**Automated PE32 Treat classification using Import Table and Deep Neural Networks**

**Abstract:**

A malware is a computer program which harms the computer in which it gets executed. Malware analysis play a major role in analysing the functionalities and behaviour of the malware. Malware analysis is a slow and tedious process which involves a lot of manual work. Finding the type of the malware will often boost up the analysis process and helps to the researcher to know what the binary is capable of. Usually researchers perform various static analysis techniques to find the category of the malware using various tools like strings, dependency walker etc., in our approach we are going to automate this process using deep neural networks.

**Keywords:** Malware, Malware Analysis, Static Malware Analysis, Malware Classification.

**Types of malware:**

**1. Backdoor:**

Backdoor is a malicious program which allows the remote attacker to gain access to the victim’s computer.

**2. Downloader:**

The sole purpose of the downloader is to download another malicious program and sometimes execute it.

**3. Keylogger:**

A keylogger is a program which continuously monitors the keystroke of the user. This helps the attacker to steal potential information like email address, password., etc.,

**4. Miners:**

This malicious program will use the resources of the victim’s computer to mine crypto-currency which is used to monetize the attacker’s wallet.

**5. Rouge software:**

Rouge software seems to behave like an original software say, antivirus and will trick the user to buy services which will end up paying to an attacker.

**6. Trojan:**

A trojan is a software which seems to behave like a legitimate program but does malicious activities in the background.

**Import Address Table:**

Import Address Table has the information about the functions which are used by an executable. These functions could help you to identify certain functionalities of the malware.

Here is an example of some functions used by a binary:



As you could see some functions like CryptEncrypt will encrypt the data which exhibits the properties of ransomware. So, we could use these functions to make our predictions.