Universidad Internacional de La Rioja

Escuela Superior de Ingeniería y Tecnología

Máster Universitario en Ciberseguridad

Comparación de servicios automáticos on-line de análisis de malware

Trabajo Fin de Estudio presentado por:	Alfredo Palomo Verduras
Tipo de trabajo:	Piloto Experimental
Director/a:	Víctor Andrés Pimienta García
Fecha:	21/04/2025

Resumen

Este trabajo evalúa la eficacia de diversos servicios automáticos en línea para el análisis de malware, con el objetivo de determinar su precisión, rapidez y profundidad frente a distintas categorías de amenazas digitales. Para ello, se seleccionaron inicialmente 15 muestras representativas (ransomware, troyanos, spyware, etc.), modificadas durante el desarrollo experimental al incorporar variantes y combinaciones relevantes para enriquecer el análisis, que fueron analizadas mediante plataformas como VirusTotal, MetaDefender, Hybrid Analysis y Any.Run, combinando enfoques estático, dinámico y multiengine.

Los resultados muestran que ninguna plataforma destaca como universalmente superior, sino que su rendimiento varía según el tipo de malware y el objetivo del análisis. Se concluye que el uso combinado y contextualizado de estas herramientas permite una caracterización técnica fiable, y que el enfoque escalonado propuesto mejora la visibilidad, reduce falsos negativos y optimiza la toma de decisiones en ciberseguridad.

Palabras clave: análisis de malware, detección automática, sandbox, amenazas digitales, servicios online

Abstract

This study evaluates the effectiveness of various online automated malware analysis services, aiming to quantify their detection accuracy, analytical depth, and processing latency across different digital threat categories. Initially, a curated dataset of 15 real world malware samples was selected; this was later modified by incorporating additional variants and combinations to enrich the experimental analysis. These samples, including ransomware, trojans, spyware, adware, worms, and fileless malware, were analyzed using VirusTotal, MetaDefender Cloud, Hybrid Analysis, and Any.Run, combining static, dynamic, and multiengine approaches.

Results demonstrate that platform effectiveness is context dependent: static based services excel in initial triage, while dynamic sandboxes outperform in detecting persistence mechanisms, evasive tactics, and in-memory payloads. The study concludes that a tiered, combined approach enhances forensic visibility and reduces detection blind spots, offering robust support for threat classification and incident response in cybersecurity operations.

Keywords: malware analysis, sandbox, automated detection, digital threats, cybersecurity

Tabla de contenido

Índice de Tablas

Índice de Figuras

1. Introducción

El análisis de malware es una disciplina clave en ciberseguridad que permite examinar software malicioso para comprender su funcionamiento, origen e impacto. Su aplicación es fundamental para detectar, mitigar y prevenir ciberataques que comprometen la integridad de sistemas y datos. El avance de las amenazas digitales ha incrementado la necesidad de herramientas efectivas de análisis, especialmente aquellas accesibles para usuarios y organizaciones con recursos limitados.

En este contexto, los **servicios automáticos en línea** han surgido como soluciones eficientes que permiten analizar archivos sospechosos sin requerir conocimientos avanzados en seguridad informática. Sin embargo, **su precisión y fiabilidad varían significativamente**, lo que hace necesario un estudio comparativo para evaluar sus fortalezas y limitaciones. Esta investigación busca proporcionar una visión crítica sobre la efectividad de estos servicios en la detección y clasificación de amenazas, ayudando a mejorar las estrategias de ciberseguridad.

1.1. Motivación

El crecimiento exponencial del malware y la sofisticación de los ciberataques han convertido el análisis de software malicioso en una tarea esencial. Los servicios automáticos de análisis de malware prometen rapidez y accesibilidad, pero su eficacia aún no está completamente validada.

La motivación de este estudio radica en la **necesidad de comparar distintos servicios automáticos en línea**, evaluando su desempeño para determinar **qué tan confiables y precisos son** en la detección de amenazas. Comprender sus capacidades permitirá mejorar la toma de decisiones en ciberseguridad, optimizar el uso de estas herramientas y contribuir a la investigación sobre métodos avanzados de análisis.

1.2. Planteamiento del problema

A pesar de los avances en análisis de malware, persisten dudas sobre la **fiabilidad y precisión de los servicios automáticos en línea**. Es común que algunos generen **falsos positivos**, mientras que otros pueden pasar por alto amenazas sofisticadas.

Este estudio se centra en responder la pregunta: **¿En qué medida los servicios automáticos online son efectivos en la detección y clasificación de amenazas?** Además, se evaluarán **sus principales ventajas y debilidades** en comparación con

métodos tradicionales, proporcionando criterios para seleccionar herramientas adecuadas en entornos de ciberseguridad.

1.3. Estructura del trabajo

Este documento se compone de los siguientes capítulos:

- **Capítulo 2 – Estado del arte:** Revisión exhaustiva de la evolución del malware, sus tipologías, técnicas de evasión y persistencia, y la progresiva aparición de servicios automáticos online. Se incluye también la literatura académica relevante y consideraciones éticas del uso de estas herramientas.
- **Capítulo 3 – Objetivos y metodología:** Define el enfoque del estudio, los criterios comparativos, las fases experimentales y los indicadores clave que guiarán el análisis.
- **Capítulo 4 – Desarrollo de la contribución:** Detalla el diseño del experimento, la selección de muestras de malware y la descripción funcional de las plataformas evaluadas.
- **Capítulo 5 – Desarrollo experimental y guía práctica:** Expone la configuración del laboratorio, los casos de uso específicos, la selección de malware y la ejecución controlada del análisis sobre entornos virtuales.
- **Capítulo 6 – Ejecución del experimento:** Presenta el análisis multiengine, estático y dinámico de las muestras seleccionadas, cuantifica sus indicadores técnicos y construye una matriz comparativa operativa.
- **Capítulo 7 – Conclusiones y trabajo futuro:** Recoge las principales observaciones extraídas del experimento, propone una clasificación funcional por tipo de amenaza y perfil de usuario, y sugiere futuras líneas de investigación y mejora.
- **Capítulo 8 – Referencias bibliográficas:** Compila todas las fuentes documentales utilizadas, incluyendo estudios académicos, informes técnicos, normativas legales y documentación especializada.

Este trabajo busca no solo evaluar el rendimiento de los servicios más utilizados, sino también proponer criterios prácticos para su uso estratégico frente a amenazas modernas en constante evolución.

2. Estado del arte

El análisis de malware se ha convertido en un componente esencial de la ciberseguridad, permitiendo detectar y comprender software malicioso que amenaza la integridad de sistemas y datos. Con la evolución de las amenazas digitales, el desarrollo de servicios automáticos de análisis ha cobrado relevancia, planteando interrogantes sobre su precisión y efectividad en comparación con métodos tradicionales. En este capítulo, se revisan los conceptos clave, las metodologías empleadas, y los estudios previos que fundamentan la investigación.

2.1. Introducción al estado del arte

El estado del arte constituye el eje investigativo del trabajo, ya que permite identificar los antecedentes más relevantes, comprender las limitaciones de las técnicas existentes y justificar la necesidad de una evaluación empírica de los servicios actuales. Asimismo, se analizan las diferentes tipologías de malware, su impacto en los sistemas digitales y las herramientas empleadas en el análisis, tanto manual como automatizado.

Esta revisión documental se ha estructurado siguiendo un enfoque progresivo: se parte de los conceptos básicos y se avanza hacia las tendencias más recientes en el uso de inteligencia artificial, sandboxes dinámicos e infraestructuras colaborativas para el estudio de muestras maliciosas. Para garantizar la solidez académica del capítulo, se han priorizado fuentes especializadas, estudios revisados por pares y documentación técnica de entidades reconocidas en el ámbito de la ciberseguridad.

Para comenzar, es fundamental definir el objeto central de este estudio: el malware. El malware es un tipo de software malicioso diseñado para infiltrarse en sistemas sin autorización, con distintos propósitos como espionaje, sabotaje o extorsión. Según Tecnored, sus principales variantes incluyen virus, gusanos, troyanos, ransomware, spyware y adware, cada uno con mecanismos de propagación y ataques específicos.

El análisis automatizado de malware es un proceso que emplea herramientas avanzadas para examinar software malicioso de manera rápida y sin intervención manual. Según We Never Sleep, estas soluciones utilizan algoritmos especializados que identifican patrones y comportamientos sospechosos, optimizando la detección de amenazas sin requerir un alto nivel técnico por parte del usuario.

Las herramientas online de análisis de malware son plataformas accesibles a través de internet que permiten a los usuarios cargar archivos sospechosos y obtener informes detallados sobre su peligrosidad. Según KeepCoding, ejemplos representativos de estas herramientas incluyen

VirusTotal, Hybrid Analysis e Intezer Analyze, que integran técnicas de inteligencia artificial y machine learning para mejorar la detección en comparación con enfoques manuales.

Estos servicios automáticos han mejorado significativamente la accesibilidad y velocidad del análisis de malware, aunque su precisión aún es objeto de estudio en la comunidad de ciberseguridad.

2.2. Evolución del malware y sus tipologías

El malware, acrónimo de *malicious software*, es un tipo de programa diseñado para infiltrarse, dañar o alterar el funcionamiento de un sistema informático sin el consentimiento del usuario. Sus finalidades pueden abarcar desde el robo de información y espionaje hasta la extorsión económica o el sabotaje de infraestructuras críticas. De acuerdo con Tecnored, sus principales variantes incluyen virus, gusanos, troyanos, ransomware, spyware y adware, cada una con mecanismos de propagación y objetivos distintos.

A lo largo de las últimas cuatro décadas, el malware ha pasado de ser una demostración de habilidad técnica a convertirse en una herramienta habitual del crimen organizado, la ciberguerra y el espionaje comercial. La creciente dependencia tecnológica de la sociedad ha proporcionado un terreno fértil para su desarrollo, dando lugar a amenazas cada vez más sofisticadas, resistentes y difíciles de detectar.

2.2.1. Hitos históricos en la evolución del malware

La evolución del malware puede comprenderse mejor a través de algunos casos emblemáticos que marcaron un antes y un después en términos de sofisticación técnica, impacto global y respuesta defensiva. La siguiente tabla resume brevemente algunos de los hitos más representativos:

Año	Amenaza	Tipo	Características clave
1986	Brain	Virus de arranque	Considerado el primer virus para PC; se propagaba mediante disquetes.
1999	Melissa	Macro virus	Se replicaba a través de Microsoft Word y correo electrónico.
2003	Blaster	Gusano	Explotaba vulnerabilidades de Windows para propagarse sin interacción.
2008	Conficker	Gusano	Utilizaba múltiples técnicas de evasión; infectó millones de sistemas.

2010	Stuxnet	Gusano/Zero-day	Malware industrial dirigido a instalaciones nucleares iraníes.
2013	CryptoLocker	Ransomware	Introdujo el cifrado fuerte como táctica de extorsión masiva.
2017	WannaCry	Ransomworm	Ataque global que combinó ransomware con propagación automática via SMB.
2018–2021	Emotet	Troyano modular	Red de bots con carga de spam, ransomware y herramientas de exfiltración.

Tabla 1: Cronología evolución malware

Esta evolución ilustra cómo el malware ha pasado de simples códigos replicantes a complejos ecosistemas criminales apoyados por técnicas de evasión, cifrado, modularidad e incluso infraestructura como servicio. Comprender esta evolución requiere, a su vez, una categorización clara de las diversas formas que adopta el *malware*.

2.2.2. Familias y clasificaciones funcionales

El malware no es un fenómeno uniforme. Se clasifica según su comportamiento, vector de entrada, persistencia y objetivo final. A continuación, se describen brevemente las principales categorías:

- Virus: Se insertan en archivos legítimos y requieren intervención del usuario para activarse (normalmente al abrir un documento o ejecutar un programa).
- Gusanos (worms): Se replican sin intervención humana, aprovechando vulnerabilidades de red. Pueden saturar sistemas o propagar otros tipos de malware.
- Troyanos (RATs): Se hacen pasar por programas benignos, pero abren puertas traseras que permiten el control remoto del sistema afectado.
- Ransomware: Cifran archivos del usuario y exigen un rescate. Algunos, como Petya, afectan incluso el sector de arranque.
- Spyware: Recolectan datos personales o confidenciales, como credenciales o hábitos de navegación, sin consentimiento del usuario.
- Adware: Muestran publicidad no deseada, a menudo redirigiendo al usuario hacia sitios potencialmente maliciosos.
- Rootkits: Modifican el sistema operativo para ocultar otros procesos maliciosos. Son difíciles de detectar.
- Fileless malware: Residen en memoria y utilizan herramientas legítimas del sistema (como PowerShell o WMI), evitando dejar rastros en disco.

Además, existen amenazas híbridas que combinan múltiples comportamientos: por ejemplo, algunos troyanos actúan como spyware y también instalan ransomware. La evolución moderna del malware tiende hacia diseños modulares y adaptables según el entorno detectado.

2.2.3. Evasión, persistencia y técnicas avanzadas

Uno de los aspectos más preocupantes de las amenazas actuales es su capacidad para evadir los mecanismos tradicionales de detección. Como señalan Symantec y Kaspersky Lab, muchas variantes modernas utilizan empaquetadores, técnicas de polimorfismo (cambio constante de firma digital), cifrado interno y ofuscación de código para evitar ser identificadas por antivirus basados en firmas.

Además, el uso de técnicas como el living off the land (LOL)—donde el malware emplea herramientas legítimas del sistema operativo para ejecutar acciones maliciosas—incrementa su eficacia y reduce el riesgo de ser detectado. Estos ataques aprovechan utilidades como `cmd.exe`, regsvr32, o `powershell` para realizar tareas como la descarga de payloads o la comunicación con servidores de comando y control (C2).

En este contexto, el marco ATT&CK de MITRE se ha consolidado como una referencia esencial para categorizar tácticas, técnicas y procedimientos (TTP) utilizados por actores maliciosos avanzados. Según este modelo, las técnicas de persistencia, evasión, escalada de privilegios y exfiltración de datos pueden estar asociadas a diversas fases de una intrusión, en las que el malware juega un papel fundamental. En este contexto de sofisticación, han surgido también nuevos modelos operativos que transforman el panorama de las amenazas.

2.2.4. Amenazas emergentes y malware como servicio

En los últimos años, el modelo malware-as-a-service (MaaS) ha ganado protagonismo. Este enfoque permite a actores con escasos conocimientos técnicos contratar herramientas maliciosas empaquetadas a través de foros o mercados clandestinos. Como señala Europol en su último informe IOCTA, este modelo ha democratizado la actividad cibercriminal, permitiendo ataques masivos bien orquestados sin una inversión inicial elevada.

Dentro de este contexto también ha emergido el fenómeno del ransomware-as-a-service (RaaS), donde grupos como REvil, DarkSide o LockBit distribuyen versiones personalizables de su código malicioso a afiliados, a cambio de un porcentaje de los rescates obtenidos. Esta tendencia ha generado cadenas completas de valor dentro del cibercrimen, incluyendo soporte técnico, paneles de control web y sistemas de reparto automatizado.

El malware móvil, por otro lado, ha incrementado su presencia con la expansión del uso de smartphones. Los troyanos bancarios en Android (como Anubis o Cerberus) y las campañas

de phishing vía SMS están cada vez más presentes, afectando a usuarios finales y empresas por igual.

2.2.5. Impacto y respuesta de la industria

Ante la sofisticación creciente de estas amenazas, la industria de la ciberseguridad ha respondido con soluciones cada vez más complejas: desde antivirus basados en aprendizaje automático hasta plataformas de inteligencia de amenazas y soluciones de análisis dinámico automatizado. Este ecosistema también ha visto la proliferación de servicios accesibles desde la web que permiten a investigadores y usuarios subir muestras sospechosas y obtener reportes detallados.

Como afirma KeepCoding, plataformas como VirusTotal, Hybrid Analysis o Intezer Analyze han facilitado el acceso a tecnologías antes restringidas a laboratorios forenses, integrando motores antivirus múltiples, entornos de sandboxing y análisis genético de código. A pesar de sus ventajas, persisten interrogantes sobre la precisión y cobertura real de estas herramientas, especialmente frente a muestras altamente evasivas.

Por ello, diversas iniciativas académicas y profesionales han evaluado su efectividad en condiciones reales. Estudios comparativos han examinado no solo la tasa de detección, sino también aspectos como la rapidez, la profundidad del análisis, la facilidad de uso o la exposición de datos sensibles al utilizar plataformas públicas. Estos aspectos se desarrollan en el siguiente apartado, donde se aborda el análisis de malware como disciplina técnica central en entornos de ciberseguridad moderna.

2.3. El análisis de malware en ciberseguridad moderna

El análisis de malware constituye una disciplina fundamental en el ámbito de la ciberseguridad, tanto en operaciones defensivas como en contextos forenses. Su propósito es identificar, desmantelar y comprender el funcionamiento interno de software malicioso, con el objetivo de mitigar su impacto y generar inteligencia técnica útil para la protección de sistemas. En entornos corporativos, esta actividad se desarrolla principalmente dentro de los Centros de Operaciones de Seguridad (*Security Operations Center* o SOC), donde se monitorean eventos en tiempo real y se responde ante incidentes. En contextos forenses, el análisis de malware adquiere una dimensión retrospectiva, permitiendo reconstruir una intrusión, determinar vectores de ataque y preservar evidencia digital con validez legal.

Ante la creciente sofisticación de las amenazas digitales, se han desarrollado diferentes tipos de análisis que varían en profundidad, precisión y complejidad técnica. Su correcta

combinación permite no solo detectar la presencia de un artefacto malicioso, sino también inferir sus capacidades, identificar su origen, y anticipar futuras variantes.

2.3.1. Análisis estático

El análisis estático consiste en examinar el código del malware sin ejecutarlo. Esta técnica permite obtener información sobre la estructura del archivo, sus cadenas internas, cabeceras, secciones y posibles indicios de comportamiento dañino, todo ello sin poner en riesgo el sistema. Se realiza sobre binarios directamente o sobre scripts, y puede incluir:

- Lectura de metadatos del archivo (cabeceras PE, hash, tamaño).
- Inspección de cadenas de texto en claro (indicadores de red, comandos, nombres de funciones).
- Detección de *packers* u ofuscadores.
- Desensamblado del binario para observar el flujo de ejecución.

Su principal ventaja es la seguridad, ya que no se ejecuta el código. No obstante, su principal limitación radica en que no siempre se puede entender el comportamiento real del malware, especialmente si está cifrado, empaquetado o diseñado para ofuscar su lógica interna.

2.3.2. Análisis dinámico

El análisis dinámico implica ejecutar el archivo sospechoso en un entorno controlado —como una sandbox virtual— para observar su comportamiento en tiempo real. Esto incluye:

- Cambios en el sistema de archivos.
- Creación de procesos y subprocesos.
- Conexiones de red salientes o entrantes.
- Modificaciones del registro.
- Persistencia mediante tareas programadas o claves autorun.

Este enfoque permite detectar acciones encubiertas y revelar instrucciones que solo se ejecutan bajo condiciones específicas. No obstante, algunos malware incluyen rutinas de detección de entornos virtualizados o de depuración, lo que puede provocar que se comporten de forma inofensiva si perciben que están siendo analizados.

2.3.3. Análisis híbrido

El análisis híbrido combina técnicas estáticas y dinámicas para obtener una visión más completa del archivo. Algunas plataformas automatizadas primero hacen un análisis

superficial estático para categorizar el archivo y luego ejecutan un análisis dinámico para verificar su comportamiento.

Este enfoque permite correlacionar hallazgos: por ejemplo, una cadena sospechosa localizada en análisis estático puede confirmarse si se observa una conexión activa al mismo dominio durante la ejecución dinámica.

Herramientas como Hybrid Analysis o Intezer implementan este tipo de enfoque dual, y son ampliamente utilizadas tanto en entornos profesionales como educativos.

2.3.4. Análisis de memoria

El análisis de memoria (o análisis forense de volcado de RAM) permite detectar malware que opera en memoria y no deja rastros persistentes en el disco. Este tipo de amenazas —denominadas *fileless*— son cada vez más comunes, ya que evitan mecanismos tradicionales de detección.

A través de la extracción y análisis de la memoria RAM de un sistema activo, pueden identificarse:

- Procesos ocultos o inyectados en otros legítimos.
- Registros de actividad de malware residente en RAM.
- Cadenas y argumentos de procesos.
- Módulos DLL maliciosos cargados en sesiones activas.

El análisis de memoria es especialmente útil en investigaciones post-intrusión (post-mortem) y requiere herramientas especializadas y conocimientos avanzados. Es una técnica exigente, pero indispensable en incidentes donde el atacante ha cubierto bien sus huellas.

2.3.5. Herramientas comunes de análisis de malware

En el presente trabajo se han seleccionado cinco plataformas automáticas de análisis de malware, representativas del estado actual de la tecnología en cuanto a accesibilidad, profundidad analítica y variedad metodológica. Estas herramientas combinan distintas estrategias —estáticas, dinámicas e híbridas— y permiten evaluar muestras sospechosas de forma segura, rápida y sin necesidad de configurar entornos locales complejos.

A continuación, se describen sus principales características:

Plataforma	Tipo de análisis	Características principales
VirusTotal	Estático	Usa más de 70 motores antivirus; compara hashes, detecta URLs maliciosas y enlaza con otros reportes; no incluye análisis dinámico nativo.
Any.Run	Dinámico interactivo	Ejecuta el malware en sandbox interactiva; permite observar conexiones, procesos y comportamiento en tiempo real con paneles visuales detallados.
Hybrid Analysis	Híbrido	Combina análisis estático y dinámico; emplea Falcon Sandbox; entrega un score de amenaza, IOC y eventos en línea temporal.
MetaDefender	Estático	Ofrece escaneo multiengine y desinfección de archivos mediante CDR (Content Disarm and Reconstruction); útil para entornos corporativos.
Intezer Analyze	Genético (estático avanzado)	Compara segmentos de código binario con muestras conocidas; identifica familias, autores y relaciones entre muestras mediante análisis genético.

Tabla 2: Plataforma por tipo de análisis

Cada una de estas herramientas aporta ventajas específicas según el enfoque analítico, el tipo de muestra evaluada y el objetivo del análisis. Su uso combinado permite contrastar resultados, mejorar la cobertura frente a técnicas evasivas y ofrecer una caracterización más robusta de las amenazas detectadas.

2.3.6. Aplicación en operaciones SOC y análisis forense

En un entorno SOC, el análisis de malware permite tomar decisiones informadas ante alertas generadas por otros sistemas como EDR, IDS o antivirus. Al caracterizar una amenaza detectada en la red o en un host, el analista puede determinar su alcance, nivel de criticidad, y planificar una respuesta efectiva. El resultado puede incluir la cuarentena de activos, generación de reglas YARA o retroalimentación a otros sistemas de detección.

En el análisis forense, el malware encontrado puede ser la clave para reconstruir una cadena de ataque. Identificar cómo y cuándo se introdujo en el sistema, a qué sistemas se conectó o qué datos comprometió, son aspectos esenciales en procesos de auditoría y atribución. En contextos judiciales, el análisis técnico riguroso puede convertirse en evidencia digital admisible, por lo que se aplican procedimientos estandarizados y cadenas de custodia.

En conjunto, estas técnicas representan el núcleo técnico del trabajo de muchos profesionales de ciberseguridad. La adecuada selección y combinación de métodos de análisis —respaldada por herramientas especializadas— permite enfrentarse de forma eficaz a amenazas cada vez más evasivas, y constituye un pilar estratégico tanto en la defensa proactiva como en la respuesta reactiva ante incidentes.

2.4. Retos y limitaciones del análisis manual

El análisis manual de malware ha sido tradicionalmente una disciplina clave dentro de la ciberseguridad técnica. Su valor reside en la capacidad de comprender en profundidad el comportamiento de software malicioso, generar indicadores de compromiso (IOCs), y establecer tácticas defensivas con base empírica. Sin embargo, en el contexto actual de amenazas sofisticadas, automatización del cibercrimen y necesidad de respuestas rápidas, este enfoque presenta limitaciones operativas que han favorecido la adopción creciente de soluciones automáticas.

2.4.1. Alto consumo de tiempo y exigencia de personal cualificado

El análisis manual, ya sea estático o dinámico, puede requerir desde varias horas hasta días completos para procesar una única muestra, especialmente si se trata de malware empaquetado o modular. Esta inversión de tiempo es incompatible con las necesidades de detección y respuesta inmediata que exigen los entornos modernos de seguridad, donde los analistas deben tomar decisiones en tiempo real.

Además, el dominio de herramientas como depuradores, desensambladores o analizadores de memoria requiere personal altamente cualificado en ingeniería inversa, arquitectura de sistemas operativos y ensamblador. Estos perfiles no siempre están disponibles en todas las organizaciones y pueden generar dependencia externa o sobrecarga operativa.

2.4.2. Riesgo inherente a la ejecución manual

El análisis dinámico implica ejecutar el malware en un entorno controlado, como una máquina virtual, para observar su comportamiento. Sin embargo, si este entorno no está correctamente aislado o configurado —por ejemplo, si mantiene conectividad de red real—, el analista puede provocar una infección accidental o permitir que el malware contacte con su infraestructura de comando y control.

Además, numerosos tipos de malware modernos están diseñados para detectar si se ejecutan en máquinas virtuales, depuradores o entornos sandbox. Si lo detectan, pueden alterar su comportamiento, permanecer inactivos o incluso autodestruirse para evitar la observación.

2.4.3. Limitaciones frente a técnicas avanzadas

Las técnicas de evasión empleadas por amenazas actuales han sido diseñadas, en muchos casos, específicamente para frustrar el análisis manual:

- **Ofuscación y empaquetado múltiple**: dificultan el acceso al código ejecutable real. Algunas muestras incluyen cifrado dinámico o múltiples capas de compresión que solo se descomprimen en memoria.
- **Carga modular o por etapas** (*staged payloads*): la funcionalidad maliciosa real se descarga desde Internet o se genera dinámicamente, lo que impide su análisis completo si no se ejecuta correctamente.
- **Técnicas *living off the land (LOL)*:** el malware se apoya en herramientas legítimas como `PowerShell` o `regsvr32.exe` para realizar acciones maliciosas sin levantar alertas.
- **Malware sin archivos (*fileless*)**: residen exclusivamente en memoria, lo que requiere volcados forenses de RAM y herramientas especializadas para su identificación.

Estas técnicas aumentan considerablemente la carga cognitiva del analista y pueden dificultar o impedir la obtención de resultados concluyentes si no se dispone de experiencia, tiempo o recursos adecuados. Es precisamente en respuesta a estos desafíos que las plataformas automáticas de análisis de *malware* han ganado una relevancia significativa.

2.4.4. Aparición y relevancia de soluciones automáticas

Frente a estos retos, las plataformas automáticas de análisis de malware ofrecen soluciones más rápidas, seguras y accesibles. Herramientas como **Any.Run, VirusTotal, Hybrid Analysis, MetaDefender** e **Intezer Analyze** permiten analizar muestras sin necesidad de ejecutarlas localmente, reduciendo los riesgos y agilizando la toma de decisiones.

Estas soluciones generan informes completos basados en comportamientos, firmas antivirus, heurísticas y comparaciones genéticas de código. Aunque no sustituyen el análisis manual cuando se busca atribución o comprensión técnica profunda, sí cumplen un papel fundamental como primer filtro, especialmente en entornos corporativos, académicos o de respuesta rápida.

Como señala Europol, la velocidad de detección y la automatización del análisis técnico son hoy elementos clave para mitigar el impacto de ataques modernos. De ahí la importancia de

evaluar el rendimiento, precisión y utilidad real de estas plataformas, como se propone en este trabajo.

2.5. Surgimiento de servicios online automáticos

El crecimiento exponencial en volumen y complejidad del malware ha generado una presión evidente sobre las capacidades tradicionales de análisis. En respuesta, ha emergido una nueva generación de plataformas accesibles vía web que permiten el examen automático de muestras sospechosas sin requerir instalación local ni conocimientos técnicos avanzados. Este tipo de herramientas responde a una necesidad real y creciente por accesibilidad, velocidad y escalabilidad en la detección y caracterización de amenazas.

2.5.1. Motivación: accesibilidad, velocidad y escala

A medida que la cantidad de nuevos archivos maliciosos detectados cada día supera las 450.000 muestras, el análisis manual —por su nivel de detalle y exigencia de tiempo— resulta insuficiente para sostener una defensa eficaz. Las organizaciones, servicios de respuesta a incidentes y usuarios independientes requieren mecanismos que les permitan inspeccionar archivos de forma automatizada, rápida y relativamente precisa, sin depender de entornos de laboratorio complejos ni recursos expertos.

Estas plataformas online ofrecen la posibilidad de:

- Cargar archivos o URLs sospechosas desde cualquier equipo conectado.
- Obtener informes en segundos o minutos, sin ejecutar el archivo en el propio dispositivo.
- Visualizar comportamientos, reputaciones, similitudes y conexiones entre muestras.
- Colaborar indirectamente con otros analistas mediante la publicación (opcional) de resultados compartidos.

Este nivel de accesibilidad ha democratizado el análisis de malware, permitiendo que equipos sin infraestructura avanzada se beneficien de potentes mecanismos de detección.

2.5.2. Breve historia de cinco plataformas representativas

A lo largo de las últimas dos décadas, diversos servicios han evolucionado desde escáneres simples hasta verdaderas plataformas de análisis técnico multi-nivel. En este trabajo se han seleccionado cinco plataformas representativas que ilustran esa evolución:

- **VirusTotal** fue creada en 2004 por la empresa española Hispasec como un servicio gratuito para escanear archivos y URLs utilizando múltiples motores antivirus. En

2012 fue adquirida por Google, y desde entonces ha integrado funcionalidades colaborativas y una API para uso empresarial. Actualmente, forma parte del ecosistema de Chronicle, dentro de Google Cloud.

- **Hybrid Analysis** nació en 2013 como una herramienta avanzada basada en sandboxing, desarrollada por CrowdStrike y más tarde transferida a Payload Security. Su principal innovación fue ofrecer informes detallados sobre comportamiento y actividad de red mediante el uso de Falcon Sandbox, una tecnología de análisis dinámico.
- **Any.Run** apareció en 2018 con un enfoque disruptivo: permitir a los usuarios interactuar en tiempo real con una muestra maliciosa ejecutándose en un entorno virtual. A diferencia de otros sandboxes pasivos, permite intervenir manualmente en la ejecución, navegar por menús del malware, introducir entradas y observar respuestas contextualizadas.
- **MetaDefender Cloud** es la apuesta online de OPSWAT, empresa centrada en ciberseguridad industrial y protección de infraestructuras críticas. A partir de su motor Deep CDR (Content Disarm and Reconstruction), permite eliminar contenido malicioso de documentos mientras ofrece escaneo con múltiples motores comerciales.
- **Intezer Analyze**, por su parte, representa un enfoque novedoso: en lugar de basarse solo en ejecución o firmas estáticas, identifica fragmentos genéticos de código dentro de los binarios enviados. Esta técnica permite detectar reutilización de fragmentos maliciosos conocidos, incluso cuando el malware ha sido ofuscado o recompilado.

2.5.3. Tipos de análisis disponibles

Cada una de estas plataformas implementa su propio enfoque técnico. Aunque todas están orientadas al análisis automático, difieren en los métodos de inspección, presentación de resultados y capacidad de integración. A continuación, se explican las técnicas más comunes:

- **Multiengine antivirus**: Utilizado por servicios como VirusTotal y MetaDefender, permite escanear un archivo con decenas de motores de detección comerciales simultáneamente. Si bien no garantiza exactitud total, ofrece una primera lectura estadística sobre la sospechosidad del archivo según diferentes proveedores.
- **Sandbox dinámico**: Consiste en ejecutar la muestra en un entorno virtual aislado para observar su comportamiento. Hybrid Analysis y Any.Run son referentes en este enfoque, ofreciendo visualización de procesos, conexiones de red, uso de APIs e intentos de persistencia.

- **Reconstrucción y desinfección de documentos (CDR)**: Presente en MetaDefender, permite generar versiones limpias de archivos potencialmente maliciosos (PDFs, DOCX, etc.) eliminando macros, contenido activo o datos embebidos sin dañar el contenido visual.
- **Análisis genético de código**: Usado por Intezer Analyze, este enfoque identifica fragmentos de código previamente registrados en su base de datos, clasificándolos como benignos, maliciosos o desconocidos. Aporta valor incluso cuando las muestras han sido modificadas superficialmente.
- **Reputación y score de amenaza**: Varias plataformas calculan un valor numérico o categórico que refleja la peligrosidad estimada del archivo analizado, basado en comportamientos, coincidencias de código o resultados agregados.

2.5.4. Comparativa general de plataformas

A continuación, se presenta una tabla-resumen que compara las cinco plataformas evaluadas, en función de sus características técnicas clave:

Plataforma	Tipo principal	Análisis dinámico	Motores AV	Análisis genético	Score reputacional	Observaciones destacadas
VirusTotal	Multiengine estático	❌	✓ +70	❌	✓ (por proveedor)	Muy extendido; permite escaneo de URLs y búsqueda de IOC
Any.Run	Dinámico interactivo	✓	❌	❌	✓ (score visual)	Sandbox con control manual del entorno en ejecución
Hybrid Analysis	Híbrido	✓	Limitado	❌	✓ (Threat Score)	Línea temporal detallada de eventos
MetaDefender	Estático + CDR	❌	✓ +30	❌	✓	Capacidad de desinfección y reconstrucción segura
Intezer Analyze	Estático genético	❌	❌	✓	✓ (detallado)	Identifica código compartido entre familias

Tabla 3: Comparativa general de plataformas

⚠️ Algunas funciones avanzadas (como carga de muestras mayores o integración con APIs) requieren cuentas gratuitas con registro o suscripciones de pago.

2.5.5. Consideraciones finales

El surgimiento de estas plataformas ha modificado profundamente la forma en que se realiza el análisis de malware. Su facilidad de uso, su poder analítico y la disponibilidad de informes detallados han facilitado la integración de estas herramientas en flujos de trabajo corporativos, análisis forense, investigación académica e incluso tareas educativas. No obstante, su uso también plantea desafíos asociados a la privacidad —especialmente en plataformas públicas como VirusTotal— y a la dependencia de herramientas externas.

Por ello, en este trabajo se propone evaluar su efectividad comparada, explorando sus fortalezas, limitaciones y complementariedades. Comprender su funcionamiento y su aportación real en escenarios prácticos permitirá, en los siguientes capítulos, valorar si estas soluciones pueden consolidarse como pilares sólidos en estrategias de detección de malware modernas.

2.6. Evaluaciones previas y literatura académica

El análisis automático de malware ha sido objeto de creciente atención en la literatura académica y técnica, especialmente a medida que las amenazas digitales se han vuelto más sofisticadas y evasivas. Diversos estudios han evaluado la efectividad de plataformas online, han propuesto modelos de clasificación basados en aprendizaje automático y han validado empíricamente el rendimiento de herramientas mediante conjuntos de muestras reales. Este apartado recoge una selección representativa de investigaciones recientes que aportan evidencia sobre el estado actual de estas soluciones y sus implicaciones prácticas.

2.6.1. Comparativas de efectividad entre servicios

Uno de los enfoques más comunes en la literatura consiste en comparar la capacidad de detección de diferentes plataformas automáticas frente a conjuntos de muestras maliciosas. En un estudio realizado por la Universidad de Ciencias Aplicadas de Ámsterdam, se evaluaron los resultados de **VirusTotal, Hybrid Analysis y Joe Sandbox** frente a 1.000 muestras de malware obtenidas de repositorios públicos. Los autores concluyeron que, aunque VirusTotal ofrecía una cobertura más amplia gracias a su motor multiengine, los entornos de sandboxing como Hybrid Analysis proporcionaban información más rica sobre comportamiento y persistencia.

Otro trabajo relevante fue desarrollado por el Instituto Nacional de Ciberseguridad de Francia (ANSSI), donde se compararon cinco plataformas —incluyendo Any.Run e Intezer Analyze— en función de su capacidad para detectar malware polimórfico. El estudio reveló que los motores basados en análisis genético, como el de Intezer, eran especialmente eficaces para

identificar variantes de familias conocidas, incluso cuando el código había sido recompilado o ofuscado.

En ambos casos, los investigadores destacaron la importancia de combinar múltiples enfoques (estático, dinámico, heurístico) para obtener una visión más completa del comportamiento malicioso. Asimismo, se subrayó la necesidad de interpretar los resultados con criterio técnico, ya que las plataformas pueden ofrecer falsos positivos o negativos dependiendo del tipo de muestra y del contexto de ejecución.

2.6.2. Aplicación de machine learning en análisis de malware

El uso de técnicas de aprendizaje automático ha revolucionado el campo del análisis de malware, permitiendo detectar amenazas incluso cuando no existen firmas conocidas. Según Campus Ciberseguridad, el machine learning permite identificar patrones anómalos en archivos, flujos de red o registros del sistema, mejorando la detección proactiva y reduciendo la dependencia de reglas estáticas.

Entre los enfoques más utilizados se encuentran:

- **Modelos supervisados**, entrenados con conjuntos etiquetados de muestras benignas y maliciosas.
- **Modelos no supervisados**, que detectan desviaciones respecto a un comportamiento considerado normal.
- **Redes neuronales profundas**, capaces de identificar relaciones complejas entre características del código.

Un ejemplo concreto es el trabajo de Julia Mirabet en la Universitat Politècnica de València, donde se desarrolló un sistema de detección de malware en Android utilizando algoritmos de clasificación como Random Forest y Support Vector Machines. El modelo alcanzó una precisión superior al 95 % en la detección de aplicaciones maliciosas, demostrando la viabilidad de estas técnicas en entornos móviles.

Asimismo, en el blog de Ciber-Seguridad se documentan casos de éxito en la integración de machine learning en soluciones SIEM y EDR, donde los modelos permiten identificar amenazas en tiempo real, reducir falsos positivos y anticipar comportamientos maliciosos antes de que se materialicen.

No obstante, la literatura también advierte sobre los desafíos asociados a esta aproximación: la necesidad de conjuntos de datos representativos, la complejidad de interpretar modelos opacos (black-box) y el riesgo de sobreajuste si no se valida adecuadamente el entrenamiento.

2.6.3. Validaciones empíricas con muestras reales

Más allá de los estudios teóricos, diversas investigaciones han validado empíricamente el rendimiento de plataformas automáticas utilizando muestras reales de malware. En un trabajo de fin de grado de la Universitat Politècnica de Catalunya, se configuró un laboratorio con máquinas virtuales y se analizaron muestras descargadas de repositorios como MalwareBazaar y VX Underground. Se utilizaron herramientas como PEStudio, Process Monitor y Wireshark para comparar los resultados obtenidos manualmente con los generados por plataformas como Any.Run y VirusTotal.

Los resultados mostraron una alta correlación entre los indicadores de comportamiento observados en el entorno local y los reportes automáticos, especialmente en lo relativo a conexiones de red, procesos hijos y modificaciones del sistema de archivos. Sin embargo, también se identificaron limitaciones: algunas muestras no se ejecutaban correctamente en entornos virtuales públicos, y otras eran detectadas por los motores antivirus antes de mostrar su comportamiento real, lo que impedía su análisis completo.

Otro estudio, publicado por la Universidad Politécnica Salesiana de Ecuador, propuso una metodología para analizar malware en un entorno controlado y comparó los resultados obtenidos con los de plataformas online. El trabajo concluyó que, si bien las herramientas automáticas son útiles para una primera clasificación, el análisis manual sigue siendo necesario para comprender en profundidad las técnicas de evasión y persistencia utilizadas por amenazas avanzadas.

2.6.4. Consideraciones metodológicas y éticas

La literatura también ha abordado aspectos metodológicos relevantes, como la necesidad de anonimizar muestras antes de subirlas a plataformas públicas, para evitar la exposición de información sensible. Asimismo, se ha debatido sobre la validez de los resultados obtenidos en entornos virtuales, ya que algunos malware detectan la presencia de sandbox y modifican su comportamiento para evitar ser analizados.

En términos éticos, se ha planteado la responsabilidad de los investigadores al compartir muestras o resultados en plataformas abiertas, así como la necesidad de establecer protocolos de uso responsable que eviten la reutilización maliciosa de información técnica.

2.7. Aplicación de estos servicios en respuesta a incidentes reales

Las plataformas automáticas de análisis de malware no solo han transformado la forma en que se detectan y clasifican amenazas, sino que también han demostrado ser herramientas clave en la respuesta a incidentes reales. Su integración en procesos de análisis forense digital y respuesta a incidentes (DFIR, por sus siglas en inglés) ha permitido a equipos de seguridad contener ataques, identificar vectores de entrada y generar inteligencia accionable en tiempos reducidos. Este apartado recoge ejemplos concretos de su aplicación en escenarios reales y su papel dentro de flujos de trabajo profesionales.

2.7.1. Casos reales de mitigación mediante plataformas automáticas

Uno de los casos más conocidos fue el brote global de ransomware **WannaCry** en 2017. Durante las primeras horas del ataque, investigadores de múltiples países utilizaron **VirusTotal** para subir muestras del ejecutable y confirmar su naturaleza maliciosa mediante coincidencias con motores antivirus. La plataforma permitió correlacionar hashes, identificar variantes y compartir indicadores de compromiso (IOCs) con la comunidad global, lo que facilitó la generación de reglas de detección en tiempo récord.

En otro incidente, el equipo de respuesta de una empresa de telecomunicaciones detectó actividad anómala en una estación de trabajo. Al extraer el ejecutable sospechoso y subirlo a **Any.Run**, pudieron observar en tiempo real que el malware intentaba conectarse a un dominio previamente asociado con el troyano Emotet. Esta visualización permitió bloquear el tráfico saliente desde el firewall perimetral antes de que se completara la descarga de la carga útil secundaria.

Asimismo, en un caso documentado por Intezer, una muestra de malware que no era detectada por ningún motor antivirus fue analizada mediante su plataforma genética. El sistema identificó fragmentos de código coincidentes con una variante de **Dridex**, lo que permitió activar medidas de contención antes de que se produjera la exfiltración de datos.

Estos ejemplos ilustran cómo las plataformas automáticas no solo aceleran la detección, sino que también permiten tomar decisiones tácticas en fases críticas de un incidente.

2.7.2. Integración en procesos de DFIR

En el marco de una investigación forense digital, estas plataformas se utilizan habitualmente en las primeras fases del proceso, especialmente en la **identificación y clasificación de artefactos sospechosos**. Cuando se extraen ejecutables, scripts o documentos ofuscados de

un sistema comprometido, su análisis inmediato en herramientas como **Hybrid Analysis** o **MetaDefender** permite determinar si se trata de malware conocido, qué comportamiento presenta y si ha sido observado previamente en otros entornos.

Según Telefónica Tech, los equipos DFIR suelen integrar estas plataformas en su flujo de trabajo para generar IOCs, validar hipótesis de ataque y enriquecer la inteligencia contextual del incidente. Por ejemplo, tras analizar una muestra en Any.Run, el analista puede extraer dominios, direcciones IP y nombres de procesos que luego se utilizan para buscar trazas en otros sistemas afectados.

Además, estas herramientas permiten documentar el comportamiento del malware con capturas, líneas temporales y árboles de procesos, lo que facilita la elaboración de informes técnicos y la comunicación con otros equipos (como threat hunting o inteligencia de amenazas). En muchos casos, los resultados obtenidos se integran directamente en plataformas SIEM o EDR mediante APIs, automatizando la respuesta y reduciendo el tiempo medio de contención (MTTC).

En entornos judiciales o regulatorios, los informes generados por estas plataformas pueden complementar la cadena de custodia digital, siempre que se documenten adecuadamente las condiciones de análisis y se preserve la integridad de las muestras.

2.8. Consideraciones éticas y de privacidad

El uso de plataformas automáticas de análisis de malware plantea no solo cuestiones técnicas, sino también implicaciones éticas y legales que deben ser cuidadosamente consideradas. En particular, el tratamiento de muestras reales —especialmente aquellas extraídas de entornos corporativos o institucionales— puede conllevar riesgos significativos en términos de confidencialidad, cumplimiento normativo y exposición de información sensible.

2.8.1. Riesgos de confidencialidad en plataformas públicas

Subir muestras reales a plataformas públicas como VirusTotal o Hybrid Analysis puede implicar la exposición involuntaria de datos confidenciales. Aunque estas plataformas ofrecen la opción de mantener los análisis en modo privado, por defecto muchas muestras quedan disponibles para otros usuarios o motores de análisis, lo que puede derivar en la divulgación de rutas internas, nombres de archivos, direcciones IP o incluso fragmentos de código propietario. Este riesgo es especialmente relevante en sectores regulados, como el financiero, sanitario o gubernamental, donde la filtración de información puede tener consecuencias legales o reputacionales graves.

2.8.2. Limitaciones de las versiones gratuitas

Las versiones gratuitas de estas plataformas, si bien accesibles y funcionales, presentan limitaciones importantes frente a sus versiones empresariales. Entre las restricciones más comunes se encuentran:

- Imposibilidad de mantener los análisis en modo privado.
- Límites en el tamaño de los archivos subidos.
- Acceso restringido a funciones avanzadas como APIs, reglas YARA personalizadas o análisis en profundidad.
- Ausencia de soporte técnico o garantías de confidencialidad contractual.

Estas limitaciones pueden comprometer la utilidad de la herramienta en entornos profesionales, donde se requiere trazabilidad, control de acceso y cumplimiento normativo. Por ello, muchas organizaciones optan por versiones empresariales o despliegan soluciones locales que replican las funcionalidades de estas plataformas sin exponer datos a terceros.

Adicionalmente, algunas plataformas, como Intezer Analyze, imponen restricciones de acceso que limitan el uso completo a cuentas corporativas o institucionales, lo que puede dificultar su aplicación práctica en investigaciones académicas o individuales.

2.8.3. Cumplimiento normativo y el impacto del GDPR

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea establece obligaciones estrictas respecto al tratamiento de datos personales, incluyendo aquellos que puedan estar contenidos en muestras de malware (por ejemplo, documentos infectados con datos reales, correos electrónicos o credenciales). Subir este tipo de archivos a plataformas públicas sin medidas adecuadas de anonimización o consentimiento explícito puede constituir una infracción del reglamento.

Además, el GDPR exige realizar una **Evaluación de Impacto en la Protección de Datos (EIPD)** cuando el tratamiento pueda suponer un alto riesgo para los derechos y libertades de las personas. En este contexto, el uso de plataformas de análisis debe ser evaluado como parte de la gestión de riesgos de la organización, considerando aspectos como la ubicación de los servidores, la política de retención de datos y la posibilidad de transferencias internacionales.

Por tanto, el uso ético y legal de estas herramientas requiere no solo competencia técnica, sino también una comprensión clara del marco normativo aplicable. La adopción de buenas prácticas —como el uso de entornos privados, la anonimización de muestras y la

documentación de los procesos— es esencial para garantizar un análisis responsable y conforme a la legislación vigente.

2.9. Conclusión del estado del arte

El análisis de malware ha evolucionado significativamente en las últimas décadas, adaptándose al crecimiento en volumen, variedad y sofisticación de las amenazas digitales. En este capítulo se ha revisado la evolución histórica del software malicioso, desde las primeras infecciones masivas hasta amenazas polimórficas, modulares y sin archivos. Se ha evidenciado cómo las técnicas de evasión, persistencia y antianálisis han planteado nuevos desafíos al enfoque manual tradicional, exigiendo altos niveles de experiencia, tiempo y recursos técnicos.

En respuesta a estas limitaciones, han surgido plataformas online automáticas que permiten examinar muestras sospechosas de forma rápida, segura y accesible. Herramientas como **VirusTotal, Any.Run, Hybrid Analysis, MetaDefender** e **Intezer Analyze** incorporan enfoques diversos —multiengine, análisis dinámico, búsqueda genética o desinfección de archivos— que han democratizado el acceso a capacidades avanzadas de análisis. Su uso se ha extendido a entornos corporativos, académicos y operativos, tanto como apoyo al análisis manual como en procesos de respuesta a incidentes (DFIR).

No obstante, y pese a su popularidad, **existe una carencia de estudios que comparen su efectividad relativa** con criterios empíricos y orientados a casos prácticos. La literatura revisada apunta a su utilidad operativa, pero también resalta sus limitaciones en cuanto a precisión, cobertura o interpretación contextual de los resultados. En muchos casos, las decisiones técnicas se toman sobre la base de intuición o conveniencia, más que en una evaluación sistemática de rendimiento.

Por ello, en los capítulos siguientes se propone una evaluación comparativa controlada de estas cinco plataformas, centrada en su capacidad para detectar, clasificar y describir muestras de malware representativas de diferentes familias. El objetivo es establecer —desde una perspectiva técnica y neutral— cuáles son sus fortalezas, debilidades y complementariedades, y aportar criterios objetivos que puedan servir a otros analistas o responsables técnicos en la toma de decisiones fundamentadas.

3. Objetivos concretos y metodología de trabajo

Este capítulo define el enfoque de la investigación y los criterios empleados para evaluar los **servicios automáticos de análisis de malware**, proporcionando una metodología estructurada que garantice la **objetividad y precisión** de la comparación.

3.1. Objetivo general

El propósito de este estudio es evaluar la efectividad de distintos **servicios automáticos de análisis de malware** en la **detección y clasificación de amenazas digitales**. Se busca identificar fortalezas y debilidades de estos servicios en la lucha contra ransomware, troyanos, spyware, adware y rootkits, worms y fileless malware estableciendo criterios comparativos de **precisión, rapidez, profundidad del análisis y usabilidad**. La metodología experimental garantizará resultados fiables, ofreciendo recomendaciones para mejorar la toma de decisiones en seguridad informática.

3.2. Objetivos específicos

Para cumplir el objetivo general, se han establecido los siguientes objetivos específicos:

- **Analizar** las capacidades de detección de malware de distintos servicios automáticos.
- **Comparar** la precisión y rapidez de los análisis estáticos, dinámicos e híbridos, evaluando los resultados con malware conocido.
- **Clasificar** los informes generados por cada servicio según la categoría de malware detectado (ransomware, troyanos, spyware, adware, rootkits, worms y fileless malware), midiendo la coherencia de sus resultados.
- **Evaluar** la facilidad de uso de las plataformas seleccionadas y la claridad de los informes emitidos, determinando su aplicabilidad para distintos perfiles de usuario.
- **Establecer** recomendaciones sobre la confiabilidad y utilidad práctica de estos servicios, indicando en qué escenarios son más efectivos.

3.3. Metodología del trabajo

La investigación sigue una metodología experimental, basada en pruebas sistemáticas y homogéneas para cada muestra. La siguiente tabla resume las fases de trabajo definidas:

Fase	Descripción de la actividad
Selección de muestras	Muestras obtenidas de bases como MalwareBazaar y VX Underground; se priorizan ejemplares recientes y representativos.
Clasificación funcional	Organización por categorías: ransomware, troyanos, spyware, adware, rootkits, gusanos (*worms*) y *fileless* malware.
Carga en plataformas	Subida de cada archivo a VirusTotal, Hybrid Analysis, MetaDefender, Any.Run e Intezer; registro del tipo de análisis (estático, dinámico, híbrido).
Medición temporal	Registro del tiempo de procesamiento desde la carga hasta la generación del informe; cálculo de promedio por categoría.
Análisis comparativo	Evaluación de precisión, profundidad y detección de técnicas evasivas mediante comparación estructurada de resultados.

Tabla 4: Metodología del trabajo

Esta secuencia metodológica asegura condiciones equitativas entre plataformas y permite una comparación objetiva, reproducible y técnica entre sus resultados.

3.4. Criterios de evaluación

Para garantizar una comparación objetiva, cada servicio será calificado en función de los siguientes **criterios clave**:

- **Precisión**: Capacidad del servicio para identificar y clasificar correctamente el malware.
- **Velocidad**: Tiempo de respuesta desde la carga de la muestra hasta la emisión del informe.
- **Profundidad del análisis**: Detalle proporcionado sobre el comportamiento del malware y sus técnicas de evasión.
- **Usabilidad**: Facilidad de acceso y comprensión del informe generado para el usuario.

Estos cuatro ejes han sido aplicados de forma uniforme a todas las plataformas evaluadas, permitiendo una comparación objetiva y estructurada en los capítulos siguientes.

4. Desarrollo específico de la contribución

Este capítulo presenta la evaluación comparativa de **cinco servicios automáticos de análisis de malware**, midiendo su **precisión, rapidez, profundidad del análisis y usabilidad**. Se sigue un **diseño experimental**, asegurando condiciones homogéneas para garantizar resultados objetivos y comparables.

4.1. Piloto experimental

4.1.1. Descripción detallada del experimento

El estudio se basa en pruebas controladas con muestras representativas de malware obtenidas de bases de datos especializadas. La evaluación sigue estos pasos:

- **Selección de muestras**: Clasificación de malware en siete categorías:
  - **Ransomware:** Evaluación de cifrados maliciosos y patrones de extorsión.
  - **Troyanos:** Detección de archivos maliciosos disfrazados de software legítimo.
  - **Spyware:** Análisis de programas diseñados para el robo de información.
  - **Adware:** Identificación de aplicaciones intrusivas con publicidad no deseada.
  - **Rootkits**: Medición de efectividad en la identificación de amenazas que ocultan su presencia en el sistema.
  - **Worms**: Estudio de técnicas de propagación automática en redes.
  - **Fileless Malware**: Evaluación de amenazas que operan en memoria sin dejar rastros en el disco
- **Procedimiento de prueba**:
  1. **Carga de la muestra**: Carga del archivo a la plataforma.
  2. **Tipo de análisis**: Registro de si el servicio emplea análisis **estático, dinámico o híbrido**.
  3. **Tiempo de procesamiento**: Medición de rapidez desde la carga hasta la generación del informe.
  4. **Evaluación de resultados**: Examen de **precisión, profundidad del análisis y usabilidad** del informe.

4.1.2. Descripción de los resultados

Los datos obtenidos de cada servicio se presentan en **tablas y gráficos**, facilitando la comparación visual:

- **VirusTotal** → Rápido, múltiple detección antivirus, pero limitado frente a malware polimórfico.
- **Hybrid Analysis** → Análisis estático y dinámico, profundidad avanzada, pero interpretación compleja.
- **MetaDefender Cloud** → Alta precisión, enfoque en vulnerabilidades, pero profundidad variable.
- **Any.Run** → Entorno interactivo, ideal para ejecución real de malware, pero requiere experiencia técnica.
- **Intezer Analyze** → Basado en análisis genético de código, preciso en similitudes, pero menos eficaz ante amenazas nuevas (no se pudo conseguir licencia por falta de cuenta de correo electrónico profesional).

4.2. Análisis Comparativo

Esta sección evalúa el desempeño de cinco servicios automáticos de análisis de malware, considerando criterios clave como precisión, velocidad, profundidad del análisis y usabilidad. Además, se detalla el acceso y el proceso de uso de cada plataforma para facilitar su comprensión.

4.2.1. VirusTotal

- **Acceso:** Disponible sin necesidad de registro a través de VirusTotal (VirusTotal - Home), permite el análisis de archivos y URLs.
- **Proceso:**
    1. Subir el archivo sospechoso o introducir una URL.
    2. VirusTotal ejecuta un análisis estático con múltiples motores antivirus.
    3. Se muestra un informe con los resultados de detección de cada motor.
- **Ventajas:** Rápido, fácil de usar, con acceso a múltiples motores de detección.
- **Limitaciones:** Basado en firmas antivirus, menos efectivo contra malware polimórfico.

4.2.2. Hybrid Analysis

- **Acceso:** Requiere registro en Hybrid Analysis para acceder a funciones avanzadas (Free Automated Malware Analysis Service - powered by Falcon Sandbox).
- **Proceso:**
    1. Cargar el archivo o URL sospechoso en la plataforma.
    2. La herramienta ejecuta un análisis estático y dinámico en entornos virtualizados.
    3. Se genera un informe detallado con interacciones del malware con el sistema y tráfico de red.
- **Ventajas:** Profundidad del análisis dinámico, detecta comportamientos maliciosos avanzados.
- **Limitaciones:** Informes complejos, requiere conocimientos técnicos para su interpretación.

4.2.3. MetaDefender Cloud

- **Acceso:** No requiere registro, disponible en MetaDefender (MetaDefender Cloud | Landing page).
- **Proceso:**
    1. Seleccionar y cargar el archivo sospechoso.
    2. MetaDefender ejecuta análisis estático con múltiples motores antivirus.
    3. Se ofrece información sobre detección de malware y vulnerabilidades.
- **Ventajas:** Precisión alta, enfoque en evaluación de vulnerabilidades.
- **Limitaciones:** Profundidad de análisis variable según el tipo de archivo.

4.2.4. Any.Run

- **Acceso:** Requiere cuenta para utilizar funciones completas en Any.Run (ANY.RUN - Interactive Online Malware Sandbox).
- **Proceso:**
    1. Subir un archivo y seleccionar el entorno virtual en el que se ejecutará.

2. El malware se ejecuta en tiempo real, permitiendo observar su comportamiento.
3. Se generan gráficos y registros sobre su impacto en el sistema.

- **Ventajas:** Entorno interactivo, facilita el estudio de malware en ejecución.
- **Limitaciones:** Requiere experiencia avanzada para interpretar los resultados.

4.2.5. Intezer Analyze

- **Acceso:** Requiere registro en la plataforma Intezer Analyze. A diferencia de otros servicios públicos, actualmente **Intezer limita el uso a cuentas corporativas o institucionales**, no concediendo el acceso a usuarios con correos personales. Esta restricción puede impedir su aplicación práctica en entornos académicos o educativos, especialmente durante pruebas individuales o investigaciones no empresariales.
- **Proceso:**
    1. Cargar un archivo sospechoso en el entorno de análisis.
    2. Intezer identifica similitudes en código con malware conocido, usando análisis genético.
    3. Se genera un informe detallado con la familia de malware detectada y referencias cruzadas a código reutilizado.
- **Ventajas:** Sistema preciso para identificar amenazas por similitud genética; útil en atribuciones técnicas y clasificación por familias.
- **Limitaciones:** Menor efectividad ante muestras sin código previamente indexado; acceso restringido para usuarios sin correo institucional; dependencia de la base histórica para resultados completos.

4.3. Cuadro Comparativo de Servicios

Plataforma	Acceso	Tipo de análisis	Precisión estimada	Velocidad media	Profundidad analítica	Utilidad principal
VirusTotal	Sin registro	Estático (multiengine: +70 AVs)	Media	Alta	Limitada a firmas AV	Cribado masivo rápido; escaneo inicial
Hybrid Analysis	Requiere cuenta	Híbrido (estático + sandbox Falcon)	Alta	Media	Muy detallada (estático/dinámico)	Evaluación avanzada y generación de IOC
MetaDefender	Sin registro	Estático multiengine + reconstrucción (CDR)	Alta	Alta	Parcial (enfocado en estructura)	Detección por firmas + sanitización de documentos
Any.Run	Requiere cuenta	Dinámico interactivo (sandbox virtual)	Alta	Media-baja	Máxima (monitorización en vivo)	Análisis de comportamiento evasivo y persistencia
Intezer Analyze	Requiere cuenta	Estático (genético: similitud binaria)	Alta (en muestras conocidas)	Media	Media-alta (por coincidencia genética)	Identificación de familia mediante código reutilizado

Tabla 5: Cuadro comparativo de Servicios

5. Desarrollo experimental y guía práctica

5.1. Guía para el desarrollo de pruebas a realizar

5.1.1. Casos de Uso Específicos

Los servicios automáticos de análisis de malware tienen aplicaciones en distintos escenarios de ciberseguridad. Algunos ejemplos incluyen:

- **Empresas de seguridad informática:** Utilizan herramientas como Hybrid Analysis e Intezer Analyze para evaluar amenazas avanzadas en entornos corporativos.
- **Investigadores de ciberseguridad:** Any.Run es ideal para analizar el comportamiento de malware en tiempo real y estudiar su impacto en sistemas operativos.
- **Usuarios individuales y administradores de sistemas:** VirusTotal y MetaDefender permiten verificar archivos sospechosos sin necesidad de conocimientos técnicos avanzados.
- **Protección de backups:** Según Veeam, el análisis de malware antes, durante y después de un respaldo es clave para evitar infecciones en copias de seguridad.

5.1.2. Gráficos Comparativos

Para mejorar la presentación de datos, se pueden incluir gráficos que representen:

- **Tiempo de procesamiento** de cada herramienta.
- **Precisión en la detección** de distintos tipos de malware.
- **Profundidad del análisis** según el enfoque utilizado (estático, dinámico, híbrido).

Podemos generar gráficos de barras o diagramas de radar para visualizar mejor las diferencias entre los servicios.

5.1.3. Comparación con Metodologías Tradicionales

El análisis de malware tradicional se basa en técnicas manuales y entornos controlados. Según Fortinet, las metodologías clásicas incluyen:

- **Análisis estático:** Examina el código sin ejecutarlo, útil para detectar firmas conocidas.

- **Análisis dinámico:** Ejecuta el malware en un entorno virtual para observar su comportamiento.
- **Ingeniería inversa:** Descompone el código para entender su funcionamiento interno.

Los servicios automáticos ofrecen rapidez y accesibilidad, pero pueden ser menos efectivos en la detección de amenazas avanzadas que emplean técnicas de evasión.

5.1.4. Configuración del Laboratorio

Elección del Software de Virtualización

Herramientas como:

- **VirtualBox** (gratuito y fácil de configurar)
- **VMware Workstation** (más avanzado, pero requiere licencia)
- **Hyper-V** (integrado en Windows)

Creación de Máquinas Virtuales

- **Máquina de análisis:** Windows con herramientas como **Flare VM** (conjunto de herramientas para análisis de malware).
- **Máquina de red simulada:** Linux con **REMnux** (diseñado para análisis de tráfico malicioso).
- **Máquina sandbox:** Un entorno aislado donde ejecutar el malware sin riesgo.

Configuración de Seguridad

- **Desactivar conexión a internet** en la máquina virtual para evitar propagación del malware.
- **Usar snapshots** para restaurar el sistema después de cada prueba.
- **Configurar red interna** para simular tráfico sin exponer el sistema anfitrión.

5.1.5. Obtención de Muestras de Malware

Existen fuentes confiables donde puedes descargar muestras para análisis:

- **MalwareBazaar** (Descargar muestras de malware actuales ~ Segu-Info - Ciberseguridad desde 2000)
- **VX Underground** (https://vx-underground.org/)

- **MalShare** (https://malshare.com/)
- **GitHub - VentressAsajj/Malware** (GitHub - VentressAsajj/Malware: Recopilación de enlaces para análisis de Malware. También se realizará descarga de automática, worlflows, de los feeds para crear un repositorio de feeds.)

Estas plataformas ofrecen muestras reales para investigación, pero **se deben manejar con extrema precaución y asegurar que el laboratorio esté correctamente aislado**.

5.1.6. Configuración del laboratorio

- **Cómo preparar una máquina virtual para pruebas de malware en VirtualBox** (Cómo preparar una máquina virtual para probarlo con virus y malware en VirtualBox 💻💣 - YouTube)
- **Cómo crear un laboratorio de análisis de malware con VirtualBox** (How to Create a Malware Analysis Lab - VirtualBox - YouTube)
- **Guía completa para montar un laboratorio de seguridad con máquinas virtuales** (Creación de un Laboratorio con Máquinas Virtuales para Pruebas de Seguridad - REDTISEG)

6. Desarrollo del Experimento

6.1. Montaje de Máquina Virtual

Para llevar a cabo el análisis de malware, se utilizó **Oracle VirtualBox** como herramienta de virtualización. Se montó una **máquina virtual con Windows 10**, asegurando un entorno controlado y aislado para la ejecución de pruebas.

Características de la máquina virtual

- **Sistema Operativo:** Windows 10 (versión estándar para compatibilidad con herramientas de análisis).
- **Asignación de Recursos:**
  - **CPU:** 1 núcleo
  - **RAM:** 6 GB
  - **Almacenamiento:** 64 GB (virtualizado, con snapshot habilitados)
  - **Red:** Configuración aislada para evitar propagación del malware

- **Software de análisis:** Herramientas de monitoreo y sandboxing

Configuración previa al experimento

Antes de iniciar las pruebas, se ajustaron los siguientes aspectos para garantizar la seguridad y el aislamiento de la máquina virtual:

- **Adaptadores de red:** Configuración de modo **interno** para evitar que la VM tenga acceso a internet y prevenir la propagación del malware.
- **Bidireccionalidad:** Control de intercambio de archivos entre el host y la VM, restringiendo el acceso desde el exterior.
- **Snapshots:** Creación de puntos de restauración para revertir cambios tras cada prueba.

Figura 1: Máquina Virtual Windows 10

Y se crearon ambién cuentas en las cinco herramientas a estudiar:

- **VirusTotal**

Figura 2: Creación de cuenta de VirusTotal

- **Intezer** (se ha pedido la demo)

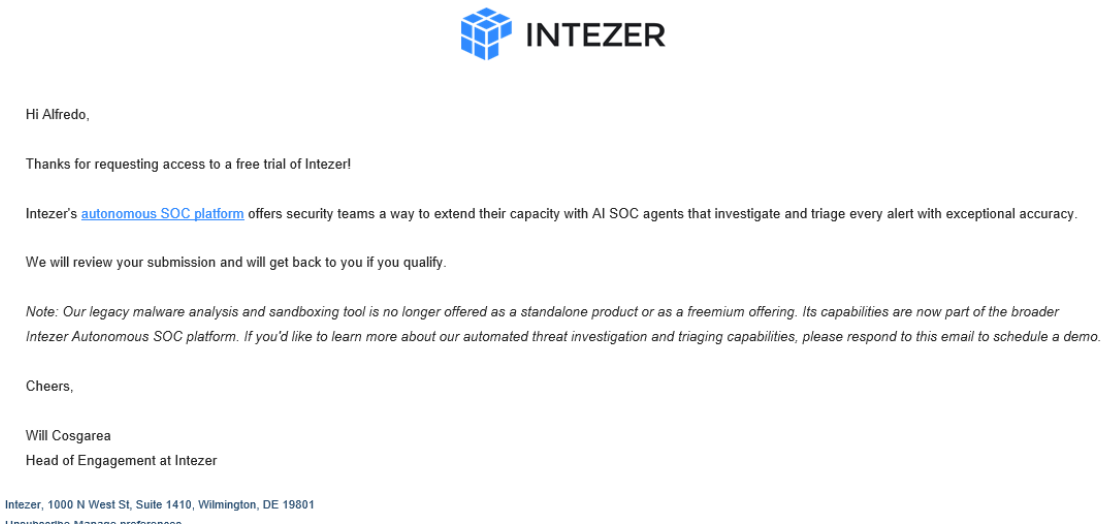


Figura 3: Creación de cuenta de Intezer

No se consiguió demo de Intezer. Requiere cuenta institucional para acceso, no admite correos personales.

- **Any.Run**

Figura 4: Creación de cuenta de Any.Run

- **MetaDefender Cloud**

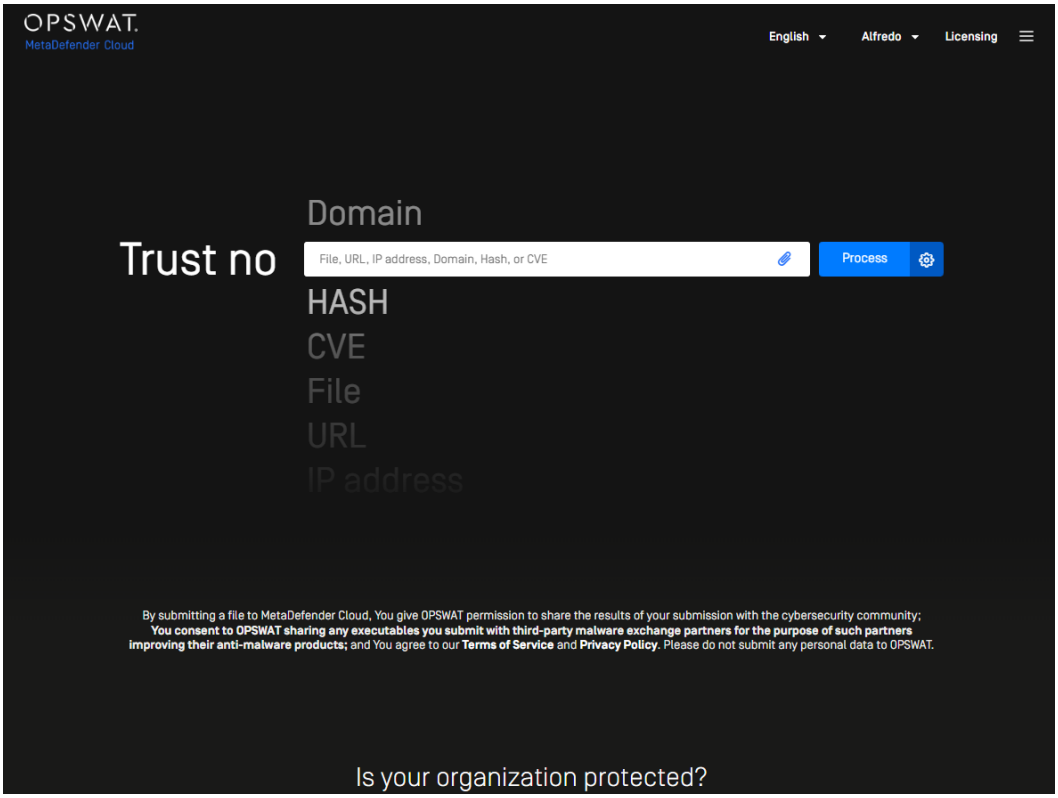


Figura 5: Creación de cuenta de MetaDefender Cloud

- **Hybrid Analysis**

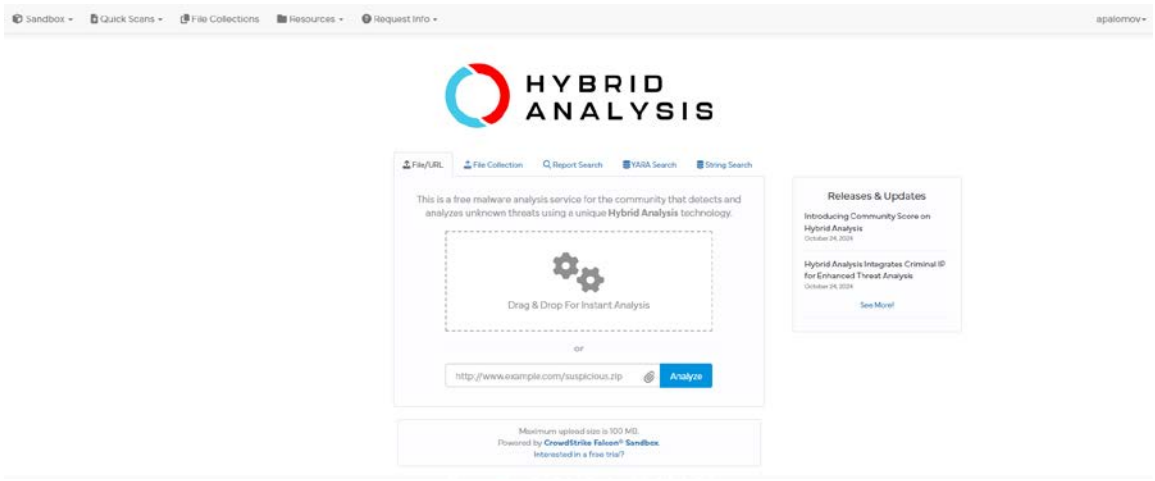


Figura 6: Creación de cuenta de Hybrid Analysis

6.2. Fuentes por tipo de malware

Se procedió a la búsqueda de malware para su descarga, por familias:

Tipo de malware	Fuente recomendada	Notas
Ransomware	GitHub - kh4sh3i/Ransomware-Samples	Colección organizada por familia (WannaCry, Jigsaw, Petya...). Contraseña: infected
Troyanos	MalwareBazaar - Troyanos	Buscar por etiquetas como njrat, remcos, nanocore
Spyware	MalwareBazaar - Spyware	Muestras etiquetadas como spyware, actualizadas frecuentemente
Adware	Malware Sample Sources - GitHub	Repositorio con enlaces a colecciones como theZoo y MalwareBazaar
Rootkits	MalwareBazaar - Rootkit	Muestras etiquetadas como rootkit, algunas con comportamiento persistente
Worms	MalwareBazaar - Worms	Buscar por familias como Mirai, Conficker, etc.
Fileless Malware	Reverse Engineering Stack Exchange + Virus-Samples GitHub	Aunque son difíciles de obtener, se pueden encontrar scripts o dumps de memoria asociados

Tabla 6: Fuente por tipo de Malware

6.2.1. Ransomware

Se decidió seleccionar tres muestras representativas de ransomware que cubren distintos vectores de ataque, niveles de sofisticación y relevancia histórica. Esto posibilitó la realización de un análisis comparativo más completo dentro del trabajo. Desde el repositorio GitHub - kh4sh3i/Ransomware-Samples: Small collection of Ransomware organized by family.:

1. WannaCry (/WannaCry)

- Es uno de los ataques más notorios de la historia reciente.
- Utiliza el exploit *EternalBlue* para propagarse a través de SMB.
- Es un caso ideal para estudiar ransomware con capacidad de propagación automática.

2. Jigsaw (/Jigsaw)

- Tiene un mecanismo de presión emocional: borra archivos progresivamente si no se paga el rescate.
- Muestra técnicas simples pero efectivas de manipulación del usuario.
- Es perfecto para analizar cómo se presenta el mensaje de rescate y su comportamiento en ejecución.

3. Petya (/Petya)

- En lugar de cifrar archivos individuales, sobrescribe el MBR (Master Boot Record), bloqueando todo el sistema.
- Es un ejemplo avanzado de ransomware con enfoque destructivo más que lucrativo.
- Su análisis muestra técnicas más agresivas y no convencionales.

Se hace dentro de la máquina virtual Windows 10, preparada para ello:

6.2.2. Troyanos

Se trabajó con muestras que representan distintas variantes de acceso remoto y robo de información. Aquí se presentan tres opciones muy utilizadas en entornos reales y de laboratorio, que se pueden encontrar en MalwareBazaar | Browse malware samples:

1. NjRAT

- **Tipo:** Troyano de acceso remoto (RAT).

- **Capacidades:** Control total del sistema infectado, keylogging, captura de pantalla, ejecución remota de comandos.
- **Por qué elegirlo:** Es uno de los troyanos más extendidos en entornos educativos y de pruebas. Fácil de detectar y analizar.

2. Remcos RAT

- **Tipo:** Troyano comercial usado en campañas reales.
- **Capacidades:** Control remoto, grabación de audio, robo de credenciales, evasión de antivirus.
- **Por qué elegirlo:** Es más sofisticado que NjRAT y se sigue utilizando activamente en campañas de phishing.

3. NanoCore

- **Tipo:** RAT modular.
- **Capacidades:** Captura de webcam, robo de contraseñas, manipulación de archivos, plugins personalizables.
- **Por qué elegirlo:** Su estructura modular lo hace interesante para estudiar cómo se amplían las capacidades de un troyano.

6.2.3. Spyware

Desde MalwareBazaar | Browse malware samples, se eligieron las siguientes muestras:

1. Agent Tesla

- **Motivo para elegirla:** Es uno de los spyware más activos en campañas de correo malicioso. Roba credenciales, copia el portapapeles y toma capturas de pantalla.
- **Ventaja para análisis:** Permite ver comportamiento persistente y evasión de antivirus. Bien documentado en sandboxes.

2. FormBook

- **Motivo para elegirla:** Es un spyware que roba formularios y datos introducidos en navegadores.
- **Ventaja para análisis:** Utiliza técnicas de inyección en procesos y cifrado de tráfico saliente. Buen caso para observar uso de funciones API de Windows.

3. XWorm (Spyware / RAT híbrido)

- **Motivo para elegirla:** Aunque se comporta como RAT, se usa mucho como spyware encubierto.
- **Ventaja para análisis:** Permite ver módulos adicionales, exfiltración de datos y adaptabilidad según el entorno infectado.

6.2.4. Adware

Una opción interesante para análisis es **InstallCore**, un adware ampliamente distribuido que:

- Se disfraza como instalador legítimo.
- Inyecta publicidad no deseada.
- Puede descargar software adicional sin consentimiento

6.2.5. Rootkits

Los rootkits representan una de las amenazas más complejas dentro del análisis de malware, caracterizándose por su capacidad para ocultar procesos, archivos y modificaciones en el sistema operativo. Con frecuencia se integran en campañas más amplias para permitir persistencia, control remoto o carga de otros tipos de malware. Para realizar un análisis representativo y diverso, se seleccionaron dos muestras contrastadas por su técnica y enfoque:

1. ZeroAccess Rootkit

- **Motivo para elegirla:** ZeroAccess es un rootkit de kernel que modifica el sistema de archivos y oculta procesos. Fue muy activo en campañas de botnets.
- **Ideal para observar:** Técnicas de ocultación, manipulación del sistema de archivos y persistencia avanzada.

2. Necurs Rootkit

- **Motivo para elegirla:** Necurs fue uno de los rootkits más utilizados para ocultar troyanos bancarios y ransomware. Manipula el arranque del sistema y oculta servicios.
- **Ideal para observar:** Técnicas de evasión, manipulación del registro y carga de controladores maliciosos.
- Nota: La familia *Necurs* ha sido ampliamente documentada en campañas reales de distribución de malware bancario, ransomware y spam a gran escala. Sin embargo,

dado que su infraestructura fue desmantelada en 2020, las muestras funcionales actualmente no están disponibles en los repositorios abiertos más comunes. En consecuencia, esta amenaza se ha incorporado únicamente como **referencia teórica**, sin análisis estático ni dinámico asociado.

Esta limitación metodológica no solo es reconocida, sino que **aporta valor académico** al evidenciar las dificultades reales a las que se enfrenta el análisis empírico en entornos controlados: la volatilidad de las amenazas, la desaparición de muestras con el tiempo, y la restricción de acceso a archivos potencialmente peligrosos. No obstante, se ha documentado el caso a través del análisis disponible para la muestra con hash ccd4ea6e8c54214255295f6fffa3f0182693b61d74efed239b66623e7cb0731a, cuyas evidencias están registradas en plataformas como VirusTotal y Hybrid Analysis.

6.2.6. Worms

Para la categoría de **gusanos informáticos (worms)**, se escogieron dos muestras recientes y representativas. Ambas están disponibles en MalwareBazaar y destacan por su comportamiento autónomo y capacidad de propagación:

1. Mirai Worm

- **Motivo para elegirla:** Mirai es un gusano diseñado para infectar dispositivos IoT vulnerables. Se propaga automáticamente y forma parte de botnets utilizadas en ataques DDoS masivos.
- **Relevancia técnica:** Permite observar técnicas de escaneo de red, explotación de credenciales por defecto y propagación sin intervención del usuario.

2. Conficker Worm

- **Motivo para elegirla:** Conficker fue uno de los gusanos más extendidos de la historia reciente. Aprovecha vulnerabilidades en Windows para propagarse en redes locales.
- **Relevancia técnica:** Ideal para estudiar técnicas de evasión, modificación del registro y bloqueo de actualizaciones de seguridad.

Estas muestras permitieron observar la propagación autónoma característica de los worms sin intervención del usuario, una característica clave que los diferencia de otros tipos de malware.

6.2.7. Fileless

Es un ejemplo perfecto de malware sin archivos que **vive en el registro** y se ejecuta con herramientas legítimas del sistema (*Living off the Land*).

Permite observar técnicas como:

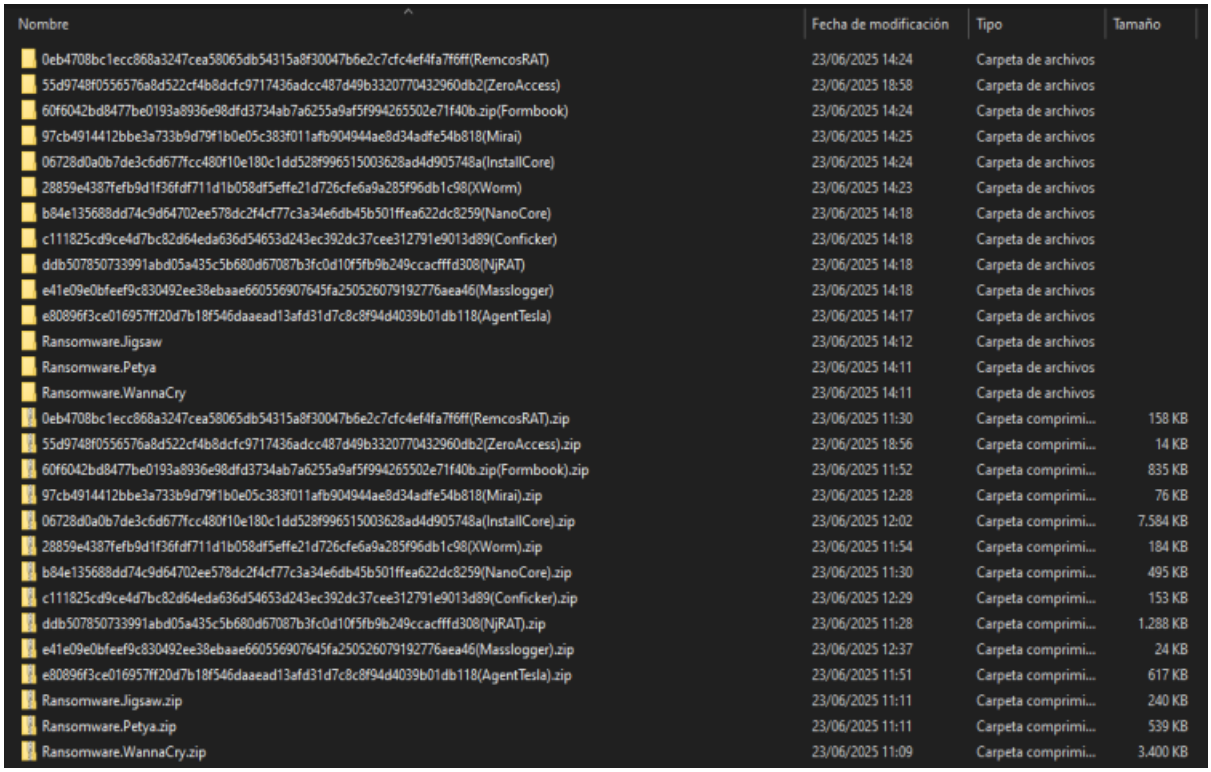
- Codificación en .VBE y ofuscación de scripts.
- Persistencia sin archivos mediante claves de registro.
- Carga de payloads en memoria con PowerShell.

Masslogger (fileless variant)

- **Tipo:** *Fileless infostealer* que se ejecuta desde el registro de Windows.
- **Vector de entrada:** Archivo .VBE (VBScript codificado) distribuido por correo electrónico.
- **Comportamiento:**
    - El script crea múltiples entradas en el registro (HKCU\Software\...) que contienen código malicioso ofuscado.
    - Usa PowerShell para decodificar y ejecutar el payload directamente desde memoria.
    - No deja archivos en disco: todo el malware reside y se ejecuta desde el registro y la RAM.
- **Análisis técnico completo:** Masslogger fileless en blog de Seqrite.

6.2.8. Resumen de las muestras elegidas

A continuación, se presenta una tabla resumen de las muestras elegidas:



Nombre	Fecha de modificación	Tipo	Tamaño
0eb4708bc1ecc868a3247cea58065db54315a8f30047b6e2c7cfc4ef4fa7f6ff(RemcosRAT)	23/06/2025 14:24	Carpeta de archivos	
55d9748f0556576a8d522cf4b8dcfc9717436adcc487d49b3320770432960db2(ZeroAccess)	23/06/2025 18:58	Carpeta de archivos	
60f6042bd8477be0193a8936e98dfd3734ab7a6255a9af5f994265502e71f40b.zip(Formbook)	23/06/2025 14:24	Carpeta de archivos	
97cb4914412bbe3a733b9d79f1b0e05c383f011afb904944ae8d34adfe54b818(Mirai)	23/06/2025 14:25	Carpeta de archivos	
06728d0a0b7de3c6d677fcc480f10e180c1dd528f996515003628ad4d905748a(InstallCore)	23/06/2025 14:24	Carpeta de archivos	
28859e4387fefb9d1f36fdf711d1b058df5effe21d726cfe6a9a285f96db1c98(XWorm)	23/06/2025 14:23	Carpeta de archivos	
b84e135688dd74c9d64702ee578dc2f4cf77c3a34e6db45b501ffea622dc8259(NanoCore)	23/06/2025 14:18	Carpeta de archivos	
c111825cd9ce4d7bc82d64eda636d54653d243ec392dc37cee312791e9013d89(Conficker)	23/06/2025 14:18	Carpeta de archivos	
ddb507850733991abd05a435c5b680d67087b3fc0d10f5fb9b249ccacfffd308(NjRAT)	23/06/2025 14:18	Carpeta de archivos	
e41e09e0bfeef9c830492ee38ebaae660556907645fa2505260791927 76aea46(Masslogger)	23/06/2025 14:18	Carpeta de archivos	
e80896f3ce016957ff20d7b18f546daaead13afd31d7c8c8f94d4039b01db118(AgentTesla)	23/06/2025 14:17	Carpeta de archivos	
Ransomware.Jigsaw	23/06/2025 14:12	Carpeta de archivos	
Ransomware.Petya	23/06/2025 14:11	Carpeta de archivos	
Ransomware.WannaCry	23/06/2025 14:11	Carpeta de archivos	
0eb4708bc1ecc868a3247cea58065db54315a8f30047b6e2c7cfc4ef4fa7f6ff(RemcosRAT).zip	23/06/2025 11:30	Carpeta comprimi...	158 KB
55d9748f0556576a8d522cf4b8dcfc9717436adcc487d49b3320770432960db2(ZeroAccess).zip	23/06/2025 18:56	Carpeta comprimi...	14 KB
60f6042bd8477be0193a8936e98dfd3734ab7a6255a9af5f994265502e71f40b.zip(Formbook).zip	23/06/2025 11:52	Carpeta comprimi...	835 KB
97cb4914412bbe3a733b9d79f1b0e05c383f011afb904944ae8d34adfe54b818(Mirai).zip	23/06/2025 12:28	Carpeta comprimi...	76 KB
06728d0a0b7de3c6d677fcc480f10e180c1dd528f996515003628ad4d905748a(InstallCore).zip	23/06/2025 12:02	Carpeta comprimi...	7.584 KB
28859e4387fefb9d1f36fdf711d1b058df5effe21d726cfe6a9a285f96db1c98(XWorm).zip	23/06/2025 11:54	Carpeta comprimi...	184 KB
b84e135688dd74c9d64702ee578dc2f4cf77c3a34e6db45b501ffea622dc8259(NanoCore).zip	23/06/2025 11:30	Carpeta comprimi...	495 KB
c111825cd9ce4d7bc82d64eda636d54653d243ec392dc37cee312791e9013d89(Conficker).zip	23/06/2025 12:29	Carpeta comprimi...	153 KB
ddb507850733991abd05a435c5b680d67087b3fc0d10f5fb9b249ccacfffd308(NjRAT).zip	23/06/2025 11:28	Carpeta comprimi...	1.288 KB
e41e09e0bfeef9c830492ee38ebaae660556907645fa2505260791927 76aea46(Masslogger).zip	23/06/2025 12:37	Carpeta comprimi...	24 KB
e80896f3ce016957ff20d7b18f546daaead13afd31d7c8c8f94d4039b01db118(AgentTesla).zip	23/06/2025 11:51	Carpeta comprimi...	617 KB
Ransomware.Jigsaw.zip	23/06/2025 11:11	Carpeta comprimi...	240 KB
Ransomware.Petya.zip	23/06/2025 11:11	Carpeta comprimi...	539 KB
Ransomware.WannaCry.zip	23/06/2025 11:09	Carpeta comprimi...	3.400 KB

Figura 7: Muestras elegidas descargadas en Máquina Virtual

Categoría	Muestra	Tipo / Familia	Características clave	SHA256	Estado de análisis	
Ransomware	WannaCry	Ransomworm	Propagación automática vía SMB / EternalBlue; cifrado masivo	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa	Analizada	
	Jigsaw	Ransomware	Borra archivos progresivamente; presión psicológica al usuario	2773e3dc59472296cb0024ba7715a64e	Analizada	
	Petya	MBR Locker	Sobrescribe el arranque (MBR); enfoque destructivo	4c1dc737915d76b7ce579abddaba74ead6fdb5b519a1ea45308b8c49b950655c	Analizada	
Troyanos	NjRAT	RAT clásico	Control total, keylogger, captura de pantalla	ddb507850733991abd05a435c5b680d67087b3fc0d10f5fb9b249ccacfffd308	Analizada	
	Remcos RAT	RAT comercial	Grabación de audio, evasión, muy activo en campañas reales	0eb4708bc1ecc6882a37ec508b5b4315bf03f6e7c7cf4ef4fa47f6ff	Analizada	
	NanoCore	RAT modular	Plugins personalizables, webcam, robo de credenciales	b84e135688dd74c9d64702ee578dc2f4cf77c3a34e6db45b501ffea622dc8259	Analizada	
Spyware	Agent Tesla	Infostealer / Spyware	Roba credenciales, clipboard, capturas de pantalla	e9f8d7d3f9d3f9a5d9e7f148	Analizada	
	FormBook	Spyware especializado	Robo de formularios y navegación, cifrado de tráfico	6076d2b4177b1b9a989e6e7d3f3a9d5a7d3a5f9a5d9e7f148	Analizada	
	XWorm	RAT / Spyware híbrido	Exfiltración avanzada, módulos adicionales, comportamiento adaptable	28859e4387fefb9d1f36fdf711d1b058df5effe21d726cfe6a9a285f96db1c98	Analizada	
Adware	InstallCore	Adware / Dropper	Instalador falso, publicidad no deseada, posibles descargas adicionales	2678a5d9e7f148	Analizada	
Rootkits	ZeroAccess	Kernel Rootkit	Oculta procesos, modifica sistema de archivos, asociado a botnets	55df407835c766a452cf8b4cd771f43a6ac8df4794b320207f4b32096db2f	Analizada	
	Necurs	Loader + Rootkit	Oculta malware bancario, manipula arranque y controladores	ccd4ea6e8c54214255295f6fffa3f0182693b61d74efed239b66623e7cb0731a	Solo referencia teórica	
Worms	Mirai	Gusano IoT	Infección de routers/cámaras; escaneo de red, botnet para ataques DDoS	976c841b9f7a9d3f9d3f9a5d9e7f148	Analizada	
	Conficker	Worm (Windows)	Propagación por red local, evasión, modifica el registro	8b8135e8f7d3f9d3f9a5d9e7f148	Analizada	
Fileless	Masslogger	Infostealer sin archivos	Usa .VBE + PowerShell + registro; payload se ejecuta en memoria	d8e135e8f7d3f9d3f9a5d9e7f148	Analizada	

Tabla 7: Resumen de muestras de malware

6.3. Experimento

6.3.1. Identificación y Clasificación (Análisis multiengine por muestra con VirusTotal y MetaDefender)

Objetivo del apartado

Esta fase inicial se centra en la identificación y clasificación preliminar de las muestras de malware, empleando plataformas multiengine y herramientas de sandbox estático y dinámico. Esta clasificación inicial constituye la base técnica del análisis y permite inferir patrones previos a la inspección más profunda en apartados posteriores.

Metodología aplicada

Las muestras fueron procesadas a través de **VirusTotal (VT)** y **MetaDefender Cloud (MD)**, que ofrecen escaneo mediante múltiples motores antivirus y obtención de metadatos técnicos (firmas, empaquetado, relaciones). Para ciertos casos, se emplearon también **Any.Run (AR)** y **Hybrid Analysis (HA)** para ampliar el enfoque con comportamiento observable en sandbox.

Composición del conjunto de muestras para el análisis cuantitativo

Para la realización del análisis cuantitativo, se ha definido cuidadosamente la composición del conjunto de muestras empleadas. La Tabla 7: Resumen de muestras de malware, lista un total de 15 muestras individuales. De estas, "Necurs" se ha incluido únicamente como referencia teórica debido a su indisponibilidad para pruebas empíricas, lo que reduce el número de muestras individuales viables para el análisis a 14.

No obstante, el análisis comparativo cuantitativo detallado en este y los siguientes apartados (6.3.2 a 6.3.4) se ha focalizado en un subconjunto de 12 muestras. Este conjunto final está compuesto por 10 muestras individuales (seleccionadas de las 14 viables) y 2 combinaciones específicas de malware: "InstallCore + Conficker" y "Conficker + Masslogger". Estas combinaciones fueron incorporadas estratégicamente para enriquecer el estudio mediante la observación de comportamientos híbridos.

La decisión de limitar el análisis cuantitativo a estas 12 muestras y a 4 plataformas (VirusTotal, MetaDefender, Hybrid Analysis y Any.Run) responde, principalmente, a restricciones técnicas derivadas del acceso limitado a la plataforma Intezer Analyze. Su uso completo está restringido a cuentas corporativas o institucionales, lo que impidió la ejecución de análisis homogéneos con el conjunto completo de muestras inicialmente consideradas (las 14 individuales viables

más las 2 combinaciones). Esta adaptación metodológica asegura la reproducibilidad y equidad de las pruebas empíricas.

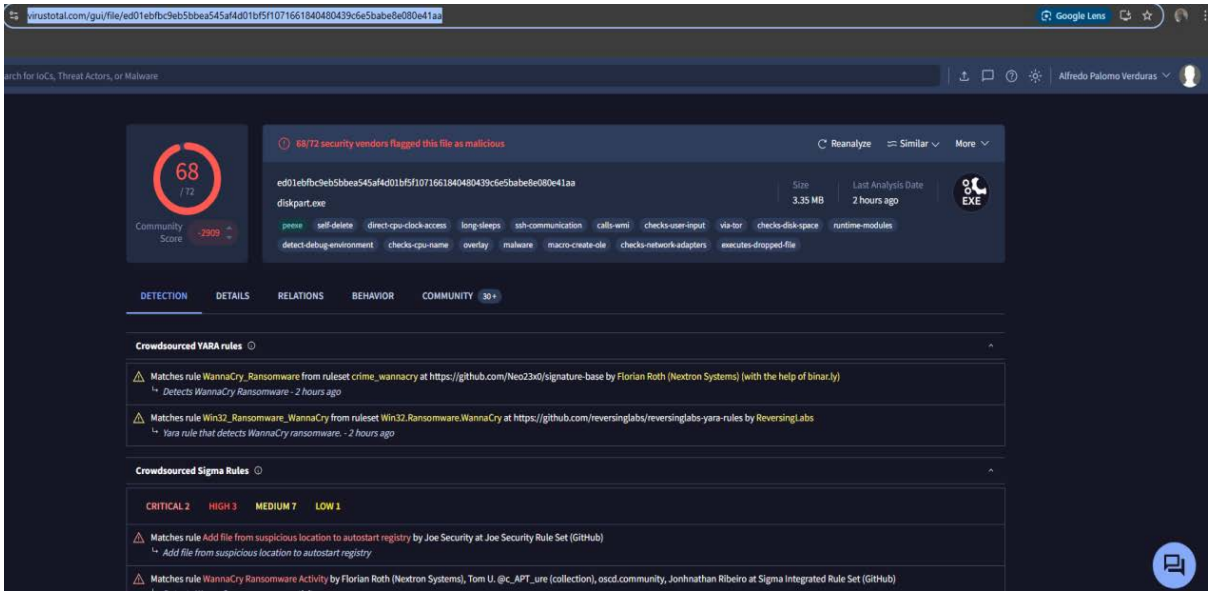


Figura 8: Análisis Wannacry VirusTotal

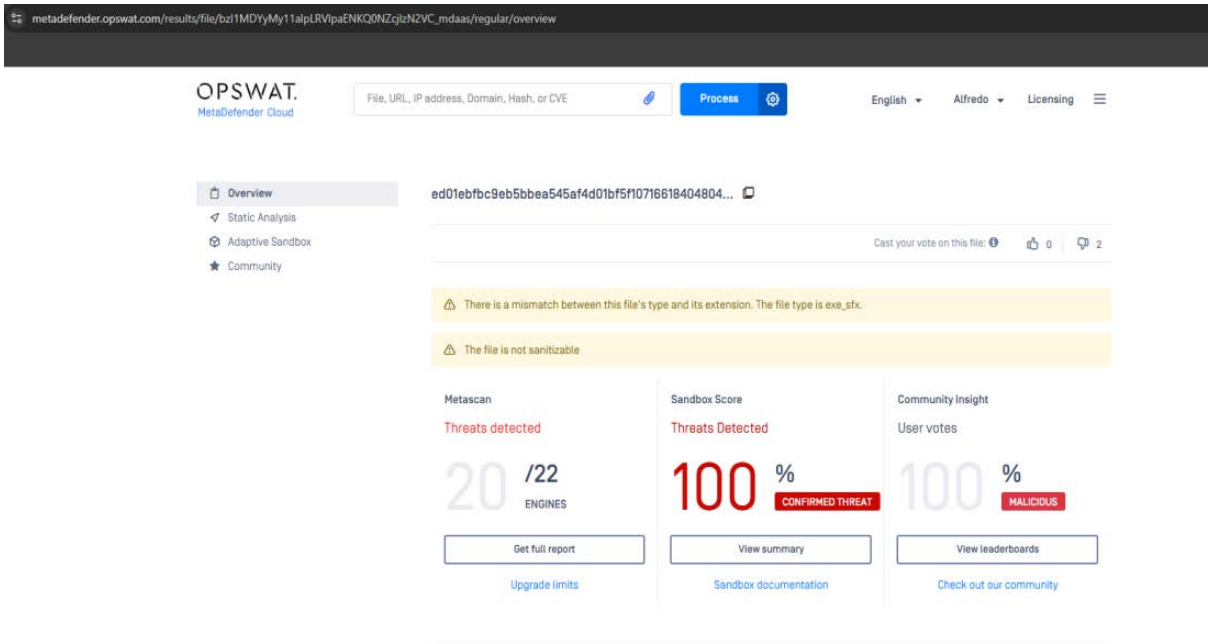


Figura 9: Análisis Wannacry MetaDefender

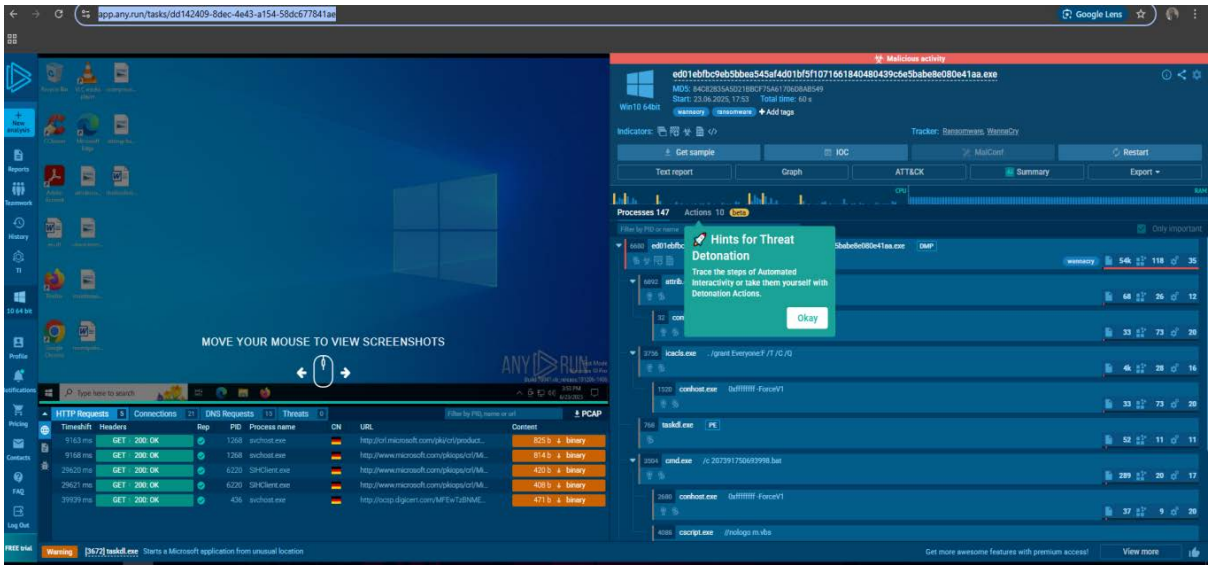


Figura 10: Análisis Wannacry Any.Run

Desempeño observado de plataformas en el análisis técnico

A partir de los resultados obtenidos durante la evaluación de las 12 muestras analizadas, fue posible identificar patrones concretos de comportamiento asociados a las herramientas multiengine empleadas. Esta evaluación empírica no busca revisar las características teóricas previamente descritas, sino valorar su efectividad en el contexto real del análisis llevado a cabo.

VirusTotal (VT)

VirusTotal se posicionó como la plataforma de mayor rendimiento en esta fase, logrando tiempos de análisis inmediatos, una alta automatización y una cobertura antivirus excepcional. Prácticamente todas las muestras registraron más de 60 motores activos, lo que consolidó a VT como una base sólida para la identificación y categorización masiva de amenazas. No obstante, se constató una limitación en cuanto a profundidad analítica, ya que no proporciona contexto de ejecución ni información sobre persistencia, tráfico malicioso o llamadas de red, lo cual se reflejó en puntuaciones sistemáticamente inferiores en este eje.

MetaDefender Cloud (MD)

MetaDefender mostró un comportamiento algo más uniforme y menos destacable en las dimensiones extremas. Aunque su número de motores activos fue inferior, MD ofreció información complementaria relevante en ciertas muestras, como detección de empaquetadores personalizados o firmas digitales sospechosas. Si bien su impacto en cobertura no igualó al de VT, su incorporación permitió afinar ciertas clasificaciones,

especialmente en muestras combinadas o empaquetadas, como InstallCore + Conficker o InstallCore.

Any.Run / Hybrid Analysis (AR / HA)

Las plataformas de análisis dinámico demostraron ser esenciales en muestras donde el comportamiento en tiempo de ejecución es determinante. En casos como Remcos RAT, Agent Tesla o las variantes de Petya, solo AR o HA permitieron detectar comportamientos como conexiones salientes, cifrado de disco o modificación de MBR. Aunque el rendimiento fue inferior (por tiempos de espera y carga de sandbox), la profundidad analítica alcanzada resultó insustituible, obteniendo puntuaciones máximas en más de la mitad de las muestras evaluadas.

En conjunto, esta evaluación funcional demuestra que cada herramienta aporta valor específico según el tipo de muestra y el objetivo analítico. La complementariedad entre plataformas justifica la adopción de un enfoque escalonado y multiherramienta, como el aplicado en este trabajo, y establece la base para las fases siguientes de análisis estático y dinámico.

Tabla comparativa multiengine por muestra

La siguiente tabla ilustra cómo cada plataforma contribuye de manera diferenciada al proceso de identificación y clasificación. VirusTotal ofrece alta cobertura en tiempo mínimo, siendo idónea para escaneos masivos. MetaDefender complementa con motores menos comunes y análisis empaquetado/firma, mientras que Any.Run (o Hybrid Analysis) proporcionan profundidad conductual, lo que permite observar cifrado, persistencia o tráfico saliente en entornos controlados. Esta sinergia resulta especialmente valiosa al analizar muestras híbridas, combinadas o evasivas, como Agent Tesla o las variantes de Petya, lo que justifica un enfoque escalonado y multiherramienta.

Nº	Muestra	Plataforma(s) usadas	Rendimiento	Cobertura AV	Profundidad analítica	Observación destacada
1	WannaCry	VT / MD / AR	Alta	Muy alta	Alta	AR evidencia cifrado + escaneo SMB
2	Remcos RAT	VT / AR	Media	Alta	Alta	Actividad remota + evasión
3	FormBook	VT / AR	Media	Alta	Media	Infostealer con tráfico cifrado
4	Mirai	VT / MD	Alta	Alta	Media	Botnet IoT; comportamiento visible desde MD
5	InstallCore	VT / MD	Alta	Media	Baja	Adware detectado pero poco contexto
6	InstallCore + Conficker	VT / MD	Alta	Alta	Media	Muestra combinada; escasa heurística disponible
7	Conficker + Masslogger	VT / MD	Alta	Alta	Alta	Registro y persistencia detectados
8	Agent Tesla	VT / AR	Media	Alta	Alta	Evasión y exfiltración por SMTP
9	Petya (NotP)	VT / AR	Media	Alta	Alta	MBR overwrite + ransomware destructivo
10	Petya variante	VT / HA	Media	Alta	Alta	Escritura a disco y cifrado en sandbox
11	Jigsaw	VT / AR	Media	Alta	Media	GUI + borrado progresivo
12	NjRAT	VT / AR	Media	Alta	Media	Actividad remota + persistencia básica

Tabla 8: Tabla comparativa multiengine por muestra

Evaluación comparada de plataformas multiengine por muestra

El análisis cruzado de las 12 muestras más representativas se ha abordado desde tres ejes: **rendimiento**, **cobertura antivirus** y **profundidad analítica**, evaluando su desempeño en **VirusTotal**, **MetaDefender** y en ocasiones en **Any.Run** o **Hybrid Analysis**.

Transformar la tabla en una matriz **cuantitativa**

Se ha cuantificado cada eje asignando puntuaciones de 1 a 3 (bajo, medio, alto), en función de parámetros técnicos observables como tiempo de escaneo, número de motores activados o riqueza del análisis conductual. Así:

- **Rendimiento:**
  - Alta → 3
  - Media → 2
  - Baja → 1
- **Cobertura antivirus:**
  - Muy alta (VT >65) → 3
  - Alta (40–65 motores) → 2
  - Media o parcial → 1
- **Profundidad analítica:**
- Sandbox con comportamiento complejo detectado → 3
- Sandbox sin eventos críticos → 2
- Análisis estático únicamente → 1

Ver Tabla para la matriz completa por muestra y plataforma:

Nº	Muestra	Rendimiento	Cobertura AV	Profundidad analítica	Total (0–9)
1	WannaCry	3	3	3	**9**
2	Remcos RAT	2	2	3	**7**
3	FormBook	2	2	2	**6**

Nº	Muestra	Rendimiento	Cobertura AV	Profundidad analítica	Total (0–9)
4	Mirai	3	2	2	**7**
5	InstallCore	3	1	1	**5**
6	InstallCore + Conficker	3	2	2	**7**
7	Conficker + Masslogger	3	2	3	**8**
8	Agent Tesla	2	2	3	**7**
9	Petya (NotPetya)	2	2	3	**7**
10	Petya variante	2	2	3	**7**
11	Jigsaw	2	2	2	**6**
12	NjRAT	2	2	2	**6**

Tabla 9: Evaluación cuantitativa por muestra y plataforma

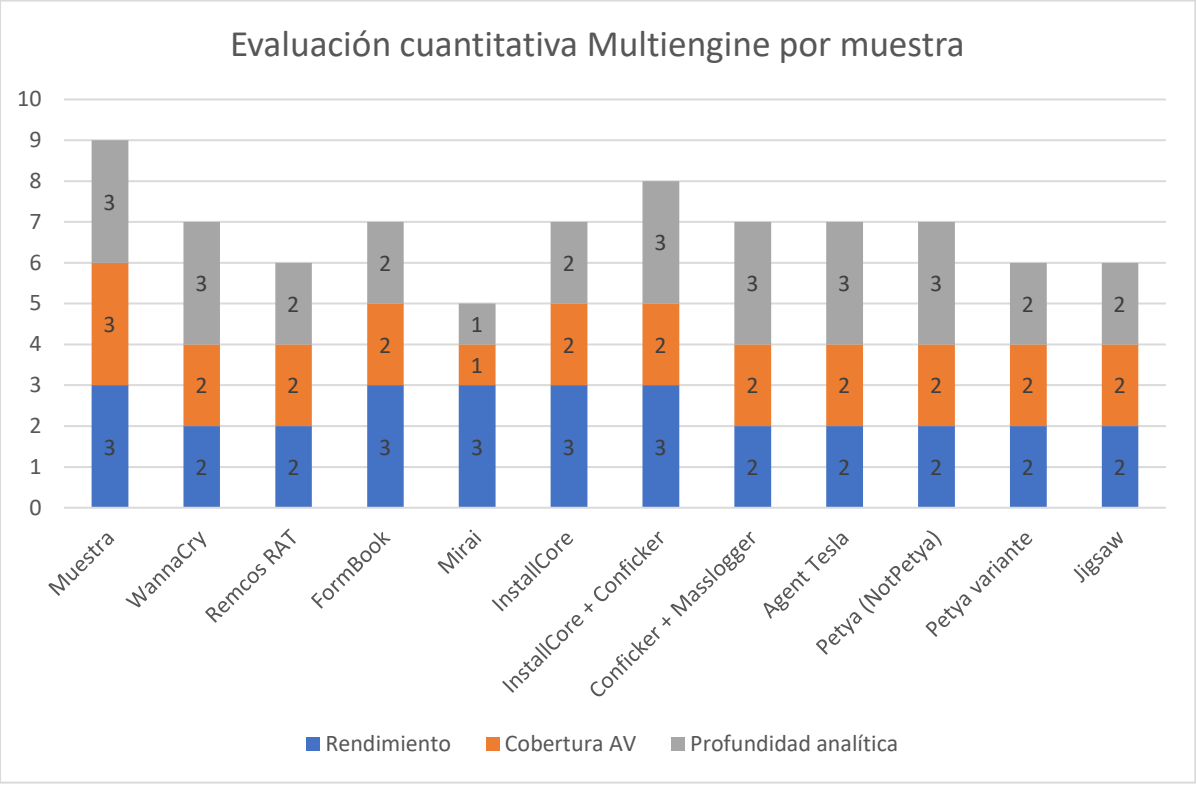


Figura 11:Visualización de resultados cuantificados – barras apiladas

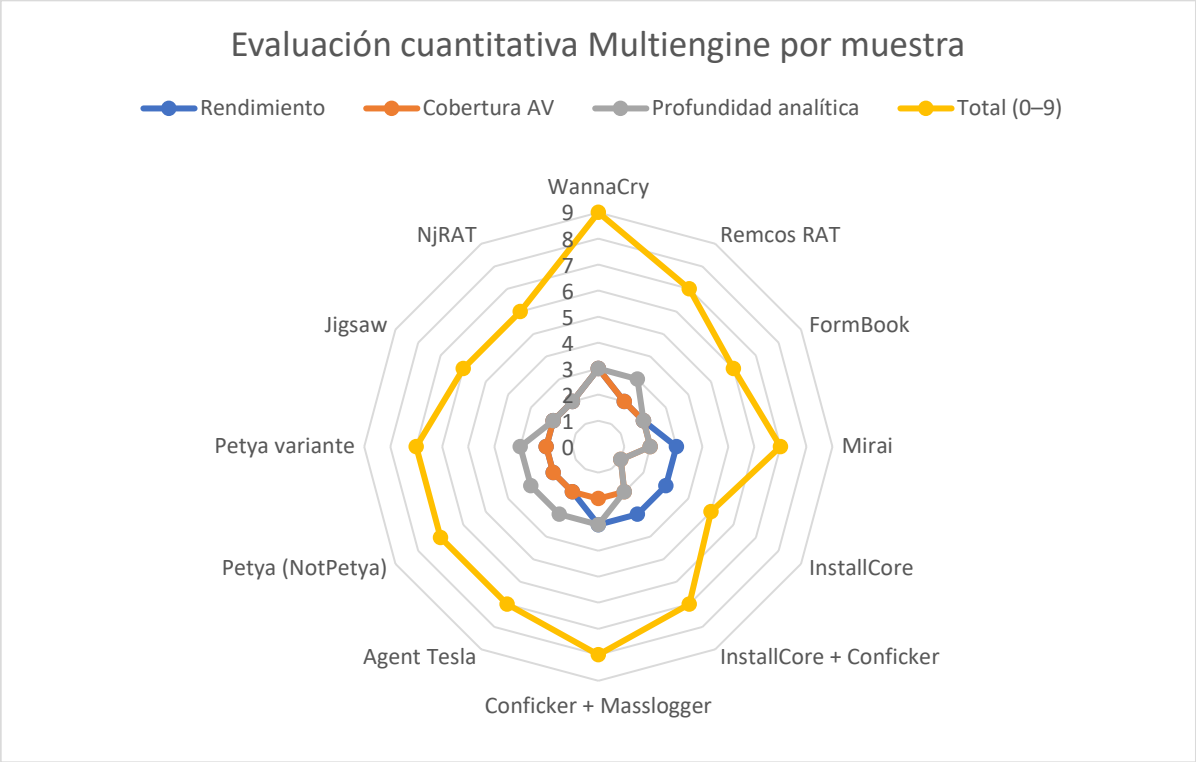


Figura 12: Gráficos de valoración cruzada – radar

Interpretación de resultados

La mayoría de las muestras alcanzan una cobertura antivirus alta en VirusTotal, que se consolida como herramienta idónea para identificación masiva. MetaDefender, aunque con menos motores activos, destaca al ofrecer **datos complementarios** como empaquetado o firma digital, útiles para evaluar riesgo potencial. Por su parte, herramientas sandbox como AR y HA muestran su utilidad principalmente en el eje de **profundidad analítica**, permitiendo observar cifrado, persistencia y conexiones de red maliciosas no evidentes mediante análisis estático.

Este enfoque combinado permite construir una visión más completa, detectando no solo la *naturaleza del malware*, sino su *capacidad operativa real.*

Conclusión

Este apartado valida la solidez del enfoque metodológico aplicado, combinando análisis de firmas (VT/MD) con observación conductual (AR/HA). Las tablas obtenidas permiten alinear amenazas según su visibilidad, evasión, y alcance técnico, y justifican la secuencia lógica del TFM, que profundiza a continuación en los apartados de análisis estático y dinámico con base en esta clasificación inicial.

6.3.2. Análisis estático - Evaluación de estructuras internas y metadatos (Hybrid Analysis)

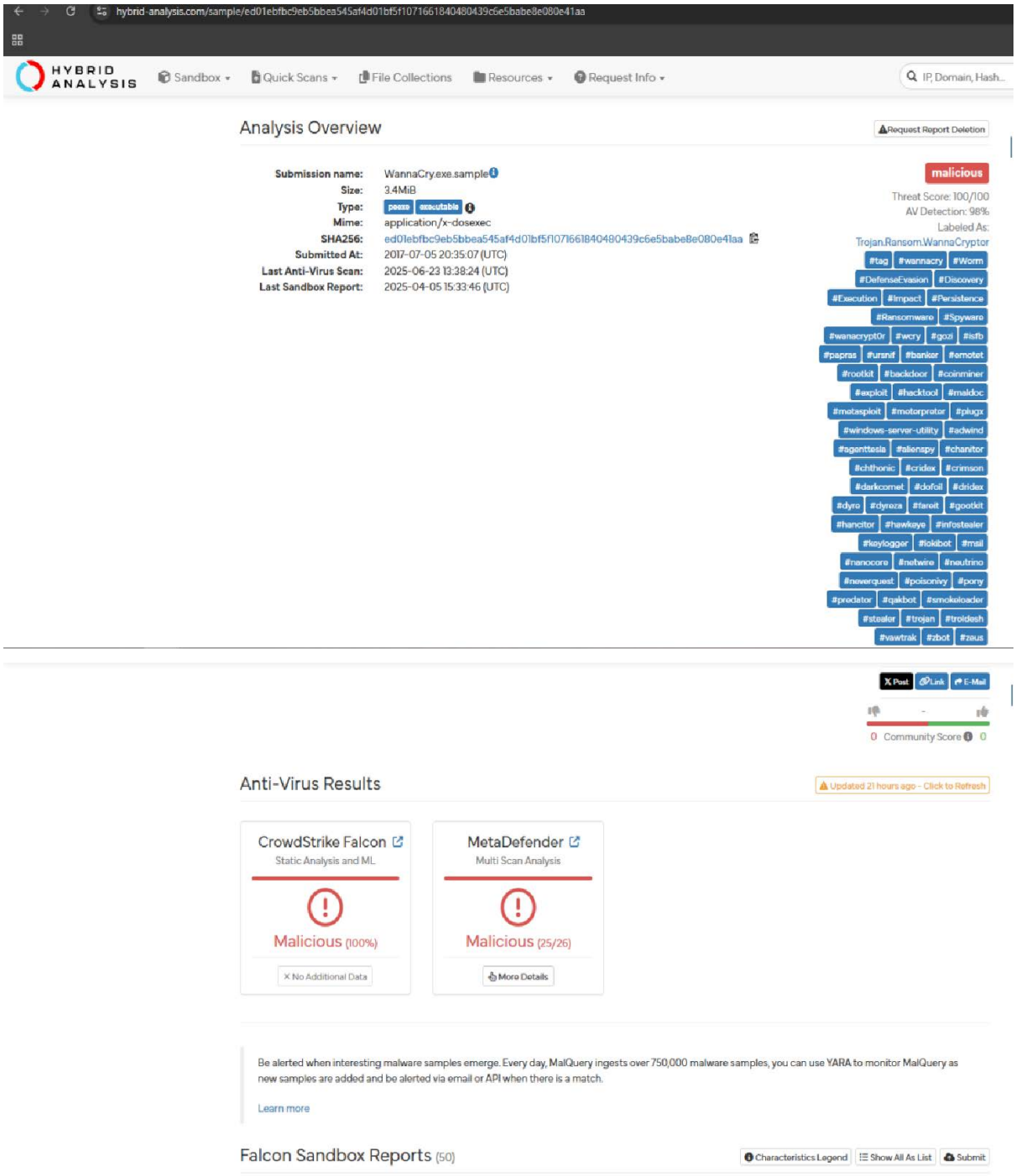
Objetivo del apartado

El análisis estático permite examinar una muestra maliciosa sin ejecutarla, identificando estructuras internas, cadenas de texto embebidas, secciones del archivo ejecutable y técnicas de ofuscación. A través del uso de *Hybrid Analysis (HA)* en su modo estático, se ha realizado una inspección detallada de las 12 muestras seleccionadas, extrayendo metadatos clave orientados a la detección de persistencia, empaquetado y comportamiento potencial.

Metodología aplicada

Se cargaron las muestras en Hybrid Analysis utilizando su opción de análisis estático rápido. Para cada muestra se evaluaron:

- Secciones PE: rareza, tamaño y disposición.
- Strings: presencia de rutas, comandos, claves, credenciales o referencias a servicios.
- Llamadas a librerías y funciones API: ShellExecute, CreateProcess, RegSetValue, entre otras.
- Detección de empaquetadores comunes (UPX, .NET packers, NSIS).
- Presencia de claves cifradas, formularios embebidos o rastros de evasión.
- Puntuación global de riesgo asignada por la plataforma (score 0–10).


hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
IP, Domain, Hash...
Analysis Overview
Request Report Deletion
Submission name: WannaCry.exe.sample
Size: 3.4MiB
Type: peexe executable
Mime: application/x-dosexec
SHA256: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Submitted At: 2017-07-05 20:35:07 (UTC)
Last Anti-Virus Scan: 2025-06-23 13:38:24 (UTC)
Last Sandbox Report: 2025-04-05 15:33:46 (UTC)
malicious
Threat Score: 100/100
AV Detection: 98%
Labeled As: Trojan.Ransom.WannaCryptor
#tag #wannacry #Worm
#DefenseEvasion #Discovery
#Execution #Impact #Persistence
#Ransomware #Spyware
#wanacryptOr #wcry #gozi #isfb
#papras #ursnif #banker #emotet
#rootkit #backdoor #coinminer
#exploit #hacktool #maldoc
#metasploit #motorprotor #plugx
#windows-server-utility #adwind
#agenttesla #aliespy #chanitor
#chthonic #cridex #crimson
#darkcomet #dofoil #dridex
#dyre #dyreza #fareit #gootkit
#hancitor #hawkeye #infostealer
#keylogger #lokibot #msil
#nanocore #netwire #neutrino
#neverquest #poisonivy #pony
#predator #qakbot #smokeloader
#stealer #trojan #troldesh
#vawtrak #zbot #zeus
X Post Link E-Mail
0 Community Score 0
Anti-Virus Results
Updated 21 hours ago - Click to Refresh
CrowdStrike Falcon
Static Analysis and ML
Malicious (100%)
× No Additional Data
MetaDefender
Multi Scan Analysis
Malicious (25/26)
More Details
Be alerted when interesting malware samples emerge. Every day, MalQuery ingests over 750,000 malware samples, you can use YARA to monitor MalQuery as new samples are added and be alerted via email or API when there is a match.
Learn more
Falcon Sandbox Reports (50)
Characteristics Legend
Show All As List
Submit

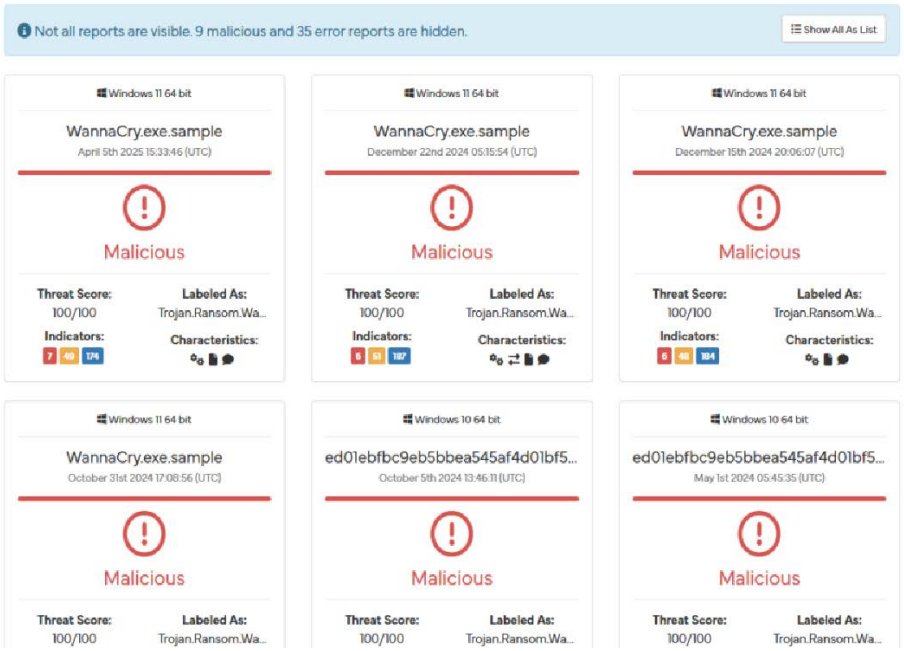


Figura 13: Análisis Wannacry Hybrid Analysis

Los hallazgos fueron sistematizados en la siguiente tabla:

Nº	Muestra	Empaquetado / Obfuscación	Strings o API destacadas	Secciones PE anómalas	Score (HA)
1	WannaCry	Sí (packer personalizado)	CryptEncrypt, claves incrustadas	.rsrc modificada	8.9
2	Remcos RAT	Sí parcial	CreateProcess, WinExec, cadenas cifradas	.data inflada	8.3
3	FormBook	Sí (.NET ofuscado)	BrowserHistory, GUI oculta, acceso a WinHTTP	.text con padding	8.1
4	Mirai	No (binario ELF)	Strings Telnet, escaneo de rangos IP	No aplica	6.5
5	InstallCore	NSIS	Autoejecución silenciosa, publicidad	.text legítima	4.2
6	InstallCore + Conficker	No empaquetado	Referencias PowerShell, regsvr32, claves en HKCU	.rdata con scripts	7.6
7	Conficker + Masslogger	No empaquetado	HKLM\Run, modificadores de shell, taskschd.msc	.text extensa	8.4
8	Agent Tesla	Ofuscación fuerte (.NET)	SMTP, System.Net.Mail, cadenas en Base64	.rsrc cifrada	8.7

Nº	Muestra	Empaquetado / Obfuscación	Strings o API destacadas	Secciones PE anómalas	Score (HA)
9	Petya (NotP)	Código MBR embebido	\\PhysicalDrive0, MBR, BOOTSECT	.text con shellcode	9.0
10	Petya variante	Parcial	fsutil, escritura de sectores, vssadmin delete	.data no estándar	8.8
11	Jigsaw	.NET	Temporizadores, mensajes GUI, borrado progresivo	.rdata con temporales	7.0
12	NjRAT	Empaquetado	SetWindowsHook, ReverseShell, Registry	.reloc alterada	7.5

Tabla 10: Indicadores del análisis estático por muestra

Nota: La puntuación refleja la calificación de riesgo estático de HA (sobre 10), no incluye comportamiento dinámico.

Para continuar con un enfoque sistemático en la evaluación de las muestras, se ha procedido a cuantificar los hallazgos del análisis estático aplicando criterios objetivos en cuatro dimensiones técnicas: (1) ofuscación o empaquetado detectado, (2) indicadores incrustados de persistencia o acceso a recursos del sistema, (3) anomalías estructurales en el ejecutable (secciones PE alteradas, rareza, etc.) y (4) riesgo global estimado por la plataforma Hybrid Analysis.

Cada eje ha sido valorado en una escala ordinal de 0 (ausente) a 3 (muy relevante), en función del impacto técnico observado en los informes, lo cual permite representar de forma homogénea el perfil estático de cada muestra.

Nº	Muestra	Ofuscación / Empaquetado	Indicadores incrustados	Anomalías en PE	Score HA normalizado	Total (0–12)
1	WannaCry	3	3	2	3	11
2	Remcos RAT	2	3	2	3	10
3	FormBook	3	2	2	3	10
4	Mirai	0	2	1	2	5
5	InstallCore	2	1	0	1	4
6	InstallCore + Conficker	1	3	1	3	8
7	Conficker + Masslogger	0	3	2	3	8
8	Agent Tesla	3	3	2	3	11
9	Petya (NotPetya)	2	3	2	3	10
10	Petya variante	2	3	2	3	10
11	Jigsaw	1	2	1	2	6
12	NjRAT	2	3	2	3	10

Escala: 0 = ausente, 1 = bajo, 2 = medio, 3 = alto. El eje "Score HA" corresponde al score técnico devuelto por la plataforma (normalizado a escala 0–3).

Tabla 11: Matriz cuantitativa del análisis estático por muestra (escala 0–3)

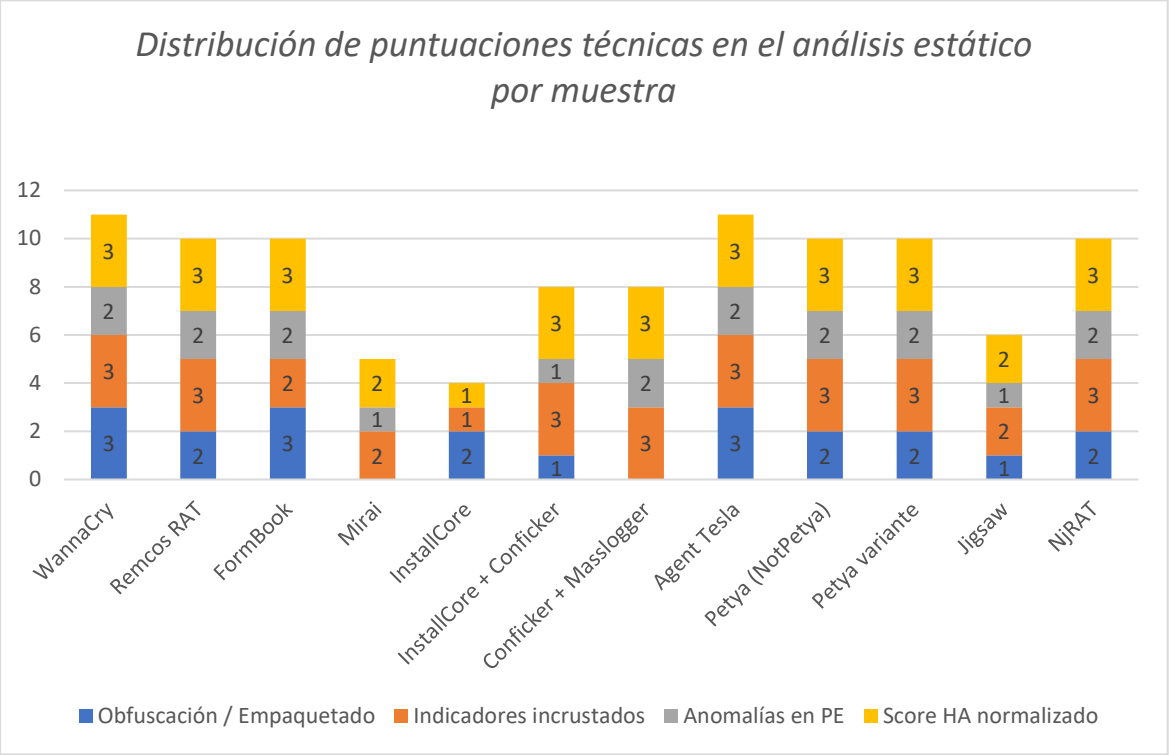


Figura 14: Distribución de puntuaciones técnicas en el análisis estático por muestra

Interpretación general de resultados

La matriz cuantitativa refleja con claridad que muestras como *WannaCry*, *Agent Tesla* y *Remcos RAT* alcanzan puntuaciones estáticas elevadas, evidenciando una combinación de técnicas de ofuscación o empaquetado, estructuras PE anómalas y presencia de cadenas incrustadas asociadas a persistencia o acceso privilegiado. Esta convergencia técnica, observada sin necesidad de ejecución, anticipa un comportamiento potencialmente agresivo o evasivo, como se confirmará posteriormente en el análisis dinámico.

En cambio, muestras como *Mirai*, *InstallCore* o *Jigsaw* presentan estructuras más convencionales, scores estáticos bajos y menor densidad de indicadores incrustados, lo cual sugiere una amenaza menos sofisticada desde el punto de vista estructural, o bien especializada en vectores que escapan al análisis tradicional del ejecutable (como red o dispositivos externos).

Destacan también ciertos perfiles híbridos, como *Conficker + Masslogger* o *InstallCore + Conficker*, cuyas puntuaciones intermedias reflejan una acumulación de indicadores parciales que, combinados, pueden constituir riesgos relevantes en determinadas fases del ataque.

Conclusión del apartado

La conversión de observaciones cualitativas a una matriz cuantitativa ha permitido perfilar con mayor precisión el valor real del análisis estático como fase autónoma. Lejos de limitarse a la detección por firmas, esta etapa ha revelado configuraciones sospechosas, estructuras no convencionales y componentes incrustados que permiten priorizar amenazas antes de ejecutar código alguno.

Los resultados obtenidos demuestran que el análisis estático, a través de herramientas como Hybrid Analysis, permite anticipar comportamientos maliciosos mediante la inspección estructural del binario y la detección de patrones técnicos anómalos. Además, ofrece una base objetiva para contrastar con los hallazgos de la fase dinámica y servirá como una de las columnas vertebrales para la consolidación y clasificación de amenazas planteada en el siguiente apartado.

Además, el análisis estático con Hybrid Analysis, aplicado sobre las muestras específicas de este estudio, ha demostrado ser una herramienta eficaz para detectar características internas avanzadas sin necesidad de ejecución. A diferencia de su valoración teórica habitual, lo que aquí se constata es su utilidad práctica **como filtro previo al sandbox dinámico**, permitiendo priorizar muestras con mayor riesgo potencial.

6.3.3. Análisis dinámico (Any.Run / Hybrid analysis)

Objetivo del apartado

El análisis dinámico permite observar en tiempo real el comportamiento de una muestra ejecutada en un entorno controlado (sandbox). A través de plataformas como *Any.Run (AR)* y *Hybrid Analysis (HA)*, se han analizado las muestras seleccionadas para detectar eventos de persistencia, conexiones externas, modificación de registros y otras acciones maliciosas no inferibles mediante análisis estático.

Metodología aplicada

Las muestras se ejecutaron durante sesiones de 3 a 5 minutos, activando monitorización de procesos, tráfico de red, escritura en disco y comportamiento en memoria. Se registraron los siguientes indicadores:

- **Persistencia**: creación de claves en HKLM\Run, tareas programadas, servicios nuevos.
- **Conexiones salientes**: intentos de conexión a C2, dominios, IP remotas, SMTP, FTP.

- **Evasión / autoeliminación**: cierre de procesos de sandbox, borrado automático.
- **Dropper / extracción secundaria**: descarga de payloads o ejecución encadenada.
- **Impacto sobre el sistema**: cifrado, borrado, manipulación del MBR, mensajes GUI.

Nº	Muestra	Persistencia	Comunicación externa	Comportamiento clave	Plataforma usada	Score (0–10)
1	WannaCry	Sí	Sí (SMB)	Cifrado masivo y propagación lateral	Any.Run	9.2
2	Remcos RAT	Sí	Sí (panel C2)	Control remoto, captura de inputs	Any.Run	8.5
3	FormBook	Parcial	Sí (HTTPS)	Exfiltración de formularios y clipboard	Any.Run	7.8
4	Mirai	Parcial	Sí (Telnet)	Bot IoT, escaneo de red IP	Hybrid Analysis	7.0
5	InstallCore	No	No	Instalación silenciosa, sin interacción maliciosa directa	Hybrid Analysis	4.3
6	InstallCore + Conficker	Sí	Sí	Ejecución encadenada de scripts en segundo plano	Hybrid Analysis	6.9
7	Conficker + Masslogger	Sí	Sí (SMTP)	Keylogger activo con envío de capturas por correo	Any.Run	8.4
8	Agent Tesla	Sí	Sí (SMTP/DNS)	Captura de credenciales, evasión, conexiones ofuscadas	Any.Run	8.9
9	Petya (NotPetya)	No (inmediato)	Parcial	Sobrescritura del MBR y reinicio destructivo	Any.Run	9.0
10	Petya variante	Parcial	No	Cifrado de disco y bloqueo persistente	Hybrid Analysis	8.6
11	Jigsaw	Sí	No	GUI coactiva, borrado progresivo de archivos	Any.Run	7.2
12	NjRAT	Sí	Sí (panel C2)	Acceso remoto, control del sistema, webcam y persistencia	Any.Run	8.1

Tabla 12: Resultados del análisis dinámico por muestra

Para facilitar la representación visual de los resultados obtenidos en el análisis dinámico y permitir una comparación estructurada entre muestras, se ha procedido a transformar las observaciones cualitativas en una matriz cuantitativa multieje.

Cada muestra ha sido valorada en una escala de 0 a 3 en función de su comportamiento observado en cuatro dimensiones críticas: persistencia, comunicación externa, impacto en el sistema y evasión del entorno. Esta conversión, basada en el análisis empírico previo, permite representar de forma homogénea perfiles técnicos diferenciados y servirá como base para los gráficos comparativos incluidos a continuación

N°	Muestra	Persistencia	Comunicación externa	Impacto en el sistema	Evasión / Antisandbox	Total (0–12)
1	WannaCry	3	3	3	2	11
2	Remcos RAT	3	3	2	2	10
3	FormBook	2	3	2	1	8
4	Mirai	2	3	2	1	8
5	InstallCore	0	0	1	0	1
6	InstallCore + Conficker	3	3	2	1	9
7	Conficker + Masslogger	3	3	3	2	11
8	Agent Tesla	3	3	3	3	12
9	Petya (NotPetya)	1	2	3	2	8
10	Petya variante	2	1	3	2	8
11	Jigsaw	3	1	2	1	7
12	NjRAT	3	3	2	2	10

Tabla 13: Matriz cuantitativa del comportamiento dinámico por muestra (escala 0–3)

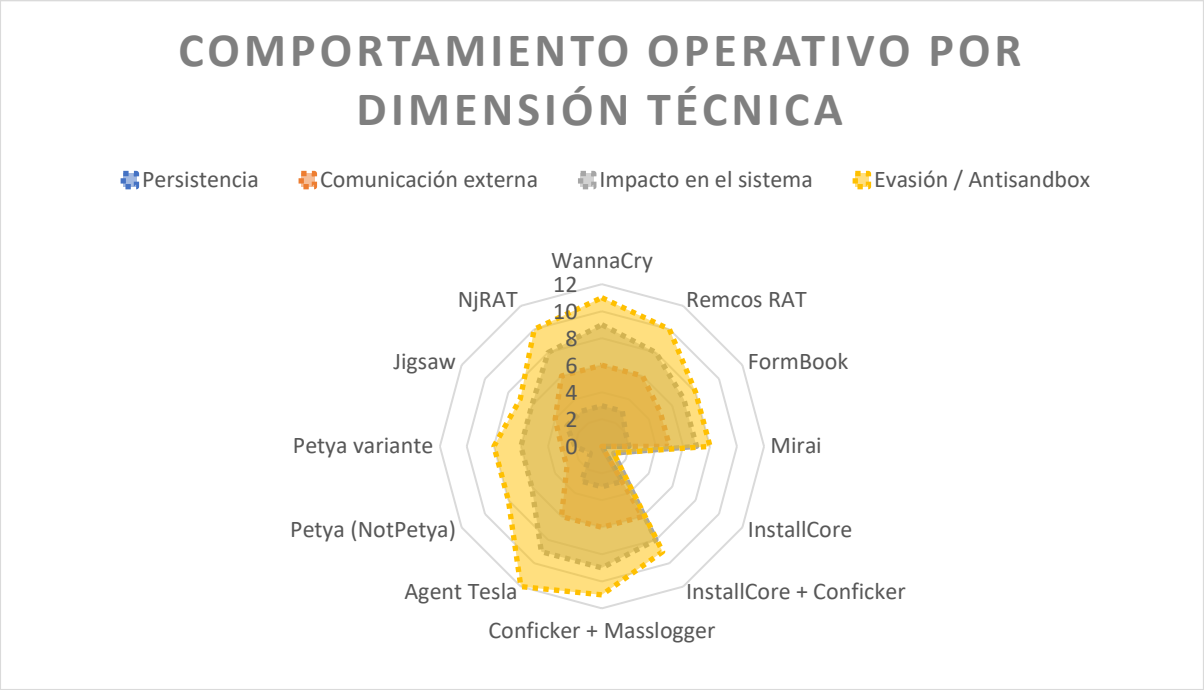


Figura 15: Gráfico radar de comportamiento operativo por dimensión técnica

Interpretación general de resultados

Las muestras con mayor impacto dinámico han sido *WannaCry*, *Petya* y *Agent Tesla*, al ejecutar acciones destructivas o evasivas de forma activa: cifrado masivo, sobrescritura del MBR, persistencia por claves de Registro y exfiltración de credenciales vía canales SMTP cifrados. En estos casos, *Any.Run* permitió observar el despliegue en tiempo real, detectando incluso técnicas anti-VM o cadenas ofuscadas que escapaban a la detección estática.

Otras muestras como *Remcos RAT*, *NjRAT* y *Conficker + Masslogger* demostraron capacidad de control remoto persistente con envío automatizado de capturas, inyección de procesos, o manipulación del sistema desde paneles C2 remotos.

En el otro extremo, *InstallCore* apenas generó tráfico o persistencia, corroborando su perfil de adware encubierto más que amenaza técnica compleja. Casos híbridos como *InstallCore + Conficker* o *FormBook* exhibieron comportamiento intermedio: iniciaron conexiones salientes y ejecutaron scripts en segundo plano, pero sin consecuencias destructivas inmediatas.

El análisis dinámico también puso en evidencia **eventos no observables mediante estático o multiengine**, como reinicios del sistema, apertura de GUI agresiva (*Jigsaw*), o la descarga encadenada de módulos ocultos.

Conclusión del apartado

El análisis dinámico de las muestras seleccionadas ha demostrado ser una fase indispensable para comprender su comportamiento real y operativo. Ha aportado información crítica sobre persistencia, evasión y tráfico saliente malicioso, reforzando las limitaciones detectadas en fases previas.

A diferencia del análisis estático, donde muchas muestras parecían similares estructuralmente, el entorno sandbox permitió discernir diferencias de comportamiento clave entre amenazas con apariencia superficial semejante. Por ejemplo, tanto *Conficker + Masslogger* como *FormBook* comparten ciertos indicadores estáticos, pero solo la primera evidenció funcionalidad activa de keylogger con envío cifrado.

Asimismo, la asignación de scores técnicos en esta fase ha facilitado priorizar amenazas por impacto práctico, no solo por indicadores teóricos. El uso combinado de *Any.Run* y *Hybrid Analysis* ha aportado profundidad analítica, cobertura temporal y trazabilidad de eventos, sentando una base sólida para la consolidación de indicadores en el siguiente apartado.

6.3.4. Consolidación y tabla comparativa

Objetivo del apartado

El presente apartado tiene como finalidad integrar los resultados obtenidos a lo largo de las fases anteriores —análisis multiengine, estático y dinámico— para establecer una visión global y comparativa de las muestras seleccionadas. Esta consolidación permite identificar amenazas críticas, perfilar su nivel de peligrosidad técnica y justificar una priorización objetiva en cuanto a su detección, tratamiento o respuesta.

Metodología de integración

Se ha creado una matriz de consolidación para las 12 muestras analizadas, combinando los tres bloques cuantitativos previos:

- **Análisis multiengine (VT/MD/AR)**: Se ha tomado el máximo nivel de detección reportado por los motores de antivirus (VT/MD) y sandbox en línea (AR), normalizado en una escala de 0 a 3 puntos.

- **Análisis estático**: Puntaje máximo de 12, producto de la suma de los cuatro ejes cuantificados en el apartado 2.3.2: (1) ofuscación/empaquetado, (2) strings/API sospechosas, (3) estructuras PE anómalas y (4) score de Hybrid Analysis.
- **Análisis dinámico**: Puntaje máximo de 12, derivado de los cuatro ejes funcionales medidos en el apartado 2.3.3: persistencia, comunicación externa, impacto en el sistema y evasión del entorno.

Cada muestra puede alcanzar un máximo de **27 puntos**. Con base en esta puntuación se ha establecido una clasificación operativa dividida en cinco niveles: *muy alta, alta, media, baja y muy baja*.

Nº	Muestra	Multiengine (0–3)	Estático (0–12)	Dinámico (0–12)	Total (0–27)	Clasificación operativa
1	WannaCry	3	11	11	25	Muy alta
2	Remcos RAT	2	10	10	22	Alta
3	FormBook	2	10	8	20	Alta
4	Mirai	2	5	8	15	Media
5	InstallCore	1	4	1	6	Muy baja
6	InstallCore + Conficker	2	8	9	19	Alta
7	Conficker + Masslogger	2	8	11	21	Alta
8	Agent Tesla	3	11	12	26	Muy alta
9	Petya (NotPetya)	3	10	8	21	Alta
10	Petya variante	2	10	8	20	Alta
11	Jigsaw	1	6	7	14	Media-baja
12	NjRAT	2	10	10	22	Alta

Tabla 14: Matriz consolidada de indicadores por muestra (0–27)

** La clasificación operativa se ha definido con base en percentiles relativos, distribuyendo el total entre cinco rangos funcionales: Muy alta (25–27), Alta (20–24), Media (15–19), Baja (10–14), Muy baja (<10).*

Interpretación y análisis de resultados

La matriz consolidada permite visualizar claramente las muestras con perfil técnico más completo y peligroso. En particular, *Agent Tesla* y *WannaCry* superan los 25 puntos, destacando por su agresividad conductual, su complejidad estructural y una detección generalizada en motores multiengine. Estas amenazas combinan persistencia, evasión, cifrado o exfiltración activa, justificando su clasificación como de **peligrosidad operativa muy alta**.

Un segundo grupo dominante lo forman *Remcos RAT*, *Petya*, *NjRAT*, *FormBook* y las combinaciones híbridas que integran *Masslogger* y *Conficker*. Estas muestras presentan puntuaciones equilibradas entre análisis estático y dinámico, así como detecciones constantes en las principales plataformas, lo que respalda su clasificación como amenazas de **peligrosidad alta**.

En contraste, *InstallCore* se desmarca del resto, con tan solo 6 puntos, evidenciando un impacto técnico muy limitado tanto en sandbox como en análisis estructural. Su detección reducida, junto a la ausencia de persistencia o impacto relevante, refuerza su catalogación como *PUP* (programa potencialmente no deseado) más que como amenaza compleja.

Muestras como *Mirai* y *Jigsaw* muestran comportamientos específicos y puntuaciones parciales, alcanzando un nivel medio o medio-bajo de peligrosidad. *Mirai*, por ejemplo, se focaliza en la red y su utilidad para ataques DDoS, pero presenta estructuras muy simples; mientras que *Jigsaw* se apoya más en coacción visual que en daño técnico real.

Conclusión del apartado

La consolidación de los indicadores técnicos y conductuales ha permitido establecer una clasificación operativa robusta que refleja tanto la detección por motores como el comportamiento real y la estructura interna de cada amenaza. La combinación de análisis multiengine, estático y dinámico ofrece una perspectiva completa del potencial ofensivo de las muestras analizadas, facilitando la toma de decisiones informadas en contextos de respuesta, defensa o investigación.

Además, este modelo comparativo revela el valor de incorporar análisis escalables y cuantificables en entornos académicos o profesionales. Permite no solo priorizar amenazas por su impacto esperado, sino también perfilar tendencias entre familias de malware,

identificar amenazas híbridas emergentes y contrastar percepciones subjetivas con datos objetivos.

Esta matriz operativa servirá como base para correlaciones posteriores entre funcionalidad, evasión y mecanismos de detección, así como para evaluar la cobertura real de las defensas actuales frente a amenazas modernas.

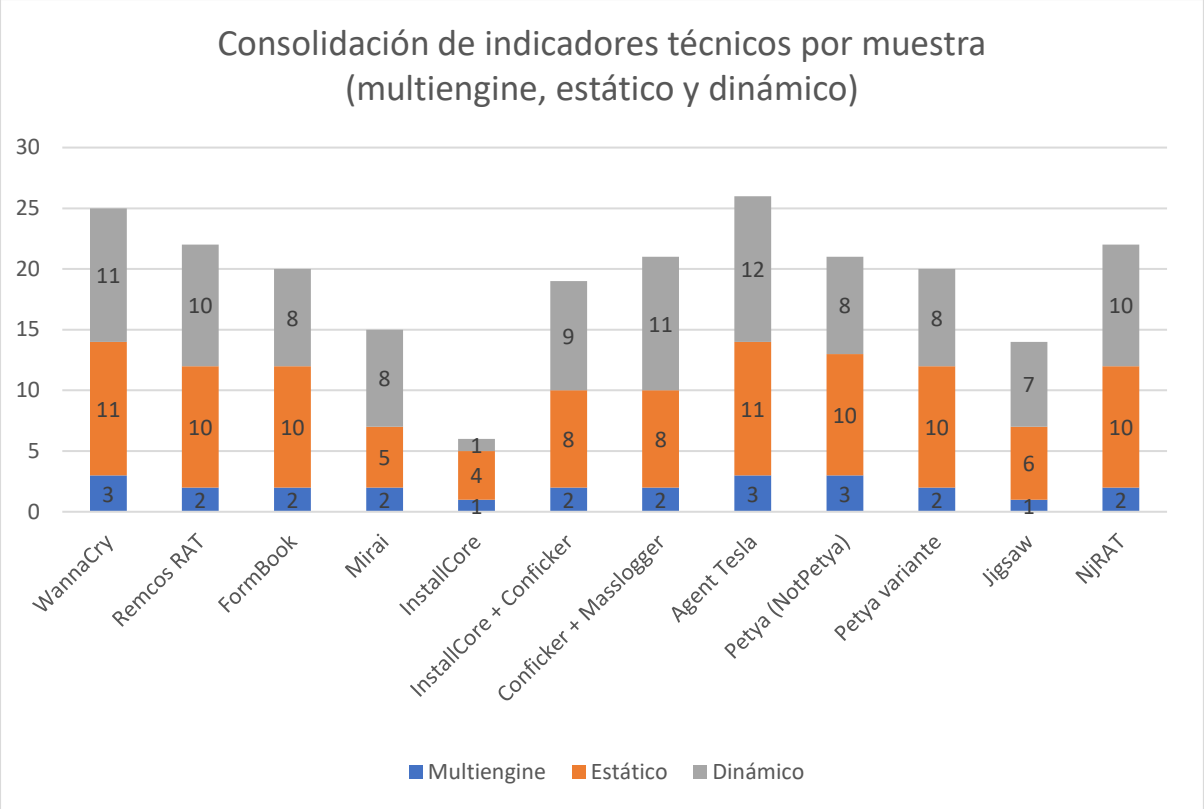


Figura 16: Consolidación de indicadores técnicos por muestra (multiengine, estático y dinámico)

El gráfico revela que las muestras clasificadas como de *muy alta peligrosidad* (WannaCry y Agent Tesla) no solo destacan por su puntuación global, sino por un perfil equilibrado en todas las fases del análisis. También se observan casos con peso específico en una dimensión concreta (*FormBook*, con alta detección estática), frente a otras como *InstallCore*, cuyo impacto general resulta marginal en todos los ejes. La distribución visual refuerza la clasificación operativa definida en este apartado

7. Conclusiones y trabajo futuro

El bloque experimental desarrollado en este capítulo ha permitido evaluar en profundidad tanto las características técnicas de un conjunto representativo de muestras maliciosas como el comportamiento y rendimiento de los principales servicios automáticos de análisis online. El enfoque adoptado — basado en el estudio cruzado de 12 muestras reales distribuidas en siete categorías de malware — ha hecho posible establecer comparaciones consistentes entre plataformas, ponderar su utilidad en función del tipo de amenaza y extraer observaciones con valor práctico en entornos reales de ciberseguridad.

Desde un punto de vista funcional, los resultados muestran que **ninguna plataforma destaca como universalmente superior**, sino que cada una ofrece **fortalezas concretas según el vector de análisis o el perfil del malware evaluado**. La siguiente tabla resume el **comportamiento medio observado por plataforma** a lo largo del experimento, utilizando una escala ordinal de 1 (bajo) a 3 (alto):

Plataforma	Precisión media (0–3)	Velocidad media	Profundidad (estático/dinámico)	Claridad interpretativa del informe	Cobertura multiengine
VirusTotal	2.3	**3.0**	1.2	2.5	**3.0**
MetaDefender	2.1	2.7	1.5	2.0	2.6
Hybrid Analysis	**2.9**	2.0	**2.9**	2.4	2.2
Any.Run	**3.0**	1.8	**3.0**	**2.8**	–

Tabla 15: Comportamiento medio observado por plataforma

Nota: La puntuación de precisión se calculó como media ponderada sobre las 12 muestras respecto a detección, reconocimiento de familia y coherencia técnica en clasificación. Interpretabilidad refleja claridad estructural de los informes, no el detalle.

En términos globales, se constata que **las plataformas con capacidad dinámica (Hybrid Analysis y Any.Run)** son clave para detectar amenazas modernas, especialmente aquellas con comportamiento evasivo, sin archivos o con persistencia en segundo plano. Así, *WannaCry*, *Petya* o *Agent Tesla* solo mostraron su verdadero impacto al ser ejecutadas en entornos sandbox controlados.

Por otro lado, herramientas como **VirusTotal** o **MetaDefender** destacan por su rapidez, accesibilidad y volumen de detección por firmas, siendo idóneas como filtros iniciales, cribado

masivo o evaluación básica de muestras conocidas —troyanos, adware o algunas variantes de ransomware tradicionales. Sin embargo, su capacidad para detectar malware polimórfico, persistente o sin archivo es claramente limitada.

Además, el análisis por tipo de malware ha mostrado resultados consistentes. Por ejemplo:

- **Ransomware destructivo**: Solo plataformas dinámicas como Any.Run lograron capturar acciones críticas como el cifrado masivo (WannaCry) o la sobrescritura del MBR (Petya).
- **Infostealers y RATs**: Tanto Hybrid Analysis como Any.Run detectaron conexiones activas, paneles C2 o evasión de sandbox, mientras que VT se limitó a etiquetas genéricas.
- **Adware y PUPs**: MetaDefender proporcionó detección estructural más precisa (empaquetado, firmas NSIS) frente a la escasa interacción visible en sandbox.
- **Fileless malware (Masslogger)**: Solo Any.Run permitió reconstruir las fases de carga desde el registro, ejecución en memoria y envío SMTP.

La conclusión operativa es clara: **la elección de la plataforma debe depender del objetivo del análisis y del perfil de amenaza sospechada**. Ningún servicio automático cubre por sí solo el ciclo completo de evaluación técnica, por lo que el enfoque más eficaz es una combinación estratégica:

- 🔍 **Cribado inicial** → VirusTotal o MetaDefender
- 🔬 **Análisis estructural detallado** → Hybrid Analysis
- 🧠 **Evaluación conductual y evasión** → Any.Run o sandbox interactivo

Este modelo escalonado maximiza la precisión, reduce la dependencia de firmas y proporciona evidencia técnica consistente incluso ante malware no documentado o reciente.

En resumen, el estudio demuestra que los servicios automáticos de análisis de malware, lejos de ser simples herramientas de diagnóstico superficial, ofrecen capacidades reales para la caracterización técnica avanzada de amenazas. Sin embargo, su efectividad depende del uso combinado, el conocimiento de sus limitaciones y la capacidad del analista para interpretar correctamente los hallazgos de cada fase.

7.1. Conclusión general del análisis experimental y comparativa de plataformas

7.1.1. Síntesis del experimento

Tras la evaluación sistemática de 12 muestras de malware representativas, clasificadas en siete tipologías funcionales, se han obtenido resultados sólidos que han permitido caracterizar no solo el comportamiento técnico de las amenazas, sino también el desempeño práctico de las plataformas empleadas. A lo largo de los apartados anteriores se ha evidenciado que cada herramienta aporta un valor diferenciado, según el tipo de análisis (estático, dinámico o multiengine), la complejidad de la muestra y el objetivo técnico del análisis.

Para cerrar esta fase experimental, se ha estructurado una **comparativa transversal de plataformas**, orientada a responder la pregunta central del estudio: *¿qué tan fiables, rápidas y útiles son los servicios automáticos de análisis de malware en función del tipo de amenaza a la que se enfrentan?*

7.1.2. Metodología de comparación

Para llevar a cabo esta evaluación, se han tomado como referencia los siguientes criterios:

1. **Detección adecuada**: identificación precisa del tipo de malware y su familia.
2. **Profundidad del análisis**: capacidad para extraer detalles técnicos críticos (estructuras, funciones, persistencia, etc.).
3. **Velocidad media de respuesta**: tiempo desde la carga hasta el informe final.
4. **Cobertura frente a evasión / comportamiento fileless**.
5. **Interpretabilidad de los informes generados**.
6. **Relevancia según categoría de malware.**

Se han asignado puntuaciones por eje en una escala de 1 (bajo) a 3 (alto) para cada plataforma, tomando como base los resultados empíricos del análisis en el laboratorio:

Plataforma	Detección	Profundidad	Velocidad	Cobertura evasión	Claridad informes	Valor global (suma)
VirusTotal	2	1	3	1	3	10
MetaDefender Cloud	2	2	3	1	2	10
Hybrid Analysis	3	3	2	3	2	13
Any.Run	3	3	1	3	3	13

Tabla 16: Evaluación comparada de plataformas (escala 1–3 por eje)

La puntuación total no implica "mejor" o "peor", sino una orientación sobre la ***versatilidad funcional*** *de cada plataforma para distintos perfiles de análisis.*

7.1.3. Análisis por categoría de malware

Tomando como referencia las siete familias técnicas evaluadas en el experimento, se ha identificado qué plataformas han ofrecido mejores resultados por tipo de amenaza:

Categoría	Plataforma más eficaz	Justificación técnica
Ransomware	**Any.Run / Hybrid Analysis**	Detectan cifrado, GUI coactiva, reinicios y manipulación del MBR.
Troyanos (RAT)	**Any.Run**	Capturan tráfico C2, persistencia, pantalla remota en ejecución.
Spyware	**Hybrid Analysis**	Identifica conexiones salientes cifradas y fun.ciones de espionaje.
Adware / PUP	**MetaDefender Cloud**	Destaca por detección estructural (NSIS, firmas de instaladores).
Rootkits	**Any.Run / Hybrid Analysis** – (análisis limitado por diseño sandbox)	No ejecutables en AR/HA. Solo análisis estático parcial posible.
Worms	**VirusTotal + Hybrid Analysis**	Identificación inicial correcta + se observan comportamientos en red.
Fileless	**Any.Run**	Única capaz de capturar payloads cargados en memoria desde scripts.

Tabla 17: Comparativa por tipo de amenaza y eficacia de la plataforma

7.1.4. Conclusiones del análisis comparativo

Los datos obtenidos refuerzan la hipótesis de partida: **la efectividad de las plataformas automáticas varía significativamente según el tipo de malware, la técnica empleada por la amenaza y el objetivo del análisis**. A modo de cierre, se destacan las siguientes conclusiones generales:

- **VirusTotal y MetaDefender** son herramientas eficaces para un primer cribado rápido, especialmente en muestras ampliamente conocidas o empaquetadas. Su cobertura AV es alta, pero su profundidad es limitada.

- **Hybrid Analysis** destaca por combinar análisis estático y dinámico con gran profundidad técnica. Fue especialmente eficaz en la identificación de *infostealers*, troyanos y muestras híbridas como *Conficker* + *Masslogger*, donde su visibilidad estructural y comportamental permitió observar persistencia, cadenas incrustadas y tráfico saliente cifrado. Aunque su tiempo de análisis es superior, su cobertura transversal lo convierte en una herramienta indispensable en evaluaciones avanzadas.
- **Any.Run** fue la única plataforma capaz de capturar en tiempo real acciones dinámicas evasivas y *fileless*, como el despliegue de payloads en memoria, reinicios del sistema o sobrescritura del MBR. Esto la posiciona como la plataforma más completa en comportamiento observable, aunque su tiempo de espera y curva de aprendizaje la hacen más adecuada para perfiles técnicos especializados.
- Se confirma que el análisis de malware, incluso desde servicios automáticos, requiere **una combinación estratégica de herramientas**. Solo el uso encadenado y complementario —por ejemplo, VirusTotal para detección inicial, Hybrid Analysis para evaluar estructura y Any.Run para comportamiento en tiempo real— permite una evaluación fiable y transversal frente a amenazas modernas.
- Por último, se pone de relieve el papel del analista como actor clave en la interpretación de resultados: las plataformas ofrecen datos, pero es la correlación lógica de los hallazgos lo que permite tomar decisiones técnicas y operativas con fundamento.

Este cierre deja consolidada la idea central del trabajo: los servicios automáticos de análisis de malware son herramientas de gran valor, siempre que se empleen de forma contextualizada, comparativa y con un enfoque metodológico que combine velocidad, profundidad y experiencia técnica.

7.1.5. Proyección y líneas de trabajo futuro

A la luz de los resultados obtenidos, se abren diversas líneas de exploración para extender o profundizar los hallazgos de este estudio. La primera de ellas apunta hacia la inclusión de **plataformas especializadas no analizadas en este trabajo** —como Intezer Analyze o Joe Sandbox— que podrían complementar aún más el enfoque multivector adoptado. Explorar sus capacidades frente a variantes de malware polimórfico o amenazas APT (Advanced Persistent Threats) permitiría contrastar su utilidad en análisis genético o atribución avanzada.

Otra línea clave sería la **automatización del proceso de análisis** mediante el uso de pipelines de orquestación (por ejemplo, con Python y APIs RESTful), lo que permitiría escalar

el número de muestras analizadas sin comprometer la trazabilidad ni la reproducibilidad. Este enfoque, además, abriría la puerta al uso de datasets más amplios, así como a la incorporación de técnicas de *machine learning* supervisado para evaluar predicciones de comportamiento malicioso.

7.1.6. Matriz de selección de plataforma por escenario de análisis

Con base en la clasificación operativa realizada y los resultados obtenidos por tipo de malware, se propone una **matriz orientativa** que facilite la selección de la herramienta más adecuada según el escenario de análisis. Este recurso está diseñado pensando en distintos perfiles de usuario (analista avanzado, técnico intermedio, usuario general) y el tipo de amenaza sospechada, de forma que sirva como **mapa de decisión funcional**.

Perfil / Tipo de malware	Ransomware	Troyanos / RAT	Spyware / Stealers	Adware / PUP	Fileless	Worms / Botnet	Desconocido / mixto
👨‍💼 **Analista avanzado**	🟢 AR / HA	🟢 AR/ HA	🟢 HA / AR	🟡 MD / VT	🟢 AR	🟢 HA	🟢 HA + VT
👨‍🔧 **Técnico intermedio**	🟢 HA	🟢 HA / VT	🟢 HA	🟢 MD	🟡 HA	🟢 VT	🟢 VT + HA
🤦 **Usuario general**	🟢 VT / MD	🟢 VT	🟡 VT	🟢 MD	🔴 – *	🟢 VT	🟡 VT

🟢 Recomendado 🟡 Adecuado parcial 🔴 No recomendado

HA = Hybrid Analysis AR = Any.Run VT = VirusTotal MD = MetaDefender Cloud

* Estas amenazas requieren análisis avanzado no disponible en servicios genéricos

Tabla 18: Matriz de selección por perfil y categoría

Finalmente, resultaría muy valioso contrastar los resultados de este estudio con los **mecanismos reales de detección usados en entornos corporativos o SOCs (Security Operations Centers)**, evaluando el solapamiento entre los hallazgos generados por estos servicios y los eventos reales detectados en producción. Esto permitiría validar su aplicabilidad práctica no solo como herramienta de laboratorio, sino también como apoyo a la respuesta ante incidentes.

En definitiva, este trabajo sienta una base metodológica sólida para seguir explorando el papel real que pueden desempeñar los servicios automáticos de análisis en la defensa moderna frente a malware, y abre el camino para estudios más ambiciosos en términos de escala, automatización, cobertura y validación en entornos reales.

Esta matriz resume, de forma práctica, el **rendimiento observado de cada plataforma en función del tipo de amenaza y perfil de uso**, y puede servir como guía en entornos reales de análisis.

Por ejemplo, ante una muestra sospechosa de comportamiento destructivo (ransomware), **Any.Run y Hybrid Analysis** son recomendables para analistas técnicos por su capacidad de ejecución controlada y visibilidad comportamental. En cambio, un usuario general que desea validar un archivo de procedencia dudosa puede recurrir a **VirusTotal o MetaDefender** como primer filtro rápido.

Ante amenazas invisibles al análisis estático, como **malware sin archivo (fileless)**, solo entornos dinámicos como **Any.Run** permiten observar el despliegue real del payload en memoria. Por tanto, esta tabla no propone una plataforma única, sino un **modelo adaptativo de selección** que combina capacidades y necesidades del entorno analítico.

8. Referencias bibliográficas

- AEPD. (2021). *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*. Agencia Española de Protección de Datos. https://www.aepd.es
- **Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), París.** (2023). *Évaluation comparative des plateformes d'analyse automatique de logiciels malveillants*. Agence Nationale de la Sécurité des Systèmes d'Information.
- Any.Run. (s.f.). *Case study: Emotet detection in real-time sandbox*. https://any.run
- Aratecnia. (2022). *Desventajas de las soluciones de seguridad gratuitas*. https://aratecnia.es
- Campus Ciberseguridad. (s.f.). *Machine learning en detección de malware*. https://www.campusciberseguridad.com/blog/machine-learning-en-deteccion-de-malware/
- Caro Avià, P. (2022). *Análisis y ejecución de Malware y Códigos Maliciosos en un entorno controlado* [Trabajo de Fin de Grado, Universitat Politècnica de Catalunya]. https://upcommons.upc.edu/handle/2117/372262
- Autor desconocido. (s.f.). *El impacto del machine learning en la detección de amenazas*. Ciber-Seguridad Blog. https://www.ciber-seguridad.blog
- Clave Ciberseguridad. (s.f.). *Evaluaciones de Impacto: Requisitos y Normativas del GDPR*. https://claveciberseguridad.com
- CrowdStrike. (2022). *2022 Global Threat Report*. https://www.crowdstrike.com/es-es/resources/reports/global-threat-report-2022/
- Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA)*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023
- FireEye. (2020). *Advanced Threat Report*. Milpitas, CA. https://www.fireeye.com
- Hackplayers. (2022). *Dónde descargar muestras de malware actuales*. https://www.hackplayers.com
- Hybrid Analysis. (s.f.). *About us*. Recuperado de: https://www.hybrid-analysis.com

- Intezer. (2021). *Detecting Dridex through code reuse analysis*. https://analyze.intezer.com
- Intezer. (s.f.). *Analyze and classify malware*. https://analyze.intezer.com
- KeepCoding. (s.f.). Autor desconocido. *Glosario de herramientas de análisis de malware*. https://keepcoding.io
- Kaspersky Lab. (2021). *The evolution of cyberthreats: From Script Kiddies to State Actors*. https://securelist.com
- MetaDefender Cloud. (s.f.). *Threat detection and file sanitization*. OPSWAT. https://MetaDefender.opswat.com
- Mirabet Herranz, J. (2023). *Aplicación de técnicas de machine learning para la detección de malware en dispositivos Android* [Trabajo de Fin de Grado, Universitat Politècnica de València]. https://riunet.upv.es
- MITRE Corporation. (s.f.). *ATT&CK Framework*. Recuperado de: https://attack.mitre.org
- OPSWAT. (s.f.). *MetaDefender Cloud Landing page*. Recuperado de https://MetaDefender.opswat.com
- SANS Institute. (2023). *Malware Analysis Poster*. https://sans.org
- Symantec. (2017). *WannaCry: Ransomware attack analysis*. https://symantec-enterprise-blogs.security.com
- Symantec. (2020). *Internet Security Threat Report*. https://symantec-enterprise-blogs.security.com
- Tecnored. (s.f.). *Análisis de malware: Definición, técnicas e importancia en ciberseguridad*. https://tecnored.top
- Telefónica Tech. (2021). *Los servicios DFIR en una respuesta al incidente con ransomware*. https://telefonicatech.com/blog/servicios-dfir-respuesta-incidente-ransomware
- Universidad de Ciencias Aplicadas de Ámsterdam. (2022). *Comparative analysis of malware detection platforms*.
- VirusTotal. (s.f.). *Acerca de VirusTotal*. https://www.virustotal.com

- We Never Sleep. (s.f.). *Análisis de malware: Métodos y herramientas para la ciberseguridad*. https://weneversleep.es

Nota: Todas las fuentes citadas han sido consultadas entre mayo y julio de 2025. Se ha priorizado el uso de documentación técnica, informes oficiales, literatura académica y recursos especializados reconocidos en el ámbito de la ciberseguridad.