A. Lara-Gutierrez, J. A. Onievaand C. Fernandez-Gago, "HoneyV: Laboratorio Automatizado de Anlisis de Malware Basado en Honeypots", *XIX Reunin Espaola sobre Criptologa y Seguridad de la Informacin (RECSI 2026)*, 2026.
NICS Lab. Publications: https://www.nics.uma.es/publications

HoneyV: Laboratorio Automatizado de Análisis de Malware Basado en Honeypots

Antonio Lara-Gutierrez
NICS Lab
Universidad de Málaga
alara@uma.es

Jose A. Onieva
NICS Lab
Universidad de Málaga
onieva@uma.es

Carmen Fernandez-Gago
NICS Lab
Universidad de Málaga
mcgago@uma.es

***Resumen*—El análisis de malware requiere de entornos controlados capaces de capturar ataques reales y generar artefactos forenses. Sin embargo, muchos laboratorios y datasets existentes se limitan a la muestra o a trazas parciales, sin preservar el contexto de captura ni ofrecer pipelines reproducibles de análisis estático y dinámico. Este artículo introduce HoneyV, un laboratorio de análisis de malware basado en *honeypots* que integra en un único flujo automatizado la captura de muestras, su análisis híbrido y la generación de un conjunto de datos estructurados. La arquitectura propuesta combina un *honeypot* como nodo de captura, un módulo de orquestación que gestiona una cola de tareas y una máquina de análisis restaurable mediante *snapshots*, equipada con herramientas de análisis híbrido. Cada muestra procesada se transforma en un paquete que incluye *hashes*, resultados de herramientas de desempaquete y perfilado, trazas de procesos, cambios en el sistema, capturas de red, volcados de memoria y el contexto original de intrusión. A partir de esta infraestructura se ha construido un dataset de validación con muestras PE organizadas en ocho familias de malware, registradas con metadatos de captura y artefactos forenses asociados. HoneyV facilita así la replicación de experimentos, la evaluación de técnicas de detección y el entrenamiento de modelos de aprendizaje automático basados en comportamiento en un entorno seguro y reproducible, estando diseñado para maximizar la trazabilidad extremo a extremo mediante la vinculación de cada intrusión registrada con los artefactos generados en la máquina de análisis.**

***Index Terms*—*Honeypots*, análisis de malware, laboratorio de análisis, análisis estático, análisis dinámico, ciberseguridad.**

I. Introducción

El panorama actual de ciberamenazas se caracteriza por un volumen creciente de ataques, una reducción drástica de los tiempos de intrusión y el uso sistemático de técnicas avanzadas de ofuscación y evasión. Informes recientes señalan cientos de grupos activos atacando de forma continuada a organizaciones de todo el mundo, con tiempos de compromiso que se miden en minutos y un incremento notable de las intrusiones en entornos *cloud* y servicios expuestos en Internet [1]. Los datos de organismos como INCIBE muestran un crecimiento de incidentes, apoyados en familias de malware cada vez más diversas y en mecanismos de ofuscación que dificultan tanto su detección como su análisis [2].

Las técnicas clásicas de defensa, como antivirus basados en firmas, Sistemas de detección y prevención de intrusiones (IDS/IPS) perimetrales o soluciones de detección y respuesta (EDR), siguen siendo necesarios, pero resultan insuficientes frente a variantes polimórficas y metamórficas, técnicas *living off the land* (LOTL), que hacen un uso malicioso de binarios legítimos del propio sistema operativo para mimetizar el *malware* con procesos confiables, o campañas que combinan malware con abuso de identidad y credenciales robadas [3], [4]. En este contexto, disponer de evidencia de ataques reales, capturada en entornos controlados, pero verosímiles, es clave para validar reglas de detección, alimentar sistemas de correlación y entrenar modelos de aprendizaje automático capaces de generalizar frente a nuevas variantes.

Los *honeypots* y los laboratorios virtualizados ofrecen un caso de uso atractivo. Al simular servicios y activos de alto interés, permiten observar tácticas, técnicas y procedimientos (TTP) de los atacantes, registrar telemetría detallada y capturar binarios maliciosos sin comprometer sistemas de producción. Además, cuando se combinan con herramientas de análisis estático y dinámico, estos laboratorios pueden transformarse en creadores de datasets de *malware*, donde cada muestra se acompaña de contexto de captura, artefactos forenses y resúmenes estructurados listos para su explotación en investigación y entrenamiento de modelos [5], [6].

Sin embargo, muchos de los datasets de *malware* disponibles actualmente presentan limitaciones importantes, pues suelen centrarse en el archivo binario y su familia, pero carecen de información sobre el entorno de captura, los comandos ejecutados, las credenciales usadas o el tráfico generado; en otros casos, la infraestructura de laboratorio es ad hoc, poco documentada y difícil de reproducir, lo que limita la comparación de resultados entre trabajos.

En este artículo se presenta HoneyV, un laboratorio de análisis de *malware* basado en *honeypots* que integra captura, análisis híbrido y generación automatizada de informes y dataset. El sistema se compone de tres componentes: (i) un *honeypot* que centraliza múltiples servicios de baja y alta interacción y actúa como núcleo de captura de muestras y *logs*; (ii) una máquina de análisis, encargado de automatizar el análisis estático y dinámico y empaquetar todos los artefactos generados; y (iii) un orquestador que mantiene e invoca la generación de un nuevo reporte cada vez que recibe una muestra, mediante un sistema de colas. Se hace uso de una máquina atacante adicional para simular intrusiones y validar extremo a extremo el flujo de trabajo. A partir de esta infraestructura se ha construido un conjunto de aproximadamente 50 muestras de *malware*, organizadas en ocho familias, donde cada entrada incluye tanto los binarios como metadatos de captura, resúmenes estáticos y dinámicos, información de inteligencia de amenazas y los *logs* originales del *honeypot*.

Las contribuciones principales de este artículo son:

- El diseño y descripción de un laboratorio de análisis de *malware* PE (*Portable Executable*) basado en *honeypots* que integra de forma nativa la captura de intrusiones,

Tabla I
ANÁLISIS COMPARATIVO DE FUNCIONALIDADES ENTRE HONEYV Y TRABAJOS RELACIONADOS DEL ESTADO DEL ARTE.

Trabajo	Enfoque principal	Captura binarios	Logs del ataque	Análisis estático	Análisis dinámico	Dataset generado
Holbel et al. (2024) [7]	Honeypot virtualizado integrado con SIEM para observar TTP en tiempo real.	(P)	✓	✗	✗	✗
Maliga et al. (2024) [8]	Pipeline de limpieza y enriquecimiento de grandes repositorios de *malware* usando servicios externos.	✗	✗	✓	(P)	(P)
RIoTPot (ACSAC 2022) [9]	Honeypots híbridos IoT/OT desplegados globalmente para obtener tráfico y eventos a gran escala.	✗	✓	✗	✗	✓
Tambe et al. (2019) [10]	Honeypots IoT reales expuestos vía VPN; detección de comandos maliciosos y descargas de *malware*.	✓	✓	✗	(P)	✗
S. Mfogo et al. (2023) [11]	Honeypot interactivo basado en modelos de lenguaje y aprendizaje por refuerzo para adaptar respuestas.	✗	✓	✗	✗	(P)
Hornet Dataset (2021) [12]	Honeypots distribuidos geográficamente para estudiar variación de ataques según la localización.	✗	✓	✗	✗	✓
HoneyV	Laboratorio que integra captura, análisis híbrido automático y generación de dataset ampliado.	✓	✓	✓	✓	✓

el análisis híbrido y la generación de un dataset estructurado, proporcionando trazabilidad completa desde el evento de ataque hasta los artefactos forenses resultantes.
- La definición de un flujo de trabajo híbrido automatizado, capaz de capturar, analizar y empaquetar cada muestra junto con sus artefactos forenses y los *logs* de captura del *honeypot* en un reporte unificado, facilitando la explotación posterior de los datos.
- La publicación de un dataset de unas 50 muestras etiquetadas en ocho familias junto con resultados de captura obtenidos mediante la ejecución del laboratorio.

El resto del artículo se organiza de la siguiente forma: en la Sección II se revisan los trabajos relacionados en *honeypots*, laboratorios de análisis y datasets de *malware*; en la Sección III se describe la arquitectura del laboratorio propuesto; en la Sección IV se detalla el flujo de análisis y la automatización implementada; en la Sección V se presenta el conjunto de datos resultante; y, finalmente, en la Sección VI se discuten los principales casos de uso antes de cerrar con las conclusiones.

II. TRABAJOS RELACIONADOS

Los trabajos recientes sobre captura y análisis de *malware* se agrupan principalmente en tres líneas: (i) despliegue de entornos controlados para estudiar tácticas y procedimientos de atacantes; (ii) pipelines de procesado y limpieza de grandes repositorios de muestras; y (iii) generación de datasets.

Holbel et al. [7] proponen un *honeypot* orientado a la observación de TTPs en redes universitarias, integrado con un SIEM para la correlación y visualización de eventos en tiempo real. Aunque capturan actividad maliciosa y describen ataques efectivos, su sistema no incorpora un pipeline automatizado de análisis estático y dinámico de los binarios obtenidos ni genera un dataset estructurado reutilizable por terceros. HoneyV, por su parte, automatiza la detección de muestras, su análisis híbrido y la organización de los artefactos resultantes.

Maliga et al. [8] presentan un pipeline para limpiar y procesar grandes conjuntos de muestras obtenidas de *feeds* u *honeypots*, utilizando servicios como VirusTotal para validar y enriquecer los binarios analizados. Sin embargo, su contribución se limita al postprocesado de colecciones existentes: no capturan muestras ni proporcionan *logs* del ataque o análisis dinámico controlado. Nuestra propuesta complementa este enfoque generando un dataset desde su origen, con telemetría de la intrusión, comandos utilizados y artefactos extraídos durante la ejecución de cada muestra.

Por su parte, RIoTPot [9] amplía el estudio de *honeypots* híbridos desplegados en entornos IoT/OT, analizando durante tres meses el impacto de la interacción, ubicación y protocolos sobre la diversidad de ataques capturados. Aunque publica un dataset con millones de eventos de red, este no incluye binarios maliciosos ni resultados de análisis estáticos o dinámicos. HoneyV se diferencia al centrarse en la captura de ejecutables maliciosos para Windows y proporcionar un pipeline reproducible de análisis híbrido.

El trabajo de Tambe et al. [10] emplea dispositivos IoT reales expuestos mediante túneles VPN para crear *honeypots* escalables, proponiendo mecanismos de *backtracking* para identificar comandos que originan conexiones maliciosas. Aunque su enfoque permite descubrir ataques de gran escala, está optimizado para IoT y no produce un flujo de análisis completo ni un dataset con artefactos forenses.

AIIPot [11] introduce *honeypots* basados en modelos de lenguaje y aprendizaje por refuerzo para prolongar la interacción con el atacante y capturar más información contextual. Su aportación se centra en la interacción inteligente, pero no aborda la captura, ejecución ni análisis detallado de binarios.

El dataset Hornet [12] se basa en *honeypots* geográficamente distribuidos y proporciona grandes volúmenes de tráfico de red, permitiendo analizar diferencias en la distribución de ataques por ubicación. Sin embargo, está limitado a flujo de red y carece de muestras ejecutables o análisis asociado.

La Tabla I muestra de forma comparativa las principales características de los trabajos revisados. Se analizan cinco dimensiones clave y se evalúa cada trabajo según dichas capacidades. Estos trabajos previos muestran aproximaciones parciales al problema, centradas bien en la captura de muestras, bien en su análisis o en la recolección de artefactos. Esta propuesta define un laboratorio unificado que integra de manera reproducible la captura, el análisis híbrido y la generación estructurada de un dataset con trazabilidad completa desde el evento de intrusión hasta los artefactos resultantes, superando así las limitaciones de las soluciones previas basadas en configuraciones ad hoc.

Asimismo, HoneyV automatiza todo el flujo de procesamiento y preserva explícitamente el vínculo entre cada ataque y los IOC asociados, lo que permite un nivel de correlación

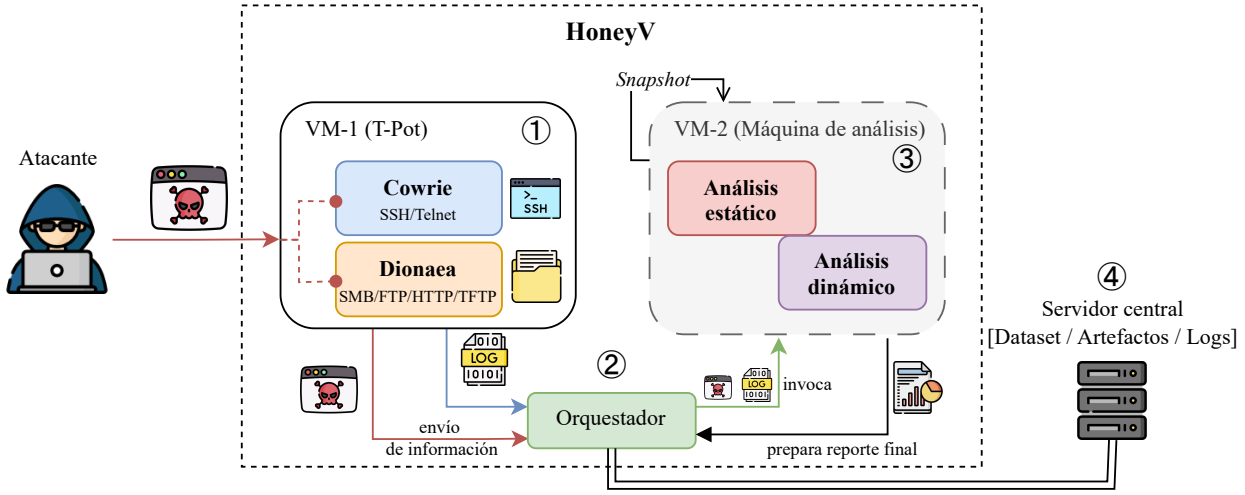

Figura 1. Diseño de la arquitectura de captura, orquestación y análisis de HoneyV

y explotabilidad de resultados. A diferencia de soluciones de análisis puras como Cuckoo Sandbox o Joe Sandbox, que se centran exclusivamente en la detonación de binarios, HoneyV integra la fase de captura como un componente nativo. Esto permite preservar la trazabilidad completa del incidente, vinculando los metadatos de red del ataque original con los artefactos forenses generados durante el análisis, algo que las sandboxes aisladas no proporcionan por defecto.

III. Arquitectura del laboratorio de análisis

La arquitectura propuesta combina un entorno de captura mediante *honeypots* [13], un módulo central de orquestación y una máquina de análisis. El diseño final se resume en la Fig. 1. Este esquema organiza el flujo completo de tratamiento de muestras maliciosas en tres etapas diferenciadas: captura, orquestación y análisis. Cada componente desempeña un papel dentro del pipeline y está diseñado para maximizar la reproducibilidad, el aislamiento y la disponibilidad de artefactos procesables para el posterior análisis.

La primera etapa (1) corresponde al entorno de captura, basado en T-Pot[1]. La elección de T-Pot frente a otras alternativas se fundamenta en su madurez, estabilidad y carácter modular. Según Ilg et al. [14], T-Pot se sitúa entre las plataformas abiertas más completas para despliegues de captación de *malware*, al combinar hasta 23 servicios de baja y media interacción con un ecosistema de visualización, registro y automatización difícil de replicar en soluciones aisladas. Su arquitectura basada en contenedores y su facilidad de despliegue lo convierten en una opción adecuada para laboratorios del calibre tratado en este artículo.

Según lo presentado anteriormente, T-Pot integra múltiples *honeypots*, aunque en nuestro sistema se emplean principalmente dos: *Cowrie* y *Dionaea*. *Cowrie* emula servicios SSH y Telnet de media interacción, lo que permite registrar comandos, credenciales y descargas de ficheros. *Dionaea*, por su parte, implementa servicios susceptibles de explotación como SMB, FTP, HTTP o TFTP, y está específicamente orientado a la captura de *payloads* y ejecutables propagados mediante explotación remota. Ambos *honeypots* constituyen las principales fuentes de muestras, ya que almacenan automáticamente los artefactos recibidos y los *logs* necesarios para contextualizar cada intento de intrusión.

La segunda etapa (2) está formada por el módulo de orquestación, encargado de gestionar el flujo de análisis. Este componente monitoriza los directorios de captura y, al detectar un nuevo binario, le asigna un identificador único que lo vincula permanentemente con los logs de su sesión de ataque. A continuación, encola la tarea y activa la máquina de análisis. El orquestador también coordina el intercambio de artefactos, recopila los resultados y los envía al servidor central, donde se almacenan de forma estructurada. Este mecanismo permite desacoplar la fase de captura de la de análisis y garantiza la trazabilidad y el procesamiento de múltiples muestras sin intervención manual.

La tercera etapa (3) corresponde a la máquina de análisis, desplegada en un entorno virtualizado con arranque limpio en cada ejecución. El uso de instantáneas de la máquina virtual de análisis garantiza que cada muestra se evalúa en condiciones controladas e idénticas, evitando contaminación entre ejecuciones y permitiendo repetir el análisis cuando sea necesario, garantizando reproducibilidad. Esta máquina ejecuta un análisis híbrido compuesto por un módulo estático, encargado de extraer cadenas, metadatos, heurísticas de empaquetado e información estructural del binario capturado; y un módulo dinámico, responsable de monitorizar procesos, cambios en el sistema de ficheros y en el registro, así como el tráfico de red generado durante la ejecución controlada del *malware*. Los artefactos obtenidos y un reporte que resume el análisis realizado son enviados al orquestador, que se encarga de alojarlos en un servidor central externo (4).

El módulo de análisis actual de HoneyV está diseñado específicamente para la instrumentación y ejecución de binarios en formato PE para sistemas Windows, dado que este sistema operativo sigue siendo el objetivo predominante en campañas de malware corporativo. No obstante, la arquitectura modular del orquestador permite la futura incorporación de *sandboxes* para entornos Linux o macOS.

[1]Disponible en https://github.com/telekom-security/tpotce

Un aspecto clave es que el módulo de orquestación asigna a cada muestra un identificador único que se propaga a lo largo de todo el pipeline. Este se utiliza para enlazar los ficheros originales procedentes de T-Pot, los artefactos generados en la máquina de análisis y el reporte JSON final almacenado en el servidor central. De este modo, HoneyV ofrece una trazabilidad de cada muestra y sus efectos, difícil de obtener con configuraciones ad hoc de los sistemas implementados.

IV. Flujo de análisis y automatización

El proceso de análisis se basa en un pipeline automatizado que se ejecuta cada vez que una nueva muestra es capturada por el *honeypot*, según el método descrito previamente. El objetivo principal es transformar el binario recibido en un conjunto estructurado de artefactos estáticos y dinámicos, manteniendo en todo momento la reproducibilidad del análisis mediante la ejecución en una máquina virtual aislada restaurada desde una instantánea base. Dicha máquina virtual ejecuta una versión de Windows que ha sido modificada con distintas medidas para evitar la detección de amenazas, permitir ejecutar cualquier tipo de muestra, y mantener el aislamiento completo de esta.

Las herramientas utilizadas se detallan en la Tabla II, soportando un flujo de trabajo automatizado coordinado por el orquestador. El ciclo comienza con la detección y selección del ejecutable más reciente junto a los artefactos previos del *honeypot*. Estos registros (tales como *logs* de conexión o comandos ejecutados por el atacante) se vinculan a la muestra mediante un identificador único para preservar el contexto de la intrusión. Acto seguido, el orquestador introduce la tarea en una cola de procesamiento y, llegado su turno, activa la máquina de análisis desde un estado limpio para asegurar la reproducibilidad. Una vez iniciado el entorno, se procede al análisis estático para la obtención de huellas criptográficas, extracción de cadenas y perfilado de metadatos o *packers*. Posteriormente, se activa el análisis dinámico mediante la configuración de monitores de sistema y red, permitiendo la ejecución controlada de la muestra para recolectar evidencias como trazas, capturas de tráfico y volcados de memoria. Finalmente, el ciclo concluye con la consolidación de todos los resultados estáticos y dinámicos en un reporte estructurado JSON y el empaquetado comprimido de los artefactos para su almacenamiento definitivo y cierre del flujo.

V. Dataset generado

Para validar la propuesta, se requiere un conjunto de binarios maliciosos representativos de distintas familias de *malware*. Se ha recurrido a fuentes abiertas y reconocidas, en particular *MalwareBazaar* y *TheZoo*, que facilitan la descarga de muestras para investigación. A partir de dichas bases se han seleccionado en torno a 50 muestras de *malware* PE, cubriendo ocho familias. Estas muestras se han elegido según:

- la diversidad de comportamiento (campañas de spam, infecciones silenciosas, auto–propagación, etc.);
- la disponibilidad de metadatos básicos (nombre, *hashes*, fecha de detección);
- la pertinencia para ejecutar ataques simulados contra *honeypots* y así registrar IOC de forma realista.

Este conjunto de datos sirve como validación funcional de la arquitectura propuesta y como punto de partida para recolecciones a mayor escala. La Tabla III muestra una panorámica de la distribución de muestras por familia y una breve descripción del comportamiento observado.

Tabla III
Distribución de muestras por familia.

Familia	#	Descripción
Adware	10	Publicidad intrusiva, inyección en navegadores y redirección de tráfico.
Botnets	5	Escaneos automatizados, propagación y DDoS.
Gusanos	5	Auto-propagación vía SMB, FTP o TFTP; descarga de *payloads* adicionales.
Keyloggers	5	Robo de credenciales y exfiltración por HTTP/SMTP.
Rootkits	5	Ocultación de procesos y persistencia mediante manipulación del sistema.
Spyware	9	Monitorización del sistema y envío de información a servidores de C2.
Troyanos	7	Acceso remoto, control completo del sistema.
Virus (otros)	7	Infección de ejecutables, polimorfismo y cifrado para evasión.

V-A. Proceso de preparación y organización

El flujo de preparación del dataset ha sido el siguiente:

1. **Descarga y verificación:** se descargan las muestras desde *MalwareBazaar* y *TheZoo*, verificando su integridad.
2. **Estructuración del repositorio:** se crea un árbol de directorios con una carpeta por familia. En cada una se almacenan las muestras junto con un fichero con metadatos y su enlace a VirusTotal.
3. **Pruebas controladas:** para la validación experimental se optó por una metodología de inyección controlada en lugar de esperar ataques orgánicos aleatorios. Esto permite verificar la precisión del sistema utilizando familias de malware conocidas, asegurando que el flujo de análisis identificaba correctamente las características esperadas de cada familia, eliminando la incertidumbre inherente a los ataques 'in-the-wild' para esta fase de evaluación. De este modo, las muestras quedan almacenadas en las rutas de captura habituales del *honeypot* y

Tabla II
Resumen de herramientas: función de detección y aplicación en la implementación del laboratorio.

Herramienta	Función y uso en la implementación
FLOSS	Extracción heurística de cadenas (incluso ofuscadas) para identificar IOC estáticos como dominios o rutas sin ejecutar la muestra.
Detect It Easy	Perfilado del binario mediante la detección de firmas de *packers* y compiladores para determinar si requiere desempaquete previo.
Ghidra	Herramienta de ingeniería inversa para el análisis manual profundo de funciones y flujos de control en casos complejos.
Process Monitor	Monitorización de la creación de procesos, modificaciones del registro y cambios en el sistema de ficheros durante la ejecución.
FakeNet-NG	Simulación de servicios de red para interceptar peticiones, permitiendo analizar el comportamiento sin salida real a Internet.
Wireshark	Captura y análisis de paquetes de red para examinar protocolos y patrones de comunicación generados durante el análisis dinámico.
ProcDump	Generación de volcados de memoria de procesos maliciosos para capturar *payloads* desencriptados o desempaquetados en RAM.
Volatility	Análisis forense de los volcados de memoria para identificar inyecciones de código y artefactos no visibles en el disco.

se comprueba que la infraestructura detecta, registra y almacena la interacción asociada.

4. **Actualización del dataset:** los reportes generados se incorporan al repositorio, aumentando la inteligencia de amenazas del sistema que lo incorpora.

El dataset final se encuentra publicado en un repositorio[2] estructurado por familias y acompañado de los reportes generados por el pipeline de análisis.

V-B. Aporte relativo del análisis estático y dinámico

Con el objetivo de cuantificar la contribución de cada técnica al conjunto final de información disponible, se ha realizado un análisis comparativo de los artefactos generados por el módulo estático y el módulo dinámico sobre el conjunto completo de muestras del dataset. Para cada reporte se extrajeron los IOC registrados, considerando las siguientes categorías:

- dominios y direcciones IP de contactos de red;
- URL y rutas de descarga;
- claves y valores de registro modificados;
- ficheros creados o modificados (*dropped files*).

A partir de estos elementos se generó, para todo el conjunto de muestras, una caracterización cuantitativa de los IOC detectados por cada técnica. Para cada categoría se contabilizaron los indicadores obtenidos exclusivamente mediante análisis estático, exclusivamente mediante análisis dinámico y aquellos identificados por ambas técnicas de forma simultánea, incorporando además el porcentaje relativo que cada grupo representa dentro de su fila correspondiente. La Tabla IV sintetiza estos resultados, mientras que la Fig. 2 muestra un desglose de los valores recogidos en la tabla pero agrupados, con el fin de poder observar la distribución de cada IOC.

Independientemente de la distribución concreta de estos valores, esta comparativa cuantitativa permite caracterizar qué tipos de información se benefician más de cada técnica y hasta que punto ambas son complementarias a la hora de correlacionar los reportes generados por el laboratorio.

V-C. Caracterización del pipeline por tipología de malware

Con el objetivo de evaluar el comportamiento operativo del laboratorio más allá de la extracción de artefactos, se realizó una caracterización cuantitativa de este considerando las distintas familias de *malware* recogidas en la Tabla III. Este análisis permite estudiar de forma conjunta aspectos relacionados con la evasión, la sensibilidad del análisis, la validez de los reportes generados, así como el rendimiento y escalabilidad del sistema bajo condiciones homogéneas.

Para ello, las muestras del dataset se agruparon según su familia, y cada experimento se repitió cinco veces empleando

[2]Disponible en https://github.com/antoniol00/HoneyV-malware-dataset

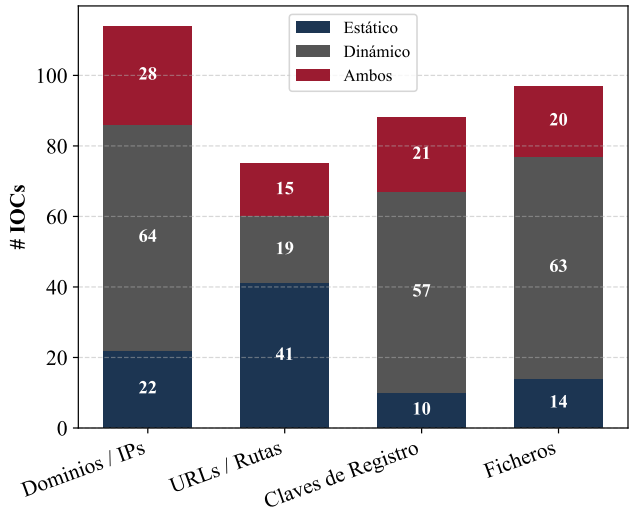

Figura 2. Distribución de IOC detectados por categoría de artefacto y método de análisis (estático, dinámico y combinado)

idéntica configuración y conjunto de entradas. Los valores reportados corresponden a la media de dichas iteraciones. Las métricas consideradas incluyen: (i) tasa de activación de las muestras, utilizada como aproximación indirecta a la resistencia frente a técnicas de evasión; (ii) validez estructural de los reportes JSON generados mediante un validador de sintaxis; (iii) porcentaje de indicadores de compromiso verificados manualmente sobre una submuestra; (iv) volumen medio de eventos dinámicos observados; y (v) métricas de rendimiento y escalabilidad, incluyendo tiempo total de análisis, *throughput* y consumo medio de recursos de CPU y RAM.

La Tabla V resume los resultados obtenidos, revelando patrones de comportamiento distintivos para cada familia. El análisis de estos datos permite extraer interpretaciones operativas de las distintas familias.

Los *rootkits* destacan como la familia más compleja de analizar. Presentan la tasa de activación más baja y el menor número de eventos dinámicos, indicando un uso efectivo de técnicas *anti-sandbox*. Paradójicamente, son los que más recursos consumen y los que requieren mayor tiempo de análisis, consecuencia de la ejecución de bucles de espera activa y escaneos del entorno que agotan el *timeout* de la sesión sin llegar a detonar la carga útil. En el extremo opuesto, las *botnets* mostraron una alta tasa de activación (82,4 %) y generaron el mayor volumen de eventos dinámicos. Este comportamiento "ruidoso" es consistente con su naturaleza: intentos agresivos de conexión a servidores de Comando y Control (C2), escaneos de red y modificaciones rápidas para persistencia. Familias como los gusanos o *adware* alcanzaron

Tabla IV
RESUMEN CUANTITATIVO DE IOC DETECTADOS POR ANÁLISIS ESTÁTICO Y DINÁMICO.

Tipo de IOC	Exclusivo estático	Exclusivo dinámico	Detectado por ambos	Total estático	Total dinámico	Total únicos	Total global
Dominios / IP	22 (15,49 %)	64 (45,07 %)	28 (19,72 %)	50 (35,21 %)	92 (64,79 %)	114 (80,28 %)	142 (100 %)
URL / rutas de descarga	41 (45,56 %)	19 (21,11 %)	15 (16,67 %)	56 (62,22 %)	34 (37,78 %)	75 (83,33 %)	90 (100 %)
Claves / valores de registro	10 (9,17 %)	57 (52,29 %)	21 (19,27 %)	31 (28,44 %)	78 (71,56 %)	88 (80,73 %)	109 (100 %)
Ficheros creados / modificados	14 (11,97 %)	63 (53,85 %)	20 (17,09 %)	34 (29,06 %)	83 (70,94 %)	97 (82,91 %)	117 (100 %)

Tabla V
EVALUACIÓN DEL RENDIMIENTO OPERATIVO DEL LABORATORIO: MÉTRICAS DESGLOSADAS POR FAMILIA DE *malware* (MEDIA DE 5 ITERACIONES).

Familia	**#**	**Activación (%)**	**JSON válido (%)**	**IOC válidos (%)**	**Eventos dinámicos (μ)**	**Tiempo total (s)**	**Throughput (muestras/h)**	**CPU (%)**	**RAM (MB)**
Adware	10	88,0	100,0	94,2	46,8	310,4	11,6	41,5	1820
Botnets	5	82,4	100,0	92,1	74,6	358,7	10,0	52,3	2190
Gusanos	5	100,0	100,0	96,5	61,9	295,6	12,2	45,8	1910
Keyloggers	5	73,6	100,0	87,4	33,7	332,8	10,8	38,9	1765
Rootkits	5	41,2	100,0	70,8	17,9	412,5	8,2	59,1	2970
Spyware	9	77,9	100,0	90,3	43,6	327,1	11,0	44,2	1885
Troyanos	7	84,6	100,0	93,8	68,2	341,9	10,5	48,7	2030
Virus (otros)	7	69,8	100,0	85,9	38,6	361,3	9,9	46,5	1975

una tasa de activación del 100 % con tiempos de análisis reducidos (295,6 s). Al estar diseñados para la auto-propagación rápida carecen de mecanismos de evasión sofisticados.

VI. DISCUSIÓN Y CONCLUSIONES

La arquitectura presentada en este artículo, HoneyV, aborda una carencia fundamental en la investigación actual de *malware*: la falta de contexto unificado. Mientras que los repositorios tradicionales y muchos trabajos relacionados se limitan a proporcionar binarios aislados o telemetría parcial de red, la solución desarrollada en este artículo integra el ciclo completo de captura, análisis y generación de artefactos en un flujo coherente y automatizado.

Los resultados experimentales validan la necesidad de combinar técnicas estáticas y dinámicas para obtener una visión completa del incidente. El análisis cuantitativo reveló una clara especialización de cada técnica. Por un lado, el análisis estático demostró ser superior para iluminar la infraestructura latente del atacante. Esto sugiere que muchas muestras contienen listas de recursos que nunca llegan a contactarse durante la ejecución en el *sandbox* debido a tiempos de espera o la caída de los servidores de comando y control. Por otro lado, el análisis dinámico permite revelar el impacto real en el *host*, superando ampliamente a la detección estática en la identificación de claves de registro y ficheros creados.

No obstante, es necesario discutir las limitaciones del diseño. Al basar la captura en *honeypots* de interacción media, la arquitectura podría no capturar ataques que requieran la explotación de vulnerabilidades específicas del kernel o interacciones complejas con aplicaciones web dinámicas que superen la lógica emulada, restricción que se puede abordar en desarrollos futuros ampliando la capacidad de emulación hacia la alta interacción. A pesar de ello, la capacidad de HoneyV para vincular el ataque original con los artefactos forenses generados aporta un nivel de trazabilidad difícil de obtener con configuraciones *ad hoc*.

HoneyV demuestra, por tanto, que es viable construir infraestructuras de análisis modulares, escalables y reproducibles utilizando herramientas abiertas. Como líneas futuras de investigación, se propone la evolución del módulo dinámico mediante técnicas de introspección desde el hipervisor (VMI), tales como la detección de vistas cruzadas (*cross-view*) o el *hooking* transparente basado en *Extended Page Tables* (EPT), para mejorar la detección de familias evasivas. Asimismo, se plantea la integración de LLM alimentados con los reportes estructurados para habilitar sistemas de razonamiento automatizado que agilicen el triaje de incidentes. De forma complementaria, se contempla el desarrollo de *honeypots* asistidos por IA para la emulación de dispositivos NAS, generando estructuras de ficheros dinámicas para optimizar la captura de muestras orientadas al secuestro de datos

AGRADECIMIENTOS

Esta publicación forma parte del proyecto "CiberIA: Investigación e Innovación para la Integración de Ciberseguridad e Inteligencia Artificial" (Proyecto C079/23), financiado por la "Unión Europea NextGeneration-EU, Plan de Recuperación, Transformación y Resiliencia", a través de INCIBE. Asimismo, ha sido parcialmente apoyada por el proyecto SecAI (PID2022-139268OB-I00), financiado por el Ministerio de Ciencia e Innovación y la Agencia Estatal de Investigación.

REFERENCIAS

[1] CrowdStrike: "Resumen ejecutivo del informe global de amenazas 2025", en *CrowdStrike Global Threat Report*, 2025. Disponible en: https://www.crowdstrike.com/es-es/global-threat-report
[2] INCIBE: "Infografía del balance de ciberseguridad 2023", Instituto Nacional de Ciberseguridad, 2024.
[3] Ö. A. Aslan and R. Samet: "A comprehensive review on malware detection approaches", en *IEEE Access*, vol. 8, pp. 6249–6271, 2020.
[4] L. Liu, B. S. Wang, B. Yu and Q. X. Zhong: "Automatic malware classification and new malware detection using machine learning", en *Frontiers of IT & Electronic Engineering*, vol. 18, n. 9, pp. 1336–1347, 2017.
[5] L. Spitzner: "Honeypots: Tracking Hackers", en *Addison-Wesley*, 2002.
[6] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil and J. Schönfelder: "A survey on honeypot software and data analysis", en *arXiv:1608.06249*, 2016.
[7] M. Holbel, C. Wright, A. Salamah and C. Collins: "Analysis of Active TTPs Against a Portable Virtualized Honeypot", en *Issues in Information Systems*, vol. 25, n. 1, pp. 265–278, 2024.
[8] M. Maliga, G. Náday and L. Buttyán: "A pipeline for cleaning and processing large datasets of potentially malicious binaries", en *MASCOT 2024*, 2024.
[9] S. Srinivasa, J. M. Pedersen and E. Vasilomanolakis: "Interaction matters: a comprehensive analysis and a dataset of hybrid IoT/OT honeypots", en *ACSAC 2022*, pp. 57–68, 2022.
[10] A. Tambe et al.: "Detection of Threats to IoT Devices using Scalable VPN-forwarded Honeypots", en *CODASPY 2019*, ACM, pp. 12–25, 2019.
[11] S. Mfogo et al.: "AIIPot: Adaptive Intelligent-Interaction Honeypot for IoT Devices", en *arXiv:2303.12367*, 2023.
[12] V. Valeros: "Hornet 40: Network Dataset of Geographically Placed Honeypots", en *Mendeley Data*, v3, 2021. DOI: 10.17632/tcfzkbpw46.3
[13] I. Mokube and M. Adams: "Honeypots: concepts, approaches, and challenges", en *Proc. 45th ACM Southeast Conference*, pp. 321–326, 2007.
[14] N. Ilg, P. Duplys, D. Sisejkovic and M. Menth: "A survey of contemporary open-source honeypots, frameworks, and tools", en *Journal of Network and Computer Applications*, vol. 220, art. 103737, 2023.
[15] M. Souppaya and K. Scarfone: "Guide to Malware Incident Prevention and Handling", en *NIST SP 800-83 Rev.1*, 2013.
[16] A. Nelson, S. Rekhi, M. Souppaya and K. Scarfone: "Incident Response Recommendations for Cybersecurity Risk Management", en *NIST SP 800-61r3*, 2025.
[17] K. Kent, S. Chevalier, T. Grance and H. Dang: "Guide to integrating forensic techniques into incident response", en *NIST SP 800-86*, 2006.