MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

MALWARE PROTECTION FOR EXTERNAL DEVICES

Shubham Bhasme, Swarupa Sathe,Ambar Lonkar,Prof.Laxmi Madhuri

Department of Computer Engineering,
Dr. D. Y. Patil School of Engineering, Pune, India.

Abstract: *As the Maximum malwares are spread from the external devices and they may infect to the system, maintaining security while transmission of data from the external storage device to the system is more challengeable in today's computer world. Malware is malicious software used to collect sensitive info or gain entrance to private computer system. Applications provide facilities for detect and prevent the malware. The aim of this paper is to detect the malware for an external storage device and maintain security and evade losing of data. Security is more significant, thus it requires to make a more secure model which can automatically provide the malware protection from the external storage devices. This application program designed is used to protect external devices like pen-drive, HDD etc. The software is loaded into external devices which user wants to protect from harmful data from the system. Hence, such type of application can be used for protecting external devices.*

Keyword: *Malware protection, computer security, dynamic analysis, classification algorithm.*

1. INTRODUCTION

Malware is an abbreviated term meaning "malicious software". This is one type of program or file that is destructive to a computer user. Network, desktops, laptops, pen drive, hard disk, mobile devices, virtual environments all are under attack. Problem is that security experts often don't have visibility into the space of progressive malware in their network. Questions needed to effective such as:

- How do we recover from it?
- Can I stop the threat at root cause?
- How we prevent it from happening again?

Investigators have use static analysis methods to identify zero day malware[1]. In static analysis the features are reserved using a PE (process explorer) file extractor API but this method fails when a file is packed or encrypted because entropy of some of packed benign

is same as that of malicious file. Hence a classification algorithm gives false alarm in this case[6]. There are many cases where code reorganization confusion is applied to a code variant of malware. Similarly a sequence of NOP instruction has been included in the code to modify the syntactic signature [5] of the variant but keep the semantics unchanged. By inserting and retrieving dummy values through the stack or memory cannot change the behavior of the program but makes difficult for reverse engineering [2].

- People connect their External Storage Device for exchanging the data so this is the entry point for malware to attack their data.
- Thus, protect the External Storage Device using software and prevent the malware to coming into storage device.
- Using different technics and algorithm the application can analyze the data for infected file and prevent them to come into external storage devices.
- After installing this malware protection software in external storage device this application provides freedom to connect external storage devices to any computer without any malware risk.

A malware is a computer program that has various kinds of malicious intents. Basically malware analyst uses two common approaches to study malware sample i.e. Static and dynamic analysis. Static method is the general approach to identify whether a file is a malicious or benign file[4].

In dynamic analysis several writers have suggested different approaches to extract the behavior specifications of malware. Static analysis of malware flops in the case of polymorphic and metamorphic malware; malware authors can change the syntax of malware but semantics remains unchanged; Using Dynamic analysis we can detect polymorphic and metamorphic malware [6].

2. PROPOSED WORK

From the literature survey, it is clear that there is a need to develop a antivirus protection for external storage device to protect the system from viruses and malicious attack. So, to meet the objectives, this paper proposed a, implementation prototype systems that characterize the inherent features of executable file and analyze them for quick and accurate analysis, which will restrict the malicious code to enter into the external devices like pendrive, external hard disk etc. The whole process of proposed system is divided into set of modules like:

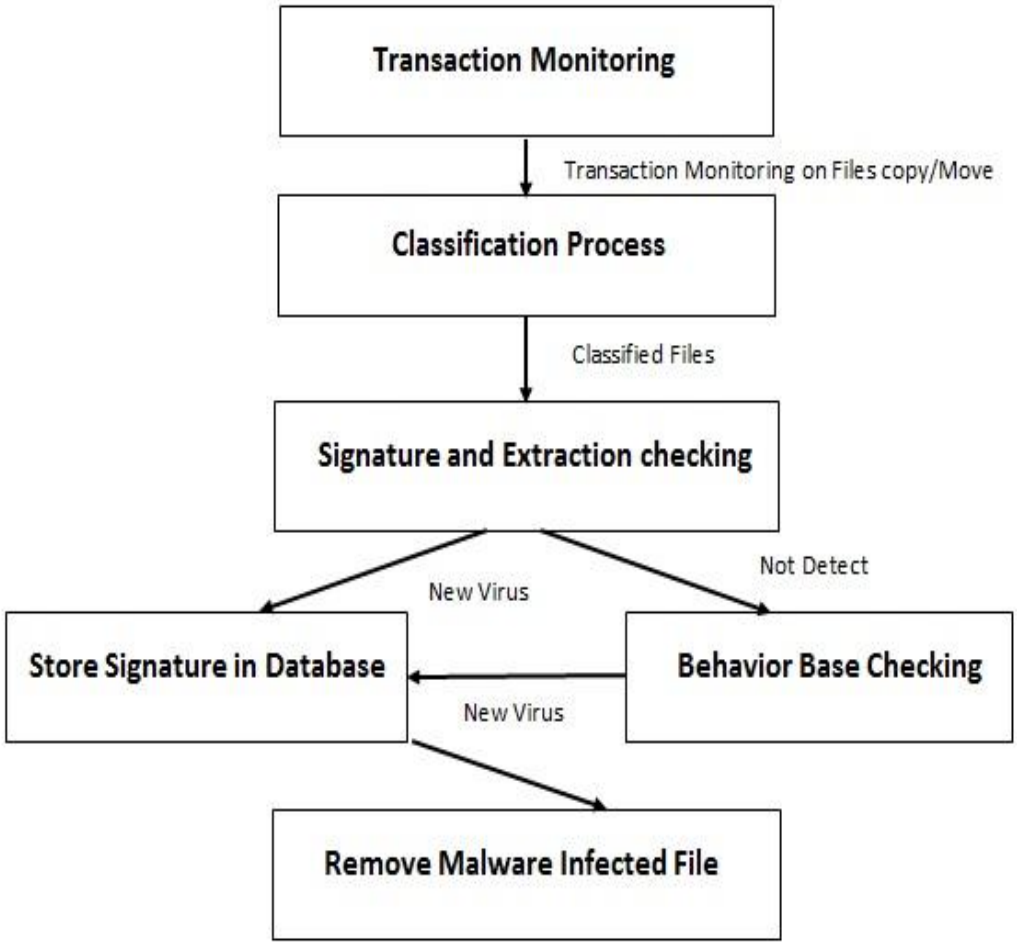

Fig.1: Proposed architecture of malware protection for external device

2.1. Transaction Monitoring System

The monitoring applications have need of data such as log file path and amount of threads to run with. Once the application is running, it needs to know what to monitor, and deduce how to monitor. For the reason that the configuration data for what to monitor is needed in other areas of the system, such as deployment, the configuration data should not be custom-made specifically for use by the system monitor, but should be a general system configuration model.

Effective monitoring or ability to monitor efficiently: Monitoring must be efficient, able to handle all monitoring areas in a timely manner, within the preferred period. This is most linked to scalability.

2.2. Classification Process

The standard technique of sorting out such files is still brute force manual analysis that requires experts. Some tools have been developed to help manage with the problem. These tools range from programs that recognize previously classified files and viruses and eliminate them, to utilities that extract strings from infected files that help in identifying the

viruses. None of the solutions are acceptable, yet. Clearly, more advanced tools are needed. In this paper, t he concept of dynamic analysis[6] is conferred as applied to viruses.

2.3 Signature Based Checking Malware

Signature based detection is the most mutual method that antivirus software uses to detect the malware. This method is slightly limited by the fact that it can only identify a limited amount of developing threats, e.g. generic, or extremely broad, signatures. When antivirus software scans a file for viruses, it checks the contents of a file against a dictionary of virus signatures. A virus signature is the virus-related code. Finding a virus signature in a file is the same as saying you found the virus itself.

2.4 Extraction Based Checking Malware

An extraction algorithm that use windows API function calls as a main feature to identify malicious executable or benign application. The algorithm completed only when the antivirus application malware protection system to run executable files and detecting its behavior protection system. It is unsuccessful if malicious executable doesn't use API functions or using for static features analysis [3]. We malware protection system carried out the algorithm improved by adding variable mi to define the maximum number that a feature is observed.

2.5 Behavior Based Checking Malware

Behavior based virus detection is a promising method capable of detecting unknown viruses. This method of virus detection does not use a signature database. Instead performing processes are monitored and their behavior is examined. If the execution behavior of a process displays virus behavior then the process can be highlighted as being a possible virus. Virus behavior is predefined by the behavior based detection method that is being implemented and is typically done by a knowledge proficient in computer viruses. The main problem of behavior based virus detection is defining a virus behavior that guarantees the detection of both known and unknown viruses while not erroneously detect benign processes as existence a virus.

Result: This has proposed a Malware Protection for External Storage Device is use to block any viruses coping to external storage device and the most obvious purpose is to remove viruses from External Storage Device and stop being infection to keep safe external storage device as well as computer.

3. APPLICATION

As security is major important task in all type of areas such as corporate world in which data protection is very important in business logics while exchanging the data, College persistence: In college life when staff or students exchange data from public computer to external storage device it will protect the personal data being infected, System scanning: To scan the whole system for removing the malware and infected file, Data protection: It is used to protect the important data being infection.

4. CONCLUSION AND FUTURE SCOPE

This proposed system will detect the malwares using malware database and provide the protection for the external storage devices while transmitting the data from external storage device to computer system & vice-versa. The external device will become more secure from malicious activities and different types of attacks.

As this paper proposes the security for external storage devices. In future it is used for implementing security in internal storage devices and also this can provide security for malware protection while sending E-mails and file attachment.

ACKNOWLEGEMENT

We would like to thank Dr. D. Y. Patil School of Engineering for providing us with all the required services. We are also grateful to Prof. Laxmi Madhuri and Prof. S. S. Das(Head of Computer Engineering Department), DYPSOE, Lohegaon , Pune for their vital support, suggestions and motivation during the entire course of the project.

REFERENCES

[1] Malicious Data Classification Using Structural Information and Behavioral Specifications in Executable.Proceedings of 2014 RAECS UIET Punjab University Chandigarh, 06 – 08 March, 2014

[2] Identification of malware activities with rules.Proceedings of the 2014 Federated Conference on Computer Science and Information Systems pp. 101–110.

[3] A scalable multi-level feature extraction technique to detect malicious executable.

a. Mohammad M. Masud & Latifur Khan & Bhavani ThuraisinghamPublished online: 23 October 2007 # Springer Science + Business Media, 2007

[4] The Design and Implementation of an Antivirus Software Advising System. 2012 Ninth International Conference on Information Technology- New Generations

[5] A Malware Detection Scheme Based on Mining Format Information.Hindawi Publishing Corporation Scientific World Journal Volume 2014, Article ID 260905.

[6] Malware Classification Using Static Code Analysis and Apriori Algorithm Improved with Particle Swarm Optimization.