ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

# A Survey on the Security Fight against Ransomware and Trojans in Android

Tatenda Trust Gotora[1], Kudakwashe Zvarevashe[2], Pranav Nandan[3]

M Tech Student, Dept of Software Engineering, Jawaharlal Nehru Technological University, Hyderabad, India[1]

M Tech Student, Dept of CSE, Jawaharlal Nehru Technological University, Hyderabad, India [2]

M Tech Student, Dept of Software Engineering, Jawaharlal Nehru Technological University, Hyderabad, India [3]

**ABSTRACT**: Android has taken the world of mobile computing to a whole different level and made possible persuasive interaction between user and mobile device. Although it's a Linux based OS most hackers and cyber criminals have found a way to manipulate it to their best interests. Of late more than 300 malware categories have been discovered since the advent of Android and the most lethal being Ransomware and Trojans. Ransomware like Android Defender and Trojans like Andr/Spy-ABN have left a plethora of Android mobile device clients shame-shocked and robbed. Google's recent security improvements on Android version 4.3 have tightened the unwanted application restriction but still more needs to be improved to protect user data. This paper seeks to highlight the mobile security threats witnessed from 2013-14, enhancement fighting techniques employed in the Android 4.3 and 4.4 versions. A sandbox cloud-based approach is proposed to circumvent the rising mobile security problems.

**KEYWORDS:** Android, Ransomware, Android Defender, Trojans, sandbox cloud-based approach, mobile security.

## I. INTRODUCTION

The growth of "Internet of things" is inevitable and mobility in the telecommunications industry will overwhelmingly blossom progressively with technology advancements. This has brought with it a lot of security threats to the "new Webtops", that is, mobile Web connecting devices (smartphones) for the last five years. Google's Android mobile OS has taken control of the smartphone world while also providing exceptional interaction with users. Android devices have become the "new Hot toy" due to increase in cyber social networks, third party e-commerce application developers and integration of sensory gadgets. Multitasking and processing speed keeps on improving with each Android device upgrade but so does malware toolkits. This makes android a moving security target by cyber criminals [1].A malware can be viewed as a form of destructive software which is able to cause malfunction, perform exhortation, cyber theft or compromise user privacy against a user's consent. Ransomware has taken a new twist in Android and keeps inflicting many devices because of user negligence and its affliction with so called "free antivirus" software [3]. Android 4.3 enforces 10 new features and Android 4.4 improves 2 more. There are profound solutions which have been introduced to halt the security threats and a possible proposed cloud-based approach expagorated in Section VII.

Fig 1 below [1] illustrates the various types of threats which have developed over the past five years which have rocked the android market with so much harm and instilling lack of trust by users to Android. Surveillance makes use of the camera or patient monitoring of sms messages or call logs and the attacker makes progressive exploits. Botnet activities are explained in Section III. Impersonation is applying identity theft with the hope of tricking mobile users. Financial category involves Ransonware and Fake App usage to exhort money from users, elaborated in section III. Data Theft encompasses usage of Man-In Browser Attacks and Trojans to extract data from the mobile device or Banking Transactions, explained in section III.

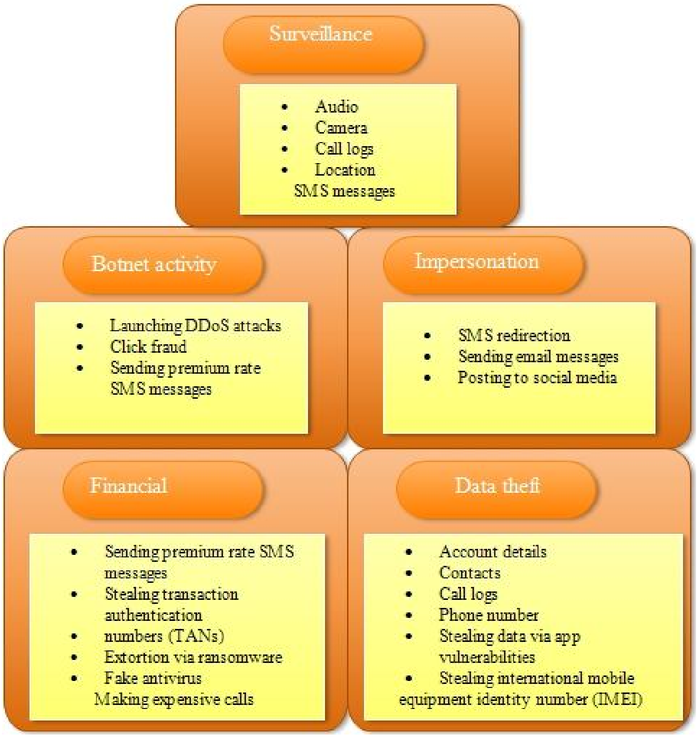


Fig 1: Threats characterization in android phone

## II. RELATED WORK

In 2013 there was an opening of floodgates of Blackhole exploit kits, malware source code and organized funding of exploits. Cybercriminals became more adept at eluding identification, relying more heavily on cryptography and increasingly placing their servers in the darknet (undetected web), according to Sophos Threat Report [1]. User layer attacks contain every exploit that is not of technical nature. Many of today's mobile malware samples are not based on a technical vulnerability, but trick the user into overriding technical security mechanisms [2].

According to a Symantec Report, the malware families decreased by 43 percent from 103 in 2012 to 57 in 2013 although the mean variants per family has increased by 50 percent from 38 in 2012 to 57 in 2013. This is due to the malware makers exploiting third party legit app source code and replacing with their malicious functionality. In 2012, Symantec's Norton Report showed that 44 percent of adults were unaware that security solutions existed for mobile devices, highlighting the lack of awareness of the mobile danger. The 2013 Norton Report showed a rise to 57 percent of adult negligence as smartphone users increased due to greater social and business demands [3].

## III. MAJOR SECURITY THREATS IN 2013-14

### *A. Ransomware*

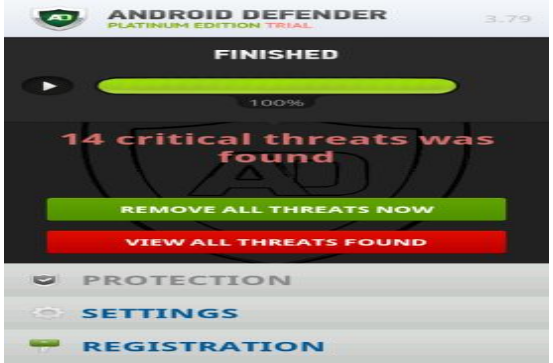
Android devices are becoming vulnerable to similar technologies that were ones created to aim windows. One of a very new kind of such threat is "*Ransomware*". Simply put, ransomware will encrypt the certain parts of users file system or it will lock the essential functionalities. It will then ask for ransom (cash) from the owners to make their own device accessible. In June 2013, first ransomware called "*Cryptolocker*" was discovered. It was targeted to android devices. Hidden under the name of an antivirus called "Android Defender", this app demands $100 to unencrypt your file system and restore your important data. It uses variety of tactics; one of them is very professional look and feel UI, and common social networks sign in. Once it is given administration privilege to protect your device from viruses, this is when the malware starts creating havoc. It registers itself as broadcast receivers for all major system wide intents like making a call, changing setting, killing tasks, install/uninstall apps or can even perform factory reset. It will even disable the Back/Home buttons and constantly present the owner with the threat of fake existing virus which requires payment offer to be made to restore the system. By the end of 2013, mutated ransomware appeared in the android world, "*Android.Fakedefender*" dubbed by Symantec. If registered to install it will setup a service to communicate with the server and run on-demand code. Even if one ignores to install the defender, the app can change operating system settings, prevent other apps from running, making the system crash and shows the fake system infected messages as shown in Fig2.1 [1] [3] [4][5] [6].

Similarly, the famous ransomware that appeared in 2013 was Trojan called "*Obad*". It can rack up the phone bill by sending premium SMS to the favor of Trojan owner. It will ask for administrator's privilege under the name *com.android.admin*. It is small and blacks out the screen for 10 seconds to activate the Bluetooth and spread to the nearby devices. Along with this, it downloads a family of backdoor Trojans. Kaspersky reports so far it is the most complicated Trojan seen in android and is distributed by mobile botnet. Google has patched the bug that allows Obad to hide in the Device Admins list in Android 4.3. But the threat remains open in all prior versions unless one explicitly installs McAfee hidden admin tool or Kaspersky labs admin tools [7].

### *B. Police Trojan*

A Police Trojan is a form of ransomware that, instead of ransom notes, display warnings that purport to come from local or national law-enforcement authorities. "Koler.A" is the new android police Trojan discovered by Kafeine a Security French Blogger in early May 2014. Once installed, the malware locks up the phone, preventing users from accessing the home screen and effectively holding the phones ransom until users pay $300. Recent developments show that it presents itself with an authentic Security authority logo as shown in Fig2.2. It makes use of malicious traffic-distribution systems (TDS) to spread. Malicious TDS's detect visitors' browsers, operating systems and countries of residence thereby redirect them to malicious Web pages with embedded browser exploit kits. The visitor's browser will be redirected to a fake pornography website that will try to trigger a drive-by download on the mobile device. [21]

Fig 2.1: Android Fakedefender pop up installation window



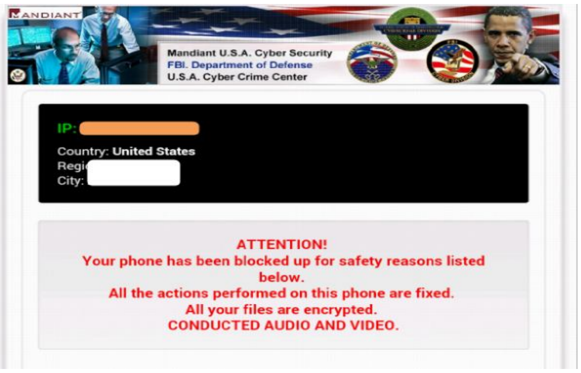
ANDROID DEFENDER
PLATINUM EDITION TRIAL 3.79

FINISHED

100%

14 critical threats was found

Fig2.2: Koler.A (Police Trojan) UI seen in the USA



Mandiant U.S.A. Cyber Security
FBI. Department of Defense
U.S.A. Cyber Crime Center

IP: [redacted]
Country: United States
Regi [redacted]
City:

ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.

### *C. Man-in-Browser*

Similarly, *Man-in-browser* attacks that were engineered for windows have been ported to android. The last occurrence of such was September 2013 and was called "*Adr/Spy-ABN (*also: *Qadars)*". It has been designed for theft while transaction is taking place. It intercepts the public keys of the owner and makes its own transaction within the given session. It is new but has already targeted the French, Dutch and Indian financial institutions [8]. Its predecessor was "*Andr/Spy-ABN (*also: *Zues)*" which would capture cookies and personal certificates from Internet explorer by injecting a code in windows, and misusing them. Once we sign in to online banking portal in android, it will present itself as an anti-fraud application ironically saying the bank now requires a new smartphone app. After verifying the phone number, it will send a link in SMS that is actually the malicious app which can exploit your certificates while doing online banking. The appearance of extensible kit called “Blackhole exploit kit” in 2012-2013 became the cause for 25% of all web threat detected by Sophos and 91% by AVG in computers [9]. This kit can be purchased and the malware can be customized as per the need of exploiter [3].

*D. Botnets*

The botnet business is now shifting to the android market. Since most mobile device users are now knowledgeable of scam emails and antivirus, botnets are becoming a means to deliver ransomware, click ads for third parties or mine Bitcoins. A botnet named as “*Andr/GGSmart-A*” (seen in China) is a command and control Trojan for mobile devices. It sends premium SMS messages that will be charged to the device owner. The benefit goes to botnet subscriber. These networks are getting organized and the Trojans act as a small part of a much bigger app. They are able to remain inactive for longer time hidden from the owner and antivirus [10]. *Android.Hehe* is a new strain of Android malware that masquerades as an “Android security” app but once installed, can steal text messages and intercept phone calls.

*E. Version fragmentation*

It is the use of various Android versions by different users. This is due to the delay or reluctance of update patches for lower versions by Device manufacturers. For instance, more than 25% of the users are still running Android 2.3, which represents a big security issue [14].

## IV. MAJOR SECURITY FEATURES OF ANDROID 4.3 and 4.4

The Android 4.3 version also called Jelly Bean brought a number of remarkable security innovation. These features have been listed below and have been welcomed well by the whole android third party vendors [11] [12] [13].

*A. SELinux*

Android 4.3 uses some of the concepts of SELinux (Security Enhanced Linux). It is a mandatory access control system in Linux to enhance the UID based app Sandbox. Essentially in Android, every application runs as a separate user in a sandbox environment. Upon installation of the application, the uid is allocated and assigned to each installed application. This makes the application more secure.

*B. Nosuid*

SetUid bit is an important flag that can be set to any executable binary in a UNIX or Linux based operating system to gain access to the root level. Hackers misuse the marked application to gain access to system calls. These activities can be malicious in nature. Now in the Android 4.3 operating system, no Android application can access the SetUid functionality. This will reduce the malicious attacks on Android devices.

*C. KeyChains and Keystore Providers*

The encrypted keys will be stored in the device. They are private keys and their corresponding certificates in credential storage. These keys are required by the app to gain access to certain hardware. Google has added security feature to create exclusive-keys that can only be accessed by that app.

*D. WPA2-Enterprise Networks*

Android 4.3 provides an API to create application which can configure Wi-Fi. Previously, it was done by third party apps. So, joining access points and organizing credentials can be done in one’s own app.

*E. Address Space Layout Randomization (ASLR)*

ASLR simply randomizes where memory processes get mapped, so attackers can only guess where their malicious payloads will end up. According to *Jon Oberheide of Duo Security* their odds now go from 1 in 2 to "maybe 1 in 1000." Every wrong guess will crash their application and the user will uninstall the malicious app.

*F. One Less Permission*

Google has also removed the "READ_LOGS" permission that let apps read low-level system log files. This was used to help malware to read sensitive logged information regarding user and information that can be misused.

*G. Total device encryption*

This allows us to encrypt our phone entirely. A passcode or PIN is required to access information inside the phone. The process is completely irreversible without performing a factory reset on the phone. So remembering the passcode or PIN is very important for the owner.

*H. Owner information displayed on the lock screen*

If we lose our phone, a personal message that is constantly being displayed on the lock screen helps people to return it. This increases the chances of recovering our phone back. It resides on: Simply go to Settings>Owner Info to enter a lockscreen message.

*I. Option to disable preloaded apps*

We cannot uninstall factory loaded apps from our phone, but now it can be disabled in the new android phones. Disabled apps cannot be launched or access the information from the phone. Also the background process services can be selected and disabled. This prevents bandwidth leakage. Also, apps that are running in background are explicit. For example: Google Maps services constantly access our location information even if it is not running. But if we disable the service, then only when we run Google maps in foreground, it will access the location information. Fig 3 depicts the levels an application has to undergo when being downloaded from Google play store.

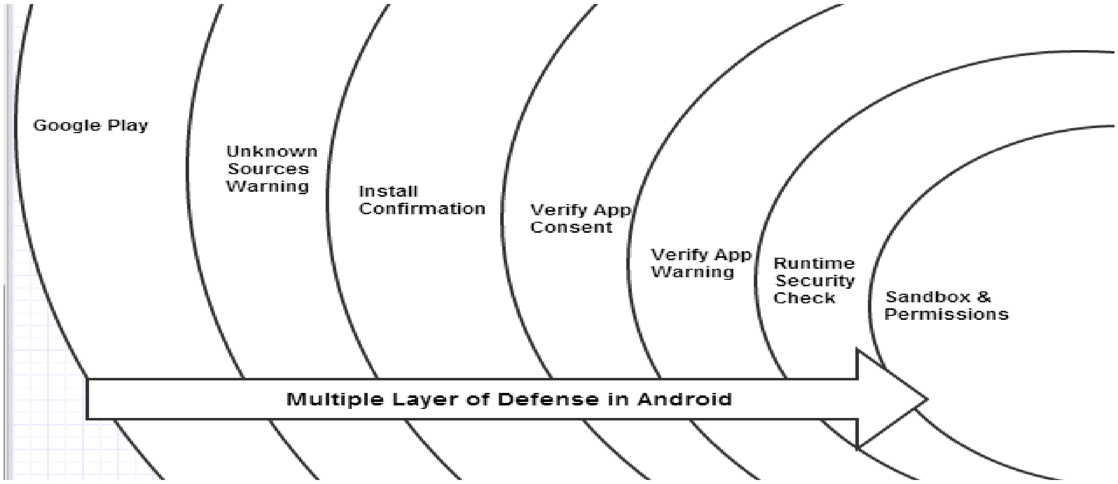


Fig 3: Android Security Levels

*J. Facial recognition*

Android phones now come with facial recognition feature to unlock it. If lighting and other conditions are not clear, it will ask for unlock code alternately. Also *Tim Bray*, an Android developer, confirms that we can't unlock it with a photograph.

*K. Android 4.4 (Kit Kat) Security Improvements*

1) *Digital certificates:* Kit Kat has an alert mechanism warning a user if a Certificate Authority (CA) is added to the device, making it easy to identify Man-in-the-Middle attacks inside local networks. At the same time, Google Certificate Pinning will make it harder for sophisticated attackers to intercept network traffic to and from Google services, by making sure only whitelisted SSL certificates can connect to certain Google domains**.**
2) *OS hardening:* SELinux is now running in enforcing mode, instead of permissive mode. This helps enforce permissions and thwart privilege escalation attacks, such as exploits that want to gain root access. Android 4.4 comes compiled with FORTIFY_SOURCE set at level 2, making buffer overflow exploits harder to implement.

## V. AVAILABLE MALWARE FIGHTING TECHNIQUES

Prevention is better cure; likewise to avoid using malware sticking to mainstream apps from trusted sources such as the Google Play store is safer. Android like many other open-source software promotes downloading and installing of apps from virtually anywhere. We can't rule out the possibility of vetting inconsistencies thus can't be trusted. For additional protection an antimalware app has to be installed on the Android device.

### A. *McAfee Antivirus & Security* and *Symantec's Norton Mobile Security*

The most familiar being two effective malware stronghold fighters, according to PC World (2013). To remove the Android defender malware Norton Mobile Security has to be installed on mobile device downloaded from Google Play Store or norton.mobi website.

### B. *AVG Mobilation*

It was released by AVG in 2011 for the Android OS platform. AVG updated its smartphone antivirus application called *ANTIVIRUSFree*, originally meant for tablet to android smartphones. It is free and has key capabilities of the Mobilation program involve ability to scan for viruses in email, downloads, text or SMS messages and allows the user to block spam SMS messages. It supports both on-demand and scheduled scanning, while offering theft protection. Using the Android device's GPS features, the program can find a lost or stolen tablet, as well remotely manage applications, lock, and wipe the device's memory. The anti-virus part protects device from malware and keeps private data safe from exploitation [14] [15].

### C. *Symantec VeriSign Identity Protection Access* (VIP) for Mobile

It was released by Symantec in 2011 initially for Apple's iOS platform but further extended for other platforms, including Android and Symbian. VIP provides an additional layer of protection to mobile devices by allowing the users to create an extra "unique security code," or a one-time password. Once created the user is then required to enter that code in addition to the usual password and log in required by the websites he or she visits that are part of the VIP Network. Currently, about 750 websites belong to the VIP Network [16].

### *Samsung Knox*

It is one of the new android enterprise solutions introduced in 2013 by Samsung. It retains full compatibility with Android and the Google ecosystem while integrating fundamental security and management enhancements. This makes it suitable for both regulated and general enterprise environments. It is based on four major assets [17]:

1) *Platform security*: Uses a comprehensive three-pronged strategy to secure the system: Customizable Secure Boot*; ensures that only verified and authorized software can run on the device, ARM® TrustZone®-based Integrity Measurement Architecture (TIMA); runs in the secure-world and provides continuous integrity monitoring of the Linux kernel, Kernel with built-in Security Enhancements for Android (SE for Android) access controls; isolates applications and data into different domains.
2) *Application Security:* Samsung KNOX container; provides security for enterprise data by isolating enterprise applications and encrypting enterprise both data at-rest (DAT) and data in transit (DIT), Encrypted File System; employing a more secure and separate encrypted File System in Samsung KNOX container completely isolated from outside applications, Virtual Private Network; offers an on-demand FIPS-certified per-app VPN providing enterprise IT administrators with the ability to configure, provision, and manage the use of VPN on a per-application basis.
3) *Mobile Device Management (MDM):* Enables the enterprise IT department to monitor, control, and administer all deployed mobile devices across multiple mobile service providers. Provides additional policies for security, enterprise integration, and enterprise applications such as asset tracking, remote control, and so on.
4) *Samsung KNOX for Enterprise:* Samsung KNOX for IT Managers; Comprehensive protection of enterprise data from leakage, malware and malicious attacks, Samsung KNOX for Employees; using different persona for work and play, Samsung KNOX for Partners; An easier way to create enterprise grade mobile applications.

### *D. Lookout*

It is a new mobile security app which is a post-pc powerful era weapon to fight malware, e-crimes. Most users have deemed it very user friendly and effective. It has a 45 million clientele base building a powerful, cloud-based protection platform. Samsung has incorporated it into the frail Knox solution to provide real-time cloud-based scanning to protect against mobile threats from email add-ons and other services [18].

*Functions of Lookout*

1. Protect your device from malware
2. Scan every app to ensure it's safe
3. Block malicious websites
4. See which apps access your private info
5. Wipe your data so no one can access it
6. Prevent encounters with phishing scams
7. Backing up your Google contacts and photos to the cloud for safekeeping.
8. Locate your phone on a Google map from any web browser if lost or missing.
9. Self-service locking or wiping a phone in the event of theft of loss.

Fig 5: Lookout User Interface on Android device

## VI. PROPOSED TECHNIQUE

*Cloud-Based Sandboxing:* On-premises sandboxing has been used for some time to check for malware in suspicious executable apps. While the results have been impressive especially compared to systems that rely exclusively on signature-based antivirus software it has its limitation. Fig 6 shows that security is being offered as a service and resources are contained on a cloud platform. Implying all cloud principles like self-service, elasticity and pay as you go are also present. Not only does it save costs but also promotes BYOD (Bring your own Device) Model.

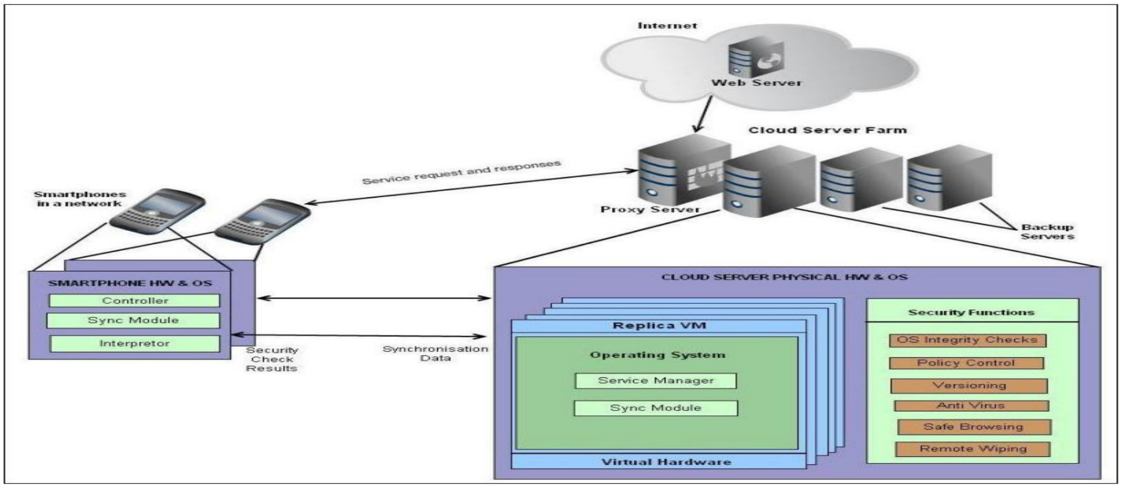


Fig 6: Cloud-based Sandboxing Architecture [19]

The cloud-based approach has the following major advantages [20]:

1) Cloud-based sandboxes are free of hardware limitations, and therefore scalable and elastic. As a result, they can track malware over a period of hours or days instead of seconds or minutes , to build robust malware profiles of targeted threats (such as the one that used a fake Mandiant APT1 report), or to uncover “Time Bomb” attacks that need to be simulated with custom times and dates (such as Shamoon).
2) Cloud-based sandboxes can be easily updated with any OS type and version, including those that aren’t part of a sandboxing appliance’s default set of images. Enterprises can also upload images and create their own custom environment.
3) Cloud-based sandboxes aren’t limited by geography. For example, attackers often target offices that are located in a different region than where the on-premise sandbox is running (typically the enterprise’s headquarters). As such, the attacker will not respond to the malware since it communicates from a different region. However, cloud-based sandboxes avoid this by allowing the malware to run from different locations worldwide**.**

## VII. CONCLUSION AND FUTURE WORK

Android device clientele base is growing ferociously likewise are the cyber perpetrators. From malware in PCs to mobile devices they keep on mutating to cater for their creators vendetta. The security fight is far from over and a lot of weapons have been unveiled over time, as shown by stiffer Android security updates in each version. The Jelly Bean’s SELinux, Total device encryption and Kit Kat’s Digital Certificates innovations have proven to be quite resourceful. Despite the various available security techniques ignorance by clientele on fake apps and version fragmentation remains strong threats. McAfee Antivirus & Security , Symantec's Norton Mobile Security and Symantec VeriSign Identity Protection Access (VIP) have halted a lot of ransomware and Trojans over the last three years. Enterprise solutions like Samsung Knox and Lookout have restored Android security trust to the mobile market. Knox Platform security, MDM and Lookout’s real-time cloud-based scanning will promote the BYOD model thus reducing Enterprise OPEX. The proposed Cloud –based sandboxing is highly scalable, will reduce version fragmentation and isn’t geographically restricted. It is the way to go although it requires maturing and gaining more clientele trust. There’s a need for future work to implement and analyze the proposed technique.

## REFERENCES

1. Sophos, “Smarter, Shadier, Stealthier Malware”, Sophos Security Threat Report 2014, http://www.sophos.com/threatreport.
2. Michael Becher; Felix C. Freiling; Johannes Hoffmann; Thorsten Holz; Sebastian Uellenbeck,; Christopher Wolf, “Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices”, IEEE Symposium on Security and Privacy, pp. 96-111, 2011.
3. Symantec Corporation, “Internet Security Threat Report 2014”, 2013 Trends, Volume 19, April 2014
4. Ransomware on Android, [online] http://www.infoworld.com/t/mobile-security/ransomware-android-it-was-only-matter-of-time-221285.
5. Fake AV and ransomware, [online] http://www.pcworld.com/article/2042693/fake-av-and-ransomware-coming-soon-to-an-android-device-near-you.html
6. Fake Security Software Attacks Android Users, [online] http://www.mobilesecurity.com/articles/555-fake-security-software-attacks-android-users
7. Obad, [online] http://www.androidauthority.com/obad-nastiest-piece-android-malware-discovered-2013-324830/
8. Nattakant Utakrit, "Review of Browser Extensions, a Man-in-theBrowser Phishing Techniques Targeting Bank Customers” , Proceedings of the 7th Australian Information Security Management Conference, pp. 110-119, 2009.
9. Blackhole Exploit, [online] http://www.securityweek.com/black-hole-exploit-business-savvy-cyber-gang-driving-massive-wave-fraud.
10. Symantec takes on one of largest botnets in history, [online] http://news.cnet.com/8301-1009_3-57605411-83/symantec-takes-on-one-of-largest-botnets-in-history/
11. SELinux NSA/CSS Research, [online] http://www.nsa.gov/research/selinux/faqs.shtml
12. Android, Android Official Website, [online] http://www.android.com/
13. Android 4.4, [online] http://www.securelist.com/en/blog/208214116/Android_4_4_arrives_with_new_security_features_but_do_they_really_matter
14. JC Torpey, AVG and Symantec Smartphone Security Program FAQs, Yahoo Voices, 28 March 2011, http://voices.yahoo.com/avg-symantec-smartphone-security-program-faqs-8157497.html?cat=15

15. Android.Fakedefender, [online] http://www.symantec.com/security_response/writeup.jsp?docid=2013-060301-4418-99&tabid=3
16. Symantec,[online]http://www.symantec.com/about/news/release/article.jsp?prid=20110209_02
17. Enterprise Mobility Solutions Samsung Electronics Co. Ltd, “White Paper : An Overview of Samsung KNOX™”, June 2013
18. Lookout, [online] https://www.lookout.com/android
19. Dennis Titze, “A Cloud-Based Security Service for Smartphones”, Master’s Thesis Informatik, 15 May 2012.
20. Aviv Raff, Cloud-Based Sandboxing: An Elevated Approach to Network Security, SecurityWeek Malware, 04 November 2013, http://www.securityweek.com/cloud-based-sandboxing-elevated-approach-network-security
21. Cryptolocker-Like Ransomware Spreads to Android Devices, [online] http://www.tomsguide.com/us/cryptolocker-ransomware-android,news-18744.html

## BIBLIOGRAPHY

**Tatenda Trust Gotora**: Born in 1988 attained his BSc degree in Computer Science at MSU, Zimbabwe in 2011. He is currently doing M Tech SE final year at JNTUH, India. He is a HIT staff development research fellow. His research interests are in the area of mobile computing, android development, information security and web services.

**Pranav Nandan**: Born in 1989 attained his BEng degree in Computer Science at Kathmandu University, Nepal in 2011. He is currently doing M Tech SE final year at JNTUH, India. Recently has been appointed as a IBM employee. His research interests are in the area of cloud computing, android development and network programming.

**Kudakwashe Zvarevashe**: Born in 1986 attained his BSc degree in Information Systems at MSU, Zimbabwe in 2010. He is currently doing M Tech IT final year at JNTUH, India. He is HIT staff development research fellow. His research interests are in the area of big data, information security, cloud computing and web services.