ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com
Journal DOI:10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

An Approach to Network Traffic Based Android Malware Detection.

***Prashant B Amrute[1], and V. Joseph Raymond[2].**

1. Information Security Cyber Forensics, Department of Information Technology, Faculty of Engineering and Technology, SRM University, Chennai, India.
2. Assistant professor, Department of Information Technology, Faculty of Engineering and Technology, SRM University, Chennai, India.

Manuscript Info

Manuscript History:

Received: 16 March 2016
Final Accepted: 22 April 2016
Published Online: May 2016

Key words:
Malware, Trojan, spyware, logact

****Corresponding Author***

Prashant B Amrute.

Abstract

Now a day, demand of smart phone apps is at its peak level. Every day millions of apps are uploaded and many of them are vulnerable which will compromise our important phone data. There are many techniques have evolved which will help the user to detect such malware and stay protected. But none of the existing malware detection technique mainly focused on the malware detection by using the network traffic behavior. In the following proposed work, malware detection phase is completely different. We will find out the Spyware, Trojan kind malware and also the application which carried out this work. We will compare the traces with the reference feature parameters and detect the suspicious behavior.

Introduction

There is a tremendous amount of growth in smart phone users these days. Most of the users use their smart phones for online banking, messaging, Google map, internet surfing, etc. More than 75% of total market share consumed by android operating system. The number of malicious applications targeting the android system are also explored in recent years. The attackers use new techniques to compromise your smart phones data.

So, the security of your device is a very important question. We are having a different techniques to carry out detection of the different malwares. These techniques and their limitations are as follows
Signature-based detection works by scanning the contents of computer files and cross-referencing their contents with the "code signatures" belonging to known viruses. Clearly there will always be new and emerging viruses with their own unique code signatures. So once again, the anti-virus software vendor works constantly to assess and assimilate new signature-based detection data as it becomes available, often in real time so that updates can be pushed out to users immediately and zero-day vulnerabilities can be avoided. [9]

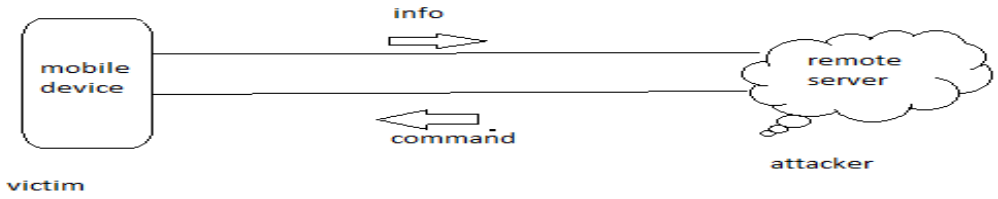
Behavior-based malware detection system is composed of several applications, which together provide the resources and mechanisms needed to detect malware on the Android platform. Each program has its own specific functionality and purpose in the system and the combination of all of them creates the behavior-Based malware detection system. [9]

Application permission based malware detection approach is, applications run in a sandbox environment however they need permissions to access certain data. At the time of installation, Android platform asks the user to grant or deny permission for the application based on the activities the application can perform. [9]

Cloud Based Malware Detection, Google Play applications are scanned for malware. Google uses a service named Bouncer to automatically scan applications on the Google Play Store for malware. As soon as an application is uploaded, Bouncer checks it and compares it to other known malware, Trojans, and spyware. Every application is

run in a simulated environment to see if it will behave maliciously on an actual device. The applications behavior is compared to the behavior of previous malicious apps to look for red flags. [9]

Most of the applications communicates to their particular remote server. When a hacker use an application to compromise victim data it will gather the data from victim's device and leaked to the remote server. Spyware are these kind of malwares who particularly do such kind of work. [1]
Whatever techniques present today to detect malwares of smart phone, none has particularly focused on detection based on network traffic.
By analyzing network traffic of smart phone we can verify that whether it's a vulnerable one or not.



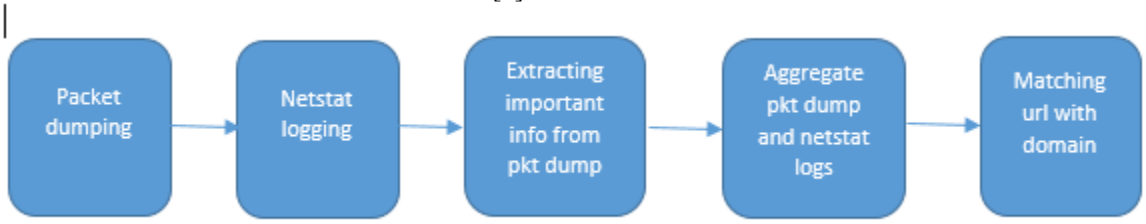
Name	Based on	Features
Signature based	Code signature Pattern matching	Ignore semantic of instruction (allow malware obfuscation)
Behavior based – static	Decompress, disassemble Search for pattern	To know malware pattern
Behavior based – dynamic	System call	Highly resource consuming
Application permission	Permission (grant/deny)	Default user policy
Cloud based	Application verification service	Novice user fail to verify

Background Theory:-

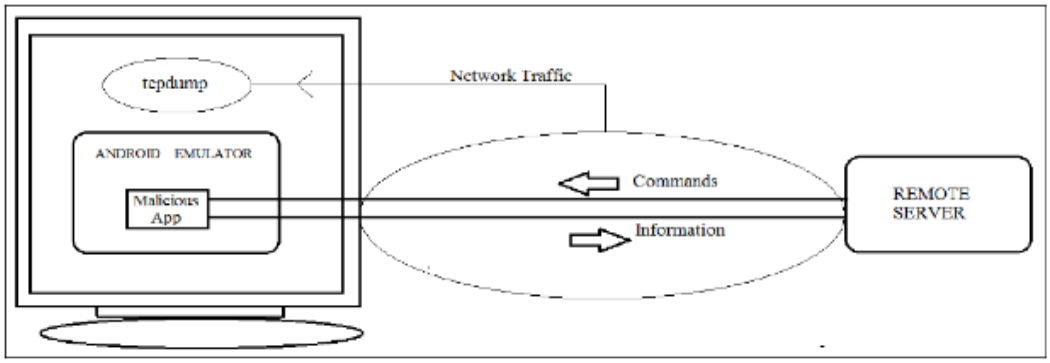
Related Works:-

Anubis is a service for analyzing malware files. We have to submit the windows executable file or android APK file and after analysis you will receive an analysis report about what the file is does. We can submit any URLs too. For that also it will provide an analysis report.

Virus total is also a service for analyzing malware files. Working is same as Anubis.
Droid Box is a dynamic malware analysis tool.
In a paper of 'Mehedeezaman' and 'Tazriansiddiqui' demonstrate a detection method based on network traffic. It is based on logging the URLs of all the remote locations that are contacted by application for a specific period of time. They have a database of known malicious domain. The application contact any of those malicious domain can be flagged as malware. In this case we have to update malicious domain list on regular basis. It will be difficult if any server which is malicious and it's not there in list. [1]

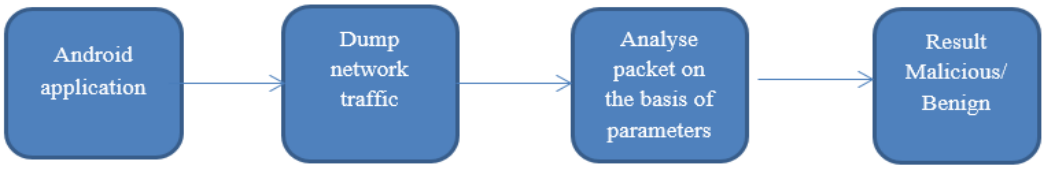


In another paper by 'Anshul Arora' amd 'Shree Garg', they differentiate the normal mobile traffic and malicious traffic on the basis some parameters and features of packet. They create a table regarding traffic features and the parameters of packet like size, incoming and outgoing flow ratio, duration of sent and received packets. They didn't mention the dumping process of a network packet. They only shows that if any application sending data to malicious server then it's flow ratio, size of packet will vary from normal traffic.[2]



Proposed work:-

In this proposed system for analyzing network traffic, take the network dump and find out which device generate that traffic. On the basis of some parameter feature, find the malicious application which is leaking important files, contacts and other important files from device.



To get the network traffic of any smart phone, we are going to use logcat command. The Android logging system provides a mechanism for collecting and viewing system debug output. Logs from various applications and portions of the system are collected in a series of circular buffers, which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages

```
C:\Users\Serene\AppData\Local\Android\sdk\platform-tools>adb devices
List of devices attached
ZX1B33PDPQ      device
emulator-5554   device
```

You can run logcat as an adb command or directly in a shell prompt of your emulator or connected device. To view log output using adb, navigate to your SDK platform-tools/ directory and execute:
>adblogcat

```
C:\Users\Serene\AppData\Local\Android\sdk\platform-tools>adb logcat
- waiting for device -
```

You can have all the results in a text file using following command.
>adblogcat -b >file1.txt

In android studio once you run DDMS(Dalvik Debug Monitor Server), to debug your applications. You can see at the bottom side all logcat results are given.

From file1.txt you can get the applications and the site they are communicating with. If any application is communicating with a malicious site is also shown there. Likewise you can differentiate genuine and malicious application.

Level	Time	PID	TID	Application	Tag	Text
D	02-17 16:14:1...	1905	2447	com.google.android.apps.maps	OpenGLRend...	Use EGL_SWAP_BEHAVIOR_PRESERVED: true
I	02-17 16:14:1...	1905	1905	com.google.android.apps.maps	Choreographer	Skipped 37 frames! The application may be doing too much work on its main thread.
I	02-17 16:14:1...	1905	2447	com.google.android.apps.maps	OpenGLRend...	Initialized EGL, version 1.4
D	02-17 16:14:1...	1905	2447	com.google.android.apps.maps		HostConnection::get() New Host Connection established 0x9f17d590, tid 2447
W	02-17 16:14:1...	1905	2447	com.google.android.apps.maps	EGL_emulation	eglSurfaceAttrib not implemented
W	02-17 16:14:1...	1905	2447	com.google.android.apps.maps	OpenGLRend...	Failed to set EGL_SWAP_BEHAVIOR on surface 0xada5f780, error=EGL_SU

Conclusion:-

In this paper, we define the various techniques to detect malware inside smart phone. We try to give an idea to implement a detection techniques on the basis of network traffic analysis of a smart phone. We use logcat and DDMS (Dalvik Debug Monitor Server) to see the results and then find out if any application is communicating with malicious server.

References:-

1. **Anarora, A.; Garg, S.; Peddoju, S.K.,** "Malware Detection Using Network Traffic Analysis in Android Based Mobile Devices," Next Generation Mobile Apps, Services and Technologies (NGMAST), 2014 Eighth International Conference on , vol., no., pp.66,71, 10-12 Sept. 2014
2. **Zaman, M.; Siddiqui, T.; Amin, M.R.; Hossain, M.S**., "Malware detection in Android by network traffic analysis," Networking Systems and Security (NSysS), 2015 International Conference on , vol., no., pp.1,5, 5-7 Jan. 2015
3. **DaiyongQuan; LidongZhai; Fan Yang; Peng Wang,** "Detection of Android Malicious Apps Based on the Sensitive Behaviors," Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on , vol., no., pp.877,883, 24-26 Sept. 2014
4. **Jun Li; LidongZhai; Xinyou Zhang; DaiyongQuan**, "Research of android malware detection based on network traffic monitoring," Industrial Electronics and Applications (ICIEA), 2014 IEEE 9th Conference on , vol., no., pp.1739,1744, 9-11 June 2014
5. **Angel Alonso Parrizas, parrizas@gmail.com Advisor: DominicusAdriyanto**"Monitoring Network Traffic for Android Devices" SANS Institute ,InfoSec Reading Room 16 January 2013
6. **Feizollah, A.; Anuar, N.B.; Salleh, R.; Amalina, F.,** "Comparative study of k-means and mini batch k-means clustering algorithms in android malware detection using network traffic analysis," Biometrics and Security Technologies (ISBAST), 2014 International Symposium on , vol., no., pp.193,197, 26-27 Aug. 2014
7. **Barbareschi, M.; De Benedictis, A.; Mazzeo, A.; Vespoli, A**., "Mobile Traffic Analysis Exploiting a Cloud Infrastructure and Hardware Accelerators," P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on , vol., no., pp.414,419, 8-10 Nov. 2014
8. **Faruki, P.; Bharmal, A.; Laxmi, V.; Ganmoor, V.; Gaur, M.S.; Conti, M.; Rajarajan, M.,** "Android Security: A Survey of Issues, Malware Penetration, and Defenses," Communications Surveys & Tutorials, IEEE , vol.17, no.2, pp.998,1022, Secondquarter 2015
9. **Prajakta D. Sawle, A. B. Gadicha**"Analysis of Malware Detection Techniques in Android" IJCSMC, Vol. 3, Issue. 3, March 2014, pg.176 – 182