UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE INFORMÁTICA

TRABAJO DE TITULACIÓN

Propuesta tecnológica, previo a la obtención del título de:

INGENIERA EN SISTEMAS

"LABORATORIO VIRTUAL DE ANÁLISIS Y COMPORTAMIENTO DE MALWARE BASADO EN TÉCNICAS Y MÉTODOS DE SEGURIDAD INFORMÁTICA PARA LOS LABORATORIOS EN LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES"

AUTOR

LITUMA BRIONES LINDA CAROLINA

PROFESOR TUTOR

ING. IVÁN ALBERTO CORONEL SUÁREZ, MSIA.

LA LIBERTAD – ECUADOR

2020

DEDICATORIA

Dedico este esfuerzo y dedicación a mi padre Dios, a mis abuelitos Vicente Briones y Vicenta Velíz por creer siempre en mí y amarme como una hija.

Deseo también dedicar este trabajo a mi esposo Kléber Loor por ser parte de este triunfo.

Carolina Lituma

AGRADECIMIENTO

Es indispensable e importante para mi agradecer primero a Dios, mi padre amado, por darme las fuerzas para seguir en esta lucha de alcanzar mi meta y escuchar siempre mis plegarias, por cada una de sus bendiciones y amor infinito.

Agradezco a mi mamá, a mis abuelitos y hermanas por creer en mí y apoyarme. Gracias por los valores fomentados y darme el aliento necesario para seguir adelante. Así mismo, agradezco a mi esposo Kléber por compartir sus conocimientos y ayudarme a crecer profesionalmente, por su paciencia en esta etapa final y apoyo incondicional.

"El ser agradecido te abre puertas", eso me enseñó la vida. Por eso es tan significativo para mi agradecer a cada uno de mis docentes, quienes me formaron y compartieron sus conocimientos. Gracias por la paciencia y dedicación en la formación de profesionales. Son un gran ejemplo para mí y siempre viviré agradecida con cada uno de ustedes: Ing. Iván Coronel, Ing. José Sanchéz, Ing. Daniel Quirumbay, Ing. Marcia Bayas, Ing. Teresa Guarda, Ing. Carlos Sanchéz, Ing. Jaime Orozco, Ing. Marcos Noroña.

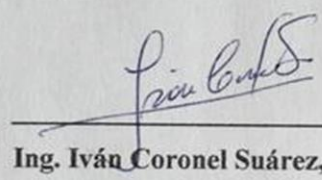
A mis amigos PhD. José María Días Nafría por la oportunidad de participar en su proyecto y su hermosa amistad, y a la Ing. Mercedes por su apoyo y guía.

Y para finalizar agradezco a mi tutor Ing. Iván Coronel por guiarme, y no ser sólo mi docente, tutor sino también un gran amigo. Gracias ing. por todo el aprendizaje, gracias porque siempre puedo contar con usted y gracias por haber aceptado ser mi tutor y papá.

Carolina Lituma Briones

APROBACIÓN DEL TUTOR

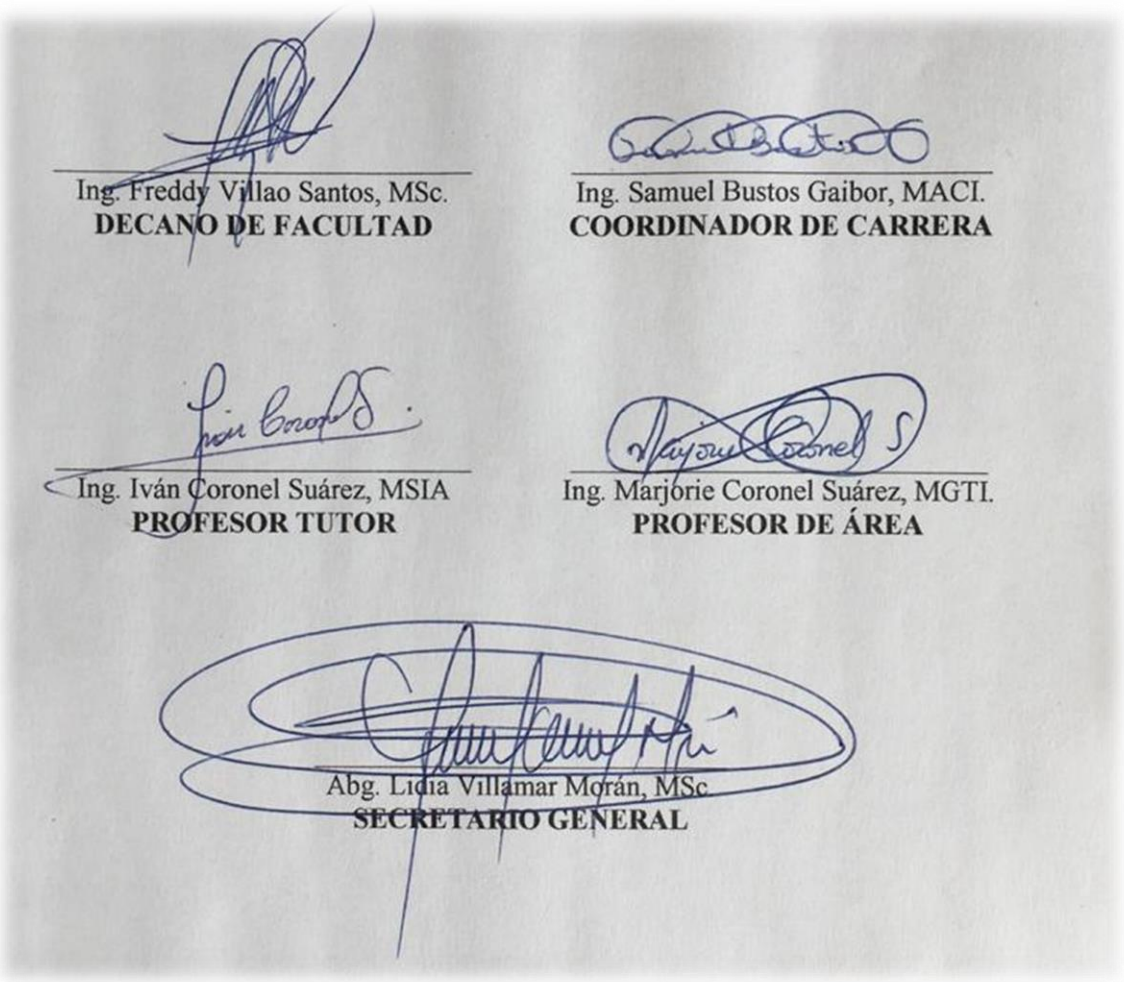
En mi calidad de Tutor del trabajo de titulación denominado: "Laboratorio virtual de análisis y comportamiento de malware basado en técnicas y métodos de seguridad informática para los laboratorios en la facultad de sistemas y telecomunicaciones", elaborado por el estudiante Lituma Briones Linda Carolina, de la carrera de Informática de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicie los trámites legales correspondientes.



Ing. Iván Coronel Suárez, MSIA

La Libertad, 11 de febrero del 2020

TRIBUNAL DE GRADO



RESUMEN

La presente propuesta tecnológica estableció como finalidad implementar un laboratorio virtual de análisis y comportamiento de malware para mejorar la seguridad y protección de datos de la red en los laboratorios de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL), debido a que en los mismos no existía un control en el tráfico de red que se generaba, lo que causaba una red inestable e insegura, provocando difusión de software malicioso (malware), infiltraciones de seguridad e incluso llegando a atentar contra la integridad de los datos que fluyen a través de las redes, anomalías que fueron motivos de análisis. Para lograr este objetivo, el laboratorio virtual se implementó en los servidores de FACSISTEL y se utilizaron herramientas de código abierto que coadyuvaron en las fases del análisis estático y dinámico, constituyéndose en una poderosa herramienta que permite realizar el estudio de las máquinas infectadas dentro de en un entorno controlado. Además, se consideró la metodología Open Information System Security Group (ISSAF), puesto que está basada en la planificación - preparación, evaluación y reportes, tres fases que permitieron examinar y emitir informes detallados de los aspectos sobre el comportamiento, datos generales y estructura del malware, los mismos que serán insumos válidos y confiables para la toma de decisiones en la creación de medidas de contención, mitigación y remediación de daños.

Palabras claves: Malware, análisis estático, análisis dinámico, tráfico de red, laboratorio virtual, análisis, reportes

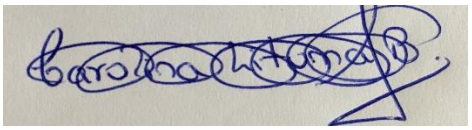
ABSTRACT

The present technological proposal established the aim of implementing a virtual laboratory for malware analysis and behavior in order to improve the security and protection of network data in the laboratories of the Faculty of Systems and Telecommunications (FACSISTEL) of UPSE, due to there was not any control in the network traffic that was generated in them, which caused an unstable and insecure network, producing the dissemination of malicious software (malware), security infiltrations and even attacking the integrity of the data flowing through the networks , anomalies that were the basic reasons for this analysis. To achieve this goal, the virtual laboratory was implemented in the FACSISTEL servers, and also open source tools were used which supported in the phases of static and dynamic analysis, the lab has become a powerful tool that allows the study of infected machines within a controlled environment. In addition, the Open Information System Security Group (ISSAF) methodology was considered, since it is based on planning - preparation, evaluation and reports, three phases that allowed examining and issuing detailed reports on aspects of behavior, general data and structure of the malware, which will be valid and reliable inputs for decision making in the creation of containment, mitigation and damage remediation measures.

Keywords: Malware, static analysis, dynamic analysis, network traffic, virtual laboratory, analysis, reports.

DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



LITUMA BRIONES LINDA CAROLINA

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

En la actualidad en este mundo globalizado donde la ciencia y tecnología avanzan vertiginosamente la seguridad en los sistemas de información se considera una prioridad tanto en las instituciones públicas como privadas. Cada día hay más información crítica y, aunque los sistemas presentan cada vez una mayor robustez, también su complejidad supone un reto a la hora de identificar vulnerabilidades en los sistemas. Teniendo en cuenta estos aspectos, es necesario contar con los medios necesarios para poder facilitar el estudio de malware y anticipar cuáles son los sistemas afectados por el mismo y bajo qué circunstancias [1].

En los últimos años se ha incrementado significativamente los ataques informáticos a nivel mundial. Los ataques más comunes son daños a sistemas informáticos, denegación de servicio, secuestro de información, robo de dinero, espionaje político e industrial y ataques a sistemas de infraestructuras críticas entre otros. Este incremento combinado con ataques a objetivos específicos ha ocasionado que los sistemas antivirus no puedan enfrentarlas. Una de las principales amenazas en la red es el malware ya que se ha convertido en uno de los programas maliciosos con una mayor tasa de propagación [2]. Motivo por el cual en la actualidad diversas empresas e instituciones han optado por crear un laboratorio para el control del tráfico de sus redes y verificar el comportamiento del malware.

El uso del internet en las instituciones superiores de educación está considerado como una herramienta fundamental para las actividades académicas y administrativas que se desarrollan diariamente. La correcta utilización del internet es una premisa básica por parte de los usuarios para el aprovechamiento óptimo del mismo. En la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) en los actuales momentos el servicio de internet se torna saturado sin conocerse cuales son las causas específicas de la ralentización de la conectividad, generando malestar en la facultad al no poder acceder de manera usual a los servicios ya que existe un número cada vez mayor de aplicaciones y de equipos terminales conectados a la misma. Por lo tanto, se generan problemas de vulnerabilidades de seguridad.

El presente trabajo de investigación fundamentado en la propuesta tecnológica se enfocó en implementar un laboratorio virtual de análisis y comportamiento de malware para perfeccionar la seguridad y protección de datos de la red en los laboratorios de la Facultad

de Sistemas y Telecomunicaciones (FACSISTEL), debido a la inexistencia de un control en el tráfico de red que se generaba, provocando que esta red estuviera expuesta y sea vulnerable a la difusión de software malicioso (malware), infiltraciones de seguridad e incluso llegando a atentar contra la integridad de los datos que fluyen a través de las redes, razones por las que el laboratorio virtual se implementó en los servidores de FACSISTEL utilizándose herramientas de código abierto que coadyuvaron en las fases del análisis estático y dinámico, constituyéndose en una herramienta esencial que permite efectuar estudios de las máquinas infectadas dentro de en un ambiente controlado.

Este documento de propuesta tecnológica esta segmentado en los siguientes capítulos:

Capítulo I: La fundamentación está constituida por el antecedente, descripción, objetivos, justificación y las metodologías empleadas en el proyecto de implementación del laboratorio virtual contextualizado en los laboratorios de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) donde se presencia constantemente una gran afluencia de dispositivos fijos y móviles pertenecientes a administrativos, docentes, estudiantes e invitados que acuden a la facultad diariamente, haciendo que el tráfico de datos en su arquitectura de red se eleve, ocasionando en varios momentos una conexión a internet lenta.

Capítulo II: La propuesta está estructurada del marco conceptual, marco teórico, que permitió profundizar en las definiciones con respecto a los laboratorios virtuales, malware, tipos de malware, y las herramientas de análisis estático y dinámico así como también estado del arte en campo científico actual de la temática planteada y la propuesta implementación y resultados obtenidos que permitieron examinar y emitir informes detallados de los aspectos sobre el comportamiento, datos generales y estructura del malware, los mismos que serán insumos válidos y confiables para la toma de decisiones en la creación de medidas de contención, mitigación y remediación de daños constituyéndose los mismos en los insumos fundamentales generados por este investigación realizada.

CAPÍTULO I
FUNDAMENTACIÓN

1.1. ANTECEDENTES

En los últimos años se ha incrementado significativamente los ataques informáticos a nivel mundial. Los ataques más comunes son daños a sistemas informáticos, denegación de servicio, secuestro de información, robo de dinero, espionaje político e industrial y ataques a sistemas de infraestructuras críticas entre otros [1]. Este incremento combinado con ataques a objetivos específicos ha ocasionado que los sistemas antivirus no puedan enfrentarlas.

Una de las principales amenazas en la red es el malware ya que se ha convertido en uno de los programas maliciosos con una mayor tasa de propagación. Motivo por el cual en la actualidad diversas empresas e instituciones han optado por crear un laboratorio para el control del tráfico de sus redes y verificar el comportamiento del malware [2].

El Security Report Latinoamérica (ESET), indica que la infección por códigos maliciosos es la primera causa de incidentes de seguridad en Latinoamérica. Según el estudio que realizó ESET en el 2017, por medio de encuestas a administradores de sistemas y ejecutivos de varias empresas, los incidentes sufridos en pequeñas, medianas y grandes empresas de Latinoamérica son causados por ciberdelincuentes [3].

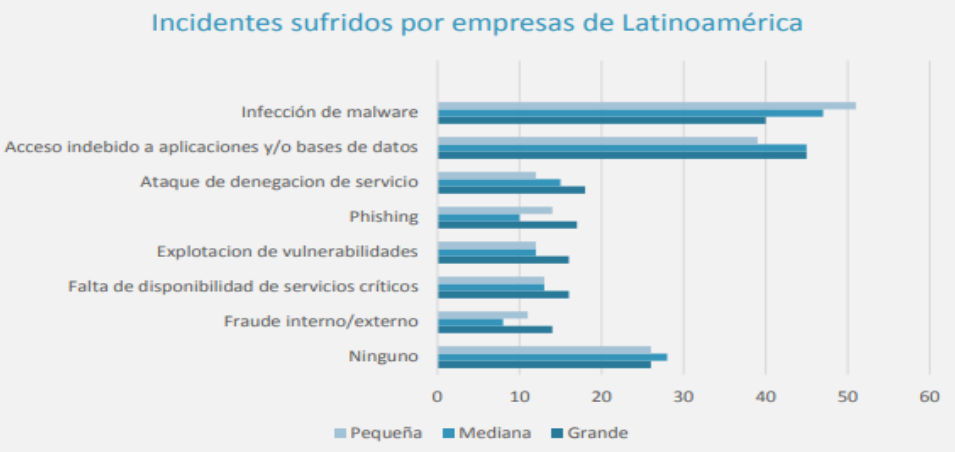


Figura 1: Porcentaje de incidentes de seguridad padecidos por empresas latinoamericanas

La Facultad de Sistemas y Telecomunicaciones (FACSISTEL) fue creada en el año 2010 y tiene cinco carreras vigentes. Actualmente dispone de cuatro laboratorios,

en el cual el servicio de internet se torna saturado sin conocerse cuales son las causas específicas de la ralentización de la conectividad generando malestar en la Facultad al no poder acceder de manera usual a los servicios ya que existe un número cada vez mayor de aplicaciones y de equipos terminales conectados a la misma. Por lo tanto, se generan problemas de vulnerabilidades de seguridad (Ver anexo 1).

En estos problemas interfieren factores tanto desde el punto de vista de los usuarios como los peligros derivados del entorno o errores humanos que alteren las redes de comunicaciones. Además, el desconocimiento acerca de la información del tráfico que atraviesa la red, de los enlaces que se encuentran saturando el ancho de banda o de cuáles son los servicios que están haciendo que la carga de los servidores sea elevada, hace imposible tener una red de telecomunicaciones óptima, haciendo que en cualquier momento los servidores o dispositivos pueden dejar de funcionar y detener servicios de vital importancia para la comunicación de la Facultad.

Kaspersky Lab es una empresa fundada por Yevgeny Kaspersky, dedicada a la creación de productos software para la seguridad informática [4]. Actualmente esta empresa tiene uno de los laboratorios físicos de análisis de malware más reconocidos mundialmente por sus investigaciones a algunos de los ciberataques más complejos y sofisticados jamás conocidos [4].

Según el recorrido virtual que ofrece la empresa en su sitio web, el laboratorio está constituido por analistas de virus denominados “pájaros carpinteros”, los cuales tienen asignado sus propios equipos, destacándose tres monitores para cada investigador, dos para analizar los virus del exterior y uno para ejecutar y estudiar los virus en directo [5].

El laboratorio físico de Kaspersky realiza análisis para clasificar y verificar el comportamiento de los diversos softwares maliciosos encontrados y así poder crear antivirus para la detección y eliminación de los mismos con plataformas de protección integrada [6].

Por los motivos expuestos y tomando como referencia la experiencia de los laboratorios de Kaspersky, la presente propuesta tecnológica está enfocada en la creación de un laboratorio virtual de análisis y comportamiento de malware que se utilizará para hacer un examen dinámico y estático [7] y proporcionar un entorno

seguro en la Facultad de Sistemas y Telecomunicaciones. Un laboratorio de análisis de malware se puede considerar como un conjunto de puntos de entrada en una cadena de herramientas. Los principales puntos de entrada son los archivos, las URL, la captura de tráfico de red y la imagen de memoria [8].

Para encontrar amenazas dentro de la Facultad, es necesario tener un laboratorio de malware disponible a través del cual las muestras recolectadas se puedan ejecutar inmediatamente y poder proteger la red.

1.2. DESCRIPCIÓN DEL PROYECTO

En los laboratorios de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) se presencia constantemente una gran afluencia de dispositivos fijos y móviles pertenecientes a administrativos, docentes, estudiantes e invitados que acuden a la Facultad diariamente, haciendo que el tráfico de datos en su arquitectura de red se eleve, ocasionando en varios momentos una conexión a internet lenta.

El no control de dispositivos conectados y verificación del tráfico que fluye en la red hace incierta la calidad e integridad de la información debido a que no se puede identificar las intrusiones malintencionadas de ciertos usuarios. Es por esta razón que se desea implementar un laboratorio virtual que permita realizar estudios para el control del tráfico de red, poder analizar las posibles causas que hacen que la misma sea lenta e insegura, solucionar dichas vulnerabilidades y verificar el comportamiento de los malware encontrados en la misma.

El presente proyecto constará principalmente de las siguientes fases:

Fase de recolección de datos:

Este trabajo se realizará obteniendo información a través de entrevistas y encuestas a los entes que forman parte de la Facultad, visitas al departamento de TIC´s y primordialmente con pruebas directas en las redes (Ver Anexo 1 y 2).

Por medio del cuestionario se podrá evidenciar que los entes de la Facultad al conectarse a la red alámbrica de los laboratorios, han sido víctimas de infección de software malicioso, frecuentemente por internet, medios extraíbles de almacenamiento de datos o por mal uso de los usuarios (ingeniería social).

La experimentación para la recolección de datos, prueba y evaluación de la funcionalidad del laboratorio virtual se establecerá mediante un análisis de la red de los laboratorios de FACSISTEL.

Se realizará un levantamiento de información de los equipos informáticos de los laboratorios a través de un inventario para obtener las características técnicas, direcciones MAC, número de equipos, entre otros. (Ver Anexo 3)

Fase de virtualización:

En esta fase se crearán las máquinas virtuales con sus sistemas operativos y sus correspondientes configuraciones en las siguientes distribuciones en caso de ser necesario:

- Distribución Linux
- Distribución Windows
- Sistemas operativos de Análisis Forense
- Firewall Pfsense

La virtualización de estos sistemas operativos se realizará en el servidor de FACSISTEL, requiriendo alrededor de 10GB de memoria RAM para el correcto funcionamiento de las máquinas virtuales. Esto servirá para simular un ambiente real de los laboratorios de FACSISTEL y realizar las pruebas correspondientes.

Fase de análisis del tráfico de la red y control de los equipos:

Se monitoreará en tiempo real el tráfico de la red, realizando el registro de las máquinas que se encuentran en los laboratorios. Además, se implementarán firewalls de control para verificar el tráfico y consumo del ancho de banda de cada equipo registrado.

Fase del análisis del comportamiento de Malware

Se seleccionará los métodos de análisis de malware existentes que son: análisis estático y análisis dinámico con técnicas de preparación, detección, análisis y prevención.

El análisis estático se realizará cuando se encuentre una amenaza que no está siendo ejecutada y el dinámico se realizará en la ejecución del malware en tiempo real para verificar el comportamiento del mismo en ambas situaciones.

Una vez seleccionado el método y técnica a aplicar, se elegirán las herramientas correspondientes para realizar el escaneo y captura de malware en la red.
Con los resultados obtenidos se pretende efectuar un estudio del comportamiento de malware a través de los equipos existentes (hardware) y las herramientas informáticas (software).

Fase de reportes:
El laboratorio virtual emitirá reportes sobre el análisis dinámico y estático del malware.
El proyecto será ejecutado con equipos como: diversos monitores que permitirán ver el tráfico, servidores de la FACSISTEL en los cuales se virtualizará equipos con diferentes herramientas para la monitorización y escaneo de las redes. En la parte de software para capturar las diversas actividades se utilizará firewall de control, scripts, depuradores, entre otras herramientas de monitoreo y seguridad informática.
La muestra tomada de la captura del tráfico de la red se ejecutará dentro del laboratorio de manera semanal. Las aplicaciones de monitoreo almacenarán cualquier actividad iniciada por el malware u otro tipo de ataque de software malicioso. Una vez ejecutado el monitoreo su salida serán los registros los cuales serán escaneados brevemente y se creará un informe detallado para tomar las medidas de seguridad.
El presente proyecto está enfocado en buscar la integración de los actuales equipos, metodologías y herramientas de monitoreo de análisis de red y conducta de malware, que ofrecen una amplia gama de posibilidades para construir un conjunto de programas informáticos que ayuden a controlar el tráfico de la red e identificar los ataques.
Se establecerán medidas preventivas y proactivas que brinden protección a los entes que conforman la Facultad. Por ello, es necesaria una combinación de herramientas tecnológicas, buenas prácticas y gestión de la seguridad para llevar a cabo el proyecto.
Este proyecto contribuirá a la línea de investigación Tecnologías y Gestión de la Información, debido a que la propuesta está relacionada con temas de

infraestructura y seguridad de las tecnologías de la información, virtualización y seguridad de la información que permitan generar información indispensable para la toma de decisiones [9].

1.3. OBJETIVOS

1.3.1. Objetivo general

Implementar un laboratorio virtual de análisis y comportamiento de malware mediante la comparación de métodos y técnicas para mejorar la seguridad y protección de datos de la red en los laboratorios de la Facultad de Sistemas y Telecomunicaciones.

1.3.2. Objetivos específicos

- Determinar las herramientas de software para el análisis de la red y monitoreo del tráfico de acuerdo a los métodos y técnicas establecidas.
- Analizar la seguridad de la red alámbrica de los laboratorios de FACSISTEL.
- Evidenciar de manera documental los resultados obtenidos del análisis realizado en el laboratorio virtual.
- Establecer medidas de seguridad pertinentes a través de estándares internacionales para soslayar futuros incidentes.

1.4. JUSTIFICACIÓN

El uso del internet en las instituciones superiores de educación está considerado como una herramienta fundamental para las actividades académicas y administrativas que se desarrollan diariamente [10]. La correcta utilización del internet es una premisa básica por parte de los usuarios para el aprovechamiento óptimo del mismo [11].

En el 2018 ESET realizó una encuesta en donde los datos finales determinaron que con un 22% Ecuador es el país con mayor índice de infecciones de malware en Latinoamérica [12].

Figura 2: Infecciones de malware por país

En la actualidad en los laboratorios de (FACSISTEL) no existe un control en el tráfico que se genera, tampoco existen medidas de seguridad para los diversos dispositivos conectados a la infraestructura de red lo que causa una red inestable e insegura, provocando difusión de software malicioso (malware), infiltraciones de seguridad e incluso llegando a atentar contra la integridad de los datos que fluyen a través de las redes, anomalías que deberían ser motivo de análisis y comportamiento del tráfico de la red.

La creación del laboratorio virtual permitirá que futuras investigaciones puedan realizar un análisis en profundidad del tráfico de red y comportamiento de malware para obtener muestras de la misma y a través de estos datos realizar nuevos estudios.

El análisis del malware, permitirá mejorar la seguridad de la red alámbrica de los laboratorios de FACSISTEL, puesto que al tener un constante monitoreo hace que el campo de acción se amplíe debido a su constante evolución en los diferentes tipos de malware. Esto a su vez hará que se tenga un record de los softwares maliciosos encontrados.

El control de los equipos conectados permitirá tener una red de telecomunicaciones óptima, ya que se podrá verificar en tiempo real el ancho de banda que cada equipo

está utilizando. Asimismo, con las restricciones en la navegación web se evitará que los usuarios ingresen a páginas poco confiables.

En cuanto a los reportes que generará el laboratorio respecto al análisis realizado, este reporte se constituye en instrumentos que poseen información valida y relevante para tomar acciones y a la vez decisiones por parte de los gestores de los laboratorios de FACSISTEL.

El estudio realizado permitirá tomar las medidas correctivas, con respecto a este tipo de amenazas que permanentemente está incidiendo en el tráfico de la red.

La Facultad de Sistemas y Telecomunicaciones será beneficiario directo ya que con la implementación de este laboratorio virtual se podrá tener el control del tráfico y seguridad de la red, además de que los estudiantes podrán realizar sus prácticas pre profesionales en el monitoreo y análisis de este laboratorio.

El departamento de Tecnología de la Información y Comunicación de la UPSE será un beneficiario indirecto puesto que con los reportes estadísticos que emitirá el laboratorio virtual, dará cabida a nuevas investigaciones que permitirán crear un laboratorio físico controlado que realice análisis avanzados respecto a la seguridad de la red y sistemas y además genere soluciones en beneficio a toda la comunidad universitaria.

El presente proyecto está direccionado al plan toda una vida, haciendo énfasis en el eje 2, el cual detalla lo siguiente:

Eje 2: Economía al servicio de la sociedad [13].

Objetivo 5: Impulsar la productividad y competitividad para el crecimiento económico sostenible de manera redistributiva y solidaria [13].

Política 5.6: Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, la protección de la propiedad intelectual, para impulsar el cambio de la matriz productiva mediante la vinculación entre el sector público, productivo y las universidades [13].

1.5. ALCANCE DEL PROYECTO

La implementación del laboratorio virtual permitirá realizar el análisis del tráfico, control en los dispositivos conectados y datos que fluyen en la red alámbrica en los

laboratorios de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena.

En el laboratorio virtual también se podrá realizar el estudio de posibles amenazas existentes en la red local de los laboratorios para determinar mediante muestras de los tipos de software maliciosos existentes dentro de la misma. Además, se mostrarán las herramientas fehacientes para el análisis.

El presente proyecto abarcará las siguientes fases:

- Fase de recolección de datos
- Fase de virtualización
- Fase de análisis del tráfico de la red y control de los equipos
- Fase del análisis del comportamiento de Malware
- Fase de reportes

El estudio de la red permitirá visualizar cuales son las condiciones reales respecto a la seguridad informática, cabe indicar que este análisis en profundidad no está direccionado a crear softwares o sistemas antivirus para combatir malware, el trabajo fundamental del laboratorio virtual es realizar el análisis del comportamiento de malware y a través de esta investigación generar reportes e informes detallados, lo que permitirá diseñar medidas de seguridad, planes de contingencia y mitigación respectivamente.

Es importante resaltar que la implementación del laboratorio virtual no asegura mejorar la velocidad del internet ni el aumento de ancho de banda, sino demostrar la presencia de software maliciosos en la red.

1.6. METODOLOGÍA

1.6.1. Metodología de investigación

Los estudios exploratorios se efectúan cuando no se han realizado investigaciones previas o existe poca información acerca del objeto de estudio [14]. La presente propuesta tecnológica no ha sido implementada en la Universidad Estatal Península de Santa Elena ya que a pesar de que existe un departamento de TIC’s no se ha creado un laboratorio para el análisis de software maliciosos. Por lo tanto, se aplicará dicha investigación para indagar respecto al tema con un amplio espectro

de medios para la recolección de información como bibliografía especializada, entrevistas y cuestionarios hacia los entes que forman parte del entorno a analizar y la observación de los procesos actuales.

La investigación diagnostica se realizará a través de encuestas a los estudiantes de la Facultad, para tener un amplio conocimiento acerca de la satisfacción y seguridad del internet alámbrico. Además, a través de los inventarios, permitirá conocer la situación actual de la infraestructura y seguridad de la red y del estado de los equipos informáticos en los laboratorios. Con esta información se podrá identificar las necesidades y mejoras a emplear en el proyecto.

Esta investigación analizará alrededor del 80% de la red para evidenciar los tipos de malware que fluyen en la misma y el comportamiento de cada uno de ellos.

1.6.2. Metodología Marco de Evaluación de Seguridad del Sistema de Información (ISSAF)

Para el presente proyecto se establecerá como base la metodología ISSAF de OISSG (Open Information System Security Group), puesto que está basada en la evaluación y análisis de seguridad de redes y aplicativos, además de dar un informe detallado de los posibles aspectos que hacen insegura la infraestructura [15].

Basado en los lineamientos de la metodología, el proyecto se enfocará en tres fases descritas a continuación:

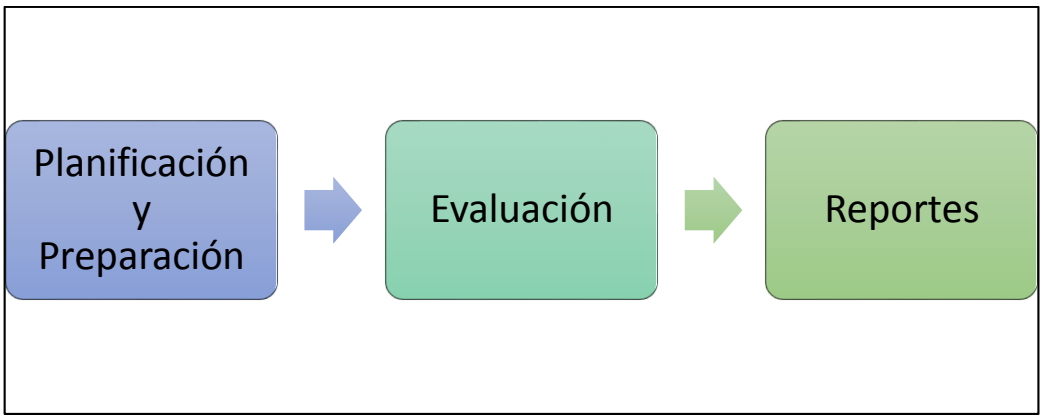


Figura 3: Fases de la metodología ISSAF

- **Planificación y preparación:** en esta fase se llevará a cabo la elaboración del cronograma del proyecto y la disposición de las diferentes herramientas y ambientes a utilizar [16].

- **Evaluación:** se realizará el test en la red cada semana para analizar el comportamiento de la misma, en donde se efectuará la recolección de información en cuanto a modificaciones y conexiones no autorizadas [16].
- **Reportes:** a través de las plantillas de esta metodología se emitirán reportes del análisis que se realizó en la red y sistemas para detallar cada uno de los softwares maliciosos encontrados en la misma [16].

1.6.3. Técnicas de investigación

A continuación, se detallan las técnicas e instrumentos de recolección de datos que serán empleados en este proyecto.

- **Técnica:**

Estado del arte, encuestas, entrevistas, inventarios y fuentes bibliográficas

- **Instrumento:**

Los cuestionarios cerrados serán dirigidos a estudiantes, docentes y administrativos de la Facultad de Sistemas y Telecomunicaciones con el objetivo de conocer el uso y satisfacción del internet a nivel general en los laboratorios. Además, se realizará una entrevista dirigida al personal del departamento de TIC's para tener información específica de la infraestructura y seguridad de la red.

Se realizará un inventario de los equipos informáticos de los laboratorios para obtener información relevante como la MAC, IP, cantidad de dispositivos, estado, etc.

Las fuentes bibliográficas permitirán realizar un análisis de la literatura especializada concerniente a la problemática investigada.

- **Población**

La población objeto de estudio la conforman los entes de FACSISTEL y el departamento de TIC's.

1.6.4. Análisis de resultados de la encuesta

La encuesta realizada fue dirigida a los usuarios de los laboratorios de FACSISTEL, de las carreras de Informática y Tecnología de la Información.

PREGUNTA 1: ¿Con qué frecuencia utiliza el servicio de internet por red en la Facultad?

Respuesta	Frecuencia	Porcentaje
Diariamente	158	98,75%
Varios días en la semana	2	1,25%
Casi Nunca	0	0%
TOTAL	**160**	**100%**

Tabla 1: Uso del internet en FACSISTEL

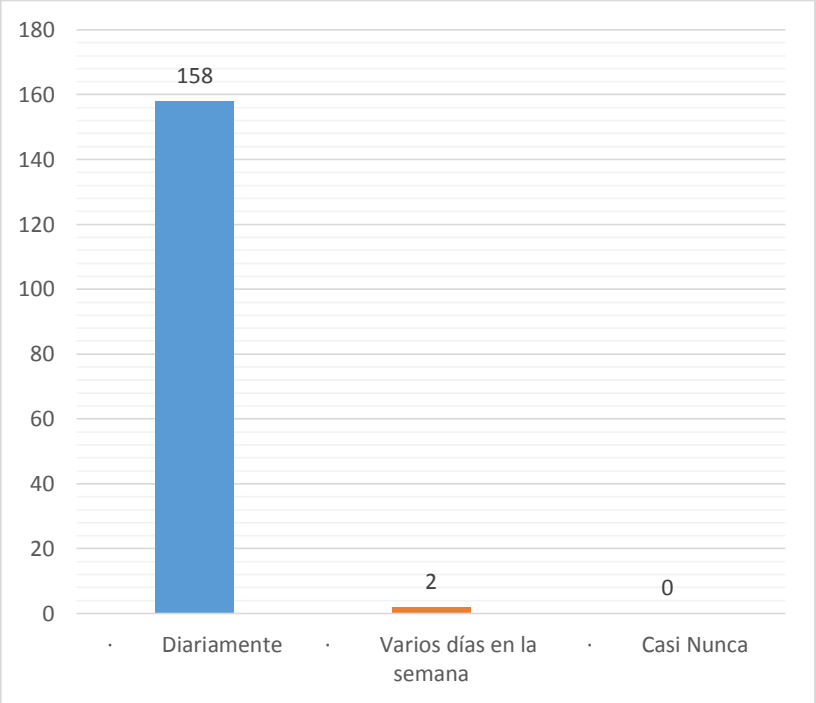


Figura 4: Uso del internet en FACSISTEL

INTERPRETACIÓN: La frecuencia con la que los usuarios utilizan el servicio de internet en un 98,75% es diario.

CONCLUSIÓN: Los resultados obtenidos nos demuestran que el uso del internet en FACSISTEL es de gran medida por los usuarios.

PREGUNTA 2: ¿En qué rango de horario considera usted que el internet se torna lento?

Respuesta	Frecuencia	Porcentaje
07:30 – 08:30	3	1,875 %
09:00 – 10:00	147	91,87 %
12:00 – 13:00	8	5 %
15:00 – 16:00	0	0 %
17:00 – 18:00	2	1,25 %
TOTAL	**160**	**100%**

Tabla 2: Rangos de horarios en que el internet se torna lento

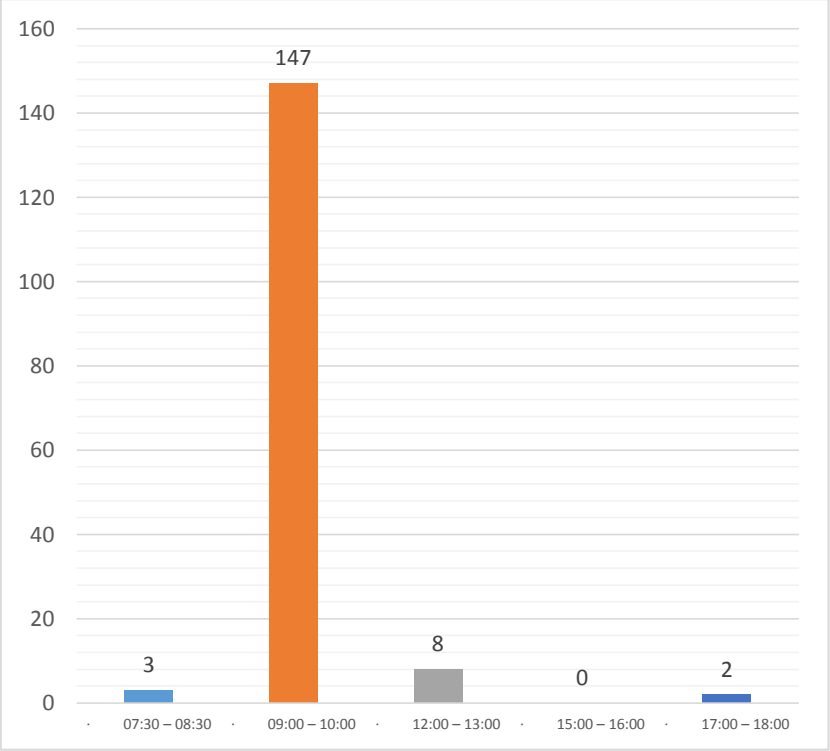


Figura 5: Rangos de horarios en que el internet se torna lento

INTERPRETACIÓN: El 91,87% de los encuestados manifiestan que el internet se torna lento en la mañana, específicamente en el rango de 09:00 a 10:00 am.

CONCLUSIÓN: El internet en la red de FACSISTEL se torna lento en horarios de la mañana sin conocerse cuales son las causas de este suceso.

PREGUNTA 3: Seleccione cuál es el laboratorio que usted más utiliza

Respuesta	Frecuencia	Porcentaje
Laboratorios de informática	103	64,37 %
Laboratorio de redes	0	0 %
Laboratorio de CISCO	57	35,62 %
TOTAL	**160**	**100%**

Tabla 3: Laboratorios de FACSISTEL más usados por los usuarios

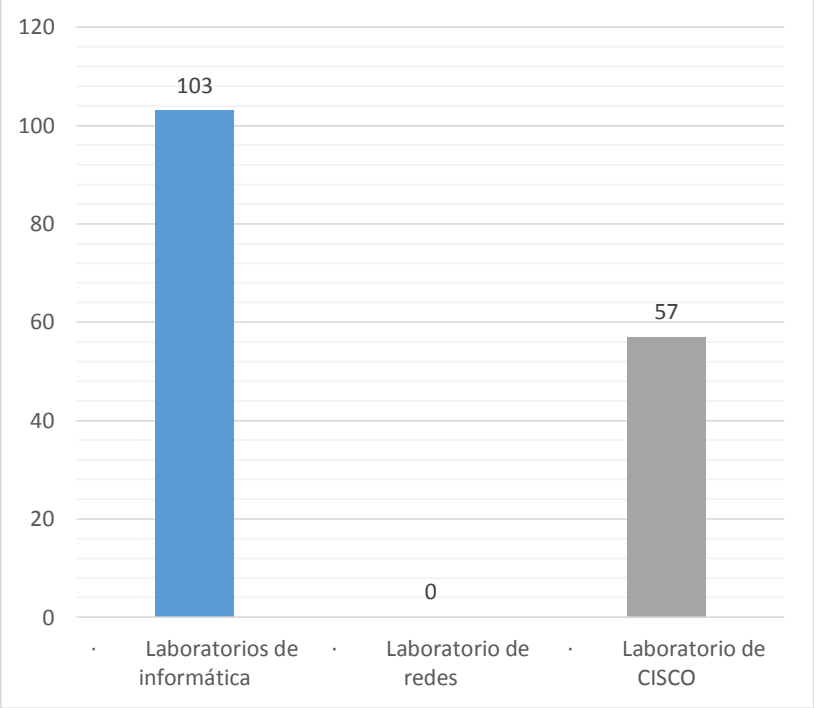


Figura 6: Laboratorios de FACSISTEL más usados por los usuarios

INTERPRETACIÓN: El 64,37% de los encuestados utilizan los laboratorios de Informática y el 35,62% utiliza los laboratorios de CISCO.

CONCLUSIÓN: Los laboratorios con que más frecuencia utilizan los usuarios encuestados son los laboratorios de informática, sin embargo, los laboratorios de CISCO también son concurridos en gran cantidad por los encuestados.

PREGUNTA 4: ¿El servicio de internet alámbrico de los laboratorios se adapta a sus necesidades como usuario?

Respuesta	Frecuencia	Porcentaje
Si	86	53,75 %
No	74	46,25 %
TOTAL	**160**	**100%**

Tabla 4: Serivicio de internet alámbrico

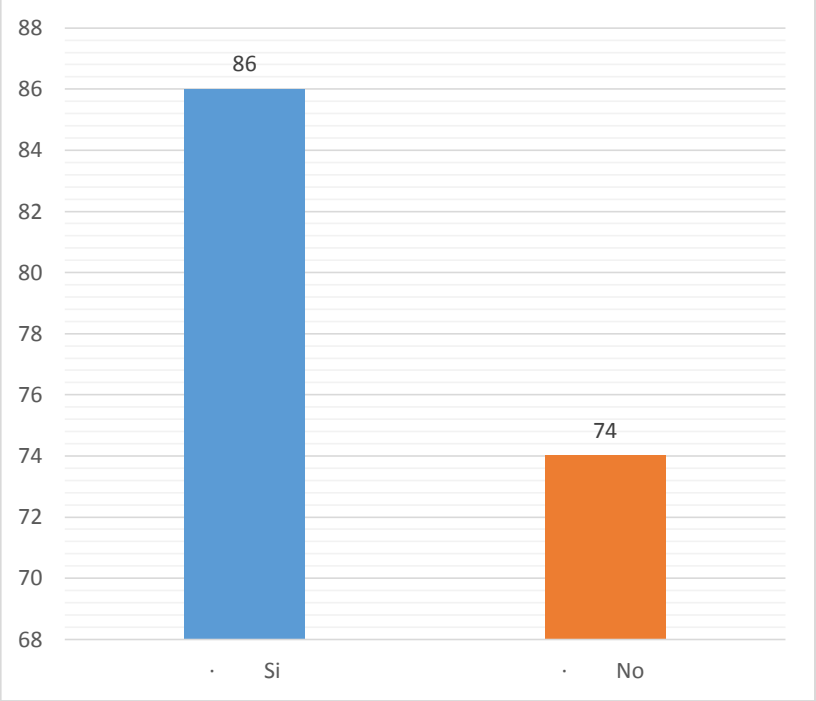


Figura 7: Servicio de internet alámbrico

INTERPRETACIÓN: El 53,75% de los encuestados sienten que el internet alámbrico de los laboratorios de FACSISTEL cubren sus necesidades de navegación, pero el 46,25% no se siente satisfecho con el servicio de internet alámbrico.

CONCLUSIÓN: En esta pregunta se puede verificar que el porcentaje de usuarios satisfechos e insatisfechos con el internet alámbrico de los laboratorios es controversial, porque solo existe 7,5% de diferencia entre las dos respuestas.

PREGUNTA 5: ¿Siente que las redes cableadas de los laboratorios poseen las seguridades informáticas necesarias? ¿Por qué?

Respuesta	Frecuencia	Porcentaje
Si	44	27,5 %
No	116	72,5 %
TOTAL	**160**	**100%**

Tabla 5: Seguridad informática de la red cableada

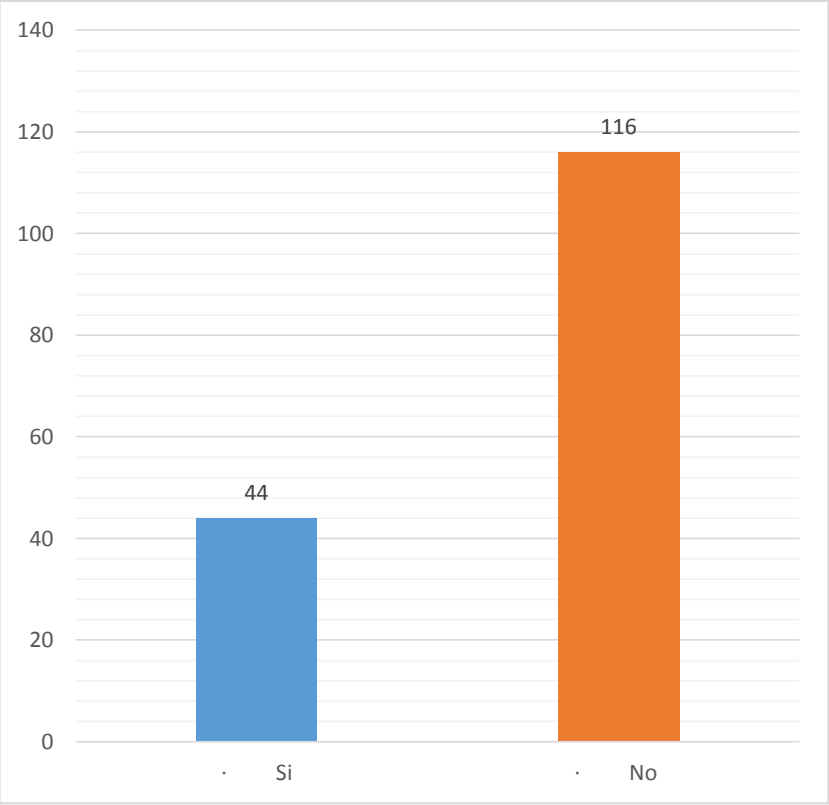


Figura 8: Seguridad informática de la red cableada

INTERPRETACIÓN: Existe un 72% de usuarios que no están de acuerdo que las redes cableadas de los laboratorios cuentan con la seguridad informática correspondiente.

CONCLUSIÓN: Los usuarios de la red cableada de los laboratorios de FACSISTEL no se sienten seguros al conectar sus dispositivos o al utilizar las máquinas de los laboratorios.

PREGUNTA 6: ¿Considera usted que existen virus dentro de la red de los laboratorios?

Respuesta	Frecuencia	Porcentaje
Si	160	100 %
No	0	0 %
TOTAL	**160**	**100%**

Tabla 6: Existencia de virus en la red

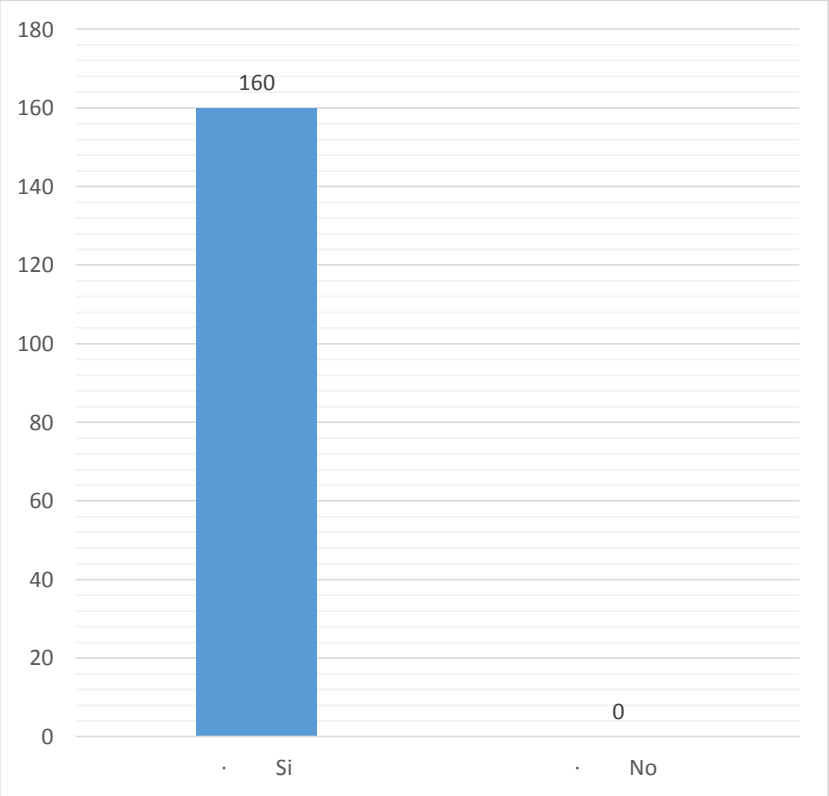


Figura 9: Existencia de virus en la red

INTERPRETACIÓN: El 100% de los usuarios encuestados manifiestan que la red de los laboratorios se encuentra con algún tipo de virus.

CONCLUSIÓN: Los usuarios en su totalidad admiten que la red de la Facultad se encuentra infectada de virus o malware.

PREGUNTA 7: ¿Se han infectado en alguna ocasión sus equipos al conectarse a la red alámbrica de los laboratorios?

Respuesta	Frecuencia	Porcentaje
Si	158	98,75 %
No	2	1,25 %
TOTAL	**160**	**100%**

Tabla 7: Infecciones de virus en la red alámbrica de los laboratorios FACSISTEL

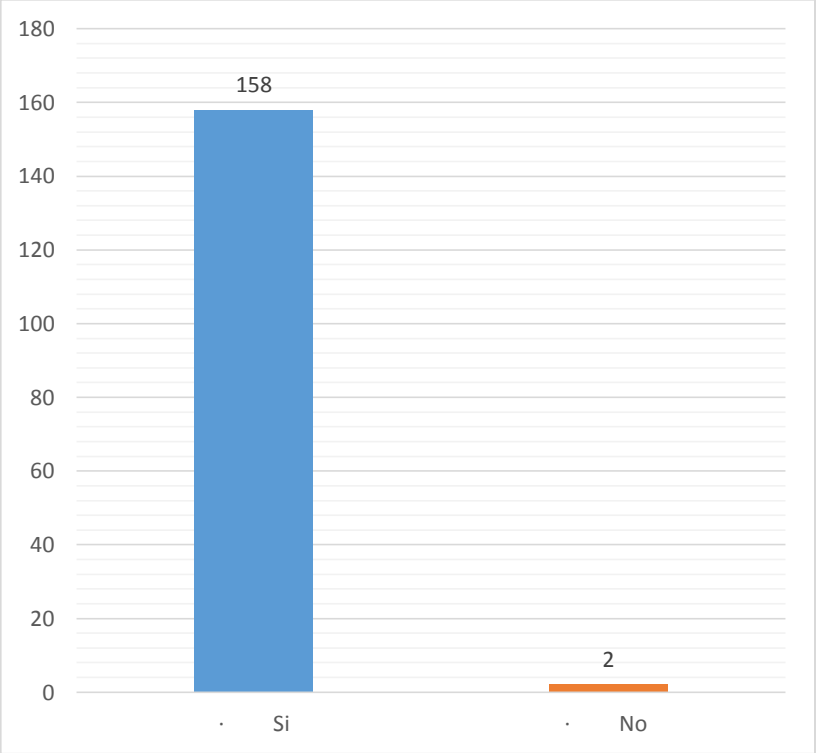


Figura 10: : Infecciones de virus en la red alámbrica de los laboratorios de FACSISTEL

INTERPRETACIÓN: El 98,75 % de los usuarios encuestados han tenido experiencias de infección en sus dispositivos al conectarse a la red alámbrica de FACSISTEL. Tan sólo un 1,25% de usuarios no han sido víctimas de aquello.

CONCLUSIÓN: Casi en su totalidad los encuestados han sido víctimas de infección al conectarse a la red de los laboratorios de FACSISTEL, ya sea ingresando a las máquinas de la misma o conectando sus dispositivos a la red.

1.7. RESULTADOS ESPERADOS

Los resultados esperados dentro de este proyecto son los siguientes:

1. Realizar la implementación del laboratorio virtual utilizando los servidores de la Facultad y configurar cada uno de los sistemas operativos que se utilizaran. En el laboratorio se monitorizará la red de los laboratorios de FACSISTEL para tener el control de cada dispositivo externo conectado a la misma.
2. Al obtener las herramientas de análisis de monitoreo de código malicioso se espera proporcionar información relevante sobre la red, verificar el nivel de seguridad de la misma y si esta pueda ser una de las causas por el cual el internet se torna lento.
3. Se espera realizar un estudio del tipo de malware, su comportamiento, actividad maliciosa y la razón para que esta se convierta en un análisis. Además, en base a la metodología se entregará un reporte e informe detallado de dicho estudio al personal indicado en el manual de procesos.
4. Se proyecta con esta propuesta tecnológica proporcionar un trabajo investigativo que sirva como punto de partida para la creación de un laboratorio físico en beneficio a la universidad.

CAPÍTULO II
LA PROPUESTA

2.1. MARCO CONTEXTUAL

Las pruebas se llevarán a cabo en la red de la Facultad de Sistemas y Telecomunicaciones, perteneciente a la Universidad Estatal Península de Santa Elena, ubicada en la Avda. principal La Libertad - Santa Elena, cantón La Libertad provincia de Santa Elena, a una latitud sur 2° 13′ 59.63″ y latitud oeste 80° 52′ 40.45″.

Figura 11: Ubicación de UPSE Matriz

2.2. MARCO CONCEPTUAL

2.2.1. LABORATORIO VIRTUAL

Laboratorio virtual es un servidor de aplicaciones que ofrece paquetes especializados de software para emular diferentes campos de conocimiento. También se los denomina como entornos virtuales diseñados para varios experimentos, a través de los cuales se simula el laboratorio de ciencias real y se vincula el lado práctico con el lado teórico [11].

Esta modalidad permite tener la libertad de hacer los experimentos sin exponerse a ningún tipo de peligro. Esto se realiza a través de aplicaciones informáticas que cubren todos los campos de la ciencia [11].

Los laboratorios virtuales están compuestos generalmente de computadoras con capacidades adecuadas, servidores y softwares de virtualización [11].

Figura 12: Laboratorio virtual de Kaspersky

2.2.1.1. Ventaja de los laboratorios virtuales:

- Ofrece un ambiente real, pero protegiendo al usuario de los peligros que enfrentan durante la realización de algunos experimentos de laboratorio peligrosos [10].
- Ayuda a resolver el problema de recursos limitados y fondos para experimentos.
- Capacidad para mostrar fenómenos y resultados muy precisos que pueden no ser medibles utilizando herramientas de laboratorio simples y que requieren equipos complejos y costosos [10].
- Los laboratorios virtuales motivan a realizar experimentos de laboratorio pues poseen un entorno interactivo donde se pueden simular experimentos o pruebas
- Satisfacen la pasión científica, permitiendo acceder fácilmente a los diversos experimentos independientemente del tiempo o el lugar [10].
- Los laboratorios virtuales permiten utilizar tecnología moderna.

2.2.1.2. Áreas de laboratorios virtuales

Las principales áreas en las que se emplea el uso de laboratorios virtuales son [11]:

- Electrónica y Comunicaciones
- Ingeniería en ciencias de la computación
- Ingeniería Eléctrica
- Ingeniería mecánica
- Ingeniería Química

- Biotecnología e ingeniería biomédica
- Ingeniero civil
- Ciencias físicas
- Ciencias químicas

2.2.2. MALWARE

La palabra malware es la abreviatura de "software malicioso", el que está diseñado para cumplir con el objetivo de infiltrarse en sistemas informáticos para ocasionar daños o extracción de información sin la autorización del propietario [17]. Es decir, cualquier software que tenga acciones dañinas para el usuario, computadora o red es considerado un malware [18].

2.2.2.1. Clasificación y comportamiento del malware

NOMBRE	COMPORTAMIENTO
BOTS	Es un malware controlado remotamente que infecta un sistema informático conectado a Internet [19].
BOTNETS	Permite que el atacante acceda al sistema, haciendo que el conjunto de máquinas infectadas con la misma botnet reciban las mismas instrucciones de un único servidor de comando y control [19].
CABALLO DE TROYA (TROJAN HORSE)	Es un malware con forma de aplicación que aparenta realizar las funciones que el usuario desea [19].
EXPLOIT	Es una malware creado para aprovechar las vulnerabilidades de seguridad que posee un sistema informático y tomar control del mismo [19].
GUSANO (WORM)	Son creados para propagarse sin advertencia o interacción del usuario, provocando un aumento en las solicitudes de servicio de tráfico de red, que eventualmente conducirán a una denegación de servicio distribuida (DDoS) [19].

INUNDADORES (FLOODERS)	Este malware funciona realizando inundaciones de información no deseadas como correo electrónico, mensajería instantánea y SMS [19].
KEYLOGGERS	Código malicioso creado para supervisar y capturar las actividades de los usuarios mediante las pulsaciones de teclas [19].
MAILERS Y MASS-MAILERS	Es un virus que convierte un sistema infectado en un servidor de correo malicioso [19].
PHARMING	Es un código malicioso encargado de redirigir el tráfico de un sitio web a uno falso [19].
PHISHINGS	Es el acto de robar información personal a través de Internet con el fin de cometer fraude financiero, robo de información, etc [19].
PUERTA TRASERA (BACKDOOR)	Es un software malicioso que permite eludir los métodos de autenticación estándar de un sistema operativo y da acceso remoto a los sistemas informáticos sin el consentimiento explícito del usuario para ejecutar comandos en el sistema local [19].
ROOTKIT	Malware que oculta la existencia de otras aplicaciones a los usuarios y se combina con otro malware, como una puerta trasera, para permitir el acceso remoto al atacante y hacer que el código sea difícil de detectar para la víctima [18].
VIRUS	Es un programa que puede infectar y copiarse en otros programas benignos [18].

Figura 13: Clasificación y comportamiento de malware

2.2.2.2. Análisis de malware

Es el estudio para verificar la funcionalidad que tiene determinada muestra de malware. El proceso que se lleva a cabo para realizar el análisis es fundamental para desarrollar técnicas de detección y prevención de código malicioso. Sin embargo,

también permite la creación de herramientas para eliminar el malware de una máquina o sistema infectado [17].

El propósito del análisis de malware es proporcionar la información necesaria para responder ante una intrusión en la red. Además, determina las acciones que se realizaron durante la infiltración y cuáles fueron los archivos o máquinas infectadas para medir y contrarrestar los daños [18].

El análisis de malware se puede realizar de dos formas: Análisis estático y Análisis dinámico.

Análisis de malware estático

Es el análisis que se realiza inspeccionando un programa o software sin ejecutarlo [17]. Es decir, este análisis permite conocer las capacidades del espécimen al examinar el código del que se compone el programa.

Técnicas y herramientas para el análisis estático

Para realizar un análisis estático se utilizan varias técnicas de acuerdo a la naturaleza del caso. A continuación, se describe algunas de ellas:

- **Huellas digitales de archivos (hashing):** el hash es un método exclusivo para identificar malware [19]. Éste realiza su análisis en las operaciones a nivel de archivo, por ejemplo, el cálculo de un hash criptográfico del binario el cual permite diferenciarlo de los demás y verificar su autenticidad en caso de modificaciones hechas al archivo [17].

  WinMD5.- permite calcular el valor hash MD5 de un archivo, además verifica la integridad del archivo realizando una comparación entre el archivo original y el actual [20].

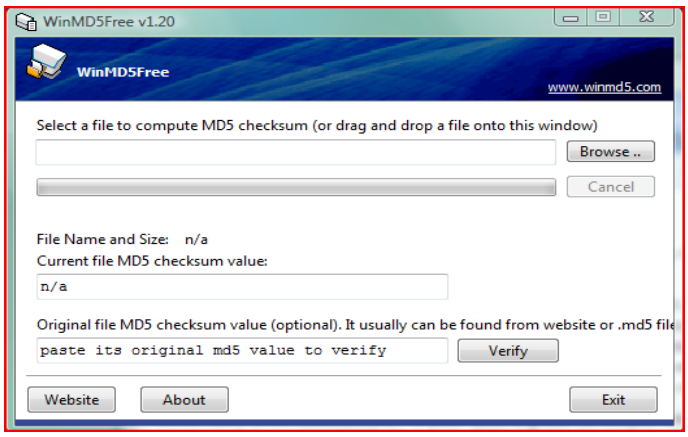


Figura 14: Herramienta WinMD5

Md5Summ. – es un software que aplica el algoritmo de generación de código hash MD5, pero también permite cambiar al método SHA1. Este programa muestra el contenido de todos los discos, como una estructura de árbol y permite seleccionar una carpeta en particular, expandiendo cualquier nodo [21].

Figura 15: Herramienta Md5Summ

- **Extracción de cadenas de texto:** El análisis de cadenas es una técnica que determina los valores que puede tomar una expresión de cadena durante la ejecución de un programa. Al examinar estas cadenas incrustadas se obtiene información sobre los componentes internos del binario inspeccionado y una base objetiva respecto a su comportamiento [17].

  Para llevar a cabo esta técnica se propone utilizar las siguientes herramientas:

  BinText. - es un software escáner creado para la extracción de cadenas de caracteres Ascii, Unicode y Resource de un archivo binario. Este software también se encarga de mostrar la posición del archivo y de la memoria [22].

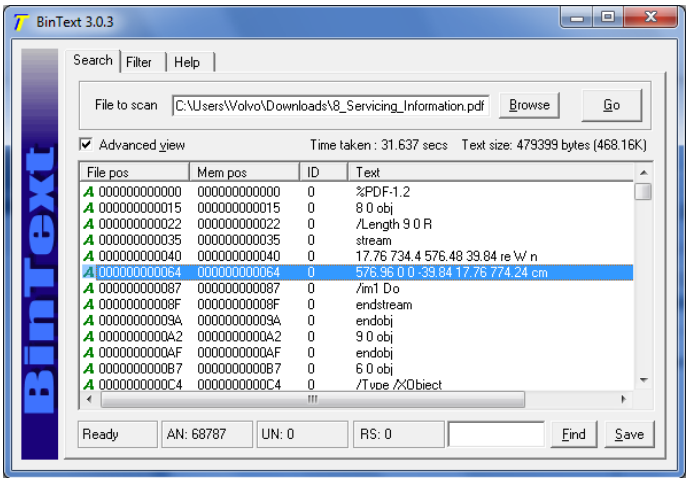


Figura 16: Herramienta BinText

Comando Strings.- es una herramienta de la suite de sysinternals que se encarga de escanear un archivo binario en busca de cadenas Unicode, Ascii o ambos, para obtener información detallada del comportamiento interno del malware como por ejemplo los protocolos, direcciones IP, puertos, rutas, entradas de registro, entre otras [23].

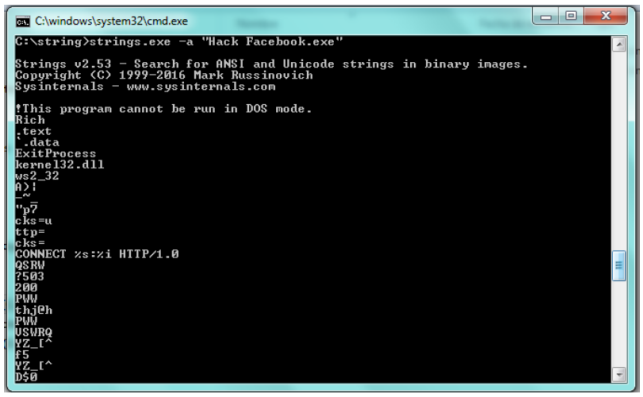


Figura 17: Herramienta Strings

- **Formato de archivo:** extrae los formatos de metadatos de un archivo determinado, para recopilar información útil. Por ejemplo, desde un binario de Windows, con formato PE (ejecutable portátil), se puede extraer información relevante, como el tiempo de compilación, las funciones importadas y exportadas, cadenas, menús e iconos [17].

Dependency Walker. - es una herramienta que se utiliza en el entorno de Microsoft Windows para obtener las funciones, módulos y librerías exportadas e importadas de un archivo ejecutable. Además, este programa muestra un diagrama jerárquico de los módulos y sus dependencias [19] .

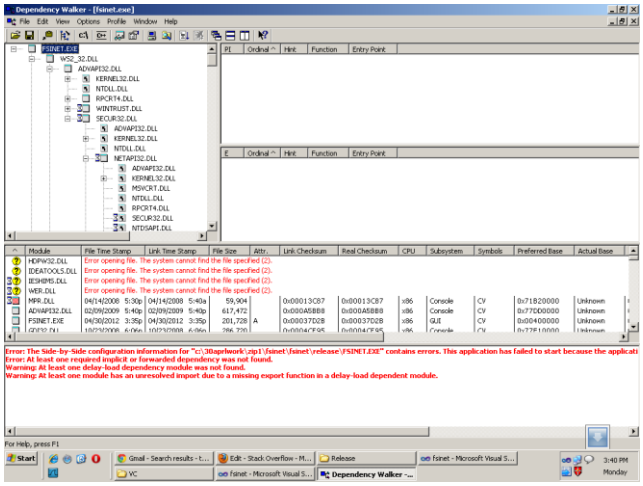


Figura 18: Herramienta Dependency Walker

PEStudio.- es un programa diseñado al análisis de cualquier tipo de archivo ejecutable. Realiza un escaneo al archivo y clasifica a través de indicadores (colores) los módulos posiblemente maliciosos del PE [19].

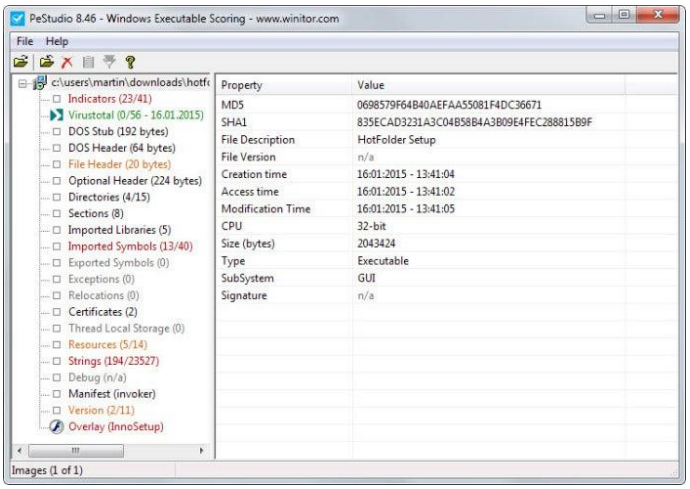


Figura 19: Herramienta PEStudio

PEBrowse. - permite ver los bytes de cada sección y muestra los datos analizados.

Este desensamblador funciona en ejecutables Win32 o Win64 y ensambles de Microsoft .NET [19], además permite abrir y examinar cualquier ejecutable sin la necesidad de cargarlo como parte de un proceso activo con un depurador. La información que proporciona está organizada en un índice de vista de árbol con las principales divisiones del archivo PE que se muestran como nodos [23].

PEBrowse proporciona una multitud de funcionalidades en la plataforma Windows que son el análisis de archivos PE, desmontaje y depuración [19].

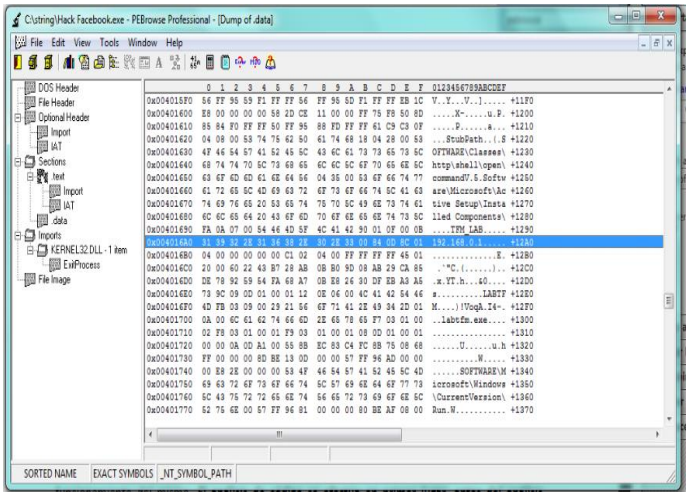


Figura 20: Herramienta PEBrowse

- **Exploración AV:** realiza escaneos a archivos binarios para detectar por lo general malware conocidos [17].
- **Detección de empaquetadores:** el malware se distribuye principalmente de forma empaquetada, ya sea encriptada o comprimida, utilizando empaquetadores los cuales hacen que el programa se vea diferente desde una perspectiva de análisis estático y su lógica. Por lo tanto, es necesario el uso de desempacadores para analizar la estructura de la muestra y ejecutar otras herramientas sobre la misma [17].

  Para desarrollar esta actividad se utilizará las siguientes herramientas:

  PEiD. - este software fue diseñado para archivos ejecutables de Windows. Su funcionamiento se basa en identificar las herramientas que se utilizaron en las técnicas de ofuscación (técnicas de polimorfismo, empaquetamiento, cifrados, y metamorfismo) para proteger al malware [19].

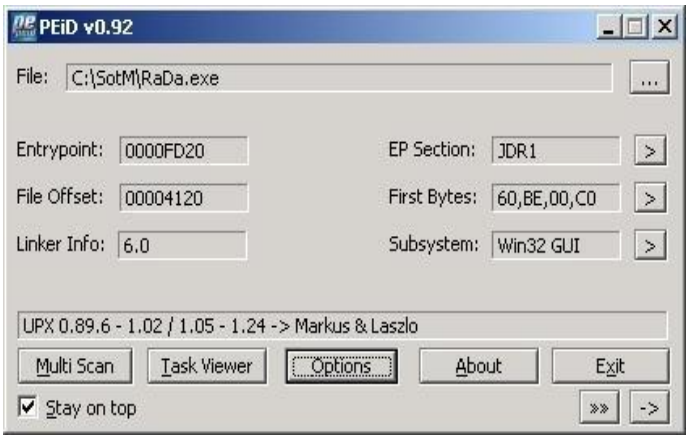


Figura 21: Herramienta PEiD

- **Desmontaje:** la mayor parte del análisis estático se basa en el desmontaje de un binario dado, esto se realiza utilizando herramientas que son capaces de revertir el código de la máquina al lenguaje ensamblador. Basado en el código de ensamblaje reconstruido, se puede inspeccionar la estructura del archivo y así examinar su objetivo [17].

  PE Explorer. - esta herramienta permite inspeccionar el funcionamiento interno de un ejecutable. Una vez que se haya analizado el archivo, mostrará un resumen de la información del encabezado y de los recursos contenidos en el PE, además esta herramienta permite explorar elementos específicos del mismo [23].

PE Explorer también proporciona varias herramientas útiles para la obtención de información como por ejemplo la búsqueda de sintaxis de funciones API, el escáner de dependencias, editor de secciones y un desensamblador para generar volcados de código anotado [23].

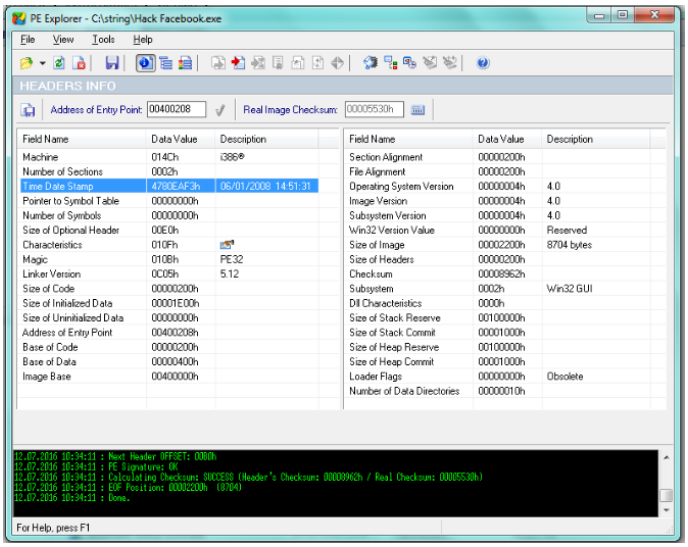


Figura 22: Herramienta PE Explorer

OllyDbg. – es el depurador de código ensamblador más utilizado por los analistas de malware, aunque no admite la depuración del kernel. Se enfoca en el análisis de código binario especialmente cuando el código fuente del programa no se encuentra disponible. Sus funciones principales se basan en encontrar traza de registros, reconocimiento de procedimientos, llamadas de API, swiches, tablas, constantes y strings, así como localizar rutinas de archivos objeto y de bibliotecas [19].

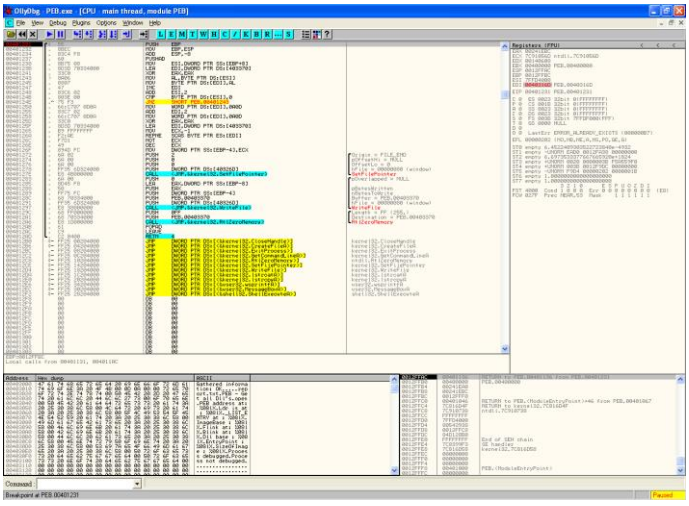


Figura 23: Herramienta OllyDbg

IDA42 Pro. - Interactive Disassembler Professional (IDA Pro) es un desensamblador distribuido por HexRays, empleado por muchos analistas de malware, ingeniería inversa y analistas de vulnerabilidad [19]. Este software soporta varios formatos de archivo, como Portable Executable (PE), Common Object File Format (COFF), Executable and Linking Format (ELF) y a.out. Sus funciones principales se basan en realizar tareas como búsqueda de funciones, análisis de pila, identificación de variables locales y entre otras [24].

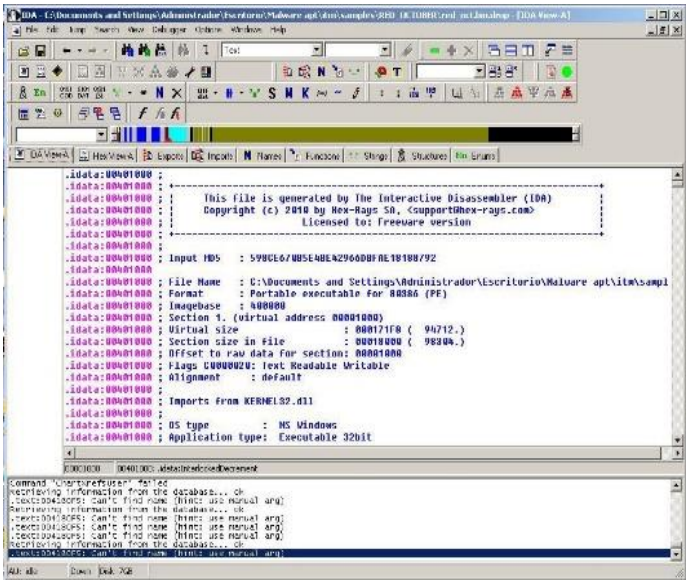


Figura 24: Herramienta IDA42 Pro

La principal ventaja del análisis estático de malware es que permite una investigación exhaustiva de un binario dado. Es decir, puede cubrir todas las rutas de ejecución posibles de una muestra de malware. Además, es más seguro que análisis dinámico ya que el código fuente no se ejecuta realmente [17].

Este tipo de análisis demanda mayor tiempo y en varias ocasiones se torna difícil ya que se requiere experiencia de acuerdo al tipo de estudio que se va a realizar [17].

Análisis dinámico de malware

Es el análisis que se realiza a un programa durante su ejecución. Es decir, se lleva a cabo cuando se ejecuta una muestra de malware en un entorno controlado, monitoreando sus acciones para realizar un estudio con respecto a las mismas [17] y examinar cómo interactúa el espécimen con su entorno .

El análisis dinámico posee la ventaja de desempacar el malware, ya que se realiza en tiempo de ejecución, permitiendo conocer el comportamiento real del programa. El principal inconveniente de este tipo de análisis es el código inactivo, es decir, a diferencia del análisis estático, el análisis dinámico monitorea solo una ruta de ejecución y, por consecuencia, obtiene una cobertura de código incompleta. Además, existe el riesgo de dañar los sistemas de terceros si el entorno de análisis no está aislado o restringido adecuadamente [17].

Existen dos enfoques básicos para el análisis dinámico de malware:

• Realizar un snapshot del estado inicial del sistema antes de la ejecución del malware y compararlo con el estado final del sistema después de la ejecución [18].

• Monitorear las acciones del malware durante la ejecución con la ayuda de una herramienta especializada, como un depurador [18].

Herramientas de análisis dinámico:

Disk Pulse. - es una herramienta que monitorea los cambios realizados en el disco duro, por ejemplo, archivos creados, editados y modificados, también genera informes y estadísticas de monitoreo de cambio de disco [19].

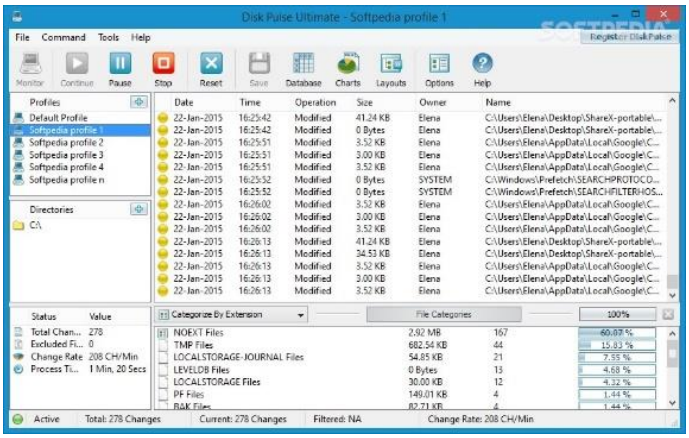


Figura 25: Herramienta Disk Pulse

Process Explorer. - es un administrador de tareas potente que se ejecuta cuando se realizan los análisis dinámicos. Este software proporciona información sobre los procesos que se ejecutan en tiempo real de un sistema [24]. Process Explorer se utiliza para detallar procesos activos, archivos DLL cargados por un proceso, varias propiedades de proceso e información general del sistema. También se utiliza para eliminar un proceso, cerrar la sesión de los usuarios e iniciar y validar procesos [19].

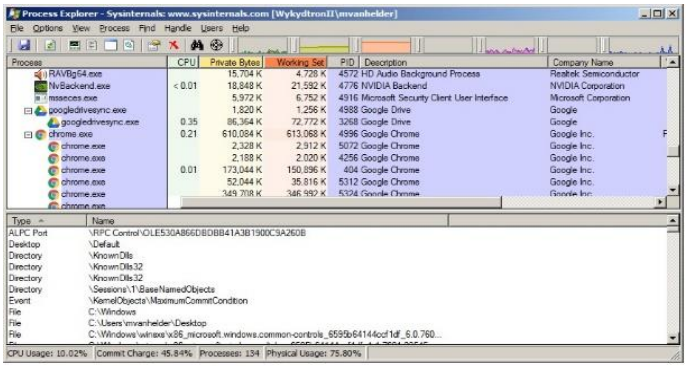


Figura 26: Herramienta Process Explorer

Process Monitor. – también llamado procmon, es una herramienta que proporciona el monitoreo de ciertos registros, sistemas de archivos, red, procesos y actividades de subprocesos [19]. Este programa ayuda a entender cómo interactúa el programa malicioso con el sistema de archivos y el registro [25].

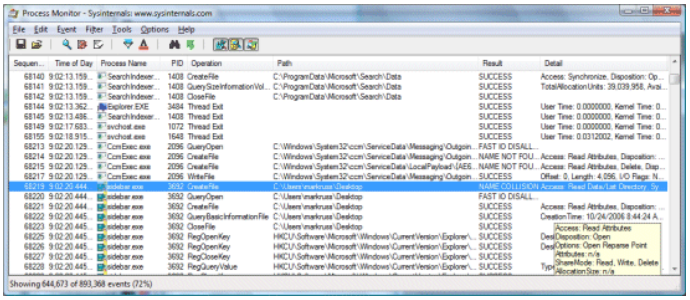


Figura 27: Herramienta Process Monitor

AutoRuns. - enumera el código que se ejecutará automáticamente al iniciarse el sistema operativo en el orden que Windows los procesa [24]. También enlista los programas que se encuentran condos para ejecutarse, los archivos DLL y los controladores cargados en el núcleo. Esto permitirá verificar si algún malware se inicia junto al sistema operativo [19].

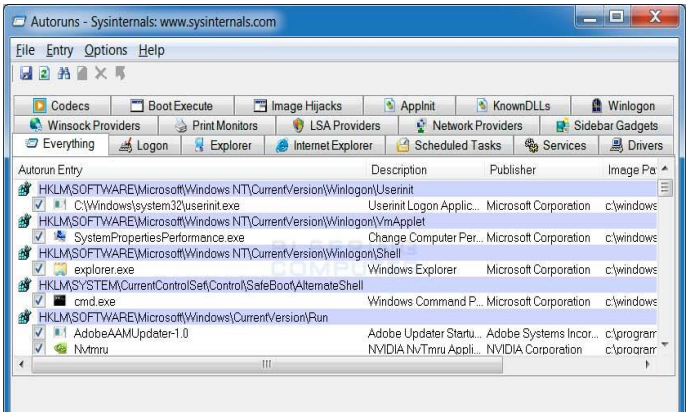


Figura 28: Herramienta Autoruns

2.3. MARCO TEÓRICO

2.3.1. Aplicación de Metodología de Malware para el Análisis de la amenaza avanzada persistente (APT) "Poison Ivy"

Esta investigación desarrollada por Pablo Gaviria donde expresa que "el avance tecnológico ha permitido crear nuevos escenarios de ataque en los cuales convergen una serie de elementos redundando en sofisticación de las amenazas. Esto requiere implementar nuevos mecanismos articulados sobre una nueva disciplina llamada Ciberdefensa, que permiten reaccionar de manera objetiva ante estos ataques" por esta razón su trabajo considera la forma de establecer la validez en la aplicación de la metodología de análisis de malware presentada por Don Javier Bermejo, en el contexto de la Amenaza Persistente Avanzada Poison Ivy [2].

Para llevar a cabo esta investigaión, fue necesario desarrollar la temática relacionada con los diferentes tipos de malware y las técnicas actuales de análisis, conocer e identificar la amenaza persistente avanzada (APT) "Poison Ivy", en relación al desarrollo metódico de cada una de las fases que componen la metodología, la aplicación de cada una de las herramientas sugeridas sobre una muestra de malware obtenida en un ambiente controlado el cual se asemejó a un escenario real. Esto permitió demostrar la importancia y funcionalidad de la metodología en particular respecto al análisis de malware como una herramienta efectiva y eficaz, alcanzando una serie de resultados obtenidos, debidamente organizados y documentados [2].

2.3.2. Laboratorio de malware: Automatización de la gestión de recursos virtuales para el estudio de malware.

En este proyecto Truyol diseñó unos laboratorios donde pudo realizar un estudio del malware. En los mismos se podrán ejecutar experimentos en entornos aislados que servirán para poder analizar el comportamiento del malware. Se proporcionó también la habilidad de crear una infinidad de entornos de red con diferentes sistemas operativos y aplicaciones que facilitarán el estudio del mismo [26].

Para crear estos entornos aislados, se ha hecho uso de la virtualización de sistemas. Esta tecnología permitió crear entornos aislados, flexibles y escalables donde poder

ejecutar cuantos experimentos sean necesarios. Por último, se realizaron una serie de experimentos y se muestran los resultados. Como resultado de los experimentos, se puede comprobar que la creación de distintos entornos resulta útil para poner de manifiesto distintos comportamientos maliciosos en función del malware ejecutado y de las aplicaciones instaladas sobre los distintos sistemas operativos [26].

2.3.3. Metodología para el análisis de malware en un ambiente controlado

Tatiana Jumbo en su trabajo de investigación estable que "Muchas entidades financieras son víctimas de ataques dirigidos mediante software malicioso conocido como malware, estos ataques cibernéticos son realizados por hackers cuya finalidad es transferir miles de millones de dólares a nivel mundial hacia paraísos fiscales. Es necesario realizar una investigación sobre los efectos y procesos de estos malware con la finalidad de encontrar mecanismos de prevención, reacción y mitigación [7]. Dado que el malware es cada vez más avanzado, muchas soluciones de prevención, como el firewall, software antivirus y antispyware, se están viendo superadas, lo cual se debe a que el malware aprovecha las ventajas de la tecnología para ser nocivo, rápido y sutil en la forma de engañar a sus víctimas. Su investigación se enfocó al análisis de malware, generando un entorno controlado en el que se pueda realizar investigaciones sobre el comportamiento de estos códigos maliciosos, mediante el uso de la herramienta CUCKOO para agilizar el análisis [7].

2.3.4. Desarrollo de un laboratorio para el análisis automatizado de códigos maliciosos

Duran Lara estableció "Es importante hacer énfasis en que las herramientas de seguridad informática, en general, tienen un tiempo de vida reducido que va de meses hasta algunos pocos años en los mejores casos, por lo tanto, es vital mantenerlas al tanto de los últimos avances y tendencias. Los resultados obtenidos son satisfactorios, ya que las pruebas realizadas con diversos tipos de malware proyectaron información que se esperaba se presentara en los análisis [8].

La herramienta se desempeñó bien en todos sus procesos de ejecución; a excepción de algunos casos muy puntuales, donde el código malicioso en ejecución afectaba un punto en particular y provocaba un rompimiento en el flujo de la herramienta TRUMAN. En relación a lo anterior se puede comentar la ocasión en que algunos

códigos maliciosos provocaban un congelamiento de la terminal de comando, y en particular, una interrupción del programa que los ejecuta, lo cual no permitía que este programa siguiera su curso y se reiniciara el equipo cliente, por lo tanto, permanecía como si se tratara de un ciclo infinito y debía ser reiniciado manualmente. Esto era un grave problema, porque ocurría con frecuencia. La solución fue agregar un proceso más en ejecución, de tal manera que las labores de ejecutar el programa malintencionado y llevar a cabo la cuenta regresiva para el reinicio del sistema fueran independientes [8].

2.4. COMPONENTES DE LA PROPUESTA

2.4.1. Virtualización

Se realizó la virtualización del laboratorio en el software Proxmox Virtual Environment, que cuenta con una licencia de código abierto.

En Proxmox se realizó la virtualización tanto de sistemas operativos Windows como Linux. A continuación, se enlistarán los sistemas operativos virtualizados en el laboratorio:

- Firewall Pfsense
- Windows 7
- Windows 10
- Windows Server
- CentOS7

2.4.2. Firewall Pfsense

Este firewall contiene una interfaz web que permite ser personalizada de acuerdo a las necesidades.

El laboratorio virtual posee un pfsense para realizar las siguientes funciones

1. Configurar el servidor DHCP para la asignación de IP estática por medio del registro de las MAC.
2. Monitoreo del tráfico de la red por medio del Traffic Graph
3. Analizar los registros de acceso de proxy, generar informes basados en la web que detallan las URL a las que accede cada usuario en la red utilizando la herramienta LightSquid.

2.4.3. Escenarios

VÍCTIMA: Se instalaron los sistemas operativos en donde se trasferirán los malware para realizar las respectivas pruebas, tanto del análisis estático como el análisis dinámico. Los sistemas operativos utilizados en este escenario son:

- Windows 7
- Windows 10

MONITORIZACIÓN Y SERVICIOS: Se creó este escenario con el fin de monitorizar el tráfico de red generado por el malware y, además, brindar los servicios para que sean vulnerados por el mismo. Los sistemas operativos utilizados en este escenario son:

- Windows Server
- Kali Linux

SERVICIOS: Se elaboró este entorno para proporcionar servicios al malware en su interacción con el medio en donde actúa, y así examinar su comportamiento. Los sistemas operativos utilizados en este escenario son:

- Windows Server
- CentOS 7

2.5. REQUERIMIENTOS

2.5.1. Requerimiento de espacio en el servidor

Para realizar la instalación de las máquinas virtuales se requiere de las siguientes características

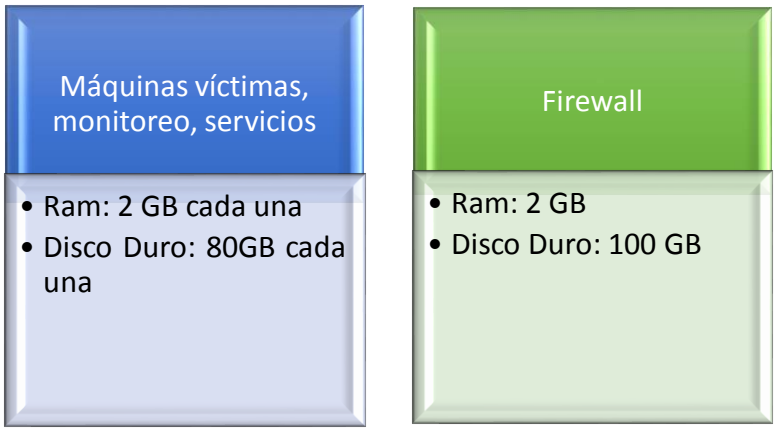


Figura 29: Requerimientos t;ecnicos de las máquinas virtuales

2.5.2. Inventario de MAC

Es necesario realizar un inventario de las MAC de cada máquina virtualizada (Windows 7, Windows 10, Windows Server) para asignarles una IP estática y poder controlarla desde el Pfsense.

2.5.3. Entorno controlado

Para soslayar los riesgos de infección de malware en la red de los servidores de FACSISTEL, es necesario la creación de una nueva red virtual (vlan) aislada, que permitirá separar los diferentes tráficos de red.

En esta nueva red virtual no dispondrá salida al internet, tan solo se podrán comunicar las máquinas del laboratorio.

2.5.4. Habilitar puertos

El malware deberá actuar en un ambiente sin restricciones, para poder estudiar su comportamiento con el entorno. Para que se cumpla con este fin es importante que en la red aislada no exista ningún tipo de restricciones y que todos los puertos del Pfsense se encuentren abiertos.

2.5.5. Snapshot

Se requiere que por cada prueba realizada en el laboratorio se realicen snapshot para tener un punto de regreso en caso de que el malware dañe el equipo. Los snapshot se realizan en el mismo servidor, ya que PROXMOX cuenta con esta funcionalidad.

2.5.6. Deshabilitar la restauración y actualización del sistema

En las máquinas víctimas, monitorización y servicios se debe deshabilitar las restauraciones y actualizaciones del sistema antes de transferir y ejecutar o examinar el malware, para evitar tráfico de red inservible en el análisis y tener información absoluta del comportamiento del software malicioso.

2.6. DISEÑO DE LA PROPUESTA

2.6.1. ARQUITECTURA GLOBAL

La arquitectura general del presente estudio esta implementada en uno de los servidores de FACSISTEL que está estructurado de la siguiente manera:

El servidor de FACSISTEL utiliza el virtualizador PROXMOX y posee un sistema operativo orientado a firewall denominado “PFSENSE”, que permite tener un control de los dispositivos conectados a la red.

La red se encuentra segmentada por medio de VLAN’S para brindar seguridad en los datos y eficiencia de la misma.

Características del servidor:

- CPUs 16 x Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz (1 Socket) Kernel Version
- Memoria RAM: 40gb
- Disco Duro: 95gb

A continuación, se puede apreciar la arquitectura global del sistema:

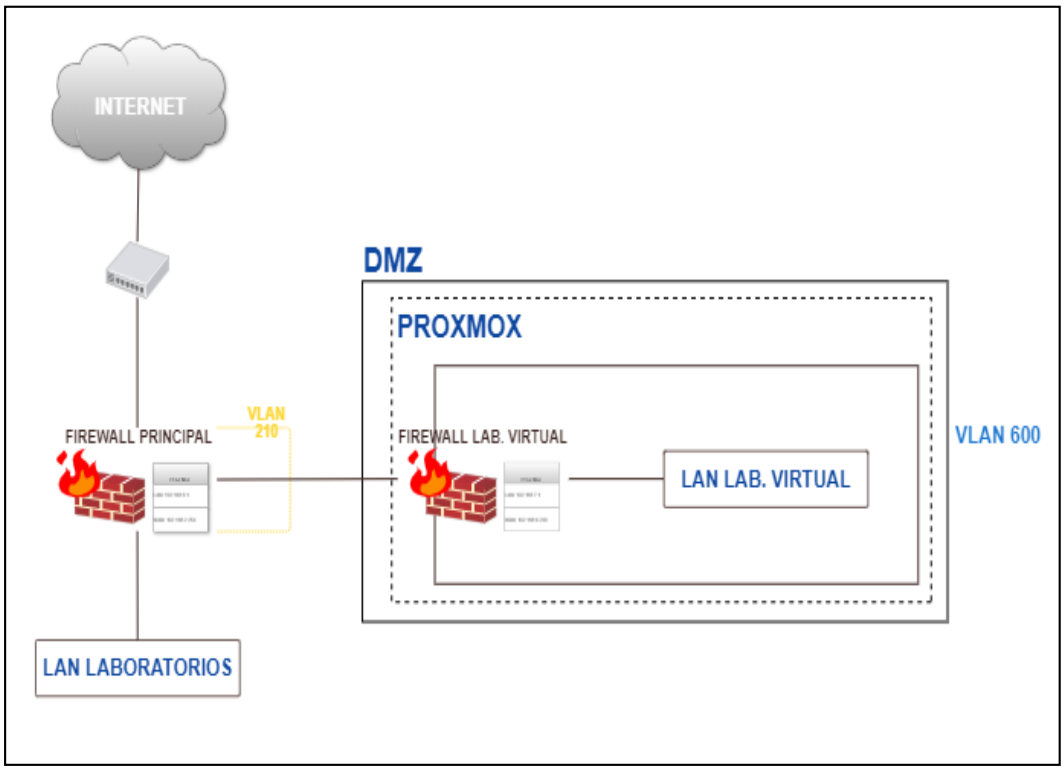


Figura 30: Arquitectura global de la red de FACSISTEL

Como se puede observar en la gráfica, la red está conectada a un router el cual se conecta al proveedor de internet de la UPSE. Así mismo, se puede observar que los laboratorios de la Facultad se encuentran segmentados dentro de una vlan para establecer comunicación entre ellos, sin embargo, el laboratorio virtual se encuentra segmentado en una vlan aislada por medidas de seguridad.

2.6.2. ARQUITECTURA DEL LABORATORIO VIRTUAL

2.6.2.1. Definición del entorno

El entorno en donde se implementó el proyecto de investigación necesariamente debía estar aislado para realizar las pruebas respectivas de modo seguro y cumplir con cada una de las metodologías. Esto con el fin de no infectar la red y que al tener un entorno controlado se pueda obtener resultados que simulen la realidad.

Para la simulación del entorno real de los laboratorios de FACSISTEL, fue necesario tener en el diseño los sistemas operativos que utilizan las máquinas de estos laboratorios, servicios, canales de comunicación, aplicativos y herramientas para la monitorización de todos los procesos aplicados.

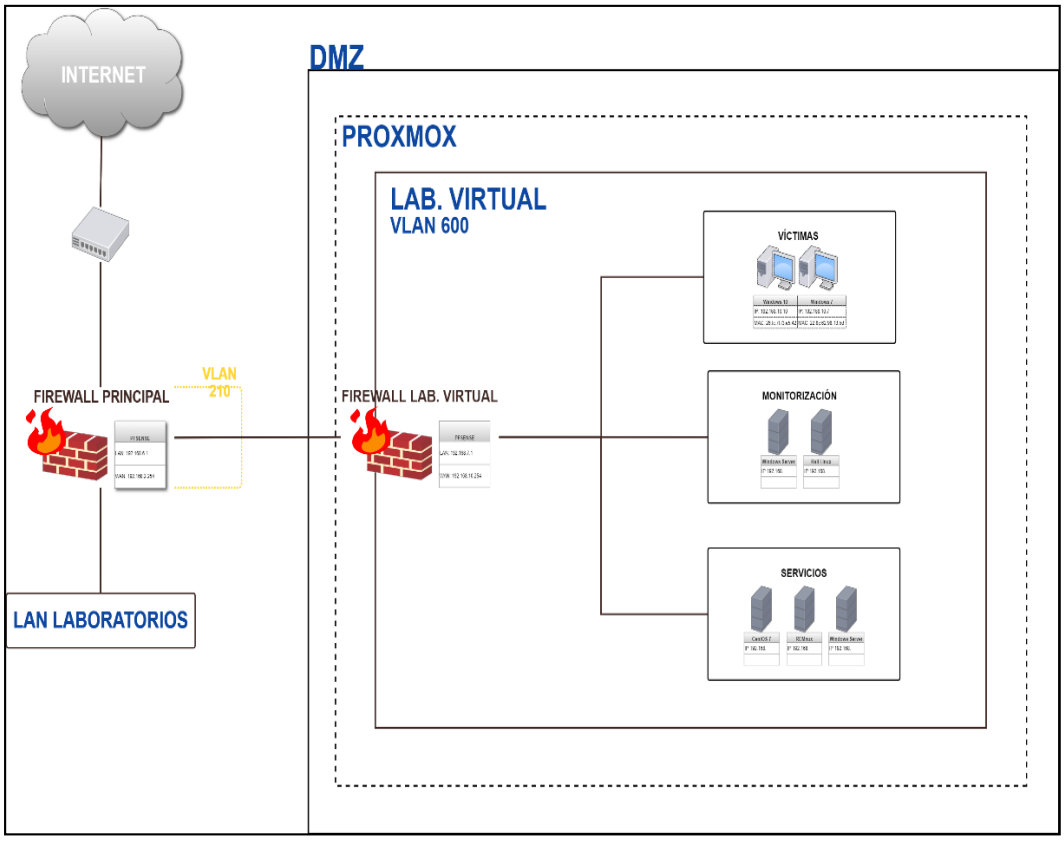


Figura 31: Arquitectura del laboratorio virtual para el análisis de malware

Los escenarios de aplicación del proyecto están compuestos de la siguiente manera:

- **Víctima:** este escenario posee los sistemas operativos Windows 7 y Windows 10. La elección de estos sistemas se basó en el inventario realizado a los laboratorios de FACSISTEL.

En este punto se realizaron las infecciones de malware para poder verificar el comportamiento del mismo sobre estos sistemas operativos.

- **Monitorización:** permite monitorizar el tráfico de red creado por el malware y además proveer los diferentes servicios del sistema
- **Servicios:** este escenario posee los sistemas operativos existentes en los servidores de FACSISTEL para que el malware verificar la interacción del malware con los servicios HTTP, DNS, DHCP, Server, entre otros.

Es importante indicar que estos entornos se encuentran virtualizados en uno de los servidores de la FACSISTEL utilizando la herramienta PROXMOX.

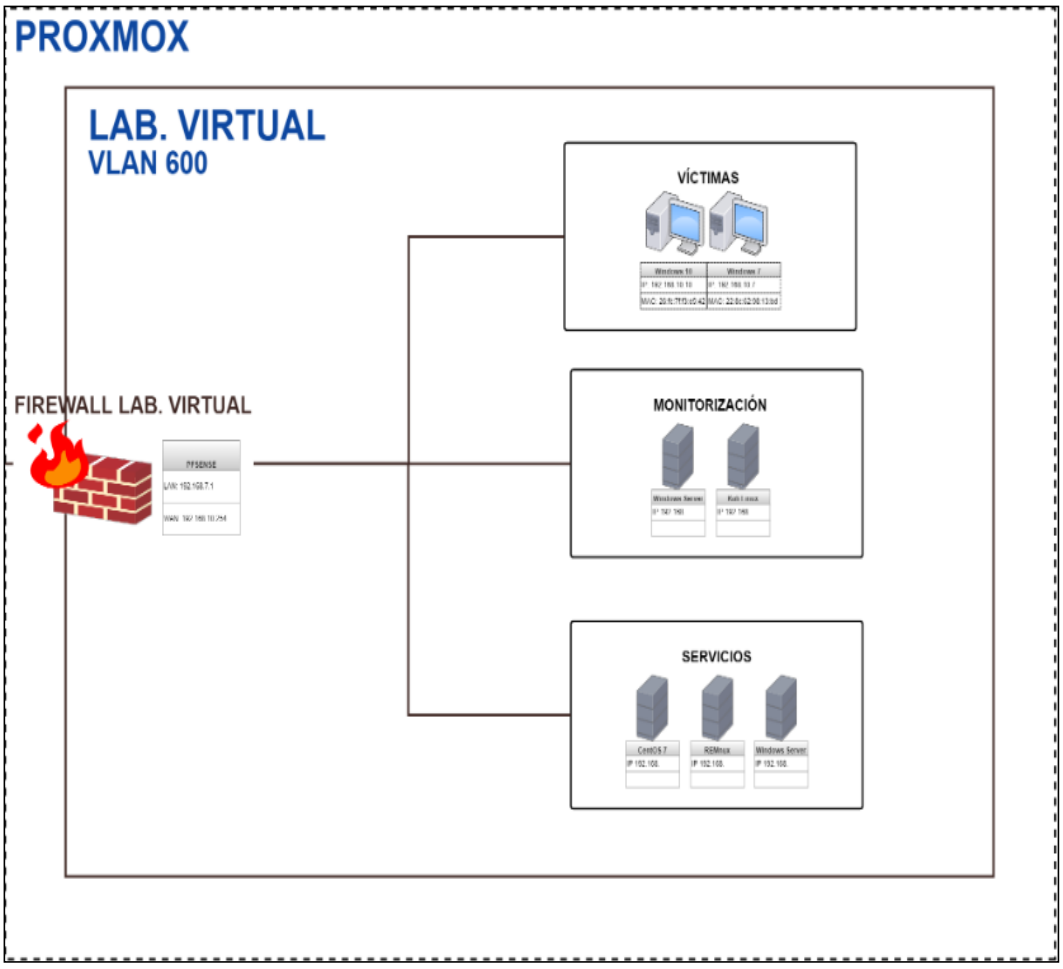


Figura 32: Escenarios del laboratorio virtual

2.6.2.2. Definición de las herramientas específicas del laboratorio

Las herramientas que se utilizaron dentro del laboratorio se eligieron de acuerdo a las metodologías de análisis. A continuación, se enlistará las herramientas utilizadas en cada entorno:

VÍCTIMA	MONITORIZACIÓN	SERVICIOS
AutoRuns	Comando Strings	REMnux
AVG	Dependency Walker	Centos6
Avira	Md5Summ	
BinText	OllyDbg	
BitDefender	PE Explorer	
Comando Strings	PEBrowse	
Dependency Walker	PEiD	
Disk Pulse	PEStudio	
ESET	Process Monitor	
IDA42 Pro		
Kaspersky		
Md5Summ		
Nmap		
OllyDbg		
Panda		
PE Explorer		
PEBrowse		
PEiD		
PEStudio		
Process Explorer		
Process Monitor		

Tabla 8: Herramientas de análisis de malware

2.7. ESTUDIO DE FACTIBILIDAD

2.7.1. Factibilidad Operativa

Para la implementación del laboratorio virtual se requirió de un personal técnico especializado en el área de redes y seguridad informática que se detalla a continuación:

CATEGORÍAS	COMPONENTES / RUBROS	CANTIDADES
Recursos Humanos	Técnico en redes	1
	Analista de Seguridad Informática	1
	Asesor especialista en redes y seguridad	1

Tabla 9: Recurso Humano

2.7.2. Factibilidad Técnica

En la factibilidad técnica se establecieron las herramientas de hardware y software de acuerdo a las metodologías usadas tanto en el análisis estático como el dinámico necesarios para la implementación del laboratorio virtual, además de otros recursos necesarios.

CATEGORÍAS	COMPONENTES / RUBROS	CANTIDADES
Recursos de Hardware	Laptop i5 monitoreo de la red (HP i5)	1
	UPS respaldo de servidores y almacenamiento	1
	Monitor 19,5'' Monitoreo	4
	Impresoras	1
	Servidores HP Proliant	1
	Partes y accesorios computacionales	-

Tabla 10: Recursos de Hardware

CATEGORÍAS	COMPONENTES / RUBROS	CANTIDADES
Recursos de Software	CentOS 7	1
	Windows 10	1
	Windows 7	1
	Programas de monitoreo de red	-
	Programas de análisis de malware	-

Tabla 11: Recursos de Software

CATEGORÍAS	COMPONENTES / RUBROS	CANTIDADES
Recursos Materiales	Suministros y accesorios	-

Tabla 12: Recursos Materiales

Luego de un estudio realizado se puede concluir que el proyecto es técnicamente factible debido a que se tiene disponibilidad de software, hardware, recursos materiales y humano.

2.7.3. Factibilidad Financiera

CATEGORÍAS	COMPONENTES / RUBROS	CANTIDADES	PRECIO UNITARIO	TOTAL
Recursos de Hardware	Laptop i5 monitoreo de la red (HP i5)	1	$800.00	$800.00
	UPS respaldo de servidores y almacenamiento	1	$4,599.00	$4.599.00
	Monitor 19,5'' Monitoreo	4	$115.18	$460.72
	Impresoras	1	$300.00	$300.00
	Servidores HP Proliant	1	$7,000.00	$7.000.00
	Partes y accesorios computacionales	-	$800.00	$800.00
				$13,959.72
Recursos de Software	CentOS 7	1	$0.00	$0.00
	Windows 10	1	$289.00	$289.00
	Windows 7	1	$199.99	$199.99
	Programas de monitoreo de red	-	$0.00	$0.00
	Programas de análisis de malware	-	$0.00	$0.00
				$488.99
Recursos Humanos	Técnico en redes	6 meses	$600.00	$3,600.00
	Analista de Seguridad Informática	2 meses	$800.00	$1,600.00
	Asesor especialista en redes y seguridad	4 meses	$1,500.00	$6,000.00
				$11,200.00
Recursos Materiales	Suministros y accesorios	-	$120.00	$120.00
				$120.00
TOTAL				**$25,648.71**

Tabla 13: Recursos Financieros del Proyecto

COSTO REAL DEL PROYECTO

A nivel de hardware el presupuesto va a tener costo cero porque se cuenta con la infraestructura de red requerida para la ejecución del proyecto. FACSISTEL posee dos servidores en el cual se podrá realizar la virtualización del laboratorio, además de UPS, máquinas de escritorio, laptop e impresora.

En software el presupuesto se torna a un costo cero, ya que las herramientas tanto para el desarrollo y análisis son de código abierto, a excepción de la licencia de Windows que ya se encuentra adquirida por la universidad.

A nivel operacional el costo también es cero ya que los recursos operacionales fueron abordados por quien ejecutará el proyecto. Este valor lo asumirá el operante del proyecto por tratarse de un tema de titulación.

Basado en este análisis, se concluye que el proyecto es factiblemente económico porque tiene un costo total de $120.00 que serán subastados por la ejecutora del proyecto. Además, se posee las herramientas, equipos y personal necesario para la realización de la propuesta tecnológica. A continuación, se describe una tabla general del presupuesto.

CATEGORÍAS	COSTOS
Recursos de Hardware	$ 0.00
Recursos de Software	$ 0.00
Recursos Humanos	$ 0.00
Recursos Materiales	$ 120.00
Total	**$ 120,00**

Tabla 14: Financiamiento del proyecto en general

2.8. RESULTADOS

2.8.1. IMPLEMENTACIÓN

2.8.1.1. Fase de inicialización

Preparación del entorno virtual (EV)

Para la preparación del EV se efectuaron los siguientes pasos:

- **Implementación del entorno virtual**
  - Realizar la instalación de las siguientes máquinas virtuales para simular un entorno real de los laboratorios de FACSISTEL

Figura 33: Escenario del entorno virtual

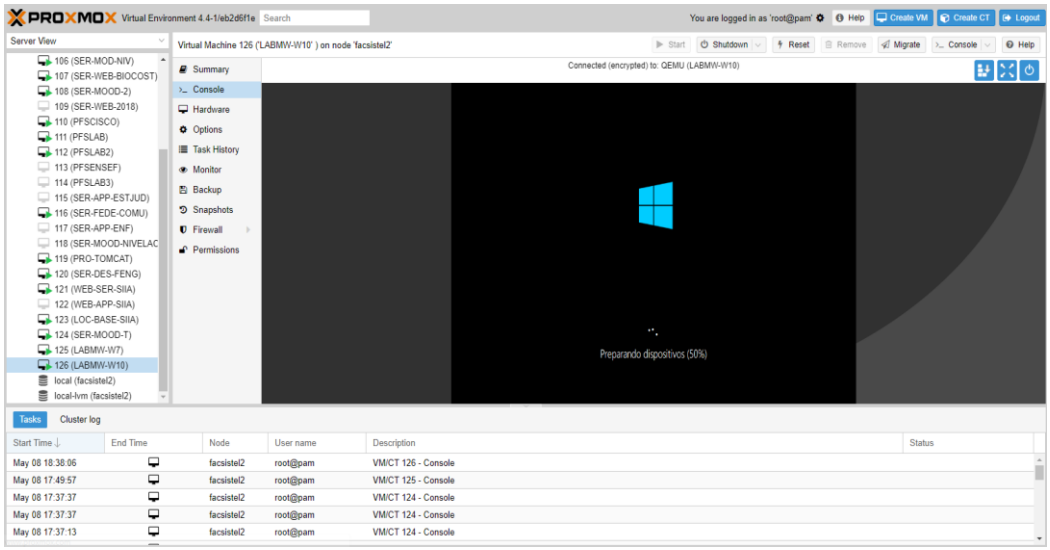


Figura 34: Entorno virtual en PROXMOX

  - Desactivar las actualizaciones del sistema, restauración y Windows defender.
  - Hacer una instantánea en vivo de Proxmox para preservar el estado inicial de las máquinas víctimas.

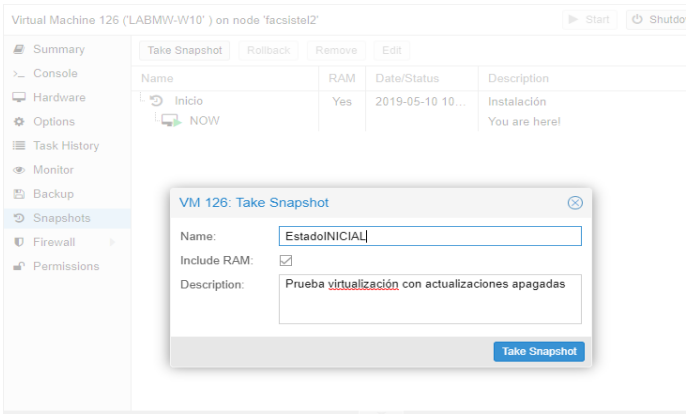


Figura 35: Snapshot del Estado Inicial

- **Herramienta Systracer**
  - Se instala en las máquinas victimas la herramienta Systracer, la misma que sirve para verificar si existen cambios en el registro del sistema.

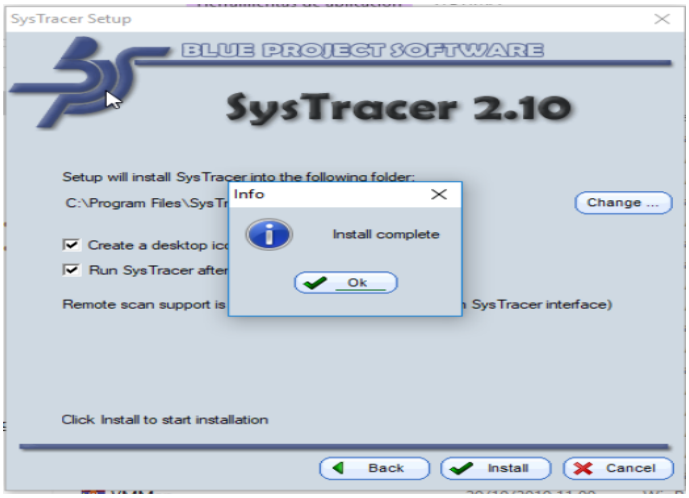


Figura 36: Instalación de la herramienta Systracer

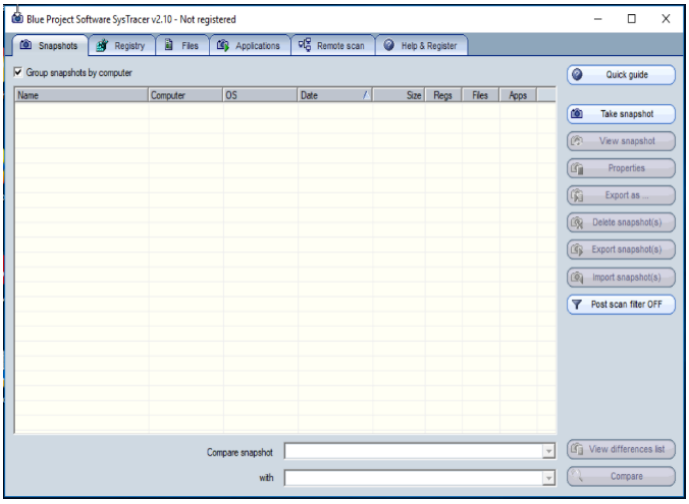


Figura 37: Entorno de trabajo de Systracer

- Es necesario establecer una línea base de la configuración inicial de máquinas víctimas, por lo que Systracer pedirá que se realice una captura del registro con el fin de obtener un estado inicial que servirá para futuras comparaciones.

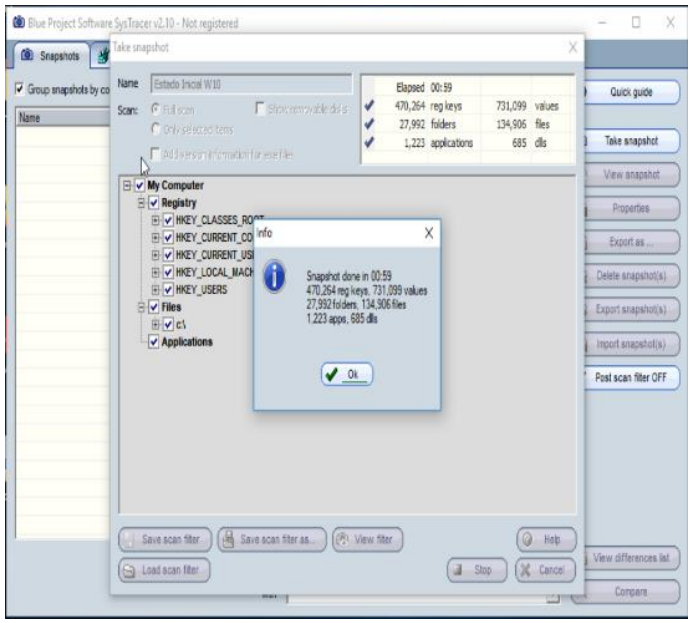


Figura 38: Creación de snapshot en herramienta Systracer

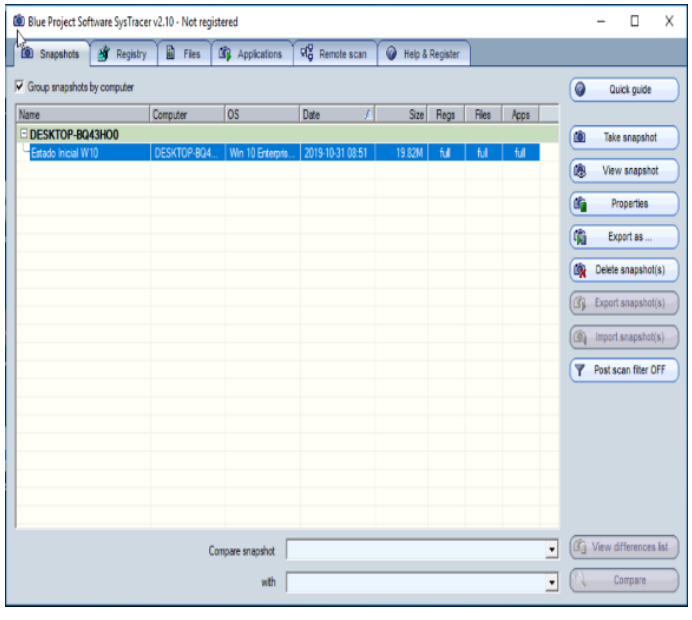


Figura 39: Línea base de la máquina virtual

- **Herramienta WinMD5**
  - Ejecutar la herramienta WinMD5 para comprobar la integridad del registro del sistema

- Abrir en la herramienta el archivo generado por el Systracer para obtener su hash

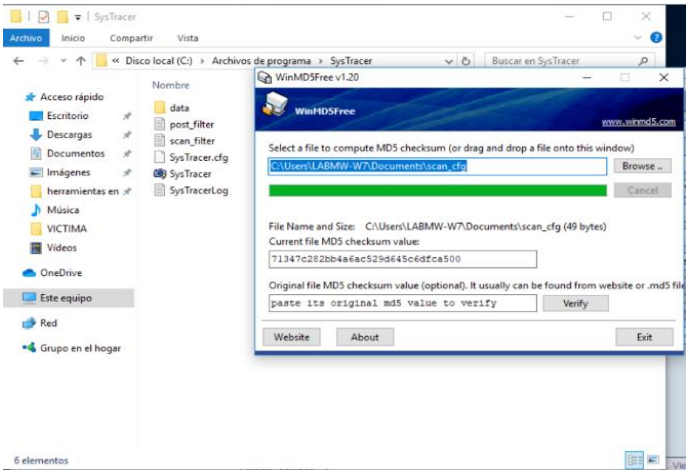


Figura 40: Hash del archivo generado por Systracer

Diagramación de la infraestructura de red

La diagramación de la infraestructura de red debe considerar las siguientes premisas:

- Registrar las direcciones MAC de las máquinas virtuales establecidas en el laboratorio virtual, que dispone de 5 máquinas.
- Diagramar la infraestructura de red del entorno virtual para la implementación del mismo:

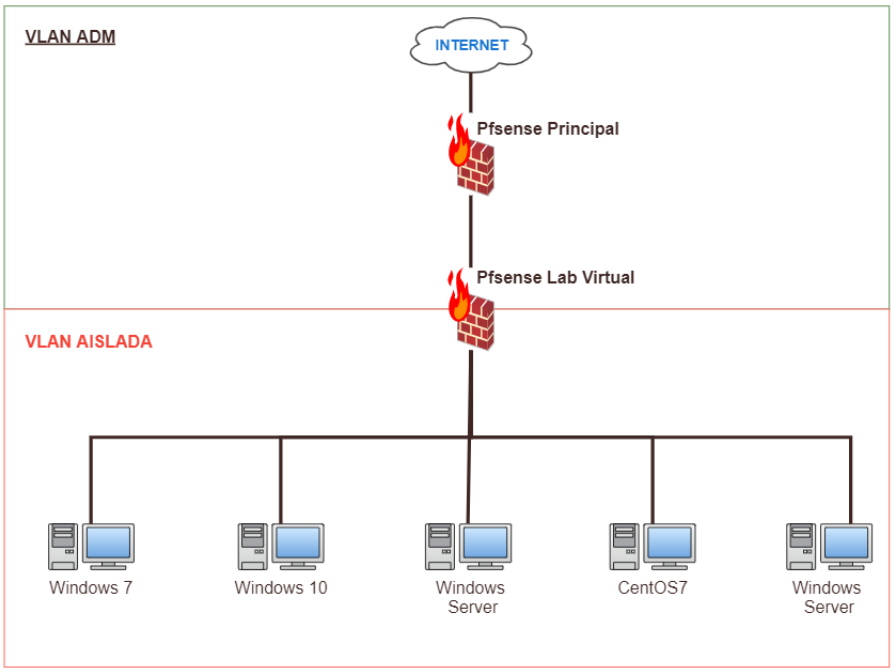


Figura 41: Diagramación de la infraestructura de red

Este diagrama está compuesto por un firewall principal (existente en los servidores de FACSISTEL para controlar la red) y un firewall conectado al principal para el control de las máquinas en el laboratorio virtual. El firewall a utilizar será el software PFSENSE.

Implementación y configuración del firewall de control (pfsense) del laboratorio virtual

- **Virtualización en PROXMOX del firewall Pfsense**
  - Para virtualizar en proxmox se procedió a agregar la imagen ISO del instalador del Pfsense. Para ello es necesario descargar la ISO de PfSense en la página oficial y agregarlo al repositorio del server PROXMOX.

Figura 42: ISO del firewall Pfsense

  - Una vez almacenada la imagen ISO en el servidor, se realizó el proceso de instalación del Pfsense con las siguientes características de hardware en la máquina virtual:

Keyboard Layout	Default
Memory	2.00 GiB
Processors	1 (1 sockets, 1 cores)
Display	Default
CD/DVD Drive (ide2)	none,media=cdrom
Hard Disk (scsi0)	local-lvm:vm-127-disk-1,size=100G
Network Device (net0)	virtio=4E:34:A8:22:32:CB,bridge=vmbr9
Network Device (net1)	virtio=CE:FD:EE:EE:E3:0D,bridge=vmbr9

Figura 43: Características de hardware del Pfsense

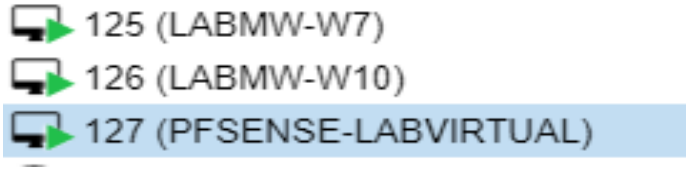


Figura 44: Firewall virtualizado en Proxmox

- En el ítem “Add” se eligió la opción “Network Device” para agregar la vlan aislada y así agrupar el conjunto de equipos de manera lógica y no física.

Nombre	Puerto/Slaves
Vmbr9	6XX

Instalación del sistema operativo del firewall Pfsense

Este proceso debe considerar lo siguiente:

- Inicializar la máquina virtual para realizar el proceso de instalación y configuración del firewall.

Figura 45: Proceso de instalación y configuración del firewall

- En la configuración de consola se selecciona la opción “Change Video Font” y “Accept these Settings” para aceptar los cambios.

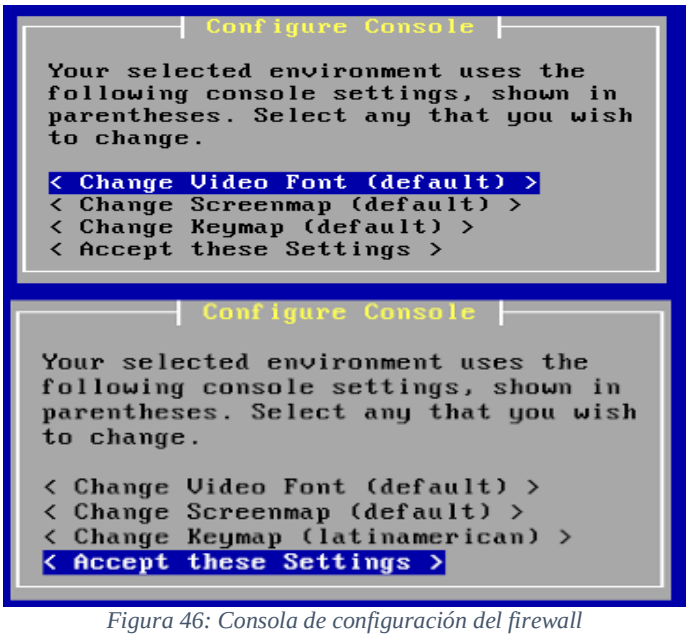


Figura 46: Consola de configuración del firewall

- Elegir la opción de instalación fácil y rápida

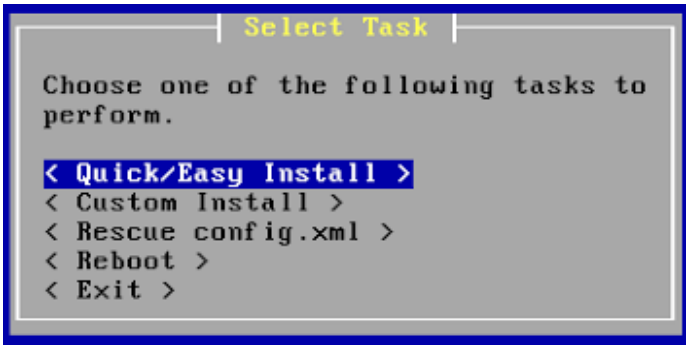


Figura 47: Opciones de instalación del firewall

- Reiniciar la consola para finalizar la instalación.

Figura 48: Interfaz de consola

- **Configuración inicial del Pfsense**
  - Para realizar la asignación y configuración de IP en las interfaces, se eligió la opción 2 “Set interface(s) IP address” y se estableció las IPs correspondientes.

Figura 49: Asignación de interfaces

  - Ingresar a la interfaz web de PfSense por medio de la interfaz LAN para realizar las configuraciones correspondientes. El usuario por defecto es “admin” y la contraseña es “Pfsense”.
- **Configuraciones generales de la interfaz gráfica del Pfsense**
  - En el menú System se encuentra la opción “Hostname”, que sirve para darle un nombre específico al firewall.
  - En la opción del DNS Servers se escribió la IP LAN del pfsense.
  - En el menú **Interfaces** se realizó la configuración de la LAN y WAN. Por defecto la LAN ya viene configurada desde la consola.

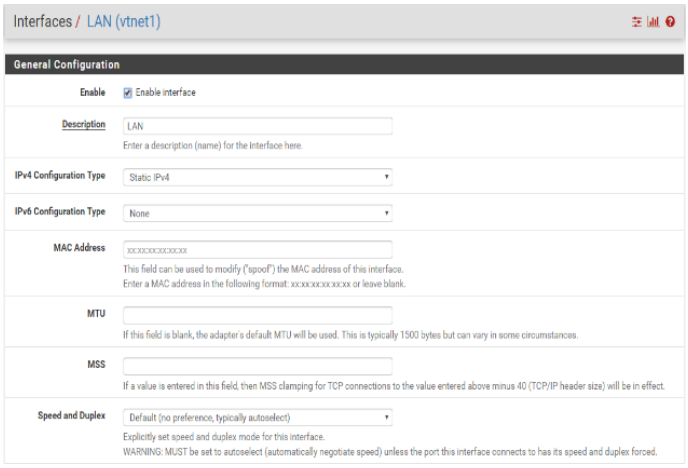


Figura 50: Configuración de interfaces

- **Paquetes de instalación del pfsense**
  - En el submenú de descarga "Package Manager" se realizó la descarga de los siguientes paquetes:

Nombre	Descripción
Lightsquid	Es una aplicación vía web, que a partir de los logs generados por Squid, nos genera informes detallados de consumo y acceso a la red de los equipos [27].
Squid	Es un servidor proxy para web con caché. Entre sus utilidades está la de mejorar el rendimiento de las conexiones de empresas y particulares a Internet guardando en caché peticiones recurrentes a servidores web y DNS, acelerar el acceso a un servidor web determinado o añadir seguridad realizando filtrados de tráfico [28].
SquidGuard	Sistema de filtrado combinado de redireccionamiento web, y el plugin del controlador de acceso para Squid. Utiliza una lista negra "Blacklists" como base de datos para denegar o permitir sitos web al usuario. Su mayor utilidad es la prevención de dominios o URLs que contengan informaciones no deseadas o nada productivas en horario laboral [29].
Suricata	Suricata es un sistema de detección de intrusiones basado en código abierto y un sistema de prevención de intrusiones [30].

Tabla 15: Paquetes de instalación del Pfsense

- **Configuración de DHCP**
  - Para el proceso de asignación de las máquinas se elaboró una lista donde se registraron las MACs de los equipos, IP address y el Hostname para etiquetar cada máquina por su nombre.

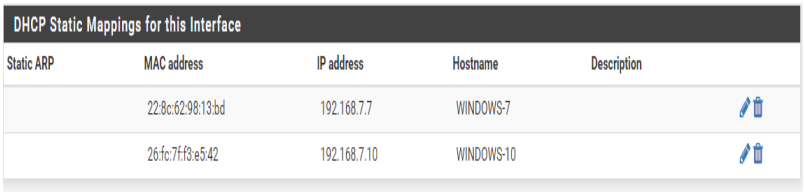


Figura 51: Configuración de DHCP estático

  - En el submenú Traffic Graph ubicado en el menú "Status" se verificó el tráfico del consumo de internet de las interfaces.

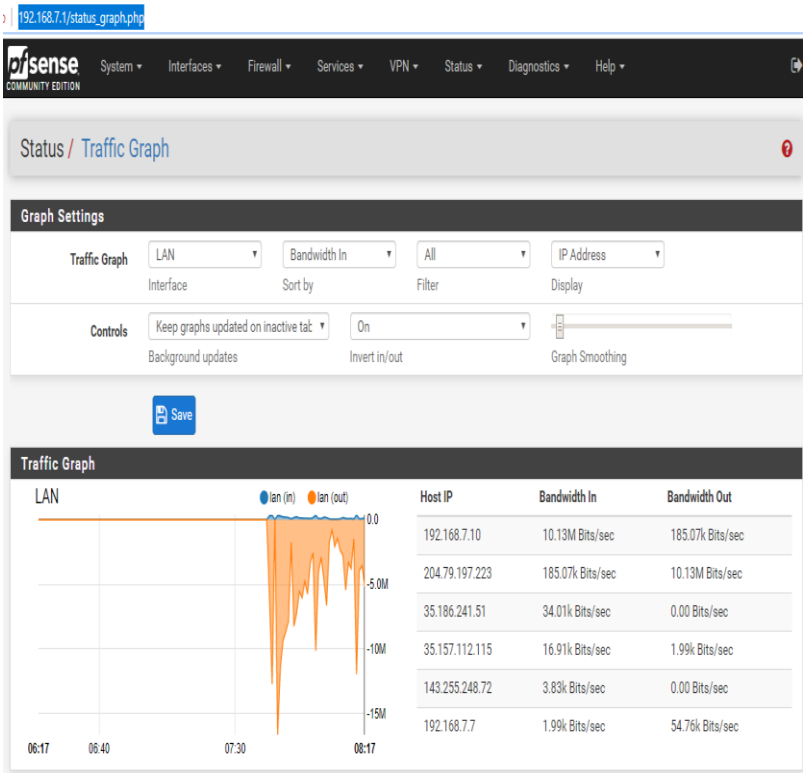


Figura 52: Tráfico de red de las máquinas virtuales

2.8.1.2. Análisis Estático

Fase de clasificación

- **Transferencia de malware**
  - Para realizar el análisis se tomaron muestras de malware en la red de los laboratorios de FACSISTEL.
  - Comprimir las muestras de malware y transferirlas a las máquinas víctimas

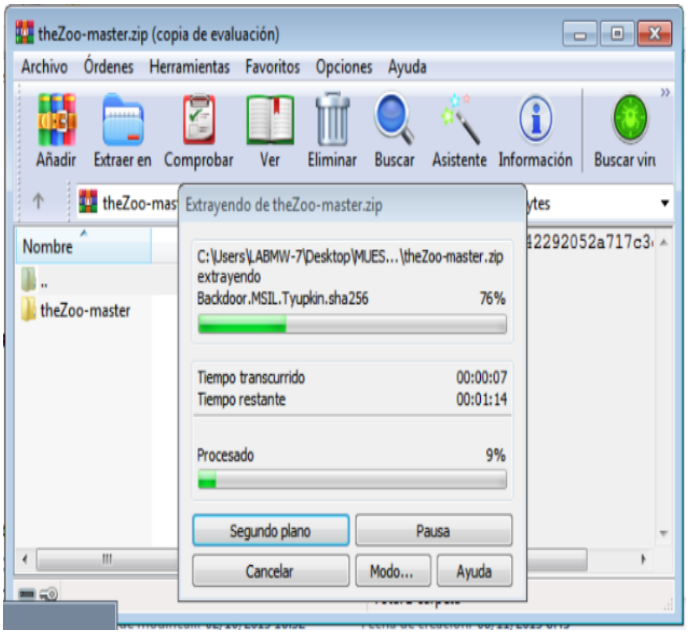


Figura 53: Transferencia de las muestras del malware

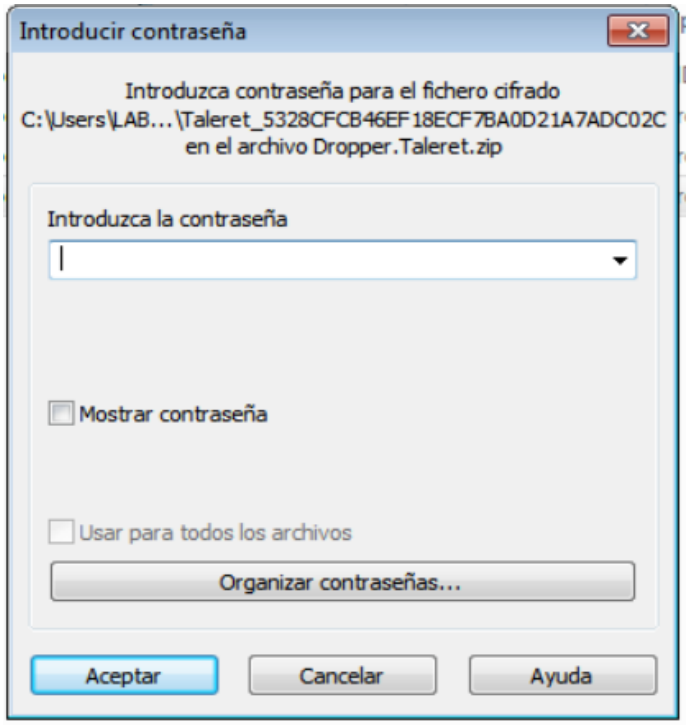


Figura 54: Transeferencia de muestras de malware

- **Identificación del malware**
  - Con la herramienta WinMD5 y MD5summer se procedió a calcular el hash md5 y SHA252 de cada malware, al igual que su tamaño y nombre del archivo. A continuación, se presentan los datos encontrados:

Nº	NOMBRE ARCHIVO	TAMAÑO	MD5	SHA256
1	hostr.exe	105.00 kb	5a559b6d223c79f3736dc52794636cfd	6f201afc797370ac6e33fafec41a794a2eb44c1bfd7d9079e3633ebe7bbb41e1
2	798_abroad.exe	1600.22 kb	f88e9b7446a6e57943728cce3cc70720	2fd5b075ab9dffe8b421a4942ecdac322d8f0fceca597a644a6a9e631901e8bc
3	abba_-_happy_new_year_zaycev_net.exe	190.40 kb	6c42954257ef80cc72266400236ea63c	3a93d0b4345900c5eddfaa574b721546312468a418f34b39bcefbbda9118b0cb
4	Win32.VBS.APT34Dropper	8,93 kb	b2d13a336a3eb7bd27612be7d4e334df	f83936a6169d91dab8cb31b27469bde584429695e87307452dc4e4293698383f
5	SDK320.msi	457.00 kb	32d5cca418b81e002bb3fdd8e4062bc9	6303ee28660f9d8bff4a494f96d681a2cebc72e5abc1ac3b0fdebcddbb7e0b8d
6	ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD	783.91 kb	e33af9e602cbb7ac3634c2608150dd18	8c870eec48bc4ea1aca1f0c63c8a82aaadaf837f197708a7f0321238da8b6b75
7	Cryptowall.bin	240.50 kb	47363b94cee907e2b8926c1be61150c7	45317968759d3e37282ceb75149f627d648534c5b4685f6da3966d8f6fca662d
8	Gchrome.exe	2861.50 kb	49fd4020bf4d7bd23956ea892e6860e9	d23b4a30f6b1f083ce86ef9d8ff434056865f6973f12cb075647d013906f51a2
9	Anti_EXE_BOOT.IMA	9.00 kb	a62f1bbe6d7fb1659ca418cc96235717	d9854b40b3827afa91d33a2ce1998716b3f8edf9bade7527334245fec127445a
10	1002.exe	251.00 kb	829dde7015c32d7d77d8128665390dab	5291232b297dfcb56f88b020ec7b896728f139b98cef7ab33d4f84c85a06d553
11	1003.exe	255.00 kb	0246bb54723bd4a49444aa4ca254845a	8cf50ae247445de2e570f19705236ed4b1e19f75ca15345e5f00857243bc0e9b
12	yesmile.exe	4.83 kb	bf586b1543e5f8131217069d520a1381	91fa185f353b790b4dfb3b468503244e4c84be8c43959b32d6821d764d5d0c41
13	zeroAccess_xxx-porn-movie.avi.exe	160.00 kb	a2611095f689fadffd3068e0d4e3e7ed	71b38f041b4a4ae169c44e3aff412e527e1156f92c27f1340a8abe70a45bee10

Tabla 16: Generación de huellas de archivo de los malwares

- **Comprobación del tipo de malware mediante Antivirus**

Se analizaron las muestras de malware con distintos antivirus para verificar los datos que detectaba cada uno de ellos. Además, se realizó un análisis comparativo para verificar qué antivirus posee mayor veracidad.

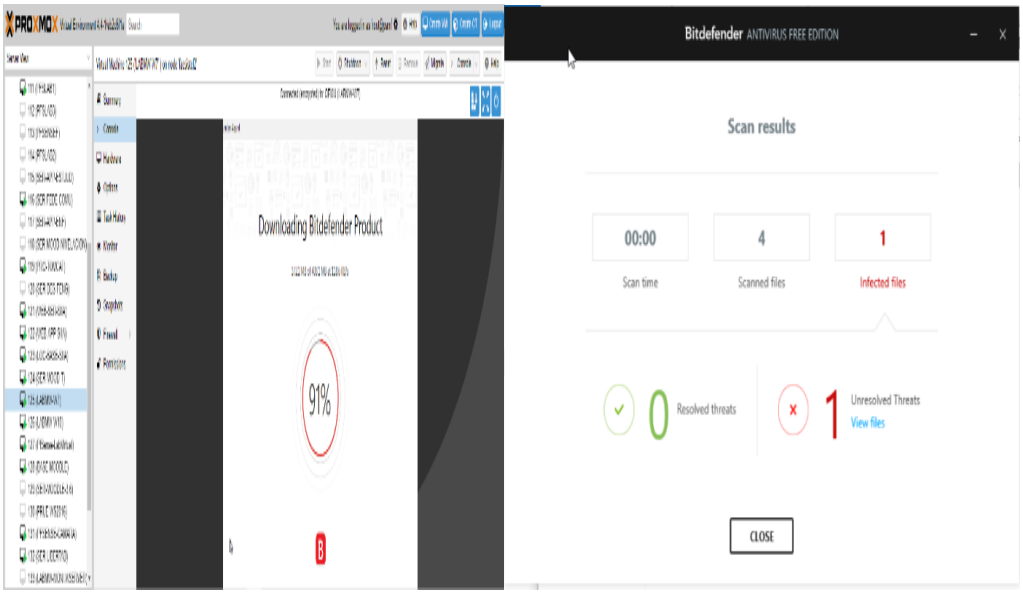


Figura 55: Antivirus Bitdefender

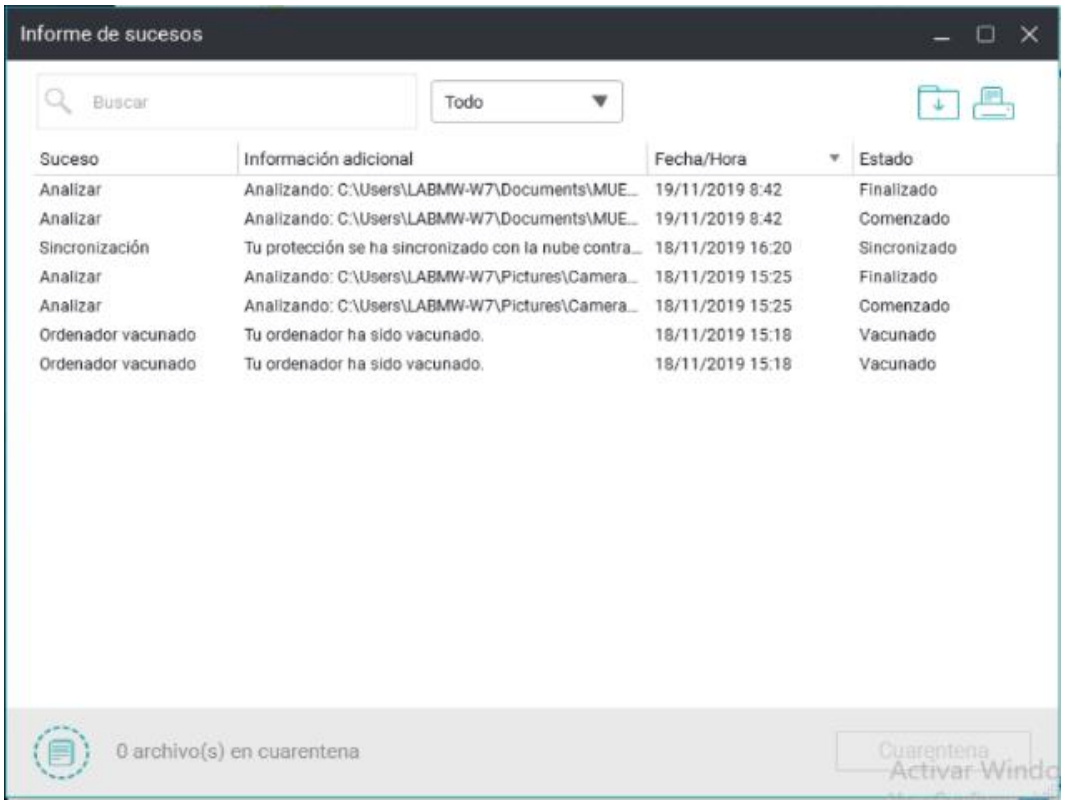


Figura 56: Antivirus Panda

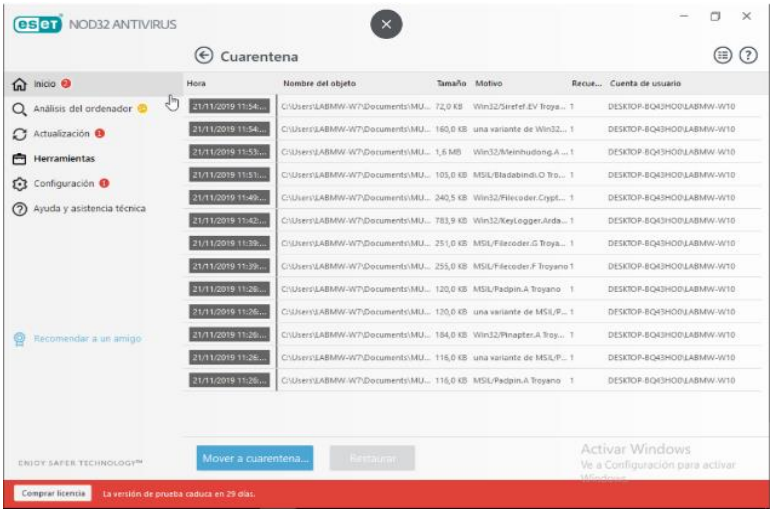


Figura 57: Antivirus ESET

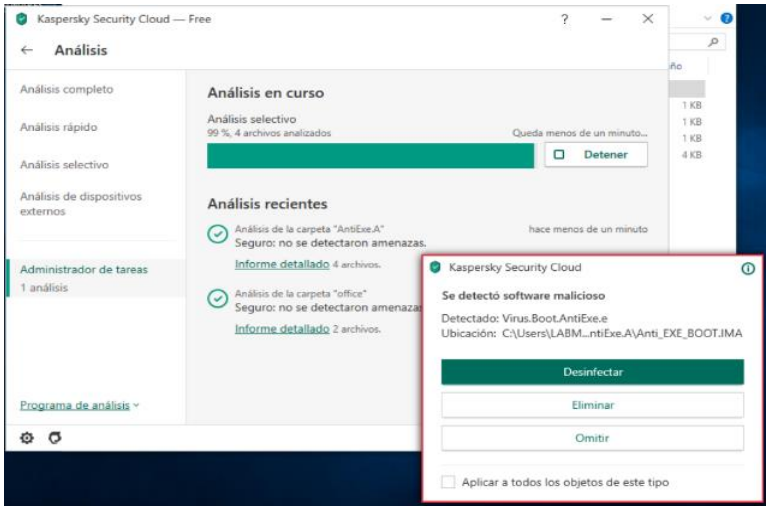


Figura 58: Antivirus Kaspersky

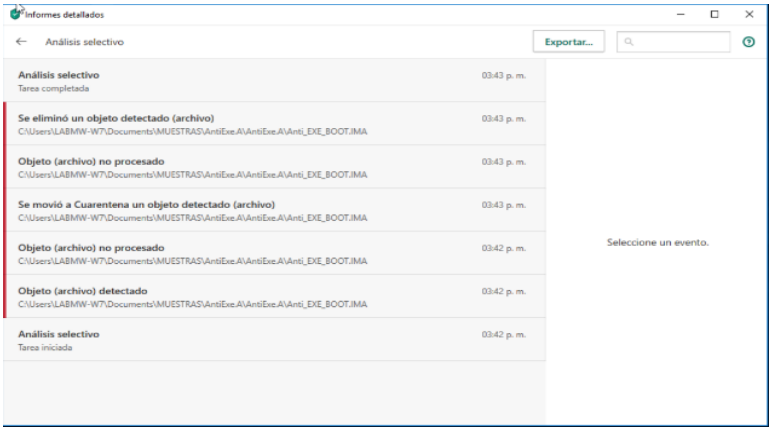


Figura 59: Antivirus Kaspersky

A continuación, se muestra el reporte generado:

NOMBRE DE LA MUESTRA	AVG	AVIRA	PANDA	BITDEFENDER	KASPERSKY	ESET
Trojan droppen	Win32:malware-gen	Tr/droppen.gen	**(No detectado)**	Trojan.agent.bild	Trojan-clicker.nsis.agent.a	Win32/meinhudong.a
Backdoor	Msil:tyupkin-a	Bds/agent.122880.16	**(No detectado)**	**(No detectado)**	Backdoor.win32.tyupkin.a	Msil/padpin.a trojano
Keylogger	Win32:ardamax-lv	Tr/spy.ardamax.ckp	Application/ardamax	Dropped:application.keylogger.ardamax.gen	Trojan-spy.win32.ardamax.cko	Win32/keylogger.ardamax.nbb
Ransware	Win32:androp	Tr/crypt.xpack.134743	Troyano	Trojan.genericd.2080196	Trojan.win32.agent.ieva	Win32/filecoder.cryptowall.d trojano
Trojan bladabin	Win32:malware-gen	Tr/barys.10755412	**(No detectado)**	Gen:variant.msilperseus.25588	Heur:trojan.win32.generic	Msil/bladabindi.o trojano
Proteus	Win32:dropper-gen	Heur/agen.1002645	Trj/ci.a	Gen:variant.razy.109057	Heur:trojan.msil.bluewushu.gen	Msil/proteus.a
Antixe.a	Antiexe	Antiexe	Virus	Antiexe.a	Virus.boot.antiexe.e	**(No detectado)**
Crypto locker	Win32:trojan-gen	Tr/ransom.grolf	Trj/ci.a	Gen:variant:ransom:blocker.3	Trojan-ransom.win32.blocker.dmcu	Msil/filecoder.f trojano
Dos	Yesmile-4304	Boo/yesmile	Virus	Yesmile.a	**(No detectado)**	**(No detectado)**
Zeroaccess	Win32:sirefef-buf	Tr/atraps.gen	Sospechoso	Gen:variant.sirefef.443	Trojan.win32.lampa.alej	Win32/sirefef.ev trojano
	Win32:malob-lj	Te/crypt.zpack.gen2	Sospechoso	Trojan.inject.akd	Backdoor.win32.zaccess.aqep	Win32/kryptik.argf trojano

Tabla 17: Datos obtenidos por los antivirus

Estos resultados comprueban que no todos los antivirus detectan los softwares maliciosos. Cabe indicar que las pruebas fueron realizadas tanto con antivirus de software libre como de licencia

Es importante resaltar que anteriormente no se contaba con un registro del comportamiento de malware en la Facultad. Sin embargo, el presente proyecto brinda los reportes necesarios con los registros de los malware analizados.

- **Búsqueda de cadenas de texto**
  - Descargar el software en la página oficinal McAffee http://www.mcafee.com/us/downloads/free-tools/bintext.aspx
  - Ejecutar la herramienta BinText, para escanear y extraer las cadenas de caracteres que se encuentran incrustadas en los archivos binarios.
  - En el botón "Browse" se debe elegir la ruta del archivo binario. Una vez elegida la ruta, dar clic en "Go" para realizar el escaneo.

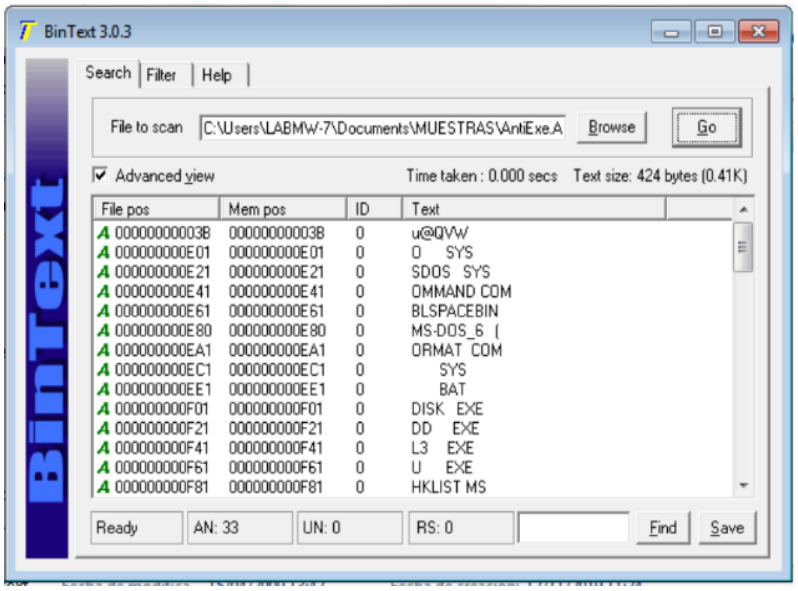


Tabla 18: Interfaz de la herramienta BinText

- **Identificación de técnicas de ofuscación**

  Para desarrollar esta actividad, la herramienta de aplicación propuesta es PEID, para analizar archivos ejecutables e identificar las técnicas de empaquetamiento, cifrado, polimorfismo y metamorfismo del malware.
  - Ejecutar el programa PEiD
  - En el casillero "File" ubicar la ruta del archivo malicioso y dar Enter.
  - La interfaz de PEiD permite obtener datos importantes del archivo como: compiladores, empacadores y criptores. A continuación, se muestra las interfaces de PEID:

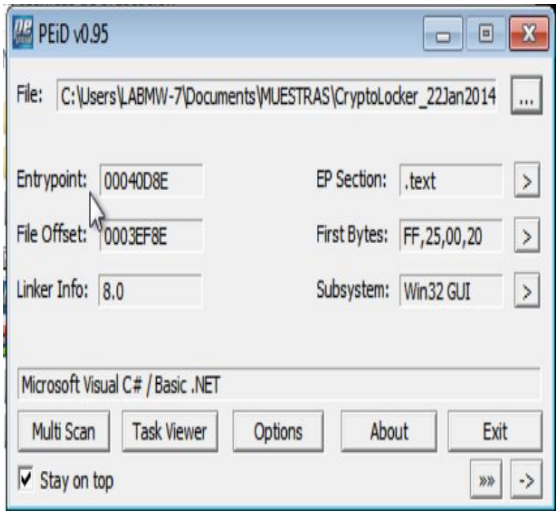


Figura 60: Interfaz principal

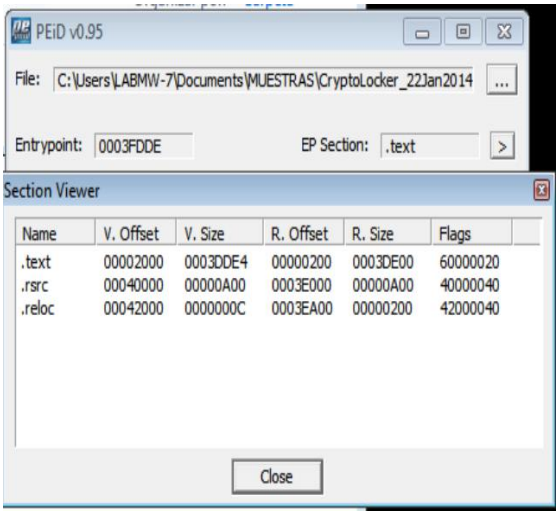


Figura 61: Visor de secciones

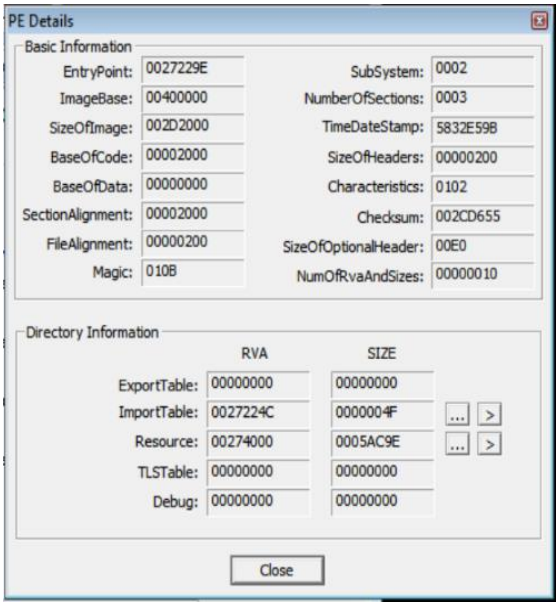


Figura 62: Detalles del archivo PE

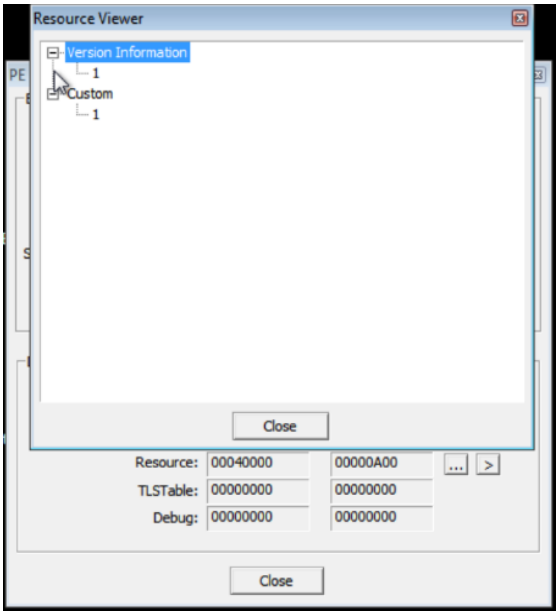


Figura 63: Visor de recursos

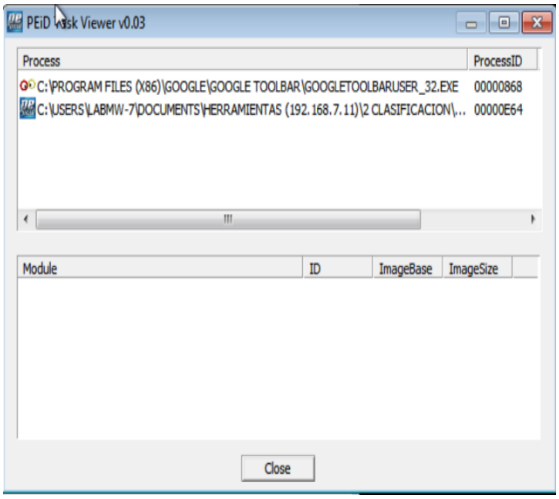


Figura 64: Visor de tareas

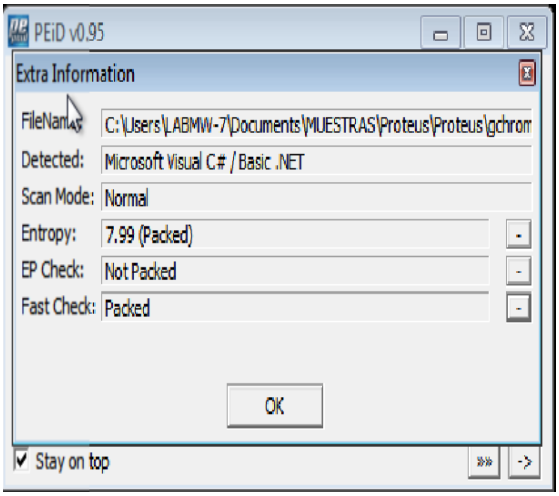


Figura 65: Información extra

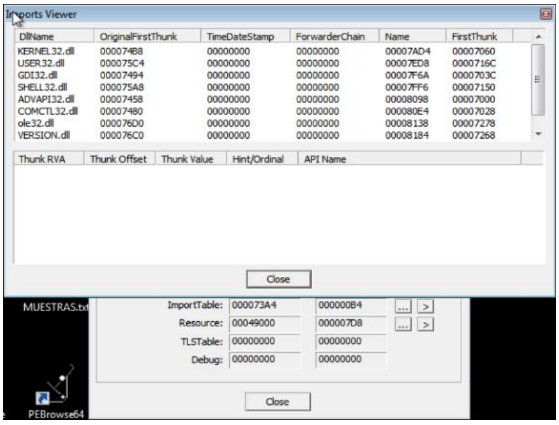


Figura 66: Visor de importación

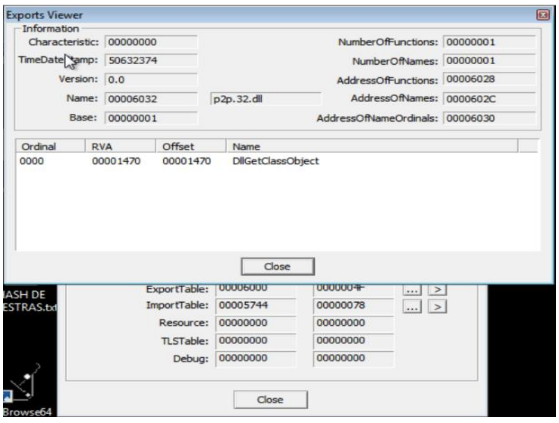


Figura 67: Visor de exportación

- **Formato y estructura del archivo**

  Para obtener información sobre el encabezado PE del malware se utilizó la herramienta PE EXPLORER que se obtuvo de la siguiente manera:

  - Descargar e instalar PE Explorer desde su página oficial http://www.pe-explorer.com/
  - En el menú File se selecciona el archivo a examinar. PE Explorer analizará el archivo y mostrará un resumen de la información del encabezado PE y de todos los recursos contenidos en el archivo PE.

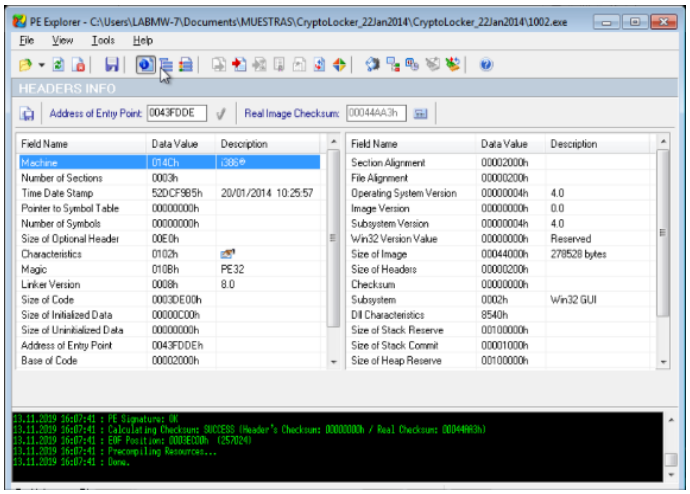


Figura 68: Interfaz principal de la herramienta PE Explorer

Para identificar los módulos y librerías del software malicioso con funciones más utilizadas por el malware, se utilizó la herramienta Dependency Walker, la misma que se instala mediante el siguiente procedimiento:

- Descargar e instalar Dependency Walker desde su página oficial http://www.dependencywalker.com/
- En el menú File se selecciona el archivo a examinar. Una vez examinado el archivo, mostrará los resultados de la siguiente manera:

- ✓ 1.- Análisis de Dependency Walker del archivo PE
- ✓ 2.- DLL que se importan
- ✓ 3.- En el panel superior derecha se muestra las funciones importadas.
- ✓ 4.- Enumera todas las funciones que pueden importarse.
- ✓ 5.- Los dos paneles inferiores enumeran información adicional sobre las versiones de DLL que se cargarían si ejecutara el programa y cualquier error informado, respectivamente.

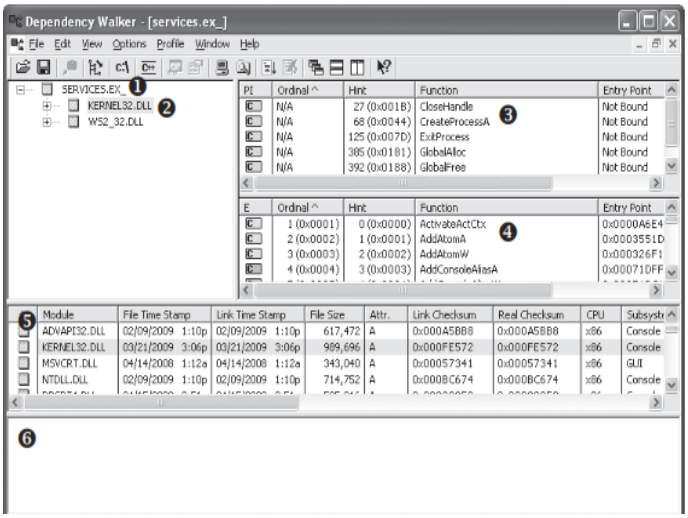


Figura 69: Herramienta Dependency Walker

Para obtener información global sobre el software malicioso, se utilizó la herramienta PEStudio. A continuación, se detalla el proceso de instalación:

- Descargar e instalar PEStudio
- En el menú File se selecciona el archivo a examinar.
- Los resultados se verifican mediante un código de color. El verde indica que no hay problemas, el naranja indica que es algo que debe analizar y el rojo los hallazgos más urgentes que se deben investigar.

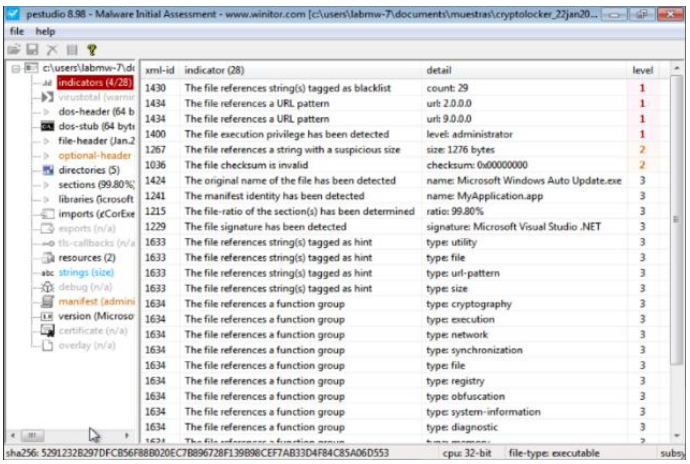


Figura 70: Interfaz principal de la herramienta PEStudio

Fase de análisis de código

Para desarrollar esta actividad es necesario utilizar el depurador OllyDBG en el análisis de los archivos. Esta herramienta se obtuvo de la siguiente manera:

- Descargar e instalar la herramienta OllyDBG
- En el menú File se selecciona el archivo a examinar y a continuación empezará a depurar el archivo.
- En la figura 55 se muestra la estructura de la interfaz de OllyDBG.

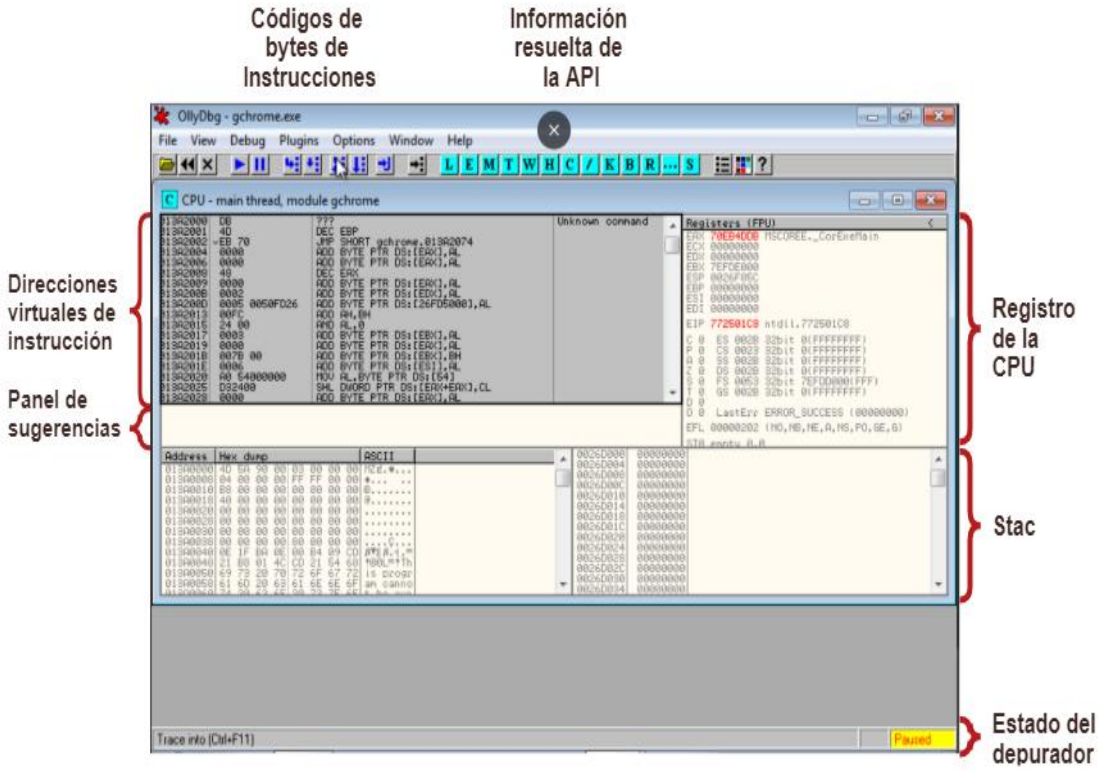


Figura 71: Estructura del software depurador OllyDBG

2.8.1.3. Análisis Dinámico

El análisis dinámico que permite observar el comportamiento del malware en ejecución se lo realizó en base a los siguientes lineamientos:

- **Ejecución del malware**
  - Realizar la ejecución del archivo malicioso
  - Una vez ejecutado el malware sobre la máquina, se capturó un snapshot mediante la herramienta Systracer, con el fin de apreciar el listado de cambios efectuados sobre el sistema.
  - Realizar la comparación de los snapshots antes y después de la infección para verificar los cambios efectuados

- **Análisis del comportamiento del malware**

Para verificar los cambios respecto a los archivos y procesos generados por el malware se utilizaron las herramientas: Disk Pulse, Process Explorer, Process Monitor y AutoRuns. Considerando lo siguiente:

- Descargar e instalar la herramienta Disk Pulse desde su página oficial http://www.diskpulse.com/downloads.html
- Para comenzar a monitorear un disco o unidad se debe ingresar la ruta del archivo en la entrada del directorio ubicada debajo de la barra de herramientas principal y presionar el botón 'Monitor' ubicado en la esquina superior izquierda de la barra de herramientas principal.
- En el cuadro de diálogo de perfil, verifique que todos los parámetros estén seleccionados correctamente y presione el botón 'Iniciar' para comenzar el proceso de monitoreo.
- De forma predeterminada, DiskPulse supervisará todos los cambios del sistema de archivos, incluidas las creaciones, modificaciones, cambios de nombre, cambios de atributos, operaciones de eliminación de archivos, etc.

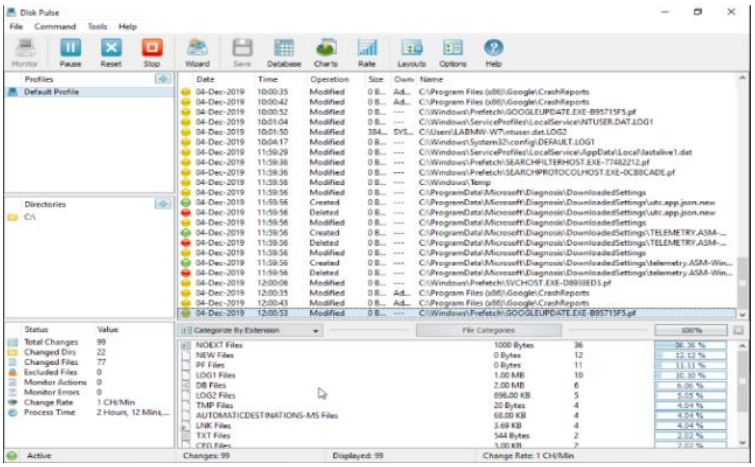


Figura 72: Interfaz de la herramienta Disk Pulse

- Descargar y ejecutar la herramienta Process Explorer desde su página oficial https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer
- Una vez ejecutada la herramienta, la interfaz principal muestra todos los procesos en ejecución
- Al pasar el cursor sobre el nombre del proceso este desplegará la línea de comando con la que se ejecuta, la ruta donde se encuentra el archivo y el servicio asociado ha dicho proceso.
- Para observar las estadísticas del proceso, se debe dar doble clic sobre el mismo.

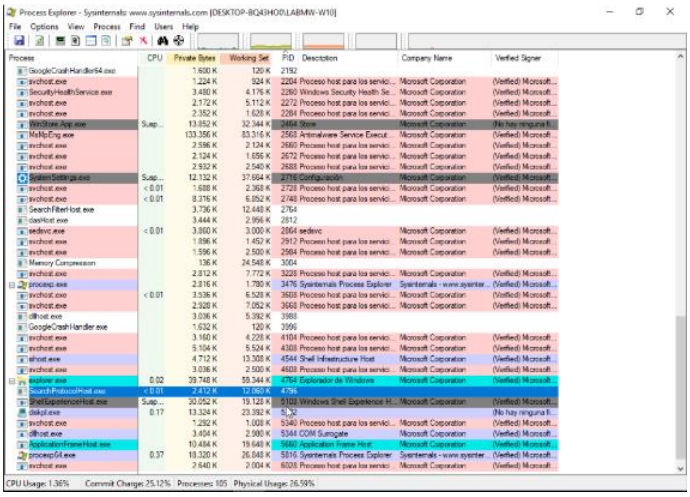


Figura 73: Interfaz de la herramienta Process Explorer

- Descargar y ejecutar la herramienta Process Monitor
- Una vez ejecutada la herramienta, la interfaz principal muestra los siguientes datos:
    - ✓ **Hora:** muestra la hora exacta en que ocurrió un evento.
    - ✓ **Nombre del proceso:** el nombre del proceso que generó el evento.
    - ✓ **PID:** el ID del proceso que generó el evento.
    - ✓ **Operación:** nombre de la operación que se está registrando, y hay un icono que coincide con uno de los tipos de eventos (registro, archivo, red, proceso).
    - ✓ **Ruta:** esta no es la ruta del proceso, es la ruta a lo que sea que este evento haya estado trabajando.
    - ✓ **Resultado:** muestra el resultado de la operación, que codifica como ÉXITO o ACCESO DENEGADO.
    - ✓ **Detalle:** muestra información adicional.

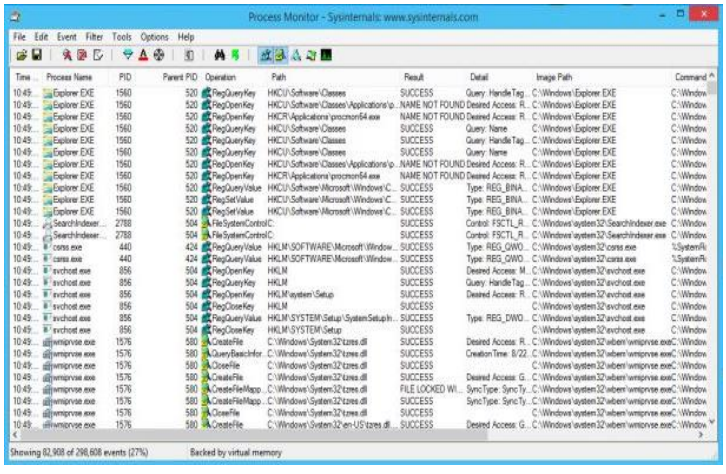


Figura 74: Interfaz de la herramienta Process Monitor

2.8.2. REPORTES DEL ANÁLISIS DEL MALWARE

Los resultados generados por el laboratorio virtual se presentan de manera detallada en las siguientes matrices:

2.8.2.1. Reporte general del análisis de malware

Los resultados de este reporte reflejan las siguientes categorías:

NOMBRE ARCHIVO	MD5	TIPO	DETALLE	RIESGOS	MODO DE INFECCIÓN
hostr.exe	5a559b6d223c79f3736dc52794636cfd	Troyano	Es un malware de tipo troyano que infecta ordenadores con sistema operativo Windows con el objetivo de ejecutar programas información del usuario o ejecutar procesos maliciosos	Este troyano puede para robar información confidencial de los ordenadores infectados, como por ejemplo direcciones IPs visitadas por los usuarios, contraseñas o datos del sistema operativo. Además esta amenaza puede descargar y ejecutar archivos, conectarse a servidores remotos o manipular el registro.	Este malware se propaga a través del uso de unidades extraíbles contaminadas, como por ejemplo memorias USB. Bladabindi crea un acceso directo con el nombre e icono de la unidad, al hacer clic en este acceso directo el malware se ejecuta y el Explorador de Windows se abre, ocultando así su presencia.
798_abroad.exe	f88e9b7446a6e57943728cce3cc70720	Adware	Es un Adware capaz de ejecutar varias tareas, como instalar otros malware, reunir datos sensibles o mostrar anuncios cuestionables mientras navegas por la web	Este Adware pued descargar, instalar o ejecutar un malware en el ordenador; operar como keylogger y reunir datos sensibles, incluyendo usuario, contraseña, información bancaria, etc.; permitir el acceso remoto al ordenador afectado; mostrar pop-ups agresivos, banners, anuncios textuales y otros anuncios que pueden no solo ser molestos sino también maliciosos.	Hay numerosos modos en los que el malware Win32: Malware-gen puede entrar en el sistema. Sin embargo, la mayor parte del tiempo viajan a través de ofuscados archivos adjuntos en emails, programas crackeados o falsas actualizaciones.
abba_-_happy_new_year_zaycev_net.exe	6c42954257ef80cc72266400236ea63c	Troyano	Es un troyano que abre puertas traseras que le permite a un atacante robar información confidencial, incluido el nombre de usuario y las contraseñas que se almacenan en la PC.	Este troyano puede arruinar todo el sistema y robar información personal. Además, este virus pone en peligro la privacidad de los usuarios de computadoras porque Trojan puede crear una puerta trasera y conectarse a un servidor remoto, lo que permite a un atacante remoto obtener el control de la computadora comprometida.	1. Videos para adultos en sitios web no seguros 2. La barra de herramientas falsa redirige el navegador web 3. Los correos electrónicos no deseados que contienen el enlace o archivo adjunto myfile.exe 4. Falsificación de archivos torrent o archivos en redes de intercambio de archivos 5. Páginas web que contiene hazañas
Win32.VBS.APT34Dropper	b2d13a336a3eb7bd27612be7d4e334df	Troyano	Fue creado para ejecutar una serie de comandos una vez que entra al sistema. Recopilará datos como la configuración del sistema, la versión de Windows, la configuración de red, etc. Los datos recopilados se enviarán al atacante remoto para su análisis.	Este troyano hará una copia de sí mismo en los archivos del sistema. Luego, se crea una entrada de registro para llamar al archivo en cada arranque de Windows. Aparte de eso, este malware también eliminará archivos no maliciosos en varias carpetas de la PC comprometida.	Se propaga adjuntando su código a otros archivos en la PC o red.

ArdamaxKeylogger	e33af9e602cbb7ac3634c2608150dd18	Keylogger	Es un keylogger comercial que rastrea la actividad en línea del usuario y registra cada pulsación de tecla escrita.	Ardamax puede poner en riesgo los datos personales financieros y privados más confidenciales del usuario.	Ardamax Keylogger debe instalarse manualmente
cryptowall.bin	47363b94cee907e2b8926c1be61150c7	Ransomware	Es un virus tipo ransomware (bloqueador de sistemas) que se infiltra en el sistema operativo del usuario	Tras entrar en el sistema con éxito, este programa malicioso encripta los archivos almacenados en el PC del usuario	Se infiltra en el sistema operativo del usuario a través de un mensaje de email infectado o una descarga fraudulenta
gchrome.exe	49fd4020bf4d7bd23956ea892e6860e9	Botnet	Lanza un ataque de varias capas en una máquina infectada donde ejecuta varios procesos destinados a la extracción de monedas, el robo de credenciales y el registro de claves. Además, el bot puede funcionar solo; Ofrece al cibercriminal enviar comandos a través de HTTP para descargar ejecutables maliciosos y ejecutarlos.	Opera como proxy, minero de cripto monedas, keylogger, descargador de malware y revisa cuentas de comercio electrónico.	Puede esconderse en adjuntos de emails de spam, ejecutándose en webs hackeadas, IRC (Internet Relay Chat), redes P2P Peer-to-Peer para compartir archivos, etc.
Anti_EXE_BOOT.IMA	a62f1bbe6d7fb1659ca418cc96235717	Virus	Infecta el registro de inicio maestro (MBR) y los sectores de inicio de DOS (DBS). AntiEXE se propaga solo cuando hay un intento de iniciar el sistema desde un disquete infectado.	Infecta los registros de arranque de disquete y los registros de arranque maestro del disco duro	El virus solo infecta los discos duros cuando se intenta arrancar desde un disquete infectado. Una vez que el virus ha infectado el disco duro, se infectarán todos los disquetes no protegidos contra escritura utilizados en la máquina.
1002.exe	829dde7015c32d7d77d8128665390dab	Troyano	Se ejecuta en la computadora, afecta en gran medida el rendimiento general del sistema. Pueden consumir recursos más de lo que la PC puede manejar, por lo tanto, provocará fallas del sistema.	El troyano instala varios programas nuevos en el equipo que harán que aparezcan anuncios emergentes en la pantalla e incluso desactiven el firewall.	Se instala en el ordenador cuando se descarga un códec de vídeo infectado o al abrir un archivo adjunto de correo infectado
1003.exe	0246bb54723bd4a49444aa4ca254845a	Ransware	Esta amenaza puede realizar una serie de acciones de elección de un hacker malicioso en su PC.	Este ransomware puede impedir usar la PC o acceder a los datos.	Esta amenaza utiliza un archivo infectado de Microsoft Office para descargar el ransomware en la PC. Puede llegar a la PC como archivo adjunto de correo electrónico no deseado, generalmente como un archivo de Word (.doc).
yesmile.exe	bf586b1543e5f8131217069d520a1381	BackDoor	Este es un virus multipartito y también sigiloso, por lo que no puede verlo en archivos o sectores de arranque cuando reside en la memoria.	Este Backdoor infecta MBR en discos duros y archivos COM y EXE cuando se ejecutan.	Este virus se propaga adjuntando su código a otros archivos en la PC o red. Es posible que algunos de los programas infectados ya no se ejecuten correctamente.
zeroAccess_xxx-porn-movie.avi.exe	a2611095f689fadffd3068e0d4e3e7ed	Botnet	Afecta los sistemas operativos de Windows. Se usa para descargar otro malware en una máquina infectada desde una botnet mientras permanece oculto usando técnicas de rootkit .	Crea un sistema de archivos ocultos Descarga más malware a la computadora infectada Roba contraseñas, tarjetas de crédito y otra información personal	Por lo general, se propaga a través de Internet, como los sitios web interactivos y enlaces

Tabla 19: Reporte general del análisis de malware

2.8.2.2. Reporte técnico del comportamiento del malware

En base a los resultados emitidos por las herramientas en el análisis estático y dinámico se muestra el comportamiento de cada código malicioso examinado:

MALWARE: BLADABINDI.EXE	
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**
Establecer elemento de inicio	C: \ Documents and Settings \ Administrator \ 「开始」 菜单 \ 程序 \ 启动 \ ec83b2d446200dcd0392570446c898a3.exe
Crea un archivo	C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ hostr.exe C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ hostr.exe.tmp
Crea un archivo ejecutable	C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ hostr.exe C: \ Documents and Settings \ Administrator \ 「开始」 菜单 \ 程序 \ 启动 \ ec83b2d446200dcd0392570446c898a3.exe
Establecer elemento de inicio	C: \ Documents and Settings \ Administrator \ 「开始」 菜单 \ 程序 \ 启动 \ ec83b2d446200dcd0392570446c898a3.exe
Encontrar archivo	FileName = C: \ WINDOWS \ Microsoft.NET \ Framework \ v4.0.30319 \ mscoreei.dll FileName = C: \ WINDOWS \ Microsoft.NET \ Framework \\ * FileName = C: \ WINDOWS FileName = C: \ WINDOWS \ WinSxS FileName = C: \ WINDOWS \ WinSxS \ x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.4053_x-ww_e6967989 \ MSVCR80.dll FileName = C: \ WINDOWS \ assembly \ GAC_32 \ mscorlib \ 2.0.0.0__b77a5c561934e089 \ mscorlib.INI FileName = C: \ Documents and Settings \ Administrador \ Configuración local \ Temp FileName = C: \ Documents and Settings \ Administrador \ Configuración local \% temp% FileName = C: \ Documents and Settings \ Administrador \ Configuración local \% temp% \ ****. Exe FileName = C: \ Documents and Settings FileName = C: \ Documents and Settings \ Administrador FileName = C: \ Documents and Settings \ Administrador \ Configuración local FileName = C: \ Documents and Settings \ Administrador \ Configuración local \% temp% \ 996E.INI FileName = C: \ WINDOWS \ assembly \ GAC_MSIL \ Microsoft.VisualBasic \ 8.0.0.0__b03f5f7f11d50a3a \ Microsoft.VisualBasic.INI FileName = C: \ WINDOWS \ assembly \ GAC_MSIL \ System.Windows.Forms \ 2.0.0.0__b77a5c561934e089 \ System.Wi
Modificar archivo	C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ hostr.exe ---> Offset = 0 C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ hostr.exe ---> Offset = 65536 C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ hostr.exe ---> Offset = 4096 C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ hostr.exe ---> Offset = 8192 C: \ Documents and Settings \ Administrator \ 「开始」 菜单 \ 程序 \ 启动 \ ec83b2d446200dcd0392570446c898a3.exe ---> Offset = 0 C: \ Documents and Settings \ Administrator \ 「开始」 菜单 \ 程序 \ 启动 \ ec83b2d446200dcd0392570446c898a3.exe ---> Offset = 65536 C: \ Documents and Settings \ Administrator \ 「开始」 菜单 \ 程序 \ 启动 \ ec83b2d446200dcd0392570446c898a3.exe ---> Offset = 4096 C: \ Documents and Settings \ Administrator \ 「开始」 菜单 \ 程序 \ 启动 \ ec83b2d446200dcd0392570446c898a3.exe --->
Modificar registro	\ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ ShellNoRoam \ MUICache \ C: \ DOCUME ~ 1 \ ADMINI ~ 1 \ LOCALS ~ 1 \ Temp \ hostr.exe

	\ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Tracing \ FWCFG \ EnableFileTracing \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Tracing \ FWCFG \ EnableConsoleTracing \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Tracing \ FWCFG \ FileTracingMask \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Tracing \ FWCFG \ ConsoleTracingMask \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Tracing \ FWCFG \ MaxFileSize \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Tracing \ FWCFG \ FileDirectory \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Tracing \ Microsoft \ NAP \ Netsh \ LogSessionName \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Tracing \ Microsoft \ NAP \ Netsh \ Active \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Tracing \ Microsoft \ NAP \ Netsh \ ControlFlags \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Tracing \ Microsoft \ NAP \ Netsh \ Napmontr \ Guid \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Tracing \ Microsoft \ NAP \ Netsh \ Napmontr \ BitNames \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Tracing \ Microsoft \ qagent \ LogSessionName \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Tracing \ Microsoft \ qagent \ Active \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Tracing \ Microsoft \ qagent \ ControlFl
Modificar registro de inicio	\ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ ec83b2d446200dcd0392570446c898a3 \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run \ ec83b2d446200dcd0392570446c89
Modificar el registro del proceso confiable del firewall	\ REGISTRY \ MACHINE \ SYSTEM \ ControlSet002 \ Services \ SharedAccess \ Parameters \ FirewallPolicy \ StandardPro
Modificar el registro de la variable de entorno	\ REGISTRO \ USUARIO \ S - * \ Medio ambiente \ SEE_MASK_NOZONECHECKS

Tabla 20: Reporte del comportamiento del malware Bladabindi.exe

MALWARE: DROPPER GEN.EXE		
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**	
Modificar el registro del proceso confiable del firewall	\ REGISTRY \ MACHINE \ SYSTEM \ ControlSet002 \ Services \ SharedAccess \ Parameters \ FirewallPolicy \ StandardProfile \ AuthorizedApplications \ List \ C: \ Documents and Settings \ Administrator \ Local Settings \ Temp \ nsf3.tmp \ ailiao.exe \ REGISTRY \ MACHINE \ SYSTEM \ ControlSet002 \ Services \ SharedAccess \ Parameters \ FirewallPolicy \ StandardProfile \ AuthorizedApplications \ List \ C: \ Program Files \ ailiao \ ailiao.exe	
Crea un archivo	C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsz2.tmp C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ System.dll C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ ailiao.exe C: \ Documentos y configuraciones \ Todos los usuarios \ Datos de aplicación \ ailiaoweb \ webico.ico C:\DocumentsAndSettings\Administrador\ConfiguraciónLocal\ArchivosTemporalesInternet\Content.IE5\C1OS62RY\ api [1].ashx C: \ Documents and Settings \ Administrador \ Configuración local \ Archivos temporales de Internet \ Content.IE5 \ C1OS62RY \ index [1] .php	C: \ Archivos de programa \ ailiao \ ailiao.exe C: \ Archivos de programa \ ailiao \ ailiaotp.exe C: \ Archivos de programa \ ailiao \ aldesk.exe C: \ Archivos de programa \ ailiao \ ailiaou.exe C: \ Archivos de programa \ ailiao \ uninst.exe C: \ Archivos de programa \ ailiao \ ailiao.lnk C: \ WINDOWS \ wininit.ini
Agregar acceso directo a una ubicación sensible	C: \ Documentos y configuraciones \ Todos los usuarios \ **「开始」 菜**单 \ **程序** \ 爱聊 \ 爱聊 .lnk C: \ Documentos y configuraciones \ Todos los usuarios \ **「开始」 菜**单 \ **程序** \ 爱聊 \ **卸**载 爱聊 .lnk	

Crear archivo ejecutable	C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ System.dll C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ ailiao.exe C: \ Archivos de programa \ ailiao \ ailiao.exe	C: \ Archivos de programa \ ailiao \ ailiaotp.exe C: \ Archivos de programa \ ailiao \ aldesk.exe C: \ Archivos de programa \ ailiao \ ailiaou.exe C: \ Archivos de programa \ ailiao \ uninst.exe
Eliminar archivo	C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsz2.tmp C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp C: \ Documents and Settings \ Administrador \ Configuración local \ Archivos temporales de Internet \ Content.IE5 \ C1OS62RY \ api [1] .ashx C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ System.dll	
Modificar archivo	C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ System.dll ---> Offset = 0 C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ ailiao.exe ---> Offset = 0 C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ ailiao.exe ---> Offset = 27737 C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ ailiao.exe ---> Offset = 60505 C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ ailiao.exe ---> Offset = 62876 C: \ Documents and Settings \ Administrador \ Configuración local \ Temp \ nsf3.tmp \ ailiao.exe ---> Offset = 95644 C: \ Archivos de programa \ ailiao \ ailiaotp.exe ---> Offset = 60505 C: \ Archivos de programa \ ailiao \ ailiaotp.exe ---> Offset = 62876 C: \ Archivos de programa \ ailiao \ ailiao.exe ---> Offset = 0 C: \ Archivos de programa \ ailiao \ ailiaotp.exe ---> Offset = 0	C: \ Archivos de programa \ ailiao \ ailiao.exe ---> Offset = 27737 C: \ Archivos de programa \ ailiao \ ailiao.exe ---> Offset = 60505 C: \ Archivos de programa \ ailiao \ ailiao.exe ---> Offset = 62876 C: \ Archivos de programa \ ailiao \ ailiao.exe ---> Offset = 95644 C: \ Archivos de programa \ ailiao \ ailiaotp.exe ---> Offset = 27737
Modificar registro	\ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Rutas de aplicación \ ailiao \ \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Desinstalar \ 爱聊 \ DisplayName \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Uninstall \ 爱聊 \ UninstallString \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Uninstall \ 爱聊 \ DisplayIcon \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Uninstall \ 爱聊 \ DisplayVersion \ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Uninstall \ 爱聊 \ URLInfoAbout \ REGISTRY \ MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Uninstall \ 爱聊 \ Publisher \REGISTRO\USUARIO\S -*\Software\Microsoft\Internet Explorer\Principal\FeatureControl\FEATURE_BROWSER_EMULATION\ ailiao.exe \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Configuración de Internet \ Conexiones	\ REGISTRO \ MÁQUINA \ SOFTWARE \ ailiao \ ailiaofilename \ REGISTRO \ MÁQUINA \ SOFTWARE \ ailiao \ ailiaofiledir \ REGISTRO \ MÁQUINA \ SOFTWARE \ ailiao \ ailiaosvrname \ REGISTRO \ MÁQUINA \ SOFTWARE \ ailiao \ UpdateVer \ REGISTRO \ USUARIO \ S - * \ Software \ ailiao \ UpdateVer \ REGISTRO \ USUARIO \ S - * \ Software \ ailiao \ sptime
Eliminar elemento de registro	\ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Configuración de Internet \ ProxyServer \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Configuración de Internet \ ProxyOverride \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Configuración de Internet \ AutoConfigURL	

Tabla 21: Reporte del comportamiento del malware DropperGen.exe

MALWARE: MYFILE.EXE	
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**
Establecer propiedad de directorio especial	C: \ Documents and Settings \ Administrador \ Configuración local \ Archivos temporales de Internet C: \ Documents and Settings \ Administrador \ Configuración local \ Historial C: \ Documents and Settings \ Administrador \ Configuración local \ Archivos temporales de Internet \ Content.IE5 C: \ Documentos y configuraciones \ Administrador \ Cookies C: \ Documentos y configuraciones \ Administrador \ Configuración local \ Historial \ Historial.IE5
Crea un archivo	C: \ Documents and Settings\Administrador\Configuración local \ Archivos temporales de Internet \ Content.IE5 \ C1OS6
Eliminar archivo	C: \ Documents and Settings\Administrador\Configuración local \ Archivos temporales de Internet \ Content.IE5 \ C1OS6
Modificar registro	\ REGISTRO \ USUARIO \ S - * \Software\Microsoft\Windows\CurrentVersion \ Configuración de Internet \ Conexiones \ SavedLegacySettings
Eliminar elemento de registro	\ REGISTRO \ USUARIO \ S - * \Software\Microsoft\ Windows\ CurrentVersion\ Configuración de Internet \ ProxyServer \ REGISTRO \ USUARIO \ S - * \Software\Microsoft\Windows\CurrentVersion\Configuración de Internet \ ProxyOverride \ REGISTRO \ USUARIO \ S - * \Software\Microsoft\Windows\CurrentVersion\Configuración de Internet \ AutoConfigURL

Tabla 22: Reporte del comportamiento del malware MyFile.exe

MALWARE: GCHROME.EXE	
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**
Archivos escritos	%APPDATA%\chrome.exe %HOMEPATH%\my documents\new text document.txt %APPDATA%\tamir.sharpssh.dll
Archivos con atributos modificados	%APPDATA%\chrome.exe
Claves de registro eliminadas	<HKLM>\SOFTWARE\Microsoft\ESENT\Process\mlfot\DEBUG\Trace Level <HKLM>\SOFTWARE\Microsoft\ESENT\Process\chrome\DEBUG\Trace Level
Procesos creados	<PATH_SAMPLE.EXE> %APPDATA%\chrome.exe <SYSTEM32>\wbem\wmiprvse.exe
Módulos de tiempo de ejecución	%APPDATA%\tamir.sharpssh.dll

Tabla 23: Reporte del comportamiento del malware Gchrome.exe

MALWARE: WIN32.VBS.APT34DROPPER	
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**
Archivos escritos	C:\ProgramData\Windows\Microsoft\Java\4E151F12A80F C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\FRM486C2GA3I8YRB6F31.temp C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\W5LHIBPL7VLDOH8MR6QC.temp

	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1da6d.TMP C:\ProgramData\Windows\Microsoft\java\dUpdateCheckers.ps1 C:\Windows\cerCAAD.tmp C:\ProgramData\Windows C:\ProgramData\Windows\Microsoft C:\ProgramData\Windows\Microsoft\java C:\ProgramData\Windows\Microsoft\java\GoogleUpdateschecker.vbs C:\ProgramData\Windows\Microsoft\java\cUpdateCheckers.bat C:\ProgramData\Windows\Microsoft\java\dUpdateCheckers.base C:\ProgramData\Windows\Microsoft\java\hUpdateCheckers.base C:\ProgramData\Windows\Microsoft\java\hUpdateCheckers.ps1 C:\Windows\cerCA02.tmp C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\OMBWPNJQPS5LM3K7Y581.temp C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF3d051.TMP C:\Windows\cerC6CC.tmp C:\ProgramData\Windows\Microsoft\Java\5DF85E052078 C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\D0AKPOMY521BK910AQY6.temp C:\Windows\cerC276.tmp	
Archivos eliminados	C:\ProgramData\Windows\Microsoft\java\dUpdateCheckers.base C:\ProgramData\Windows\Microsoft\java\hUpdateCheckers.base C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\FRM486C2GA3I8YRB6F31.temp C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\W5LHIBPL7VLDOH8MR6QC.temp C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF1da6d.TMP C:\Windows\cerCAAD.tmp C:\ProgramData\Windows\Microsoft\java\cUpdateCheckers.bat C:\Windows\cerCA02.tmp C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\OMBWPNJQPS5LM3K7Y581.temp C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF3d051.TMP C:\Windows\cerC6CC.tmp C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\D0AKPOMY521BK910AQY6.temp C:\Windows\cerC276.tmp	
Claves de registro abiertas	HKEY_USERS\.DEFAULT\Software\Microsoft\Windows Script Host HKEY_USERS\.DEFAULT\Software\Microsoft\Windows Script Host\Settings HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings
Procesos creados	C:\Windows\System32\schtasks.exe C:\Windows\System32\whoami.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\wscript.exe C:\Windows\System32\certutil.exe C:\Windows\System32\cmd.exe
Módulos en tiempo de ejecución	advapi32.dll kernel32.dll	RasPbFile RTUTILS.DLL

	comctl32.dll KERNEL32 SHLWAPI.dll KERNEL32.dll USER32.dll GDI32.dll ADVAPI32.dll Secur32.dll NTDLL.DLL ws2_32 RASAPI32.DLL	rpcrt4.dll ntdll.dll netapi32.dll DisableImprovedZoneCheck WS2HELP.dll hnetcfg.dll C:\WINDOWS\System32\wshtcpip.dll C:\WINDOWS\system32\MSCTF.dll C:\WINDOWS\system32\msctfime.ime C:\WINDOWS\system32\Msctf.dll

Tabla 24: Reporte del comportamiento del malware Win32.vbs.apt34dropper

MALWARE: KEYLOGGER.EXE		
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**	
Archivos escritos	C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\@1.tmp C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\@2.tmp C:\WINDOWS\system32\28463\DPBJ.001 C:\WINDOWS\system32\28463\DPBJ.006 C:\WINDOWS\system32\28463\DPBJ.007 C:\WINDOWS\system32\28463\DPBJ.exe C:\WINDOWS\system32\28463\key.bin C:\WINDOWS\system32\28463\AKV.exe C:\WINDOWS\system32\28463\DPBJ.009 C:\WINDOWS\system32\28463\May_31_2013__13_29_53.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_54.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_55.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_56.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_57.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_58.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_59.jpg C:\WINDOWS\system32\28463\May_31_2013__13_30_01.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_54.jpg	C:\WINDOWS\system32\28463\May_31_2013__13_30_02.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_37.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_38.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_39.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_40.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_41.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_42.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_43.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_44.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_45.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_46.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_47.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_48.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_49.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_50.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_51.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_52.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_53.jpg
Archivos eliminados	C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\@1.tmp C:\WINDOWS\system32\28463\DPBJ.005.tmp C:\WINDOWS\system32\28463\DPBJ.008.tmp C:\WINDOWS\system32\28463\DPBJ.002.tmp C:\WINDOWS\system32\28463\DPBJ.009.tmp C:\WINDOWS\system32\28463\May_31_2013__13_29_53.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_54.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_55.jpg	C:\WINDOWS\system32\28463\May_31_2013__13_42_44.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_45.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_46.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_47.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_48.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_49.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_50.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_51.jpg

	C:\WINDOWS\system32\28463\May_31_2013__13_29_56.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_57.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_58.jpg C:\WINDOWS\system32\28463\May_31_2013__13_29_59.jpg C:\WINDOWS\system32\28463\May_31_2013__13_30_01.jpg C:\WINDOWS\system32\28463\May_31_2013__13_30_02.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_37.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_54.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_38.jpg		C:\WINDOWS\system32\28463\May_31_2013__13_42_52.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_53.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_53.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_39.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_40.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_41.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_42.jpg C:\WINDOWS\system32\28463\May_31_2013__13_42_43.jpg
Clave de registro eliminado	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\\Ardamax Keylogger		
Procesos creados	C:\WINDOWS\system32\28463\DPBJ.exe C:\WINDOWS\system32\28463\DPBJ.exe" "		
Módulos de tiempo de ejecución	c:\docume~1\<USER>~1\locals~1\temp\@1.tmp ole32.dll netapi32 rpcrt4.dll ws2_32.dll comctl32.dll gdi32.dll user32.dll indows\system32\wshtcpip.dll c:\w wininet.dll mpr.dll kernel32.dll	shell32.dll setupapi.dll clbcatq.dll secur32.dll version.dll advapi32.dll wsock32.dll ntdll.dll shlwapi.dll comdlg32.dll oleaut32.dll riched20.dll	ntmarta.dll psapi.dll oleacc.dll uxtheme.dll dpbj.006 dpbj.007 c:\windows\system32\mswsock.dll dnsapi.dll c:\windows\system32\winrnr.dll rasadhlp.dll hnetcfg.dll

Tabla 25: Reporte del comportamiento del malware Keylogger.exe

MALWARE: CRYPTOWALL.EXE	
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**
Escribir datos sobre procesos remotos	C: \ Documents and Settings \ Administrator \ Local Settings \% temp% \ ****. Exe, WriteAddress = 0x00400000, Size = 0x00000400 TargetPID = 0x00000594 C: \ Documents and Settings \ Administrator \ Local Settings \% temp% \ ****. Exe, WriteAddress = 0x00418000, Size = 0x00000200 TargetPID = 0x00000594 C: \ Documents and Settings \ Administrator \ Local Settings \% temp% \ ****. Exe, WriteAddress = 0x00419000, Size = 0x00009400 TargetPID = 0x00000594 C: \ Documents and Settings \ Administrator \ Local Settings \% temp% \ ****. Exe, WriteAddress = 0x00424000, Size = 0x00000600 TargetPID = 0x00000594 C: \ Documents and Settings \ Administrador \ Configuración local \% temp% \ ****. Exe, WriteAddress = 0x7ffdb008, Tamaño = 0x00000004 TargetPID = 0x00000594

	C: \ WINDOWS \ explorer.exe, WriteAddress = 0x000cfffc, Tamaño = 0x00000004 TargetPID = 0x000000f4 C: \ WINDOWS \ system32 \ svchost.exe, WriteAddress = 0x000cfffc, Tamaño = 0x00000004 TargetPID =
Establecer contexto de hilo	C: \ Documents and Settings \ Administrador \ Configuración local \% temp% \ ****. Exe
Establecer elemento de inicio	C: \ Documents and Settings \ Administrador \ 「开始」 菜单 \ 程序 \ 启动 \ 9ea714cd.exe
Modificar registro de inicio	\ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ 9ea714c \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce \ * ea714c \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ 9ea714cd \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce \ * ea714cd
Crea un archivo	C: \ 9ea714cd \ 9ea714cd.exe C: \ Documents and Settings \ Administrator \ Application Data \ 9ea714cd.ex
Crear archivo ejecutable	C: \ 9ea714cd \ 9ea714cd.exe C: \ Documents and Settings \ Administrator \ Application Data \ 9ea714cd.exe C: \ Documents and Settings \ Administrador \ 「开始」 菜单 \ 程序 \ 启动 \ 9ea714cd.exe
Modificar registro	\ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Configuración de Internet \ Conexiones
Eliminar elemento de registro	\ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Configuración de Internet \ ProxyServer \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Configuración de Internet \ ProxyOverride \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Configuración de Internet \ AutoConfigU
Modificar registro de inicio	\ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ 9ea714c \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce \ * ea714c \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ 9ea714cd \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce \ * ea714cd

Tabla 26: Reporte del comportamiento del malware Cryptowall.exe

MALWARE: 1003.EXE	
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**
Modificar registro de inicio	\ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ 252409E5CD \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce \ * 252409E5CD
Proceso de matanza	TASKKILL = "taskkill" / F / IM% temp% \ ****. Exe C: \ Documents and Settings \ Administrador \ Configuración local \% temp% \ ****. Exe
Crear proceso sin mostrar ventana	ImagePath =, CmdLine = "taskkill" / F / IM% temp% \ ****. Exe
Proceso de creación	[0x00000410] ImagePath = C: \ WINDOWS \ system32 \ taskkill.exe, CmdLine = "taskkill" / F / IM% temp% \ ****. Exe
Crea un archivo	C: \ Documents and Settings \ Administrator \ Application Data \ 252409E5CD.exe
Crear archivo ejecutable	C: \ Documents and Settings \ Administrator \ Application Data \ 252409E5CD.exe

Modificar archivo	C: \ Documents and Settings \ Administrator \ Application Data \ 252409E5CD.exe ---> Offset = 0 C: \ Documents and Settings \ Administrator \ Application Data \ 252409E5CD.exe ---> Offset = 65536 C: \ Documents and Settings \ Administrator \ Application Data \ 252409E5CD.exe ---> Offset = 131072 C: \ Documents and Settings \ Administrator \ Application Data \ 252409E5CD.exe ---> Offset = 196608
Modificar registro	\ REGISTRO \ USUARIO \ S - * \ Software \ 252409E5CD \ Keys \ \ REGISTRO \ USUARIO \ S - * \ Software \ 252409E5CD \ Archivos \ \ REGISTRY \ USER \ S - * \ Software \ Microsoft \ Windows \ ShellNoRoam \ MUICache \ C: \ Documents and Settings \ A
Modificar registro de inicio	\ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ Run \ 252409E5CD \ REGISTRO \ USUARIO \ S - * \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce \ * 252409E5CD

Tabla 27: Reporte del comportamiento del malware 1003.exe

MALWARE: 1002.EXE		
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**	
Archivos con atributos modificados	C:\Users\Johnson\AppData\Roaming\591A7704AC.exe C:\Users\Johnson\AppData\Roaming\591A7704AC.exe\:Zone.Identifier:$DATA C:\Users\Johnson\AppData\Local\Temp\829dde7015c32d7d77d8128665390dnalysis_subject.exe	
Claves de registro eliminadas	HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP HKU\S-1-5-21-3712457824-2419000099-45725732-1001\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP	
Procesos creados	C:\Users\Johnson\AppData\Local\Temp\829dde7015c32d7d77d8128665390dnalysis_subject.exe C:\Users\Johnson\AppData\Roaming\591A7704AC.exe C:\Windows\system32\taskkill.exe	
Árbol de procesos	C:\Users\Johnson\AppData\Local\Temp\829dde7015c32d7d77d8128665390dnalysis_subject.exe C:\Users\Johnson\AppData\Roaming\591A7704AC.exe C:\Windows\system32\taskkill.exe	
Módulos de tiempo de ejecución	c:\windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac\comctl32.dll c:\windows\assembly\nativeimages_v2.0.50727_64\system\adff7dd9fe8e541775c46b6363401b22\system.ni.dll c:\windows\assembly\nativeimages_v2.0.50727_64\system.core\83e2f6909980da7347e7806d8c26670e\system.core.ni.dll c:\windows\microsoft.net\framework64\v4.0.30319\mscoreei.dll c:\windows\system32\api-ms-win-downlevel-ole32-l1-1-0.dll c:\windows\system32\api-ms-win-downlevel-shlwapi-l1-1-0.dll c:\windows\microsoft.net\framework64\v2.0.50727\mscorjit.dll c:\windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll c:\windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a\gdiplus.dll	c:\windows\system32\usp10.dll c:\windows\system32\wininet.dll c:\windows\system32\imm32.dll c:\windows\system32\lpk.dll c:\windows\system32\clbcatq.dll c:\windows\system32\msctf.dll c:\windows\system32\urlmon.dll c:\windows\system32\cryptsp.dll c:\windows\system32\setupapi.dll c:\windows\system32\rsaenh.dll c:\windows\system32\ole32.dll c:\windows\system32\ntdll.dll c:\windows\system32\normaliz.dll c:\windows\system32\uxtheme.dll

	c:\windows\assembly\nativeimages_v2.0.50727_64\system.drawing\5910828a337dbe848dc90c7ae0a7dee2\system.drawing.ni.dll c:\windows\system32\api-ms-win-downlevel-version-l1-1-0.dll c:\windows\microsoft.net\framework64\v2.0.50727\culture.dll c:\windows\assembly\nativeimages_v2.0.50727_64\system.configuration\091b931d0f6408001747dbbbb05dbe66\system.configuration.ni.dll c:\windows\system32\api-ms-win-downlevel-advapi32-l2-1-0.dll c:\windows\system32\api-ms-win-downlevel-normaliz-l1-1-0.dll c:\windows\assembly\nativeimages_v2.0.50727_64\system.xml\ee795155543768ea67eecddc686a1e9e\system.xml.ni.dll c:\windows\system32\api-ms-win-downlevel-advapi32-l1-1-0.dll c:\windows\system32\oleaut32.dll c:\windows\system32\user32.dll c:\windows\system32\userenv.dll c:\windows\system32\shell32.dll c:\windows\system32\rpcrt4.dll c:\windows\system32\psapi.dll c:\windows\system32\iphlpapi.dll c:\windows\system32\propsys.dll c:\windows\system32\advapi32.dll c:\windows\system32\api-ms-win-downlevel-user32-l1-1-0.dll c:\windows\assembly\nativeimages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll c:\windows\system32\ws2_32.dll c:\windows\system32\dnsapi.dll c:\windows\system32\iertutil.dll c:\windows\system32\mswsock.dll c:\windows\system32\bcrypt.dll c:\windows\assembly\nativeimages_v2.0.50727_64\system.windows.forms\6c352ff9e3603b0e69d969ff7e7632f5\system.windows.forms.ni.dll c:\windows\microsoft.net\framework64\v2.0.50727\mscorwks.dll c:\windows\system32\kernelbase.dll c:\windows\system32\wship6.dll c:\windows\system32\ntmarta.dll c:\windows\system32\windowscodecs.dll c:\windows\system32\rtutils.dll c:\windows\system32\wbem\wbemprox.dll c:\windows\system32\netapi32.dll c:\windows\system32\srvcli.dll c:\windows\system32\rpcrtremote.dll	c:\windows\system32\apphelp.dll c:\windows\system32\devobj.dll c:\windows\system32\mscoree.dll c:\windows\system32\secur32.dll c:\windows\system32\rasadhlp.dll c:\windows\system32\nsi.dll c:\windows\system32\msvcrt.dll c:\windows\system32\sechost.dll c:\windows\system32\winnsi.dll c:\windows\system32\sspicli.dll c:\windows\system32\shdocvw.dll c:\windows\system32\profapi.dll c:\windows\system32\cryptbase.dll c:\windows\system32\dwmapi.dll c:\windows\system32\shlwapi.dll c:\windows\system32\wldap32.dll c:\windows\system32\gdi32.dll c:\windows\system32\version.dll c:\windows\system32\kernel32.dll c:\windows\system32\shfolder.dll c:\windows\system32\cfgmgr32.dll c:\windows\system32\wshtcpip.dll c:\windows\system32\dhcpcsvc.dll c:\windows\system32\rasapi32.dll c:\windows\system32\webio.dll c:\windows\system32\winhttp.dll c:\windows\system32\dhcpcsvc6.dll c:\windows\system32\rasman.dll c:\windows\system32\credssp.dll c:\windows\system32\wtsapi32.dll c:\windows\system32\winsta.dll c:\windows\system32\ntdsapi.dll c:\windows\system32\wkscli.dll c:\windows\system32\wbemcomn.dll c:\windows\system32\wbem\wbemsvc.dll c:\windows\system32\framedynos.dll c:\windows\system32\wbem\fastprox.dll c:\windows\system32\dbghelp.dll c:\windows\system32\netutils.dll c:\windows\system32\mpr.dll

Tabla 28: Reporte del comportamiento del malware 1002.exe

ZEROACCESS_XXX-PORN-MOVIE.AVI.EXE_		
COMPORTAMIENTO	**INFORMACIÓN DETALLADA**	
Escribir datos sobre procesos remotos	C: \ WINDOWS \ explorer.exe, WriteAddress = 0x01ee0000, Size = 0x00000430 TargetPID = 0x00000700 C: \ WINDOWS \ explorer.exe, WriteAddress = 0x01ee0000, Size = 0x0000028e TargetPID = 0x00000700 C: \ WINDOWS \ system32 \ services.exe, WriteAddress = 0x00740000, Size = 0x00000244 TargetPID = 0x0000028c C: \ WINDOWS \ system32 \ cmd.exe, WriteAddress = 0x0013f000, Tamaño = 0x0000004c TargetPID = 0	
Autoborrado	C: \ Documents and Settings \ Administrador \ Configuración local \% temp% \ ****. Exe	
Proceso de creación	[0x00000824] ImagePath = C: \ WINDOWS \ system32 \ cmd.exe, CmdLine = "C: \ WINDOWS \ system32 \ cmd.exe"	
Crea un archivo	C: \ RECICLADOR \ S-1-5-18 \ $ 13b271b64a22cc2cbba0b97c3b013b74 \ @ C: \ RECICLADOR \ S-1-5-18 \ $ 13b271b64a22cc2cbba0b97c3b013b74 \ n	C: \ RECYCLER \ S - * \ $ 13b271b64a22cc2cbba0b97c3b013b74 \ @ C: \ RECICLADOR \ S - * \ $ 13b271b64a22cc2cbba0b97c3b013b74 \ n
Crear archivo ejecutable	C: \ RECICLADOR \ S - * \ $ 13b271b64a22cc2cbba0b97c3b013b74 \ n	C: \ RECICLADOR \ S-1-5-18 \ $ 13b271b64a22cc2cbba0b97c3b013b74 \ n
Modificar archivo	C: \RECYCLER\S-1-5-18\$ 13b271b64a22cc2cbba0b97c3b013b74 \ @ ---> Offset = 0 C: \RECYCLER\S-1-5-18\$ 13b271b64a22cc2cbba0b97c3b013b74 \ n ---> Offset = 0	C:\RECYCLER\S - *\$ 13b271b64a22cc2cbba0b97c3b013b74 \ @ ---> Offset = 0 C:\RECYCLER\ S - *\ $ 13b271b64a22cc2cbba0b97c3b013b74 \ n ---> Offset = 0
Modificar registro	\ REGISTRO \ USUARIO \ S - * _ CLASES \ clsid \ {fbeb8a05-beee-4442-804e-409d6c4515e9} \ InprocServer32 \ ThreadingModel \ REGISTRO \ USUARIO \ S - * _ CLASES \ clsid \ {fbeb8a05-beee-4442-804e-409d6c4515e9} \ InprocServer32 \ \ REGISTRO \ MÁQUINA \ SOFTWARE \ Clases \ CLSID \ {5839FCA9-774D-42A1-ACDA-D6A79037F57F} \ InprocServer32 \ \ REGISTRY \ USER \ S - * \ SessionInformation \ ProgramCount	
Eliminar elemento de registro	\ REGISTRO \ MÁQUINA \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run \ Windows Defender	

Tabla 29: Reporte del comportamiento del malware ZeroAccess.exe

2.8.2.3. Reporte de la estructura del malware

En base a los resultados emitidos por las herramientas en el análisis estático y dinámico se muestra la estructura de cada código malicioso examinado:

NOMBRE DEL ARCHIVO	COMPILADOR	ENTROPY	SECCIONES	DETALLE DE SECCIONES	TAREAS	VERSION	DLL
1002		6,99	3	.text .rsrc .reloc	2	1	mscoree.dll
1003	Microsoft Visual C# / Basic .NET	7,16	3		2	1	mscoree.dll
PROTEUS	Microsoft Visual C# / Basic .NET	7,99	3	.text .rsrc .reloc	2	1	mscoree.dll
TROJAN BLADA		5,33	4	.text .sdata .rsrc .reloc	2	1	mscoree.dll
TROJAN DROPP	Nullsoft PiMP Stub [Nullsoft PiMP SFX] *	6,26	5	 .text .rdata .data .ndata .rsrc 	2		KERNEL32.dll USER32.DLL GDI32.dll SHELL32.dll ADVAPI32.dll COMCTL32.dll ole32.dll VERSION.dll
ZERO ACCESS	Microsoft Visual C++ Private Version 1 [Overlay]	6,21	4	.text .rdata .data .reloc	2		ntdll.dll KERNEL32.dll ADVAPI32.dll MSWSOCK.dll WS2_32.dll

Tabla 30: Reporte de la estructura del malware

CONCLUSIONES

- Las herramientas se seleccionaron de acuerdo a los criterios de análisis estático (WinMD5, extracción de cadenas de texto, bin text, etc) y también de análisis dinámico (Disk pulse, Process explorer. Autoruns, etc) para cumplir de forma metódica cada una de las fases establecidas. Además, la instalación del firewall permitió obtener un control y monitoreo de la red del laboratorio virtual.
- El uso de software con licencia de código abierto y la virtualización permitieron el ahorro de costos, hardware y espacio físico, y a su vez se pudo obtener la simulación de un entorno real.
- La red alámbrica de los laboratorios de FACSISTEL, según los resultados obtenidos de las encuestas aplicadas, poseen ciertas vulnerabilidades en la red por las constantes infecciones.
- Los reportes generados por el laboratorio virtual muestran la estructura, comportamiento e información general del malware. Estos datos permitirán realizar un estudio con mayor profundidad para la elaboración de planes de contingencia y seguridad para los laboratorios de FACSISTEL.
- El firewall Pfsense es de gran utilidad para el control de cada dispositivo conectado a la red. Esto nos permite verificar qué máquina están siendo infectadas, además de restringir el acceso a páginas no confiables en los laboratorios de FACSISTEL.
- Es importante resaltar que la evolución lógica de los sistemas no queda exenta del ataque del software malicioso o malware, por lo que su estudio en el laboratorio virtual en base al análisis estático y dinámico se constituyen en elementos claves para evitar que los sistemas estén desprotegidos e inseguros.
- Finalmente, el laboratorio virtual para FACSITEL se constituye en una herramienta esencial en un entorno controlado para poder seguir desarrollando análisis prospectivos de código maliciosos que están en constante evolución y cambio. En este propuesta tecnológica se ha visto cómo poder analizar el comportamiento del malware, en base a herramientas específicas y se puede notar que no todo el malware deja el mismo rastro pero sí tiene un patrón común en su proceso de infección.

RECOMENDACIONES

- Se recomienda verificar la compatibilidad de las herramientas con el sistema operativo y los requisitos de instalación de las mismas.
- Es sustancial establecer snapshots por cada prueba que se realice en el laboratorio virtual para poder tener un punto de retorno y soslayar daños que pueda ocasionar el malware.
- Se sugiere implantar reglas en los laboratorios de FACSISTEL para que las máquinas no sean remplazadas o movilizadas a otro laboratorio, debido a que esto ocasiona que el control de las mismas en el firewall sea inexacto.
- Se considera fundamental promover la creación de un área específica, con los puertos de la red aislada, en donde se puedan conectar las máquinas para realizar los análisis y de esta manera evitar los riesgos de infección a la red.
- El personal que realice las funciones de monitorización, análisis y reporte, deberán ser estudiantes de FACSISTEL que deseen realizar sus prácticas profesionales en esta área.
- En base a este proyecto y por medio de los reportes que proporciona el laboratorio virtual se podrían realizar investigaciones prospectivas para la implementación de antivirus, análisis específicos de malware, técnicas forenses, entre otras.

BIBLIOGRAFÍA

[1] CISCO, «Reporte Semestral de Seguridad,» Cisco, San José, 2019.

[2] P. Gaviria, Aplicación de Metodología de Malware para el Análisis de la amenaza avanzada persistente (APT) "Poison Ivy". Tesis, San Juan de Pasto: Universidad Internacional de la Rioja, 2016, p. 167.

[3] ESET, «Eset Security Report Latinoamérica,» ESET, 2017.

[4] Kaspersky Lab, «Kaspersky Lab,» 2019. [En línea]. Available: https://latam.kaspersky.com/about/team/eugene-kaspersky. [Último acceso: 16 Mayo 2019].

[5] ABC, «ABC Redes,» 13 Mayo 2014. [En línea]. Available: https://www.abc.es/tecnologia/redes/20140507/abci-antimalware-laboratorio-201405062115.html. [Último acceso: 16 Mayo 2019].

[6] Kaspersky Lab, «10 ventajas que solo puede ofrecer una solución de seguridad basada en una plataforma integrada,» Kaspersky Lab, Iberia.

[7] T. Jumbo Tene, Metodología para el análisis de malware en un ambiente controlado, Mayo: Universidad Politécnica Salesiana, 2017.

[8] Durán Lara, Jorge Christian;, Desarrollo de un laboratorio para el análisis automatizado de códigos maliciosos, México: Universidad Nacional Autónoma de México UNAM, 2012.

[9] UPSE, «FACSISTEL,» 29 Mayo 2019. [En línea]. Available: http://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Itemid=463. [Último acceso: 29 Mayo 2019].

[10] B. Zempoalteca Durán, J. F. Barragán López, J. González Martínez y T. & Guzmán Flores, «Formación en TIC y competencia digital en la docencia en instituciones públicas de educación superior,» *Apertura (Guadalajara, Jal.),* vol. 9, nº 1, pp. 80-96, 2017.

[11] M. Alegría Diaz , Uso de las tic como estrategias que facilitan a los estudiantes la construcción de aprendizajes significativos, Guatemala: Universidad Rafael Landívar, 2015.

[12] ESET, «Eset Security Report Latinoamérica,» ESET, 2018.

[13] Consejo Nacional de Planificación, Plan Nacional de Desarrollo 2017-2021-Toda una Vida, Quito: Senplades, 2017.

[14] R. H. Sampieri, C. F. Collado y P. B. Lucio, Metodología de la investigación, México: Mcgraw-hill, 1998.

[15] OWASP Inc., «OWASP,» 19 Febrero 2019. [En línea]. Available: https://www.owasp.org/index.php/Penetration_testing_methodologies. [Último acceso: 5 Mayo 2019].

[16] D. F. Ortiz Aristizábal, Desarrollo de metodología para hallazgos de vulnerabilidades en redes corporativas e intrusiones controladas, Bogotá: Fundación Universitaria los Libertadores, 2015.

[17] S. Gadhiya y K. Bhavsar, «Techniques for Malware Analysis,» *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, nº 4, pp. 972-975, 2013.

[18] C. Willems, T. Holz y F. Freiling, «Toward automated dynamic malware analysis using CWSandbox,» *IEEE Computer Society,* vol. 5, nº 2, pp. 32-39, 2012.

[19] M. Sikorski y A. Honig, Practical malware analysis: The Hands-On guide to dissecting malicious software, San Francisco: No Starch Press, 2012.

[20] WinMD5, «WinMD5Free,» 2019. [En línea]. Available: http://www.winmd5.com/. [Último acceso: 5 Septiembre 2019].

[21] L. Pascoe, «MD5Summer,» Windows MD5 Sum generator, [En línea]. Available: http://www.md5summer.org/. [Último acceso: 3 Septiembre 2019].

[22] S. Yusirwan, Y. Prayudi y I. Riadi, «Implementation of Malware Analysis using Static and Dynamic Analysis Method,» *International Journal of Computer Applications,* vol. 117, nº 6, pp. 11-15, 2015.

[23] . L. Cheng y G. Jontze, «Análisis estático y dinámico de una muestra de malware en sistemas Microsoft Windows XP para determinar qué efectos produce sobre un sistema infectado,» Quito, 2017.

[24] P. A. Gaviria, Aplicación de Metodología de Malware para el Análisis de la amenaza avanzada persistente (APT) “Poison Ivy”, Tesis de Maestría, 2016.

[25] L. Zeltzr, Introduction to Malware Analysis, SANS Technology Institute, 2010.

[26] A. Parra Truyol, «Laboratorio de malware: Automatización de la gestión de recursos virtuales para el estudio de malware,» Tesis de Maestría, 2013.

[27] S. Albin, «Binbert,» 2016. [En línea]. Available: https://www.binbert.com/blog/2010/12/pfsense-squidguard-lightsquid/. [Último acceso: 12 Agosto 2019].

[28] D. Arboledas, Administración de rede telemáticas, Españá: Ra-Ma, 2015.

[29] EcuRed, «EcuRed,» MediaWiki, [En línea]. Available: https://www.ecured.cu/SquidGuard. [Último acceso: 13 Agosto 2019].

[30] J. Astudillo, F. Ortiz y A. Jiménez, «Adaptación de IDS/IPS Suricata para que se pueda convertir en una solución empresarial,» *Dspace,* vol. 1, nº 1, pp. 1-12, 2012.

[31] Kaspersky Lab, «Desarrollo de las amenazas informáticas en el segundo trimestre de 2019. Estadística,» AO Kaspersky Lab., 2019.

[32] Cisco Security Research, «Reporte Anual de Ciberseguridad 2018,» Cisco, 2018.

[33] Malwarebytes Labs, «State of Malware Report,» Malwarebytes, 2019.

[34] VU Labs, «Informe 2018 - 2019 de ciberseguridad en entornos digitales,» VU Security, 2018.

[35] ESET, «ESET Security Report Latinoaméricana 2018,» ESET, 2018.

[36] Kaspersky, «Comunicados de prensa: Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina,» 13 Agosto 2018. [En línea]. Available: https://latam.kaspersky.com/about/press-releases/2018_panorama-de-amenazas-phishing. [Último acceso: 10 Septiembre 2019].

[37] Symantec, «Internet Security Threat Report,» Symantec Corporation, United Stated of America, 2019.

[38] It's FOSS, «Best Linux Distributions for Hacking and Penetration Testing,» It's FOSS, 11 Mayo 2019. [En línea]. Available: https://itsfoss.com/linux-hacking-penetration-testing/. [Último acceso: 2019 Junio 20].

ANEXOS

Anexo 1: Formato para el cuestionario

CUESTIONARIO PARA ESTUDIANTES DE FACSISTEL

1. ¿Con qué frecuencia utiliza el servicio de internet por red en la Facultad?

- Diariamente
- Varios días en la semana
- Casi Nunca

2. ¿En qué rango de horario considera usted que el internet se torna lento?

- 07:30 – 08:30
- 09:00 – 10:00
- 12:00 – 13:00
- 15:00 – 16:00
- 17:00 – 18:00

3. Seleccione cuál es el laboratorio que usted más utiliza

- Laboratorios de informática
- Laboratorio de redes
- Laboratorio de CISCO

4. ¿El servicio de internet alámbrico de los laboratorios se adapta a sus necesidades como usuario?

- Si
- No

5. ¿Siente que las redes cableadas de los laboratorios poseen las seguridades informáticas necesarias? ¿Por qué?

- Si
- No

_____

6. ¿Considera usted que existen virus dentro de la red de los laboratorios?

- Si

- No

7. ¿Se han infectado en alguna ocasión sus equipos al conectarse a la red alámbrica de los laboratorios?

- Si
- No

8. Si su respuesta en la pregunta anterior fue afirmativa, por favor, de acuerdo a su experiencia, mencione qué tipo de virus infectó su dispositivo

_____

Anexo 2: Formato para entrevista

LABORATORIO VIRTUAL DE ANÁLISIS Y COMPORTAMIENTO DE MALWARE UTILIZANDO TÉCNICAS Y MÉTODOS DE SEGURIDAD INFORMÁTICA PARA LOS LABORATORIOS EN LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

PRESENTACION:

La presente entrevista forma parte del trabajo de titulación "Laboratorio virtual de análisis y comportamiento de malware utilizando técnicas y métodos de seguridad informática para los laboratorios en la Facultad de Sistemas y Telecomunicaciones" y tiene como objetivo realizar una investigación en el Departamento de Tecnología de la Información y Comunicación de la UPSE acerca de la infraestructura y seguridad de la red. La información brindada en esta entrevista es de carácter confidencial. Agradezco su colaboración

INICIO

_____

Empresa: Universidad Estatal Península de Santa Elena
Persona entrevistada: _____
Función: Jefe del Departamento de Tecnología de la Información y Comunicación

ETAPA 1: SITUACIÓN ACTUAL DEL INTERNET

1.1. ¿Qué proveedor de servicio de internet proporciona conectividad a la UPSE?

1.2. ¿Cuál es el ancho de banda que recibe la universidad por parte del ISP?

1.3. ¿Cómo está distribuido el ancho de banda en las extensiones de la universidad?

1.4. ¿Cómo está distribuido el ancho de banda en el campus de la universidad?

1.5. ¿Cuál es el ancho de banda que reciben los laboratorios de la Facultad de Sistemas y Telecomunicaciones?

1.6. ¿Qué topología de red tiene la UPSE?

1.7. ¿Qué tipo de segmentación tiene la red de la UPSE, por vlans, por IP, o ambas?

1.8. ¿Cuántas vlans tiene FACSISTEL y cuáles son?

ETAPA 2: HARDWARE Y SOFTWARE

2.1. ¿El departamento de TIC's dispone de dispositivos de Hardware para la seguridad informática?

2.2. ¿En los switches de la UPSE se ha implementado algún tipo de seguridad? ¿Qué tipo?

2.3. ¿El router principal pertenece a la UPSE?

2.4. ¿El departamento de TIC's se encarga de la administración del router principal?

2.5. ¿Existe a nivel de software un IDS o IPS?

2.6. ¿Cómo controla el comportamiento de la red a nivel de seguridad?

2.7. ¿Tiene el proveedor algún tipo de control sobre la seguridad de la red?

ETAPA 3: SEGURIDAD

3.1. ¿El departamento de TIC's lleva una estadística con respecto al promedio de usuarios conectados a la red alámbrica en el día?

3.2. ¿En qué lapsos de tiempo se presenta en la red la mayor cantidad de usuarios conectados?

3.3. ¿El departamento de TIC's tiene un área encargada del control y análisis de las redes? ¿Qué tipo de control?

3.4. ¿El departamento de TIC's lleva una estadística de incidentes de seguridad con respecto a softwares maliciosos en la red?

3.5. ¿Según su experiencia cree usted que cuando la red se torna lenta uno de los motivos puede ser la presencia de malware? ¿Por qué?

3.6. ¿Considera usted que es necesario en la universidad crear un laboratorio de análisis y comportamiento de malware? ¿Por qué?

3.7. Durante el tiempo que usted ha laborado en el departamento, ¿recuerda algún incidente de seguridad sobre las redes de la UPSE?

Anexo 3: Inventario de MAC

Anexo 4: Reportes de malware en los últimos años

REPORTES A NIVEL MUNDIAL

Kaspersky

Según los datos de Kaspersky Security Network: Los productos de Kaspersky para la protección de dispositivos móviles detectaron:

Paquetes de instalación maliciosos	Paquetes de instalación de troyanos bancarios móviles	Paquetes de instalación de troyanos extorsionadores móviles
753 550	13 899	23 294

En el reporte del segundo trimestre del 2019 de Kaspersky muestra que el paquete de aplicaciones más infectado es Microsoft Office, puesto que la proporción de exploits se ha incrementado en un 72%. Esta cifra es considerada debido que para los delincuentes informáticos ésta es la forma más fácil de insertar malware en los equipos que utilizan dicho paquete [31].

Los navegadores se encuentran en el segundo lugar de lista de aplicaciones vulnerables con un 14%, en su gran mayoría los atacantes aprovechan los errores de codificación [31].

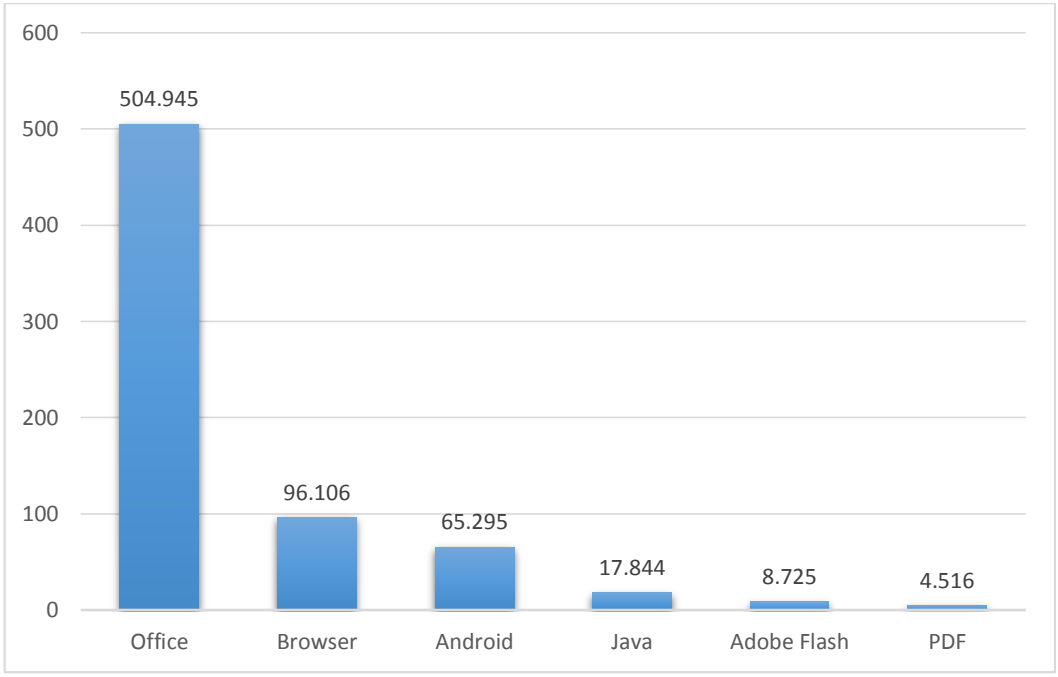


Figura 75: Aplicaciones vulnerables utilizadas por los ciberdelincuentes

En este reporte también se puede observar los países en donde se originan los ataques por internet, encabezado por Estados Unidos (23,72%).

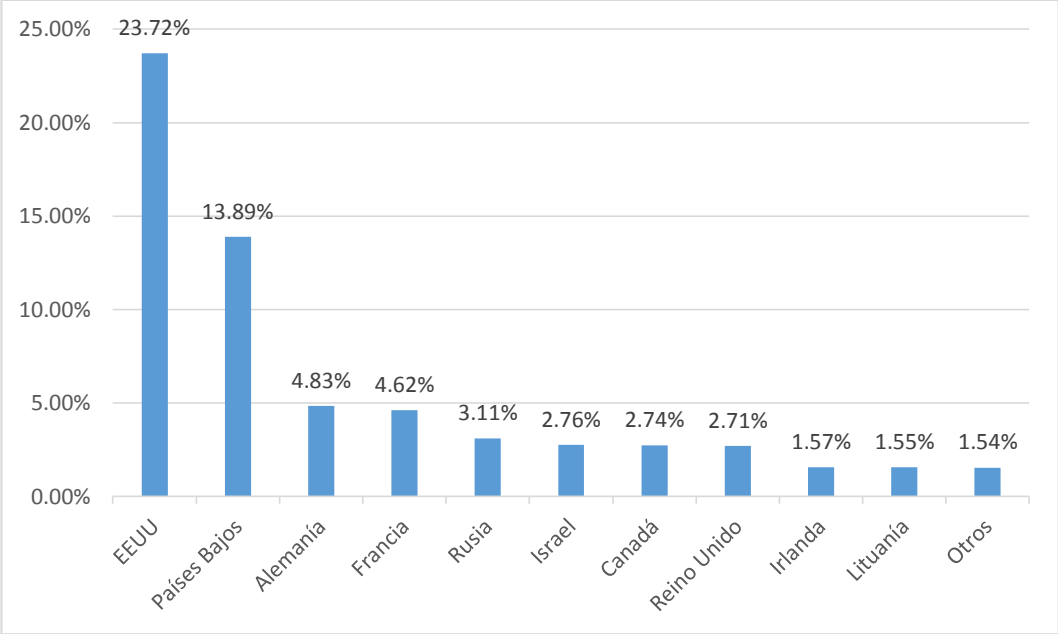


Figura 76: Top 10 de los países fuentes de los ataques web

En una de las secciones del reporte presentado, muestra el porcentaje de usuarios atacados por malware en los diversos países, liderando a Argelia con un 20,38%, seguido de Venezuela con un 19,13% [31].

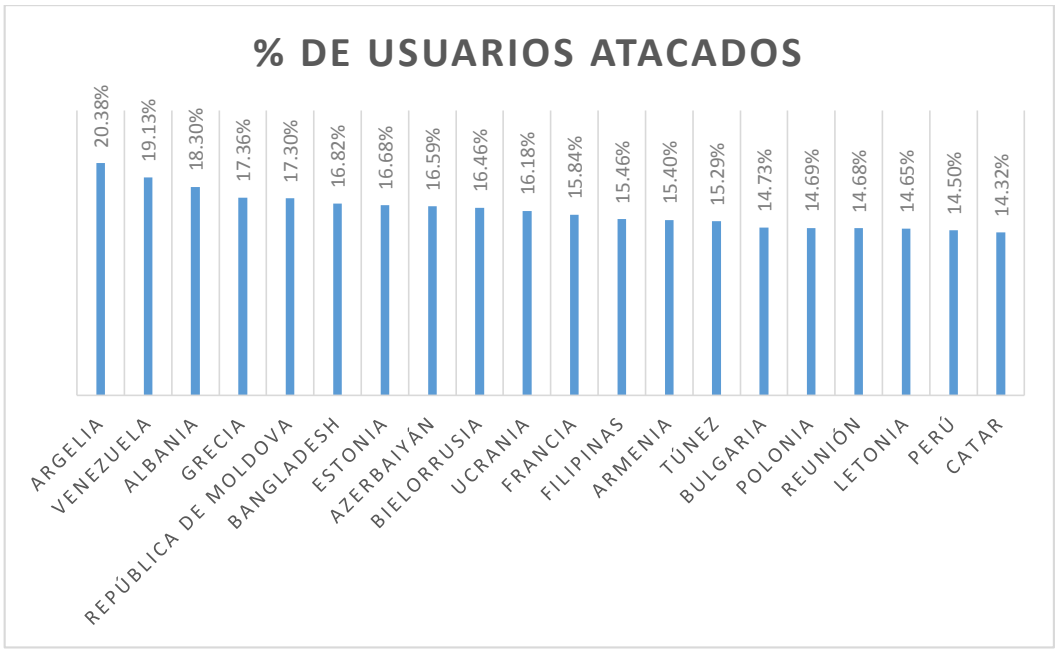


Figura 77: Países donde los usuarios se sometieron a mayor riesgo de infección mediante Internet

CISCO

El reporte anual de Ciberseguridad 2018 de CISCO en la investigación a amenazas detectadas en los correos electrónicos, destaca las 10 extensiones de archivos más frecuentes utilizadas por el malware para encubrirse. El 38% corresponde al paquete de Microsoft Office, el 37% a archivos de extensiones .zip, .jar, .7z, .rar, y el 14% los archivos pdf [32].

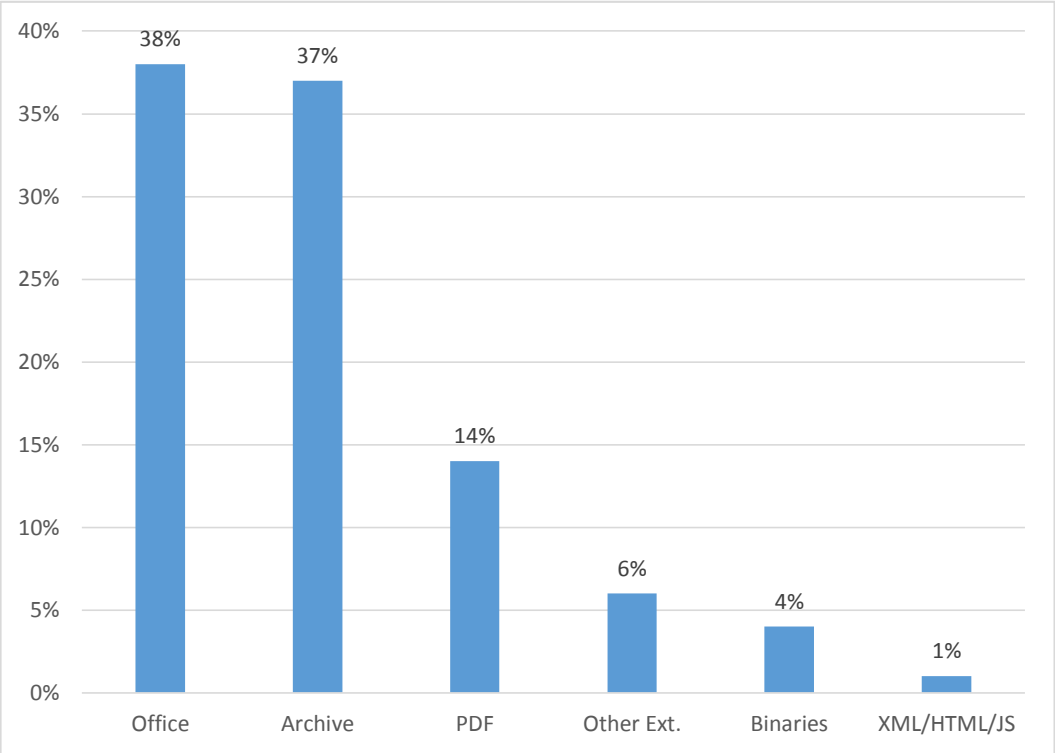


Figura 78: Principales 10 extensiones de archivos maliciosos

MALWAREBYTE

El reporte del Estado de Malware 2019 de la empresa Malwarebytes Labs, nos muestra un top 10 de los principales softwares maliciosos que se han detectado en el período 2017 – 2018, acentuando al trojan, backdoor y spyware como principales atacantes. Además, este informe hace una comparación del índice de infecciones ocurridas en el 2017 y 2018, teniendo como resultado un descenso del 3% en el año 2018 [33].

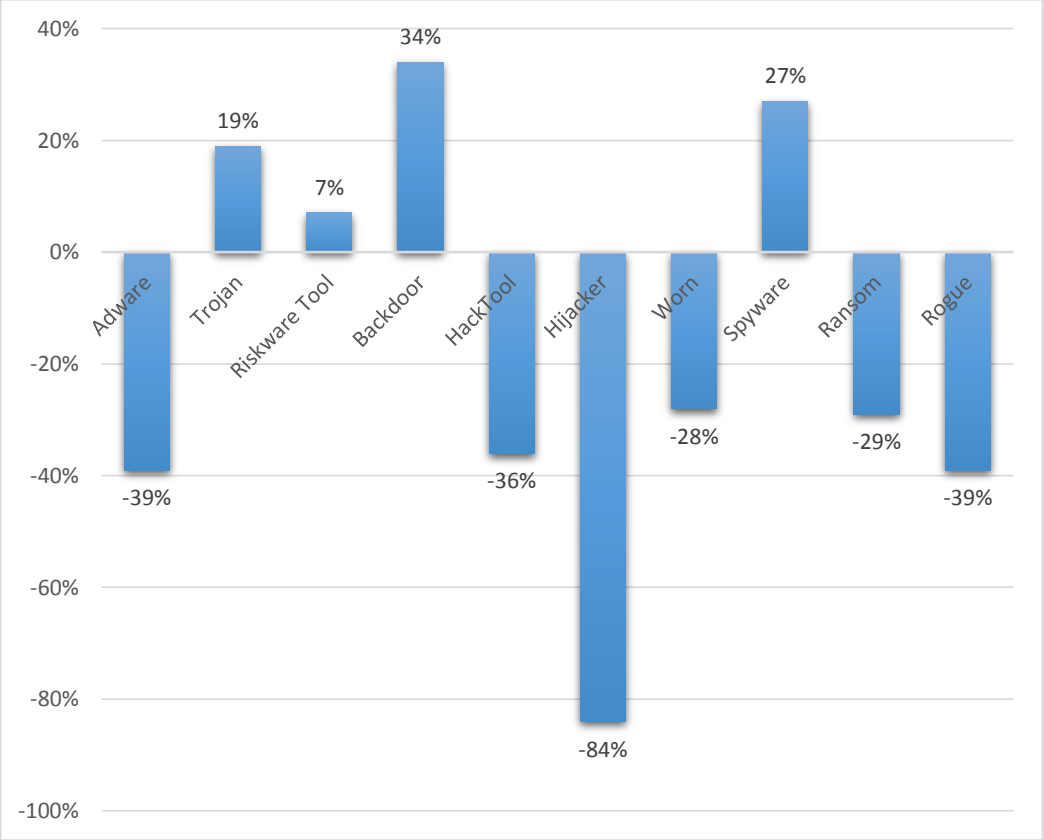


Figura 79: Top 10 de malware detectados

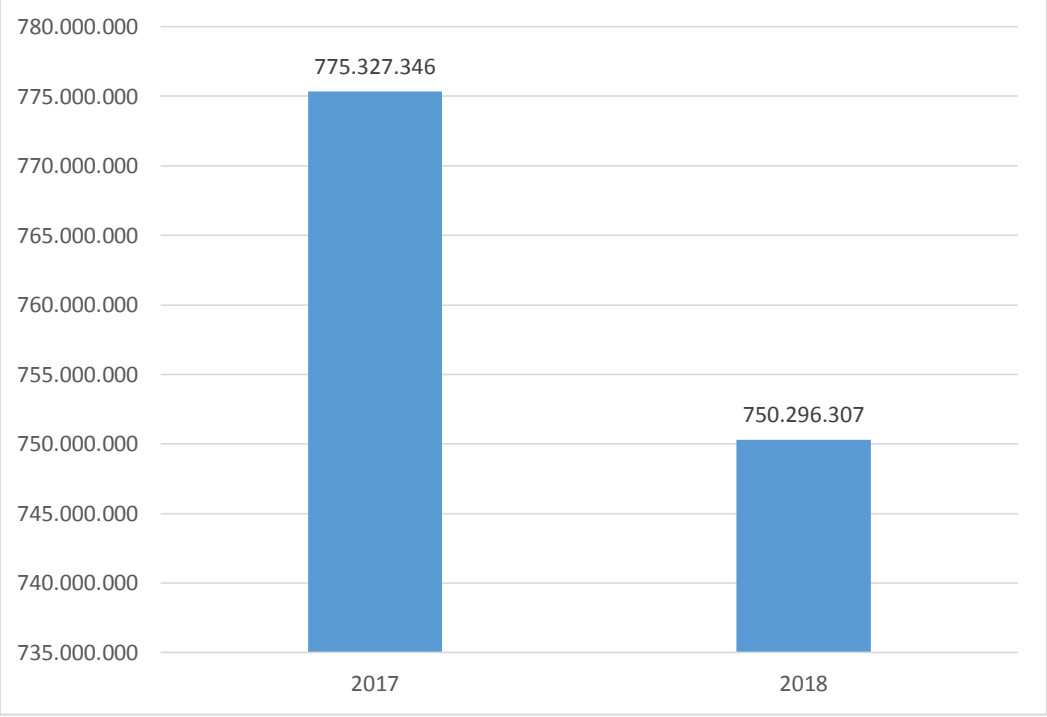


Figura 80: Detección general de los años 2017 – 2018

Según el reporte de Malwarebytes, el país con mayores ataques informáticos es Estado Unidos. Seguido de Brazil, el cual es frecuentemente atacado por el tipo de malware "click fraud" para generar dinero a través del frade en anuncios. Por otra parte, la principal amenaza de malware que enfrentan la gran mayoría de países es el "backdoors", ocasionado especialmente a una mayor necesidad de parchear y asegurar puntos finales [33].

	País	**Mayor amenaza**
1	Estados Unidos	Robo de información
2	Brazil	Clic fraud
3	Reino Unido	Adware
4	Vietnam	Backdoors
5	India	Backdoors
6	Indonesia	Backdoors
7	Francia	Adware
8	Italia	Criptominería
9	Tailandia	Backdoors
10	Rusia	Backdoors

Tabla 31: Los 10 principales países con mayor cantidad de detecciones de malware

REPORTES A NIVEL LATINOAMÉRICA

VU Security

VU Security en su encuesta realizada a organizaciones de América Latina en el 2018, destacó que los usuarios reciben frecuentemente amenazas informáticas por medio del phishing con un 88,4% y el malware en segundo lugar con un 82,2% [34].

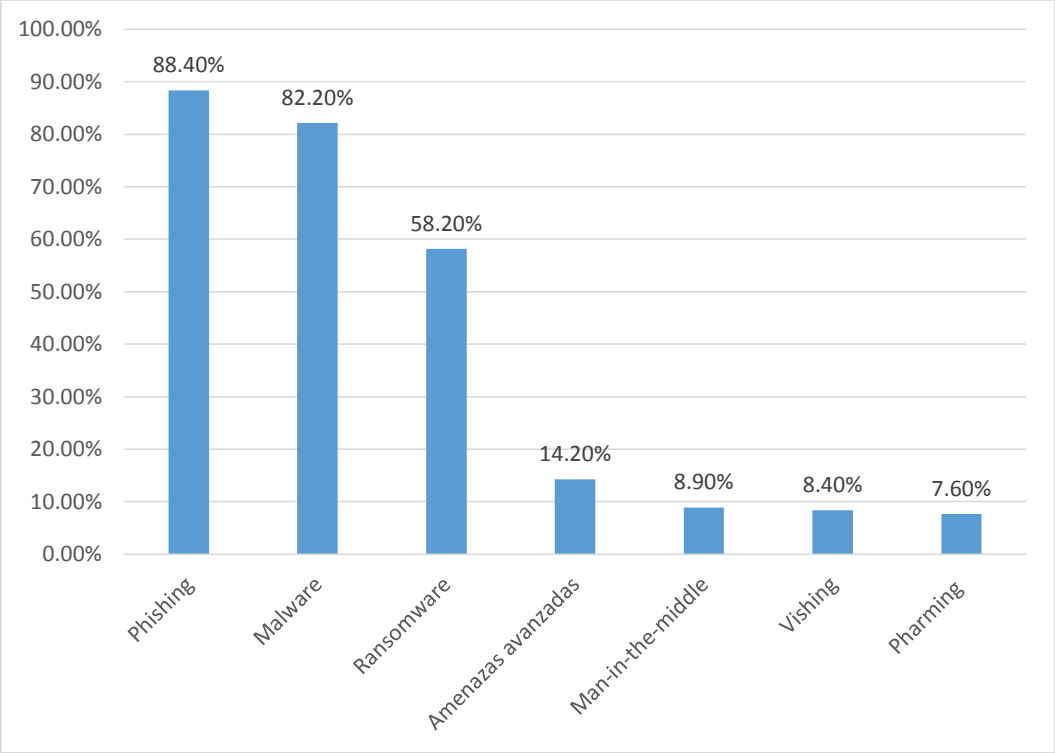


Figura 81: Amenazas online más frecuentes

ESET

El informe de ESET en las empresas latinoamericanas muestra un cambio significativo en comparación con los informes de los anteriores años, en el cual el malware era la principal amenaza de seguridad informática. Sin embargo, este año el informe muestra al ransware con un 57% liderando la lista de ataques informáticos y al malware lo ubica en tercer lugar con un 53% [35].

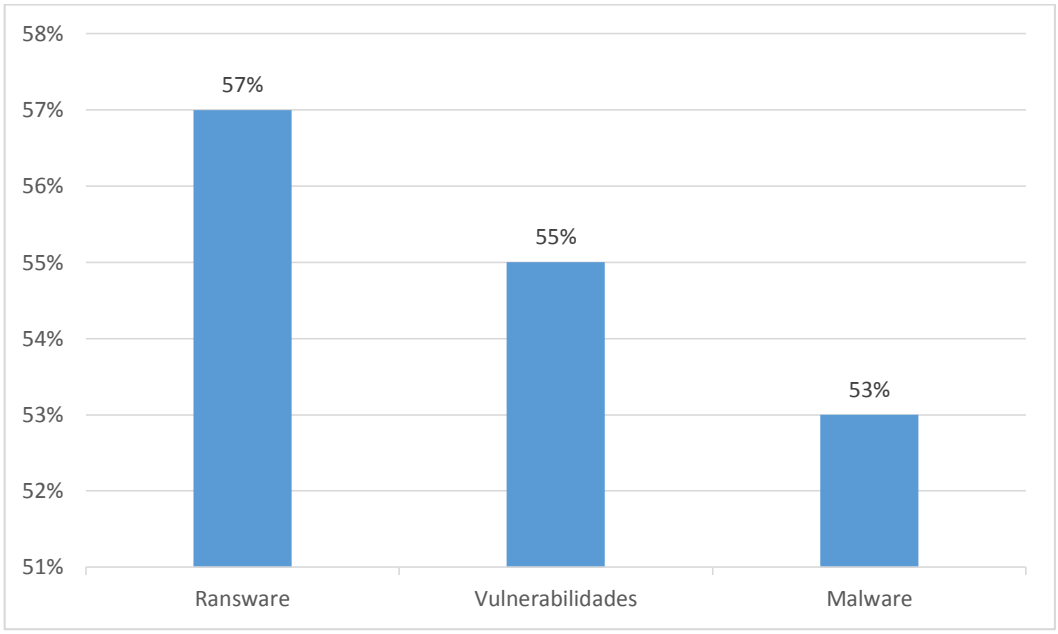


Figura 82: Ataques informáticos en empresas latinoamericanas

En el siguiente gráfico de empresas latinoamericanas encuestadas, destaca a Venezuela y Ecuador como los dos países que más incidentes por malware han sufrido. Así mismo, muestra a El Salvador y Paraguay con menores índice de infecciones informáticas [35].

Figura 83: Mapa de infecciones de malware por país

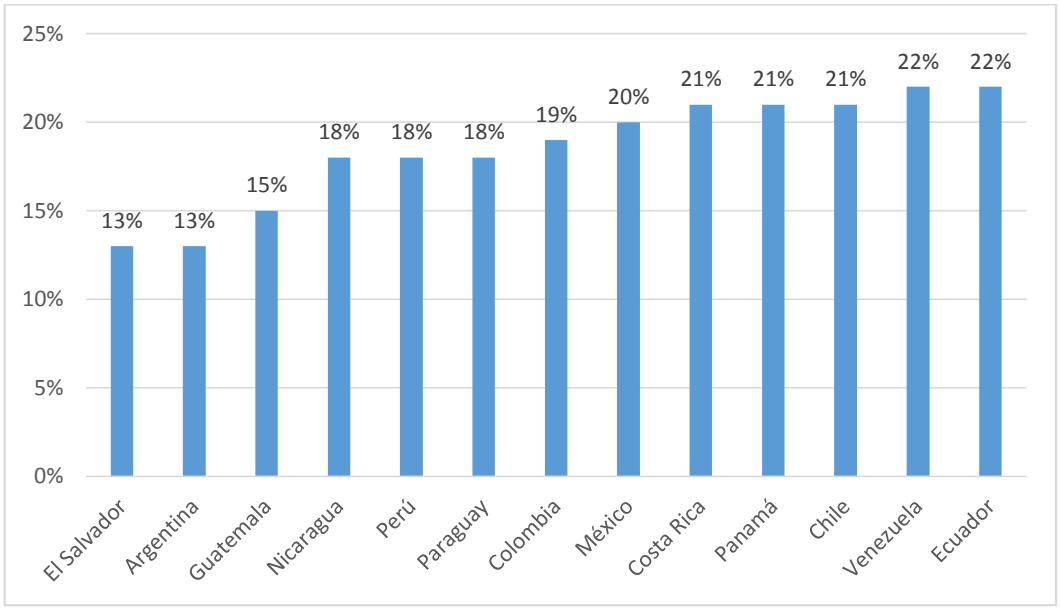


Figura 84: Infecciones de malware por país

KASPERSKY LAB

En el 2018 Kaspersky en la Octava Cumbre de Analistas de Seguridad informó que la infección por malware aumento un 60% en América Latina, teniendo un promedio de 746 mil ataques por día en los últimos 12 meses de este año [36].

El ataque por phishing fue uno de los más detectados en la región, principalmente en Brasil. Estas ciberamenazas han sido orientadas en su gran mayoría al robo de dinero [36].

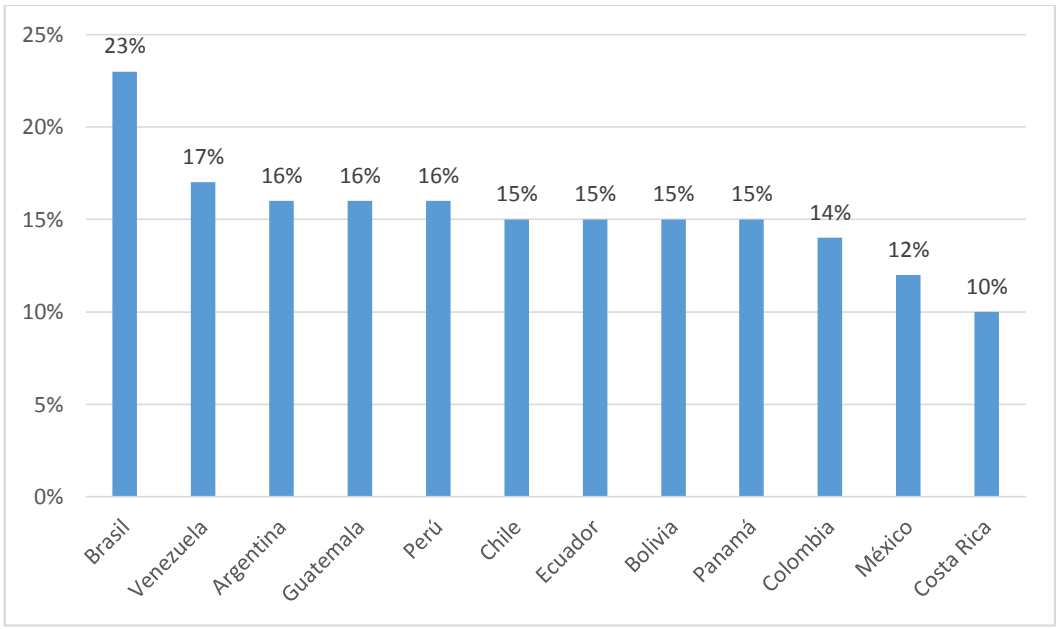


Figura 85: Ranking de países latinoamericanos afectados por phishing durante los primeros 7 meses de 2018

SYMATEC

En la 24ª edición del Informe Anual de Seguridad (ISTR) de Symantec, la compañía especialista en ciberseguridad, dentro del contexto latinoamericano, posiciona a Brasil como el país con mayores ataques informáticos seguido de México y Venezuela. Estos resultados fueran basados en ocho métricas, entre estas se toma en cuenta el malware y sus derivados (spam, phishing, bots, etc) y ransomware [37].

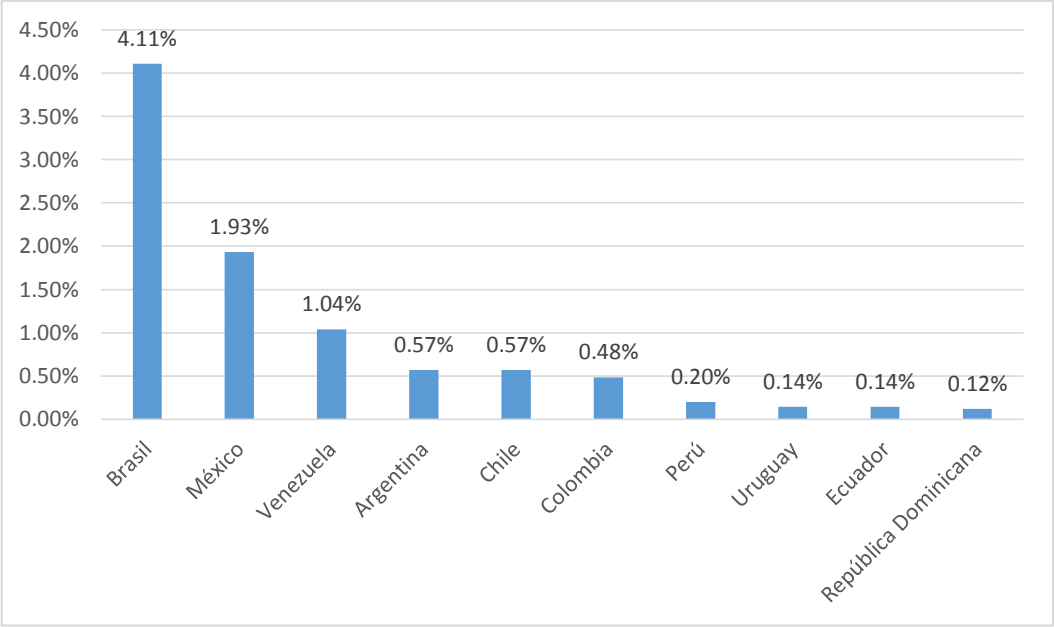


Figura 86: Top 10 de amenazas detectadas en América Latina y el Caribe por país

Anexo 5: LOGS DE AVIRA

MALWARE: ANTIEXE
Comienzo del análisis: 2019-11-11 15:33:40 11/11/2019,15:33:40.954 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\AntiExe.A\AntiExe.A\Anti_EXE_BOOT.IMA 11/11/2019,15:33:40.954 [INFO] [DETECTION] file contains 'AntiExe' 11/11/2019,15:33:45.173 [INFO] repair.rdf loaded (version: 1.0.52.22) 11/11/2019,15:33:45.188 [INFO] Repair of Generic started. 11/11/2019,15:33:45.204 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future 11/11/2019,15:33:45.204 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future 11/11/2019,15:33:45.204 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future 11/11/2019,15:33:45.204 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future 11/11/2019,15:33:45.204 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future 11/11/2019,15:33:45.204 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future 11/11/2019,15:33:45.204 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future 11/11/2019,15:33:45.204 [WARN] Can't set registry value: RootKey:HKEY_LOCAL_MACHINESubKey:SOFTWARE\WOW6432Node\Avira\Antivirus\Overwrite_Keys\HKEY_USERS\S-1-5-21-29309056-561047823-3208175115-1001\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell ValueName: UseAsDefault (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2 11/11/2019,15:33:45.204 [WARN] Can't set registry value: RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ValueName: shell (64 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2 11/11/2019,15:33:45.204 [WARN] Can't set registry value: RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ValueName: shell (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2 11/11/2019,15:33:49.298 [INFO] Repair of Generic finished successfully. 11/11/2019,15:33:49.298 [INFO] Repair of AntiExe started. 11/11/2019,15:33:49.298 [WARN] Repair.rdf: MalwareID: antiexe or its sub id's are not defined in the malware table 11/11/2019,15:33:49.313 [INFO] Repair of AntiExe finished successfully. 11/11/2019,15:33:49.313 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\AntiExe.A\AntiExe.A\Anti_EXE_BOOT.IMA 11/11/2019,15:33:49.313 [INFO] [ACTION] Clean -- End of scan : 2019-11-11 15:33:49 Duration : 00m:08s:593ms The scan has been done completely. 0 Scanned directories 0 Scanned archives 1 Scanned files 0 Skipped files 0 Ignored files 1 Detected files 1 Infected files cleaned 11 Warnings

MALWARE BACKDOOR.MSIL.Tyupkin
Comienzo del análisis: 2019-11-11 12:27:01
11/11/2019,12:27:04.188 [ERROR] FP notifica un error 0x1F para el archivo 'C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin.a.ViR' [I:10, S:111]
11/11/2019,12:27:04.188 [INFO] Modo de análisis de productos 1 activado (FP) [I:10, S:111]
11/11/2019,12:27:04.188 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin.a.ViR
11/11/2019,12:27:04.188 [INFO] [DETECTION] file contains 'TR/Rogue.118784.17'
11/11/2019,12:27:04.376 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin.c.ViR
11/11/2019,12:27:04.376 [INFO] [DETECTION] file contains 'BDS/Aladino.118784'
11/11/2019,12:27:04.501 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.Win32.Tyupkin.c2.ViR
11/11/2019,12:27:04.501 [INFO] [DETECTION] file contains 'BDS/Rogue.912297'
11/11/2019,12:27:04.673 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.Win32.Tyupkin.d.ViR
11/11/2019,12:27:04.673 [INFO] [DETECTION] file contains 'BDS/Rogue.912833'
11/11/2019,12:27:04.751 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.Win32.Tyupkin.h.exe.ViR
11/11/2019,12:27:04.751 [INFO] [DETECTION] file contains 'BDS/Agent.122880.16'
11/11/2019,12:27:12.048 [INFO] repair.rdf loaded (version: 1.0.52.22)
11/11/2019,12:27:12.079 [INFO] Repair of Generic started.
11/11/2019,12:27:12.079 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:27:12.079 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:27:12.079 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:27:12.079 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:27:12.079 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:27:12.079 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:27:12.079 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:27:12.079 [WARN] Can't set registry value: RootKey: HKEY_LOCAL_MACHINE SubKey: SOFTWARE\WOW6432Node\Avira\Antivirus\Overwrite_Keys\HKEY_USERS\S-1-5-21-29309056-561047823-3208175115-1001\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell ValueName: UseAsDefault (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:27:12.095 [WARN] Can't set registry value: RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ValueName: shell (64 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:27:12.095 [WARN] Can't set registry value: RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ValueName: shell (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:27:16.360 [INFO] Repair of Generic finished successfully.
11/11/2019,12:27:16.376 [INFO] Repair of TR/Rogue.118784.17 started.
11/11/2019,12:27:27.626 [WARN] Variable :\ProductId\: is deprecated and will be removed in future
11/11/2019,12:27:28.188 [INFO] Repair of TR/Rogue.118784.17 finished successfully.
11/11/2019,12:27:28.204 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin.a.ViR
11/11/2019,12:27:28.204 [INFO] [ACTION] Clean
11/11/2019,12:27:28.204 [INFO] Repair of BDS/Aladino.118784 started.
11/11/2019,12:27:38.438 [INFO] Repair of BDS/Aladino.118784 finished successfully.
11/11/2019,12:27:38.438 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin.c.ViR
11/11/2019,12:27:38.454 [INFO] [ACTION] Clean
11/11/2019,12:27:38.454 [INFO] Repair of BDS/Rogue.912297 started.
11/11/2019,12:27:48.688 [INFO] Repair of BDS/Rogue.912297 finished successfully.
11/11/2019,12:27:48.688 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.Win32.Tyupkin.c2.ViR
11/11/2019,12:27:48.688 [INFO] [ACTION] Clean
11/11/2019,12:27:48.704 [INFO] Repair of BDS/Rogue.912833 started.
11/11/2019,12:27:58.782 [INFO] Repair of BDS/Rogue.912833 finished successfully.

```
11/11/2019,12:27:58.798 [INFO]  C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.Win32.Tyupkin.d.ViR
11/11/2019,12:27:58.798 [INFO]  [ACTION] Clean
11/11/2019,12:27:58.798 [INFO]  Repair of BDS/Agent.122880.16 started.
11/11/2019,12:28:09.782 [INFO]  Repair of BDS/Agent.122880.16 finished successfully.
11/11/2019,12:28:09.782 [INFO]  C:\Users\LABMW-W7\Documents\MUESTRAS\Backdoor.MSIL.Tyupkin\Backdoor.MSIL.Tyupkin\Backdoor.Win32.Tyupkin.h.exe.ViR
11/11/2019,12:28:09.782 [INFO]  [ACTION] Clean
------------------------------------------------------------
End of scan : 2019-11-11 12:28:09
Duration : 01m:08s:047ms
The scan has been done completely.
    0 Scanned directories
    0 Scanned archives
    6 Scanned files
    0 Skipped files
    0 Ignored files
    5 Detected files
    5 Infected files cleaned
   11 Warnings
```

MALWARE: Keylogger.Ardamax

```
Comienzo del análisis: 2019-11-11 12:41:15
11/11/2019,12:41:16.001 [INFO]  C:\Users\LABMW-W7\Documents\MUESTRAS\Keylogger.Ardamax\Keylogger.Ardamax\ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18
11/11/2019,12:41:16.001 [INFO]  [DETECTION] file contains 'TR/Spy.Ardamax.ckp'
11/11/2019,12:41:27.813 [INFO]  repair.rdf loaded (version: 1.0.52.22)
11/11/2019,12:41:27.860 [INFO]  Repair of Generic started.
11/11/2019,12:41:27.860 [WARN]  Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:41:27.860 [WARN]  Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:41:27.860 [WARN]  Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:41:27.860 [WARN]  Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:41:27.860 [WARN]  Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:41:27.876 [WARN]  Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:41:27.876 [WARN]  Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:41:27.876 [WARN]  Can't set registry value:  RootKey: HKEY_LOCAL_MACHINE SubKey: SOFTWARE\WOW6432Node\Avira\Antivirus\Overwrite_Keys\HKEY_USERS\S-1-5-21-29309056-561047823-
3208175115-1001\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell ValueName: UseAsDefault (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:41:27.876 [WARN]  Can't set registry value:  RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
ValueName: shell (64 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:41:27.876 [WARN]  Can't set registry value:  RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
ValueName: shell (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:41:31.970 [INFO]  Repair of Generic finished successfully.
11/11/2019,12:41:31.970 [INFO]  Repair of TR/Spy.Ardamax.ckp started.
11/11/2019,12:41:40.891 [WARN]  Variable :\ProductId\: is deprecated and will be removed in future
11/11/2019,12:41:41.454 [INFO]  Repair of TR/Spy.Ardamax.ckp finished successfully.
11/11/2019,12:41:41.470 [INFO]  C:\Users\LABMW-W7\Documents\MUESTRAS\Keylogger.Ardamax\Keylogger.Ardamax\ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18
11/11/2019,12:41:41.470 [INFO]  [ACTION] Clean
------------------------------------------------------------
End of scan : 2019-11-11 12:41:41
Duration : 00m:25s:812ms
```

MALWARE: Ransomware.Cryptowall

```
Comienzo del análisis: 2019-11-11 12:55:25
11/11/2019,12:55:25.829 [INFO]    C:\Users\LABMW-W7\Documents\MUESTRAS\Ransomware.Cryptowall\Ransomware.Cryptowall\cryptowall.bin
11/11/2019,12:55:25.829 [INFO]    [DETECTION] file contains 'TR/Crypt.XPACK.134743'
11/11/2019,12:55:33.173 [INFO]    repair.rdf loaded (version: 1.0.52.22)
11/11/2019,12:55:33.188 [INFO]    Repair of Generic started.
11/11/2019,12:55:33.204 [WARN]    Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:55:33.204 [WARN]    Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:55:33.204 [WARN]    Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:55:33.220 [WARN]    Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:55:33.220 [WARN]    Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:55:33.220 [WARN]    Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:55:33.220 [WARN]    Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:55:33.220 [WARN]    Can't set registry value:  RootKey: HKEY_LOCAL_MACHINE SubKey: SOFTWARE\WOW6432Node\Avira\Antivirus\Overwrite_Keys\HKEY_USERS\S-1-5-21-29309056-561047823-
3208175115-1001\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell ValueName: UseAsDefault (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:55:33.220 [WARN]    Can't set registry value:  RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
ValueName: shell (64 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:55:33.220 [WARN]    Can't set registry value:  RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
ValueName: shell (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:55:37.485 [INFO]    Repair of Generic finished successfully.
11/11/2019,12:55:37.485 [INFO]    Repair of TR/Crypt.XPACK.134743 started.
11/11/2019,12:55:49.657 [WARN]    Variable :\ProductId\: is deprecated and will be removed in future
11/11/2019,12:55:50.251 [INFO]    Repair of TR/Crypt.XPACK.134743 finished successfully.
11/11/2019,12:55:50.251 [INFO]    C:\Users\LABMW-W7\Documents\MUESTRAS\Ransomware.Cryptowall\Ransomware.Cryptowall\cryptowall.bin
11/11/2019,12:55:50.251 [INFO]    [ACTION] Clean
----------------------------------------------------------------
End of scan : 2019-11-11 12:55:50
Duration : 00m:24s:656ms
The scan has been done completely.
     0 Scanned directories
     0 Scanned archives
     1 Scanned files
     0 Skipped files
     0 Ignored files
     1 Detected files
     1 Infected files cleaned
    11 Warnings
```

MALWARE: Trojan.Bladabindi

Comienzo del análisis: 2019-11-11 13:04:22
11/11/2019,13:04:22.204 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Trojan.Bladabindi\Trojan.Bladabindi\hostr.exe
11/11/2019,13:04:22.204 [INFO] [DETECTION] file contains 'TR/Barys.10755412'
11/11/2019,13:04:32.048 [INFO] repair.rdf loaded (version: 1.0.52.22)
11/11/2019,13:04:32.079 [INFO] Repair of Generic started.
11/11/2019,13:04:32.079 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,13:04:32.079 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,13:04:32.095 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,13:04:32.095 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,13:04:32.095 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,13:04:32.095 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,13:04:32.095 [WARN] Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,13:04:32.095 [WARN] Can't set registry value: RootKey: HKEY_LOCAL_MACHINE SubKey: SOFTWARE\WOW6432Node\Avira\Antivirus\Overwrite_Keys\HKEY_USERS\S-1-5-21-29309056-561047823-3208175115-1001\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell ValueName: UseAsDefault (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,13:04:32.095 [WARN] Can't set registry value: RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ValueName: shell (64 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,13:04:32.095 [WARN] Can't set registry value: RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ValueName: shell (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,13:04:36.188 [INFO] Repair of Generic finished successfully.
11/11/2019,13:04:36.188 [INFO] Repair of TR/Barys.10755412 started.
11/11/2019,13:04:45.970 [WARN] Variable :\ProductId\: is deprecated and will be removed in future
11/11/2019,13:04:46.595 [INFO] Repair of TR/Barys.10755412 finished successfully.
11/11/2019,13:04:46.610 [INFO] C:\Users\LABMW-W7\Documents\MUESTRAS\Trojan.Bladabindi\Trojan.Bladabindi\hostr.exe
11/11/2019,13:04:46.610 [INFO] [ACTION] Clean

End of scan : 2019-11-11 13:04:46
Duration : 00m:24s:750ms

The scan has been done completely.

0 Scanned directories
0 Scanned archives
1 Scanned files
0 Skipped files
0 Ignored files
1 Detected files
1 Infected files cleaned
11 Warnings

MALWARE: 798_abroad.exe

```
Comienzo del análisis: 2019-11-11 12:13:14
11/11/2019,12:13:16.876 [ERROR]    FP notifica un error 0x1F para el archivo 'C:\Users\LABMW-W7\Documents\MUESTRAS\Trojan.Dropper.Gen\Trojan.Dropper.Gen\798_abroad.exe' [I:10, S:111]
11/11/2019,12:13:16.891 [INFO]     C:\Users\LABMW-W7\Documents\MUESTRAS\Trojan.Dropper.Gen\Trojan.Dropper.Gen\798_abroad.exe
11/11/2019,12:13:16.891 [INFO]     [DETECTION] file contains 'TR/Dropper.Gen'
11/11/2019,12:13:21.938 [INFO]     repair.rdf loaded (version: 1.0.52.22)
11/11/2019,12:13:22.032 [INFO]     Repair of Generic started.
11/11/2019,12:13:22.032 [WARN]     Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:13:22.032 [WARN]     Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:13:22.032 [WARN]     Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:13:22.032 [WARN]     Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:13:22.032 [WARN]     Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:13:22.032 [WARN]     Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:13:22.032 [WARN]     Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,12:13:22.032 [WARN]     Can't set registry value:  RootKey: HKEY_LOCAL_MACHINE SubKey: SOFTWARE\WOW6432Node\Avira\Antivirus\Overwrite_Keys\HKEY_USERS\S-1-5-21-29309056-561047823-
3208175115-1001\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell ValueName: UseAsDefault (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:13:22.032 [WARN]     Can't set registry value:  RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
ValueName: shell (64 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:13:22.032 [WARN]     Can't set registry value:  RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
ValueName: shell (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,12:13:34.501 [INFO]     Repair of Generic finished successfully.
11/11/2019,12:13:34.532 [INFO]     Repair of TR/Dropper.Gen started.
11/11/2019,12:13:47.329 [WARN]     Variable :\ProductId\: is deprecated and will be removed in future
11/11/2019,12:13:47.970 [INFO]     Repair of TR/Dropper.Gen finished successfully.
11/11/2019,12:13:47.970 [INFO]     C:\Users\LABMW-W7\Documents\MUESTRAS\Trojan.Dropper.Gen\Trojan.Dropper.Gen\798_abroad.exe
11/11/2019,12:13:47.970 [INFO]     [ACTION] Clean
------------------------------------------------------------
End of scan : 2019-11-11 12:13:48
Duration : 00m:33s:906ms
The scan has been done completely.
    0 Scanned directories
    1 Scanned archives
    1 Scanned files
    0 Skipped files
    0 Ignored files
    1 Detected files
    1 Infected files cleaned
   11 Warnings
```

MALWARE: AntiExe

```
Comienzo del análisis: 2019-11-11 15:33:40
11/11/2019,15:33:40.954 [INFO]	C:\Users\LABMW-W7\Documents\MUESTRAS\AntiExe.A\AntiExe.A\Anti_EXE_BOOT.IMA
11/11/2019,15:33:40.954 [INFO]	[DETECTION] file contains 'AntiExe'
11/11/2019,15:33:45.173 [INFO]	repair.rdf loaded (version: 1.0.52.22)
11/11/2019,15:33:45.188 [INFO]	Repair of Generic started.
11/11/2019,15:33:45.204 [WARN]	Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,15:33:45.204 [WARN]	Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,15:33:45.204 [WARN]	Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,15:33:45.204 [WARN]	Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,15:33:45.204 [WARN]	Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,15:33:45.204 [WARN]	Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,15:33:45.204 [WARN]	Variable :\OverwriteKey\: is deprecated and will be removed in future
11/11/2019,15:33:45.204 [WARN]	Can't set registry value:  RootKey: HKEY_LOCAL_MACHINE SubKey: SOFTWARE\WOW6432Node\Avira\Antivirus\Overwrite_Keys\HKEY_USERS\S-1-5-21-29309056-561047823-3208175115-1001\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\shell ValueName: UseAsDefault (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,15:33:45.204 [WARN]	Can't set registry value:  RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ValueName: shell (64 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,15:33:45.204 [WARN]	Can't set registry value:  RootKey: HKEY_USERS SubKey: S-1-5-21-29309056-561047823-3208175115-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ValueName: shell (32 bit): El sistema no puede encontrar el archivo especificado.. Error Code: 2
11/11/2019,15:33:49.298 [INFO]	Repair of Generic finished successfully.
11/11/2019,15:33:49.298 [INFO]	Repair of AntiExe started.
11/11/2019,15:33:49.298 [WARN]	Repair.rdf: MalwareID: antiexe or its sub id's are not defined in the malware table
11/11/2019,15:33:49.313 [INFO]	Repair of AntiExe finished successfully.
11/11/2019,15:33:49.313 [INFO]	C:\Users\LABMW-W7\Documents\MUESTRAS\AntiExe.A\AntiExe.A\Anti_EXE_BOOT.IMA
11/11/2019,15:33:49.313 [INFO]	[ACTION] Clean
------------------------------------------------------------
End of scan : 2019-11-11 15:33:49
Duration : 00m:08s:593ms
The scan has been done completely.
    0 Scanned directories
    0 Scanned archives
    1 Scanned files
    0 Skipped files
    0 Ignored files
    1 Detected files
    1 Infected files cleaned
   11 Warnings
```

Anexo 6: Normas de seguridad informática

POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA

I. INTRODUCCIÓN

Con la definición de las políticas y estándares de seguridad informática se busca establecer en el interior de los laboratorios de la Facultad de Sistemas y Telecomunicaciones una cultura de calidad operando en una forma confiable.

La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de los entes de la Facultad en materia de seguridad.

Las normas y políticas han sido establecidas según las siguientes normas ISO:

ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.

ISO/IEC 27004 Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.

Cabe indicar que las normas expuestas en este documento sirven de referencia, en ningún momento pretenden ser normas absolutas, las mismas están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad de la información y los servicios prestados por la red a los usuarios finales.

Toda persona que utilice los servicios que ofrece la red y los dispositivos informáticos, deberá conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

NORMAS COMPLEMENTARIAS ESPECÍFICAS

DE LOS LABORATORIOS DE INFORMÁTICA

1) Las computadoras de los laboratorios estarán registradas en el firewall Pfsense para tener un control de cada una de ellas.

2) Los estudiantes que deseen utilizar sus equipos en la red alámbrica de los laboratorios deberán registrar su MAC con el administrador encargado.

3) El monitoreo del tráfico de las máquinas en el firewall se darán de manera constante, en caso de verificar un tráfico anormal se procederá a tomar acciones en la máquina involucrada.

4) Se restringirán los sitios web que contengan software malicioso.

5) Las máquinas infectadas deberán ser analizadas en el laboratorio virtual siguiendo los protocolos correspondientes

6) Los reportes generados por el Lightsquis (herramienta del firewall Pfsense) se realizarán cada semana para su debido análisis. En caso de sospecha de software malicioso se procederá con su inmediato análisis.

7) El uso de dispositivos externos debe ser aprobado por el encargado de los laboratorios y comunicado a el administrador.

8) Las máquinas que se encuentran en los laboratorios deberán ser etiquetadas y reportados en el caso de alterarse el orden donde se encuentran ubicadas originalmente.

Anexo 7: Reporte Urkund

IC-FIT-INF-005

La Libertad, 11 de febrero del 2020

Ing. Freddy Villao S.
Director (E) de Carrera
En su despacho.

Por medio de la presente me es muy grato saludarle y poner a su disposición el resultado del análisis del software anti-plagio URKUND del documento con el tema de titulación "LABORATORIO VIRTUAL DE ANÁLISIS Y COMPORTAMIENTO DE MALWARE BASADO EN TÉCNICAS Y MÉTODOS DE SEGURIDAD INFORMÁTICA PARA LOS LABORATORIOS EN LA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES", correspondiente a la Sra. LITUMA BRIONES LINDA CAROLINA, estudiante de la Carrera de Informática.

URKUND

Urkund Analysis Result

Analysed Document:	CAROLINA LITUMA BRIONES.docx (D63746838)
Submitted:	2/11/2020 2:15:00 PM
Submitted By:	${Xml.Encode(Model.Document.Submitter.Email)}
Significance:	1 %

Ing. Iván Coronel Suárez, MSIA

Docente Tutor

C.C.: Dirección Carrera Informática, Archivo

UPSE
DECANATO DE SISTEMAS Y TELECOMUNICACIONES
RECIBIDO
FECHA: 11 FEB 20
HORA: 11:30
FIRMA AUTORIZADA