INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

A study of signature-based and behaviour-based malware detection approaches

Adit Kumar Chakravarty
adit.chakravrty@gmail.com
S. J. C. Institute of Technology, Chikkaballapur, Karnataka

Aditya Raj
adi006raj@gmail.com
S. J. C. Institute of Technology, Chikkaballapur, Karnataka

Subham Paul
paulsubham100@gmail.com
S. J. C. Institute of Technology, Chikkaballapur, Karnataka

Apoorva S.
apoorvasgs28@gmail.com
S. J. C. Institute of Technology, Chikkaballapur, Karnataka

ABSTRACT

In the present scenario, one of the biggest threats to computers and mobile devices is malware. There are two approaches to detect and prevent malware infections: Signature-based and Behavior-based approach. The Signature-based approach is more widely used, but this outlook can only be used to detect existing and old malware and it does not allow understanding future threats and militating against these threats. The Behavior based approach uses a dynamic analysis method to understand and classify malware. However, it is still not as favored as its counterpart due to its limiting behavior. In this paper, we study both Signature-based and Behavior-based approaches to determine which the favorable approach to malware detection is.

Keywords— *Signature-based approach, Behavior based approach, Anomaly, Specification-based*

1. INTRODUCTION

Malware is a software that is designed to invade a computer or mobile device to harm the system and cause a negative impact on a user's security, reliability and privacy. Malware can be in the form of programs, scripts or any active content. Computer users require major security mechanisms in their systems to protect against the internet. **I.**

The number of malwares on the internet is getting more and more diverse and greater in number. Hence, existing malware detection methods are becoming obsolete and new techniques are required to efficiently tackle malware infections. In this paper, we will examine different malware detection techniques that use either Signature-based approach or Behavior-based approach.

2. ANTI-MALWARE ENGINE

The purpose of an anti-malware engine is to detect and eliminate malware when it tries to attack a computer. It has three main functions:

2.1 Scan the computer

The engine must examine the critical components of a computer, such as the main memory and the hard disk. In case there is some kind of anomaly in any component, it can mean that the system has been infected.

2.2 Detect the malware if present

After a component has been detected for anomalous behavior, it will be examined further to detect the presence of malware. The engine uses signatures of patterns of known malwares from a list called the Blacklist and verifies if the anomalous behaviour matches any of the available behaviours. In case they match, the malware will be classified according to the type of signature it matched to, such as virus, trojans, etc.

2.3 Elimination of the malware

After the malware is detected and classified, it is eliminated from the system and the computer is rolled back to a previous stable state. In some cases, the malicious file is isolated from other files.

3. SIGNATURE-BASED MALWARE DETECTION

Signature-based detection is a malware detection approach in which at least one byte of the code will be compared to an existing signature of already existing malwares, which are stored in a database known as Blacklist. The idea here is that most malwares are to be identified via patterns or signatures. This is the most commonly used malware detection approach. However, it has its own limitations:

3.1 Vulnerable to Evasion

Since this approach is based on signatures from known malwares, hackers can easily evade this technique by altering

the code, for example, changing the order of function blocks present in the code.

3.2 Zero-day Attacks

Signature-based detection will not be able to detect malwares that don't have their signature stored in the Blacklist. Also, this approach becomes less efficient if a varying form of the same malware attacks a system. Hence they are unable to detect malwares with diverse forms. Another major drawback to this technique is that as more and more signatures are added to the database, it becomes extremely large and difficult to handle.

4. WHITELISTING: AN ALTERNATIVE TO SIGNATURE-BASED BLACKLISTING

After hackers started to exploit Signature-based blacklisting, a new technique was introduced which was called Whitelisting. This technique also falls under the Signature-based approach. In this technique, only acknowledged software can be installed and executed on a user's computer. Any software that will not be in the whitelist will be strictly prohibited from executing in the system. Though Whitelisting is a proven method of protecting computers from external malwares, it creates a very inflexible domain where the users cannot freely download and use software. The other drawbacks of Whitelisting are:

- It creates an irritating user experience where the user will constantly be subjected to disturbance due to pop-up warnings and alert dialogue boxes.
- Malwares cannot be detected inside a whitelisted software. For example, if a browser is whitelisted then malwares can easily inject themselves into the browser without being detected.

5. BEHAVIOUR-BASED MALWARE DETECTION

Behavior-based malware detection approach observes the behaviour of software to ascertain if the software is malicious. When software is executed in the system, the behavior-based method analyses the executed code if notice if there are any anomalies from the regular sequence of the code. If an anomaly is caught, the behavior is compared to existing malicious existing behaviors and then eliminated once a match is found. The behaviours observed during the execution of the software are actually the system calls that are issued to the operating system.

Since Behavior-based detection does not only depend on the signature of existing malwares but also takes the operation of the software into consideration, it overcomes the drawbacks that were found in the Signature- based approach.

6. ANOMALY DETECTION: A BEHAVIOR-BASED MALWARE DETECTION TECHNIQUE

Anomaly detection is a major technique that falls under the Behavior-based malware detection technique. In this technique, the normal behaviour of software is stored as a reference. Any divergence from this normal behaviour will be marked as an anomaly.

The anomaly detection method can be better understood if compared to credit card fraud detection. Every customer that owns a credit card will have a "spending profile" stored in the database of the credit card companies. If there is any major divergence in the current expenditure records of the customer from the spending profiles, the profile will be marked as dubious. For example, if the spending records of a customer display that there has been an abnormal expenditure of money in a shop in Mumbai when the customer has not shopped in Mumbai for the past 3 years, then that transaction will be marked as an anomaly. In the same way, if the behavior-detection system observes write calls to a directory by a program that never writes to that directory, then that behaviour will be marked as suspicious as it will be an anomaly from the normal behaviour. However, this method has two drawbacks:

6.1 Vulnerable to false alarms

Some systems have complicated behaviors which makes it a complex task to build a model for the normal behaviour of the software. An inefficient model will lead to false alarms as a result of which wrong behaviours will be marked as an anomaly.

6.2 Vulnerable to mimicry attacks

In a mimicry attack, a hacker disguises his malicious code into a piece of code that falls under the normal behaviours of the software. In this case, the malware will not be detected. The anomaly detection method is vulnerable to mimicry attacks. However, for this, the hacker must know the normal behaviour of the software via which he wants to infiltrate the computer.

7. SPECIFICATION-BASED MONITORING METHOD

Specification-based monitoring method is a combination of the behavior-based detection approach and signature-based malware approach. Here, the events that occur from the program to the operating system are invigilated by a policy. Under this policy, actions such as "allow", "deny", or "log" is specified for any particular event.

For example, some browsers have a specified policy of not automatically executing any file that is downloaded from a website that is not listed on the Whitelist. Such specification policies are very useful in preventing infection of a computer via methods such as "drive-by- downloads". The advantages of Specification- based monitoring over Anomaly detection method are the following:

7.1 Increased resilience

In this method, policy fabrication will be separated from policy enforcement. It is possible that a policy can be induced by the anomaly detection method for specification-based monitoring. It is more extensive.

7.2 Lesser chances of false alarms

Enforcing policies that can be adjusted as required makes it easier to build models that may have lower chances of causing false alarms.

8. CONCLUSION

In this paper, we have studied the various advantages and disadvantages of the Signature- based and Behavior-based approach. The signature-based approach works best for malwares that are commonly found in systems but is weak against multiform and malwares with altered codes. In contrast, the Behavior-based approach works best for all kind of malwares. However, it falls short when malware is discussed as the normal behaviour of any software that is being monitored. Also, it creates a strict environment which may lead to user dissatisfaction and it may generate false alarms for several normal operations if the behavioral model of the software is not constructed efficiently. Lastly, it can be concluded that the Specification-based monitoring method is a far efficient technique as it encompasses both Signature-based and

Behavior-based approaches which give users sufficient protection and also good user experience.

9. REFERENCES

[1] http://en.wikipedia.org/wiki/Malware

[2] Mila Dalla Preda, Mihai Christodorescu, Somesh Jha and Soumya Debray, "A Semantics-Based Approach to Malware Detection", ACM Transactions on Programming Languages and Systems, Vol. 30, No. 5, Article 25, Pub. Date: August 2008.

[3] Yong Tang, Bin Xiao and Xicheng Lu, "Signature Tree Generation for Polymorphic Worms", IEEE Transactions on Computers, VOL. 60, NO. 4, APRIL 2011.

[4] Yoshiro Fukushima, Akihiro Sakai, Yoshiaki Hori and Kouichi Sakurai, " A Behavior- Based Malware Detection Scheme for Avoiding False Positives", 978-1-4244- 8915-2/10/$26.00 ©2010 IEEE

[5] Yong Tang and Shigang Chen, "An Automated Signature-Based Approach against Polymorphic Internet Worms", IEEE Transactions on Parallel and Distributed Systems, Vol. 18, NO. 7, JULY 2007.

[6] Wei Yu, Nan Zhang, Xinwen Fu and Wei Zhao, "Self-Disciplinary Worms and Countermeasures: Modeling and Analysis", IEEE Transactions on Parallel and Distributed Systems, Vol. 21, NO. 10, OCTOBER 2010.

[7] Asaf Shabtai, Eitan Menahem and Yuval Elovici, "F-Sign: Automatic, Function-Based Signature Generation for Malware", IEEE Transactions on Systems, Man and Cybernetics – Part C: Applications and Reviews, VOL. 41, NO. 4, JULY 2011.

[8] Ashwini Mujumdar, Gayatri Masiwal, Dr B. Meshram, "Analysis of Signature-based and Behavior-based Anti-Malware Approaches", International Journal of Advanced Research in Computer Engineering and Technology, Vol. 2, Issue 6, June 2013.

