JMEA Journal of Modern Educational Achievements
Volume 5, 2024 https://scopusacademia.org/

Detection Of Malware Intrusions For System Security

Shoraimov Khusanboy[1, a)]

[1]*Assistant of the Department, "Systematic and Practical Programming", Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi, Uzbekistan,*

[a)]Shoraimovkhusan@gmail.com

Abstract. Network assaults are getting more and more complex with the improvement of web innovation. It's hard for the conventional detection frameworks to recognize strange traffic. Intrusion Detection System is an application that is used to investigate all organization traffic and caution the clients if there has been unauthorized access. Intrusion Detection System is similar to a firewalls that screens network traffic and decides if it should be allowed or not. Modern malware uses a lot of techniques, but it's not effective. The analysis tools take a lot of effort to find the hidden software; it's usually possible to find it in a real run. An approach to do the analysis is to use an operating system that strays from real behavior. It's important to find the presence of malicious behavior and have enough evidence of it's intent. The investigation of an association's organized traffic is related to the sudden increase in demand for customer PCs. Associations can use a strategy to secure the whole network. It is possible for this methodology to be used in the system. Malware discovery frameworks can give organization security.

INTRODUCTION

The computer and its network are vulnerable to malicious software. It can cause the computer to crash, and it can also take users' privacy. To keep the system safe, an intrusion detection system is needed.

A. There are issues with current software.

Current malware programs hide their presence on the system, making it difficult to detect them. Because of this, there's no software that can find what's in the system. After comparing the two, most of the anti-malware software identifies the malicious software. It was already detected from the past. A combination of more than one method is needed. Associations can use a strategy to secure the whole network. The method makes it possible to find the malicious software on the system devices.

B. There is a need for a new detection system.

Malware recognition frameworks can give organization security.With the improvement of web innovation, network assaults are getting more and more convoluted, making it hard for conventional malware location frameworks to successfully recognize strange traffic. The data-traffic investigator can assist with identifying polymorphic malware dependent on network-traffic.

SYSTEM OVERVIEW

Based on the efficiency, reliability, security, availability and determining that not one model can give a perfect protection against the sophisticated malware, we compare the detection systems. To find a solution. Machine Learning helped us design a better intrusion detection system.

1. Pre-processing: The data collected is the features of the files that were downloaded through the internet.

Some features that were collected are more likely to be affected than others. The features that are needed for the extract are stored in the dataset.

2. Dataset: There are features in the dataset which don't contain any affected features but which can help to determine with other similar data documents.

The input data file contains Virus Share files which can be used to find the malicious software. There is a large dataset with both Legitimate and Virus share features.

3. Features: 55 of the collected features were given to the Machine Learning algorithm to further select the features needed after the dissociation.

All the sites on the blacklist can be harmful to the system. The below Figure III. There is a block diagram of the Malware Detection System.

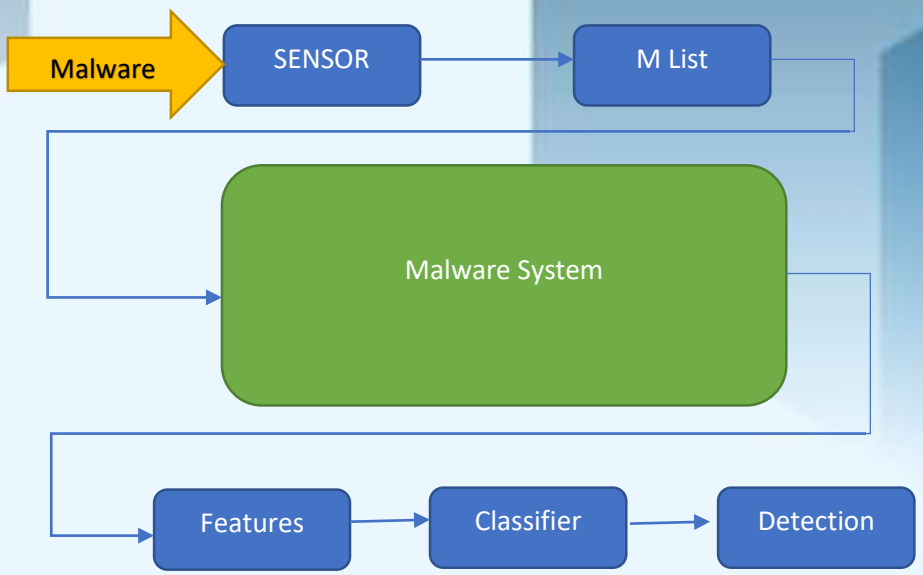

FIGURE 1. System layout

A. Sensor: A sensor is used to detect and monitor the network traffic of the system.

This traffic contains all the incoming and outgoing data with the site's IP address to trace back after detecting the malicious software on the site.

B. Malware List: The Black List contains sites that can be harmful to the system.

The black lists contain publicly available (black) lists which have harmful scripted sites detail and that cantrigger as an unexpected attack, and addition to that there are also blocked websites data and their IP addresses taken from other virus detection systems and all of this is going to interrupt the sensor to find malware. It also has websites which allow the download option when we visit the site and this can also be blocked, it avoids the websites which are free from any malware.

C. Classifier and Features:

1.The system logs contain network traffic. A set of features is taken from the dataset and used for the detection of malicious software.

2. Decision Tree and Random Forest were used to extract the features from the data set.

3. The process is divided into two parts. The figure explains the process of detecting malicious websites on the internet. Figure 1 explains the process of detecting the suspicious files on the system

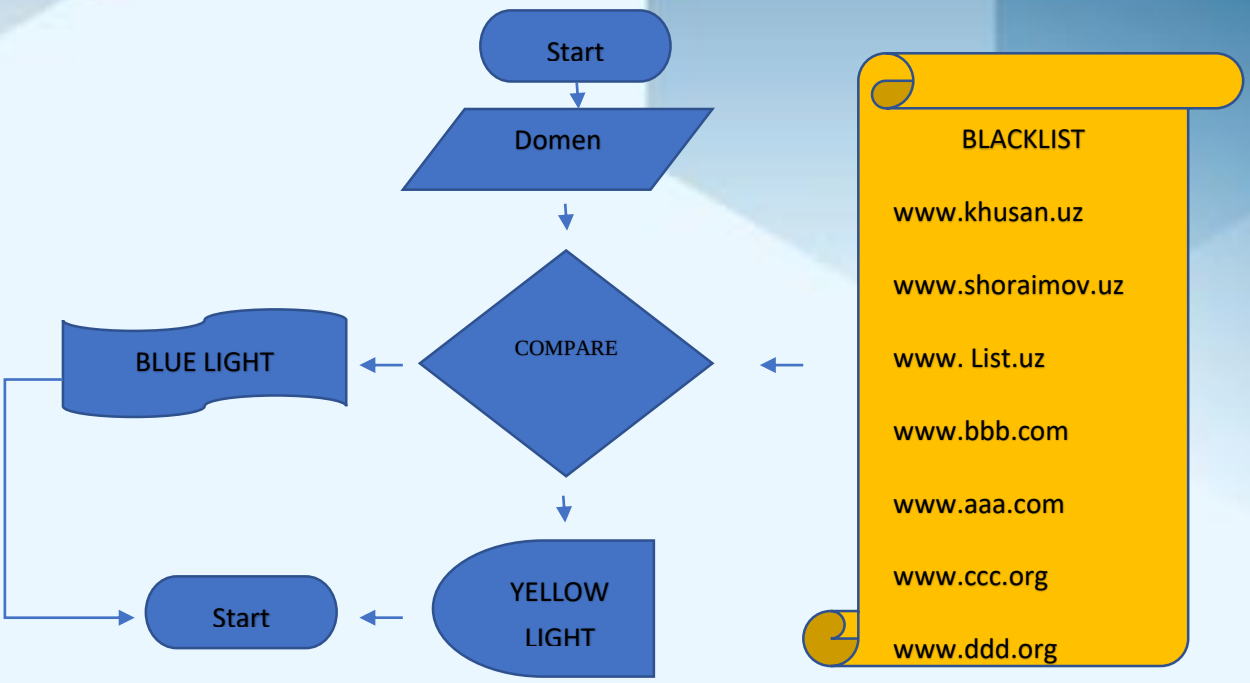

FIGURE 2: Detection on the network

The process begins when a web is used to search the internet. After entering the site id address and trying to load the site, the site's ip address is recorded and compared with the Blacklisted sites which contain malicious software. If the site is safe, it will indicate it with a red light if matched, otherwise it will be a green list.

RESULTS

The features that are required to train the Machine Learning algorithm are collected by the dataset. There were 55 features taken from the dataset which were relevant and most likely to be used to get infections. The 55 feature feature is shown in figure 2.

```
Id features:
1. F image(0.090)
2. F Machine(0.082)
3.MajorsubsytemVersion(0.008)
4. f char(0.094)
5. Resourse(0.020)
6. feature SectionMeanEntropy(0.002)
```

FIGURE 3. Collected Features

Decision Tree and Random Forest were used to extract the features from the data set. The efficiency was taken out from both methods after they were done. The most efficient algorithm will be used to detect the malicious software in the system.

The features will be saved in a directory. The latest files which have been downloaded on the system are scanned and given an indication of what is in that document. The system is protected from unwanted files that are stored in the system.

CONCLUSION

There are different forms of traditional based approaches, these models operate with raw data collected as input, without requiring any type of expert domain knowledge and input features, it can provide a very powerful approach. The architectures are capable of learning from the inputs. It is possible to find the malicious software present in that file using these features. It's easy to detect using a machine learning based classification. More security is given by using two methods for detecting. Not only does it protect it from the internet, but it also protects it from the malicious software inside the system. The only way to increase the dynamic more approach is to use the methodologies already presented. Machine Learning can be used to train the Malware intrusion detection system to detect new threats. The system can be protected from avoiding malicious sites by using the publicly available blacklist. The system is most likely to be intruded with human-created malware with the advancement of technology and human interruption. There are improvements that can be done in this area. It's possible to add new features to this software with the help of machine learning. The latest files which have been downloaded on the system are scanned and given an indication of what is in that document. The system is protected from unwanted files that are stored in the system.

There are different forms of traditional based approaches, these models operate with raw data collected as input, without requiring any type of expert domain knowledge and input features, it can provide a very powerful approach. The architectures are capable of learning from the inputs. It is possible to find the malicious software present in that file using these features. It's easy to detect using a machine learning based classification. More security is given by using two methods for detecting. Not only does it protect it from the internet, but it also protects it from the malicious software inside the system. The only way to increase the dynamic more approach is to use the methodologies already presented. Machine Learning can be used to train the Malware intrusion detection system to detect new threats. The system can be protected from avoiding malicious sites by using the publicly available blacklist. The system is most likely to be intruded with human-created malware with the advancement of technology and human interruption. There are improvements that can be done in this area. It's possible to add new features to this software with the help of machine learning.

REFERENCES

1. G.D. Penna, L.D. Vita and M.T. Grifa, “MTA-KDD’19: A Dataset for Malware Traffic Detection“ in ITASEC - 2020.
2. M. Gao, Li Ma, H. Liu, Z. Zhang, Z. Ning and J. Xu, “Malicious Network Traffic Detection Based on Deep Neural Networks and Association Analysis” in Sensors (Basel) - 6 March 2020.
3. Sudarshan N & P.Dass, “Malicious Traffic Detection System using Publicly Available Blacklist’s” in IEEE Conference of International Journal of Engineering and Advanced Technology (IJEAT) - August 2019.
4. M. Skrzewski, “Flow Based Algorithm for Malware Traffic Detection” in International Conference on Computer Networks - July 2011.
5. Dmitri Bekerman, Bracha Shapira, Lior Rokach and Ariel Bar, “Unknown Malware Detection Using Network Traffic Classification” in 2015 IEEE Conference on Communications and Network Security (CNS).
6. Paul Prasse, Lukas Machlica, Tomas Pevny, Jiri Havelka and Tobias Scheffer, “Malware Detection by Analysing Network Traffic with Neural Networks” in IEEE Conference of Symposium on Security and Privacy Workshops - May 2017.
7. J. J. Parekh, Ke Wang, S. J. Stolfo, “Privacy-Preserving PayloadBased Correlation for Accurate Malicious Traffic Detection”.
8. Nancy Agarwal and Syed Zeeshan Hussain, “A Closer Look at Intrusion Detection System for Web Applications” in IEEE Conference of Security and Communication Networks Volume - 2018.