IBIMA Publishing
Journal of Information Assurance & Cyber security
http://www.ibimapublishing.com/journals/JIACS/jiacs.html
Vol. 2016 (2016), Article ID 955268, 8 pages
DOI: 10.5171/2016.955268

Research Article

A Comparative Analysis of Various Security Applications for the Android Operating System

Michael Abelar

Biotechnology High School, Freehold, United States of America

Correspondence should be addressed to: Michael Abelar; miabelar@ctemc.org

Received date: 26 January 2016; Accepted date: 8 February 2016; Published date: 19 October 2016

Academic Editor: George Kostopoulos

Abstract

The number of devices running the Android operating system is increasing with over 900 million Android devices currently registered. As the Android operating system grows, security becomes increasingly important. While the current Android operating system protects against system compromising viruses, it does not provide full protection against malware, adware, spyware and Trojan viruses. This creates issues for device security, privacy, and functionality. To counter this, a number of antivirus applications have been made available to detect such malicious applications that host these viruses. However, with more hackers looking to Android, it is essential that users have the best antivirus applications to protect their devices. In this study, fifteen applications that host malware, adware, spyware and Trojan viruses were programmed to test antivirus applications. The viruses also displayed how the harmful code can be incorporated into an Android application. Additionally, a web server was programmed to accept data from the host applications. The efficacies of the twenty most popular antivirus applications were determined by introducing the viruses into the target phone through Android application packages. After testing all twenty applications, it was found that Mobile Security & Antivirus by AVAST Software detected all fifteen harmful applications, making it the most effective antivirus application tested. On the other hand, the other nineteen Android antivirus applications detected, at most, four of the host applications. The experiment can serve to maximize security on devices running Android and provide understanding of how antivirus applications function.

Keywords: Android, Virus, Security, Malware

Introduction

The number of devices running the Android operating system has been increasing with over 900 million Android devices registered (Epstein 2013). With the increasing growth of the Android operating system, the importance of security has also grown. While

Cite this Article as: Michael Abelar (2016), "A Comparative Analysis of Various Security Applications for the Android Operating System ", Journal of Information Assurance & Cyber security, Vol. 2016 (2016), Article ID 955268, DOI: 10.5171/2016.955268

the Android operating system does protect against system compromising viruses, it does not provide full protection against malware, adware, spyware and Trojan viruses (Drake 2014, p. 56). For instance, the number of malware applications on the market has grown by 13987 between 2011 and 2012 (Namestnikov 2012). This creates issues for the phone's security, privacy and functionality. Therefore, the need to protect one's device from such attacks is essential. Android antivirus applications are available to detect such malicious applications that host these viruses. However, which Android antivirus application detects the most viruses? Another article by Raymond.cc suggested that it is ideal to only have one antivirus application to maximize performance and power usage. Ideally, one antivirus application is best to have; however, which antivirus application will work the best so that I will only have to have one antivirus application installed to be fully protected against malicious attacks? In addition, there is a debate as to whether it's even worth having an antivirus application. German researchers at AV-Test argue there is no need for antivirus applications (Rubenking 2011). Meanwhile, some sources state that some antivirus applications are more efficacious than others but do not provide a full and detailed report of the results which led to such conclusions (Russell 2015) (Hindy 2016) (Eddy 2013). This project hopes to address the questions of which antivirus application is best or if it is necessary to have one. To test this, I programmed fifteen applications that contain malicious code to see which antivirus application/applications is the most effective for an Android device.

Materials and Methods

Research Question

Which Android antivirus application/applications will have the highest efficacy at detecting Android-targeting viruses?

Purpose

To investigate which of the most popular Android antivirus applications works the best at detecting malicious Android applications.

Hypothesis

All twenty of the selected Android antivirus applications will be able to detect all fifteen malicious viruses programmed in this experiment.

Null Hypothesis

There is no statistically significant difference between the efficacies of the Android antivirus applications.

Experimental Components

For this experiment, the independent variable will be the antivirus application used. The dependent variable will be the amount of programmed viruses detected. Finally, the positive control in this experiment will be an Android application with known Malware from European Expert Group for IT-Security.

Materials

Android Studio Software, any computer, USB cable, Android Device running Android 5.0/Android Lollipop, 15 Android Antivirus Applications, access to a web server with FTP, and text editor.

Programmed Virus Applications

Table 1: Programmed Malicious Applications*

Name of Application	Function
Malware Downloader	Downloads more malicious files to the Android Device in the background.
Send Device System Information	Sends the phone's system information in the background to a web server.
Unintended Calling	Acts in the background and immediately calls back the latest dialed number after hanging up. This application serves to annoy the user repeatedly and disrupt other phone functionality.
Delete Text Messages	Acts in the background and deletes all of the user's text messages whenever the user receives a new text message. This application prevents the user from reading new text messages.
Voice Tap	Uses the phone's microphone to listen in on the user. The application then sends all conversations from the user to a server. The app operates in the background until manually closed.
File Creator	Operates in the background and creates hundreds of new files in order to make the user run out of storage on their phone.
File Deletor	Scans the phone's SD card and randomly deletes files on the SD card.
Get Text Messages	Gets all of the user's text messages and sends them to a web server.
Send Contact Information	Operates in the background and sends all of the host's contacts and contact information to a web server.

Send Call Logs	Operates in the background and sends all of the host's call history to a web server.
Send Text Messages	When opened, the application sends a text message promoting a product to the entire list of contacts on the user's phone. This is known as adware.
Send Wifi Information	Operates in the background and gets the user's IP address and wifi information and sends it to a web server.
Start Up Spammer	Changes the settings of the user's phone whenever the phone is restarted. The app also makes a call to the most recent contact to further interrupt the user and the phone.
Fake Sign In	Prompts the user to sign into their Google Account. However, this is a fake sign-in and the username and password from the fake sign-in goes to a web server.
Known Malware (INTENDED USE [no date]).	Adopted from the European Expert Group for IT-Security which will serve as a positive control for this experiment. The virus itself does nothing. However, according to the European Expert Group for IT-Security, all antivirus softwares should be able to recognize it because it contains common malware patterns.

*15 viruses were created using *Android Studio*. These applications serve no real purpose except to house the malicious code. All malicious Android applications may be found at: https://drive.google.com/file/d/0B0eVAS0XtNo0VnIwWjlNT0YxOGM/view?usp=sharing

Procedure

1. A web server was then programmed and configured using the programming language PHP to take the information requests from the applications and post them onto a text document.

2. The applications that were written in Java and XML were then compiled into Android application packages.

3. The Android application packages were transferred onto the Android device running Android 5.0.

4. To test the antivirus application, each antivirus application was installed and then each virus was installed by opening the Android application packages with the antivirus installed. The Android antivirus applications include the twenty most popular antivirus applications on Google Play:

1. Norton Security and Antivirus
2. 360 Security - Antivirus Boost
3. AntiVirus Security - FREE by AVG
4. Antivirus and Mobile Security by TrustGo
5. Mobile Security and Antivirus by AVAST
6. Bitdefender Antivirus Free
7. Cm Security Antivirus AppLock
8. Dr. Web v.9 Anti-virus Light
9. Mobile Security and Antivirus by ESET
10. Malwarebytes Anti-Malware
11. Security and Antivirus - Free by McAfee
12. Comodo Security and Antivirus
13. Avira Antivirus Security
14. Antivirus Booster and Cleaner by PSafe Technologies
15. Free Antivirus 2015 Security by Antivirus Pro
16. Antivirus for Android by Android Antivirus
17. F-Secure Mobile Security
18. Mobile Security and Antivirus by Bullguard
19. AndroHelm Antivirus
20. Antivirus Free-Mobile Security by NQ Creative Apps

5. The number of malicious applications detected by each antivirus application was recorded.

Data Collection and Analysis:

To collect data for each antivirus application, whether or not the application was able to detect the fifteen applications containing malicious code will be recorded. These data will be recorded in a 20 by 15 table. The data will then be analyzed to determine which antivirus application has the highest efficacy at detecting the harmful applications by looking at the antivirus application that detects the most malicious applications. With the data, one can then confirm or reject my hypothesis and properly answer my research question.

Results

After recording how many applications each Android antivirus application detected, a graph displaying the resulting data was generated:

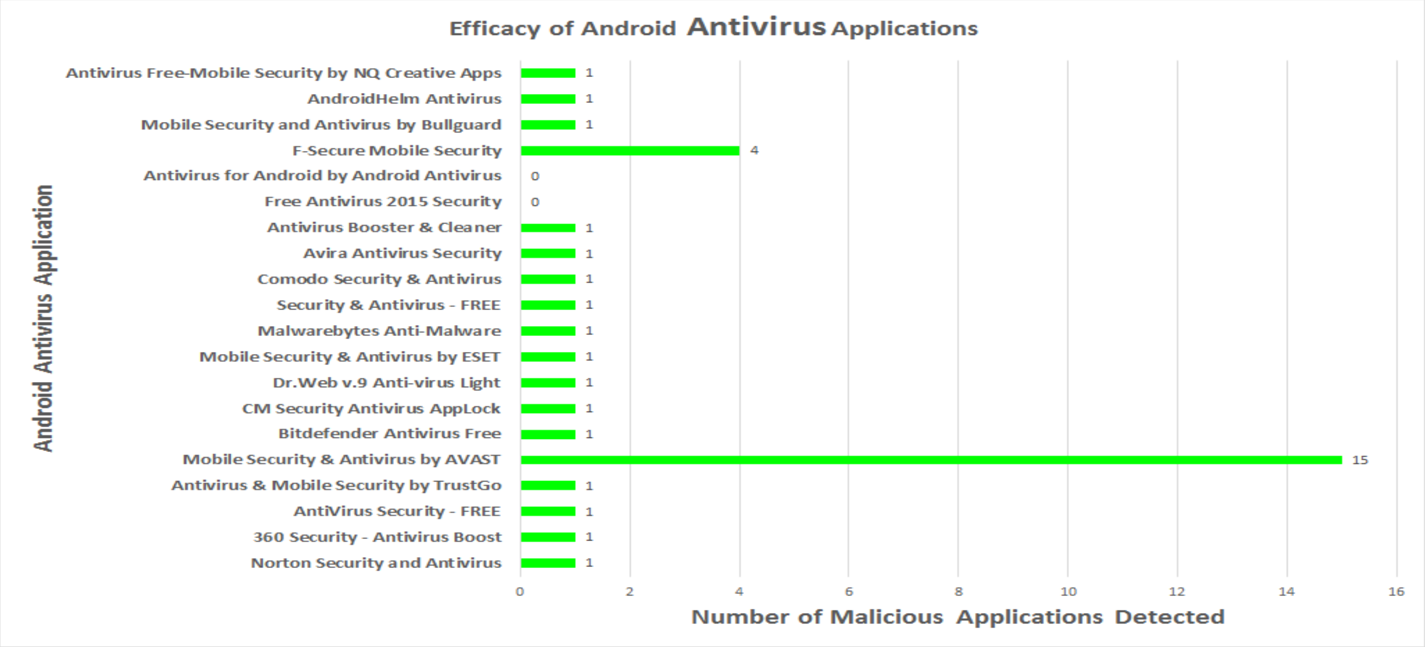

Figure 1: Efficacy of Android Antivirus Applications

As shown by the graph, it was found that *Mobile Security & Antivirus* by AVAST performed the best by detecting one hundred percent of the antivirus applications. Following, was *F-Secure Mobile Security* which only detected four of the fifteen applications. Those applications were the *Known Malware, Unintended Calling, Send Text Messages,* and *Start Up Spammer*. Two applications, *Free Antivirus 2015 Security* and *Antivirus for Android,* did not detect any applications including the positive control. The rest of the applications, only detected one common malicious application. That application was *Known Malware* which acted as the positive control. Overall, one application detected 100 percent of the malicious applications. One application detected 27 percent of the malicious applications. Eleven applications detected seven percent of the malicious applications. Finally, two applications detected zero percent of the malicious applications.

In addition, for all of the antivirus applications, all of the malicious applications that were programmed to send data to remote web servers did succeed. This shows that antivirus applications only alert the user about the threat of data leakage. The information was successfully sent to the remote programmed web server without any notification from all the antivirus applications.

Conclusion

Based on the results, it was found that one application, *Mobile Security & Antivirus* by AVAST was the only application to detect all fifteen programmed Android viruses. Due to this evidence, along with the ineffective rates of the other antivirus applications, I choose to reject my hypothesis stating that all twenty of the selected Android antivirus applications will be able to detect all fifteen malicious viruses programmed in this experiment. In fact, my data suggest that quite the opposite occurred: only one application was able to detect all viruses. Meanwhile, the other fourteen applications only detected an average of 1.1 malicious applications.

The significance of this experiment extends to greater cyber security for the Android Operating System. Since one antivirus application is shown to be ideal for any device, the one antivirus application that should be installed onto any Android device is *Mobile Security & Antivirus* by AVAST. With a world where more and more of one's information is being stored on his/her mobile device, security is essential. Information leaking which was the theme of many malicious applications programmed needs to be identified or the user can be put at great risk by hackers. As supported by the data, *Mobile Security & Antivirus* is the application that has proven to protect one's information and phone by alerting the user after installing a malicious application. Another significant point this experiment brings up is the surprising fact that the majority of the most popular antivirus applications are ineffective at detecting such malicious applications. The other nineteen antivirus applications are trusted by hundreds of millions of Android users on a daily basis. To have shown that most of these trusted applications failed to detect fourteen individual malicious applications implies that the fundamentals of the virus databases for the antivirus applications will not universally protect every user. Therefore, users need to be considerate when choosing an antivirus application because as shown, most antivirus applications cannot even detect two simple malicious applications. The experiment also supports that the virus databases of many antivirus applications are relatively weak. Virus databases are databases that store information about viruses for the antivirus application to use. When the antivirus application scans an application, it compares the application's contents with the known virus code in the virus database. If there is similarity, the antivirus application tags the scanned application as malicious and alerts the user. Since these virus databases have been shown to not support the source code of the malicious applications, the source code in this project can be submitted to such antivirus application companies to improve their applications and provide better security to hundreds of millions. This project also can improve antivirus applications in general by pointing out that *Mobile Security & Antivirus* by AVAST uses a special feature called "Privacy Advisor" which works by analyzing what target applications have access to. For example, the *Voice Tap* application. When scanning, Privacy Advisor saw that *Voice Tap* has access to the microphone and to the internet and then it tagged the application as malicious. This feature is unique only to *Mobile Security & Antivirus* by AVAST which is one of the main reasons the antivirus application had such success at detecting malicious applications. Malicious applications tend to contain questionable permissions such as internet access and system information. Based on this information, this experiment's data suggest that in order to improve security, other antivirus applications should start to weigh the access or permissions of the target applications more to maximize device security.

Although the experiment extended itself greatly to mobile cybersecurity, there are many next steps needed to maximize security on Android devices with Antivirus applications. In further research, more malicious applications, varying in function, could be created to test the full extent of the efficacy of Android antivirus applications. In addition, the malicious applications used in this experiment were relatively light in the amount of payload making it difficult for antivirus applications to pick up. However, in future research, malicious applications with little to large payloads will need to be tested to further point out weaknesses in the antivirus applications. Another aspect of research that can be expanded upon is the target devices. For this experiment a Samsung Galaxy S5 was used which runs the latest version of Android, Android 5.0. Antivirus applications may not be updated to perform the best at Android 5.0, hence, more devices including tablets and more versions will need to be used. Finally, the applications were introduced locally through Android Application Packages from Android Studio. However, the majority of users do not download applications this way. The majority of users use Google Play to download applications for their Android devices. In the future, all antivirus applications could be introduced through Google Play to create the ideal environment to test antivirus applications.

References

1. Drake, J.J., 2014. Android hacker's handbook, Indianapolis, IN: John Wiley & Sons.

2. Eddy, M., 2013. The Best Android Antivirus Apps. The Best Android Antivirus Apps. Available from: http://www.pcmag.com/article2/0,2817,2425153,00.asp.

3. Epstein, Z., 2013. Video: Watch the live stream of Google's big Google I/O 2013 keynote right here. Available from: http://bgr.com/2013/05/15/google-io-keynote-live-stream.

4. Hindy, J., 2016. 15 best antivirus Android apps and anti-malware Android apps. 15 Best Antivirus Android Apps And Anti-Malware Android Apps. Available from: http://www.androidauthority.com/best-antivirus-android-apps-269696/.

5. INTENDED USE. Intended Use. Available from: http://www.eicar.org/86-0-intended-use.html.

6. Namestnikov, Y., 2012. IT Threat Evolution: Q2 2012. IT Threat Evolution: Q2 2012. Available from: http://securelist.com/analysis/quarterly-malware-reports/36623/it-threat-evolution-q2-2012/.

7. Rubenking, N., 2011. Report: Most Free Android Antivirus Apps Useless. Report: Most Free Android Antivirus Apps Useless. Available from: http://securitywatch.pcmag.com/none/290411-report-most-free-android-antivirus-apps-useless.

8. Russell, H., 2015. Five basic steps for protecting your Android device from viruses. Five Basic Steps For Protecting Your Android Device From Viruses. Available from: http://www.androidcentral.com/three-basic-steps-protecting-your-android-device-viruses.

Michael Abelar (2016), Journal of Information Assurance & Cybersecurity, DOI: 10.5171/2016.955268