







¿Cómo Funciona un Antivirus? ☐☐

Técnicas modernas de protección contra malware en la era digital

Introducción a los Antivirus Modernos

-  **Evolución significativa:** De simples detectores a suites de seguridad sofisticadas
-  **Múltiples capas de protección:** Combinación de técnicas tradicionales y avanzadas
-  **Inteligencia Artificial:** Detección más precisa contra amenazas sofisticadas
-  **Protección integral:** Contra todo tipo de malware (virus, spam, adware, spyware...)

"Los antivirus modernos monitorizan comportamientos 'sospechosos' y combinan varias técnicas para proteger el sistema."



Técnica de Scanning (Análisis por Firmas)

Definición

- ✓ Técnica tradicional que **compara archivos** con base de datos de patrones conocidos

Proceso Básico

- 1 Base de datos con **firmas de malware** conocido
- 2 Cálculo de "**huella digital**" (hash) del archivo
- 3 Comparación con firmas en la base de datos

Actualizaciones 2023-2024

- ↗ **Firmas de comportamiento** en lugar de estáticas
- ☁ **Cloud-based scanning** para mejor rendimiento

"En la primera ejecución, el programa debe descargar una base de datos de patrones. Sin ella, el antivirus no puede funcionar."

How Antivirus Software Works

Antivirus software uses one or more detection methods to examine unknown software for signs it is a virus.

To remove viruses or prevent their download, antivirus software uses:



Signature detection to look for specific code from known viruses.



Heuristic detection to find suspicious architecture and behavior in code.



Cloud and sandbox analysis to run suspicious programs inside a contained and secure system to see what they do.



HIPS (Host Intrusion Prevention System) as a way to bridge firewalls and other security systems for added protection.

🧠 Técnicas Heurísticas y de Análisis Comportamental

📌 Definición

Métodos que detectan **malware desconocido** analizando código y comportamiento en busca de patrones sospechosos

📌 Tipos de Análisis Heurístico (2023-2024)

🔗 Análisis Estático

Examina código **sin ejecutarlo**

- AST: árboles de sintaxis
- Control de flujo
- Análisis de dependencias

▶ Análisis Dinámico

Ejecuta código en **entorno aislado**

- Sandboxing en la nube
- Multi-OS simulation
- Análisis prolongado

📈 Comportamiento en Tiempo Real

Monitorea **actividades anómalas**

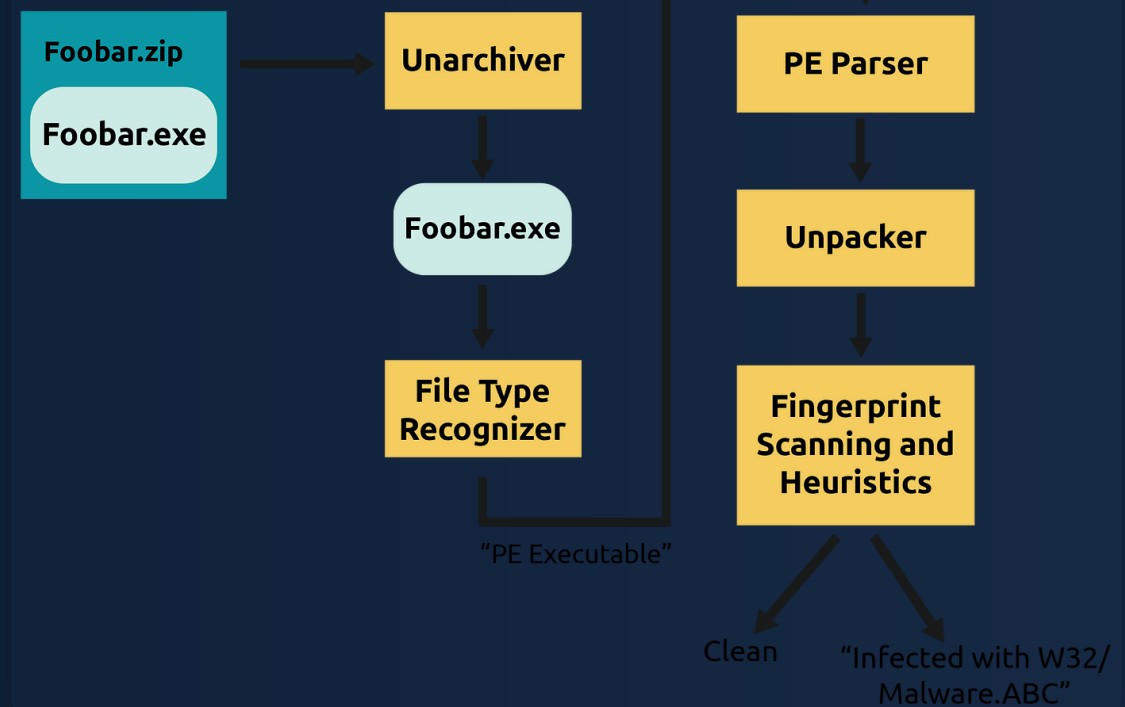
- Machine Learning
- Grafo de procesos
- Protección ransomware

🔍 Análisis de Memoria

Examina **memoria RAM**

- Inyección de código
- Objetos de memoria
- Rootkits y malware fileless

Here is how the AV Detection Engine works:



"Los sistemas modernos utilizan machine learning para reducir falsos positivos, aprendiendo de millones de muestras."

🔧 Inteligencia Artificial y Machine Learning en Antivirus

⚙️ Proceso Básico

1

Entrenamiento
con millones
de muestras

2

Extracción de
características

3

Creación de
modelos
predictivos

4

Implementación
en tiempo
real

🔗 Modelos de IA Utilizados



Redes Neuronales Convolucionales

Análisis de código como
"imágenes"
Detecta patrones visuales en el
código



Redes Neuronales Recurrentes

Análisis de **secuencias** de
comportamiento
Identifica patrones temporales



Modelos de Transformadores

Análisis de **código fuente** y
lenguaje
Detecta técnicas de ofuscación



Detección de Anomalías

Identifica comportamientos
inusuales
Detecta malware zero-day



Caso Práctico: Microsoft Defender con IA



200 billones de señales
diarias



Actualizaciones automáticas
diarias



1.200M amenazas bloqueadas



Detección en < 60 segundos



Técnicas Avanzadas Modernas (2023-2024)

Protección contra Evasión con IA

Detección y contrarrestamiento de técnicas avanzadas de evasión

- ✓ **Detección de sandboxing:** Identifica intentos de detectar entornos de análisis
- ✓ **Análisis de tiempo:** Detecta malware con activación retardada

Protección contra Ransomware

Mecanismos especializados para prevenir cifrado no autorizado

- ✓ **Controlled Folder Access:** Solo aplicaciones autorizadas pueden modificar carpetas críticas
- ✓ **Análisis de patrones:** Detecta intentos de cifrado masivo en tiempo real

Integración con Threat Intelligence

Conexión con redes globales de inteligencia sobre amenazas

- ✓ **Compartición de inteligencia:** Comunidades de seguridad comparten información sobre nuevas amenazas
- ✓ **Análisis de IOC:** Identificación rápida de patrones de ataque

Protección para Entornos Cloud

Extensión de la protección a entornos cloud y virtualizados

- ✓ **Análisis de tráfico cloud:** Monitoreo de APIs y servicios cloud
- ✓ **Protección de contenedores:** Detección de malware en entornos Docker y Kubernetes

Principales amenazas y vulnerabilidades en entornos cloud



Configuraciones incorrectas



Accesos no autorizados



Interfaces y APIs inseguras



Amenazas internas



Vulnerabilidades del sistema




Ataques de malware y ransomware


"La mayoría de virus entran en los sistemas vía correo electrónico. No abrir ni ejecutar ficheros adjuntos si no se conoce a ciencia cierta el contenido."

Cómo se Elimina un Virus

1 Aislamiento Inicial


El antivirus aísla el malware para evitar daños adicionales


 **Cuarentena:** Aísla archivos sin eliminarlos

 **Bloqueo C2:** Corta comunicación con servidores

2 Eliminación del Malware


El antivirus elimina el código malicioso del sistema

 **Eliminación precisa:** Solo código malicioso

 **Reparación:** Restaura archivos infectados

3 Restauración del Sistema

El antivirus restaura el sistema a su estado previo


 **Configuraciones:** Restaura parámetros alterados

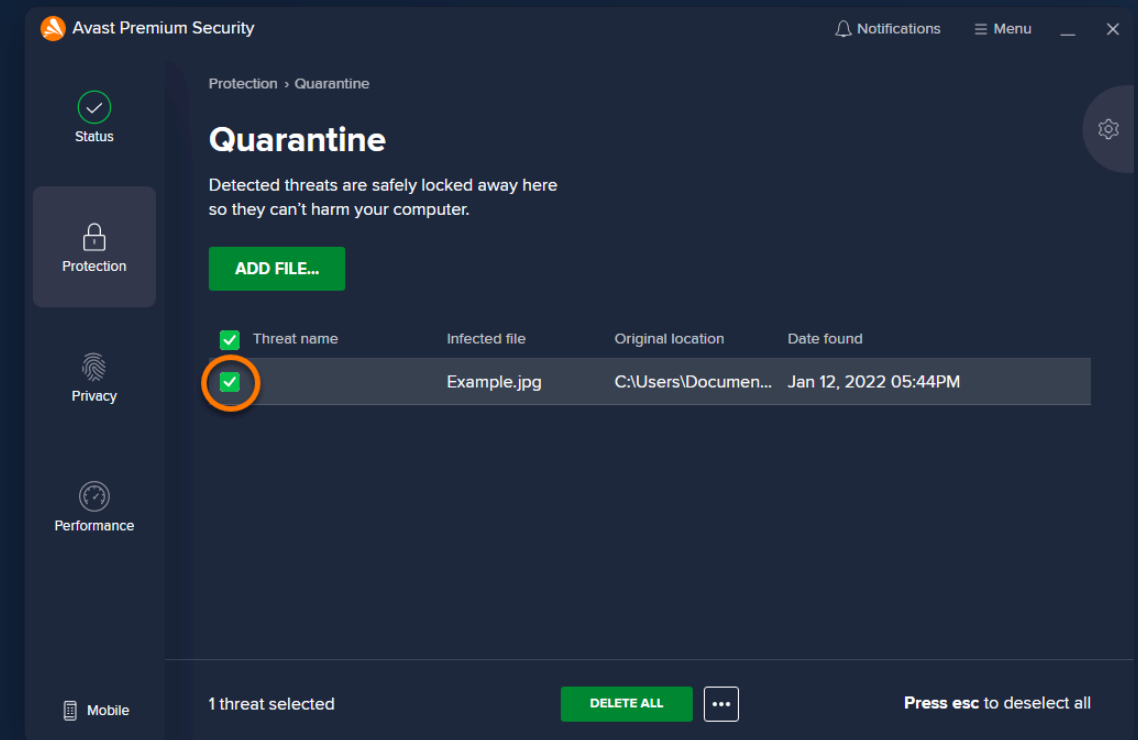
 **Registro:** Revierte modificaciones peligrosas

4 Protección Post-Infección

Implementa medidas para prevenir futuras infecciones

 **Firmas personalizadas:** Genera firmas específicas

 **Threat intelligence:** Comparte información



"La eliminación de un virus consiste en eliminar el archivo que contiene el virus o eliminar el código del virus dentro del archivo infectado. También el antivirus debería poder reparar cualquier daño causado en el equipo."

⚠ Limitaciones de los Antivirus Modernos y Cómo Superarlas

⚠ Limitaciones Inherentes

- ⚙️ **Amenazas Zero-Day**
No detectan amenazas completamente nuevas
- ⚙️ **Malware Fileless**
Reside solo en memoria RAM
- ⚙️ **Evasión con IA**
Atacantes usan IA para evadir detección
- 📈 **Crecimiento 2023**
+142% ataques con IA

🛡 Estrategias para Superarlas





- 🔍 **Defensa en Profundidad**
Combina múltiples capas de seguridad
- 🔄 **Actualizaciones Automáticas**
Mantén sistema y apps actualizadas
- 📁 **Copias de Seguridad**
Regla 3-2-1: 3 copias, 2 medios, 1 externa
- 🎓 **Educación Continua**
Capacita en identificación de amenazas

"Si sospechamos que tenemos un virus, intentar chequearlo con distintos antivirus para descartar el contagio."



Herramientas Esenciales para Técnicos de Reparación

Para Diagnóstico de Infecciones





- | | |
|--|---|
|  Microsoft Safety Scanner
Escaneo rápido sin instalación |  ESET Online Scanner
Base de datos actualizada en tiempo real |
|  Kaspersky Virus Removal Tool
Especializado en malware persistente |  Malwarebytes
Excelente para segunda opinión |

Para Limpieza Profunda

Procedimiento Recomendado

- | | |
|--|---|
| 1 Arrancar en Modo Seguro | 2 Copia de seguridad de datos |
| 3 Ejecutar Windows Defender | 4 Ejecutar Malwarebytes |
| 5 Usar herramientas especializadas | 6 Restaurar configuraciones |

Para Prevención de Futuras Infecciones

- | | |
|--|---|
|  Suite de Seguridad Confiable
2-3 opciones según necesidades |  Actualizaciones Automáticas
Sistema y aplicaciones |
|  Copias de Seguridad
Regla 3-2-1 |  Autenticación de Dos Factores
Para cuentas importantes |

