Global Information Assurance Certification Paper

Mobile A/V: Is it worth it?

GIAC (GCIH) Gold Certification and ISE 5501

Author: Nicholas Dorris, Nicholas.r.dorris@gmail.com
Advisor: *Johannes Ullrich*

Accepted: 5/18/19

Abstract

In the mid 2010's, mobile devices such as smartphones and tablets have become ubiquitous with users employing these gadgets for various applications. While this pervasive adoption of mobile devices offers numerous advantages, attackers have leveraged the languid attitude of device owners to secure the owner's gadgets. The diversity of mobile devices exposes them to a variety of security threats, as the industry lacks a comprehensive solution to protect mobile devices. In a bid to secure their assets and informational resources, individuals and corporations have turned to commercial mobile antivirus software. Most security providers present mobile versions of their PC antivirus applications, which are primarily based on the conventional signature-based detection techniques. Although the signature-based strategy can be valuable in identifying and mitigating profiled malware, it is not as effective in detecting unknown, new, or evolving threats, as it lacks adequate information and signature regarding these infections. Mobile attackers have remained ahead via obfuscation and transformation methods to bypass detection techniques. This paper seeks to ascertain whether current mobile antivirus solutions are effective, in addition to which default Android settings assist in the prevention or mitigation of various malware and their consequences.

1. Introduction

Mobile security breaches have increased steadily, which aligns with the increase in the number of mobile device users. For most organizations that rely on their networked resources, the mobile devices in use serve as both key assets and threat entry points. Such devices are considered assets, as they not only enable the swift flow of information across employees, branches, and regions but also remotely facilitate in the ongoing management of organizational operations. On the contrary, mobile devices serve as a threat entry point should they fail to implement appropriate information security or cybersecurity mechanisms. A direct consequence of such a failure could be an easy entry of malware into the organizational network to inflict harm. Indeed, damage is not limited to theft of information but extends beyond to include damage to the operational and technical environment, causing a stoppage of the information and communication technology infrastructure in its entirety.

It is also worth noting that consequences are linked with personal use of mobile devices in the absence of rigorous security measures. Here, mobile devices primarily refer to smartphones and Tablet PCs that typically comprise an LED or OLED touchscreen. Nonetheless, regardless of the type of mobile device in use, security threats remain unrestricted. According to the Verizon Mobile Security Index, "Mobile devices now have access to much of the same valuable corporate data—customer lists, bank details, employee personal data, billing information and much more—as those using fixed connections. And many also hold the credentials that we use to access other resources, including the numerous cloud services that employees now depend on to do their jobs" (Verizon Mobile Security Index, 2019). The "mobile phone as an appendage" is more apparent than ever, whether or not an individual is "on the clock."

According to a recent research report, approximately one fifth of the total IT professionals working for different organizations experienced some form of data breach involving a mobile device (Hamblen, 2016). Most of these breaches were linked to an abrupt increase

in mobile devices usage, including smartphones and tablets within the workplace (Hamblen, 2016). This research further highlights that at least 24% of the participants reported connecting their mobile devices to malicious Wi-Fi hotspots, while 39% had downloaded malware through their mobile devices while at work (Hamblen, 2016). Concerns related to the lack of controls on the Bring Your Own Device policy were raised as part of the research study (Hamblen, 2016). In 2017, a major breach involving mobile devices occurred via the free-to-play mobile game called Family Farm Seaside, resulting in the exposure of user-specific information of 3.3 million users (DiGiacomo, 2018). During the same year, the Malaysian Telcos and mobile virtual network operators were targeted with a massive hack attack that leaked the information of 46.2 million mobile phone users, including phone numbers, names, and addresses, along with the IMEI numbers of mobile devices (DiGiacomo, 2018). Additionally, Reliance Jio, a prominent mobile service provider in India, was struck by a similar attack that exposed user IDs, phone numbers, email addresses, and other personally identifiable information of 120 million customers via the mobile network (DiGiacomo, 2018). With the current culture of everything being tied to a virtual identity, this presents problems at several levels, such as: personal business, professional business and social media.

1.1 A Brief Overview of Mobile Antivirus

A mobile antivirus is essentially an antivirus software developed exclusively for the respective mobile operating system. The purpose of a mobile antivirus is to protect against malware, Trojans, viruses, hacking, and other forms of data breaches. Commonly-used mobile operating systems include Android, iOS, and Windows, while less - commonly- used systems include Blackberry, Bada, MeeGo, Palm OS, and Symbian OS. Although each of these operating systems possesses distinct features and interactive attributes, their general purpose is homogenous: to enable mobile device users to interact with the mobile devices and perform a range of computing operations. As with any conventional antivirus program, a mobile device antivirus software repeats the same task

of continuously screening the system to promptly identify, avoid, and neutralize external threats that could otherwise result in an information security breach.

Antivirus programs functions in a systematic and sequential manner. First, the mobile device antivirus scans the directories and partitions within the internal and external storage drives of the device in question (Rosencrance, 2018). It comprises a set of known malicious patterns, which it uses to automatically compare the directories, files, and folders to detect threats. Second, it allows the end user to schedule daily, weekly or monthly scans to perform similar functions (Rosencrance, 2018). Some antivirus software even allows users to schedule scans on a per-install basis, in which each application is scanned for malware upon the first installation. Third, the antivirus allows users to manually initiate virus or malware scans at any time while selecting specific directories, files, or folders that are likely to be breached (Rosencrance, 2018). Finally, it allows users to quarantine and completely remove the identified malware to ensure a more secure user experience (Rosencrance, 2018).

Recognized as signature-based detection, almost all antivirus programs function similarly. However, nominal differences could still exist based on the mobile operating system involved. Considering that Android OS is the most used mobile device OS in the world, used by 65.53% of global users as opposed to 32.34% of iOS users, this paper focuses on Android OS and the mobile antivirus software designed for it (Mybroadband Staff Writer, 2017).

One may also argue as to which types of mobile devices require an antivirus. From this perspective, it is debatably true that mobile devices that are engaged for personal and professional purposes are both susceptible to threats. Information security breaches, hacking, malware attacks, and Trojan viruses are only a few of the more common threats, in addition to man-in-the-middle attacks and ransomware. Undoubtedly, mobile devices that are either lost or stolen also are susceptible to prominent threats. Mobile devices used for personal reasons contain both generic and classified information

that, if leaked, could be severely damaging. They generally contain information such as images, videos, text messages, entire social media conversations, and other private data, that is not intended to be exposed to third parties. Contacts, emails, email attachments, downloaded files, and sensitive mobile applications, such as mobile banking applications in which the usernames and passwords are stored are also among significant types of information that could be breached, stolen, and even sold over the dark web. According to Google Inc., its trademark Google Photos application that allows users to back up and store their images and videos on the cloud, was used by 500 million users who had uploaded approximately 2.1 billion photos on a daily basis (Matney, 2017).

Mobile devices used for professional purposes are at a greater risk of the aforementioned threats, primarily due to the highly sensitive and classified information that they carry. For instance, client-specific data, details on suppliers, inventory, plans for growth and development of the organization, manufacturing secrets, and financial data could be breached in the absence of antivirus software. This could eventually result in dire outcomes. It is therefore viable to argue that mobile devices, whether they are for personal or professional use, must have an antivirus software installed to protect against the rising threats and vulnerabilities. A research report by Ismail (2017), published on the Information Age website, highlighted the absence of up-to-date security patches across Android mobile devices as a major reason behind rising security breaches and the use of custom ROMs, Jailbroken ROMS, and cracked Country Locks, which are common across major Android smartphone manufacturers. The lack of proper physical protection of digital intellectual property, including mobile devices, while at the workplace is yet another loophole that can best be addressed by certain antivirus software that automatically lock the devices after a few seconds or minutes, depending on the user preferences assigned. In the absence of such physical protection, official mobile devices that are left with several files running could be compromised by a guest or an insider while the data owner is unaware.

1.2 Thesis Statement

The current research study contends that the existing state of mobile device security is weak. By installing strong mobile antivirus software, end users of Android-based mobile devices can implement a series of settings and security tweaks, including anti-malware, anti-theft capabilities, remote data wipe, SMS blocking, private space, and traffic monitoring, among others. In addition, several antivirus software accompany a stock lock screen that mandates the use of a device lock, pin, pattern, or password. Intruder detection is yet another key, built-in feature of many mobile antivirus software that could be implemented to quickly take a picture of any intruders and send the picture via email to notify the owner. Thus, this research aims to determine the extent of the effectiveness of some well-known mobile antivirus programs while also identifying the set of innate—default—Android OS security settings that could facilitate in both the mitigation and prevention of malware attacks.

2 Background Study

2.1 Use of Mobile Devices

The nature and severity of the problem which requires an effective resolution can be best comprehended by elaborating the widespread use and adoption of mobile devices. In 2016, 62.9% of the world's population possessed a smartphone (Statista.com, 2019). This penetration of mobile phone ownership is projected to increase by at least 5%, to reach 67%, by the end of 2019 (Statista.com, 2019). According to the most recent statistics, the total number of mobile phone users reached 5 billion worldwide (Statista.com, 2019). This depicts a 4.68% increase in the number of global smartphone users compared to 2017, when this number was lower (Statista.com, 2019). Consider Figure 1 below:

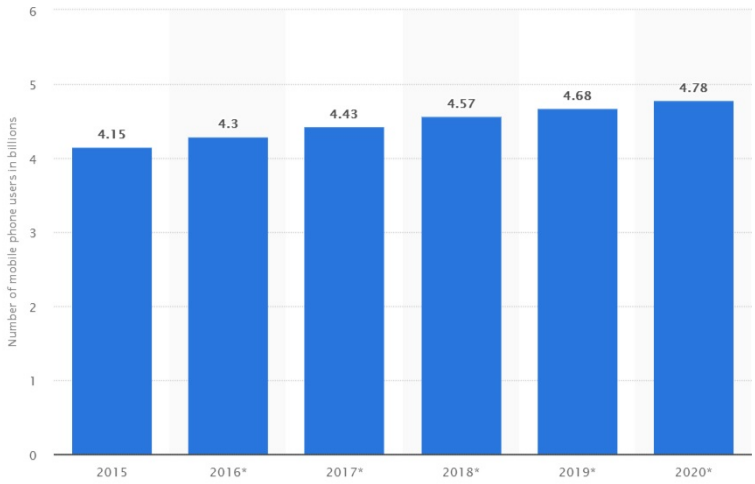


Figure 1 Increase in Smartphone Usage (Statista.com, 2019)

While Figure 1 depicts the widespread use and adoption of smartphones, the same survey further projects that this number will continue to grow in the coming years. Among countries with the highest number of smartphone owners and users, China and India represent the top of the list with 1.5 billion and 1 billion users, respectively (Statista.com, 2019). Much of this growth is attributed to the increasing popularity of smartphones (Statista.com, 2019). Thirty-eight percent of global mobile phone users were smartphone users in 2014, while this percentage has increased to 50% as of 2018 (Statista.com, 2019). The trend is somewhat similar: at least 25 million Android tablet PCs were sold by Samsung alone in 2017, while the total number of tablet PC users on a global scale reached 1.49 billion in the same year (Statista.com, 2019). The widespread use and ownership of tablet PCs is depicted in Figure 2 below:

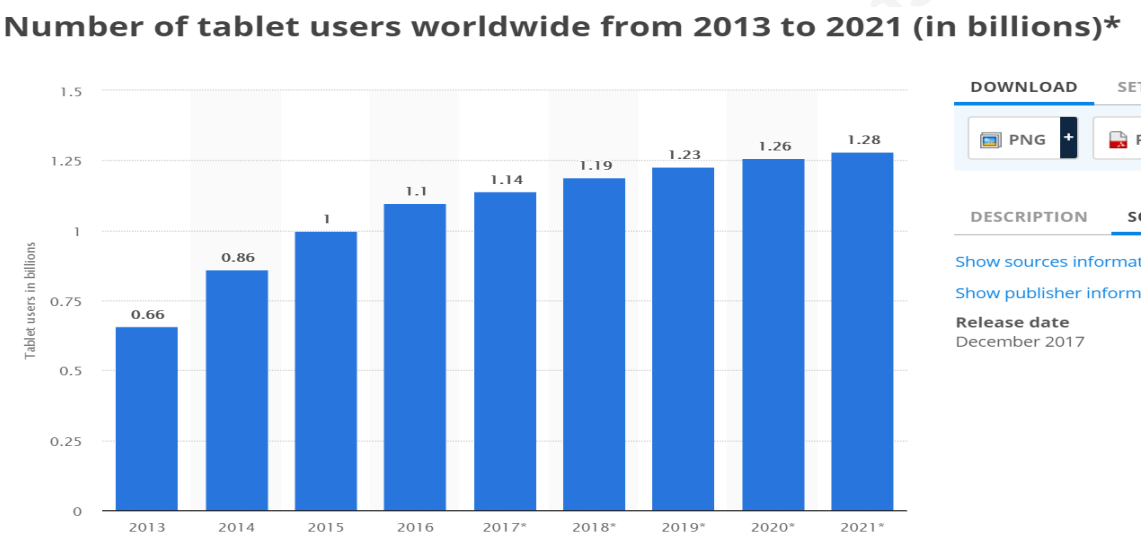


Figure 2 Increase in Tablet PC Usage in Billions (Statista.com, 2019)

Based on Figure 2, the substantial increase in use and ownership of tablet PCs is evident: this number increased from 0.66 billion users in 2013 to 1.23 billion users in 2019 (Statista.com, 2019). This number further projects to increase in the coming years to reach 1.28 billion in 2021 (Statista.com, 2019).

2.2 Android OS Structure

2.2.1 File Structure

The Android OS leverages the capabilities of the Linux file system structure with a single root, as depicted in Figure 3 below:

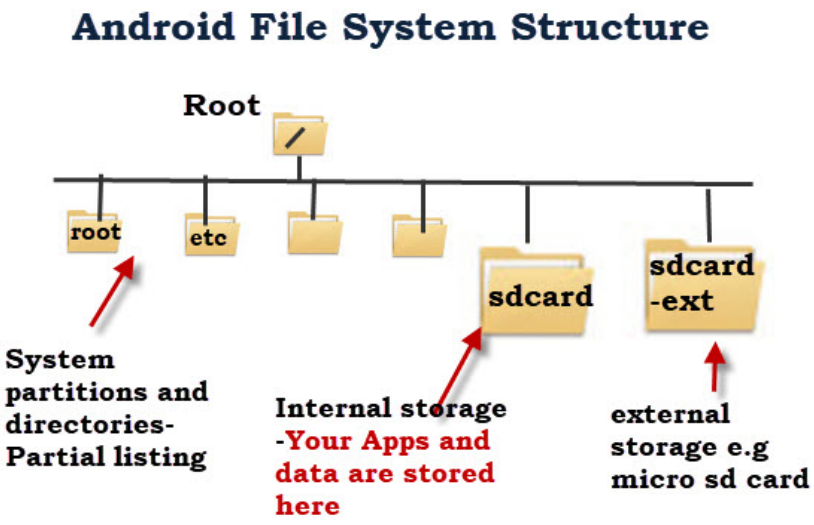


Figure 3 Overview of Android OS File Structure (Steve, 2017)

In general, the Android OS protects the directories and partitions unless the end users have rooted their devices, which provides easy access to these components (Steve, 2017). Contrary to the Windows OS that uses drive letters, the Android OS presents partitions and physical disks under the root as directories, similarly to UNIX (Steve, 2017). Generally, no default file manager accompanies the OS; however, certain device manufacturers using newer versions of Android OS provide a file explorer. Otherwise, end users must download third-party file managers to access, manage, and organize file structures (Steve, 2017). User files and data are stored in the sdcard partition, which also is also comprised of application settings and data (Steve, 2017). Regardless of the presence of an external sdcard, the Android OS still possesses an sdcard partition. Opening the sdcard partition presents a list of files and folders, similar to Figure 4 below:

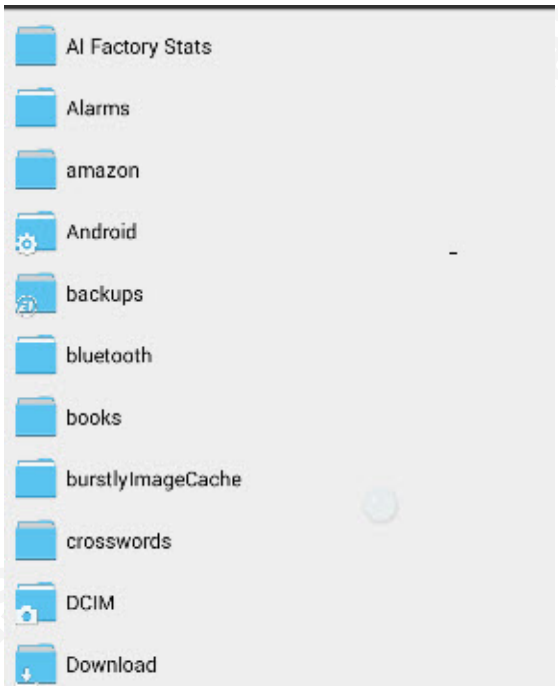


Figure 4 Overview of SDCARD Partition in Android (Steve, 2017)

Key data and files included within these file directories and partitions include images, audio files, documents, videos, and other forms of multimedia. Regarding file associations, the Android OS uses an application to open specific file extensions and types, such as .doc, .docx, pdf, and .RAR files. As soon as the file extension is tapped, it might prompt a message to select the preferred program from the "Complete Action Using" dialog box, in which clicking the "Always" button causes the default application to open similar file types in the future.

2.2.2 Permission Structure

Similar to every major operating system, Android OS requires end users to allow a series of permissions before they can use the underlying applications and features. These permissions pertain to hardware-related and software-related permissions. Hardware-related permissions prompt the end user to allow or deny access to various hardware components of the mobile device, including cameras, the microphone, GPS,

and sensors. On the other hand, software-related permissions could include the ability to read/write text messages and access multimedia files in the Gallery application, among others. While these permissions are generally mandatory for a variety of applications to function swiftly, others could require needless access to hardware or software, which must be manually regulated by the end user.

The central purpose of embedding permissions within the Android OS is to ensure that the mobile user's data is always kept private and confidential. However, users need to be wary in allowing or denying these permissions, as some permissions could grant access to unnecessary user-specific data. Alternatively, denying permissions to certain programs and settings within the Android OS might render the mobile device vulnerable to key threats. By default, the permission structure across all the Android OS versions is that no application is allowed permission to access any hardware/software, which could also serve as a precautionary measure.

2.3 Evaluation of Mobile Malware

Key insights into the effectiveness of mobile antivirus will be best achieved by evaluating mobile malware. This necessitates the identification and evaluation of common threats, their origins, and the underlying consequences.

2.3.1 Common Threats to Mobile Devices, Origins, and Consequences

Considering empirical evidence gathered from a highly reliable source, the common threats to mobile devices include data leakage, unsecured Wi-Fi, network spoofing, and spyware (Kaspersky, 2019). This list extends to include malware infections and identity theft.

2.3.2 Data Leakage

The history of data leakages or breaches dates to when users began storing their data across computing devices (Kaspersky, 2019). Perhaps the most prominent threat to

mobile devices is data leakage, which could eventually result in identity theft. Data leakage is almost always inadvertent and occurs when a user downloads and installs mobile applications (Kaspersky, 2019). Certain mobile applications are identified as "riskware," as they demand the end users to provide permission to almost all the hardware embedded within the mobile device and linked software, thereby opening access to private data (Kaspersky, 2019). Such mobile applications are known to report personal and organizational data to their respective remote servers, where it is vulnerable to further mining and planning cybercrimes such as identity theft (Kaspersky, 2019). Moreover, hostile enterprise-signed mobile applications powered by specialized malware could result in data leakage via the distribution of a unique code that exploits internal—unspecified—vulnerabilities to spread the confidential data across a variety of corporate networks without prompting any warnings or anomalies (Kaspersky, 2019).

2.3.3 Unsecured Wi-Fi

Another major threat to today's mobile devices arises when the devices connect to an unsecured Wi-Fi network or a network that is poorly secured through the default network password. The absence of WPA and WPA2 PSK leaves the Wi-Fi networks open, upon which cybercriminals can capitalize. Connecting to an unsecured Wi-Fi network indicates that all the data, files, communications, and transactions being performed through the device could become compromised. According to the report by Kaspersky (2019), a practical experiment involving three British politicians resulted in their social media, PayPal, and VoIP conversations being compromised.

2.3.4 Network Spoofing

First identified in 1989 by Steve Bellovin of AT&T as a security risk, network spoofing, or IP spoofing, involving fake access points established by hackers, has increased remarkably (Kaspersky, 2019). As soon as a mobile device connects to the fake access point, the device's data and communications can be easily intercepted by the hackers in

whatever manner they planned. Some attackers might even lure a potential victim into creating an account to access the free access point; several users employ the same user accounts and passwords across multiple services, which allows hackers to easily guess their login details on mobile banking services. A direct consequence is the breach of highly confidential details, including credit card numbers, bank account numbers, financial status, and streams of income, among others.

2.3.5 Spyware

Initially described in 1995 by Usenet, spyware can be defined as a program whose purpose is to monitor or track the online activities of an end user (Kaspersky, 2019). Such spyware is commonly utilized by spouses, bosses, and coworkers to keep track of the activities, conversations, and transactions in which their counterpart is involved (Kaspersky, 2019). Tracking internet habits, monitoring the number of website visits, and even revealing personal details of users are some prominent consequences of this threat.

2.4 Discussion of Mobile Antivirus

2.4.1 History of Mobile Antivirus

The history of mobile antivirus is as old as the first reports of the mobile malware dubbed Cabir in 2004, which was essentially a worm transmitted via Bluetooth and displayed the message "Caribe" upon phone startup, followed by the reports of CommWarrior in 2005 and RedBrowser in 2006 (ESET, 2016). In an attempt to neutralize mobile malware, the first mobile antivirus programs were developed. However, it was not until 2017 that the complete and dedicated mobile antivirus software, such as AVG, Avast, and McAfee, had been completed.

2.4.2 The Development of Mobile Antivirus

A report by Tripwire highlighted the potential inability of openly securing mobile devices via an antivirus due to SDK and other available toolkits (Tripwire, 2013). However, it is

reasonable to argue that the steady increase in mobile malware and threats triggered the development of mobile antivirus software. Originally developed to identify, detect, and remove viruses, Trojans, and malware from traditional computers, antiviruses were further diversified to support the more innovative mobile computing powered by Android-based smartphones and tablet PCs (Tripwire, 2013). Unlike computer antivirus programs, mobile antivirus programs were developed to offer limited functionality—Specifically, the ability to protect against ransomware, denial of service, and distributed denial of service attacks. Over time, as mobile device breaches witnessed a steady increase, mobile antivirus software also began to diversify regarding capability and functionality. Today, mobile antivirus software has been developed to such an extent that companies offer rigorous security accompanied by a variety of security features that suit today's needs. These include remote data wipe, password protection, real-time virus and malware scanning, virus removal, Wi-Fi network scanning and protection, multimedia vaults, find-my-phone, anti-theft functionality, and remote locking capabilities.

2.5 Popular Mobile Antivirus Applications

2.5.1 Avast Antivirus

According to a recent report, the Avast Antivirus application was declared the top mobile antivirus platform (Drake, 2019). Key features include the ability to remotely wipe the mobile device's data in the event of theft or should the device be lost (Drake, 2019). Additionally, it offers a mobile firewall enhancement accompanied by basic antivirus functions such as call blocking, an anti-theft feature, and VPN (Drake, 2019). Most importantly, the antivirus is free to download from the Google Play Store.

2.5.2 BitDefender

Similar to Avast Antivirus, BitDefender also is free to download from the Play Store and offers automatic, scheduled, and manual antivirus scans to end users. The antivirus remains running in the background, frees up storage space and resources, and

enables longer battery life (Drake, 2019). Additionally, a built-in privacy advisor tool that provides an added layer of security to the end users is included.

2.5.3 Kaspersky Lab

Kaspersky Lab is another high-quality antivirus application available on the Google Play Store that effectively sniffs out and neutralizes malware (Drake, 2019). Moreover, it allows end users to block malicious links or websites and boasts a detection rate of 99.9%, as revealed by the AV-Test trials conducted in 2017 (Drake, 2019)., Automatic and scheduled scanning is available in addition to anti-theft, spam protection, and privacy advisor (Drake, 2019).

3. Analysis

3.1 Tools Utilized in the Experiment

The current research study utilized an array of tools, including Alcatel Raven LTE smartphones, Android 7.1.1 Nougat OS, mobile malware samples websites such as Koodous, VirusTotal, Kaspersky, Sophos, and McAfee Mobile Antivirus. There was also a service plan utilized for each phone and additional apps to perform basic diagnostics.

3.1.1 Alcatel Raven LTE Smartphones

Also recognized with the model number A574BL, Alcatel Raven LTE smartphones are powered by the Android 7.1.1 Nougat operating system and offer a compact design, a 5-inch TFT-TN Display, 16GB of internal storage, and 2GB of RAM (TFGuide.com, 2019). Powering the phone is the Qualcomm Snapdragon 210 chipset, clocked at 1.1 GHZ in a quad-core setting. The rear camera is a 5MP shooter, while the front camera boasts a 2MP lens. A 2200 mAh battery allows users to enjoy a seven-day standby time and up to 15 hours of talk time (TFGuide.com, 2019). Additional features include accelerometer and proximity sensors and hearing aid compatibility.

3.1.2 Android 7.1.1 Nougat

Released in August 2016, the 7.1.1 Nougat is one of the most -used Android versions across smartphones and tablets. It is the seventh major version of the Android OS that offers the split-screen multitasking feature, the Doze power saving mode, a recent applications button, a picture-in-picture mode, a refreshed notifications panel, bundled notifications, and direct reply features (Android Beat, 2016). The QuickSettings tile API, along with the redesigned settings menu, also are among the prominent enhancements of this OS version, in addition to Night Mode and Data Saver mode. Features that are relevant this research study include a strong file explorer, DPI scaling, and call blocking capabilities (Android Beat, 2016).

3.1.3 Websites for Mobile Malware Sampling

Since this research involves determining the effectiveness of mobile antivirus, the collection of mobile malware samples is a major aspect. To accomplish this, the following websites are utilized:

Koodous: This website serves as a rich resource for mobile malware samples, as it currently enlists 8,305,110 malware samples that perform various types of malicious activities.

VirusTotal: This website serves as a resource both for analyzing mobile malware and for retrieving key resources linked with mobile malware.

3.1.4 Mobile Antiviruses

For the current research study, three mobile antivirus platforms are used, including Kaspersky Lab, Sophos, and McAfee Mobile Antivirus. Sophos Mobile Security for Android is a real-time antivirus and threat-scanning software that protects mobile devices while also ensuring high performance and increased battery life. The McAfee Mobile Antivirus is developed by McAfee Labs and offers a unique set of tools and features that enable strong device protection against a range of malware. Kaspersky Lab, previously mentioned above, also provides similar features. The effectiveness of each of these antivirus platforms is tested.

3.2 Lab Setup

The process to baseline the smartphone was simple. Readying the smartphone entailed simply powering on, creating a Gmail account, updating to the available updates, enabling all of Google's services/protections, and activating the SIM. Three of the four phones tested had installed an A/V solution mentioned above, and a fourth phone was used as a control. After some consideration on how to best gather the technical information, it was necessary to install three additional applications to collect information regarding data. Two diagnostic applications, Phone Doctor Plus and Test your Android, were used to

provide CPU utilization, battery temperature, memory utilization, and other relevant data. Those statistics were collected and logged in an Excel spreadsheet for tracking purposes. The third installation was Dropbox, which is deemed the most effective method of transporting malicious APKs (Android Package). Perhaps the most vital setting modification to note was "allowing" installations of applications from unknown sources. This would allow the phone to install any application not included on the Google Play Store. The reasoning behind each decision during APK installation was that if the A/V notified me, then I would follow that advice, save for on the control phone. However, if an APK requested permissions or settings modifications, then those also would be followed. There would not be any priority on which is first, based on the expectation that an A/V would quickly detect the malware. This rule was ignored for the control.

3.2.1 Malware Samples

The malicious APKs were easily searchable on the Koodous database. The selected malware included different discovery dates, behaviors, uses, and demographic targets to best broaden the change at successful infection. Additionally, these were filtered via "rating=>-1" to search for samples rated as malicious. The list below contains either the name or the tag of the APKs used to best identify the behaviors.

Fuckers: An application that simply received a negative score.

Luck.APK: Metasploit/MSFVenom Reverse TCP shell.

MetaMask: An application tagged as an SMS Clipper (i.e., forwarding SMS messages to an outside resource).

Confirmacion: SMS/Hidden App Tagged APK: Tagged as an SMS and hidden application, the intent is to utilize the SMS functionality while also hiding from the user's gaze.

Flexnet Variant: An Android botnet.

Free Bitcoin: Anubis Variant: A variant of Anubis, a popular banking Trojan.

Exodus Variant: A recent spyware that is likely linked to the Italian government.

3.2.2 Fuckers

This APK had a "date submitted" of Sep 20, 2017, so the expectation was for the A/V to detect the malware quickly. On the control phone, Google Play Protect displays a notification warning a potential user prior to installation. After installation, the application then requests permissions that should not have been necessary for its functionality, but these are enabled for the purpose of this study. Shortly afterward, the application was no longer observed on the home screen or anywhere easily visible via normal operating conditions. The application was, however, still located via meticulous searching.

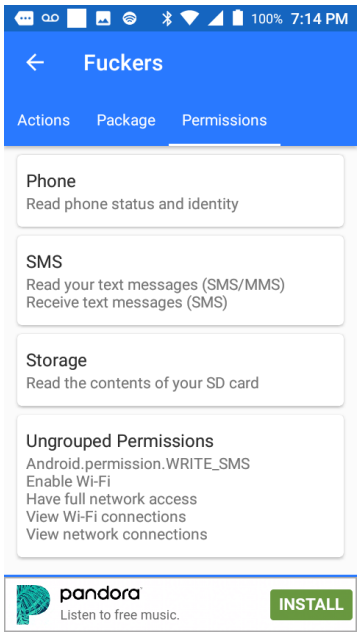
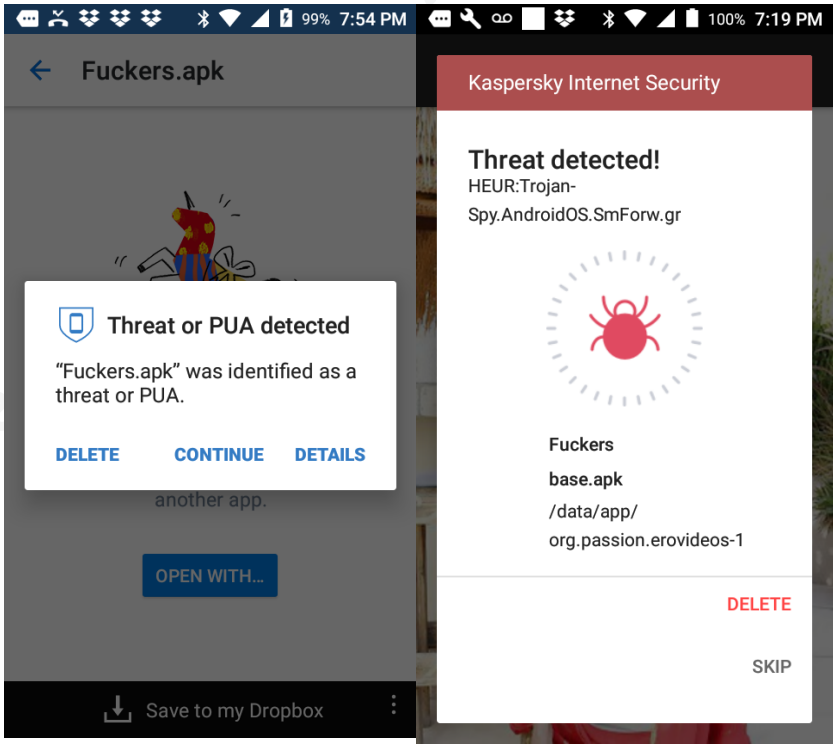


Figure 3 Malicious APK Permissions

The A/V-enabled phones produced better results, which appeared to be the beginning of a pattern. Both Kaspersky and McAfee allowed the application to download/install;

however, detection of a threat occurred within approximately five seconds. The approach of the Sophos differed in two aspects. First, an option was offered to "scan the link," which appears to scan the URL of the hosted file. Scanning the link would not be necessary, as the APKs were transported via Dropbox. Second, Sophos would scan the APK prior to installation, which would detect this APK as a PUA, a "potentially unwanted application," and would successfully not allow the download.



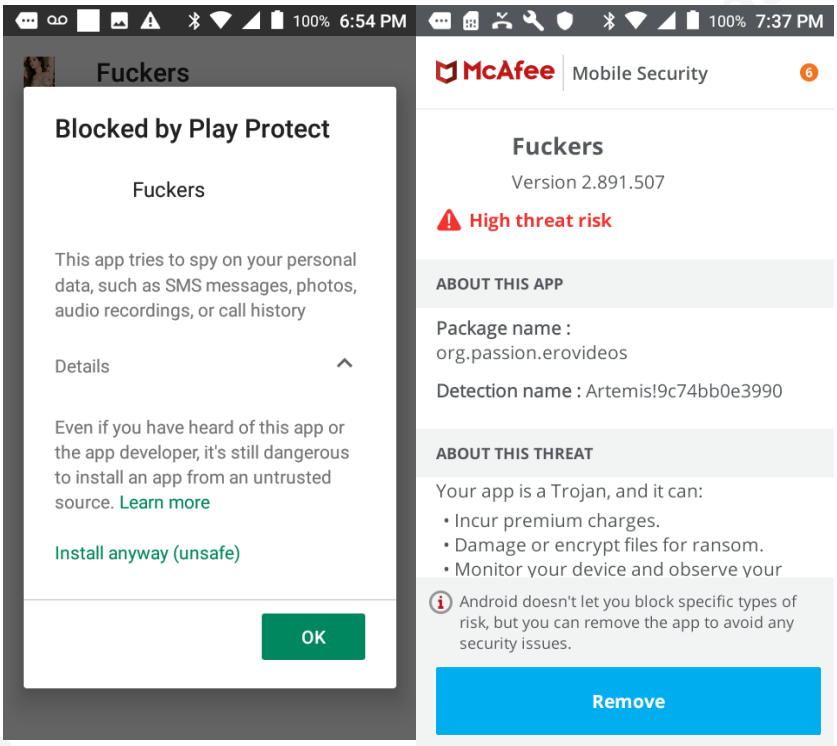


Figure 4 Most Consistent Interactions with Malicious APK

3.2.3 Luck.apk (msfvenom/metasploit)

This APK, titled "Luck.apk," was created via msfvenom and intended to create a reverse shell that could be accessed via meterpreter. The injection was successful on the control phone, though Google Play Protect did provide a prompt prior to installing again, advising against downloading/installation. The A/V-enabled phones again proved successful. The Kaspersky and McAfee A/Vs allowed the APK to install and then promptly displayed a notification of the threat and the prompt for deletion. However, it is important to note that a meterpreter session was still established prior to the APK's removal. Sophos once again did not allow installation due to its scanning functionality.

3.2.4 MetaMask (SMSclipper)

The MetaMask application was tagged as SMSclipper, which indicates it would clip SMS messages from a user's mobile device and forward the results to a third party. At one point, this application was available on the Google Play Store but was recently removed due to the discovery of malicious behavior. When attempting to install on any of the phones, Google Play Protect presented a different notification. It refused to allow the installation, and there was no way to bypass this.

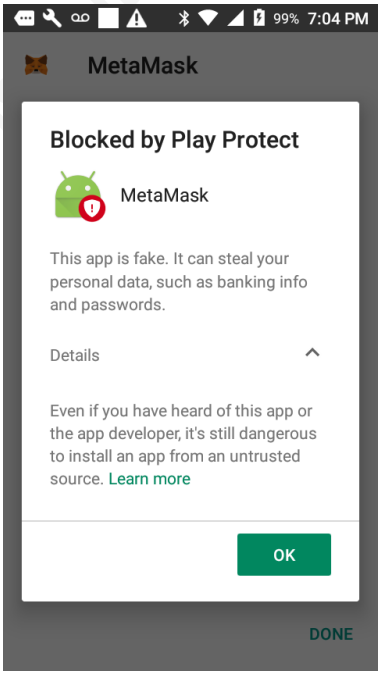


Figure 5 Google Play Protect in Action

3.2.5 Confirmacion (SMS)

This APK was selected due to it being discovered more recently than the others (March 9). On the control phone, after the Google Play Protect notification and eventual installation, the application presented a screen displaying "Hello World", requested SMS permissions to read/send, and shortly vanished from the application screen or home

screen. The results differed for each of the A/V devices. Kaspersky detected the threat and deleted it after the installation, as it had done previously. Likewise, Sophos reacted similarly to its previous uses. McAfee, on the other hand, allowed the application installation and did not detect it as a threat. Interestingly, over several days, 50 or more SMS messages were sent from the McAfee phone to an unknown phone, whose contents included the IP and MAC address of the phone. This is attributed to Confirmacion due to an Android-based warning regarding the application's involvement. The control phone did successfully send one message, but no others.

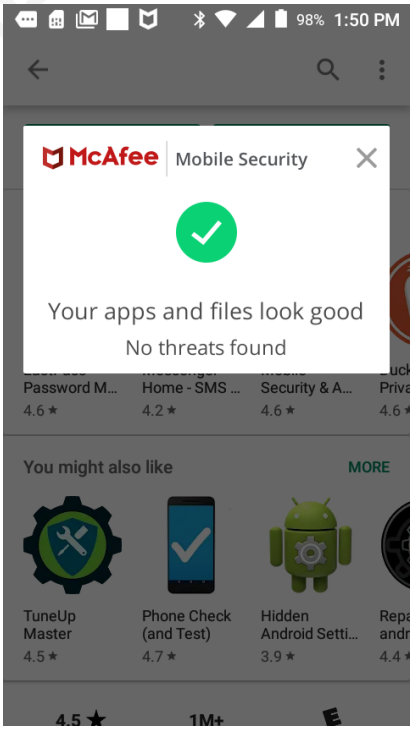


Figure 6 McAfee Failing to Detect Confirmacion

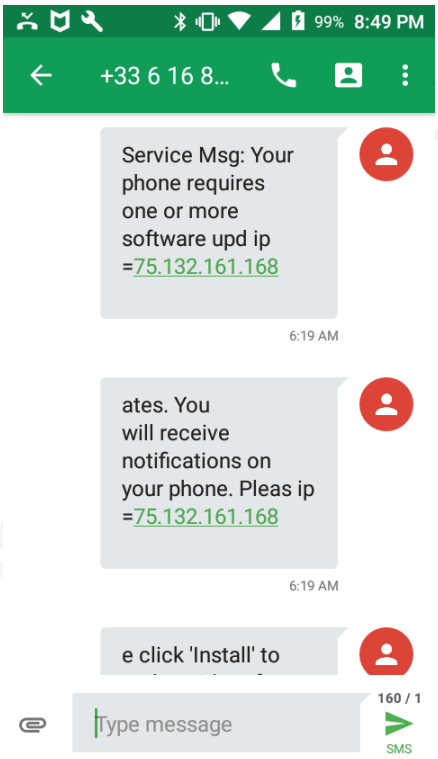


Figure 7 McAfee Phone Sending SMS Messages to an Unknown Recipient

3.2.6 Flexnet Variants (botnet)

These results were similar to those of MetaMask in that the APK was not allowed to install due to Google Play Protect. Two separate applications were tested, and the results were consistent across all phones for both cases.

3.2.7 FreeBitcoin (Anubis Variant)

This application caused the most interesting interaction between the APKs observed, as it forces the user to take action to modify new settings. On the control phone, after installation, the application noticeably forces the user to enable a previously

non-existent setting known as “Android Security”, and normal functionality is not restored until this is enabled.

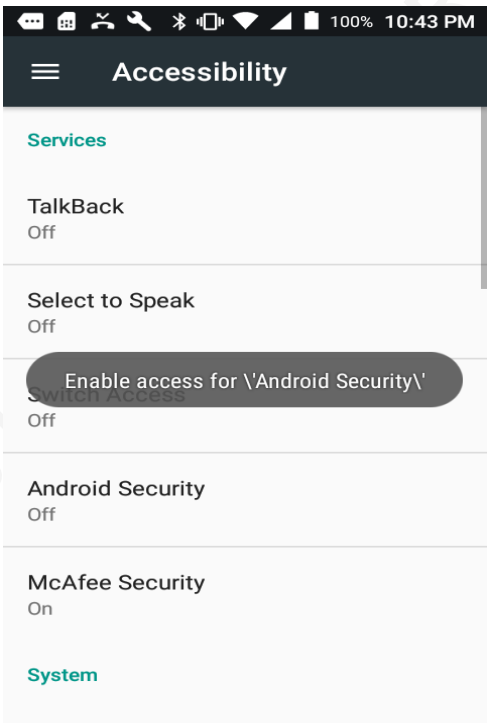


Figure 8 Android Security Permissions

Both Kaspersky and McAfee reacted identically, albeit detecting the threat. However, due to the study’s restraints, the Android Security setting was enabled because it not only appeared first but also redirected the phone's screen while fighting the A/V notification. After enabling this setting, a flurry of notifications appeared on the phone and were unable to be observed due to the various screens opening and closing too quickly. Both McAfee and Kaspersky still detected the threat, but they were unable to uninstall due to the window to click "delete" quickly disappearing. Sophos reacted as it had previously; therefore, no installation had ever occurred.

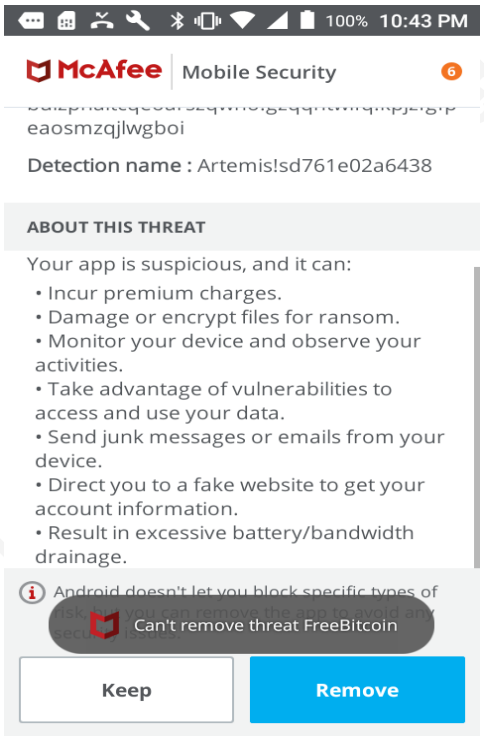


Figure 9 Unable to Remove the Application

3.2.9 Exodus Variants

The APK had been tagged as variants of Exodus, whose open source research indicates a link to the Italian government. The control phone once again displayed a warning via Google Play Protect but allowed the installation. The application then vanished from the home or application screen. The A/Vs had performed as they had previously, with Kaspersky and McAfee both installing and then detecting while Sophos never allowed the installation due to its scanning functionality.

3.3 Examination of Secondary Effects

Most attributes such as storage, memory, and CPU were consistent between the beginning and end of the study. Though variations occurred, they were well within

typical increases and decreases of daily use, though is interesting to note that the battery temperature moved from 31C to 27.6C; however, several unnecessary modifiers existed, such as moving the lab to another building in addition to normal outdoor temperature transitioning from winter to spring.

4. Results and Discussion

4.1 A/V Mitigation and Prevention

Malicious APKs that circumvented the Google Play Protect were generally installed and quickly detected via the Kaspersky and McAfee A/Vs. Although it is encouraging to note the speed of detection, the possibilities should a malicious application modify any important settings, as in the case of the "FreeBitcoin" interaction with McAfee and Kaspersky, are concerning. Although not exclusive to mobile A/Vs, this is akin to allowing a burglar into the cash register and then sounding the alarm. Sophos, which scans an APK prior to installation, is the ideal process. This mitigated the potential threat before it could ever gain a foothold onto the smartphone. Another benefit, with Sophos in particular, was the link-checking functionality, which is believed to have prior scanned the URL.

4.2 Native Android Settings

If followed, two commonalities could prove to be more invaluable than any antivirus: Google Play Protect and the prompting of permissions before an application could use a function, such as SMS, internet, and location, among others. Google Play Protect was not an expected boon, as none of the packages would originate from the Play Store; however, numerous examples exist of Google Play Protect displaying a warning and even blocking the downloads of some APK. This was not expected but is a desirable result when applied outside the scope of this study. Next is the granularity of an Android application to request permissions to a function of a smartphone. Similar to the User Access Control of

Windows Vista, an application that requires access to a service, this would perform a single request for that service. Although functionality would be hindered if a required access is not permitted, the phone provides more control to the user than of what an application is capable. These permissions were prompted on many APK installations that were successful, generally on the control smartphone, as that is where most of the successful installations occurred.

5. Results and Discussion

Though the research indicates that mobile antivirus is generally successful when confronted with malware, it is not a necessary software for non-careless users. With the recommendations below in addition to a more security-oriented mindset, a smartphone is not likely to be compromised outside of any forthcoming methods. However, that is not always the case, and in those scenarios, antivirus software serves as viable control to secure an individual or an organization.

5.1 A/V Recommendations

Analysis prior to installation is the most important feature observed in the employed A/V software. The ability to scan a threat proved invaluable in protecting the phone and prevented any possible interaction a malware could provide to a user, such as enabling malicious settings. The only tested solution that provided this feature was Sophos, although surely other do as well. An additional requested feature would be the capability of quarantining an APK during the installation process or shortly thereafter. This would alleviate some of the fear in which the A/V solutions would allow an APK to install prior to being detected as a threat.

5.2 Native Android Settings Recommendations

The setting of "allowing installations of apps from unknown sources" proves to be the most important setting on an Android phone regarding defense from malicious APKs.

Though enabling this setting does remove possible access to legitimate applications, none of the malicious APKs tested would have been possible without this setting enabled, which is disabled "out of the box." Another feature worth noting is Google Play Protect, which must be enabled. Though it does not necessarily scan a malicious APK prior to installation, it does notify the user prior to installation, which is more desirable than the typical A/V actions of allowing an APK to install and detecting the threat post-installation. Last, providing granular permissions regarding what an application can read/write should always be as restrictive as possible. If a user follows the recommendation above, the most likely vector would be via the Google Play Store, which although not perfect, is consistently monitored. The final recommendation is to not grant access to an unknown application, a known application, or a service that is not required. If an application is not explicitly linked to SMS functionality, then it should not have access to SMS.

References

Android Beat. (2016). *Android 7.0 – 7.1.1 Nougat: All the New and Hidden Features.* Retrieved from http://www.androidbeat.com/new-hidden-android-n-features/

Callaham, J. (2018). *The history of Android OS: its name, origin and more*. *Android Authority*. Retrieved from https://www.androidauthority.com/history-android-os-name-789433/

DiGiacomo, J. (2018). *Data Beach Statistics For 2018 Plus Totals From 2017 | Revision Legal %. Revision Legal*. Retrieved from https://revisionlegal.com/data-breach/2018-statistics/

DMR. (2016). *140 Amazing Smartphone Statistics and Facts (2018)*. Retrieved from https://expandedramblings.com/index.php/smartphone-statistics/9/

Drake, N. (2019). *Best Android antivirus app of 2019. TechRadar*. Retrieved from https://www.techradar.com/best/best-android-antivirus-app

ESET. (2016). *A history of mobile malware from Cabir to SMS Thief | WeLiveSecurity*. *WeLiveSecurity*. Retrieved from https://www.welivesecurity.com/2016/11/01/history-mobile-malware-cabir-sms-thief/

Express.co.uk. (2017). *Revealed: Top uses of our smartphones - and calling doesn't even make the list*. Retrieved from https://www.express.co.uk/life-style/science-technology/778572/Smartphone-phone-common-reason-use-call

Hamblen, M. (2019). *One-fifth of IT pros say their companies had mobile data breach*. *Computerworld*. Retrieved from https://www.computerworld.com/article/3048799/one-fifth-of-it-pros-say-their-companies-had-mobile-data-breach.html

Ismail, N. (2017). *Common security vulnerabilities of mobile devices - Information Age*. *Information Age*. Retrieved from https://www.information-age.com/security-vulnerabilities-mobile-devices-123464616/

Kaspersky. (2019). *Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store*. Retrieved from https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

Mybroadband Staff Writer. (2017). *The most popular operating systems for smartphones and PCs*. *Mybroadband.co.za*. Retrieved from https://mybroadband.co.za/news/software/232485-the-most-popular-operating-systems-for-smartphones-and-pcs.html

Rosencrance, L. (2018). *What is antivirus software (antivirus program)? - Definition from WhatIs.com*. Retrieved from https://searchsecurity.techtarget.com/definition/antivirus-software

Security Innovation Europe. (2015). *The Rise of Mobile Security: Are you at risk? Securityinnovationeurope.com.* Retrieved from https://www.securityinnovationeurope.com/storage/app/media/downloads/ISPA/The-Rise-of-Mobile-Security.pdf

Statista.com. (2018). *Number of mobile phone users worldwide 2015-2020 | Statista*. (2019). *Statista*. Retrieved 24 March 2019, from https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

Steven, C. (2017). *Android File System and Directory Structure Explained*. *Stevesandroidguide.com*. Retrieved from http://www.stevesandroidguide.com/android-files/

Tripwire, I. (2013). *Mobile Antivirus: FUD, Fact and Fiction. The State of Security*. Retrieved from https://www.tripwire.com/state-of-security/security-data-protection/is-mobile-antivirus-just-a-myth/

Mobile Security Index 2019. (2019). Retrieved, from https://enterprise.verizon.com/resources/reports/mobile-security-index/