Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 465 – 471

Procedia Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)

An Android-based Trojan Spyware to Study the NotificationListener Service Vulnerability

Huda Abualola[a], Hessa Alhawai[a], Maha Kadadha[a], Hadi Otrok[a,*], Azzam Mourad[b]

[a]*Department of ECE, Khalifa University, Abu Dhabi, UAE*
[b]*Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon*

Abstract

Security attacks continue to emerge on daily basis due to the fast growth in the number of smart devices and mobile applications. Attacks take different malware forms such as Spyware and Trojan exploiting different operating system vulnerabilities, specially the well known vulnerable operating system; Android OS. In this paper, we study the malicious use of the "NotificationListener" service in Android 4.3 and 5.0. A Trojan application, known as SMS backup, is developed to spy the notifications of other applications. Such an application requires only two permissions that include "Notification Access" and "Internet". These permissions are used to extract and send user's messages of other applications to the attacker's email through Internet. Our malware is able to alter and/or delete the notification before being displayed. For experimental results, the malware was tested against notifications of WhatsApp, BBM, SMS, and Facebook messenger using different Android versions including Lollipop 5.0. Experiments show that our malware succeeded against all the tested applications running Android version 4.3. Moreover, BBM and SMS messages are still extractable in the newer version of Android (Lollipop 5.0).

Peer-review under responsibility of the Conference Program Chairs

Keywords: Mobile spy; Spyware; Trojan; Android; Notification

1. Introduction

Spyware is a malware that spys the user's activities. Such activities might include login information; username and password, or personal files such as images and chat logs. However, as Spyware cannot easily spread on their own, Trojans are used to hide them by offering a legitimate functionality to the user. Norton statistics show that 37% of cybercrimes around the world are due to the combination of Spyware and Trojan[1]. Since Android dominates the market share with 45.4%, most of the cybercrimes are designed to target such an operating system[2]. Aside from the high number of Android users, the number of applications is increasing rapidly where there are about 2 million applications uploaded on Google Play store[3]. This rapid increase adds to the complexity of validating these applications against their required permissions. For example, 61% of the applications that require the "READ_SMS"

*Corresponding author. Tel.: +971 (0)2 401 8095 ; fax: +971 (0)2 447 2441 .
E-mail address: hadi.otrok@kustar.ac.ae

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.210

permission are classified as malicious[4], while only 12% requiring the same permission are benign. Lack of validation resulted in almost 750 thousand attacks through Trojan SMS malware being detected and blocked by Kaspersky products[5]. In addition to Google Play, unofficial stores exist with high download rate of more than 800 thousand downloads, despite their lower validation techniques[6]. This indicates that smart devices' users are open to all types of attacks especially for Android.

Since Android notifications are App-Controlled views, developers are allowed to customize them through applications without restrictions. Spamming and Phishing are the only two types of attacks that exploited the notification customization ability[7]. Spam notifications are prompt notifications containing a link to a malicious website that is visited once the notification is either dismissed or triggered. These notifications take the form of advertisements that would attract the user to trigger them. On the other hand, phishing attacks are executed by posting a notification that replicates other applications' notifications asking for the user's credentials.

As far as we know, we are among the first efforts to maliciously use the "NotificationListener" service to spy and share messages received by other applications such as WhatsApp, BBM, and Facebook messenger. An SMS backup application is used as a Trojan to hide the Spyware Software activity of notification extraction. Extraction is done by reading notification view fields, "bigContentView" and "TickerText", of the received message. However, Android has prevented reading "bigContentView" field of other applications' notifications starting "Lollipop" and later versions. Thus, our malware can read WhatsApp, BBM and Facebook messages up to and including "Kitkat" version which dominates the market with a share of 66.8%[8]. While, BBM messages are still extractable in Android Lollipop 5.0 because the message content is completely written in the "TickerText" field that is still extractable. Also, our malware leaks the SMS messages to the attacker for all Android versions, since it has "READ_SMS" permission to provide the front application functionality.

In summary, the main contribution of this paper is the development of a Trojan Spyware that uses "Notification Access" and "Internet" permissions to extract and send information from an Android device to attacker's email. The application is considered a Trojan malware since it provides the users with useful functionalities; SMS backup and notification customization, while collecting users' messages without their knowledge which is a Spyware activity. The "Notification Access" permits our malware to read and change notifications' contents. Additionally, the "Internet" permission is used to send extracted information to the attacker's email without their knowledge. This malware has been tested for different Android versions including Lollipop 5.0 where we have shown the applicability of the attack on all targeted applications before Lollipop 5.0, as well as BBM and SMS on version 5.0.

The rest of the paper is organized as follows. Section 2 includes literature review. Section 3 includes explanation of the proposed application model. Section 4 illustrates the experimental results. Finally, section 5 includes proposed suggestions to prevent this Trojan Spyware attack.

2. Literature Review

This section illustrates existing mobile phone Spyware attacks and the available detection techniques for Spyware.

2.1. Existing Mobile Spyware

Multiple Spy attacks targeting Android devices were reported. Spyware can be hidden in different shapes and spread in different techniques in order to perform its malicious purpose which is usually data theft. "SW.SecurePhone" and "SW.Qieting" are both two applications that work as Spyware to monitor user's activities[9]. SW.SecurePhone starts by running in the background after getting installed, then monitors the phone and stores the collected information including calls and messages on the device's SD Card. Every 20 minutes, these information are sent to a server over the internet. However, SW.Qieting sends the collected messages to another mobile phone without user's intervention or knowledge.

Another mobile Spyware that has spread lately is called "FlexiSpy"[10]. This Spyware hides in applications that pretend to be for your children's protection or for catching cheating spouses. However, in the background, it collects all the phone activities including SMS messages and call history.

In addition, Spamvertsing is a popular notification malware that works by pushing advertisement to Android users. Different products like fake anti-viruses are advertised though attractive pop-up notifications shown to the user, while

most of them being malicious ads[11]. Another form of fake notifications, login credentials requests for popular applications like Facebook such that the user is directed to the official application after the user's information has been stolen[7].

2.2. Spyware Detection Techniques

This section illustrates some detection techniques that are used to find out spying activities on smart devices.

2.2.1. Signature Based Detection

Signature based anti-Spyware utilize a previously defined database that contains a number of legitimate software. It compares between the newly installed application and the ones in its database[12]. The problem with this detection technique is that it needs to regularly update its database. Otherwise, the false negative detection rate would be too high.

2.2.2. Behavior Based Detection

Behavior based anti-Spyware also utilize some pre-defined database. However, this database contains the known scenarios and behaviors for malicious and non-malicious activities. The problem with this method is that it is difficult to define accurately the behavior of a Spyware. Especially that a Spyware might be hidden inside applications that claim to monitor a device. An example of behavior based detection technique proposed is called "Gatekeeper" which manage Spyware by identifying and monitoring the "Auto-Start Extensibility Points" (ASEPs)[13]. ASEPs are the set of extensibility points that allows programs to auto-start.

2.2.3. Data Mining Based Detection

In this type of detection, a classifier is used to tell whether this application is a malicious software or not. A classifier is generated using existing malicious and non-malicious software databases[12]. The classifier uses data mining algorithms where it identifies events or attributes that do not match the expected pattern defined in the database. Data mining was found to be more effective than the other two techniques regarding Spyware detection.

2.2.4. Advanced Behavior Detection

A proposed advanced behavior Spyware detection technique do not detect a specific behavior of Spyware[14]. However, it detects general behavior of different Spyware classes such as leaking information outside the applications' limits. This technique works on reducing the percentage of false positives by combining static and dynamic analysis of Spyware behaviors. In addition, the technique used characterize applications' behaviors precisely in their interaction with browser events.

3. The Malware Model

In this section, our Trojan Spyware attack model is explained including the legitimate and malicious activities along with snapshots of the malware. The application model flowchart is shown in figure 1. In this figure, we show the normal and malicious behaviors of the application where the green represents the Trojan's activities and the red represents the Spyware's activities.

3.1. The Trojan Activity Model

The application provides the user with SMS messages backup feature along with a customized SMS notification with a reply option. Once the user starts the application, a pop-up message prompts him to enable the "Notification Access" permission from the settings to permit the application's functionalities. After the permission is granted, the user may enter his email in the text field shown on the application's main screen to activate the SMS backup feature. While the email is registered, the application sends emails to the user every time a new SMS is received containing its content. Moreover, SMS notifications are replaced with another containing a direct reply feature.

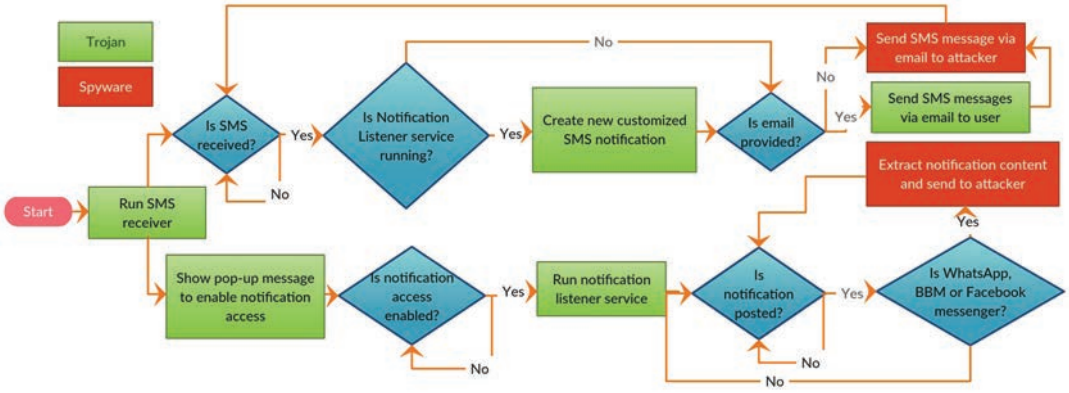
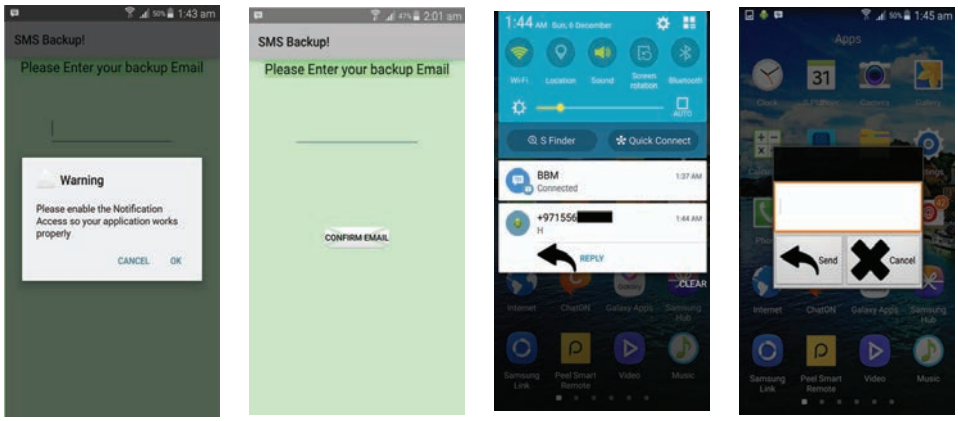


Fig. 1: Application flowchart

From implementation perspective, multiple services; "NotificationListener" and "smsReceiver", run in the background and receive calls from the system when a new notification is posted or an SMS is received respectively. Both services start only when the user grants the "Notification Access" permission to the application. The first functionality; backing up SMS messages, is implemented completely in the "onReceive()" method provided by "smsReceiver" service, such that the new SMS content is extracted then sent via email to the user. The second functionality; replicating SMS notification with additional features, is provided to the user by creating the replicate inside the "onReceive" method while deleting the original notification in the "cancelNotification()" method of "NotificationListener" service.

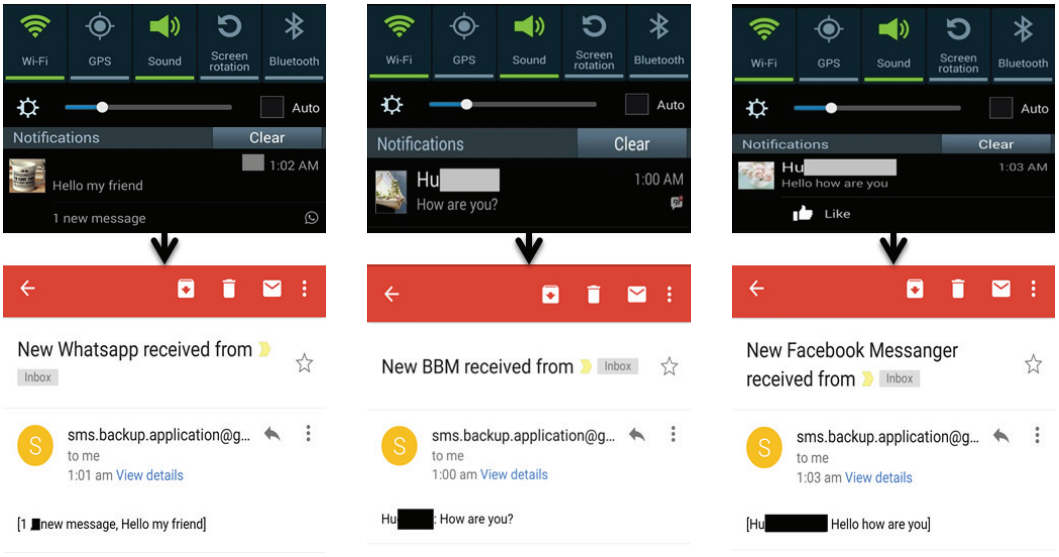
3.2. The Trojan Views

The first time the user runs the application, a pop-up message, shown in Figure 2a, is displayed prompting the user to enable notification access and directs him to notification access settings page when clicking "OK" button. The user will be able to see the application's main screen as shown in Figure 2b after enabling notification access. The main screen contains an EditText element, accepts input in the format of an email address while declining any other input, for the user to enter his backup email. Moreover, the new notification as demonstrated in Figure 2c has a reply button to view the reply field dialog once clicked. The reply dialog containing an EditText element, shown in Figure 2d, pops up to allow writing and sending a reply without closing the running application by clicking "send" button in the dialog.



(a) Pop-up (b) Main screen (c) SMS notification (d) Reply text box

Fig. 2: Application Interface



(a) WhatApp notification test (b) BBM notification test (c) Facebook notification test

Fig. 3: Spyware results on Android 4.3

3.3. The Spyware Activity Model

The attack activities run in the background using "NotificationListener" service to target Whatsapp, Facebook Messenger and BBM notifications. Once a notification related to one of the targeted applications is posted, the message content is extracted then sent to the attacker's email. The message extraction is implemented in the "onNotificationPosted" method by parsing "bigContentView" or "TickerText" fields of the notification view. "bigContenView" includes the message's content while "TickerText" field has the header of the message. Whatsapp, Facebook Messenger messages are extracted by parsing "bigContentView", meanwhile, "TickerText" is parsed to extract BBM messages. For security purposes, Android has prevented access to "bigContentView" such that it returns "NULL" in version 5.0 and later, keeping "TickerText" accessible. As BBM notification's structure include the complete message in the "TickerText" field, their messages are still extractable from the notification in version 5.0 and later in contrast to previously mentioned applications. That allows our Trojan Spyware to work for all targeted applications on "Kitkat" and lower versions as well as BBM on "Lollipop" 5.0 and later.

4. The Malware Experimental Results

We have tested our malware using Galaxy S4 with two different Android versions of Android 4.3 and 5.0. The Spyware has been tested against multiple applications which are WhatsApp, BBM, SMS and Facebook messenger. Table 1 shows the applicability of our Spyware on different Android versions against the targeted applications.

According to our results and as shown in table 1, WhatsApp and Facebook messenger notifications' content can be extracted only in Android 4.3 and below. However, BBM and SMS messages can be sent to the attacker in both versions; Android 4.3 and 5.0.

Results of spying on Android 4.3 notifications are demonstrated in figure 3. The notification panel style which is colored black with full screen panel shows that the smart device used support "Kitkat" version. In figure 3a, the WhatsApp massage received is sent to the attacker's email. In addition, figures 3b and 3c demonstrate BBM and Facebook messenger notifications' and the emails that were sent to the attacker respectively.

The test of our malware on Android 5.0 has been done against BBM and SMS messages. The SMS notification received is shown in figure 2b along with the email received by the attacker in figure 4a. On the other hand, figure 4b demonstrates the BBM message the user received and the email with the message content sent to the attacker.

Table 1: Applicability of opposed applications on Android versions.

Applications	Android 4.3	Android 5.0
WhatApp	✓	✗
Facebook Messenger	✓	✗
BBM	✓	✓
SMS	✓	✓

5. Security Enhancement Solution

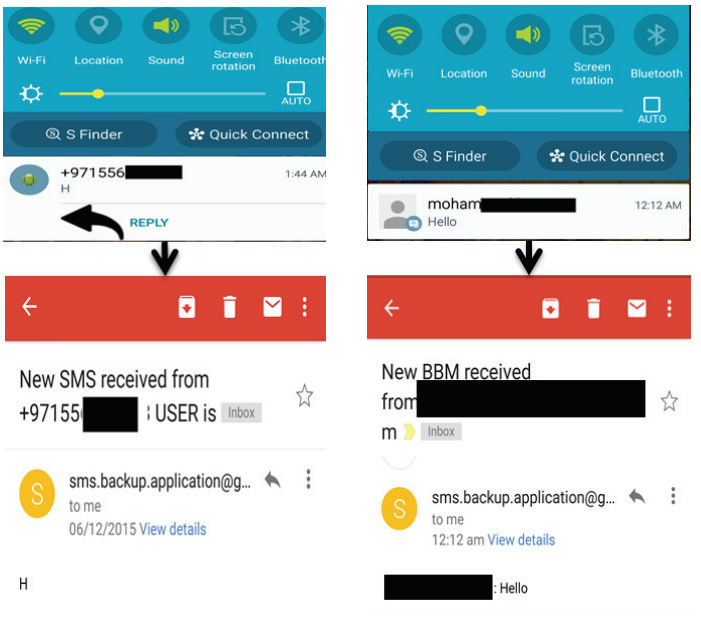
Solutions to such a Trojan Spyware are proposed in this section. Solutions depend on the application's development and accessibility of other applications.

5.1. Application's Notification Structure

In the new Android version Lollipop, applications cannot get the notification view of other application to retrieve their content, even if notification access is granted. However, BBM notification still includes the message and the sender in the "TickerText" field making it vulnerable since "TickerText" can be retrieved and used by other applications that have notification access. Therefore, BBM has to consider changeing their notification structure to secure their messages against such an attack.

5.2. Notification Access by Android

Most of the users are not aware of the permissions they give to the applications. Even if they are aware, they overlook these permissions in return of the features applications provide. Therefore, Android should change the notification access permission to be only for applications with admin permission since sharing notification contents is not needed between applications.



(a) SMS attack test (b) BBM notification test

Fig. 4: Spyware results on Android 5.0

6. Conclusion

As smart devices are penetrating to people's everyday life without the correct security measurements, different vulnerabilities are exploited on daily basis. A vulnerability that we targeted, in this work, was the "NotificationListener" service, where we have developed and tested an Android-based Trojan Spyware that exploited it. The Trojan offers the user with SMS message back-up and notification customization services. Simultaneously, the Spyware App runs on the background to forward all received notifications' contents to the attacker's email. Results showed that our malware was able to successfully extract/update and forward messages from WhatsApp, BBM, Facebook Messenger and SMS messages for Android devices running Kitkat 4.3. Moreover, our results showed the applicability of our malware on BBM and SMS messages with devices running Lollipop 5.0. This is due to the misuse of the notification structure that BBM application supports and due to the abuse of the "SMS_READ" permission which is needed by SMS messages.

Acknowledgment

This work has been supported by Khalifa University of Science, Technology & Research (KUSTAR), the Associated Research Unit of the National Council for Scientific Research, CNRS-Lebanon, and Lebanese American University (LAU).

References

1. Ae.norton.com . Trojan horse - trojans - spyware - cybercrime — norton uk. 2016. URL: http://ae.norton.com/cybercrime-trojansspyware.
2. Burguera I, Zurutuza U, Nadjim-Tehrani S. Crowdroid: behavior-based malware detection system for Android. ACM; 2016, p. 15–26.
3. Appbrain.com . Android operating system statistics - appbrain. 2016. URL: http://www.appbrain.com/stats/.
4. Guo C, Xu J, Liu L, Xu S. Using association statistics to rank risk of android application. In: Computer and Communications (ICCC), 2015 IEEE International Conference on. 2015, p. 6–10. doi:10.1109/CompComm.2015.7387530.
5. Kaspersky.com . The number of financial attacks against android users tripled in 2014 — kaspersky lab. 2016. URL: http://www.kaspersky.com/about/news/virus/2015/The-Number-of-Financial-Attacks-Against-Android-Users-Tripled-in-2014.
6. Abura'ed N, Otrok H, Mizouni R, Bentahar J. Mobile phishing attack for android platform. In: Innovations in Information Technology (INNOVATIONS), 2014 10th International Conference on. 2014, p. 18–23. doi:10.1109/INNOVATIONS.2014.6987555.
7. Xu Z, Zhu S. Abusing notification services on smartphones for phishing and spamming. In: Presented as part of the 6th USENIX Workshop on Offensive Technologies. Bellevue, WA: USENIX; 2012,URL: https://www.usenix.org/conference/woot12/workshop-program/presentation/Xu.
8. Developer.android.com . Dashboards — android developers. 2016. URL: http://developer.android.com/about/dashboards/index.html.
9. tagkey20113. Android marketplace hit by malware. Computer Fraud & Security 2011;2011(3):3 –. URL: http://www.sciencedirect.com/science/article/pii/S1361372311700252. doi:http://dx.doi.org/10.1016/S1361-3723(11)70025-2.
10. Xu N, Jia W. Numen: Where and what are you doing now. In: System Science and Engineering (ICSSE), 2010 International Conference on. 2010, p. 338–43. doi:10.1109/ICSSE.2010.5551723.
11. Mansfield-Devine S. Android malware and mitigations. Network Security 2012;2012(11):12 – 20. URL: http://www.sciencedirect.com/science/article/pii/S1353485812701046. doi:http://dx.doi.org/10.1016/S1353-4858(12)70104-6.
12. Ha P. Malicious android spyware creator faces up to 10 years in prison. 2016. URL: http://www.neowin.net/news/malicious-android-spyware-creator-faces-up-to-10-years-in-prison.
13. Wang YM, Roussev R, Verbowski C, Johnson A, Wu MW, Huang Y, et al. Gatekeeper: Monitoring Auto-Start Extensibility Points (ASEPs) for Spyware Management. USENIX; 2004, p. 33–46.
14. Kirda E, Kruegel C, Banks G, Vigna G, Kemmerer R. Behavior-based Spyware Detection. Usenix; 2006, p. 273–88. URL: http://static.usenix.org/legacy/events/sec06/tech/full_papers/kirda/kirda_html/.