GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A NOVEL HYBRID NETWORK TRAFFIC ANALYSIS BASED MALWARE DETECTION

Prof. Rama Prabha.K.P
School of Information Technology and Engineering, VIT University
Vellore-632014, Tamilnadu, India

ABSTRACT

Malware present in any system is one of the vulnerability which becomes harmful for the system by leaking the sensitive information to the remote server. Mobile malware use to transfer the sensitive and vital information of the cell phone to the remote server which stores and analyze the information which may cause a serious threat to the security of the cell phone data. This paper focuses on implementing a hybrid approach to detect malware in a system . In this method we are detecting the malware by maintaining a record for black listed threats which we call a trusted domain backlist. By making use of this domain black list it is possible to detect the vulnerabilities happening often in a system. The proposed system also focuses on whitelisting, a popular technique used to prevent unauthorized programs from running in a user system. Also the system attempts to assess the risk that code is malicious based on characteristics and patterns. Overall the paper aims towards designing an intellectual system which will be of prime importance in malware detection there by making a cell phone as more secured device.

Keywords- *malware, remote server, blacklisted domains.*

I. INTRODUCTION

Today more than 70% of electronics devices run the Android operating system. Smart phones and tablets are widely using devices based on Android Operating system. Android operating system has some important features such as open nature and relatively less restrictions on application distribution system. Due to which it has always been an attractive platform for malware.

But Kaspersky Labs and INTERPOL published a report on Android based devices and 20% of such devices uses their software were atta| cked at least once by malware. Mobile m| alware is malicious software that is specifically built to attack mobile phone or smartphone systems. These types of malware rely on exploits of particular operating systems (OS) and mobile phone software technology, and represent a significant portion of malware attacks in today's computing world, where mobile phones are increasingly common. Mobile malware generates the threats for users, because mobile generally store some confidential data such as important contacts, credit/debit card information, private photos and messages, bank account details and other sensitive information that can be leaked.

Just because of the tremendous incre| ase in growth of Android malware, various effective malware detection methods are required. There are two types of mal| ware detection methods are exist such as sta| tic (code analysis) and dyn| amic (runtime/behavioral analysis). It is hard to detect sne| akiest ma| lware using static analysis, because they can easily affect by the malicious code with help of random keys. Also some malware download the malicious code at runtime and remove it after execution. There exist some static and dynamic malware detection methods in the literature to detect the malware for known malware signature. This paper presents network traffic analysis based malware detection method. This method is effective against malware that communicte with malicious remote servers. In this method, databases of known malicious domains are used and applications that contact to the malicious domains can act as a malware. This paper describes all the details of detection method by providing the information about tools and techniques required for it.

Rest of the paper is organized as follows, Section II explained the literature survey, Section III describes the malware detection procedure in two different steps, Section IV gives the details about malware detection process.

II. RELATED WORK

Chandramohan et al. [3] has given a high-level overview of various detection methods. Zhou et al. [2] collected, classified and published a large collection of 1260 Android malware. Presented system uses the malware samples from their collection to evaluate detection method. Isohara et al. [4] demonstrated a system-call logging based method. But there exists no work that demonstrates network traffic-based malware detection method in details. This paper demonstrates the network traffic-based malware detection analysis and provides the better solution.

III. MALWARE DETECTION PROCESS

In this paper a combinational effort of signature based detection and behavioral profiling is put into action for detecting and avoiding malware.

A. Signature based detection

A signature based detection system focus on specific security issues. It is a security filter that operates somewhat like a law enforcement officer who seeks to identify criminals based on their *modus operandi,* or mode of operation. Specific actions and/or code sequences are compared against a database of known signatures, or predefined strings in code that are indicative of malware. In signature based detection both blacklisting and whitelisting are carried out for efficient malware detection.

This blacklisting process is furt her subdivided into four tasks:
1] Monitoring information sources
2] Collecting malware samples
3] Executing samples matching the top threats
4] Conducting a detailed analysis of malware's behavior

1] Monitoring information sources

The information sources from various major security vendors are monitored and a database is maintained for currently active threats. It is a process of Data aggregation where Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.

2] Collecting malware samples

A large collection of malware samples are collected, classified and correlated against the stored threat databases. Samples are collected using honeypots and from known malicious URLs. **Correlation** looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information.

3] Executing samples matching the top threats

The samples collected are executed by comparing the current signature against the top threats in a sandbox environment.

4] Conducting a detailed analysis of malware's behavior

A detailed analysis of malware's behavior is performed and a new signature is built if a sample fails to trigger a signature.

Whitelisting

Whitelisting is a popular technique that allows only approved software to install and run in a system. Software products that are not explicitly on the control list lock down the system. Whitelisting is simple and gives the administrator/company the most control over what comes into the network or runs on the machines. The advantage of whitelisting is that nothing that is not on the list can run or get through.

B. Behavioral profiling

Behavioral methods attempt to assess the risk that code is malicious based on characteristics and patterns. Signature and anomaly based security mechanisms perform a type of behavioral based security. Files and programs that are likely to present a threat, based on their behavioral patterns, are blocked. Online behavioral profiling is based purely on a limited set of user actions collected by detection systems. That is why current detection systems have opted to analyze normal user behavior, define a normal user profile and then raise a red flag if an action outside of that "normal" profile occurs.

IV. CONCLUSION

This paper describes the different types of m| alware detection techniques and their effectiveness with specific types of
malware. System Provides the behavioral detection method for detecting mobile
malware that can commu| nicate with
blacklisted domains and pass sensitive personal / financial information.

REFERENCES

1. *Kaspersky Lab and INTERPOL Survey Reports, "Mobile cyber threats."*
2. *Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in IEEE Symposium on Security and Privacy, San Francisco, CA, May 20-23, 2012, pp. 95–109.*
3. *M. Chandra Mohan and H. B. K. Tan, "Detection of mobile malware in the wild," IEEE Computer, vol. 45, no. 9, pp. 65–71, Sep 2012.*
4. *T. Isohara, K. Takemori, and A. Kubota, "Kernel-based behavior analysis for android malware detection," in Internation Conference on Computational Intelligence and Security, Hainan, Dec 3-4 2011, pp. 1011–1015.*
5. *Netstat command.*
6. *Wireshark, A network protocol analyzer for Unix and Windows.*
7. *Shark for Root, an android application to capture incoming and outgoing packets.*
8. *Android Debug Bridge.*
9. *Strace, a diagnostic userspace utility for Linux.*
10. *Mehedee Zaman, Tazrian Siddiqui, Mohammad Rakib Amin, Md. Shohrab Hossain, "Malware Detection in Android by Network Traffic Analysis", IEEE Computer,2015.*
11. *The Case for Network-based Malware Detect ion* ***www.alcatel-lucent.com***