**Static Malware Analysis using Hybrid Analysis**

**What is Static Malware Analysis?**

Static Malware Analysis, often called code analysis, involves examining a malware file's binary code without executing it. This method helps understand the malware's structure and purpose by uncovering key details like file names, checksums (e.g., MD5 hashes), file types, and sizes. By inspecting the code, analysts can gather valuable technical information, such as the malware's functionality, network signatures, exploit packaging methods, and dependencies.

Key techniques in static analysis include:

File fingerprinting: Identifying unique attributes of a file.

Local and online malware scanning: Using tools like Hybrid Analysis to detect malicious signatures.

Strings search: Extracting readable text to identify clues within the malware.

Identifying packing and obfuscation methods: Detecting techniques used to hide or compress malware code.

Finding portable executable (PE) information: Analyzing metadata in Windows PE files.

Identifying file dependencies: Revealing external libraries or modules the malware relies on.

Malware disassembly: Breaking down the binary code to study the instructions it executes.

These techniques help cybersecurity professionals identify and understand the malicious behaviors embedded in a program before it runs.

**Walkthrough**

This guide shows you how to check for malware using Hybrid Analysis, a free online tool to examine suspicious files and web addresses. We'll walk you through uploading a virus file and making sense of what the scan tells you.

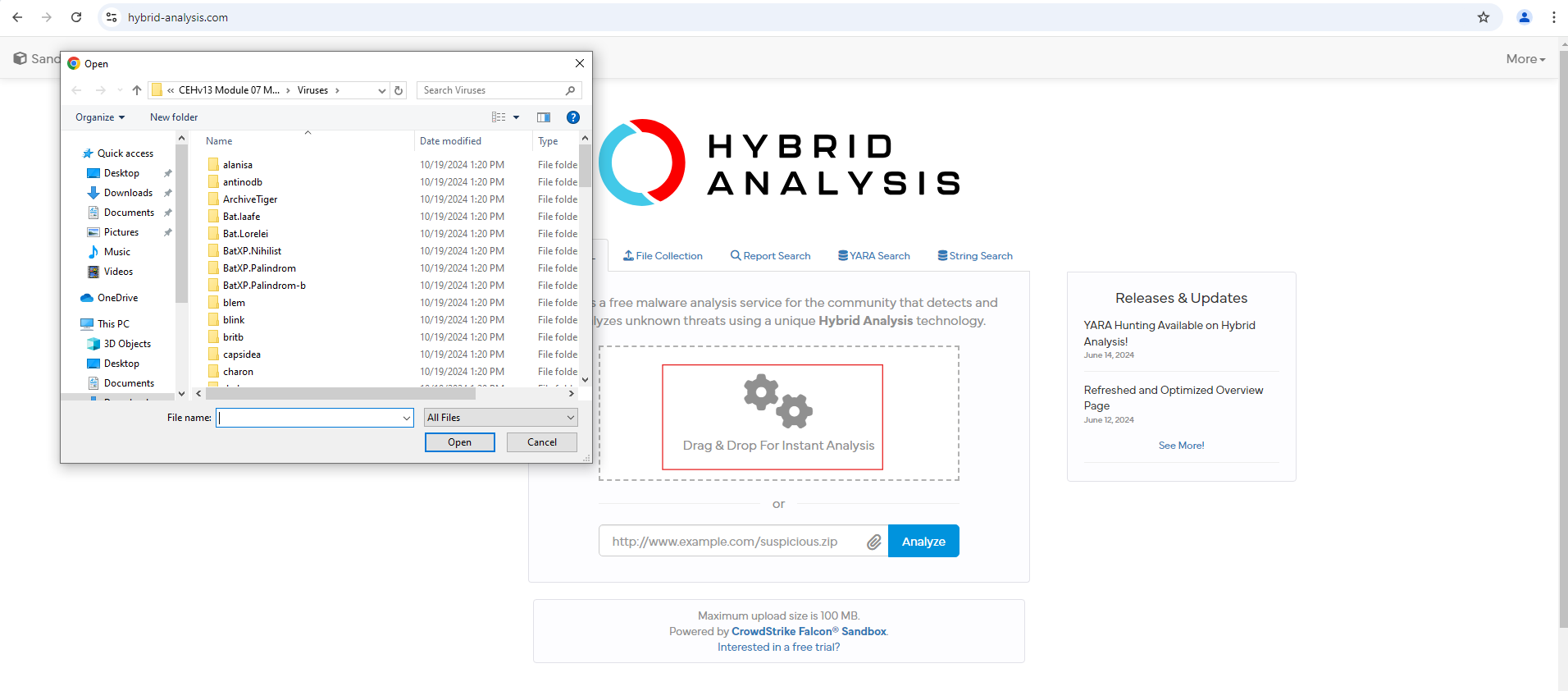
Step 1: Open the Hybrid-analysis site - **https://www.hybrid-analysis.com**

A screenshot of a computer

Description automatically generated

Step 2: Upload the Suspicious File

1. On the HYBRID ANALYSIS main page, locate the **Drag & Drop For Instant Analysis** section.
2. Click this section, and an Open file window will appear.



Step 3: Select the Virus File

1. In the Open window, navigate to the folder where your virus file is located.
2. In this walkthrough I have selected the file named tini.exe and click Open.

A screenshot of a computer

Description automatically generated

Step 4: File Upload

1. After selecting the file, the Getting Things Ready page will load, indicating that the file is being uploaded. Wait until the progress bar reaches 100%, signifying that the upload is complete.
2. Check the following boxes:
   1. I agree to the Hybrid Analysis Terms & Conditions and have read the Privacy Notice.
   2. I'm not a robot.
3. Click Continue.

A screenshot of a computer

Description automatically generated

Step 5: Choose Analysis Environment

1. The Analysis Environments page will appear. Select the Windows 11 64-bit radio button.

2. Click Generate Public Report.

A screenshot of a computer

Description automatically generated

Step 6: Viewing the Analysis Results

1. Once completed, the Analysis Overview page will be displayed.
2. On the Analysis Overview page, note the following details:
   1. The Threat Score (in this case, 100, which indicates a highly malicious file).
   2. Additional information like the SHA hash value of the file.

A screenshot of a computer

Description automatically generated

Step 7: Anti-Virus Results

1. Scroll down to the Anti-Virus Results section.
2. This section shows the results from various online anti-virus engines, such as CrowdStrike Falcon and MetaDefender.

A white background with red and blue text

Description automatically generated

Step 8: View Detailed Results for MetaDefender

1. To explore the results further, click the More Details icon next to the MetaDefender entry.

A white background with red and blue lines

Description automatically generated

1. A pop-up will appear showing the detailed results for MetaDefender’s scan. Once reviewed, close the pop-up window.

A screenshot of a computer

Description automatically generated

Step 9: Falcon Reports and Incident Response Information

1. Continue scrolling down the Analysis Overview page to review other information, such as:
   1. Reports from Falcon which provides insights into malware behavior, including file system changes and network activity.

A screenshot of a computer

Description automatically generated

* 1. Incident response details, such as Indicators of Compromise (IoCs) and recommendations for containment and remediation, helping security teams manage the threat effectively.

A screenshot of a computer

Description automatically generated

Step 11: Additional Tools for Online Malware Scanning

Besides Hybrid Analysis, there are several other online malware scanning tools you can use for further investigation:

1. Any.Run: Online sandbox at [https://app.any.run]
2. Valkyrie Sandbox: At [https://valkyrie.comodo.com]
3. JOESandbox Cloud: Available at [https://www.joesandbox.com]
4. Jotti: Multi-engine malware scanner at [https://virusscan.jotti.org]

Step 10: Concluding the Analysis

This completes the process of scanning malware using Hybrid Analysis, where you successfully uploaded and analyzed a suspicious file. The report generated provides valuable information about the file’s threat score, anti-virus results, and behavioral analysis. These insights help identify potential risks, guiding further actions such as containment, incident response, and remediation. Now, you can close the web browser and any open windows.