R.A.T Detection Using Python

Mr. Mohammed Ratlamwala , Mr. Omkesh Rane

Project Guide: Prof. Martina D'Souza (B.E IT, M.E Comp)

Abstract- ***Considering the internet world is very vast data flows all over the world from one end to another end millions users are connected to internet, day by day internet security has becoming the major concern of the world more new methods are implemented to make it secure, attackers find different ways to exploit it. R.A.T is one of the powerful hacking tool which is used over the internet by the attacker, to exploits the user personal data. This R.A.T detection is software which helps in detecting the R.A.T in the user system. The paper describes about this software about its development, application and its technical implementation.***

Index Terms- R.A.T, Machine learning, Remote Administrator Trojan, machine learning, Process tracking, Malicious, Legitimate.

1 INTRODUCTION

1.1 BACKGROUND

In the world of growing computer and internet, data security has become one of the important aspect of today's world, as every individual have their personal laptop and desktop connected internet they are connected to the virtual world , they can access any data they want over the internet, no doubt internet is a great technology and boon to modern world, but there are some people who use this technology for exploiting other people security and data by using various exploiting method which in turn cause loss of data, exploiting their privacy and many more damage.

R.A.T detection System is the system which helps to detect the attack done by the exploiter, basically R.A.T attack is one of the common attack done by the attacker to the individual, this attack is done my sending a file to the user, the file may be of any format like photo, video, doc etc. When user access that file he doesn't know that his system has been exploited, the attacker then can remotely monitor the individual's activity like his process, data any information in his system at other side user don't get any indication that he has been exploited by the attacker. This is the main reason why R.A.T is so powerful tool for exploiting any individual over the internet and sometimes it is undetected.

1.2 AIM AND OBJECTIVE

The aim of this project is to implement the software on the user end. The project focuses on developing a system which can detect whether given PE file is legitimated or infected with malicious code with the help of supervised machine learning approach and K-N-N algorithm, with the help of this software user can safeguard his system by scanning the downloaded files before executing it.

1.3 MOTIVATION

As the software provides scanning which helps user in detecting whether the file is legitimate or malicious which helps in stopping the attacker from exploiting the system and becoming vulnerable to the attacker.

As the user is provided with the software he has to manually scan the suspected file before executing the file, it will display result whether that PE file is legitimate or remote administrator Trojan, if he/she fails to scan PE file before executing it, it will exploit the system which is the loop hole in the software

The R.A.T detection software provides detection of remote administrator Trojan and other malicious software which gets downloaded in the system via mail or from any other websites and can harm the working of the system and expose sensitive data from the system

2. LITERATURE SURVEY

2.1 RELATED WORK

Host-based malware detectors have the advantage that they can observe the complete set of actions that a mal-ware program performs. It is even possible to identify malicious code before it is executed at all[2] , we use KNN algorithm, Similarity calculation among samples is a key part of KNN algorithm.[1]

2.2 Problem Statement

R.A.T is one of the most popular hacking tool for hackers which exploits the victim system to the attacker and sometimes it is difficult for antivirus to detect it, this allows the full control of the victim system to attacker

3 Proposed System

The project "R.A.T detection using python" is implemented on python using k-n-n algorithm. This system follows machine supervised learning approach to learn characteristics of benign and malicious file. User scan the file which is suspected of being infected by R.A.T the program applies machine learning algorithm which are already trained and give a report to the user whether the file is clean or infected, thus giving the user authentication of the file

3.1 Proposed Architecture

The proposed system uses machine learning approach in detecting malicious file. The classifier is given data set of legitimate and malicious PE file it than trains the classifier and then use classifier to check whether file is malicious or legitimate

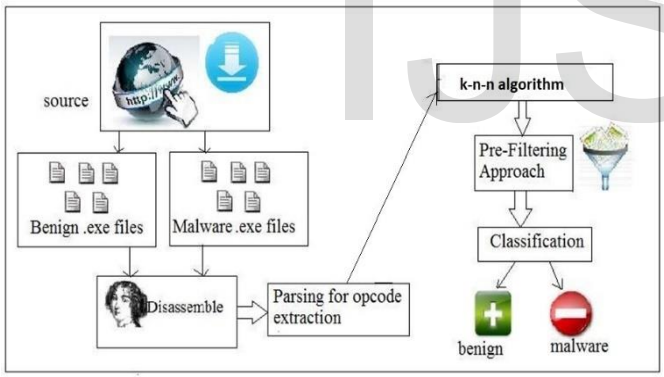
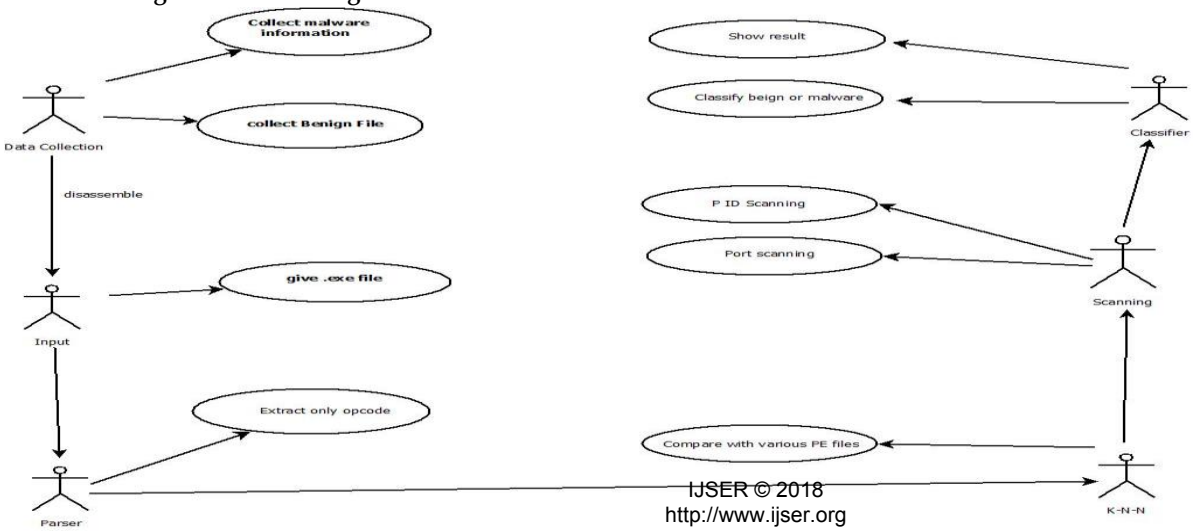


Fig 3.1 System Architecture

Fig 3.2 Use case Diagram



4. Working Methodology

With R.A.T detection using python the file is static checked for the occurrence and binding of any malicious or harmful code within the original file

4.1 Importing

Dependencies such as pandas for data analysis, numpy for maths, pickle to save our learn features as a byte stream, scikit-build train and test a machine learning model first we load a data source we have a csv file on our local machine called data CSV that contains a labeled data set of PE files labeled as
Either legit or malicious.

4.2 Classifier

we create an array of models we're going to test each model on our data set using our extracted features as inputs and compare their prediction results whichever model has the best results is the one we will use to detect malware on our feature set then scoring the prediction accuracy we'll print out each score then calculate a winner by finding the highest prediction accuracy we'll print out the winner then save the algorithm weights and features to the classifier folder

5. CONCLUSION

The paper explains the concepts of R.A.T detection software it also explains the modules that are implemented to provide a complete software, it also explains the complete benefits of the software for the user regarding his personal computing security.

6. REFERENCES

[1] Yun-lei cai, Duo ji, Dong-feng cia " A KNN Research paper classification mwthod base on Shared neighbor",proceedings of NTCR – 8 Workshop Meeting, June 15-18,2010 Tokyo Japan

[2] Clemens Kolbitsh Paolo Milani Comparetti Christoper Kruegel, "Effective and Efficient Malware detection at end Host" In IEEE Symposium on Security and Privecy (2005)

[3] Joshua Abah, Wazir O.V, Arthur U.M. "A Machine learning Approach to Anomaly- Based Detection on Android Platform" International Journal of Network security & its Application (IJNSA) Vol, No.6, November 2016

[4] Dan Jiang, Kazumasa Omote "An Approach to Detect Remote Access Trojan at Early Stage of Communication ". 2015 IEEE 29th International Conference on Advanced Information Networking and application.