UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICACEV

PROCESO DE TITULACIÓN

JUNIO 2023 - OCTUBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

ANÁLISIS COMPARATIVO DE CIBERSEGURIDAD ENTRE MALWARE Y RANSOMWARE PARA CONOCER EL SOFTWARE MÁS SEGURO ANTES LOS VIRUS FRECUENTES QUE EXISTEN DENTRO DE LAS COMPUTADORAS.

EGRESADA:

VERDEZOTO LOOR JENYFFER KATIUSKA

TUTOR:

CEVALLOS MONAR CARLOS ALFREDO

AÑO 2023

SUMMARY

During the pandemic, there have been more attacks from these malicious viruses, both malware and ransomware. In the development of this comparative case study, we are interested in knowing which of these viruses in question are more harmful to computers, the malware virus, is known to be malicious software, it has a broad category that is encompassed by many programs designed exclusively to damage, steal or compromise computer systems, in which by installing this virus, viruses, worms, Trojans and spyware can be included, among others. In others, malware generally seeks to infiltrate systems without the user's prior knowledge or consent to steal data or cause damage. On the other hand, ransomware is more specific than malware, since it encrypts the victim's files, demanding an additional ransom value to unlock certain information or data in particular, explaining a brief summary. This type of virus is used by cybercriminals because it serves to extort users and organizations, threatening permanent data loss if the requested ransom is not paid. It is essential through this comparative analysis of cybersecurity, to consider the functions, advantages, disadvantages and important characteristics of how these malicious viruses are designed, malware is the most diverse and can spread through multiple vectors, while Ransomware generally spreads through emails and malicious downloads or links. Importantly, ransomware damages can cause critical data loss and costly downtime, the probability of data recovery is very high in case of malware, since most malicious programs do not encrypt files. This document will list the most important and appropriate security software.

Keywords

Viruses, Cybersecurity, Malicious, Software, Programs.

RESUMEN

Durante la pandemia se han suscitado más ataques de estos virus maliciosos tanto como malware y ransomware, en el desarrollo de este caso de estudio comparativo se encuentra inclinado en conocer cuál es de estos virus en mención, son más dañinos para las computadoras, el virus malware, es conocido por ser software malicioso, tiene una categoría amplia que esta englobada por muchos programas diseñados exclusivamente para dañar, robar o comprometer sistemas informáticos, en la cual mediante la instalación de este virus se pueden incluir virus, gusanos, troyanos y spyware, entre otros, por lo general el malware busca ser infiltrado en sistemas sin el previo conocimiento o el consentimiento del usuario para robar datos o causar daños. En cambio el ransomware es más específico que el malware, ya que este encriptan los archivos de la víctima exigiendo un valor adicional del rescate para desbloquear cierta información o datos en particular, explicando un breve resumen este tipo de virus es utilizado por los ciberdelincuentes porque sirve para extorsionar a usuarios y organizaciones, amenazando con la pérdida permanente de datos si no se llega a pagar sobre ese rescate solicitado. Es esencial mediante este análisis comparativo sobre la ciberseguridad, por se llegaran a considerar las funciones, ventajas, desventajas y características importante en cómo se encuentran diseñados estos virus maliciosos, el malware es el más diverso y puede propagarse a través de múltiples vectores, mientras que el ransomware generalmente se propaga a través de correos electrónicos y descargas o links maliciosos. Es importante que los daños del ransomware pueden causar pérdida de datos crítica y tiempo de inactividad costoso, la probabilidad de recuperación de datos es muy alta en el caso de malware, ya que la mayoría de los programas maliciosos no cifran los archivos. En este documento se enlistará los softwares de seguridad más importantes y adecuado.

Palabras claves

Virus, Ciberseguridad, Maliciosos, Software, Programas.

INTRODUCCIÓN

La tecnología ha tenido muchos avances en los últimos años, más aún con la pandemia que existió hace un par de años atrás, permitiendo abarcar todo lo que es dispositivos móviles y más importantes las computadoras en la cual muchos usuarios se dedicaron al trabajo virtual en donde se observó que muchas de estos ordenadores tenían problemas con los diferentes virus que se detectaban dentro de las computadoras un sin número de estos virus que se desconocían, este proyecto comparativo se encuentra inclinado en conocer cuál es el software más seguro en el ámbito de ciberseguridad entre Malware y Ransomware.

El objetivo general de este caso de estudio es de evaluar y comparar la efectividad de diferentes soluciones de seguridad cibernética en la detección, prevención y mitigación de amenazas de malware y ransomware en sistemas informáticos, mediante un gran análisis que se realizará, se buscará identificar el software de seguridad más eficiente y adecuado para proteger los sistemas informáticos contra las amenazas de virus más comunes.

Malware “software malicioso” este es uno de los softwares que se encuentra con muchas variedades de programas diseñados con intenciones dañinas hacia los ordenadores, como por ejemplo, virus, troyanos, gusanos y spyware. Son agentes diseñados para infiltrarse en sistemas informáticos, propagándose rápidamente en los datos confidenciales que están en las computadoras, mientras que el Ransomware ha sido destacado por su capacidad de bloquear el acceso a archivos y sistemas, exigiendo un rescate a cambio de la restauración de los datos que han sido secuestrados. Este estudio comparativo propone abordar este desafío al realizar un análisis exhaustivo de la ciberseguridad entre los software ya nombrados, a través de pruebas controladas y evaluaciones rigurosas, destacando las características que será la clave para dar con la solución a la seguridad, se observará mediante las investigaciones que se realizarán cuál de

ellas demuestra ser más resistente y eficaz contra las amenazas de virus más frecuentes en el entorno digital.

Este proyecto se guiará mediante la línea investigativa de Sistemas de información y comunicación, emprendimiento e innovación, y su sublínea de investigación de redes y tecnologías inteligentes de software y hardware.

METODOLOGIA

Metodología Descriptiva

La metodología investigativa a utilizarse dentro de este proyecto comparativo es la descriptiva, ya que es importante para esta investigación porque permitirá la recopilación, análisis y presentación objetiva de información relevante sobre las diferentes soluciones de seguridad cibernética en relación con la detección, prevención y mitigación de amenazas de malware y ransomware.

Técnica e Instrumento

Técnica e instrumento investigativo de este trabajo se utilizará la aplicación de Google Trends que es una de los aplicativos importante que ha diseñado Google en la cual mediante imágenes se observan cómo se encuentran los softwares mencionados haciendo más eficaz y eficiente este desarrollo investigativo, para conseguir los resultados y obtener una buena conclusión conociendo cual es el software más seguro en el ámbito de seguridad.

DESARROLLO

En el mundo digital cada vez más interconectado, la ciberseguridad se ha convertido en una preocupación crucial. El malware y ransomware son dos de las amenazas más comunes que enfrentan los usuarios de computadores. El malware es un término general que abarca diversos tipos de software malicioso diseñado para infiltrarse y dañar sistemas, mientras que el ransomware es un tipo específico de malware que cifra los archivos del usuario y exige un rescate para desbloquearlos. Para lograr una mejor investigación en base a este tema se deberá elegir un software de seguridad sólido es esencial para mitigar estos riesgos.

En el ámbito de protección de datos o información se encuentra la ciberseguridad, está siendo parte en gran parte a nivel mundial, en la actualidad nadie se encuentra a salvo de ser una víctima en el tema de ciberataques; siendo más frágil las empresas, instituciones financieras, gobiernos, hospitales, pymes y muchos usuarios que finalmente se encuentran con amenazas en internet. Se debe comprender la importancia de la seguridad informática, en la cual esto debe permitir obtener una mejor perspectiva sobre las estrategias y mejores prácticas que se desean implementar en todas las organizaciones que se encuentran con este tipo de problemas.

Ilustración 1. Ciberseguridad

Fuente: (Peralta, 2019)

Según muchos de los expertos por parte de la Asociación de Auditoría y Control de Sistemas de Información "ISACA", esto se define como una "capa de protección de los archivos de información o de datos", los términos de seguridad informática o de seguridad de datos son utilizados para proteger de cierta manera la información electrónica, es importante reconocer que uno de los objetivos generales de este tema de seguridad es generar confianza entre clientes, proveedores y el mercado en su conjunto.

En este mundo denominado "hiperconectado", se lo menciona de tal manera ya que la mayoría de las actividades o tareas son realizadas desde línea y electrónicamente, los empresarios y líderes mundiales ven los ciberataques como uno de los grandes riesgos que enfrentan hoy en día en el ámbito de ciberseguridad convirtiéndose como el mayor desafío.

Según el autor de la página web **(security, 2018)**. El primer hacker de la historia fue Neville Maskelyne. En el año 1903, se interceptó la primera transmisión telegráfica inalámbrica, demostrando la vulnerabilidad del sistema de Marconi. Jhon Draper, es reconocido como Captain Crunch, fue el primer ciberdelincuente. Jhon Draper fue el que descubrió el sonido de un silbato en una caja de cereal Cap'n Crunch es capaz de interrumpir la señal de un teléfono, utilizando llamadas gratuitas.

En los años 70 apareció el primer Malware de la historia, Creeper, en un programa que se replicaba de sí mismo mostrando un mensaje ¡Soy un canalla, atrapame si puedes! Desde ese momento inicio el primer software antivirus Reaper, cuya función era únicamente de prevenir las infecciones por parte de Creeper. A lo largo de todos esos años, a medida que la tecnología iba en su etapa de evolución, ha ido aumentando más información en la web, al igual que el valor y la importancia de la información en línea para las organizaciones y los ciberdelincuentes.

En la década de los 1980 se observó el aumento del malware y el desarrollo de software antivirus más eficaz. En la actualidad existen plataformas Endpoint Detección y Respuesta "EDR" en la cual ayudan a tener un mejor control y protección en las computadoras de ataques de malware debido a su enorme crecimiento que ha logrado en todo estos años.

MALWARE

En los años en 1971, Robert Thomas "BBN Corporation" creo un programa Creeper que viajaba entre computadoras conectadas a Arpanet, mostrando mensajes como se lo menciono al principio de la investigación. OpenMind de David Harley, este es un consultor de seguridad informática e investigador de ESET "por parte de la comunidad de investigación se deberá pensar en el programa experimental Creeper como el primer virus o gusano". Un año antes de la creación de MALWARE el taller de Cohen, Rich Skrenta, estudiante de 15 años, se dedicó a desarrollar Elk Cloner, es uno de los primeros virus informáticos que fue propagado fuera del laboratorio. Skrenta diseño el programa para bromear con sus amigos cuyas computadoras Apple II estaban infectadas, en la cual al insertar un disco con un juego que contenía esta clase de virus.

Ilustración 2. MALWARE

Fuente: (Panduru, 2022)

Según la autora del sitio web **(Panduru, 2022)**. A continuación se enlistará los ejemplos más importantes de los MALWARE.

- **CovidLock**

A medida que todo el planeta se encontraba en su debido descanso por la pandemia del año 2020, los piratas informáticos se encontraban más activos, explotando el miedo creado por la pandemia "Covid 19". Este tipo de virus es malicioso permitiendo infectar a los objetivos principales como archivos maliciosos que creen que proporcionan información sobre una enfermedad. En la cual mediante su instalación este virus cifra todos los datos del dispositivo de Android y niega acceso al usuario, para lograr recuperar archivos, pide rescate de un valor de 100 dólares por unidad.

- **Emotet, troyano 2018**

Emotet se convirtió en el malware más peligroso y destructivo por parte del Departamento de Seguridad Nacional de EE.UU en el año 2018. Es uno de los caballos de Troya que se utiliza para robar toda la información financiera, como registros bancarios y criptomonedas. El gesto se distribuye mediante correos electrónicos de forma maliciosa en forma de Spam y phishing, Uno de los mayores ataques de malware de Emotet incluyendo la ciudad de Allentown, Pensilvania, que causo muchos daños por el valor de 1 millón de dólares, y el banco chileno de Consorcio, que causó daños por 2 millones de dólares.

- **WannaCry**

Este es uno de los ataques maliciosos únicos, es denominado asi porque una vez que se infiltra en un sistema, se replica sin cambiar ningún archivo ni afectar el sector de arranque. Se utilizó en

uno de los ataques más devastadores del 2017, infectando 230.000 computadoras y causando daños por 4.000 millones de dólares en menos de un día. Se propaga principalmente a través de correos electrónicos fraudulentos y aprovechando vulnerabilidades en versiones anteriores de Windows, en algunos correos electrónicos de phishing afirman haberse infectado con WannaCry, pero no son detectados con facilidad ya que estos son solos correos electrónicos no deseados diseñados para engañarlo para que paguen el debido rescate.

- **Petya 2016**

Fue vista en el año 2016 cuando esta comenzó a propagarse a través de correos electrónicos de phishing. Petya es en realidad una familia de diferentes tipos que ha causado muchas pérdidas estimadas en más de 10 millones de dólares.

- **CryptoLocker**

Este fue uno de los ejemplos de Malware que destacó en su momento, fue a inicios del 2013, este utilizaba claves de cifrado inusualmente grandes, lo que causaba dolores de cabeza por asi decirlo a los expertos en ciberseguridad. Es uno de los troyanos que accede y cifra archivos del sistema. Los piratas informáticos utilizan tácticas de ingeniería social para engañar los empleados para que descarguen en sus computadoras e infecten redes enteras.

- **Stuxnet worm “gusano” 2010**

Este virus Stuxnet como es denominado, tiene sus inicios por primera vez en 2010, en el tiempo que se utilizó en ataques políticos al programa nuclear de Irán. Se trata de un gusano muy sofisticado que explota múltiples vulnerabilidades de día cero de Windows e infecta dispositivos a través de unidades de USB.

- **Zeus Troyano 2007**

Es uno de los troyanos que se ejecuta en el sistema operativo de Windows y se propaga a través de archivos adjuntos de correos electrónicos y sitios de phishing maliciosos, reconocido por su rápida difusión y duplicación de entradas al teclado.

Según el autor del sitio web **(Torrenegra, 2019)**. Se mostrará mediante cuadros las ventajas y desventajas de MALWARE.

Ventajas	Gran detección de virus polimórficos o desconocidos.
	Fácil de actualizar la base de virus.
	Análisis demasiado rápido.
	Fácil instalación.
	Ligero.
	Consume muy pocos recursos.

Tabla 1. Ventajas de MALWARE

Creado por: Jeniffer Verdezoto

Desventajas	Utiliza muchos recursos, poniendo lenta la PC.
	Lento a la hora de escanear.
	Analiza pocos archivos como “zip, ace, rar”
	No es software libre.
	Faltan muchas opciones.
	Algunos problemas para detectar con archivos comprimidos.

Tabla 2. Desventajas de MALWARE

Creado por: Jeniffer Verdezoto

Malware es un software cualquiera que realiza acciones maliciosas en un sistema informático, se encuentra diseñado deliberadamente con fines delictivos y sus funciones funcionan sin el consentimiento del usuario. El Malware no debe confundirse con el software corrupto, es también capaz de causar daños al sistema debido a los errores de códigos, pero no se encuentra diseñado intencionalmente con intenciones maliciosas.

Este software antimalware se encarga de combatir, prevenir, detectar y eliminar programas maliciosos. El software antivirus se utiliza a menudo indistintamente para describir el software que protege contra las amenazas cibernéticas, aunque el término "antivirus" solo se refiere a los virus informáticos de tipo malware.

Según el autor del sitio web **(Chavez, 2019)**. Se indicará mediante un cuadro las características principales que tiene el software Malware.

Características principales de Malware	Su código es programado para producir inherentemente ciertos tipos de ciberataques.
	Contiene todo tipo de software malicioso.
	Realiza muchas acciones sin el consentimiento del usuario.
	Intenta colarse en el sistema objetivo.
	Su actividad en el sistema puede pasar por desapercibida.
	Los ataques de malware son ilegales y, por lo tanto, están penados por la ley.

Tabla 3. Características de MALWARE

Creado por: Jeniffer Verdezoto

Según el autor de la página web **(Regan, 2022)**. Se enlistarán las señales más importantes de una infección maliciosa de malware.

- **Disminuciones repentinas del rendimiento.**

El malware puede utilizar un gran parte de la potencia de procesamiento de su dispositivo, provocando graves ralentizaciones, por lo tanto eliminar malware es una forma de acelerar su computadora.

- **Bloqueos y cierres del sistema frecuentes.**

Algunos tipos de malware pueden causar fallas en el sistema o en la computadora, mientras que otros pueden también causar fallas al consumir demasiada RAM o elevar la temperatura de la CPU. El uso constante y elevado del CPU puede indicar malware.

- **Archivos eliminados o dañados.**

El malware a menudo se encuentra eliminando o dañando archivos para causar tantos caos como sea posible dentro del computador.

- **Una gran cantidad de anuncios emergentes.**

La función de este adware es enviarle Spam a través de ventanas emergentes, otros tipos de malware también pueden generar alertas y anuncios emergentes.

- **Redirecciones del navegador.**

Si el navegador sigue redireccionándolo a sitios no deseados, es posible que un ataque de malware haya cambiado su configuración de DNS.

- **Contactos reciben mensajes extraños por parte de usted.**

Algunos tipos de malware se encuentran distribuidos por correos electrónicos o enviando mensajes a los contactos de las víctimas. Una aplicación de mensajería segura que puede proteger sus comunicaciones contra comunicaciones ilegales.

- **Nota de Rescate.**

Este informa de su existencia secuestrando por asi decirlo, la pantalla con una nota de rescate exigiendo un pago para recuperar los archivos. Una nota de rescate de manera fácil de descubrir que malware hay en su computadora.

- **Aplicaciones desconocidas.**

El malware se puede instalar en otras aplicaciones en su dispositivo, si ve un programa nuevo que no ha instalado, puede ser el resultado de un ataque de malware.

Mediante un cuadro se indicará los pasos más importantes para proteger la computadora del ataque malicioso Malware.

Pasos importantes para proteger al computador.	Instalar un Antivirus y Antimalware
	Mantener siempre el sistema operativo actualizado.
	Actualizar el software y demás Aplicaciones.
	Utilizar Firewalls
	Tener cuidado con los correos electrónicos y enlaces.
	Usar contraseñas de mucha protección.
	Realizar copias de seguridad regulares.

Tabla 4. Pasos importantes para proteger el computador

Creado por: Jeniffer Verdezoto

RANSOMWARE

El ransomware es un malware que se ejecuta "bloqueando los datos", los cifra con claves y luego pide que se pague esa clave para poder descifrarlas nuevamente y acceder desde el inicio a sus datos. Existen muchos ransomware que tienden a obligar a sus víctimas a tomar las medidas necesarias, incluyendo una fecha de vencimiento en la demanda de rescate. Tomando en cuenta que si el rescate no se paga antes de una fecha determinada, la clave que se ha descifrado se destruirá y todos los datos del rescate nunca estarán disponibles.

Según el autor del sitio web **(Daniela, 2019)**. El primer ransomware conocido como "troyano AIDS", apareció en 1989. Se distribuyó por correo en disquetes de usuarios de computadoras de todo el mundo. El malware es uno de los programas que se oculta en cifra de archivos en el ordenador del usuario y exige un rescate en moneda alemanda para desbloquear cierta información el conocido Deutsche Mark. El creador del troyano con el AIDS fue el médico estadounidense Joseph Pope, en la cual fue arrestado después de que la policía encontró un alista de nombres y direcciones posibles víctimas en su ordenador.

Al conocido Joseph Popp le diagnosticaron esquizofrenia paranoide y no fue condenado a ningún delito debido a la condición mental que este personaje padecía. En ese momento ese ataque no fue perfecto como lo pensaban, pero si existió la propagación de virus estuvo limitada por la necesidad de enviar disquetes, lo que sentó las bases para un ransomware más avanzado.

CryptoLocker fue uno de los primeros y más marcados de los ransomware que apareció a inicios de septiembre del año 2013, se propagó con tanta rapidez a través de los correos electrónicos y sitios web maliciosos que ofrecían descargas de softwares gratuitas.

Ilustración 3. RANSOMWARE

Fuente: (Ransomware, 2019)

Según el autor del sitio web **(Garza, 2022)**. A continuación se enlistará los ataques más importantes del ransomware.

- **Locker ransomware "bloqueador de equipo" – "impide el acceso al equipo o dispositivo".**

Este es un tipo de ransomware se puede hacer pasar por autoridades policiales a cambio de un rescate. Automáticamente acusando a la víctima de complicidad en un delito "que va desde una simple infracción de derechos de autor hasta de pornografía infantil" la computadora estaría bajo investigación y bloqueada. Por ejemplo en este tipo de hackeos el famoso Reveton afirmó fraudulentamente ser parte de una agencia legítima de aplicación de la ley y bloqueo de acceso a los usuarios y a las computadoras infectadas, exigiéndoles pagar una "multa" para restablecer el acceso normal.

- **Crpyto ransomware "bloqueador de datos" – "impide el acceso a archivos o datos".**

Este es el primer gran ataque de ransomware criptográfico de toda la industria. Este sistema utiliza un cifrado prácticamente irrompible para bloquear los archivos, carpetas y almacenes de

datos de los usuarios. La parte más temible de este ransomware es que incluso después de eliminar el malware, los datos y archivos permanecerán cifrados y bloqueados. En cuanto a los casilleros de contraseñas se basan en técnicas de ingeniería social para los objetivos potenciales durante su ejecución. Cuando las víctimas han sido parte de este ataque reciben un correo electrónico que contiene archivo de ZIP protegido con contraseña que dice ser de una empresa de logística.

- **CryJoker**

A inicios del año 2016 se descubrió una nueva forma de ransomware denominada CryJoker. Este cifra los archivos de la víctima utilizando el algoritmo AES-256 y luego exige un rescate para liberar la información. CryJoker afecta a ordenadores que se ejecutan en el sistema operativo Microsoft Windows, aunque CryJoker aún en ese entonces no se utilizaba mucho, los expertos en la rama de seguridad han comenzado a advertir a las empresas, instituciones financieras y demás, sobre la existencia de este nuevo ransomware.

Utiliza métodos de cifrados sólidos, también afecta a 30 tipos diferentes de archivos y elimina todas sus instantáneas. Los ataques de CryJoker suelen empezar desde un correo electrónico que al intentar engañar al destinatario o usuario que este abra el instalador disfrazado de PDF. El usuario del correo electrónico abre el archivo, se descarga un instalador o genera un ejecutable necesario para llevar a cabo el ataque, luego de esto el CryJoker escanea el disco de su computadora en busca de 30 tipos de diferentes archivos incluidos PDF, textos, Microsoft Word y Excel, también es enviado mediante los archivos como de imagen como JPG o PNG. Después de cifrar todos los archivos, agrega ".CryJoker" a la extensión del archivo. Se identifica un ejemplo como un archivo llamado "BusinessForecasts.docx" se convertirá en "BusinessForecasts.docx.cryjoker".

Según el autor del sitio web **(Kaspersky, 2019)**. Extorsionar a los usuarios con este tipo de ransomware no es un invento del siglo XXI. Los registros del ransomware original se remontan en el año 1989. El primer caso específico de ransomware se registró en Rusia en 2005. Desde ese año el ransomware se ha convertido en un fenómeno global, con cada nuevo tipo de ransomware, su creación sigue siendo efectiva. El número de ataques de ransomware aumentó exponencialmente en el año 2011. En respuesta a este aumento, especialmente del el 2016, los desarrolladores de software de antivirus han prestado especial atención en el ransomware.

Según el autor del sitio web **(Fortia, 2021)**. Existen muchas prevenciones sobre estos ataques de ransomware.

- **Datos cifrados en el punto final.**

Es importante conocer que significa un ataque de denegación de servicio en un dispositivo, si hay suficientes máquinas afectadas y el tiempo de recuperación le cuesta demasiado dinero a la empresa afectada, se puede cancelar por el rescate. Por ejemplo si es un fabricante se puede perder millones de dólares debido al tiempo de inactividad.

- **Extorsión por exfiltración de datos.**

Hacer pública la información de una víctima puede dañar la reputación de una organización, especialmente si la víctima almacena datos de los clientes y otros datos privados. Si el primer vector no se puede controlar, el segundo vector es de 100% para prevención. Las organizaciones y las empresas necesitan una solución de prevención de pérdida de datos “DLP” de confianza cero para comenzar a construir barrear contra el fraude y los ataques dirigidos. Estos son muy

diferente de las soluciones DLP. Pero en este caso las DLP tradicional no protegen todos los datos de forma predeterminada, si no que intenta bloquearlos para que no abandonen el punto final.

Según el autor de la página web **(KeepCoding, 2022)**. Mediante un cuadro se mostrará las características principales de Ransomware.

Características principales de los ransomware	Ransomware en servicio tiene su propio modelo de negocio.
	Desarrolladores.
	Afiliados a los ciberdelincuentes.
	Botmasters “agentes que administran redes de ordenadores infectados”.
	Analistas.
	Negociadores.
	Lavado de activos por medio de criptomonedas.
	Coautores anónimos.

Tabla 5. Características principales de los ransomware

Creado por: Jeniffer Verdezoto

Según el autor de la página web **(Pathak, 2021)**. Para que las computadoras no se encuentren desprotegidas y que los diferentes ataques maliciosos tanto como malware y ransomware se debe conocer los softwares más eficiente en protección contra estos virus que afecta al desarrollo de las computadoras. Mediante un cuadro se mostrará los softwares más importantes.

Importantes softwares de seguridad	Avast One
	Avira
	Kaspersky Premium
	Bitdefender
	AVG Ultimate
	Malwarebytes Essential
	Norton 360

Tabla 6. Softwares más seguros

Creado por: Jeniffer Verdezoto

Se mostrará un cuadro sistemático sobre los softwares de seguridad que se debe tener hacia los ataques maliciosos de malware y ransomware.

Características	**Software A**	**Software B**	**Software C**	**Software D**
Tipos de protección	Malware Ransomware	Malware Ransomware	Malware Ransomware	Malware Ransomware
Detección en tiempo real	Sí	Sí	Sí	Sí
Análisis Heurístico	Sí	Sí	Sí	Sí
Protección contra ransomware	Sí	Sí	Sí	Sí
Limpieza y eliminación	Sí	Sí	Sí	Sí
Actualizaciones frecuentes	Diarias	Semanales	Quincenales	Mensuales
Impacto en el rendimiento	Bajo	Moderado	Bajo	Muy bajo
Soporte técnico	24/7 chat	Email	Teléfono	Email/Chat
Otras Funcionalidades	Firewall Navegación Segura	VPN Firewall	Protección de correo Control parental	VPN Protección de identidad

Precio Anual en dólares	$40	$60	$50	$70

Tabla 7. Cuadro sistemático comparativo de los softwares.

Creado por: Jeniffer Verdezoto

Según el autor del sitio web **(Thalesgroup, 2019)**. La seguridad del software es un mecanismo de protección para diseñar la seguridad, ayudarlo a seguir siendo funcional dentro de la computadora, permitiendo resistir a los diferentes ataques que sean realizados mediantes los virus. El software se rige a varias pruebas de seguridad para comprobar la capacidad de resistir a los ataques maliciosos antes del gran lanzamiento en el mercado. Los ataques malware pueden ser muy dañinos para cualquier software, comprometiendo la integridad, autenticación y disponibilidad. Es importante conocer que si el programador tiene en cuenta estos conocimientos durante la fase de programación, en lugar de después, se podrá detener los daños antes de que comience.

Según el autor del sitio web (Unila, 2022). Se indicará un listado importante de cómo prevenir algunas amenazas dentro de los computadores.

- Se necesita crear contraseñas largas, en la cual se debe incluir símbolos, caracteres y números.
- Comprobar que el sistema operativo y las demás herramientas se encuentren con todas las técnicas de protección.
- Actualice el sistema operativo de la computadora y el software antivirus.
- Es recomendable no visitar hipervínculos o archivos de adjuntos que desconozca, ya que los hackers mediante sus virus capturan mediante estos links la información confidencial que existen dentro del computador.

CONCLUSIONES

Cuando se trata de seguridad, prevenir y mitigar la amenaza de malware y ransomware, protegerse contra el malware requiere implementar fuertes medidas de seguridad, como un software de antivirus, uso de firewalls y actualizaciones periódicas de software. También es considerado que los usuarios tengan conocimiento sobre la importancia de ciberseguridad y la identificación de amenazas potenciales. Es muy adecuado realizar copias de seguridad periódicas de los datos críticos y mantener una estrategia sólida de recuperación de datos. El ransomware se ha convertido en una de las amenazas más lucrativas para los ciberdelincuentes y pagar el rescate no garantiza la recuperación de datos, en la cual siempre el usuario o empresa debe estar preparado para posibles pérdidas de información o datos.

El malware como el ransomware representa una grave amenaza para la ciberseguridad moderna. Elegir una u otra como "segura" no es fácil, ya que ambas amenazas requieren enfoques de seguridad diferentes. La mejor estrategia es adoptar un enfoque holístico de la ciberseguridad que aborde todas las amenazas potenciales y cuente con medidas adecuadas de prevención, detección y respuesta. La capacitación y la concientización de los usuarios les ayudaran para saber cómo protegerse contra estos riesgos, y la colaboración entre las organizaciones y la comunidad en seguridad es fundamental para estar un paso delante de los ciberdelincuentes en constantes evolución.

La ciberseguridad es una responsabilidad compartida que debe tomarse en serio en todos los niveles, desde usuarios individuales hasta organizaciones y gobiernos. Mediante esta investigación se inclina que ambas son ataques directos para las computadoras unas más complejas que otra, lo recomendable para estos casos es instalar un excelente antivirus que ayude al computador a mantener guardados confidencialmente toda la información existente dentro de sí.

BIBLIOGRAFÍAS

Chavez, J. (3 de julio de 2019). *Malware*. Obtenido de Malware: https://www.ceupe.com/blog/malware.html

Daniela. (13 de abril de 2019). *Historia del Ransomware*. Obtenido de Historia del Ransomware: https://www.interbel.es/historia-ransomware/

Fortia. (21 de septiembre de 2021). *Características y Prevención de los Ataques Ransomware.* . Obtenido de Fortia - Fortia RRHH Software.: https://fortia.com.mx/ciberseguridad/caracteristicas-y-prevencion-de-los-ataques-ransomware/

Garza. (25 de enero de 2022). *La historia del ransomware* . Obtenido de Quanti Solutions : https://quanti.com.mx/articulos/la-historia-del-ransomware-historia-tipos-de-ransomware-y-futuros-impactos/

Kaspersky. (19 de abril de 2019). *El ransomware: qué es, cómo se lo evita, cómo se elimina.* . Obtenido de latam.kaspersky.com.: https://latam.kaspersky.com/resource-center/threats/ransomware

KeepCoding. (22 de agosto de 2022). *Características de los ransomwares actuales.* Obtenido de KEEPCODING TECH SCHOOL : https://keepcoding.io/blog/caracteristicas-de-los-ransomwares/

Panduru. (23 de febrero de 2022). *ATTACK SIMULATOR*. Obtenido de EJEMPLOS DE MALWARE: https://attacksimulator.es/blog/10-ejemplos-de-malware-los-mas-famosos-y-devastadores-casos-de-la-historia/

Pathak, A. (29 de septiembre de 2021). *Software de seguridad premium todo en uno de confianza para uso personal.* Obtenido de Geekflare: https://geekflare.com/es/premium-security-software/

Peralta, S. E. (15 de mayo de 2019). *Oferta de programa formatico sobre Gestión de Ciberseguridad* . Obtenido de Oferta de programa formatico sobre Gestión de Ciberseguridad : https://educacioncontinua.ucuenca.edu.ec/ucuenca-dec-oferta-programa-formativo-sobre-gestion-de-ciberseguridad/

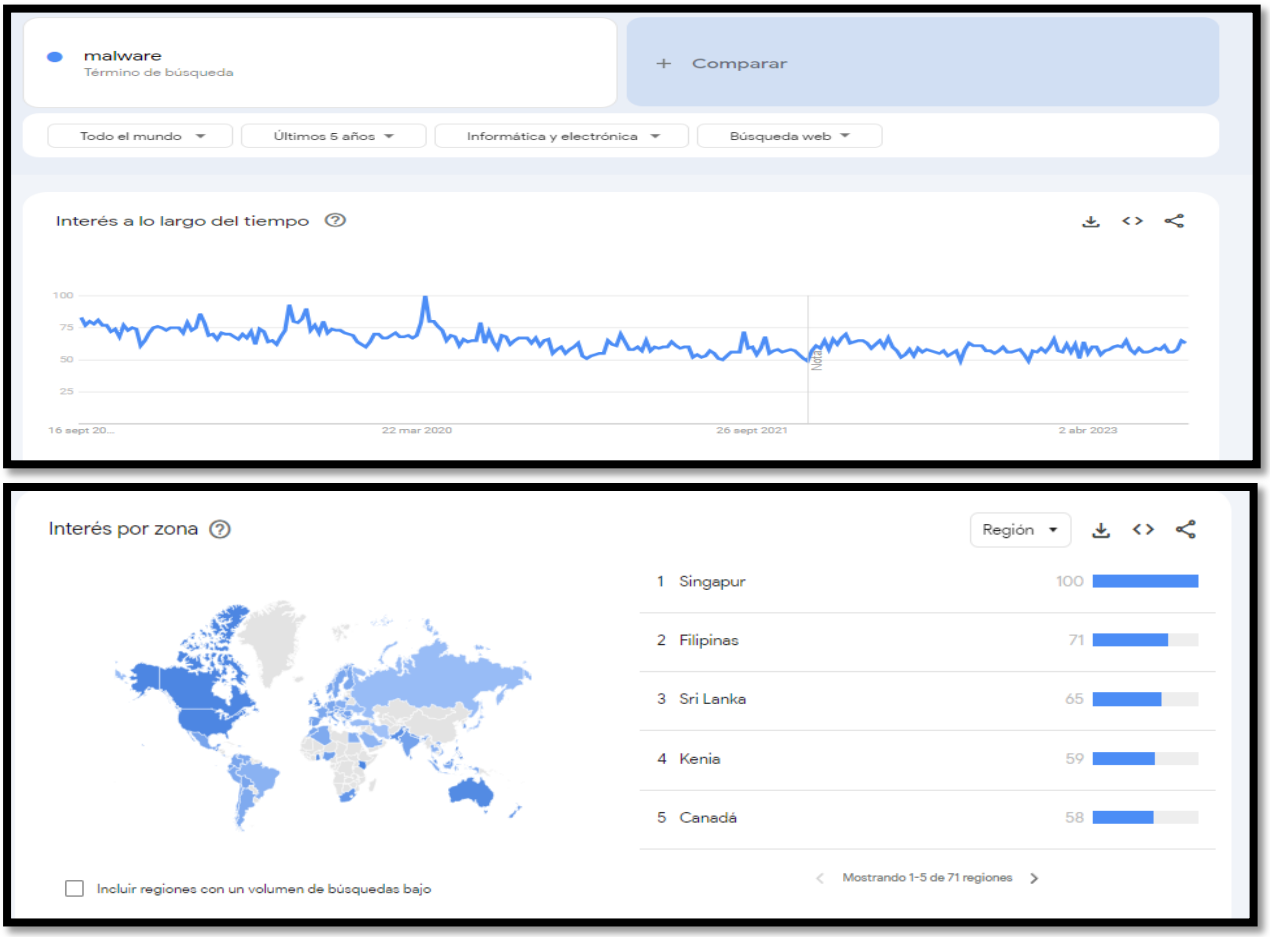
Ransomware. (5 de junio de 2019). *Ataques Ransomware*. Obtenido de Oficina de Seguridad del Internauta: https://www.incibe.es/ciudadania/ayuda/ransomware

Regan. (14 de febrero de 2022). *Guia definitiva de Malware*. Obtenido de Guia definitiva de Malware: https://www.avg.com/es/signal/what-is-malware

security, I. (25 de Septiembre de 2018). *Ciberseguridad* . Obtenido de Ciberseguridad: https://www.infosecuritymexico.com/es/ciberseguridad.html

Thalesgroup. (27 de mayo de 2019). *Seguridad del Software*. Obtenido de Seguridad del software : https://cpl.thalesgroup.com/es/software-monetization/what-is-software-security

Torrenegra, E. (20 de Septiembre de 2019). *Los virus informáticos* . Obtenido de Los virus informáticos : https://losviruseninformatica83w23.blogspot.com/2015/11/ventajas-y-desventajas-de-los-virus.html



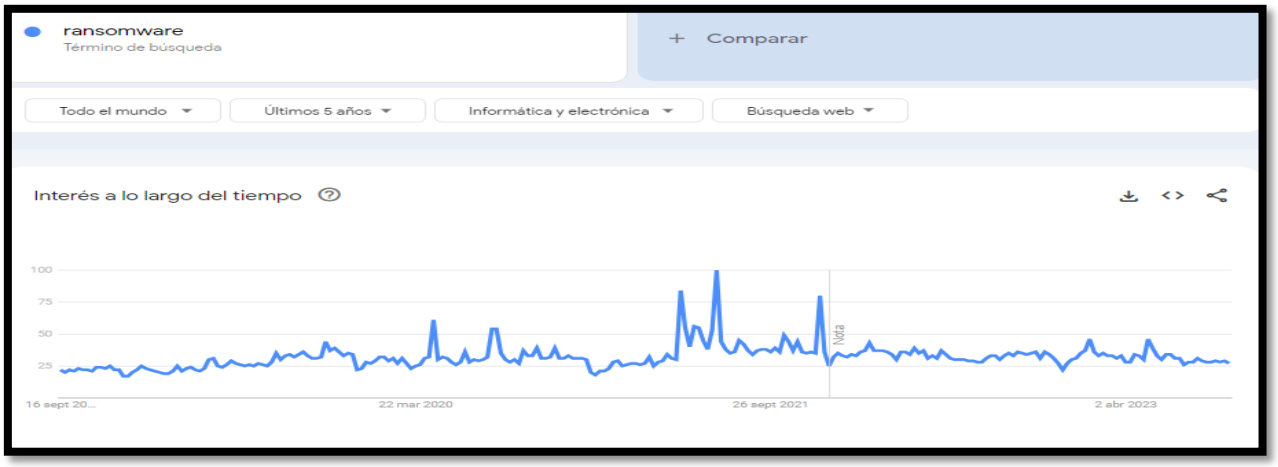
Unila. (16 de marzo de 2022). *Importancia de la seguridad informática*. Obtenido de Importancia de la seguridad informática: https://www.unila.edu.mx/por-que-es-importante-seguridad-informatica/

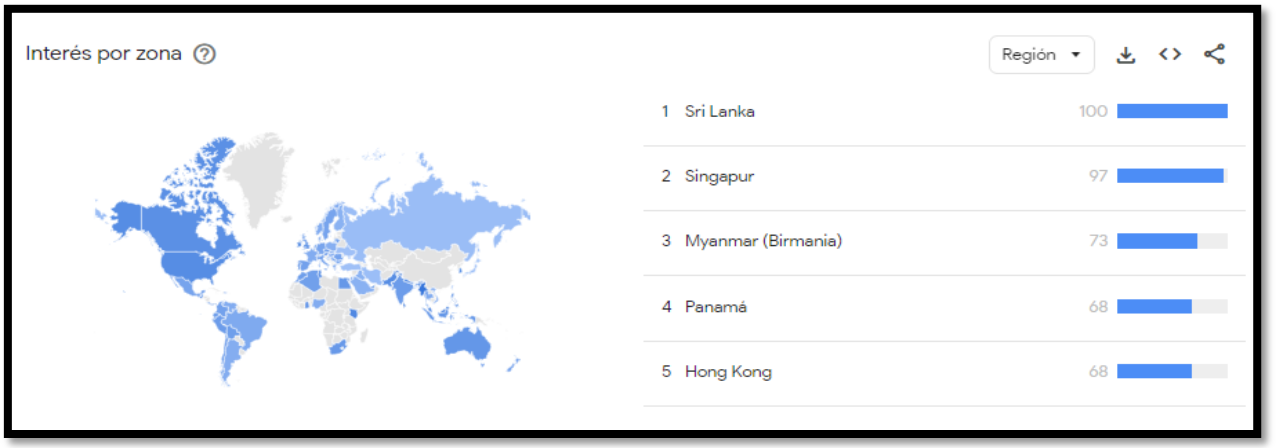
ANEXOS

Anexo 1

Fuente: Google Trends

Análisis: En la siguiente imagen se puede observar que el virus malware en los últimos 5 años se mantuvo atacando a los diferentes ordenadores de los países tanto de Singapur y Filipinas, postulándolo en los primeros puestos, logrando capturar información confidencial.

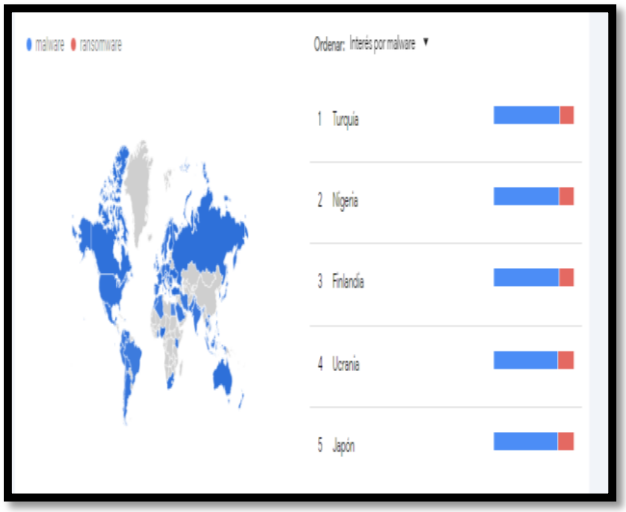


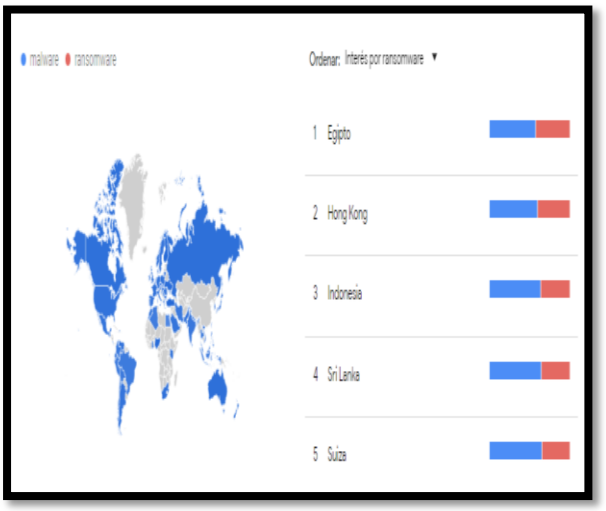


Fuente: Google Trends

Análisis: Se observa en la imagen que durante los últimos 5 años este virus denominado ransomware en el año 2021, obtuvo una cifra alta, permitiendo mostrarse en algunos países un ataque masivo por parte de este virus en mención.


malware
Término de búsqueda
ransomware
Término de búsqueda
Añadir comparación
Todo el mundo
Últimos 5 años
Informática y electrónica
Búsqueda web
Interés a lo largo del tiempo
100
75
50
25
Media
16 sept 20...
7 jun 2020
27 feb 2022
Nota


malware
ransomware
Ordenar: Interés por malware
1 Turquía
2 Nigeria
3 Finlandia
4 Ucrania
5 Japón


malware
ransomware
Ordenar: Interés por ransomware
1 Egipto
2 Hong Kong
3 Indonesia
4 Sri Lanka
5 Suiza

Fuente: Google Trends

Análisis: En la siguiente gráfica se observa que el virus Malware durante los últimos 5 años ha tenido despuntes significativos, llegando a la conclusión que este virus es uno de los más utilizados para capturar o filtrar información importante existentes de las computadoras.

Anexo 2

CERTIFICADO DE ANÁLISIS
magister

ANÁLISIS COMPARATIVO DE CIBERSEGURIDAD ENTRE MALWARE Y RANSOMWARE PARA CONOCER EL SOFTWARE MAS SEGURO ANTES LOS VIRUS FRECUENTES QUE EXISTEN DENTRO DE LAS COMPUTADORAS.

4% Similitudes
2% Texto entre comillas
< 1% similitudes entre comillas
1% Idioma no reconocido

Nombre del documento: CASO DE ESTUDIO VERDEZOTO.docx
ID del documento: 4784059604ef6479915fc831c0426811324ead31
Tamaño del documento original: 217,16 kB
Autor: Jenyffer Katiuska Verdezoto Loor

Depositante: Jenyffer Katiuska Verdezoto Loor
Fecha de depósito: 18/9/2023
Tipo de carga: url_submission
fecha de fin de análisis: 19/9/2023

Número de palabras: 4074
Número de caracteres: 26.593

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	attacksimulator.es | 10 ejemplos de malware: Los más famosos y devastadores ca... https://attacksimulator.es/blog/10-ejemplos-de-malware-los-mas-famosos-y-devastadores-casos-d...	1%		Palabras idénticas: 1% (54 palabras)
2	fortia.com.mx | ▷ Ransomware: Características y Prevención- Fortia https://fortia.com.mx/ciberseguridad/caracteristicas-y-prevencion-de-los-ataques-ransomware/	< 1%		Palabras idénticas: < 1% (36 palabras)
3	www.bbvaopenmind.com | La historia de los virus informáticos https://www.bbvaopenmind.com/tecnologia/mundo-digital/la-historia-de-los-virus-informaticos/	< 1%		Palabras idénticas: < 1% (27 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.infosecuritymexico.com | Ciberseguridad https://www.infosecuritymexico.com/es/ciberseguridad.html	< 1%		Palabras idénticas: < 1% (11 palabras)
2	www.doi.org https://www.doi.org/10.1109/CIMPS52057.2020.9390114	< 1%		Palabras idénticas: < 1% (10 palabras)
3	www.avg.com | ¿Qué es el malware? | Cómo funciona y qué hace | AVG https://www.avg.com/es/signal/what-is-malware	< 1%		Palabras idénticas: < 1% (10 palabras)