**ON Demand File Scan Using API’s-**

**How does the Antivirus File Scanning work?**

To identify malicious files, every antivirus software depends largely on signatures. When malware is discovered all around the world, it is analysed by malware researchers or dynamic analysis systems. After it has been established that the file is malware, a suitable signature of the file is extracted and uploaded to the antivirus software’s signature database.

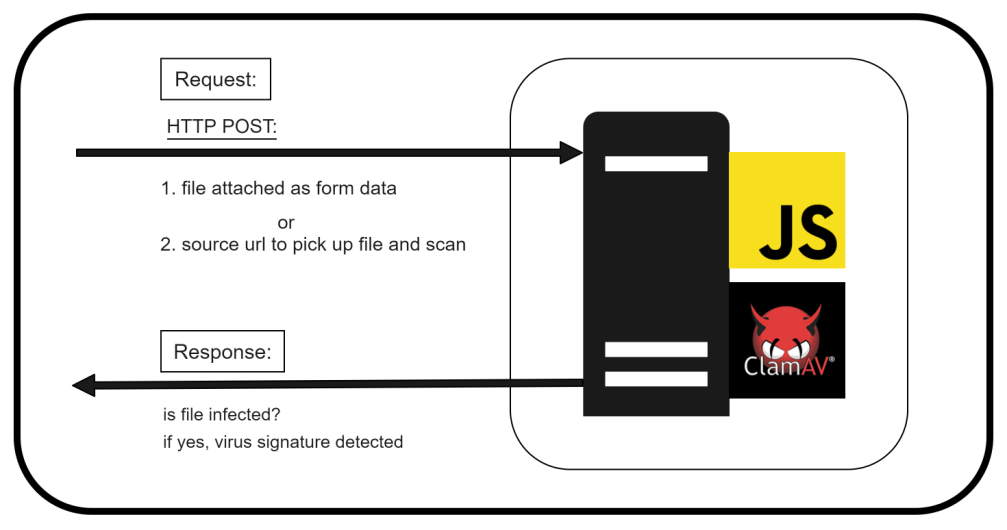
**Solution:**

A common practice is to have anti-virus software on an isolated server and scan the files. This does not help much because it is not always possible to **route our file through this server** and it does not support scanning a file on-demand.

This means that our solution should have an **anti-virus engine and exposing it as an API for file analysis**.:

[Clam-AV](https://www.clamav.net/) is an open-source antivirus toolkit able to detect all known virus signatures. It comes with an embedded database containing a virus signature against which a file is analysed. This database is updated daily when any new virus signatures are detected worldwide.

install this on an isolated server and expose it as a REST API. The JavaScript is used to read an incoming file in the HTTP form data and transfer it to clam-AV with the clamd daemon. The daemon functions by listening to commands on the sockets shown in clamd.conf.



Exposing Clam AV as API server -  
  
1. We have to pull Clam AV Docker image server. The image Detail can be found here, <https://hub.docker.com/r/clamav/clamav>. Then We have to expose a server, we have docker image <https://hub.docker.com/r/benzino77/clamav-rest-api>, this uses Node JS.The Git Repo for the solution is here. <https://github.com/benzino77/clamav-rest-api>.

2. We have two in one Docker image <https://hub.docker.com/r/ajilaag/clamav-rest>. It means we don’t have to run clam image separately. It will expose a rest api server also for it, this uses GO as rest server. Git hub repo can be found here , <https://github.com/ajilaag/clamav-rest>.