ARTIFICIAL INTELLIGENCE BASED ANTIVIRUS

Aswini sree,Ayshwarya,Kowsalya
Asst.Prof M.Sangeetha, Dept.of Computer Science, Panimalar Engineering College, India

ABSTRACT— *In this paper, we focus on the dynamic invocation of code and patterns based on the existing antivirus model. This emphasizes an artificial intelligence model in developing the code which will do the Invocation automatically and start to execute in case of any virus files available. The virus files can be identified through the signatures and patterns via the type / name of files which already exists. In this case, the user will train the model for the type of virus. An intelligent system will take care of future detection with those pattern. The operations involve the 3 step process Validating the behavior of the files and following the validation an automatic event detection happens and event will be handled to process in case of virus detection.*

Keywords— Malware ,Virus detection ,Pattern ,Machine Learning.

1, INTRODUCTION

The problem of spam or Unsolicited Bulk Email (UBE) is becoming a pressing issue. In spite of the development of many anti-spam techniques, the war against spam is far from being successful. This is partly due to several characteristics of spam that make it a difficult problem. E-MAIL communication is prevalent and indispensable nowadays. However, the threat of unsolicited junk emails, also known as spams, becomes more and more serious.

In this paper, we explore to devise a more sophisticated email abstraction, which can more effectively capture the near duplicate phenomenon of spams. Motivated by the fact that email users are capable of easily recognizing similar spams by observing the layouts of e-mails, we attempt to represent each e-mail based on the e-mail layout structure. Fortunately, almost all e-mails nowadays are in Multipurpose Internet Mail Extensions (MIME) format with the text/html content type. In view of this observation, we propose the specific procedure Structure Abstraction Generation (SAG), which generates an HTML tag sequence to represent each e-mail. Different from previous works, SAG focuses on the e-mail layout structure instead of detailed content text. In this regard, each paragraph of text without any HTMLtag embedded will be transformed do a newly defined tag <my text=>.

In the field of collaborative spam filtering by near-duplicate detection, a superior e-mail abstraction scheme is required to more certainly catch the evolving nature of spams. Compared to the existing methods in prior research, in this paper, we explore a more sophisticated and robust e-mail abstraction scheme, which considers e-mail layout structure to represent e-mails.

2, PROPOSED ALGORITHM: Malware bytes anti-malware scanner

- The Malware anti-malware scanner algorithm is configured to use the interpreted virtual memory states and the interpreted virtual disk states to detect system's malware and the affected files.
- Based on non-intrusive machine introspection without perturbing their execution, the resources extrapolating guest functions by interpreting the virtual memory states and the virtual disk states.
- The object malware algorithm detects the system and enables out-of-the box, tamper-resistant virus detection without losing the semantic view.

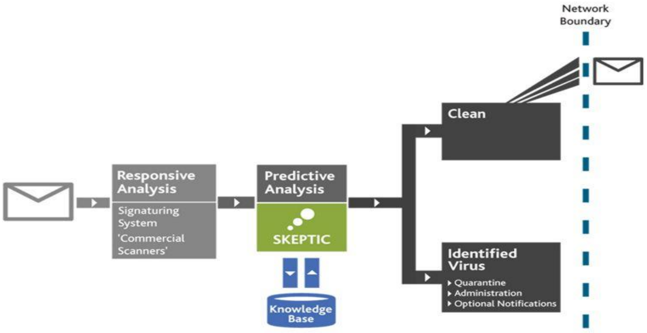
3, SYSTEM ANALYSIS

3.1 Existing System

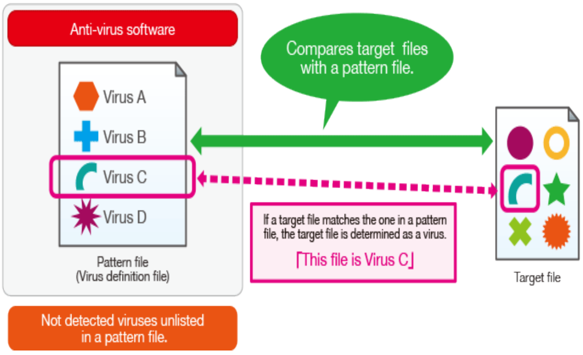
Existing System focus on the event driven actions. The three main diagnostic phases that emerges are behavior modeling , event detection and event handling. The existing system provides an automated process in handling and detecting the virus signature and delete it and identify the standard formats of the viruses such as exe and vbs files.

4, PROPOSED ARCHITECTURE

The architecture of proposed virus detection system is shown in below figure.



Proposed system mainly focusses on the AI system. Custom file formats will be deleted based on the user feedback provided. Custom virus signature can be added and it will be evaluated on the files and based on the outcome the files will be deleted. Automated email system in case of file detection.


Anti-virus software
Virus A
Virus B
Virus C
Virus D
Pattern file
(Virus definition file)
Compares target files with a pattern file.
If a target file matches the one in a pattern file, the target file is determined as a virus.
「This file is Virus C」
Target file
Not detected viruses unlisted in a pattern file.

5, IMPLEMENTATION

5.1 Virus Pattern Define

- Creating the signature code for the input code
- Feed it into the system.
- Looping through the searching methodologies to search for the possible viruses in the input file injected into the system
- This module utilizes the Signature match algorithm in matching the input format with the stored formats.

5.2 Antivirus Activation – Virus Check

- De-patternized the ASCII content / bytes in to the original data.
- Match content to check the possibility of viruses
- Virus indicate the user for action

5.3 Dynamic Pattern Feed

- Editing the name of the viruses, If wrongly feed into the system.
- Editing the patterns of the virus formats.
- View all the virus patterns
- Edit the actions taken on the files and viruses

5.4 Virus Alert/Action

- Final module includes the type of actions taken on the viruses.
- User will be given an option to finalize the future actions to be taken on the viruses. In case, if it comes from different sources.
- The actions specified will be reconfirmed to the user before taking an action.
- The viruses will be moved to a very safe location in the machine. In case, it is needed for future references

VI. CONCLUSION AND FUTUREWORK

In this paper, we have proposed to come up with a machine learning frameworks that generically detects as much malware samples as it can, with the tough constraint of having a zero false positive rate. This will not only easily detect known viruses but act as a knowledge that will detect newer forms of malicious files. The infected file data set is provided as an input to the system to detect the event handling. The number of generated rule is reduced, by removing the redundant rules, to make system analysis efficient. The performance of the proposed AI based virus detection system is evaluated for accuracy and compared with existing antivirus. It is inferred that the proposed virus detection system outperforms the existing system. Finally, our results have proposed techniques for improving the current state of virus detection and provide security to the system.

REFERENCES

#1. “Data-driven Event Triggering For Iot Applications”-panayiotis Kolios,*Senior Member, IEEE*,and Marios Polycarpou, *Fellow, IEEE,* IEEE Internet Of Things Journal, Vol. 3, No. 6, December 2016

#2. “Efficient Virus Detection Using Dynamic Instruction -Sequences”-Jianyong Dai, Ratan Guha, Joohan Lee,journal Of Computers, Vol. 4, No. 5, May 2009

#3. C. G. Cassandras, "Event-driven control communication and optimization", *Proc. Chin. Control Conf.*, pp. 1-5, Jul. 2013.

#4. Microsoft Antimalware Team, “Microsoft Security Intelli-gence Report (January - June 2015),” 2015.

#5. C. Nachenberg, “Computer virus-antivirus coevolution,” *Communications of the ACM,* vol. 40, no. 1.