International Journal of Recent Advances in Multidisciplinary Topics
Volume 2, Issue 10, October 2021
https://www.ijramt.com | ISSN (Online): 2582-7839

A Signature-Based Malware Detection System

Rahul Agrawal[1*], Yogesh Sharma[2], Harsh Awasthi[3], Pravin Landge[4]
[1,2,3]*Student, Department of Information Technology, SVKM'S NMIMS MPSTME, Shirpur, India*
[4]*Assisitant Professor, Department of Information Technology, SVKM'S NMIMS MPSTME, Shirpur, India*

***Abstract*: The advancement of the utilization of cell phones, for example, cell phones and tablets, has quickened as of late, as these gadgets have encountered a decrease in cost along with an expansion in usefulness and administrations accessibility. In this unique situation, because of its transparency and free accessibility, the Android working framework (OS) has gotten not just a significant partner in the market of cell phones however has likewise become an appealing objective for cybercriminals. In this undertaking, we backer to introduce some latest things and results in the Android malware investigation and identification research territory. We start by quickly portraying the Android's security model, trailed by a conversation of the mark-based malware investigation methods to give an overall perspective on the examination and identification measure. From that point onward, a depiction of a specific arrangement of programming improvements, which represent a portion of the talked about strategies, is introduced went with by a bunch of viable outcomes. At last, we make a few inferences about the future advancement of the Android malware investigation region. The fundamental commitment of this section is a depiction of the acknowledgment of static and dynamic malware investigation methods and rules that can be computerized and planned to program framework apparatuses to disentangle investigations. Additionally, a few insights regarding the utilization of calculations for malware orders and the utilization of the snaring programming procedures for signature examination execution are given.**

***Keywords*: Malware detection, Signature-based technique, Risk detection, Cyber security.**

1. Introduction

These days, cell phones, such as cell phones and tablets, have gotten exceptionally mainstream because of a decrease in their expense and an expansion in their functionalities and administrations accessibility. Also, the developing pattern of executing bring your own gadget (BYOD) approaches in associations has additionally added to the selection of these advances for ordinary correspondence exercises as well as to help to undertake systems, industrial applications, and business exchanges, which raise new security issues. Malware diseases have tormented associations and clients for quite a long time and are becoming stealthier and expanding in number constantly. Thus, this application is used to secure the user's device. In this task, we acquaint strategies with advance the utilization of lower-level miniature engineering highlights in the inconsistency-based identification of malware misuses. Existing malware location methods can be characterized along with two measurements, i.e., location approach and the malware highlight the target.

2. Procedure

The ability to scan & secure a device for general applications targeted at normal human-computer interaction is a core objective of Malware Detection.

1) Malware Detection

In this phase, the algorithm first detects the presence of malware and then tracks and keeps a count of detected applications that contain malware in it.

2) Signature-Based Detection

Mark-based identification is one of the most widely recognized methods used to address programming dangers levelled qat your PC. These dangers incorporate infections, malware, worms, Trojans, and the sky is the limit from there. Your PC must be shielded from an overwhelmingly huge volume of risks. Accomplishing this insurance is tremendously reliant on an all-around made, progressed, signature-based identification overseeing affairs. This kind of discovery includes your antivirus having a predefined archive of static marks (fingerprints) that speak to known organization dangers.

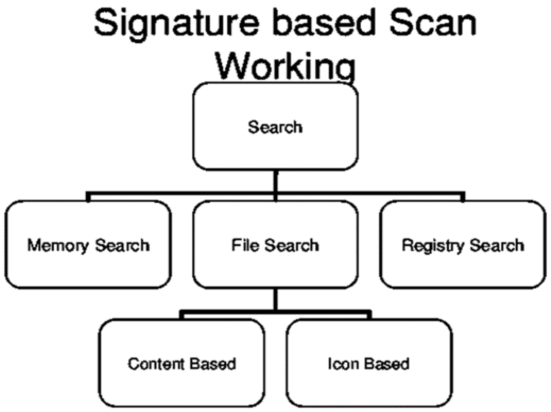

Fig. 1. Signature based scan working

*Corresponding author: rahul14.agrawal@gmail.com

3. Review Analysis

1) A user-centric machine learning framework for cyber security operations center- by Charles Feng [2017 IEEE (ISI), 2017, pp. 173-175, DOI: 10.1109/ISI.2017.8004902.]

Providing Cyber security is not an easy task. It is very complex, and from this paper, I understood how the SIEM (Security Information and Event Management) system is in place to normalize security events from different preventive technologies and flag alerts. The paper states that the SIEM (Security Information and Event Management) system is built-in for companies or governments to detect malicious activities & how SOC (Security Operation Centre) team develops so-called use cases with a pre-determined severity based on the analysts' experiences.

The main idea of the paper is to provide:

- A user-centric machine learning system that leverages big data of various security logs, alert information, and analyst insights to the identification of risky users.
- A novel data engineering process is offered, which integrates alert information, security logs, and SOC analysts' investigation notes to generate features and propagate labels for machine learning models.

Thus, the whole machine learning system is implemented in a production environment and fully automated from data acquisition, daily model refreshing, to real-time scoring, which greatly improves SOC analysts and enhances enterprise risk detection and management.

2) Machine Learning and Deep Learning Methods for Cybersecurity- by Yang Xin, Lingshuang Kong [IEEE Access(Volume: 6) DOI: 10.1109/ACCESS.2018.2836950]

The timely development of the Internet led to cyber-attacks and changes rapidly, and the cyber security situation is not optimistic. In this paper literature review of DL (Deep Learning) and ML (Machine Learning) methods for network security are present.

The main idea of the paper is to provide:

- Datasets for network intrusion detection for training and testing systems, the ML (Machine Learning) and DL (Deep Learning) methods cannot work without representative data, the research for ML (Machine Learning) and DL (Deep Learning) methods is still in progress.
- The ML (Machine Learning) and DL (Deep Learning) model needs to be retrained long-term and quickly, discussing the challenges of using ML/DL for cyber security.

3) Machine Learning Security: Threats, Countermeasures, and Evaluations- by Mingfu Xue; Chengxiang Yuan, Heyi Wu, Yushu Zhang, Weiqiang Liu [IEEE Access (Volume: 8) DOI: 10.1109/ACCESS.2020.2987435]

Machine learning security is a very active research direction. There have been a lot of works on tit-for-tat attacks and defenses in recent years. Machine learning-based applications are ubiquitous, yet machine learning systems still face a variety of security threats throughout their life cycles. Machine learning security is an active research topic and remains an open problem

The main idea of the paper is to provide:

- This paper can hopefully provide comprehensive guidelines for designing secure, robust, and private machine learning systems.
- The transferability can be used to launch attacks in black-box scenarios effectively. A general conclusion is that the threats are real, and new security threats are constantly emerging. For example, studies show that there is a transferability in adversarial examples, which means adversarial examples can generalize well between different machine learning models
- Machine learning security is an active research topic and remains an open problem. This paper presents a comprehensive survey on machine learning security covering the whole lifecycle of machine learning systems with respect to five major types of attacks and their corresponding countermeasures.

4) A Study of Cyber Security Challenges and its Emergning Trends on Latest Technologie- By G.Nikhita Reddy, G.J.Ugander Reddy. [International Journal of Engineering and Technology - UK ISSN: 2049-3444, Volume 4 No.1 January 2014]

Today the Internet is the fastest-growing infrastructure in everyday life. We are unable to safeguard our private information in a very effective way, and hence these days, cybercrimes are increasing day by day.The main idea of the paper is to give a brief introduction to Cyber Security, Cyber Crime. The paper also states about trends changing Cyber Security, how social media plays an important role in Cyber Security, & the importance of Cyber Ethics.

Some of the key points covered in the paper are:-

- Trends Changing Cyber Security: Web servers, cloud computing & its services, APT's & targeted attacks, Encryption of code.
- Role of Malware Scanners
- Role of Firewalls
- Role of Anti-virus software
- Cyber Security Techniques
- Cyber Ethics

5) Efficient signature-based malware detection on mobile devices- by Venugopal, Deepak | Hu, Guoning [Nokia Inc, 6000 Connection Dr, Irving, TX 75039]

The threat of malware on mobile devices has been gaining attention recently. It is important to provide security solutions to these devices before these threats cause widespread damage. However, mobile devices have severe resource constraints in terms of memory and power.

Some criteria for malware detection on mobile devices include:

- The detection method must use memory and computational resources efficiently and not drain the device battery.
- The detection method must have a low false alarm rate, i.e., considering a non-malware file as malware.
- The detection method must be easy/cost-efficient to update over the wireless network.

The impact of mobile devices and mobile malware on our daily lives cannot be underestimated. It is essential to give due attention to the computational limitations of mobile devices to design an effective solution. This paper, it is described signature-based malware detection that is well suited for use in mobile devices.

6) A survey on heuristic malware detection techniques- by Zahra Bazrafshan; Hashem Hashemi; Seyed Mehdi Hazrati Fard; Ali Hamzeh [The 5th Conference on Information and Knowledge Technology 10.1109/IKT.2013.6620049]

In this paper author investigated heuristic malware detection methods. Moreover, a brief overview of advantages, disadvantages, and features is given. Indeed, a high false-positive ratio is the most disadvantage of heuristic malware detection. Also discussed are malware detection methods and proposed a novel classification scheme for malware detection techniques. The author also had a brief overview of inadequacies in the malware detection methods and discussed how these shortcomings are covered by alternative methods and introduced the strategies used to defeat detection methods called "concealment strategies." The purpose of the paper is to present a procedure that could be suitable for further studies and to develop malware detection techniques.

7) Signature-based search algorithm- by S.A Khakoo [IEEE International Conference on Acoustics, Speech, and Signal Processing - Glasgow, UK (23-26 May 1989)]

In this paper, the authors discussed the frequency labeling search technique that significantly improves over commonly used motion estimation methods. The author had found that the importance of the high accuracy of this algorithm is considerably increased when the distortion function attains a significant minimum value at one location in the search space. Furthermore, the author had seen that the accuracy of our technique could be adjusted to different suit applications by changing the several coefficients used in the signature and the size of the candidate set. Such flexibility is absent from the accuracy of the other two algorithms. Finally, while it is computationally more expensive than other approaches, the computational cost falls within the range reasonable for real-time applications.

8) A Framework for Malware Detection Using Combination Technique and Signature Generation- by Zolkipli, Mohamad Fadli, Jantan Aman[IEEE Second International Conference on Computer Research and Development (ICCRD 2010) - Kuala Lumpur (2010.05.7-2010.05.10)]

This paper proposed a new framework for malware detection using a combination signature-based technique and GA technique. The framework will preserve computer systems, both well-known and new malware attacks. This is an essential contribution because zero-day malware attacks can be identified using the GA technique, and a signature will be created automatically by a generator that can be used by signature detection for future reference. To improve efficiency and better performance of computer operation, this research will be continued by implementing an integrated tool that can integrate all three main components of this framework.

9) A Study on the behavior-based Malware Detection Signature- by Barolli, Leonard, Xhafa, Fatos, Yim, Kangbin [A Study on The behavior-based Malware Detection Signature. 10.1007/978-3-319-49106-6(Chapter 66)]

This paper conducted an association analysis of the malicious behaviours of malicious apps, which were studied to generate the primary data for implementing the automated malicious app detection system, and the malicious behaviours of malicious apps that were collected by the system, and derived malicious app signatures that can be used for detecting malicious apps. Currently, the author is using this signature information to develop and test an algorithm for detecting malicious apps. Currently, available security systems related to malicious apps use the app installation APK file to check if there is any malicious code or use authority information, and the static analysis data of the source codes to detect malicious apps or conduct a dynamic analysis of network packets when they are executed to detect malicious apps. This paper analysed the domestic and overseas research and investigation data that has been confirmed so far, and the malicious apps that were collected, and conducted an association analysis of the derived malicious behaviors to derive the characteristics of the malicious behaviors of malicious apps (malicious app signatures). If this information is utilized, it will be possible to detect malicious apps more accurately. In the future, the author is planning to use the malicious app signatures derived in this paper to develop technologies and systems for detecting malicious apps.

10) Dynamic Signature-based Malware Detection Technique Based on API Call Tracing- by Oleg Savenko, Andrii Nicheporuk, Ivan Hurman, and Sergii Lysenko

Based on API call tracing, this paper describes a method for establishing a virus signature. A proposed form of signature is used to detect malware with this technique. The call frequency and type of interaction of crucial API calls comprise the program's behavior signature, which is based on API call tracing. The proposed signature allows us to distinguish malicious from benign applications by the existence of key API calls and their interaction. The efficacy of malware detection was found to be up to 96.56 percent in the trial results. he current malware detection technique, which uses a proposed form of a signature, has demonstrated good detection accuracy and is aimed at antivirus industry experts who work on malware analysis and database assistance. Like most dynamic approaches, our method has some limitations, which are mostly connected to the obfuscation and detection evasion strategies used by malware developers attempting to create stealth malware.

4. Challenges

Malware detection system faces many problems as discussed in these problems are:

- *Database Update:* The virus database should be updated at regular intervals to recognize any new malware.
- *Permission:* The user should always grant all permission required to perform a specific task

- *Background run issue*: The application is tracking malware in real-time, so it should run in the background process of the device all time.
- *Battery Consumption*: Since the application will run in the background, it will consume some amount of used battery.

5. Conclusion

The consistent turn of events and quick difference in the savvy gadgets market has expanded the number of administrations and applications advertised. As these gadgets coordinate with the client's regular exercises, they become alluring focuses for digital lawbreakers. In this sense, noxious programming (malware) has become a principal security issue in this territory. Even though malware is certifiably not another issue in the IT business, contrasts among PC and shrewd gadgets make savvy gadgets security an alternate issue limited to the specific highlights of cell phones.

References

[1] C. Feng, S. Wu and N. Liu, "A user-centric machine learning framework for cyber security operations center," IEEE International Conference on Intelligence and Security Informatics (ISI), 2017, pp. 173-175, 2017.

[2] Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," in IEEE Access, vol. 6, pp. 35365-35381, 2018,

[3] M. Xue, C. Yuan, H. Wu, Y. Zhang and W. Liu, "Machine Learning Security: Threats, Countermeasures, and Evaluations," in IEEE Access, vol. 8, pp. 74720-74742, 2020,

[4] Gade, Nikhita Reddy & Reddy, Ugander. (2014). A Study of Cyber Security Challenges And Its Emerging Trends On Latest Technologies, 2014.

[5] Venugopal, Deepak and Hu, Guoning. 'Efficient Signature Based Malware Detection on Mobile Devices'. 1 Jan. 2008: 33 – 49. Print.

[6] Z. Bazrafshan, H. Hashemi, S. M. H. Fard and A. Hamzeh, "A survey on heuristic malware detection techniques," The 5th Conference on Information and Knowledge Technology, pp. 113-120, 2013.

[7] Z. Bazrafshan, H. Hashemi, S. M. H. Fard and A. Hamzeh, "A survey on heuristic malware detection techniques," The 5th Conference on Information and Knowledge Technology, pp. 113-120, 2013.

[8] S. A. Khakoo, "Signature-based search algorithm," International Conference on Acoustics, Speech, and Signal Processing, pp. 1874-1877 vol.3, 1989.

[9] M. F. Zolkipli and A. Jantan, "A Framework for Malware Detection Using Combination Technique and Signature Generation," 2010 Second International Conference on Computer Research and Development, pp. 196-199, 2010.

[10] Oh, Sungtaek & Go, Woong & Lee, Taejin. A Study on The behavior-based Malware Detection Signature, pp. 663-670., 2017.