# Instituto Tecnológico y de Estudios Superiores de Monterrey

## MA2005B Aplicación de Criptografía y Seguridad 101

Profesor: Oscar Labrada

# Análisis de Malware en Máquina Virtual

Evidencia 1 - Examen argumentativo (Reporte Técnico)


**Equipo 5:**

Joana Itzel Barreto López A01425283
Carlos Alberto Gómez San Pedro A01658377
Joaquin Sainz Muleiro A01783801
Maximiliano García Suástegui A01657689
Arath Mendivil Mora A01660670



Campus Monterrey
5 de septiembre de 2024

# Análisis de Malware en Máquina Virtual

## Contents

# 1 Introducción

## 1.1 Contexto del Proyecto

En el mundo de la ciberseguridad, uno de los mayores desafíos es protegerse del malware, que es el código maligno creado con la intención de dañar o robar información de las computadoras. El crecimiento continuo de tales amenazas ha permitido la creación de soluciones sólidas de seguridad informática, como los antivirus, para identificar, bloquear y erradicar los códigos dañinos antes de que puedan hacer algo malo. Sin embargo, la investigación y el análisis del comportamiento del malware en un entorno controlado son críticos para hacer que esas herramientas sean más potentes y precisas. Este fue

un proyecto que involucró la ejecución y el análisis del malware en una máquina virtual, teniendo el software antivirus Kaspersky como la medida de protección y prevención. Para lograr esto, se descargaron, ejecutaron y analizaron cinco muestras de códigos maliciosos para probar las capacidades del software de detección y prevención de amenazas con respecto a su identificación y eliminación de peligros.

## 1.2 Objetivos

Como se mencionó, el propósito principal de este proyecto es estudiar varios tipos de malware a través de su ejecución en un entorno controlado y observar el comportamiento del código malicioso junto con la respuesta del software Kaspersky. A partir de ello buscamos dar respuestas a las siguientes preguntas:

- ¿Qué ofrece Kaspersky como una característica de seguridad en términos de detección y eliminación de malware?
- ¿Qué hace cada malware y cuáles son sus posibles efectos en un sistema vulnerable?
- ¿Cuál de los malwares examinados fue el más complejo de seguir y analizar? ¿por qué?
- ¿Cuál de ellos es el más peligroso para el sistema?

Como parte de este estudio, se presenta un informe detallado de todas las amenazas, incluyendo su comportamiento y su impacto en el sistema, también se evalúa la efectividad de la plataforma proporcionada por el socioformador, Kaspersky, para encontrar, bloquear y eliminar las amenazas.

# 2 Metodología

## 2.1 Entornos Virtuales Utilizados

Para el desarrollo del proyecto, se utilizaron dos máquinas virtuales (VMs) con diferentes sistemas operativos: una VM con *macOS* y otra con *Windows 10*. A continuación, se describen brevemente las características de cada VM y el proceso de configuración de los entornos.

### 2.1.1 Máquina Virtual con macOS

La primera VM ejecutó *macOS Sonoma*, siendo el entorno principal para el análisis de este proyecto. El software de virtualización utilizado para esta VM es Parallels Desktop que es un software de virtualización para macOS que permite ejecutar sistemas operativos adicionales en máquinas virtuales dentro de una Mac.

La configuración de la máquina virtual con macOS incluyó los siguientes pasos:

1. **Descarga de Parallels**: Se descargó e instaló la herramienta de virtualización *Parallels* desde su sitio web oficial. Este software permite la creación y gestión de máquinas virtuales con una variedad de sistemas operativos.
2. **Configuración del Entorno de Virtualización**: A través del software, se especificó el sistema operativo que tendría la VM y se dejaron las configuracions prestablecidas.
3. **Instalación del Sistema Operativo**: Se utilizó una imagen oficial de macOS para llevar a cabo la instalación.

Las características de esta VM fueron:

- **Versión de macOS:**La versión del sistema operativo corresponde a Sonoma 14.6
- **Memoria RAM Asignada:** 6 GB
- **Espacio en Disco Duro:** 256 GB
- **Configuración de Red:** Red interna
- **Configuración de Procesadores:** 2 Núcleos de CPU

### 2.1.2 Máquina Virtual con Windows 10

La segundad VM se configuró utilizando el sistema operativo *Windows 10*, descargado y ejecutado a través del software de virtualización *Oracle VirtualBox*. El proceso de configuración general fue el siguiente:

1. **Descarga de Oracle VirtualBox**: Se descargó e instaló la herramienta de virtualización *Oracle VirtualBox* desde su sitio web oficial. Este software permite la creación y gestión de máquinas virtuales con una variedad de sistemas operativos.
2. **Creación de la VM**: A través del asistente de creación de VM de VirtualBox, se seleccionaron las configuraciones iniciales, incluyendo la asignación de memoria RAM, procesadores y espacio en disco virtual.
3. **Instalación de Windows 10**: Se utilizó una imagen de disco de instalación (*.iso*) oficial de *Windows 10*. La instalación del sistema operativo se realizó de manera estándar, siguiendo el asistente de instalación de Windows.

Las características específicas de la VM con Windows 10 fueron las siguientes:

- **Sistema Operativo y Versión:** Windows 10 (64-bit)
- **Memoria RAM Asignada:** 4 GB
- **Espacio en Disco Duro:** 25 GB (Almacenamiento Dinámico)
- **Configuración de Red:** Red interna
- **Configuración de Procesadores:** 1 Núcleo de CPU

## 2.2 Obtención de Malware

Para llevar a cabo el análisis, se utilizaron diferentes fuentes de malware según el sistema operativo de las máquinas virtuales.

Para el caso de la máquina virtual con macOS, los códigos maliciosos fueron descargados desde **M**alware Bazaar. Se seleccionaron los siguientes tipos de malware:

| **Nombre** | **Tipo de Malware** | **Descripción Técnica** |
|---|---|---|
| **OSX.Defma** | Adware/FakeAV | Muestra falsas alertas de seguridad para engañar a los usuarios y redirigirlos a sitios web no seguros. Principalmente molesto con ventanas emergentes. |
| **OSX.Amos** | Spyware | Recolecta información privada del usuario, como datos de navegación y credenciales, y la envía a servidores remotos. |

En la máquina virtual con Windows 10, los códigos maliciosos fueron descargados desde el repositorio de GitHub *The Zoo*, el cual contiene una amplia colección de muestras de malware para propósitos de investigación y análisis. Se descargaron las siguientes muestras:

| **Nombre** | **Tipo de Malware** | **Descripción Técnica** |
|---|---|---|
| **Zeus (Zbot)** | Troyano bancario | Diseñado para robar información bancaria y credenciales. Funciona a través de keylogging y modificación de páginas web en navegadores. |
| **AgentTesla** | RAT (Remote Access Trojan) | Actúa como un spyware y keylogger, recolectando credenciales y datos almacenados. Se distribuye a menudo por correos electrónicos maliciosos. |
| **ZeroAccess** | Rootkit | Obtiene acceso administrativo, permite el control remoto del equipo y se oculta de antivirus. Se usa en redes botnet y para actividades ilegales como minería de criptomonedas. |

Todas las muestras de malware estaban comprimidas en archivos *.zip*, los cuales requerían contraseñas específicas para su extracción. Se manejaron con sumo cuidado en un entorno controlado y seguro para minimizar los riesgos. Las contraseñas fueron proporcionadas por los mismos repositorios o fuentes.

## 2.3 Ejecución del Malware

La ejecución de los códigos maliciosos se llevó a cabo de forma diferenciada entre las dos máquinas virtuales, asegurando siempre que cada prueba se realizaba en un entorno aislado.

En la máquina virtual con *Windows 10*, los códigos *Zeus* y *ZeroAccess* se ejecutaron antes de instalar Kaspersky, lo que permitió observar cómo estos malwares interactúan con el sistema sin la interferencia de un antivirus. Ambos códigos fueron ejecutados sin protección, lo que resultó en diferentes efectos dentro de la VM, incluyendo alteración de archivos, configuraciones críticas del sistema y la ralentización del mismo.

Después de la instalación de Kaspersky, se intentó ejecutar los malwares *AgentTesla*, *Zeus* y *ZeroAccess* nuevamente. Sin embargo, Kaspersky detectó y bloqueó su ejecución casi de inmediato, mostrando una gran efectividad en su sistema de detección.

En cuanto a la máquina virtual con macOS, se ejecutaron los malwares *OSX.Defma* y *OSX.Amos*. Debido a la naturaleza menos agresiva del primero (adware), su impacto fue principalmente la generación de alertas falsas y ventanas emergentes.

En cambio, *OSX.Amos*, al ser spyware, trató de ejecutar en segundo plano procesos para recolectar información del sistema, pero fue eventualmente detectado y detenido por las herramientas de seguridad.

Uno de los principales problemas encontrados fue que tras la ejecución de *ZeroAccess* en la VM de Windows sin protección, el sistema quedó inutilizable, obligando a restablecer la máquina virtual para poder continuar con las pruebas. Esto demostró la gravedad y complejidad de algunos de los malwares probados.

# 3 Resultados

En esta sección, se presentan los resultados obtenidos durante el análisis de los códigos maliciosos en las VMs. Los resultados incluyen observaciones sobre el comportamiento de cada malware, la efectividad de Kaspersky en la detección y prevención, así como una evaluación de la complejidad y peligrosidad de cada código malicioso.

## 3.1 Resultados en la VM de macOS

En la VM con macOS, *OSX.Defma* se comportó como un adware típico, redirigiendo la navegación a sitios web llenos de publicidad no deseada. El malware intentó modificar el motor de búsqueda predeterminado del navegador, cambiando las configuraciones de Safari y Chrome, y agregar extensiones maliciosas sin el consentimiento del usuario. Kaspersky detectó y bloqueó estas modificaciones, identificando los archivos y procesos relacionados con *OSX.Defma* como adware de bajo riesgo. La herramienta de eliminación de adware integrada en Kaspersky fue finalmente efectiva para limpiar por completo el sistema.

Por otro lado, *OSX.Amos* mostró un comportamiento más agresivo. Se trata de un troyano que permite acceso remoto al sistema infectado. Durante las pruebas, *OSX.Amos* intentó establecer conexiones no autorizadas con servidores externos, lo que fue bloqueado por Kaspersky en tiempo real. El malware también trató de obtener privilegios de administrador mediante la ejecución de scripts ocultos para tener control completo del sistema. Kaspersky detectó estos intentos y, posteriormente, puso en cuarentena los archivos maliciosos. A diferencia de *OSX.Defma*, *OSX.Amos* fue detectado como una amenaza de mayor riesgo debido a su capacidad para comprometer la seguridad y privacidad del sistema, permitiendo potencialmente a los atacantes robar datos sensibles y realizar acciones remotas en la máquina virtual.

## 3.2 Resultados en la VM de Windows

El análisis de los malwares en la VM con Windows 10 reveló comportamientos distintivos de cada uno. **Zeus (Zbot)**, un troyano bancario, se ejecutó exitosamente antes de instalar Kaspersky pero no generó daños significativos al sistema por la falta de información para *robar*.

**AgentTesla**, un Remote Access Trojan (RAT), fue facilmente bloqueado por Kaspersky al momento de intentar su ejecución. El software antivirus identificó el malware en tiempo real y previno su actividad maliciosa.

Por último, **ZeroAccess** ocultó archivos y procesos, causando que la VM se volviera inestable y requiriera un restablecimiento. Posteriormente, Kaspersky bloqueó el malware antes de que pudiera ejecutarse completamente, evitando que causara más daños al sistema.

## 3.3 Evaluación de Complejidad y Peligrosidad

Entre los malwares analizados, ZeroAccess se destacó como el más complejo de analizar debido a su naturaleza de rootkit. Su capacidad para ocultarse y alterar el sistema

provocó una inestabilidad significativa, complicando su análisis.

Por otro lado, *OSX.Amos* y *ZeroAccess* fueron identificados como los más peligrosos: OSX.Amos, por su habilidad para credenciales y datos de navegación por su naturaleza de "espía", y ZeroAccess, por su capacidad para tomar control del sistema y ocultarse de los antivirus. Aunque el potencial peligro de OSX.Amos no fue explotado dada a la falta de información disponible en la VM de macOS lo consideramos como un malware de alto riesgo.

## 3.4 Eficiencia de Kaspersky

Kaspersky demostró una alta eficacia en la detección y prevención de malware en tiempo real. Los malwares que intentaron ejecutarse después de la instalación de Kaspersky fueron detectados y bloqueados de manera efectiva.

Este análisis revela que Kaspersky no solo detecta y previene amenazas conocidas, sino que también ofrece una respuesta efectiva ante intentos de ejecución de malware, lo que resulta crucial para la seguridad en entornos de pruebas y uso real.

# 4 Referencias

The Zoo. (s.f.). The Zoo: A collection of malware samples. https://github.com/ytisf/theZoo

About Kaspersky Internet Security. (s.f.). https://support.kaspersky.com/KIS/2020/en-us/87342.htm

¿Qué es la ciberseguridad? — Seguridad de Microsoft. (s.f.).https://www.microsoft.com/es-es/security/business/security-101/what-is-cybersecurity

Threat Encyclopedia — Trend Micro (US). (s.f.). https://www.trendmicro.com/vinfo/us/threat-encyclopedia