ISSN 2320 - 2602
Volume 5 No.5, May 2016
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst01552016.pdf

SMS Monitoring System For Detecting Premium SMS Malware In Smart Phone

Luna Ojah[1], Amarjyoti Pathak[3], ,Shrabani Medhi[2],

[1]Girijananda Chowdhury Institute of Management and Technology, India, luna.2aug@gmail.com
[2]Girijananda Chowdhury Institute of Management and Technology, India, amarpathak_cse@gimt-guwahati.ac.in
[3] Girijananda Chowdhury Institute of Management and Technology, India, shrabani26@gmail.com

ABSTRACT- We are trying to develop a SMS monitoring system for detecting malware on Android System. The warning system monitors the API calls related with suspicious activity and warn the user with a message. The warning system is able to detect for user suspicious activities running on the service layer and can take user consent to block the API call. We find that malware calls specific API calls through analysis of android malware samples.

Key words- Malware ,Smartphones, Bening application

1. INTRODUCTION

Malicious applications cause financial threats by collecting user information and sending premium rate SMS messages, To protect phones from the threats , many anti malware companies have developed anti malware applications. These anti malware applications are normally based on signature. The technical based on signature is fast and simple to detect known malware. But it is not able to detect new malware and it take 48 days to receive a signature for a new malware.[1]

Malware aimed at Android smart phones alone has grown over the last few months, threatening Android security, and other platforms are additionally coming under attack. In additament to malware, the other two major categories of threats to mobile contrivances are personal spyware and grayware. Spyware amasses information such as utilizer location,SMS messages, and call history without the victim's cognizance.[2]

1. SMART PHONE

Mobile phones have become the central computing and communication device today. Since August 2006, more mobile phones than inhabitants are registered in Germany . As the capabilities of these devices increase, they are not simple voice-centric handsets anymore; rather they represent tone step towards realizing the vision of **Mark Weiser called ubiquitous computing.** In this vision, Weiser describes that classical computers will be replaced by small, intelligent, distributed, and networked devices that will be integrated into everyday objects and activities. This replacement can be already observed in shops and warehouses using tags for monitoring and controlling items. But also the evolution of smart phones can be seen as part of this vision since they represent a possibility to making use of technical and computational capabilities in mobile context.

Smart-phone is the trend of unified communications which integrate telecoms and Internet services onto a single device because it has combined the portability of cell-phones with the computing and networking power of PCs.

2.MALWARE

Malware is a combination of the two words malicious and software, which clearly indicates that malware is a computer program with malicious intentions. In order to understand what these malicious intentions actually are, we introduce the terms: infection vector and infection payload. The infection vector describes which techniques are used to distribute them malicious application. Several known approaches are: e.g. file injection ,file transport, exploit, or boot sector corruption. The infection payload represents the actual content that is used to harm the victims' machine. Several known possibilities for payloads are: deleting files, denying service, or logging keystrokes.[5]

Malware can be propagated using several techniques and communication interfaces, ranging from an exploit to using social engineering. Regarding smartphones, the most used infection mediums are Bluetooth, Internet,MMS, Memory Card, and USB

The first proof-of-concept smart-phone worm, *Cabir,*has recently appeared. This is among the first signs of thee expansion of the Internet security threats into other networks like telecom networks by the means of inter operating devices, e.g., smart-phones that are endpoints to both networks

An overwhelming 79 percent of all mobile malware threats target devices running Google's Android operating system, according to a joint unclassified memo from the U.S. Department of Homeland Security and Department of Justice."Android is the world's most widely used mobile

operating system and continues to be a primary target for malware due to its market share and open source architecture.

- The platform is open , anyone can develop and publish application for Android market , The attacker can easily deliver malicious application onto unsuspected user.[3]

- The presence of alternative Android market make this problem worse because of lack in review method thus making them unreliable source of application.

- The android uses permission based security model to have access to different functionalists of the device. This model provide information about the access and privilege capabilities of the application , this may be an indication of malicious application to the technical user but normal user mainly ignore it.[3]

3. NEED FOR DETECTION OF MALWARE IN SMARTPHONE

These security threats are troublesome due to the large amount of personal data that smartphone users store in their phones as well as confidential transactions that these users perform using voice and/or data interface of their smartphones.[4] Additionally this malicious code leads to both a dramatic drain in the battery, as well as creating an abnormal load on the cellular network.

Smartphones contain security-sensitive information of a user such as contacts, SMS, photos, and GPS information. Because smartphones are always turned on and ready to connect to the Internet, that sensitive information is in danger of leakage. Various kinds of malware are more and more attacking smartphones, especially Android phones. The mobile malware is growing at a faster clip isn't surprising, but the rise suggests attackers are starting to see Android as a potentially lucrative attack avenue. About half of malicious apps focus on conning the user out of money by signing them up for pricey premium services. Cyber criminals often create and distribute Trojan viruses that infect a victim's mobile phone, so that the phone makes calls or sends SMS text messages – without the user knowing. The malware will direct these unauthorized calls to premium-charge numbers – or to chargeable SMS text services – that are operated by the criminal.By infecting large numbers of phones – and getting each phone to make several calls or send several texts – the criminal can generate a significant revenue stream.

4. FRAMEWORK OF THE RESERCH

4.1 PREMIUM SMS MALWARE

Premium-rate number. Typically, these are "short codes", which are shorter than usual phone numbers. Each country and carrier regulates short codes differently, but usually an oversight body issues the short codes for a fee. In the United States for example, a dedicated short code may cost $1500 USD to set up and then $1000 per month. A shared short code where the message must be preceded by a keyword can be obtained for as low as $50 per month.

When calling or sending an SMS to a short code, the caller is billed a premium rate above the normal cost of an SMS or phone call. The revenue is then shared by the attacker, carrier, and the SMS aggregator. The attacker receives 30-70% of the premium rate charge depending on the carrier, amount charged per message, and number of messages received. Most carriers allow a premium rate of up to $10.00 per message, but some carriers will allow charges in excess of $50.00 per message. If the attacker uses an SMS aggregator, the attacker will pay an additional fee. SMS aggregators provide short code services such that clients share the same short code, but are able to bill and differentiate services by ensuring users place a specific keyword related to their service within the SMS. This allows multiple services to essentially split the cost of a single short code number.

Android applications can request permissions to send SMS messages at installation. T**hese SMS messages Can be sent without the user confirmation. Sending an SMS to a premium short code causes the phone owner to incur a charge on their phone bill and the attacker to generate revenu**e. An application can easily send multiple messages, inflating charges. However, short codes are usually carrier and country-specific. This means multiple short codes are needed or threats may only target specific regions.

Premium-call phone numbers are also available, but may be restricted from automatically being dialed on some devices. In addition, the dialer will be present on-screen and possibly noticed by the user.

5. STUDIES AND FINDINGS

5.1. STATIC ANALYSIS OF PREMIUM RATE SMS BILLING APPLICATION

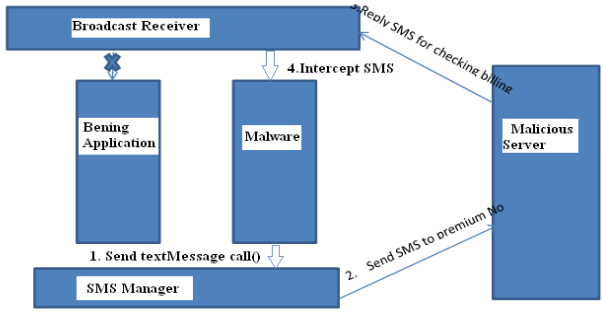

Figure:1 Premium rate sms billing application model

When malware is installed , malicious Receiver is registered to broadcast messages from malicious server to only malware so that the user can't realize whether specific number messages are delivered or not .Because the priority of malicious broadcast receiver is higher than SMS broadcast receiver .After malware is started ,sending TextMessage() of SMS Manager API on the service layer invoke to send a message with the premium no which is already defined in the source code.[6]

Malicious server receive a message from the user phone and then the server sent a message to the user phone for that SMS billing is charged. After the phone receives the message malicious broadcast Receive which is already registered intercepts the message and the original SMS app does not receive the message.
The code used in malicious application to send premium SMS are
SmsManager.*getDefault*().sendTextMessage(881151, **null**, "text!", **null**, **null**);

The premium no is already defined in the source code [6]

5.2. IMPLEMENTATION

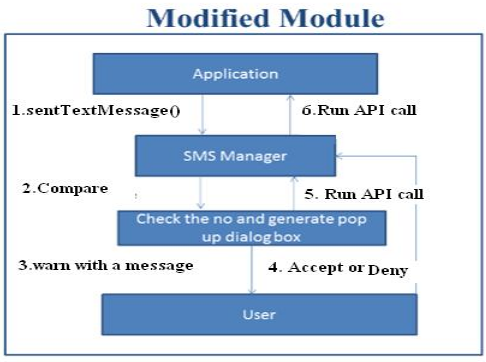

Figure:2 Modified Model

Few changes are done in the SmsManager.class file in android.telephony package to monitor for a specific API call that is sendTextMessage(). If sendTextMessage() call is invoked then first it will compare the no of digits in the phone no, if it is less than 10 digit no then the sendTextMessage() function will generate a popup message into the user screen so that the user can decide whether the message should be send or not.

- In the current android system there is no way that the user can know that any API is using the sendTextMessage() function to send sms.
.
- It can block specious sendTextMessage () API calls if the user is not sure about running API calls.

Snap-Short

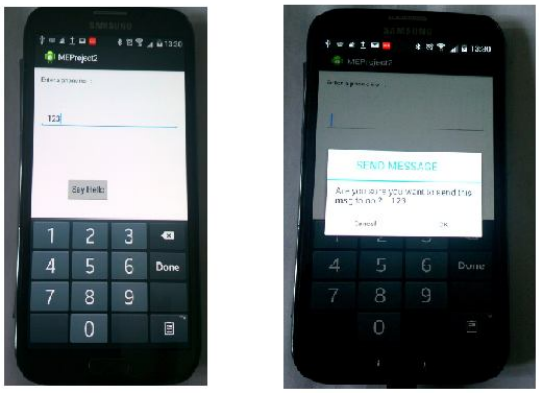

Fig:3 :Application snapshot

6.CONCLUSION

Here we have analyzed a malware that send premium rate SMS to remote server. The main reason to choose these malware is causing most financial threats. We have seen that malware uses specific API calls for malicious activities. The premium rate SMS billing application uses sendTextMessage() of SMS manager API with the target number which is already defined by malicious developer.
The existing anti – malware application are based on signature for detecting malware. If malware is transformed to avoid detecting based on signature , the signature of malware is changed. Therefor the existing anti- malware application do not detect new and unknown malware because they have no signature.
In order to address this problem , this warning module is proposed, which will block API calls to send message to premium numbers.

7.FUTURE WORK

There is a limitation that the user is familiar with android application but has minimum knowledge of malware. This work is the first step in detecting premium SMS android malware . Next step is to compare normal android application with malicious application for developing automated system for malware detection. In order to keep the latest data set the warning system must be periodically updated with latest bening application and malware application.

REFERENCES

[1].J.Oberheide ,E cooke and F Jahania,"Cloudv:Nversion antivirus in the network cloud",in Proc ,17th USENIX Security Symposium, 2008, pp.2.2-1-2.2-6

[2] Malware Prevention and Detection System using S mart Phone Sachin M. Kolekar ,Department of Computer Engineering,STES's Smt. Kashibai Navale College of Engineering, Pune-41 Parikshit N. Mahalle, Ph.D Department of Computer Engineering,STES's Smt Kashibai Navale College of Engineering, Pune-41

[3].An Automated Malware Detection System for Android using Behaviour-based Analysis ,Abela, Kevin Joshua L. Delas Alas,Jan Raynier P. Angeles Don Kristopher E. Tolentino , Robert Joseph

[4].A Survey on Malware and Malware Detection System , Imtihal A.Saeed, Ali Aelamat, Ali M.A Abuagoub

[5].Malware Detection Through Decision Tree Classifier, Kanran Morovati, Sanajay Kadam

[6]. Warning System for Detecting Malicious Applications on Android System , Sung-Hoon and Seung –Hun Jin