***What is sandboxing?***

Sandboxing is a security technique used to run programs or code in a controlled and isolated environment. This restricted space, known as a sandbox, prevents the program from making unauthorized changes to the system or accessing sensitive data. It is widely used to safely test untrusted applications, analyze potentially malicious files, and ensure that even if harmful code is executed, it cannot affect the rest of the system. Sandboxing is commonly implemented in web browsers, mobile operating systems, and cybersecurity tools, offering an effective way to minimize risk while maintaining functionality.

***What sandboxing do?***

Sandboxing works by creating a restricted, isolated environment where a program or code can run without affecting the rest of the system. Think of it like a virtual room with locked doors — the program can do whatever it wants inside that room, but it can’t get out to harm the rest of your computer or network.

1. Isolation of Resources:  
   The sandbox gives the program limited access to system resources — such as files, memory, network, or hardware. It can’t interact with sensitive parts of the system outside its sandbox.
2. Access Control:  
   The sandbox applies strict permissions. For example, it might block the program from reading personal files, writing to system folders, or connecting to the internet.
3. Monitoring Behavior:  
   The system can watch what the program does inside the sandbox. This is useful for testing or analyzing suspicious software without any risk to the host machine.
4. Automatic Cleanup:  
   After the program finishes running, the sandbox can be wiped clean, ensuring no leftover files or changes remain.
5. Use of Virtualization or Containers:  
   Sandboxing can be implemented using technologies like virtual machines (VMs) or containers (e.g., Docker) that simulate separate operating environments.

How sandboxing works

There are various types of sandboxing tools like virustotal, any.run, hybrid analysis and more. Here I use “*hybrid analysis and virustotal”*  for sandboxing

Step 1

* ***Virustotal***

Here’s the official website of virustotal “<https://www.virustotal.com/gui/home/upload>”

When I open the website I'm using, it shows like this

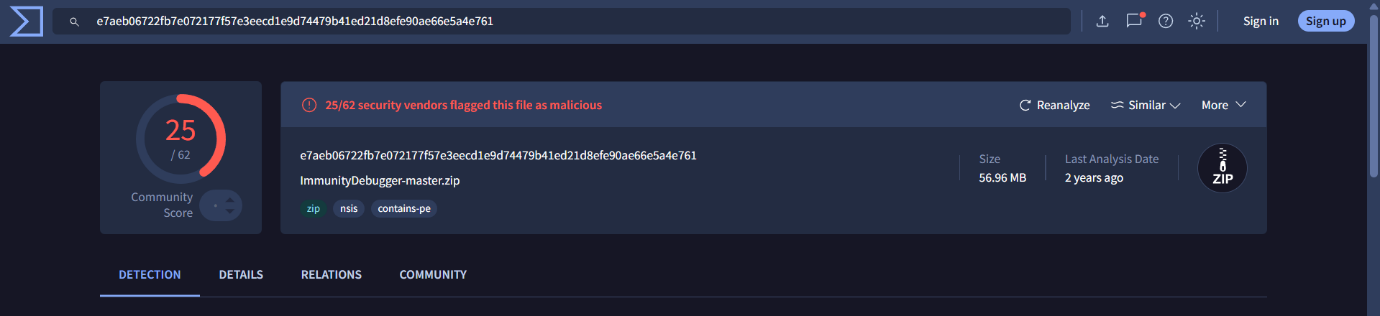


Here’s the official website of virustotal, now I choose my file which one I want to scan



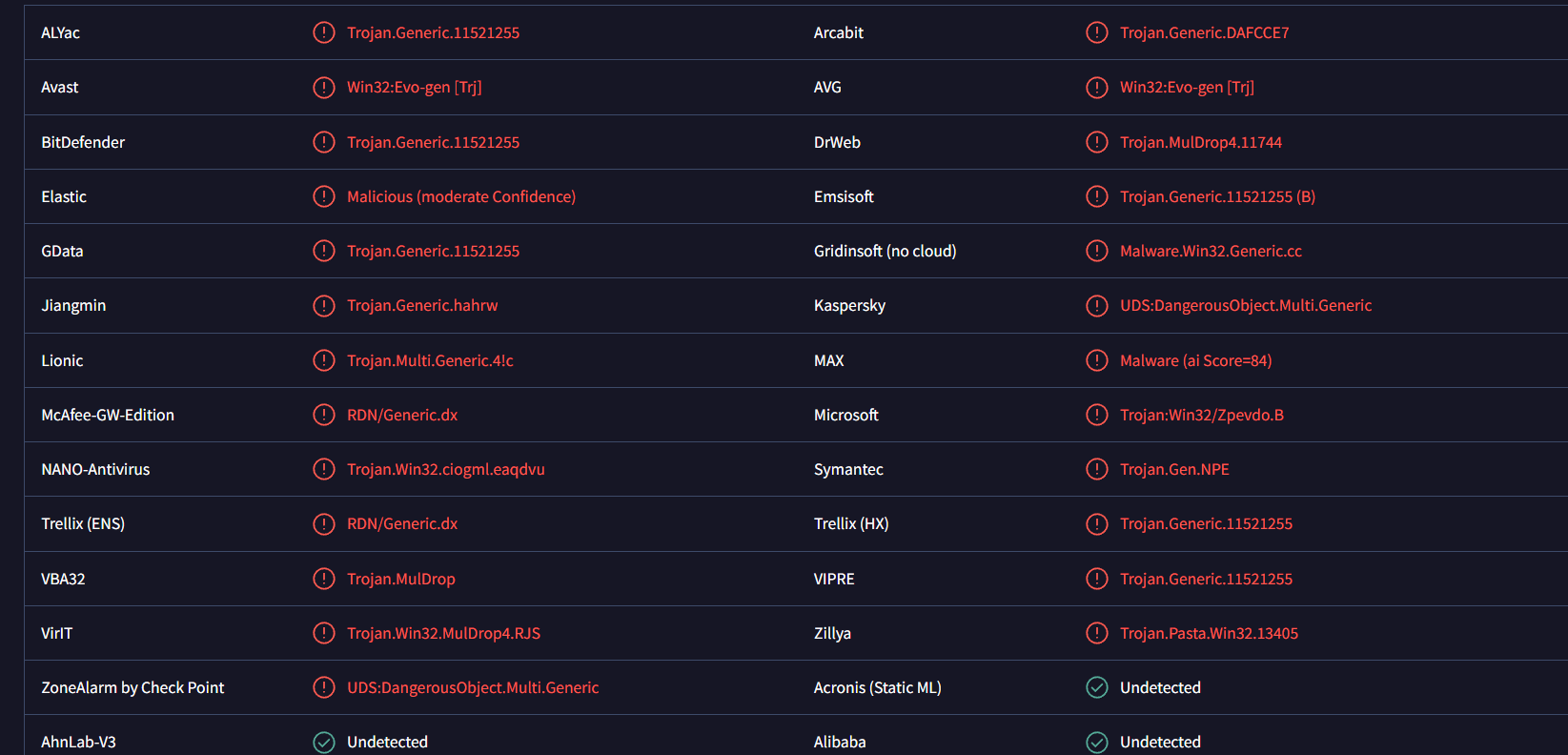
When I choose a file which one I want to check. The website starts checking the file in dept

After this I get the result here



There are 25 malicious flags are founded here

Just below there you get more result



What you get here?

* **Each row** represents a different antivirus (AV) engine or security vendor (e.g., Avast, BitDefender, Kaspersky, Microsoft).
* **The red warnings** (like Trojan.Generic.11521255, Win32:Evo-gen [Trj], etc.) are detections — the AV software believes the file contains malware or is malicious.
* **Green "Undetected" results** mean that the antivirus did **not detect** the file as malicious.

Key obervations

Most antivirus engines **detected the file as malicious**, identifying it as some form of **Trojan** or **malware**.

Common tags:

* Trojan.Generic: A general or heuristic detection for trojans.
* MulDrop: Indicates a **dropper**, which installs additional malware.
* UDS.DangerousObject: Kaspersky’s term for a potentially dangerous file.

Step 2

* ***Hybrid analysis***

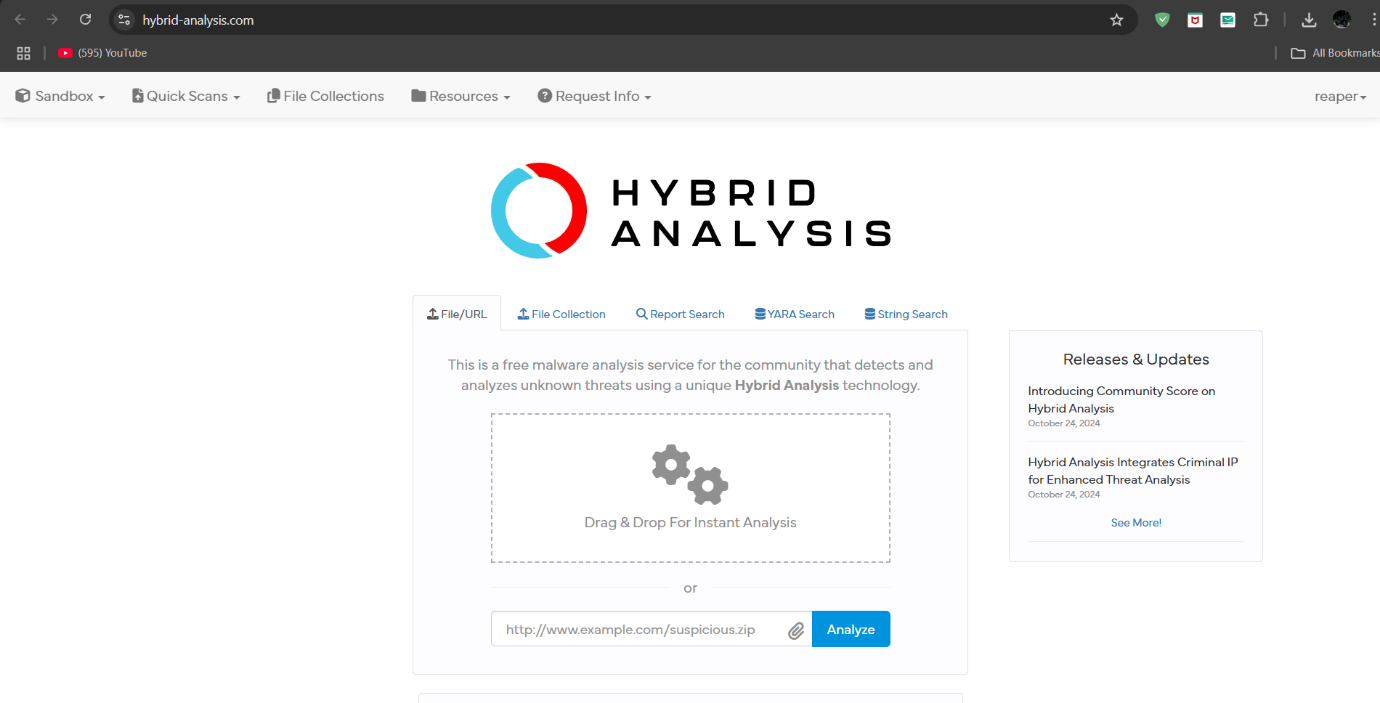
Here’s the official website of hybrid analysis

<https://hybrid-analysis.com>

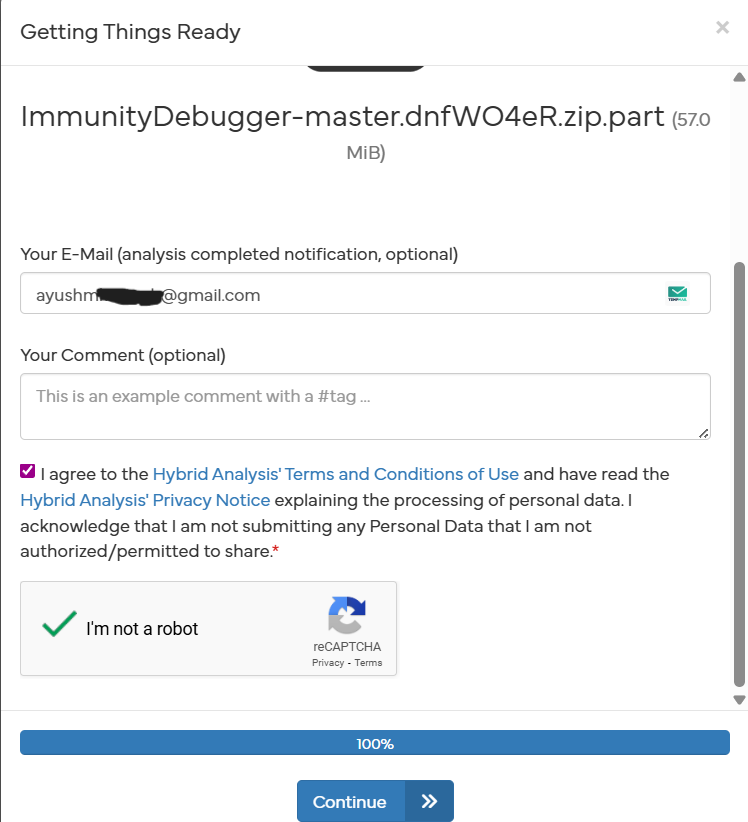
hybrid analysis are also similar like virustotal but little bit different

**Hybrid Analysis** is a more detailed sandbox environment that shows exactly what a file does when executed.

First I open a website

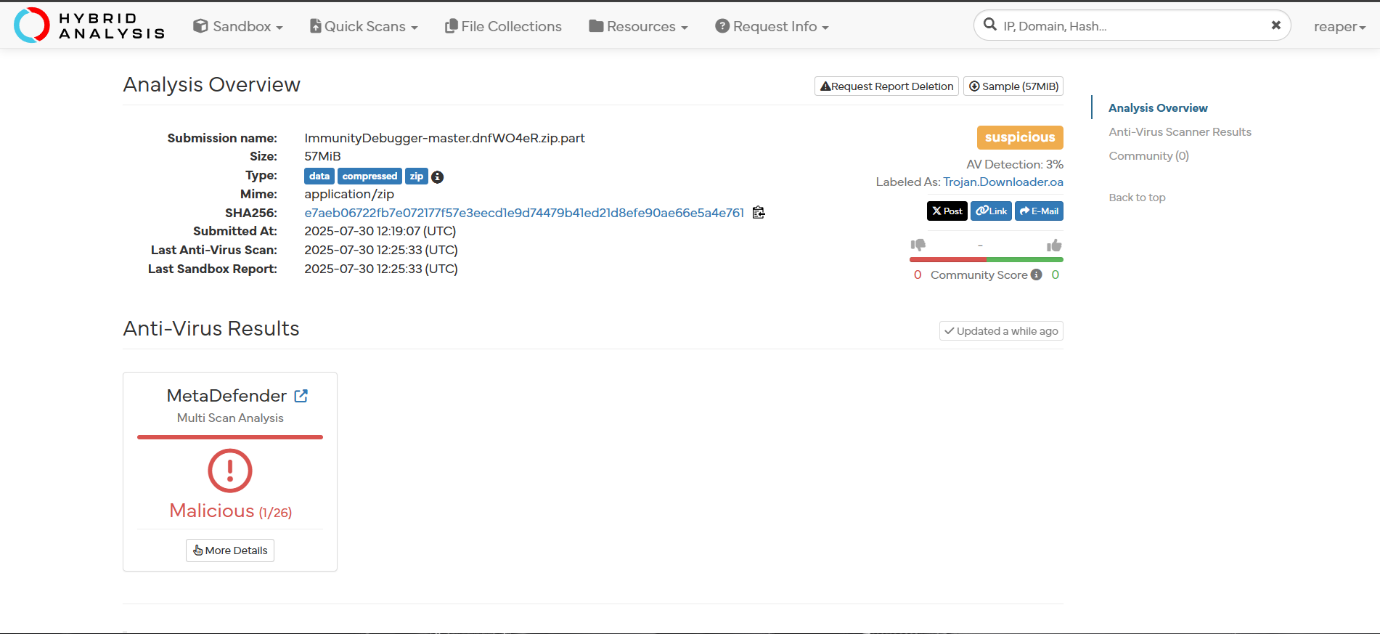


Its look Like this after this I clnk on “drag & Drop” box to select my file



And here I upload some details (optional) after that agree term’s and conditions and then verify ourself and then click continue

After that your file started scanning and finding malicious act in zip file



If your file found malicious it’s count in malicious and turn in red

If your file didn’t found in malicious act it’s count in clean and turn in green

As you see you get here some more details like

 **Submission Name:** ImmunityDebugger-master.dnfWO4eR.zip.part  
This is the name of the uploaded file — likely a **partial ZIP archive** containing the source or binary of "Immunity Debugger" (a well-known reverse engineering tool).

**Size:** 57 MiB  
This is quite large for a ZIP file — potentially raising suspicion.

**Type:** application/zip  
Indicates it’s a ZIP archive, possibly compressed software or project files.

**SHA256 Hash:**  
e7aeb06722fb7e072177f57e3eec...  
This unique fingerprint identifies the file. Helpful for cross-referencing with other malware databases.

**Submitted At:** 2025-07-30 12:19:07 (UTC)

**Last Anti-Virus Scan & Sandbox Report:** 2025-07-30 12:25:33 (UTC)

Some suspicious I found

**AV Detection:** 3%  
This means only **1 out of 26** antivirus engines flagged it as malicious.

**Labeled As:** Trojan.Downloader  
The engine that flagged it suspects the file is a **Trojan Downloader**, a type of malware designed to download more malicious files from the internet.

**Anti-Virus Results**

* **MetaDefender (Multi-Scan):**
  + **Malicious (1/26)** — Only 1 antivirus flagged it.
  + This *could* be a **false positive**, but also a sign of an **early-stage or low-profile threat**.