

Forum:[Hack Forums](#)

Thread: [\[MRT-X Analysis\] Analyzing a File with Hybrid Analysis](#)

Tha Sneak - March 19, 2025, 5:08 am

? How to Analyze a File with Hybrid Analysis & Detect Malicious Characteristics ?

? What is Hybrid Analysis?

[Hybrid Analysis](#) is a cloud-based malware sandbox that allows you to upload and analyze suspicious files. It provides static & dynamic analysis, behavioral reports, YARA rule matching, and signature-based detection.

? Why Use Hybrid Analysis?

- ? Safe environment for running malware.
- ? Detects persistence mechanisms, API calls, and network traffic.
- ? Matches against known malware signatures.
- ? Identifies malicious file modifications and registry changes.

? Step 1: Preparing Your File for Analysis

Before uploading a suspicious file, consider these precautions:

- ? If analyzing malware, use a VM to avoid infecting your system.
- ? Compress the file in a password-protected ZIP (e.g., password: "infected") to prevent accidental execution.
- ? Ensure no sensitive data is included in the sample.
- ? Note: Hybrid Analysis shares results publicly, so avoid uploading confidential information.

? Step 2: Uploading a File to Hybrid Analysis

- 1 Go to [Hybrid Analysis](#).
- 2 Click "Submit a Sample".
- 3 Select the file (.exe, .dll, .doc, .pdf, .zip, .js, etc.) you want to analyze.
- 4 Choose an Analysis System (Windows 10, Windows 7, or Linux).
- 5 Select an Execution Mode:
 - Full Analysis: Runs the file in a sandbox.
 - Static Analysis: Scans without execution.
- 6 Click "Submit" and wait for the report to generate.

? Tip: You can also enter a URL or hash (MD5, SHA-256) to check if the file was previously

analyzed.

? Step 3: Interpreting the Hybrid Analysis Report

Once the scan is complete, review the malware report by checking these key sections:

? Threat Score: Hybrid Analysis assigns a score from 0-100. A high score indicates strong malicious behavior.

? File Information: Displays hashes (MD5, SHA-256), file size, and format.

? File Structure: Lists embedded resources, PE headers, and suspicious sections.

? Process Activity: Shows processes created during execution.

? Registry Modifications: Displays new registry entries, persistence mechanisms, and system changes.

? Network Activity: Captures IP connections, DNS queries, and outbound requests.

? YARA Rule Matches: Identifies patterns matching known malware families.

? Tip: A score above 70 usually means the file exhibits high-risk behavior.

? Step 4: Detecting Malicious Characteristics

Look for suspicious indicators in the report:

? Common Red Flags:

? Code Injection: If the file injects code into explorer.exe, svchost.exe, or winlogon.exe, it may be a trojan or RAT.

? Process Spawning: If it launches cmd.exe, powershell.exe, or wscript.exe, it may execute system commands.

? File Drops: If it writes a file in C:\Users\Public, C:\Windows\Temp, or AppData\Roaming, it may be setting up persistence.

? Persistence Mechanisms: If it modifies HKLM\Software\Microsoft\Windows\CurrentVersion\Run, it can execute on startup.

? Network Communication: If it connects to suspicious IPs, C2 servers, or Tor nodes, it may be a backdoor.

? Obfuscation Techniques: If it loads packed/unpacked DLLs, encrypts code, or modifies memory, it may be hiding activity.

? Tip: Use the "Indicators of Compromise (IOCs)" section to identify malicious behavior.

? Step 5: Extracting & Investigating IoCs

IoCs (Indicators of Compromise) help identify malware behavior.

? Extract Hashes:

Copy MD5, SHA-256 hashes from the report and check on:

- [VirusTotal](#)
- [Malpedia](#)

? Check Suspicious Domains & IPs:

Use:

- [AbuseIPDB](#)
- [URLVoid](#)

? Analyze Process Behavior:

Review parent-child process relationships for unusual execution patterns.

? Check for Code Injection:

If the file modifies memory of another process, it may be attempting to hide execution.

? Tip: Hybrid Analysis often provides a full network dump—download and analyze with Wireshark.

? Step 6: Next Steps & Remediation

If the file is confirmed as malware, take these steps:

? For Personal Use:

- ? Delete the file and remove it from quarantine.
- ? Run a full system scan using [Malwarebytes](#) or [Microsoft Safety Scanner](#).
- ? Check Windows startup entries and remove unknown entries.
- ? Change passwords if malware captured credentials.

? For Enterprise Use:

- ? Isolate infected systems and investigate logs.
- ? Block C2 IP addresses and malicious domains in firewall rules.
- ? Check endpoint logs for lateral movement.
- ? Deploy YARA rules to detect similar threats in your network.

? Tip: Report new malware samples to security communities like [MISP](#) and [Hybrid Analysis](#) to improve global detection.

? Conclusion

Hybrid Analysis is a powerful tool for detecting and investigating malware. By following this guide, you can:

- ? Identify malware behaviors and suspicious activities.
- ? Extract hashes, IPs, and IoCs for further investigation.
- ? Determine persistence mechanisms and process injection techniques.
- ? Take action to mitigate and remove malware threats.

? Stay Safe & Keep Learning! ?