

Muhammad Aalian (22-10469)

Asad Shehzad (22-10008)

**Project Description:**

Anti-Malware detection using Heuristic and Signature based detection. The team has been assigned a GitHub repository of an anti-malware tool using signature based detection from its database and the objective of the project is to improve it and add some modifications. Signature based detection runs hashing algorithm on the files to be scanned and matches them with the known viruses in its database, however viruses are often adapting and this method might be bypassed by a newer virus if its hash is not present in the database.

To improve that, the team has come up with a solution, to add heuristic based malware detection on top of signature based malware detection. Rather than using a list of viruses as a reference to determine whether a device contains malware, heuristic virus detection spots viruses by identifying files with suspicious behavior or code infrastructure and flagging them as potentially dangerous. By doing this, an additional layer of security has been added.

**Steps to proceed:**

* Choose appropriate programming language such as Python or C.
* Update hashes present in the database of signature based detector.
* Using the github repo i.e. phpMussel, make changes to the code to fit the project description.
* Code a heuristic based detector model.
* Test it against common viruses and some uncommon in a virtual environment.
* Make updates necessary.
* Compile both signature and heuristic based detectors to run on a file to be scanned through conditional control statements.
* Add necessary updates.

**Possible Outcomes:**

As the older version of phpMussel will be tested against an infected file whose hash it doesn’t have in its database, the expected outcome is a failure to detect the virus, however with the addition of heuristic based detection alongside signature based, the expected outcome is **virus detected.**