CS GY-9223 Mobile Security Project
Evaluation of Antivirus softwares for Android mobile devices

Kannan, Suvetha sk5897@nyu.edu
Raghunathan, Preethi pr1316@nyu.edu

Synopsis

1. Abstract
2. Attack Tree - Malicious apps methods of entry into the mobile device
3. Evaluation and analysis of features in the Antivirus software
4. Evaluation of antivirus based on permissions requested by the antivirus software
5. Evaluation of antivirus against malwares and malicious apks
6. Consolidated Evaluation based on features, permissions and malware detection
7. Conclusion

Abstract

Security Issues in mobile applications are on the rise as mobile devices are being used for various purposes such as e-mails and online mobile banking transactions. There are various mobile operating systems in the market such as Android by Google, iOS by Apple, Blackberry OS and Symbian. Among these, Android is the operating system that has dominated the mobile market. Antivirus software or mobile security softwares help in preventing malwares attacking the mobile devices. We are going to analyze and evaluate the effectiveness of antivirus softwares against malwares, spywares and botnets in Android mobile devices. Our project evaluates four antivirus softwares Norton, ESET, McAfee and Comodo. Criteria for evaluation of the antivirus softwares is based on the features offered by the antivirus, permissions required by the antivirus and malwares detected by the antivirus software. For the evaluation of the features provided by the antivirus, we have evaluated the efficiency of the antivirus software and comparing it with the features provided by the other antivirus softwares. For evaluating the antivirus softwares based on the permissions required, we have considered the permissions requested by the antivirus against the permissions required by the other antivirus softwares. For evaluating the malware detection by the antivirus software, we have created an experimental attack by infecting the mobile device with four malicious apk files called AMTSO.apk, FaceRecognition.apk, BadNews.apk and AV.apk, and determined if the malwares in the apk files were detected by the antivirus softwares and also checked if the antivirus software prevents the malicious apk files from installing or not.

Attack Tree

In order to evaluate the methods of entry for the malicious apps and code into a mobile device, we have created an attack tree to understand whether the antivirus software prevents all the attacks possible on a mobile device. The attack tree discusses the methods of entry for malicious apps through third party appstores, email attachments, SMS/MMS messages or attacks due to vulnerabilities in the code of the apps already installed in the mobile device.

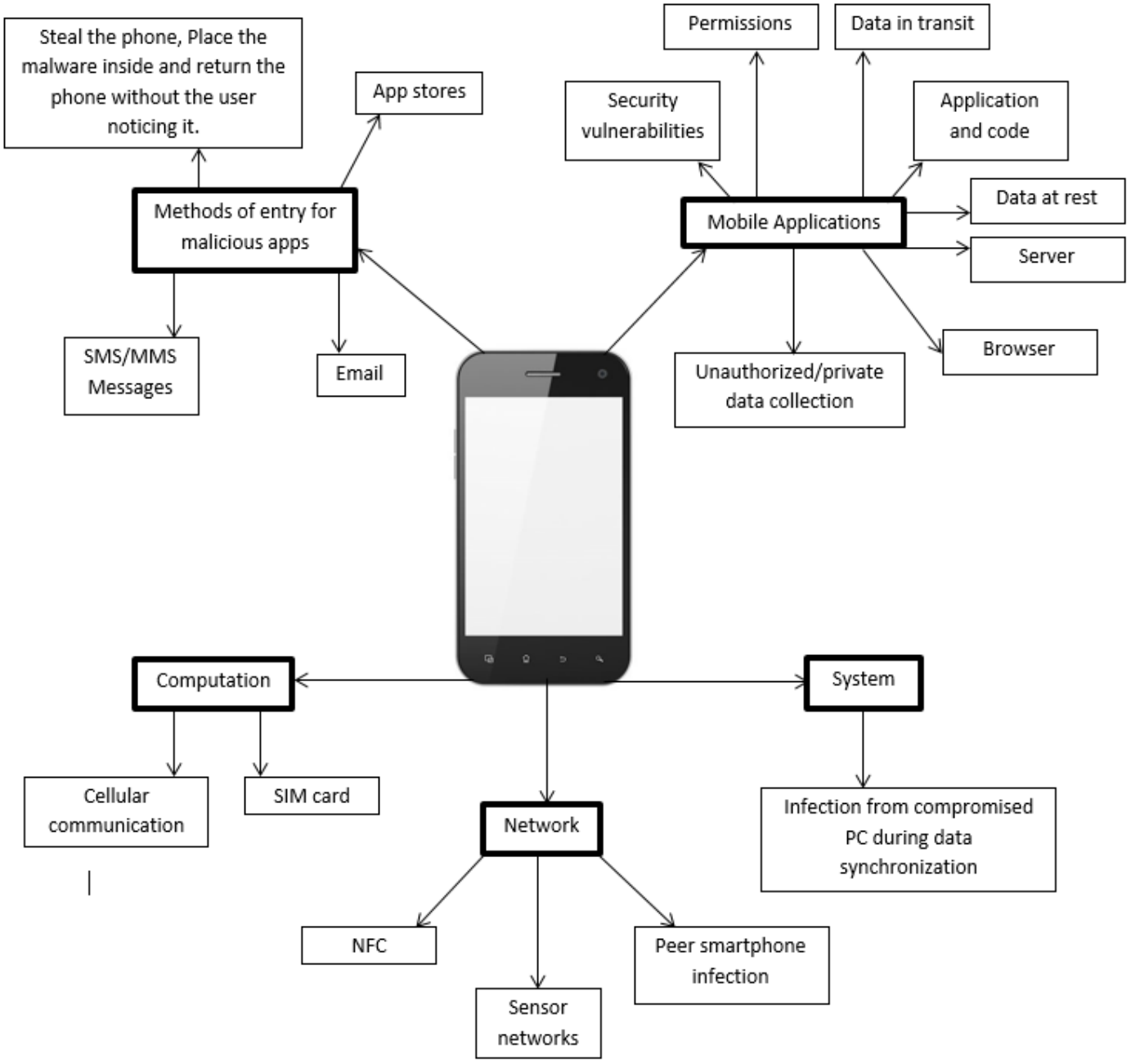

Figure.1 Attack Tree

Methods of entry for malicious apps:

1. **App stores:**
   - **Third party app stores:** Apps for Android OS can be downloaded from many third party app stores. These app stores are the main source of malware for Android phones. The inspection of the apps for malware is not that strict in the other third party app stores and hence, it is easy to upload malware onto the app store.
   - **Google Playstore:** The google playstore uses a software called Google Bouncer to investigate the app for malwares even before the app is launched in the appstore. When an app is uploaded into the Google Play Store, Bouncer starts its service immediately and it starts analyzing for any known malware, spyware and Trojans. It also does behavioural analysis on the application to look for any indications if the app is

misbehaving. Bouncer also holds a list of red flags in code it obtained from the applications it already analysed and it compares the red flags with the current app it is working on. All the apps are first run on Google's cloud infrastructure and the behavior of the app is simulated in the Android user's device to look for malicious and hidden behaviour.

2. **Email:** An attacker can simply send apk files or malicious URLs through emails and lure the user into downloading applications from them. This is another source for the attackers to use to install malware onto the mobile phones

3. **SMS/MMS messages:** A variety of attacks can be carried out using this channel. All configuration messages for the phones are sent through this service which means that a phone's configuration can be changed by just sending an SMS/MMS message to it. Malicious URLs can be sent using this service as well.

4. **Steal the phone, install malware and return the phone without the user noticing it:** This method is not common as it is difficult to carry out especially in the current world where users don't go anywhere without their phones and are always carrying it around with them.

Malwares in Mobile applications:

1. **Application and code:** It is possible to extract Android applications from the phone in their binary format. A number of techniques can then be used to break apart the application. This can help in determining the functions of the application such as the following.

    - How the application communicates to the server
    - The types of requests sent to remote servers and their format
    - If the application interacts with other components on the phone
    - If the application is writing files to the underlying operating system
    - Cryptographic Functions
    - Third party libraries in use

2. **Permissions:** In the Android security model, due to the sandbox mechanism, each application is assigned a unique low privileged user ID (UID) and is run as that user in a separate process. Also, applications can only access their own files. With this isolation in place, applications are able to communicate via different components. These communications between components are a critical area of focus for assessing the security of a mobile application. Most Android applications do not adequately place permissions around their components. Some applications were found to contain the 'debug' flag. Even though this is removed by default within the Eclipse ID, it can still end up in the production application.

3. **Data in transit:** Most applications communicate with a server. We need to have some means to authenticate the communicating party and ensure confidentiality of data by having proper cryptographic algorithms implemented for this purpose.

4. **Data at rest:** One of the challenges in mobile security is the protection of data stored in the device. If the device is stolen it would be easy for an attacker to get the data stored on the phone. Another common problem is preventing unauthorized parties from gaining root access on the phone. It is fairly easy, nowadays, to gain root access on the phones which eventually leads to gaining access to an application's data and configuration files.

5. **Server:** We are aware that there exists a large number of web vulnerabilities such as username enumeration, SQL injection, broken session management and information disclosure. To protect against these attacks certain measures must be taken at the server side such as strong validation of requests must be done, the server should not allow the client to make logic decisions and the server must be able to validate the mobile application.

6. **Browser**: The browser is the most targeted in any system. Many types of attacks are possible such as phishing, click jacking, cross site scripting, Man-in-the-middle, uffer overflows and so on. Even with the increased security that is provided in today's browsers the probability of all these attacks are still high.

7. **Security vulnerabilities:** Mobile applications are susceptible to security vulnerabilities from code level issues and/or run-time flaws in the application. Another form of security vulnerabilities arise from using the app, identifying flaws/exposures and exploiting them to gain unauthorized access to data. Almost all the mobile platforms run a sandox which reduces the likelihood of a code level security issue from being externally exploitable. Using secure coding techniques should also help reduce these vulnerabilities.

8. **Unauthorized/private data collection:** The mobile phone contains a rich pool of personal information about its user. This information could be photos, important documents stored on the phone, location data, etc. The problem in this part is collecting the user's data without the user's permission. Many mobile applications use some of this data. For example, google maps use our location to help us determine a quick route to our destination. But there are also some information that should never be accessed by the applications. This information can be collected by developing malicious applications and tricking the user into downloading them.

Computation:

1. **Cellular Radio:** Cellular radio is processed by a broadband chip, increasingly implemented as a software defined radio. The broadband chip can run other installed programs that can access the mobile devices memory, communications and other processors. A program running within application processor may be interacting with a rogue program installed in the broadband processor. Secure applications need to consider the risks of interacting with the broadband processor.

2. **SIM card:** The SIM card itself is a small computing machine with its own memory and processor. It too may be compromised with rogue software installed that can access memory, communications systems and the main application processor.

Network:

1. **Sensors:** The mobile device has a lot of sensors which are sometimes used for authentication, authorization and confidentiality. Therefore, compromising these sensors can mean compromising the phone and its applications. Some sensors such as fingerprint scans are sufficiently imprecise that applications are already wary of the data provided. Noisy environments, diverse measurement conditions and natural variability have limited the use of single biometrics for authentication. The GPS sensor can play an integral part of a security architecture based on geofencing. GPS signals can be spoofed, thereby subverting the geofenced capability expected by an application.

2. **NFC:** Charlie Miller has found a vulnerability in Android that affects earlier versions of Android – Gingerbread and Icecream Sandwich with versions lower than 4.0.1. Apps on the mobile device use NFC and these apps could have bugs. For Example, the Android Beam app works with a simple touch with another NFC enabled Android device and it could automatically load a webpage of the "toucher's" choosing. This widens the attack surface to include HTML, JavaScript, PNG, JPG, GIF, mp3, mp4 and just about any thing that can be loaded into a browser.

3. **Peer smartphone infection:** Some phones in the vicinity of a user's phone could be affected by malware that can actively scan and infect peer smartphones either through the internet or through the SMS messaging service or even through bluetooth. As a result, the malware can spread to the user's phone as well. The first smart-phone worm uses this method.

System:

1. **The entire mobile device is itself vulnerable when the security features are not used properly:**

    - Users choose not to set a passcode, or use a weak PIN, passcode or pattern lock.
    - Rooting phones can expose sensitive data.
    - Security flaws may exist with the software that comes preinstalled with the mobile device. Recently some Android handsets that contain these softwares were found to have had bugs that could be used to wipe the handset, steal data, and even eavesdrop on calls.

2. **Infection from compromised PC during data synchronization:** Synchronization software like ActiveSync are used by users synchronize their e-mails, calendar, or other data on their smartphones with their desktop. Therefore, to ultimately infect a smartphone, attackers can first infect the ActiveSync software in the desktop, and then the smart-phone will be infected during the next synchronization with the user's mobile device.

Evaluation and analysis of features in the antivirus applications:

We have made a tabulation of what all features a particular antivirus system offers according to the information provided in the google playstore for that particular antivirus application.

	Features	Comodo	ESET	Norton	Mcafee
2	On-demand scan	✓	✓	✓	✓
3	Automatic scanning	✓	✓	✓	✓
4	Cloud scan	✓			
5	SD card scam	✓			✓
6	Scheduled scan	✓	✓		
7	Photo capture when phone lost	✓	✓	✓	✓
8	App lock	✓			✓
9	Remote data wipe	✓	✓	✓	✓
10	SMS/Call blocking		✓	✓	✓
11	Lock phone if SIM card removed			✓	
12	Alarm to find phone	✓	✓	✓	✓
13	Backup and restore data	✓		✓	✓
14	Safe web browsing		✓	✓	✓
15	Device monitoring		✓		
16	Installed application audit		✓		
17	Lost device last location stored		✓	✓	✓
18	Controlling device through web	✓	✓	✓	✓
19	Remote device lock	✓	✓	✓	✓
20	Uninstall protection	✓			✓
21	Multi-user app profile protection				✓
22	Battery optimization		✓		✓
23	Memoery cleanup				✓
24	storage cleanup				✓
25	Track data usage				✓
26	Wifi security				✓
27	Ad free app environment				✓
28	Anti theft	✓	✓		
29	Location of lost phone on map	✓	✓	✓	✓
30	Quarantine where all discovered items reside		✓		
31	Automatic updates of key modules		✓		
32	Mobile security education videos		✓		
33	List of network addresses mapped to phone when lost		✓		
34	On screen message to device finder	✓	✓		
35	App protection			✓	✓

Table.1 Evaluation and analysis of the features in the antivirus softwares (Comodo, , ESET, Norton and McAfee)

We had downloaded all the antivirus applications onto our phones to check what all features are offered for free. According to what we have found the following provides a list of free features that each antivirus system offers.

Features of McAfee:

1. Auto scan
2. Real time scan
3. Schedule scan
4. Battery optimization
5. Clean storage
6. Data managing
7. Call blocking
8. Wifi and web security

9. Backup
10. Find device

Features of Norton:

1. App advisor
2. Schedule scan
3. Auto scan
4. SD card scan
5. Call blocking
6. Anti-theft
7. Contact backup

Features of Comodo:

1. Call blocking
2. Schedule scan
3. Real time protection
4. SD card scan
5. Cloud scan
6. Wifi security
7. Report false detection

Features of ESET:

1. Auto scan
2. On demand scan
3. Lock and unlock device

As we can see from the above list and the tabulation results, McAfee provides us with a rich set of security features when considering both only free features and all available features. Therefore, overall security based on the analysis of the features provided by our chosen set of antivirus applications overall security is best provided by McAfee. However, there was one contradiction that we found when we installed this antivirus application. After installation it presented us with the following alert.

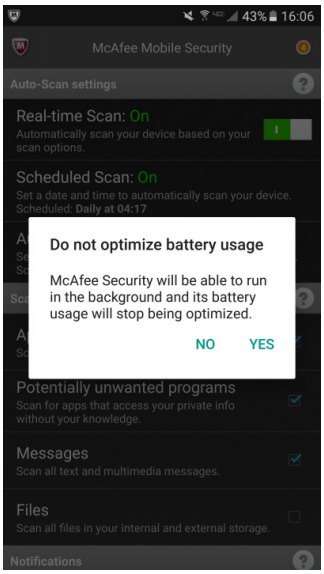

Figure.2 McAfee does not optimize battery when it runs.

The above picture clearly tells us that McAfee does not optimize battery. But it does provide the user with an option to optimize battery when the phone has low battery.

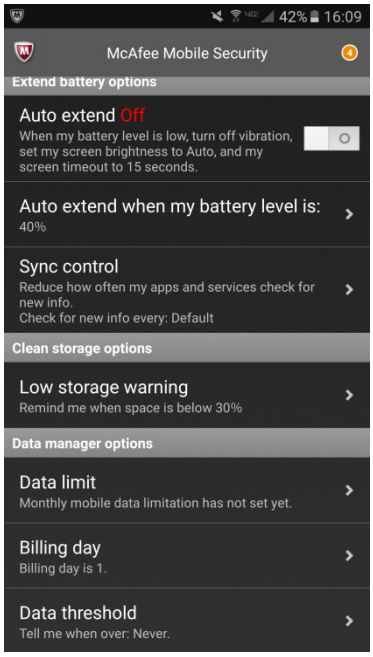

Figure.3 Battery optimization offered by McAfee.

As we can see, it offers battery optimization when the battery becomes low by setting the display to auto, changing screen timeout to 15 seconds, turning off vibration and reducing how often the phone's applications and services check for new information (SYNC control).

Rank	Antivirus Application
1	McAfee
2	Norton
3	Comodo
4	ESET

Table.2 Ranking of the different antivirus applications based on free and all offered features.

Mobile device Configuration

1. Android 4.3 (Jellybean) OS
2. Xperia M – Sony with 2GB internal memory, 1.5 GHz processor
3. Device was factory reset with no information on the device prior to the experimental attack.

Antivirus softwares installed on the phone

1. Symantec Norton Antivirus
2. ESET
3. McAfee
4. Comodo

Permissions requested by the Antivirus softwares

1. **Norton Antivirus**
   Permissions requested by Norton antivirus before installing the app in the phone is shown in below figure.

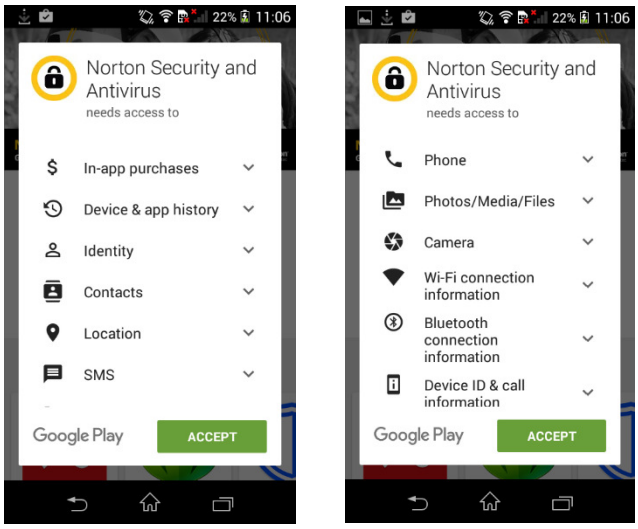

Figure.4 Permissions requested by the Norton Antivirus app

After the app was installed on the mobile device, the antivirus app performed an automated scan of the entire mobile device. The scan done by the antivirus and the success message showing that the mobile device was protected along with the details about any risky apps installed on the phone was shown as seen in the above figure.

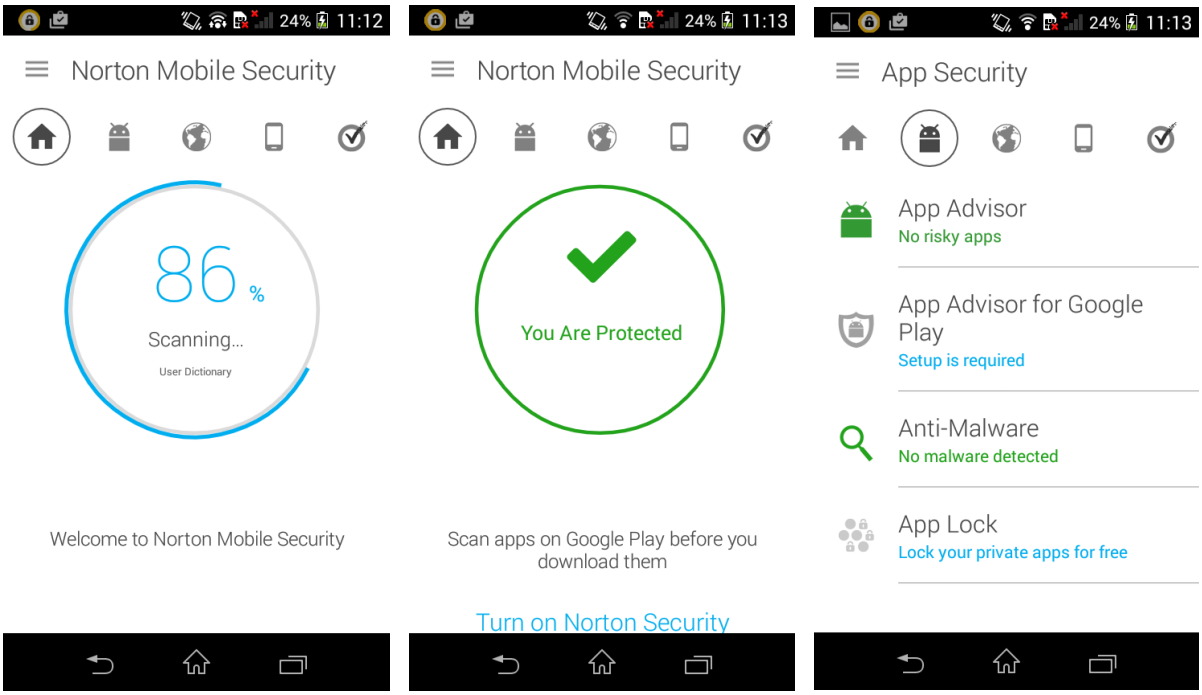

Figure.5 The antivirus scans the mobile device, notifies that the user's mobile device is secure and that there are no malwares in the mobile device.

2. ESET

Permissions requested by the antivirus are shown in the below figure.

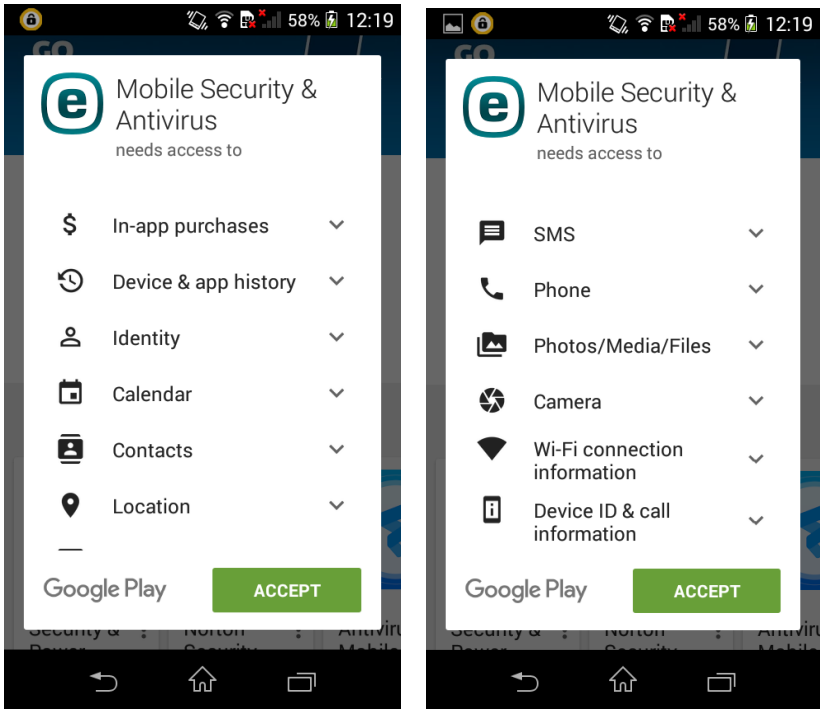

Figure.6 Permissions requested by the ESET antivirus

Permissions requested by Norton did not include Calender app permissions, whereas the ESET antivirus requests permissions to the Calendar app too.

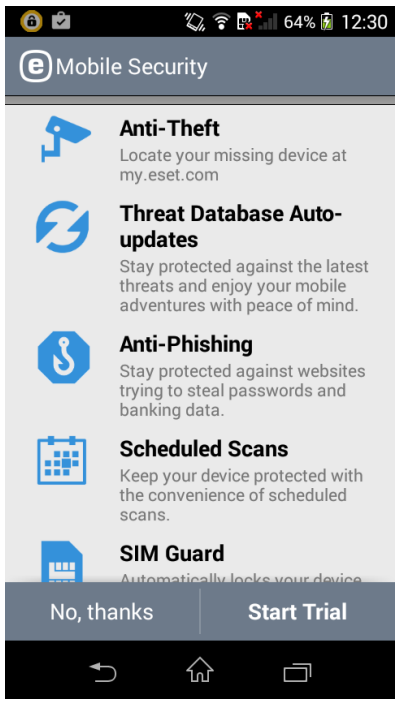

Figure.7 Features provided by the ESET antivirus app

3. McAfee

Permissions requested by McAfee are shown in the below figure along with the features provided by McAfee

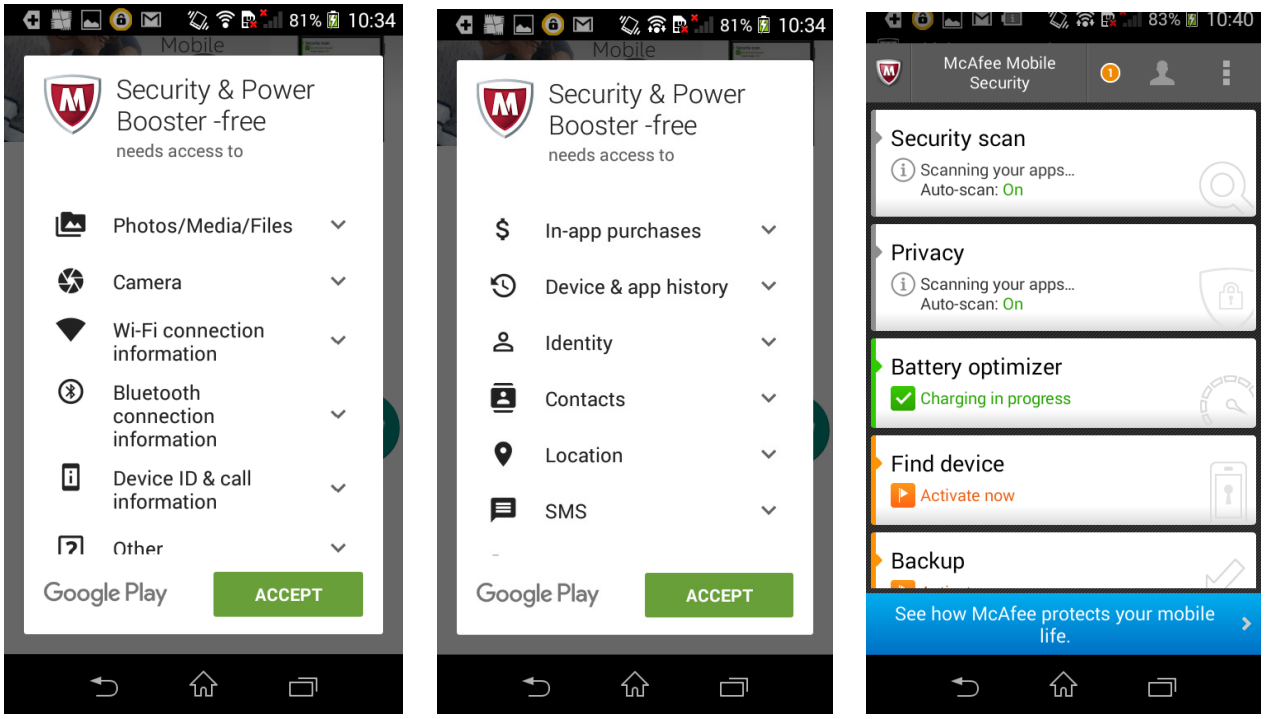

Figure.8 Permissions requested by McAfee and Features provided by McAfee

4. Comodo

Permissions requested by Comodo are shown in the below figure.

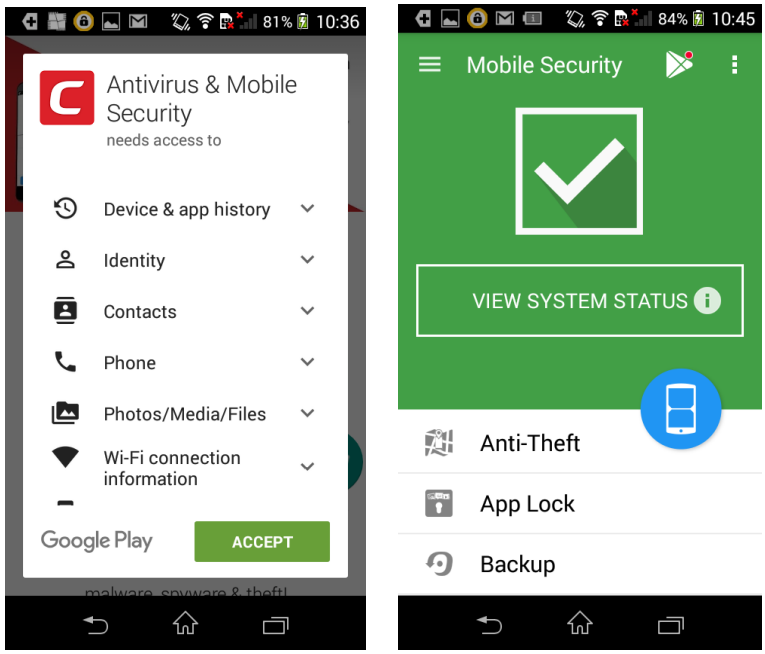

Figure.9 Permissions requested by Comodo and the features provided by Comodo

Evaluation based on Permissions

1. Calendar

a. Norton Antivirus, ESET and Comodo antivirus apps do not require permissions to the Calendar app on the phone.

b. If the user wants to maintain privacy of his/her calendar events being monitored by the antivirus software, he can choose amongst Norton, ESET and Comodo antivirus since it does not request for Calendar app permissions.

2. **File permissions** requested by the antivirus softwares are almost the same except for Comodo, which did not request access to the following apps,
    a. Wifi Connection information
    b. Bluetooth connection information
    c. SMS
    d. Location

Eventhough Comodo did not require access to the apps requested by Norton, ESET and McAfee, Comodo is least recommended amongst the above listed antivirus softwares. Also, the Comodo antivirus can be easily uninstalled since it does not provide password protection for the antivirus app by itself, it recommends a third party app for the same process called 'App Lock'

Antivirus	Recommended
Norton	High
ESET	High
McAfee	High
Comodo	Low

Table.3 Evaluation of the Antivirus software based on the permissions required.

Experimental Attack with malicious apps

In order to evaluate the antivirus softwares, we downloaded malicious apk files into the Android device we used for testing.

Evaluation of the antivirus softwares against malware

The state of the device plays a very important during the evaluation of the antivirus softwares also the level to which the system gets infected by malwares is also different depending if the mobile device is **rooted or unrooted**.

In a rooted mobile device, the chances that the malware has modified the devices system files are very high. All of our evaluations have been performed only for the mobile device **that has not been rooted**. In order to verify the malicious app initially even before we tried to install the malware on the mobile device, we used metadefender for the verification of the app to check if it is malicious or not. Metadefender in turn runs the malicious app by a means of signature based analysis where the signature of the malwares that are already known is compared with the signature of the malware currently present in the malicious app. Metadefender consolidates the app details whether the app has malicious code or not by running it through 43 antivirus engines that have a huge database of details pertaining to the app.

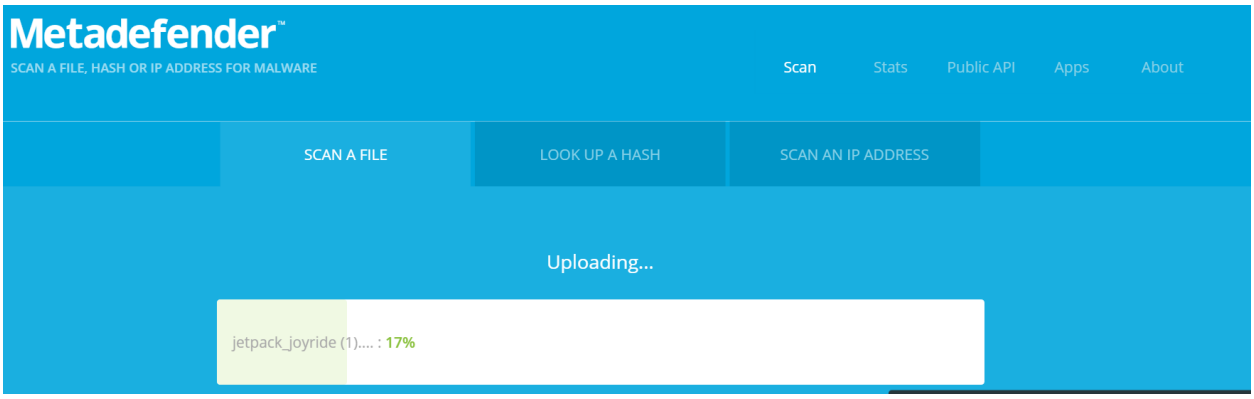

Figure.10 APK file evaluation by Metadefender before malware analysis on the mobile device

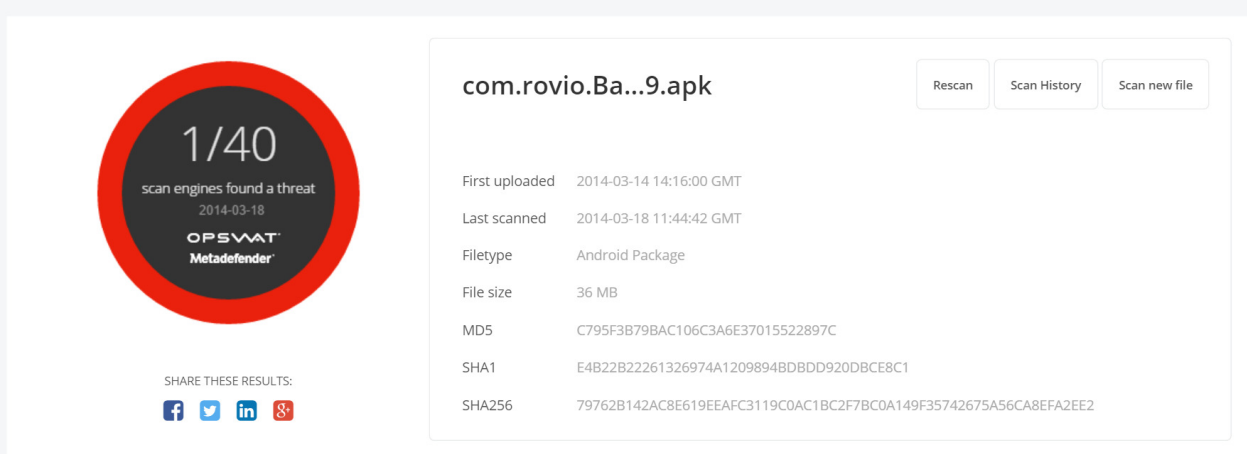

Figure.11 Example of a threat identified in the apk file, if the number of scan engines that determined the threat is small it could be a False Positive

ENGINE	SCAN TIME	LAST UPDATED	RESULT
AegisLab	22657 ms	Mar 18 2014 (770 days ago)	AdWare ✖
Agnitum	32 ms	Mar 17 2014 (771 days ago)	✔
Ahnlab	7226 ms	Dec 30 1899 (42486 days ago)	✔

Figure.12 Reason for the apk file having a threat is detected as AdWare.

Signature based malware analysis versus Behaviour based malware analysis

In the signature based malware analysis, only the malwares already known to the system will be flagged, whereas the behaviour based malware detection is done by understanding how the app should work, and even if one part of the app works in a way it is not supposed to and if an anomaly is detected then the app will be flagged. The chances of a false negative in the signature based system is low whereas the malwares may go undetected in that system whereas in the behavior based system, the chances of false positives is very high, since the system will flag any action that has not been previously seen which could be both normal behavior as well as abnormal behavior. Currently, the antivirus softwares perform behavior based malware analysis.

Malwares can be:

1. Trojans
2. Adwares
3. Spywares
4. Botnets
5. Ransomwares

For the evaluation of the antivirus softwares, we have used malicious apps that were available for research purposes and also a few cracked/modified versions of common games and apps that have Trojans and adwares. The list of malwares we used is as follows:

1. Trojan malware from amtso (A test file to evaluate the antivirus apps) testfile.apk
2. AV.apk (Audio/Video)
3. FaceRecognition.apk

4. BadNews.apk

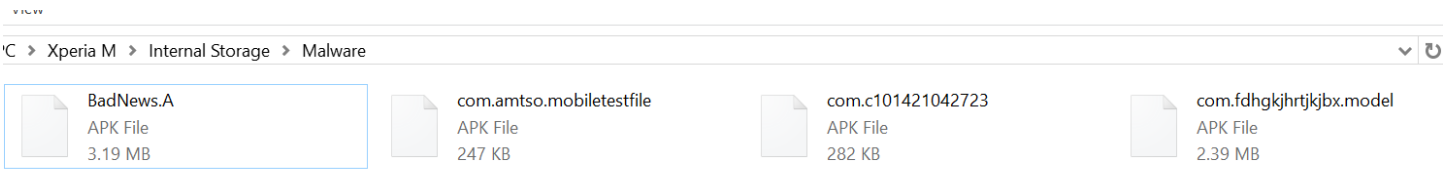

Figure.13 Malwares used to test the antivirus softwares

The above listed apk files were not downloaded from the Google play store, these are apps that have never available on the Google play store. The apk files were retrieved from researchers working on malware analysis in virustotal.com.

1. **Evaluation of Trojan malware from amtso**

The amtso test file was obtained from the Norton website, this malware is a Trojan. A Trojan is a type of malware in an app where the app does not do what it claims to be doing. The first step that was done after obtaining the malicious apk file was, we ran the malicious file through Metadefender to determine how many scan engines were already aware about the malware.

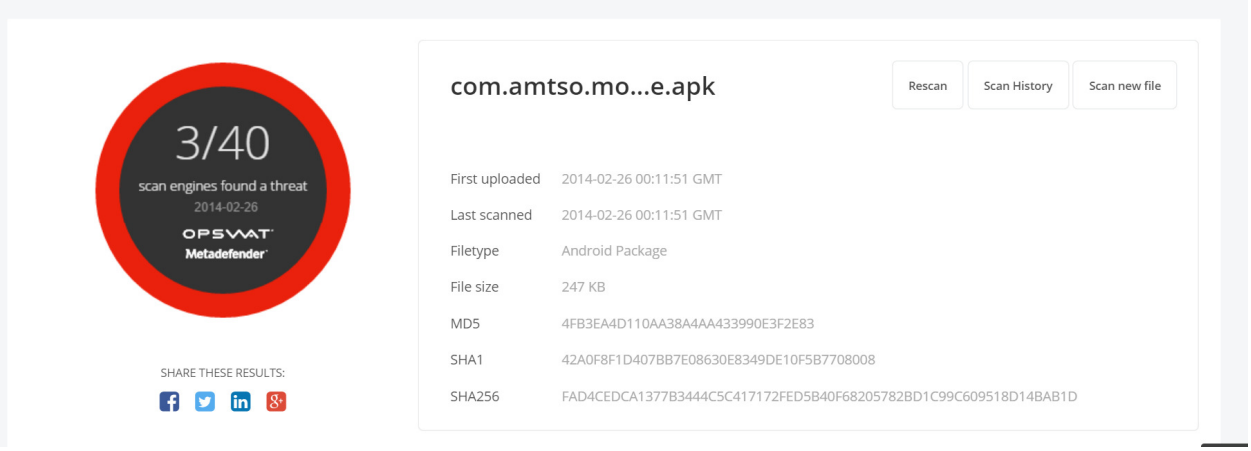

Figure.14 Malware analysis results from the website Metadefender.com

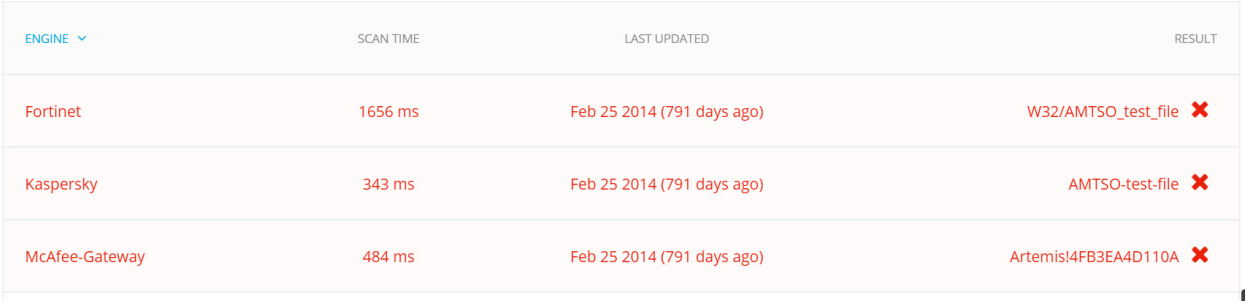

Figure.15 The three scan engines that determined the threat in the apk file were Fortnet, Kaspersky and McAfee.

The above scan engine results are from almost 2 years ago. The results of ESET and Norton in the same scan engine results were not able to determine if the apk file has a malware or not. So, the conclusion of the results from Metadefender.com is that the ESET and Norton did not have the malware details in their database and were unaware of this type of a Trojan

malware but during our experimental attack ESET and Norton antivirus softwares classified the malware as a Trojan so the databases of ESET and Norton are now uptodate.

Next, we moved the malicious apk to the filesystem of the mobile device.

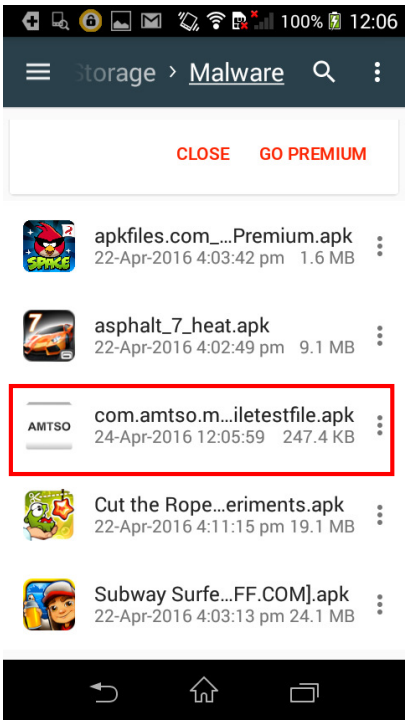

Figure.16 Screenshot from the mobile device with the amtso apk files along with other apk files

After adding the malicious apk file to the file system of the mobile device, the next step we did was, we tried to install the apk and checked if the antivirus apps that were already installed in the mobile device were reacting to the new file added to the system. Auto-scan was not turned on during the experimental attack process.

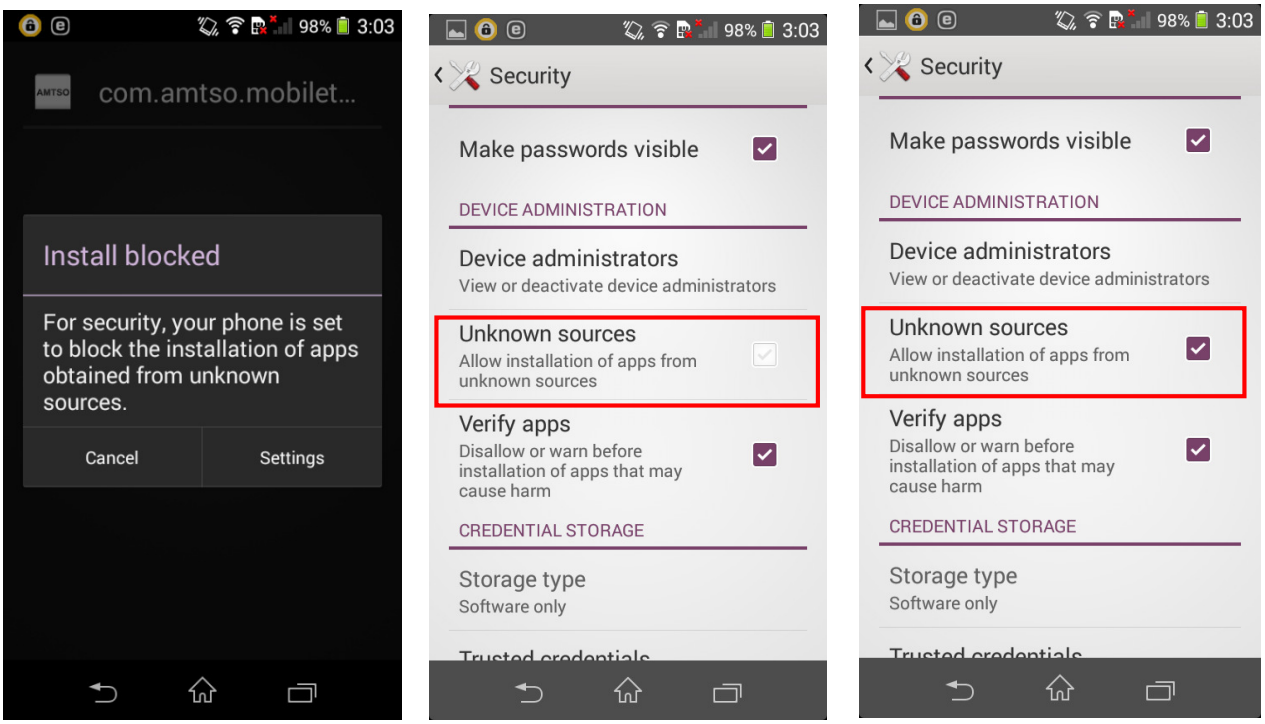

Figure.17 Installing a third-party software on the mobile device

When we tried to install the third party apk on the mobile device, as shown in the above figure we were not allowed to install any third party software without modifying the settings so the install process was immediately blocked. We had to go to Settings -> Security and choose the option Unknown sources as shown in the last two screenshots to the right in the above figure. After choosing the option to install apps from unknown sources, we were provided with the following options to install the apk file with:

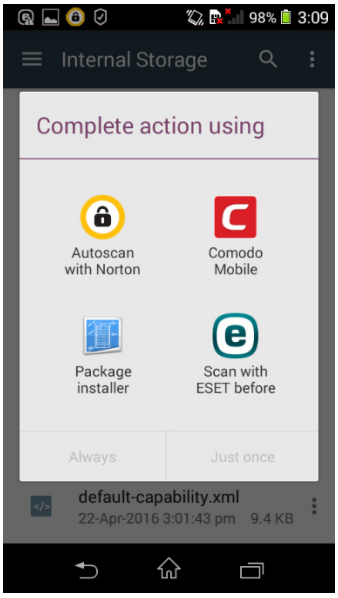

Figure.18 Options provided before installing the apk

We were provided with four options when we were trying to install the malware, no preferences or settings were modified in any of the antivirus softwares that were already installed in the mobile device. The four options were:

1. Autoscan with Norton
2. Comodo Mobile
3. Package Installer
4. Scan with ESET before

Eventhough the McAfee antivirus was installed in the mobile device, the McAfee antivirus did not provide with an option to scan the file unlike ESET, Norton and Comodo.

ESET, Norton and Comodo antivirus softwares offered to scan the apk file before letting the user install an apk file into the mobile device.

1. **Install the malware using the Package Installer.**

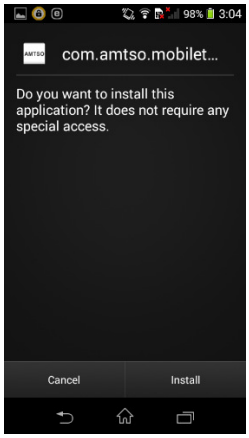

Figure.19 Installing malware using package installer

By default, when an apk file is installed in Android we use the Package Installer in order to install the software on the mobile device. The malware/malicious apk file did not have any file permissions and it just prompts to the user to install the apk file without any file permissions since there are no permissions to accept. Upon clicking install, the malicious apk file launches itself and app gets installed in the mobile device. So, this experimental attack proves that this is one of the ways in which the users are tricked into installing the malicious apps in their mobile device and none of the antivirus softwares in the mobile alerted the user or prevented the user from installing a malware.

2. **Install the malware using Autoscan by Norton**

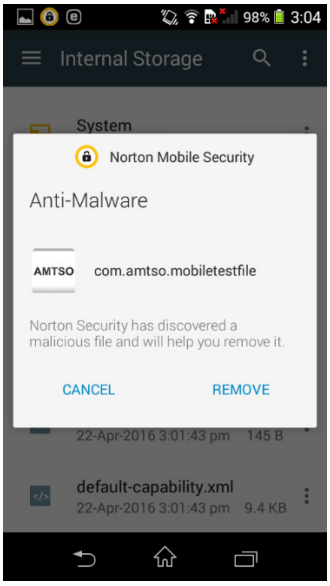

Figure.20 Norton detects the malware in the malicious apk file and does not allow the user to install the malicious apk.

When we chose the option to autoscan the malicious apk using Norton antivirus before installing the malware, Norton immediately determined the presence of malware and alerted the user and provided the user to only remove the apk file from the mobile device.

3. **Scan with ESET before**

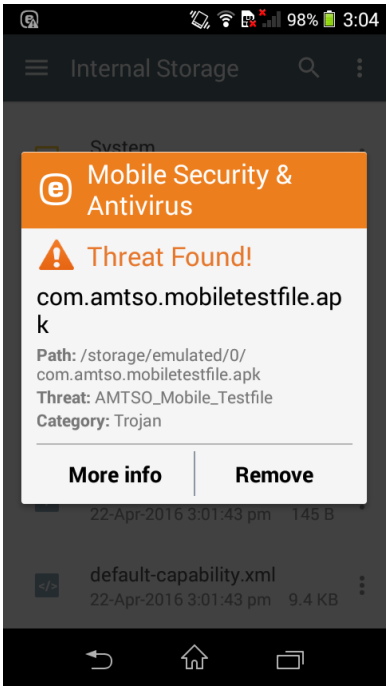

Figure.21 ESET alerts the user of the malware detected in the mailicious apk

Unlike Norton, ESET determined the category of malware as Trojan. Norton alerted the user about the malware and it did not describe the type of the malware. In ESET scan, when the user chose the option More Info he/she is provided with the below Threat Details.

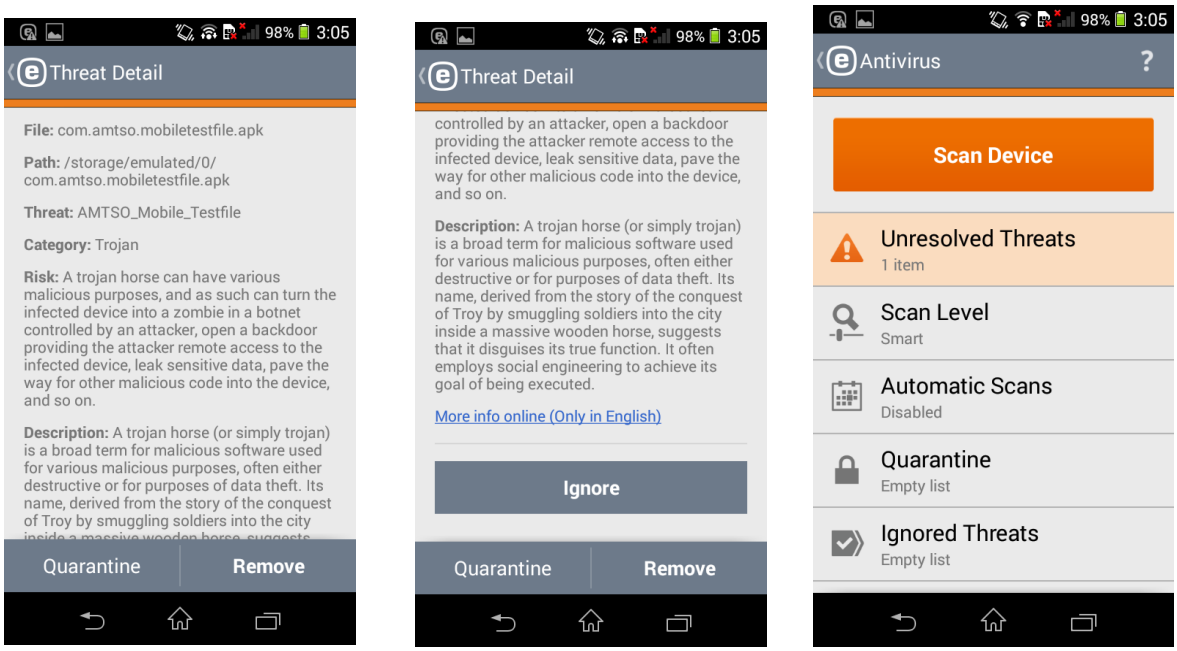

Figure.22 Threat details about the malware in the user's mobile device

Also, the user is provided with the following options:

a. Quarantine
Quarantine moves the malicious apk file to a different isolated location to ensure that the malware does not tamper with the file system of the mobile device.

b. Ignore
The Ignore option is provided to the user at the end of the Threat details section. The chances of the malicious apk being determined as a malware even though the apk is not a malware exists due a high false positive rate, so the user is provided with an option to ignore the apk file at their own risk.

c. Remove
Remove option deletes the malicious apk file from the mobile device.

The ESET antivirus also provides a notification to the user, prompting them about the unresolved threat.

4. Comodo
When the user chooses the option to install the apk file using Comodo, the antivirus software just scans the malicious apk and does not find the malware. It just provides the user an option to install the malicious apk file.

Evaluation of the antivirus softwares based on the malicious AMTSO apk file with a Trojan

Antivirus	AutoScan by Default	Detect Malware
Norton	Yes	Yes
ESET	Yes	Yes
McAfee	No	No
Comodo	Yes	No

Table.4 Evaluation of the antivirus softwares based on the malicious AMTSO apk file with a Trojan

2. **Evaluation of Malware Trojan in AV.apk**
    a. **Evaluation of Trojan in AV.apk by Norton**

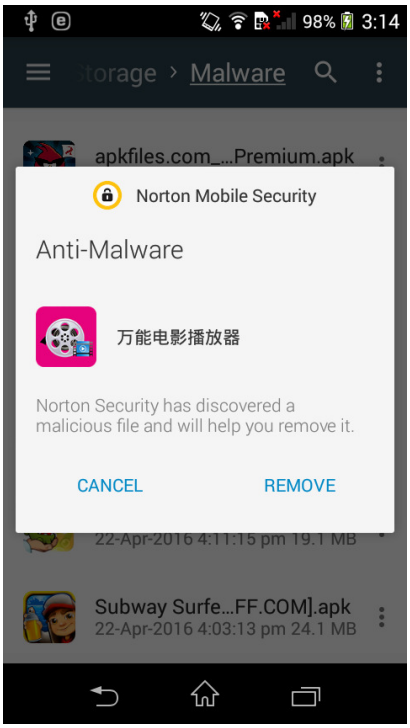

Figure.23 Norton detects the Malware

During the autoscan before installing the apk file, Norton antivirus detects the malware

a. **Evaluation of Trojan in AV.apk by ESET**

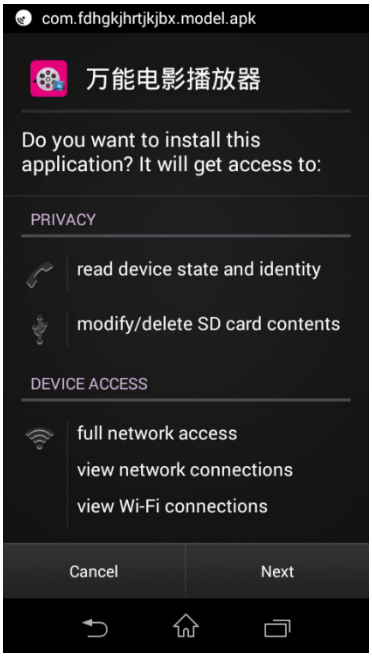

Figure.24 ESET does not detect the Malware

When the user, chooses the option to scan using ESET before the malicious file is installed, ESET does not detect the Trojan.

Metadefender Analysis of Trojan in AV.apk

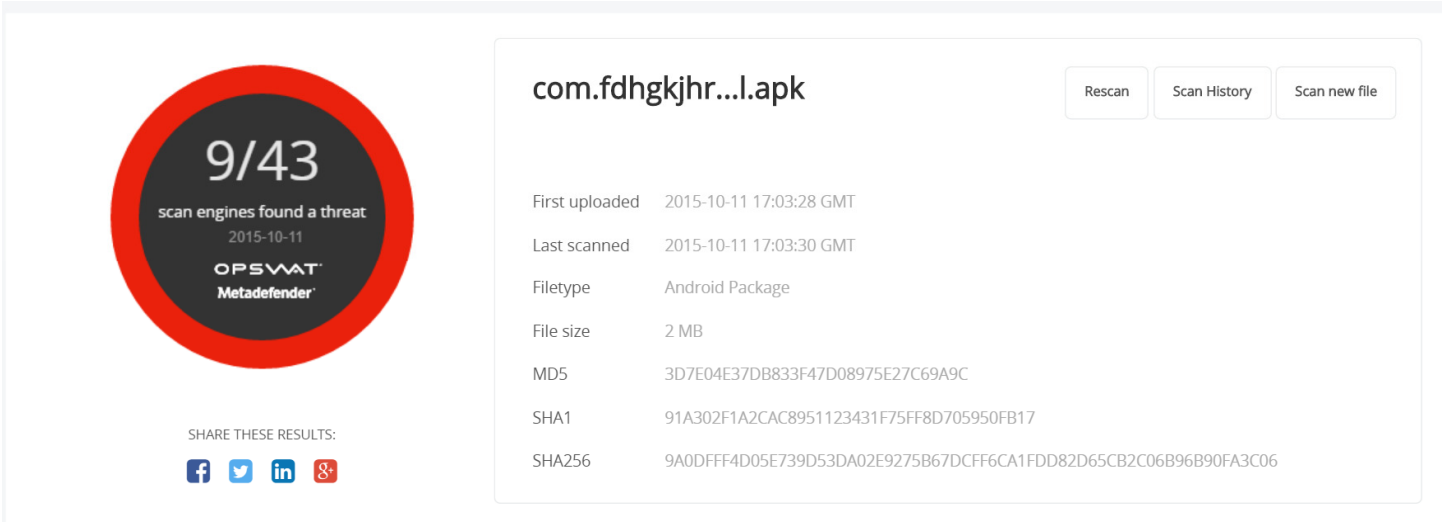

Figure.25 Analysis of the apk file by Metadefender and detects a threat by 9 different scan engines

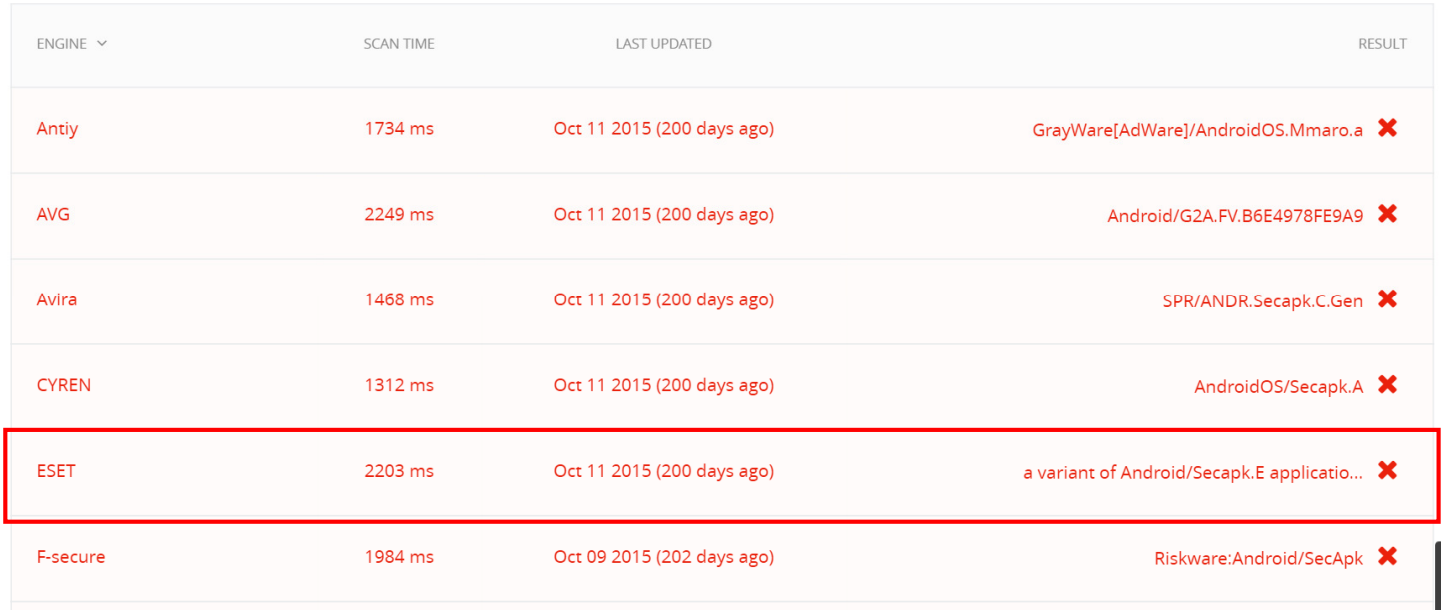

Figure.26 ESET scan engine detects the malware in Metadefender but does not detect the malware on the mobile device

Evaluation of the antivirus softwares based on the malicious AV.apk file with a Trojan

Antivirus	AutoScan by Default	Detect Malware
Norton	Yes	Yes
ESET	Yes	No
McAfee	No	No
Comodo	Yes	No

Table.5 Only Norton have detected the malware successfully which has been proved by Metadefender as a malware

3. **Evaluation of Malware FaceRecognition.apk**

   a. **Evaluation by Norton**

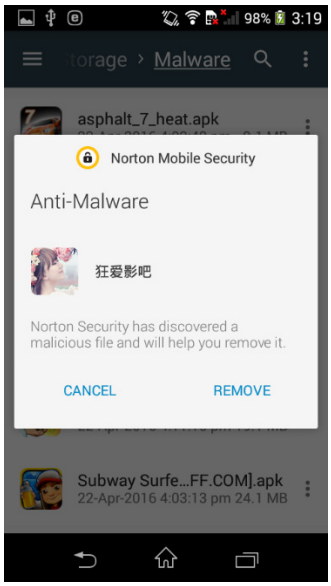

Figure.27 Norton detects the malware

   b. **Evaluation by ESET**

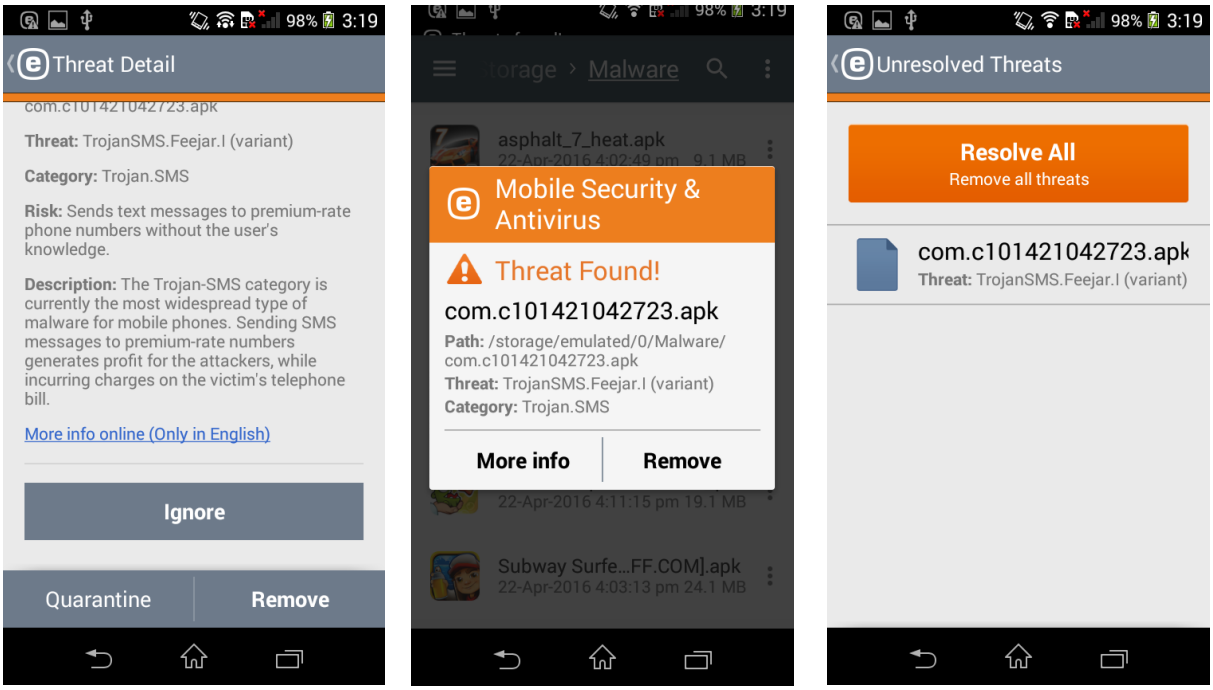

Figure.28 ESET detects the SMS Trojan in the malicious apk file

Evaluation of the antivirus softwares based on the malicious FaceRecognition.apk file with a Trojan

Antivirus	AutoScan by Default	Detect Malware
Norton	Yes	Yes
ESET	Yes	Yes
McAfee	No	No
Comodo	Yes	No

Table.6 Norton, ESET and McAfee have detected the malware as SMS Trojan successfully

4. **Evaluation of Malware BadNews**

a. **Evaluation of malicious apk Bad News by Norton**

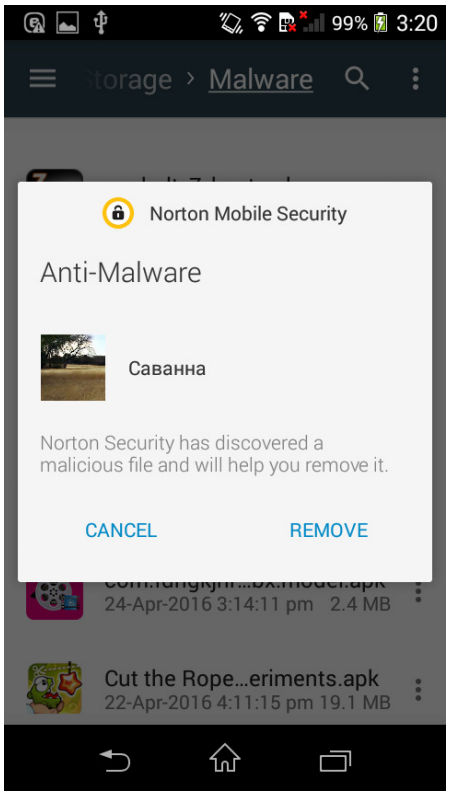

Figure.29 Malware detected by Norton

b. **Evaluation of malicious apk Bad News by ESET**

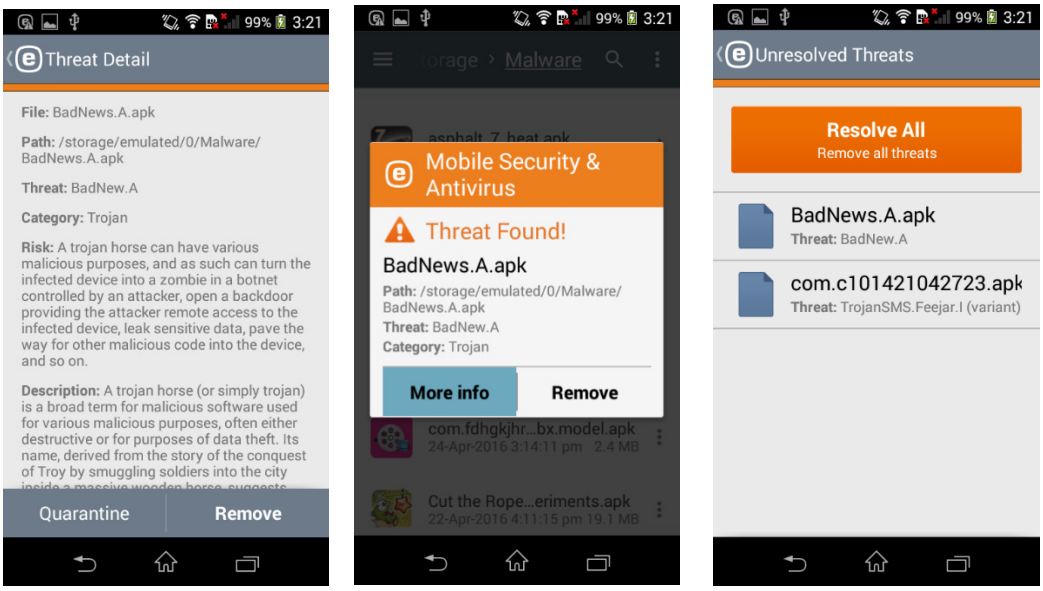

Figure.30 Trojan Detected by ESET

Evaluation of all the malicious apks by running a Scan using McAfee

After adding all the malicious apk files to the mobile device, since McAfee did not provide an option to auto scan the app by default, we performed a manual scan of the mobile device and McAfee said the mobile device was protected and did not consider the malicious apk files as a threat, as shown in the below figure.

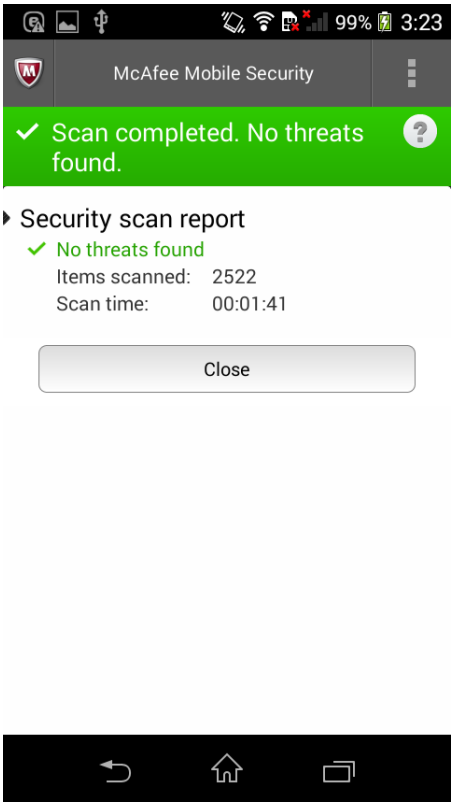

Figure.31 None of the malicious apk files were detected by McAfee during the scan

Evaluation of all the malicious apks by running a Scan using Comodo

Eventhough Comodo provided an option to scan the apk files before installing, the option did not work, so we tried to scan the files in the mobile device by using Comodo and it did not detect the malicious apk files.

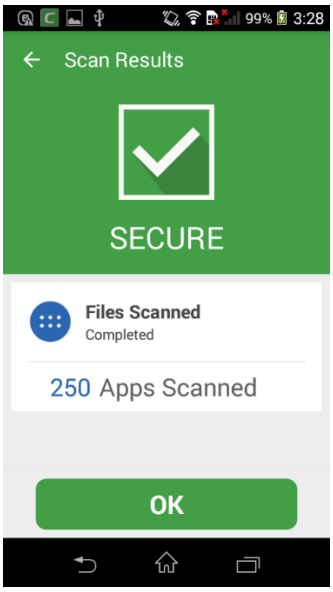

Figure.32 Comodo scan that did not detect the malicious apk files in the device

Evaluation by performing a full scan using Norton and ESET

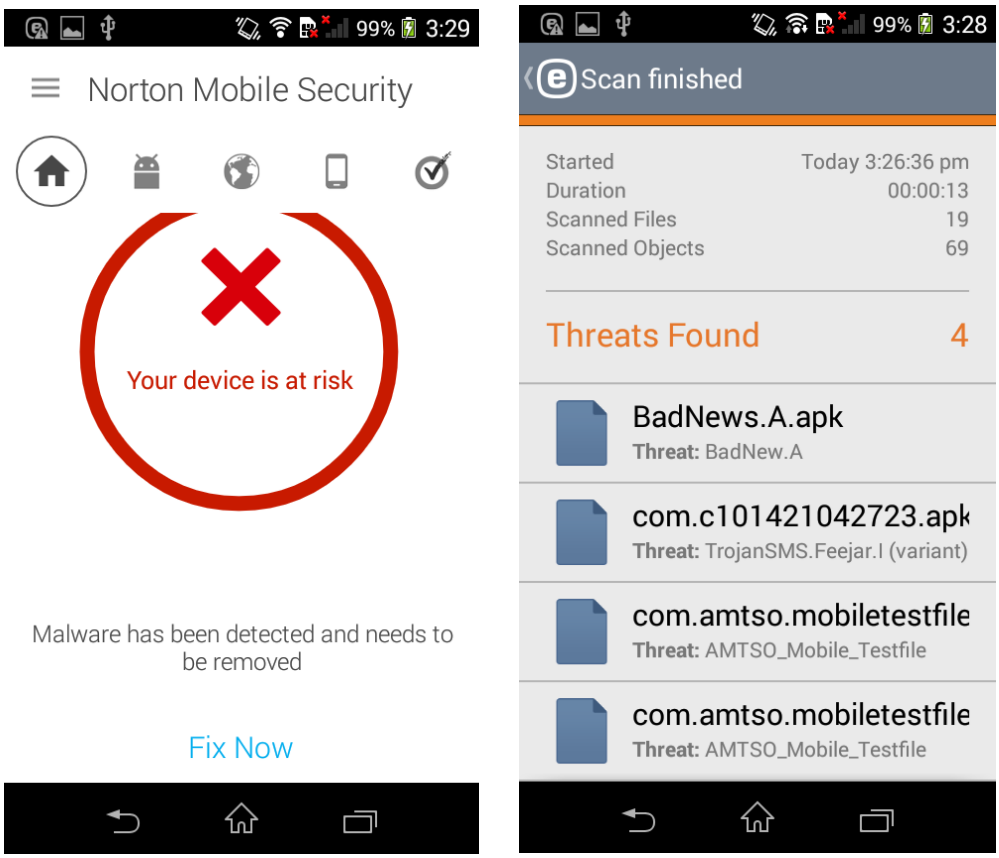

Figure.33 Norton and ESET detected the malwares in the malicious apk files and alerted the user

Evaluation of the antivirus softwares based on the above results

	AutoScan by Default	Detect Malware			
		AMTSO.apk	AV.apk	FaceRecognition.apk	BadNews.apk
Norton	Yes	Yes	Yes	Yes	Yes
ESET	Yes	Yes	No	Yes	Yes
McAfee	No	No	No	No	No
Comodo	Yes	No	No	No	No

Table.7 Evaluation of the antivirus softwares based on the above results

Conclusion

Based on the features offered by the antivirus softwares, McAfee provides the maximum features for free compared to Norton, Comodo and ESET. But McAfee did not detect the malwares in the malicious apk files according to our experimental attack. The next best antivirus software that provides a lot of features is Norton antivirus which detected all the malwares in the malicious apk files.

The four malicious apk files were detected only by Norton as malwares. ESET failed to detect one apk file and McAfee and Comodo failed to detect all the malicious apk files as Malwares.

Based on the attack tree and the methods of entry determined by us, after the research we have proof that Norton antivirus protects the mobile device against malicious apps being installed on the mobile device.

In order to provide a zero-day vulnerability protection, Norton provides with Proactive Exploit Protection where immediate updates for any apps that could be infected in the future by sending out a fix to delete the malicious code as soon as it was discovered.

Norton antivirus is the recommended antivirus software based on the criteria and the experimental attack in our research project.

References:

1. http://www.rsaconference.com/writable/presentations/file_upload/mbs-w01_v2.pdf
2. http://dl.acm.org/citation.cfm?id=2661696
3. https://www.nowsecure.com/resources/secure-mobile-development/primer/mobile-security/
4. http://research.microsoft.com/en-us/um/people/helenw/papers/smartphone.pdf
5. https://datatheorem.github.io/resources/DataTheorem.MobileAppThreatModel.pdf
6. https://nakedsecurity.sophos.com/2012/08/01/black-hat-dont-stand-so-close-to-me-an-analysis-of-the-nfc-attack-surface/
7. https://play.google.com/store/apps/details?id=com.wsAndroid.suite&hl=en
8. https://play.google.com/store/apps/details?id=com.eset.ems2.gp&hl=en
9. https://play.google.com/store/apps/details?id=com.comodo.cisme.antivirus&hl=en
10. https://play.google.com/store/apps/details?id=com.symantec.mobilesecurity&hl=en
11. http://readwrite.com/2013/04/23/5-signs-Android-smartphone-infected-malware/
12. http://www.Androidcentral.com/help-my-Android-has-malware
13. http://thehackernews.com/2016/02/secure-Android-phone.html
14. https://www.sans.org/reading-room/whitepapers/commerical/choosing-anti-virus-software-784