ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 13 -18 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

Detection Of Malware Using Signature Based Algorithm Undergoing Database Verification

P Sai Ram[1], A Sri Harsha[2], E Uma Shankari[3], N V Krishna Rao[4]
[1]B Tech CSE Dept., Institute Of Aeronautical Engineering, India, sairam.iare@gmail.com
[2]B Tech CSE Dept., Institute Of Aeronautical Engineering, India, Harsha14700@gmail.com
[3]Assistant Professor CSE Dept., Institute Of Aeronautical Engineering, India, umashankari.917@gmail.com
[4]Associate Professor CSE Dept., Institute Of Aeronautical Engineering, India, krishisri@gmail.com

ABSTRACT

Due to the change in working, the rate of change from traditional phones to smartphones is huge. This is because that smartphones provide a large number of apps for users to be downloaded and installed. However, this indicates that the devices can be easily attacked by some third party users by spreading malware through various apps. This is a serious problem and it should be addressed by both preventive methods and effective detection techniques. This article first discusses about the vulnerability of smartphones to various security attacks. Then it presents behavior of different types of malware and their threats. Next, it reviews the existing malware prevention and detection techniques. Besides more research in these directions, it points out efforts from all the stake holders required to defend against such malware.

KEYWORDS:

Defenses, Malware, Mobility, Smartphones.

INTRODUCTION

Smartphones grew in number year-by-year when compared to traditional mobile phones because smartphones are general-purpose handheld devices which provide computing and communication and they support multimedia communications, they also support different entertainment applications. Due to the change in user requirements and due to change in the demand of new features, the traditional mobile phones have been updated into smartphones with in no time. According to the IDC (International Data Corporation), over one billion units of smartphones were shipped worldwide.

This indicates that more and more people have started using smartphones when compared to the traditional mobile phones. This is because of the increase in the features provided by the smartphones. There will come a day where every person will have a smartphone. And the most important feature is that the user can install and run whatever application needed and the applications which aren't provided by the smartphone. This makes it more flexible to the user.

These applications are provided in the app stores namely Google Play for Android platform and Apple App store for iOS platform. These app stores are the places where different app developers can upload their applications and different users can download the needed apps. And the main problem arises here as majority of these apps lack basic security and many other apps are malware prone. The greedy app developers or some third party developers can easily embed malware into these apps and can easily spread those infected/malicious apps to different smartphones via these app stores. It is believed that there are a millions of malicious apps in both Google Play and Apple App store. This is a serious security issue and if any user downloads any of these apps, then there is a serious security problem over his information.

In the rest of the article, we will see the different types of threats caused by malware, what makes smartphones vulnerable to these attacks, what are the issues faced due to these malware and what are the defensive techniques to be applied. We will also see about the different stake holders, what are the efforts required to be put in by these stake holders to prevent these malware. We will then conclude with the future research work required to prevent the malware.

MALICIOUS BEHAVIOR

Mobile malwares can be identified though their propagation behavior, remote control behavior, and malicious attack behavior. How the malware is transferred to victims is referred to the propagation behavior. The remote control behavior shows how the mobile malware exploits the infected device with the help of a remote server. The attack behavior refers to how the malware, after infecting a victim's devices, attacks the devices via different communication channels (e.g. Bluetooth). Once the malware gets into the user's device, it will start showing its effect and it will try to gain the access over the vital information of the user like account details, several important transactions, etc. that may take through smartphone.

THREATS OF MALWARE

Before going into the concept of how to defend the malware attacks, it is important to know about the different types of attacks caused by malware and the damage done by them. Then we can know about how to defend them.

1. Phishing Attacks:

A phishing attack is a well-known threat for PC users. This type of attack does not need to attack the user's systems in any way. It is a platform-independent attack and can readily be applicable to smartphones. The malware only needs to contain

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 13 -18 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

URLs of faked web sites, which masqueraded as trusted web sites, to steal personal information such as credit card details. It has been found that approximately 25 percent of malware contains suspicious URLs. There are several reasons for hackers to choose smartphones to phish users. First, it is easy to disguise infected apps as legitimate apps and distribute them in app markets. Second, smartphones tend to have a small screen, so it is easier to disguise trust cues on which users rely to decide whether it is risky to submit credentials, for example, cues that indicate whether the site is enabled by Secure Sockets Layer. Third, there are various channels in smartphones that hackers can use for phishing, example, instant messaging, short message service (SMS), and so on. Fourth, users are often not aware that phishing can be a risk on smartphones. Also, many users trust their smartphones more than their PCs. Consider an example of any online shopping website. It consists of a page for transactions. Here, a user will enter all his/her credentials so that the transaction will be taken place successfully. But in some situations, the URL of these pages would be replaced by a fake one and the page layout would similar or almost same as the original one. So, when a user enters all the details, he/she might think that their data is entered in the correct place, but actually what happens is that their details are stolen with the help of a fault page without their knowledge. Thus their details can be incurred.

2. Spyware Attacks:

Malware that covertly collects user's various information stored in their infected smartphones are referred to as spyware. The amount of personal data and sensitive information stored in and processed by smartphones makes them attractive targets for spyware. Moreover, covert channels are available in smartphones for returning collected information to hackers. Sometimes, even when an app seems to have a legitimate need to send data to the outside world, the permission settings of smartphones may not be granular enough to prevent abuse of such a permission. For example, a weather app can have the permission to send location data to some weather information servers, but if it is implanted with spyware, it can abuse the permission by sending the same location data to advertisement servers for spamming marketing information. Depending on the type of information being collected, different levels of damage can be incurred. In the above example where user's location information is used to trigger spam messages, users are only annoyed. However, if more sensitive information is collected, more serious damage can be done.

3. Surveillance Attacks:

Smartphones are commonly equipped with sensors such as a Global Positioning System (GPS) sensor, accelerometer, microphone, and camera. Combined with the fact that they are closely associated with their owners, smartphones infected with suitable spyware can be used to keep targeted users under surveillance. In particular, the GPS sensor is particularly useful as it can provide highly sensitive personal information. There are already examples of legitimate apps that are exploited by hackers to keep the targeted users under surveillance. Moreover, even apps that are not originally designed as spyware may be covertly configured to support tracking. For example, consider a room or a location which is under the control of an organization. They have decided to track everyone who are in that region. Then, every person who enters that specific region will get tracked by that organization without the knowledge of that user.

4. Diallerware Attacks:

Hackers can gain access over financial charges to smartphone users by diallerwares, which send premium-rate SMS messages without user's awareness. The original purpose of premium-rate SMS messages and calls were to provide value-added services such as news and stock quotes, with the cost being charged in the user's phone bills. Premium-rate calls are abused for the hacker’s profit under this attack. Hackers lure owners of infected smartphones into signing up premium-rate services controlled by themselves. For example, HippoSMS is an Android malware that sends SMS messages to a premium-rated number. It blocks SMS messages from service providers so that users are not aware of the unwanted additional charges.

5. Financial Malware Attacks:

Financial malware aims to steal credentials from the smartphones or perform man-in-the-middle attacks on financial applications. Similar to PCs, smartphones are also vulnerable to financial malware. Financial malware may simply be a key-logger that collects credit card numbers. In a more sophisticated form, it may be an app impersonating a real banking app. If users download and run the app, the hacker can launch a man-in-the-middle attack for banking transactions.

6. Worm-Based Attacks:

A worm can damage and compromise the security of smartphones. Moreover, it duplicates itself, typically propagating from one device to another, using different means through an existing network without the users’ intervention. In fact, worms can be easily spread by just one click to infect smartphones in any part of the world with a large chance of success. Moreover, as network function virtualization will be introduced into next generation mobile networks to reduce capital and operating expenditures, worm-based attacks to the virtualization environment and hence to smartphones are expected to increase.

7. Botnets:

A botnet is a set of zombie devices that are infected by malware so that hackers can remotely control them. When a number of smartphones are compromised and remotely

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 13 -18 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

controlled, a mobile botnet is formed. Botnets impose serious security threats to the Internet, and most of them are used in organized crime, launching attacks to gain money. Some examples include sending spam, Denial-of-Service attacks, or collecting information that can be used for illegal purposes. Once a smartphone is infected, it becomes a zombie for cyber-attacks.

All these attacks are done through specific malware which are generally hidden in an app and then, those apps are spread throughout the app stores.

The table 1 shows us the different types of attacks caused by malware.

Table 1: Different types of attacks launched by malware

Attack	**Description**
Phishing	Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details and sometimes, indirectly, money, often for malicious reasons.
Spyware	Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
Surveillance attacks	A specific user will be monitored closely with out his/her concise and this is basically done by adding few apps or sensors to user's smartphones and basically without their knowledge.
Diallerware attacks	User's money will be stolen with the help of a malware that makes hidden calls or sends SMS.
Financial malware attacks	User's credentials are stolen through performing Man-in-middle attacks.
Worm-based attacks	It is a malware program that replicates itself in order to spread to other devices. Unlike virus, it doesn't needed to be attached to any other program.
Botnets	It is a malware, by which, when a smartphone gets infected, can be accessed through a remote device.

WHAT MAKES SMARTPHONES VULNERABLE TO MALWARE

There are a lot of factors which make smartphones vulnerable to security attacks, and these are given below.

First, smartphones contains the personal data of that particular user. In particular, financial transactions such as online banking and shopping are carried out by more and more users from their smartphones, some data can be very sensitive. So, these data can be easily be hacked by the hackers with the help of some malware and the user will not be even aware of that.

Second, more smartphones are based on the same platform (Android). Android has a policy of open-source kernel, with the help of which, the malware writers can gain a deeper understanding of the mobile platform. This makes the development and publishing of third party apps easy to gain market share. As a result, there is a wide scope for the hackers to create and publish malware. At the same time, as users download and install a lot of apps for their smartphones, the chances of installing malwares increases as well.

Third, most users feel that their smartphones are just mobile phones, where a number of apps related to either communication or entertainment are installed and they just use those apps. They are not aware of the fact that the smartphones are almost the replacement of the computers and also they aren't aware that their smartphones are vulnerable to cyber-attacks. As a result, they do not pay enough attention towards the security measures. Moreover, the user installs what-ever app he/she needs without even knowing about the app permissions or any security issues. This makes the smartphones more vulnerable to security issues.

ISSUES FACED DUE TO MALWARE

Compared to computers, there are a different number of security principles in smartphones. In particular, the multiple technologies to access the internet makes the smartphone more prone to security attacks. The following three factors distinguish mobile security from traditional computer security:

• Mobility: Smartphones have high mobility. They are carried to each and every place by its user. Therefore, the risk of being stolen or physically damaged is more in the case of smartphones.

• Strong personalization: Generally, there will be only a single owner to each and every smartphone. This means that every person's personal data would almost be stored in their smartphone. This makes them more vulnerable of the data being stolen.

• Strong connectivity: People connect to different websites in internet through different apps in their smartphones. This means that they visit a lot of locations every-day, in which, they may also visit the websites which are infected with some malicious code or program. Therefore, without their knowledge, the malware gets into the user's smartphone.

Also, smartphones have limited resources of power, memory and processing speed when compared to a computer. This means that a lot of programs or apps would not be supported by them. In the same way, many complex malware detection algorithms may not be supported by them.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 13 -18 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

DEFENSE TECHNIQUES

Defense techniques against malware may include either prevention of malware from entering into the smartphones or the removal of malware which is present in the user's smartphone.

Prevention techniques:

The prevention techniques are used to prevent the malware from entering into the smartphones of users. This can be achieved with the co-operation of all the stake holders. Who are the stake holders? What is their role? These major points are discussed below.

There are majorly three different stake holders. The app developer, the app store administrator and the smartphone user itself. The roles of each and every stake holder are as follows:

1. Application Developers:

Application developers should make sure that their apps follow all the policies governing secure coding and privacy and they should not access unnecessary information. Then, it would be difficult for the malware to reside in the applications based on their security weakness and hence it makes difficult for a malware to attack a smartphone. For example, developers can use some unique identifier or some unique numbers instead of the IMEI number. Also, the important and sensitive information stored locally or sent to remote servers should be encrypted. If third-party libraries are used in the development of apps, proper care should be taken by appropriate mechanisms. Moreover, while Android apps have about 100 built-in permissions that control operations such as dialing the phone and sending short messages, developer should take care that only the required permissions are given to the app, thus the use of such permissions should be minimized. Since smartphone users generally just use the default settings, careful use of built-in permissions by application developers is particularly important. And moreover, the app developers should provide additional security features to their applications against different security attacks.

2. App Store Administrators

Administrators of app stores should strictly check every uploaded app, and proper action should be taken against the malicious apps. Recently, server-side vetting processes have been developed to detect and then remove malicious apps from app markets with varying levels of success. Moreover, this helps the developers if administrators have a well-defined security policy. For example, app should send confirmation to Apple's security rules before they can be distributed via the App Store. Apple approves apps though a mechanism code signing with encryption keys. Apps can be installed in iPhones only through downloading the apps present in the Apple App store. This makes sure that only the apps which satisfies all the rules and conditions can be downloaded by the user.

3. Smartphone Users

Smartphone users play a vital role in preventing malware from entering their devices. They should only install the apps which are highly reliable and only the apps which they need the most. Generally, any user install different types of new apps without having a proper knowledge about them. There are many apps in the app stores that ask for a huge number of permissions, which, aren't required in truth. But any user doesn't check these permissions before installing any new app. This means that the user is directly or indirectly allowing the malware to enter into his smartphone. And moreover, many people keep their WiFi and Bluetooth on all the time, which makes proximity malware to get into their smartphones.

So, user should always check for app permissions and should have at-least basic knowledge on the apps to be downloaded and should always be careful with different wireless networks.

Therefore, one can say that the prevention of malware can be achieved only with the co-operation of all the stake holders which is shown in the Fig 1.

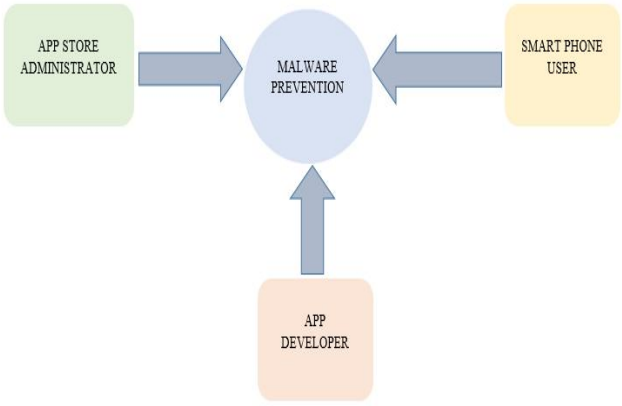

Fig 1: Co-operation among stake holders

DETECTION TECHNIQUES

Till now, the malware detection were done basically using two techniques, either signature based or anomaly based. Signature detection involves searching network traffic for a series of bytes or packet sequences known to be malicious. A key advantage of this detection method is that signatures are easy to develop and understand if you know what network behavior you're trying to identify. For example, you might use a signature that looks for particular strings within an exploit payload to detect attacks that are attempting to exploit a particular buffer-overflow vulnerability. The events generated by a signature-based IDS can communicate what caused the alert.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 13 -18 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

With anomaly-based techniques, the normal system behavior is taken into consideration first. Then the malware is detected whenever the system behavior doesn't match with the modeled normal behavior.

The detection techniques are classified into different techniques and those are shown in the Fig 2.

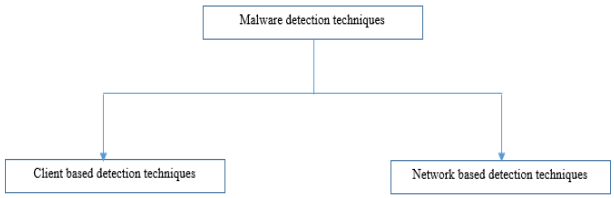

Fig 2: Classification of detection techniques.

Based on the perspective of the location where these malware detection goes place, there are two major domains, namely Client based detection and Network based detection, which, is also shown in the Fig 2.

Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulation network intrusion detection systems.

Host Intrusion Detection Systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

RELATED WORK

All these above techniques require a lot of computing time and would require a lot of resources. In the modern day technology, this is also a major issue. So, what is required to reduce the computing time? Should we reduce the complexity of algorithms? This isn't a good idea since reducing the complexity means that we are allowing our smartphones to host a number of malwares.

So, the key solution would be to link up the detection algorithm with a database. Every app is classified into a particular category and each category of app should contain the specific number of permissions.

Suppose, an app contains huge number of permissions than required, then, that app may be malicious. So, different categories of apps present in the market, what are the required permissions for each category are maintained in that database. Also a list of potential malicious apps will also be maintained. This means that when-ever any new app is downloaded by the user, that specific app should undergo a database verification before applying detection algorithms on it. Which means that majority of the malicious apps would be detected there itself. But it is not 100% accurate and sometimes, the results may be misleading. Therefore after applying the database verification, if the malicious app isn't detected, then, the detection algorithms will be applied on them. The only problem with the database is that it requires more space. And moreover, the database is needed to be updated on day-to-day basis.

Though it has few disadvantages, the computing time can be reduced and many malicious apps can be detected which aren't thought to be so. One more additional feature is that the database can provide the data about the permissions that an app may require. Thus, the addition of database will detect malware and will also provide basic knowledge about the apps to the user. To make this happen, the co-operation of app store administrator and app developer. App developer should provide the required permissions for each category of app and the app store administrator should co-operate for time-to-time updating of database. Instead, one more idea is to provide the same database in the app store itself and then the database verification may take place at app store server. This means that the majority of the malicious apps can be detected at the app store itself and it can be deleted from the app store.

CONCLUSION AND FUTURE WORKS

On a whole, we can say that the market penetration of smartphones would increase in the future. This also means that the malware distribution will also increase rapidly. Efforts are required from all the stake holders to keep the malware at bay.

Even though the existing preventive approaches and detection tools can help prevent some of the attacks, the behavior of malware is changing rapidly and malware developers always find a number of ways to attack the smartphones. Therefore, advancements are needed in the

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 13 -18 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

malware detection algorithms to detect multiple types of malware successfully. Moreover, the limited resources in mobile devices should be taken into account in the design of such sophisticated software. We may assume that in the future the task of identifying malware attacks on smartphones will be shared between the cloud and the device. The computationally intensive tasks should be carried out in the cloud, while detection by reduced classification schemes can be carried out locally by the device. We conclude this article by suggesting the following future research directions.

More attention should be paid on the emerging types of the malware as most of the malware are hidden in the third party apps. The databases should be made available to publically, so that everyone can access the database and can know about the different malwares.

A change is required in the users, who generally think that smartphones are just normal handheld mobile devices. They should know that the smartphones are almost substitute to computers. Users should install the apps very carefully and should have a very good idea about their device.

Most of the malware are created by app developers and then they are embedded into other commonly used apps. So care should be taken such that any type of malware cannot be created in the app developing software. Few defensive techniques should be implemented such that the malware cannot be coded at all. If the malware isn't created, then it cannot be spread in any means.

REFERENCES

[1] Daojing He, Sammy Chan, Mohsen Guizani, "Mobile Application Security: Malware Threats And Defenses", Wireless Communications, IEEE, Vol. 22, pp. 138-144, Feb. 2015.

[2] S. Ramu, "Mobile Malware Evolution, Detection and Defense", EECE 571B Unpublished Term Survey paper, pp. 1-4, April 2012.

[3] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices", IEEE Communication Surveys & Tutorials, Vol. 15, pp. 446–71, First Quarter 2013.

[4] Pang-Chieh Wang, Jun-Yu Chen, Shu-Fen Yang, "A practical approach to manage applications and prevent malware spreading in mobile environment", Consumer Electronics (GCCE), IEEE 3rd Global Conference, pp. 549-550, 2014.

[5] Pieterse H, Olivier M.S, "Security steps for smartphone users", Information Security for South Africa, pp. 1-6, 2013.

[6] Khurram Majeed, Dr Yanguo Jing, Dr Dusica Novakovic, Prof Karim Ouazzane, "Behaviour Based Anomaly Detection for Smartphones Using Machine Learning Algorithm", International conference on Computer Science and Information Systems, pp. 67-73, 2014.

[7] Min Zhao, Tao Zhang, Jinshuang Wang, Zhijian Yuan, "A Smartphone Malware Detection Framework based on Artificial Immunology", JOURNAL OF NETWORKS, Vol. 8, pp. 469-476, FEBRUARY 2013.

[8] Ashwini Mujumdar, Gayatri Masiwal, Dr. B. B. Meshram, "Analysis of Signature-Based and Behavior-Based Anti-Malware Approaches", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), Vol. 2, pp. 2037-2039, June 2013.

[9] Imtithal A. Saeed, Ali Selamat, Ali M. A. buagoub, "A Survey on Malware and Malware Detection Systems", International Journal of Computer Applications (0975 – 8887) Vol. 67, pp. 25-31, April 2013.

[10] Penning, N., Hoffman, M., Nikolai, J., Yong Wang, "Mobile malware security challeges and cloud-based detection", Collaboration Technologies and Systems (CTS), 2014 International Conference, pp. 181-188, 2014.