IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Analysis of Android Malware Scanning Tools

Prerna Agrawal[1*], Bhushan Trivedi[2]

[1,2]GLS University, Ahmedabad, Gujarat, India

*Corresponding Author: prerna.agrawal@glsuniversity.ac.in

DOI: https://doi.org/10.26438/ijcse/v7i3.807810 | Available online at: www.ijcseonline.org

Accepted: 11/Mar/2019, Published: 31/Mar/2019

***Abstract* –** The usage of Mobile Technology is rapidly increasing day by day. With the usage of Android mobiles, the threat of malware is also increasing day by day. All the private and confidential data in Android devices have a high risk of malware. Various Android malware scanning tools are freely available for use. This paper analyses different kinds of Android Malware scanning tools with a proper comparison, pros and cons and their future scope.

***Keywords* –** Mobile, Android, Mobile Security, Malware, Scanning tools**.**

I. INTRODUCTION

Today Mobile Technology is used extensively and it is growing very fast since 2008 [19] [20]. Each and every day new Android devices are being activated [18]. As mobile technology is providing ease and comfort in all the tasks it also has high risks [18]. Malware threats are also increasing day by day. So the Android devices have a high risk of malware [18].

There are many Malware Analysis techniques available for analysis of malware [18]. There are many existing Android malware scanning tools available in the market [7]. As the malware threat is growing day by day there is a need for proper malware detection [18]. In paper [18] comparison of Android, Malware Techniques is shown properly. In paper [18] a malware detection technique is already proposed. To implement this technique a proper malware scanning tool is also needed [18]. So there is also a need to study the existing malware analysis tools and perform a proper analysis to know their limitations.

The paper is divided into the following sections: Section II describes different types of Android Malware Scanning Tools. Section III provides a comparative study of Android Malware Scanning Tools. Section IV provides the conclusion of the paper.

II. TYPES OF ANDROID MALWARE SCANNING TOOLS

There are many Android Malware Scanning Tools available in the market. Some tools are available online and some are downloadable. Some tools are available for free and some tools are chargeable. Here online tools available as services free of cost are focused. The online tools studied are AVC UnDroid, AndroTotal, VirusTotal, NVISO ApkScan, VirSCAN, and Hybrid Analysis [1-6] [7].

A. AVC UnDroid

This tool is publicly available online as a service and performs scanning of suspicious Android applications. To use this service firstly you have to select the apk file you want to scan. After the selection of the file, you need to start the file upload. The file will be uploaded and scanned automatically. After the scanning is completed a detailed scanning report is shown [15]. This tool performs Static Analysis [16]. The analysis is based on Buster Sandbox, Analyzer, ssdeep, APKTool and engines of several different mobile security vendors [16].

B. AndroTotal

This tool is publicly available online as a service and performs scanning of suspicious Android applications. To use this service you have to select the apk file and upload it. The file will be uploaded and scanned automatically. After the scanning is completed a detailed scanning report is shown [2] [10]. AndroPilot is the library developed and used for this tool [10]. AndroTotal service is currently in beta phase [10].

C. VirusTotal

VirusTotal is an owned subsidiary of Google [8] [9]. This tool is publicly available online as a service and lets you upload and scan files, submit and scan URLs, IP Address, Domain and Hash Files [11][13]. There are multiple ways to submit the files, URLs etc. for scanning. VTZilla is a Firefox extension that allows scanning of files, URLs [9]. The VirusTotal Windows uploader allows scanning of files in Windows Explorer [9]. VirusTotal has an Android application that allows scanning and provides scan reports [9]. There are public and private APIs also available which allows the scanning of files [9]. It performs static and dynamic analysis. VirusTotal also provides a detailed scan summary report with detailed results [12].

D. NVISO ApkScan

This tool is publicly available online as a service and performs scanning of suspicious Android applications [4]. To use this service firstly you have to select the apk file you want to scan. After the selection of the file, you need to start the file upload. The file will be uploaded and scanned automatically. After the scanning is completed a detailed scanning report is shown [4]. It performs both static and dynamic analysis.

E. VirSCAN

This tool is publicly available online as a service and performs scanning of suspicious Android and compressed files [14]. To use this service firstly you have to select the file you want to scan. After the selection of the file, you need to start the file upload. The file will be uploaded and scanned automatically. After the scanning is completed a detailed scanning report is shown [14]. VirSCAN only scans files, which may contain viruses, Trojans, backdoors, spyware, dialers, and key-loggers [14]. VirSCAN supports bulk file scanning and performs static analysis.

F. Hybrid Analysis

This tool is publicly available online as a service and lets you upload and scan files, submit and scan URLs, IP Address, Domain and Hash Files [17]. It uses Falcon Sandbox framework to perform malware scanning [17]. Falcon Sandbox is a high-end malware analysis framework with a very agile architecture [17]. It supports multiple file extensions for file upload and scan. It supports bulk file analysis and performs hybrid analysis [17]. It also provides a detailed scanning summary report.

III. COMPARATIVE STUDY OF ANDROID MALWARE SCANNING TOOLS

In this section, a detailed comparison is discussed between different Android Malware Scanning Tools [1-6]. The following parameters are: Tool name, No of Scanners, Different Inputs, File Formats, File Size Upload, Scanning Time, Bulk File Scanning, Analysis Technique, Output, Summary Report, and Programming Language.

- *No of Scanners*

This parameter defines total no of scanners used by the tool for malware scanning. AndroTotal [2] takes a total of 8 scanners for scanning the malware. VirusTotal [3] takes a total of 59 scanners for scanning the malware. NVISO ApkScan [4] takes a total of 59 scanners for scanning the malware. VirSCAN [5] takes a total of 32 scanners for scanning the malware. Hybrid Analysis [6] takes a total of 59 scanners for scanning the malware.

- *Different Inputs*

This parameter defines the different types of input taken by the tool for malware scanning. AVC UnDroid [1] takes files as an input for scanning the malware. AndroTotal [2] takes files and JSON messages as an input for scanning the malware. VirusTotal [3] takes Files, URL, IP Address, Domain, and Hash File as an input for scanning the malware. NVISO ApkScan [4] takes files as an input for scanning the malware. VirSCAN [5] takes files as an input for scanning the malware. Hybrid Analysis [6] takes Files, URL, IP Address, Domain, and Hash File as an input for scanning the malware.

- *File Formats*

This parameter defines the different types of file formats taken as an input by the tool for malware scanning. AVC UnDroid [1] takes only apk files for scanning the malware. AndroTotal [2] takes only apk files for scanning the malware. VirusTotal [3] takes apk, exe, ipa, zip, rar files for scanning the malware. NVISO ApkScan[4] takes only APK files for scanning the malware. VirSCAN [5] takes apk, zip, rar files for scanning the malware. Hybrid Analysis [6] takes exe, scr, pif, .dll, com, cpl, Ms office files, apk, pdf, sct, lnk, chm, hta, wsf, js, vbe, vbs, swf, pl, ps1, svg, py, pl, eml files for scanning the malware.

- *File Size Upload*

This parameter defines the maximum file size to be uploaded on the tool for malware scanning. AVC UnDroid [1] takes file upload size up to 7 MB. VirSCAN [5] takes the file upload size up to 20 MB.

- *Scanning Time*

This parameter defines the total time taken by the tool for scanning a file and display its result. AndroTotal [2] takes a total 3 to 4 minutes for scanning a file and display its result.

- *Bulk File Scanning*

This parameter defines that the tool can perform Bulk file scanning or not. AVC UnDroid [1] does not perform bulk file scanning. AndroTotal [2] does not perform bulk file scanning. VirusTotal [3] performs bulk file scanning. NVISO ApkScan [4] does not perform bulk file scanning. VirSCAN [5] performs bulk file scanning. Hybrid Analysis [6] performs bulk file scanning.

- *Analysis Technique*

This parameter defines the analysis technique used by the tool for analyzing the malware. AVC UnDroid [1] uses a static analysis technique for analyzing malware. AndroTotal [2] uses a static analysis technique for analyzing malware. VirusTotal [3] uses static and dynamic analysis technique for analyzing the malware. NVISO ApkScan [4] uses static and dynamic analysis technique for analyzing the malware.

VirSCAN [5] uses a static analysis technique for analyzing malware. Hybrid Analysis [6] uses a hybrid analysis technique for analyzing malware.

- *Output*

This parameter defines the list of parameters given as an output in a report after analyzing the malware. The report of AVC UnDroid [1] gives MD5, SHA256, SHA1, Requested Permissions, API Calls, Dangerous Calls, Action/Intent, Activities, Anomalies features, Receivers, Services, and Adware SDKs. The report of AndroTotal [2] gives SHA256, SHA1, MD5, File Size, Detections, Package Name, File Name, IsMalware. The report of VirusTotal [3] gives SHA1, MD5, File type, TRiD, file size, certificate details, Permissions, Activities, Services, Receivers, Providers, Intent Filters, Bundle Information, file system mechanism and process actions, service actions, Synchronization signals, Modules loaded, Highlighted actions and Dataset Actions. The report of NVISO ApkScan [4] gives SHA256, MD5, File Size, Disassembled source code, Disk activity, Screenshot of Analysed application, Network activity, Automatically placed calls and text message, Cryptographic activity, Information Leakage, Services started, ADB Logcat file. The report of VirSCAN [5] gives SHA1, MD5, File type, Found Malware. The report of Hybrid Analysis [6] gives Risk Assessment, Malicious Indicators, Suspicious Indicators, General Information, File Size, File Type, SHA256, Version Information, File permissions, File Activities, Receiver Certificates, Extracted Strings, Extracted files, Runtime Notifications.

- *Summary Report*

This parameter defines that the tool provides a summary report or not after scanning the malware. AVC UnDroid [1] provides a summary report. AndroTotal [2] provides a summary report. VirusTotal [3] provides a summary report. NVISO ApkScan[4] provides a summary report. VirSCAN [5] does not provide a summary report. Hybrid Analysis [6] provides a summary report.

- *Programming Language*

This parameter defines that in which programming language the tool is designed. AndroTotal [2] is designed in Python. VirusTotal [3] is designed in Curl, Python, and PHP.

TABLE I. COMPARISON OF ANDROID MALWARE SCANNING TOOLS

Tool Name	**No of Scanners**	**Different Inputs**	**File Formats**	**File Size Upload**	**Scanning Time**	**Bulk File Scanning**	**Analysis Technique**	**Output**	**Summary Report**	**Programming Language**
AVC UnDroid[1]	Not mentioned	Files	apk	Up to 7 MB	Not mentioned	No	Static	MD5, SHA256, SHA1, Requested Permissions, API Calls, Dangerous Calls, Action/Intent, Activities, Anomalies features, Receivers, Services, Adware SDKs.	Yes	Not mentioned
AndroTotal[2]	8	Files, JSON Messages	apk	Not mentioned	3 – 4 minutes	No	Static	SHA256, SHA1, MD5, File Size, Detections, Package Name, File Name, IsMalware	Yes	Python
VirusTotal[3]	59	Files, URL, IP Address, Domain, Hash File	apk, exe, ipa, zip, rar	Not mentioned	Not mentioned	Yes	Static, Dynamic	SHA1, MD5, File type, TRiD, file size, certificate details, Permissions, Activities, Services, Receivers, Providers, Intent Filters, Bundle Information, file system mechanism and process actions, service actions, Synchronization signals, Modules loaded, Highlighted actions and Dataset Actions	Yes	Curl, Python, PHP
NVISO ApkScan[4]	59	Files	apk	Not mentioned	Not mentioned	No	Static, Dynamic	SHA256, MD5, File Size, Disassembled source code, Disk activity, Screenshot of Analysed application, Network activity, Automatically placed calls and text message, Cryptographic activity, Information Leakage, Services started, ADB Logcat file	Yes	Not mentioned
VirSCAN[5]	32	Files	apk, zip, rar	Up to 20 MB	Not mentioned	Yes	Static	SHA1, MD5, File type, Found Malware	No	Not mentioned
Hybrid Analysis[6]	59	Files, URL, IP Address,	exe, scr, pif, .dll, com, cpl,	Not mentioned	Not mentione	Yes	Hybrid	Risk Assessment, Malicious Indicators, Suspicious Indicators, General	Yes	Not mentioned

		Domain, Hash File	Ms office files, apk, pdf, sct, lnk, chm, hta, wsf, js, vbe, vbs, swf, pl, ps1, svg, py, pl, eml		d			Information, File Size, File Type, SHA256, Version Information, File permissions, File Activities, Reciever Certificates, Extracted Strings, Extracted files, Runtime Notifications.		

IV. CONCLUSION

Proper Malware detection is a very important aspect of today's mobile technology. With the increase in day to day malware, there is also a need for a proper malware detection scheme with a robust Malware detection scanning tool. Based on the limitations of the existing Android malware scanning tools it can be concluded that most of the tools do only Static Malware analysis. Most of the tools provide only file upload as an input for performing malware analysis. Most of the tools support a small file size upload for Malware scanning. The tools also do not support bulk file scanning. The time taken by the tools for a single file scan is also more.

A robust malware scanning tool is needed which overcomes all the limitations of the existing scanning tools which will perform hybrid analysis and can be implemented as a service. Also, the output given by the existing scanning tools can be combined and a more detailed and proper summary report can be given.

REFERENCES

[1] "AVC UnDroid", Online Link: https://undroid.av-comparatives.org

[2] "AndroTotal: Scan Android Application", Online Link: http://andrototal.org

[3] "VirusTotal: Analyse suspicious files", Online Link: https://www.virustotal.com

[4] "NVISO ApkScan: Scan Android Applications for Malware", Online Link: https://apkscan.nviso.be/

[5] "VirSCAN.org: Submit and scan your file", Online Link: http://www.virscan.org

[6] "Hybrid Analysis", Online Link: https://www.hybrid- analysis.com

[7] "Top 7 Online Android APK Malware analysers", Online Link: https://www.yeahhub.com/top-7-online-android-apk-malware-analyzers-free/

[8] "VTI for Threat Investigations", Online Link: https://vt-gtm-wp-media.storage.googleapis.com/vti-threat-investigation-use-case.pdf

[9] Randy Abrams, "*Virus Total Tips, Tricks and Myths*" Virus Bulletin Conference, Oct 2017. Online Link: https://www.virusbulletin.com/uploads/pdf/magazine/2017/VB2017-Abrams.pdf

[10] Federico Maggi, Andrea Valdi, Stefano Zanero, "*AndroTotal: A Flexible, Scalable Toolbox and Service for testing Mobile Malware Detectors*" Conference on Security and privacy in smartphones & mobile devices ACM, Nov 2013.

[11] "Virus Total Getting Started", Online Link: https://support.virustotal.com/hc/en-us/articles/115003895489-Get-Started

[12] "Virus Total Reports", Online Link: https://support.virustotal.com/hc/en-us/articles/115002719069-Reports

[13] "Virus Total API", Online Link: https://support.virustotal.com/hc/en-us/articles/115002100149-API

[14] "VirSCAN About us", Online Link: http://www.virscan.org/language/en/about

[15] "AVC Undroid About", Online Link: https://undroid.av-comparatives.org/about.php

[16] "AVC Undroid FAQs", Online Link: https://undroid.av-comparatives.org/faq.php

[17] Hybrid Analysis FAQs", Online Link: https://www.hybrid-analysis.com/faq

[18] Prerna Agrawal, Bhushan Trivedi "*A Survey on Android Malware and their Detection Techniques*", Third International Conference on Electrical, Computer and Communication Technologies (ICECCT) IEEE, Coimbatore, Feb 2019 (Paper to be Published).

[19] S.Birundha, Dr. V. Vanitha "*Survey on Mobile Malware Detection Techniques in Android Operating System*" International Journal on Applications in Information and Communication Engineering, vol. 2 issue. 4 Apr 2016.

[20] Saba Arshad, Abid Khan "*Android Malware Detection and Protection: A Survey*" International Journal of Advanced Computer Science and Applications, vol. 7 no. 2 2016.

Author's Profile

Ms. Prerna Agrawal completed her Master of Computer Application from Gujarat University, Ahmedabad, Gujarat, India in 2008. She is currently working as an Assistant Professor in the Faculty of Computer Technology (MCA) at GLS University. She is currently pursuing her Ph.D. from GLS University, Ahmedabad, Gujarat, India. She has total of 7 years of teaching experience and 1-year industry experience. Her main research work focuses on Android Malware and Application Security.

Dr. Bhushan Trivedi completed his Master of Computer Application from MS University, Baroda, Gujarat, India in 1988. He completed his Doctor of Philosophy from Hemchandracharya North Gujarat University, Gujarat, India in 2008. He is currently working as a Director and Dean in Faculty of Computer Technology (MCA) at GLS University. He has more than 20 years of teaching experience. He is acting as a Ph.D. guide at GLS University. His main research area is on Intrusion Detection. He has 4 patents on his name. He has currently 8 research scholars enrolled under him. He has published more than 50 research papers in various national and international journals and conferences.