se mantiene en los dispositivos después de instalarse. Busca datos útiles del usuario y los cifra, después del cifrado elimina los datos originales y solicita al usuario que pague el rescate para obtener una clave privada para descifrar los datos bloqueados (Skulason, 1990).

Este tipo de ataques no realizan ninguna modificación en los archivos críticos del sistema, esto permite que el usuario tenga control a otras opciones y poder continuar realizando otros trabajos excepto en los archivos encriptados (Skulason, 1990).

- WANNACRY

El 9 de febrero de 2017, investigadores de Fortinet descubrieron la primera muestra de WannaCry, la dominaron versión beta del ransomware (J. L. Garcia Rambla, 2014).

Esta versión encriptaba los archivos utilizando el algoritmo AES-128 y no tenía ningún componente gusano implementado. El 28 de marzo del 2017 los mismos investigadores encontraron una mejor versión denominada WannaCry 1.0, utilizaba un diccionario codificado que le permitía acceder a las carpetas compartidas del Server Message Block (SMB) (S. Trigo, 2017).

MATERIALES Y MÉTODOS

Consta de 4 etapas.

PRIMERA ETAPA

La primera etapa hace uso de las técnicas del meta-análisis para seleccionar documentos relacionados al tema. Se desarrollaron criterios de selección para que el proceso de recolección sea los más preciso posible para desarrollo de los objetivos.

SEGUNDA ETAPA

En la segunda etapa a partir de la revisión del contenido de los estudios se consolidó toda la información necesaria para conocer los tipos de ataques de ransomware más comunes y los softwares que afectan. Se precisaron los problemas causados por los ataques ransomware y los efectos que tienen en la economía. También se detalló los países más afectados y su posición para contrarrestar ransomware en sus organizaciones.

TERCERA ETAPA

Consta de una simulación en ambiente controlado del tipo de ransomware que más se repitió en los trabajos seleccionados considerándose como uno de los más comunes, WannaCry. El propósito de la simulación es conocer el modus operandi de los atacantes y cómo el programa malicioso infecta y encripta los archivos. Se utilizaron programas y herramientas de detección, y recuperación de información.

CUARTA ETAPA

Aquí se encuentra un compilado de la información obtenida por los análisis bibliográficos y la simulación. Contiene consejos, tips y técnicas de prevención, detección y recuperación de archivos afectados por ataques ransomware en ordenadores, sintetizando los puntos clave de nuestra investigación.

RECURSOS HUMANOS, INSUMOS Y EQUIPOS EMPLEADOS

RECURSOS BIBLIOGRÁFICOS

- Libros
- Artículos

- Tesis
- Entrevistas

RECURSOS SOFTWARE

- Windows 10
- Microsoft Word
- Microsoft Power Point
- Python
- Visual Studio
- Mendeley
- Debian GNU/Linux

RECURSOS HARDWARE

- Computadoras
- Smartphones

RESULTADOS

PRIMERA ETAPA

REVISIÓN SISTEMÁTICA

Para cumplir con el primer objetivo se realizaron las siguientes preguntas:

1. ¿Cuál es el tipo de ransomware que con mayor frecuencia secuestra información de los ordenadores?
2. ¿Cuál es la información más perseguida para ataques de cualquier tipo de ransomware?

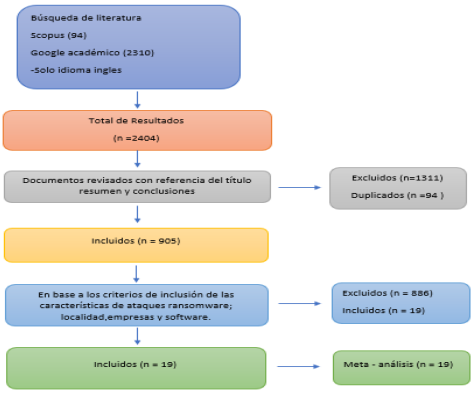

Ilustración 1 Estudios seleccionados para características de ataques ransomware. Fuente: Autores

En la ilustración 1 se observa los estudios seleccionados para la búsqueda de los tipos de ransomware más comunes fueron 16, en cada uno de los estudios no se encontró el tipo de ransomware más común que afectara a todo tipo de institución, pero, se observó cuáles son los que se mencionan frecuentemente en varios estudios realizados, como por ejemplo, en el estudio de Maxat Akbanov (Ransomware detection and mitigation using software-defined networking: The case of WannaCry) y en el de Rdra Baksi junto a Shambhu Upadhyaya (Decepticon: A Theoretical Framewoek to Counter advanced Persistent Threats).

Para conocer otras características de los ataques ransomware se tomaron un total de 19 trabajos que responden a las siguientes preguntas:

1. ¿Cuáles son los países o regiones que según los últimos años han sufrido más ataques ransomware?
2. ¿Cuáles son los tipos de empresas que han sido más atacadas por ransomware?
3. ¿Existe algún software ya sea, sistemas operativos o plataformas digitales que los ciberdelincuentes prefieran?

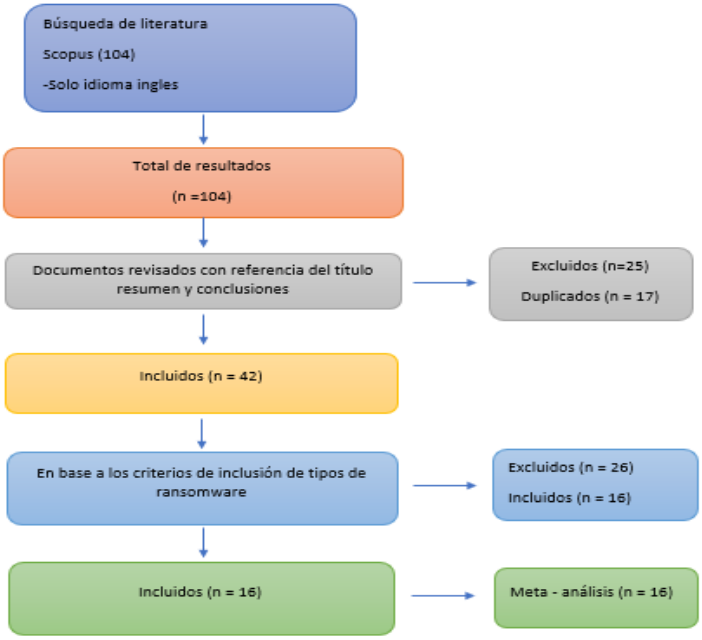

Ilustración 2 Estudios seleccionados para tipos de ransomware. Fuente:Autores

SEGUNDA ETAPA
TIPOS DE RANSOMWARE MÁS COMUNES

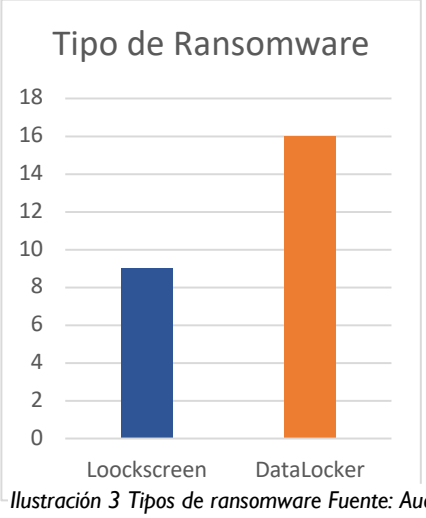

Ilustración 3 Tipos de ransomware Fuente: Auotres

Según los estudios existen dos grandes tipos de ransomware con objetivos similares, pero con enfoques diferentes que son:

- Locker ransomware
- Cripto ransomware.

De ellos se derivan las diferentes familias ransomware como WannaCry, Locky o Policial. En la ilustración 3 se puede observar que en 9 documentos de los 16 se pronuncia con frecuencia el tipo de ransomware Loockscreen y en los 16 documentos sin excepción alguna está presente el Datalocker, por la siguiente razón se concluye el tipo de ransomware Datalocker es el más común. Su popularidad se debe a sus propiedades y porque es preciso en llegar a la información más importante por el usuario y encriptarla. Los targets principales son archivos con extensiones doc, pdf, txt, en otras palabras, los documentos de los usuarios.

Entre los 4 ransomware graficados en el histograma, el ransomware WannaCry es uno de los más comunes, siendo de los más populares hasta el momento, debido al gran impacto que ha ocasionado en varias instituciones públicas y privadas a nivel mundial.
El ransomware Locky es de tipo Datalocker y también fue popular por su característica de secuestro. En el estudio "Ransomware detection and mitigation using software-defined networking: The case of Wannacry" se realizan pruebas con el ransomware WannaCry para monitorear el dispositivo y observar cual es la característica por la cual es uno de los más populares.

OTRAS CARACTERÍSTICAS DE LOS ATAQUES RANSOMWARE

Todos los rescates pedidos de los ransomware más comunes comparten el tipo de moneda digital como medio de pago. Se muestran los ataques ransomware y las monedas digitales que comúnmente utilizan.

FORMAS DE ATAQUES RANSOMWARE

La forma en la que las personas se infectan de ransomware casi siempre son ataques dirigidos que llegan al correo. Los atacantes envían links en los emails para que al hacer clic redirija automáticamente a la persona a una página donde se encuentra el ransomware. La segunda forma más común es por medio de documentos adjuntos en el email como archivos comprimidos documentos de texto, pdfs, entre otros.
Casi siempre se ha realizado un estudio previo a fondo de la víctima para conocer su comportamiento e intereses personales. Así garantizan que el ataque sea efectivo, tal práctica se conoce como ingeniería social. En tercer lugar, están los sitios web que no cuentan con seguridades correspondientes (https, SSL), luego los medios sociales y por último USB infectadas o dispositivos externos manipulados.

TERCERA ETAPA
SIMULACIÓN DE ATAQUE RANSOMWARE WANNACRY

La simulación se realizó en una máquina virtual para evitar contaminar la información de la PC personal.
Primero se configuró una máquina virtual en Virtual Box con el sistema operativo Windows 10 en su última versión, la elección del SO fue en parte arbitraria basándonos en cuál es el SO más común. Se realizaron las configuraciones correspondientes para aislar la PC virtual del ordenador principal deshabilitándole el adaptador de red quitándole la conexión a internet y bloqueando la entrada de dispositivos externos. El ransomware fue descargado desde internet.

En la ilustración 7 se observa que el archivo "WannaCry.rar" se encuentra comprimido, esto no quiere decir que así será siempre el modo de ataque, puede que se encuentre dentro de archivos o programas ejecutables, que una vez instalados en el sistema operativo pueden ocasionar severos daños.
Para continuar, se verificó el estado de Windows Defender, si estaba activo continuaríamos con el proceso de ejecución del WannaCry.

Inmediatamente el sistema de seguridad de Windows detecta un ransomware en el sistema, el cual puede causar daños en nuestros documentos, en este ejemplo afectaría a los documentos pdf que tenemos en el escritorio.
Y una vez ejecutado el malware siguen intactos, es decir nuestra información sigue segura. Esto es gracias a que el equipo de seguridad de Windows corrige y analiza frecuentemente las posibles amenazas que infectan a los usuarios.

La base de datos que contienen información de los virus se va actualizando constantemente entonces es más fácil detectar un ransomware. Pero los ciberdelincuentes encuentran la forma de burlar los antivirus por lo que se debe tener cuidado al descargar archivos y navegar por internet.

¿QUÉ PASARÍA SI NO ESTUVIERA ACTIVADO EL SISTEMA DE WINDOWS DEFENDER EN NUESTRO DISPOSITIVO?

Posteriormente los documentos y archivos quedan en formato. wncry.

Algunos ransomware reinician el sistema y no dejan entrar al usuario este es el caso de los LoockScreen. WannaCry no reinicia el sistema, sino que encripta mientras el usuario usa su computadora.

La mayoría de sus documentos fueron encriptados si no es que todos lo han sido, existe la probabilidad que los pierda para siempre. La importancia de los archivos depende del valor que tengan, pueden ser simplemente imágenes personales o, al contrario, documentos muy importantes de su trabajo.

CUARTA ETAPA

TÉCNICAS ANTE ATAQUES RANSOMWARE

- PREVENCIÓN

La mejor forma de evitar ser víctima de un ataque ransomware es ser muy meticuloso con la seguridad de los sitios web que visita, los archivos que descarga o los dispositivos que inserta a su computador. Cualquier técnica por más simple que parezca ayudará a la integridad de su ordenador.

Existen varios tipos de navegadores, unos se dedican completamente a la confidencialidad de la información de los usuarios y otros se enfocan en la rapidez de las búsquedas. Los navegadores también presentan fallos de seguridad que los hace vulnerables.

Se debe elegir un navegador que bloquee las páginas que intentan obtener permisos o que no cuentan con seguridad estándar. Las alternativas más seguras son:

- Opera
- Brave
- Mozilla Firefox

DETECCIÓN

El uso de antivirus es muy importante porque permite detectar amenazas y eliminarlas, pero no existe mejor antivirus que la cautela de la persona misma.

Los antivirus más populares son buenos y casi en su mayoría tienen las mismas finalidades y funciones. La gran mayoría son servicios de paga, si usted es una persona que navega siempre en páginas seguras de internet el antivirus que viene por defecto en Windows (Windows Defender) será suficiente para su seguridad. Pero si maneja información sensible deberá suscribirsea un servicio de antivirus o antimalware. Los más populares son:

- Kaspersky
- Norton

- ESET
- Avast
- McAfee

MITIGACIÓN

Si somos víctimas de ataques ransomware lo primero que debemos hacer es aislar la computadora el resto de la red como forma de seguridad.

Existen varias herramientas que permiten desencriptar archivos infectados por ransomware uno de ellos es el servicio en línea "No More Ransom" que contiene herramientas desencriptado para varios tipos de ransomware, potenciada por organizaciones públicas y privadas.

DISCUSIÓN

Se analizaron los tipos de ransomware más comunes y la información más atacada para así determinar cuál es más propensa a sufrir ataques ransomware, en el que se determinó que Wannacry está presente en el 100 % de los documentos incluidos para la investigación. También se conocieron los inconvenientes que ocasiona el ransomware en los datos de los ordenadores infectados gracias a la simulación de ataque ransomware realizada. Resultado de la revisión de los estudios y de la simulación se obtuvo conocimiento del modus operandi de los ciberatacantes y la forma en la que infectan a sus víctimas. Se realizó un estudio de las características de los ataques ransomware con respecto a la localización donde han tenido mayor impacto, expresando los países y regiones que han sido más afectados. Con respecto a la economía, se conoció una estimación de 200.000 millones de dólares perdidos por ransomware, y gracias a la revisión se determinaron los tipos de empresas u organizaciones más propensos y que más han sufrido ataques ransomware en los últimosaños, según "The State of Ransomware 2020" un 60 % de los ataques realizados en el 2020 fueron dirigidos a medios de comunicación y entretenimiento. Se conocieron los sistemas operativos que los atacantes prefieren, y los medios de esparcimiento de este tipo de malware. Con la información obtenida anteriormente de los estudios realizados y la información adquirida de primera fuente, producto de la simulación del ataque ransomware considerado más común, se elaboró un compendio de prácticas de prevención, detección y mitigación de ataques ransomware. En él se detallan las formas más comunes en que los ciberdelincuentes engañan a las personas e infectan sus ordenadores, para luego pedir dinero a cambio de desencriptar su ordenador. Aquí se describen algunos métodos para detectar y detener ransomware que ayudarán a los usuarios evitar ser víctimas de este gran problema.

REFERENCIAS

A. Alzahrani, A. A. (2020). *Ransomware in windows and android platforms.*

A. F. Osorio-sierra, M. J.-h. *Proceso para la identificación , clasificación y control del comportamiento de familias Ransomware.*

ABC. (2020). *Los peligros del «ransomware»: la gran amenaza de las empresas en internet.*

BleepingComputer. (2016). *Locky Ransomware Information, Help Guide, and FAQ.*

Cahua, R. B. (2014). *Introducción al meta-análisis tradicional.*

Eguía, A. (2016). *http://1.bp.blogspot.com*. Obtenido de http://1.bp.blogspot.com/-ufPhFylcQPY/TopwlPmsByI/AAAAAAAAMxI/hw_N_64fyxA/s1600/facebook-phishing.jpg.

Ferbrache, D. (1992.). *A Pathology of Computer Viruses.*

Fortinet. (2020). *https://www.fortinet.com*. Obtenido de https://www.fortinet.com/blog/threat-research/wannacry-evolving-history-from-beta-to-2-0

Ghorpade, R. S. (2018). *Ransomware attacks: Radical menace for cloud computing.*

Gibson, J. (2020). *No more Ransom.*

J. L. Garcia Rambla, C. A. (2014). *Ataques en redes de datos IPv4 e IPv6.*

K. Cabaj, P. G. (2017). *The impact of malware evolution on the analysis methods and infrastructure.*

Kokare, R. K. (2020). *A Survey on Malware Detection and Classification.*

M. Akbanov, V. G. (2019). *Ransomware detection and mitigation using software-defined networking: The case of WannaCry.*

M. Humayun, N. Z. (2020). *Internet of things and ransomware: Evolution, mitigation and prevention.* Egiptoç.

Martin, M. C. (2017). *Seguridad Informática: virus ransomware, el Secuestro virtual de datos es Posible.*

Microsoft. (s.f.). *https://answers.microsoft.com/*. Obtenido de https://answers.microsoft.com

Moya, A. M. (2008). *La Investigación en la era de la Información. Guia para realizar la biliografias y fichas de trabajo.*

muycomputer.com. (2019). *www.muycomputer.com*. Obtenido de https://www.muycomputer.com/2019/12/16/pagar-rescate-ransomware-microsoft/

Perez, J. (2017). *Malwa*. Obtenido de https://www.hijosdigitales.es/es/2017/12/google-chrome-no-regala-iphone-una-estafa/

PODGÓRSKI, G. (2020). *Analysis of the internet activity of employees in the context of threats and their activity in the network – a case study*.

R, B. (2019). *Diseños cuasi-experimentales y longitudinales.*

R. Lipovský, L. Š. (2015). *The Rise of Android Ransomware.*

Romero, F. J. (2018). *Ransomware , hacking y phishing : conducta típica del delito de daños.*

S. Trigo, M. C. (2017). *Ransomware: seguridad, investigación y tareas forenses.*

Sánchez-Meca, J. (2010). *Cómo realizar una revisión sistemáticay un meta-análisis. sensorstechforum.com*. (s.f.). Obtenido de https://sensorstechforum.com/es/remove-windows-banned-lockscreen-virus/

Skulason, E. W. (1990). *The Authoritative International Publication on Computer Virus Prevention, Recognition and Removal.*

Sophos. (2020). *THE STATE OF RANSOMWARE 2020.*

Toaza, A. L. (2013). *Análisis heurístico de malware aplicado a la detección de documentos pdf maliciosos en el gobierno autónomo descentralizado municipalidad de Ambato.* Ambato.

VALLEJO, D. A. (2018). *Trabajo de titulación previo a la obtención del título de: Ingenieros de Sistemas.* Quito.

Vásquez, C. A. (2014). *Meta-análisis aplicado a Business Intelligence para la toma de decisiones objetivas en entidades financieras.*

Wilson, D. B. (1999). *Practical Meta-Analysis-Lipsey & Wilson Overview Practical Meta-Analysis The Great Debate.*

Zambrano, N. Z. (2019). *Ciberseguridad y su aplicación en las Instituciones de Educación Superior.* espam.edu.ec.

Zurita, J. A. (2019). *ESCUELA POLITÉCNICA NACIONAL FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA.* Quito.