ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering
ICRITCSA
M S Ramaiah Institute of Technology, Bangalore
Vol. 5, Special Issue 2, October 2016

An Introduction on Mobile Malware and its Prevention

Shruti Prabhuli Ghatnatti[1], Spoorti A[2], Surekha B[3]

Assistant Professor, Bachelor of Computer Application, K.L.E.S's B.C.A, Hubballi, India[1]

Student, Bachelor of Computer Application, K.L.E.S's B.C.A, Hubballi, India [2, 3]

Abstract: In today's digital world, people are so into the technology they forget to keep secure their data and information which is stored on their devices. The rapid increase of economic issues in the world makes person to leak the data and make money in a hawkish way. This may become a threat to the individual's life. The threat is termed as Malware which is injected in user's device to access the information unknowingly. This paper attempts to describe the mobile malware and its precautions.

Keywords: User Device, Mobile Malware, Detection Techniques, Malware Types.

I. INTRODUCTION

Usage of Smartphone is rapidly increasing and it is increasingly becoming a sophisticated device. Now days, mobile computing is adopted for many purposes such as to save contact numbers, personal data, financial transactions, process internet access, social networking, gaming and checking emails. Smartphone has brought convenience to people's life, at the same time, it causes problems of security. People now days download applications which require some information to be accessed from device and there is an increase in chance that other users will gain access to personal information.
Mobile malware threat is a real challenge in mobile devices. This threat is exacerbated with the increasing number of mobile devices accessing to the internet as a basic and daily service. Some of the malware are harmful to the mobile devices in many ways [1]. Such as exhausting battery use, destructing files and fraudulently sends SMS or Email to the contacts without the knowledge of the mobile device owner.

Mobile malware can be from the following cases mobile users receives a text message from someone they didn't know and an SMS requesting the user to click on an embedded link specified in the message, a "voicemail" to subscribe. Such techniques hide the internal codes that the hackers use to inject a malware onto the phone and attempt to access over personal data .One security threats over the use of mobile devices is SMS fraud which is a common threat in all smart phones. It working is as follows: the users receive a message asking them to subscribe their services for a specific period. The busy life of users makes them to subscribe for the services unknowingly by providing personal information like bank details. Initially they charge free of cost and later after several periods of service they charge and the deduction of the amount is not intimated to the users.

In this paper, we describe the threats in current mobile security problems and development of suitable solution we focus on our research on malware. Malware is software program designed to damage or do other unwanted actions on the computer system.

II. HISTORY

Malware always rises where there is popular platform, a range of attack vectors and some means of monetization, and mobile devices offer all three.
If we look back to 2000, with the launch of the Ericsson R380 and the Nokia 9210, it took over 3 years for the first examples of mobile malware to arrive.

In June 2004, security researches from Kaspersky Lab sent copies of the first mobile virus, cabir. It is a worm that infected the Symbian's 60 OS, This malware code was written by members of an international group of virus writers.

A few months later a cracked version of game called mosquito appeared on the internet. Along with the popular game the package contained Trojan.mos. Each time the game played the Trojan would send a premium SMS message to certain number, making it the first mobile virus to take money from its victims.

By the end of 2004, Cabir and mosquito had been joined by skuller, another Symbian Trojan. Skuller exploited a vulnerability in Symbian replacing system icons with skull and cross bones alternatives, then delete application files, installing corrupt the infecting user files.
In 2005, Symb OS Comm Warrior. A entered the scene. These malware variants have been floating around mobile phone networks for years.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

In 2006, Trojan. Read Browser. A, the first Trojan for J2ME that could infect different mobile phone platforms was Trojan. Read Browser. A.
In 2010, Symb OS. Zeus Mitmo, is also one of the threats that was capable of destroying bank account transaction text messages from the infected mobile device to the attackers.
In 2011, android. Geinimi was an early bot for mobile devices, mobile botness have became popular and are used for click fraud and premium text message scams.
And also the first android threat to use an exploit to elevate its privileges was Android. Rootcager .

III.ARCHITECTURE

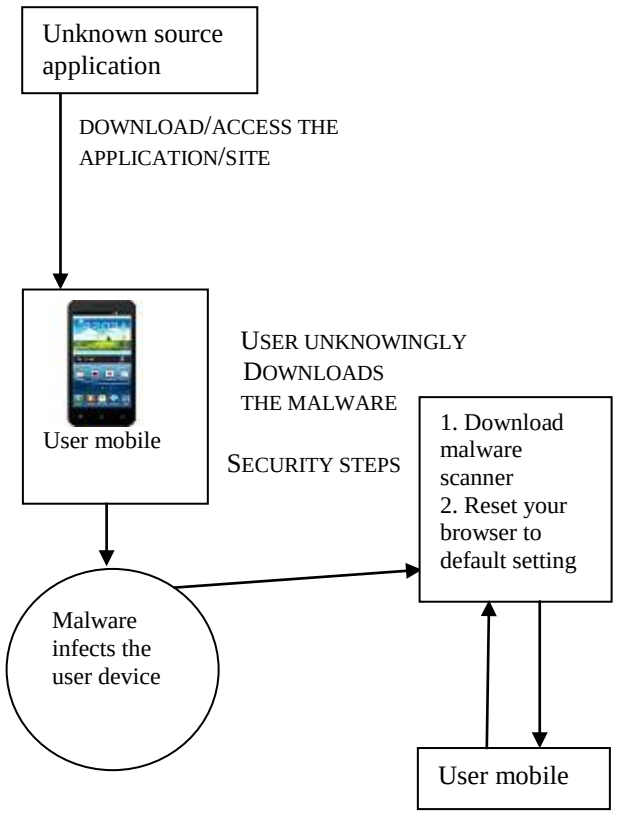

Fig1.Malware infecting user device

In this Fig1, we are explaining how the malware attacks to the mobile device and what are its prevention steps.
When users download the application from the unknown source like accessing unauthorized site, downloading fake security software, malware transfer from text messages and it may be by tracing QR code, unknowingly malware attacks mobile device, then mobile device will be infected by malware. There are some security steps to overcome the effect of malware, they are:

1. Reset your browser to default setting:
If mobile is infected by malware then you can reset browser to its default settings.

2. Download malware scanner:
If mobile is infected from malware then download some malware scanners like avast, 360 securities, CM security, clean master etc and also we can scan all apps for malware by remote lock feature.

3. Encrypting the devices:
By encrypting the device we can protect our devices so that it is difficult to break in and steal the data or the contents of devices and also setting the password for device and sim is must.

4. Cloud sharing alternatives:
Users can access data from cloud by using any devices.

5. Install apps from trusted sources:
Like Google play, apple Appstore and read the reviews, read the privacy policies.

IV. TYPES OF MALWARE AND DETECTION

1. Virus
Virus is a small program having harming intention and it has ability to create multiple copies of itself. Its work is inserting virus code in an executable code. When the file starts running then the Virus code will start its execution.

2. Worm
Worm starts sending replication of itself to other system through network without noticing the authorization of the user. Worm spread through network and the devices will be infected. It encrypts files delete files or sends junk email to user.

3. Spyware
The software which collects private information of the user this can happen when users download free or trial software. It assembles the data like account number email, address, password, credit card number etc.

4. Adware
Adware is advertising supported software includes plays or downloads advertisement. In system automatically downloads some of the free games and It denotes clients are some examples of the common adware programs.

5. Trojans
Trojan horse is injected by its designer in an application. Remote hijackers use this malware to launch their attack and they use system for their system.

6. Botnet
Botnet is one of the types of malware that takes the control of system distantly and sends malware. Bought will not wait for a command from the third party by sitting around the infected machine. On the other hand, it looks for the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICRITCSA

M S Ramaiah Institute of Technology, Bangalore

Vol. 5, Special Issue 2, October 2016

communication having like occurrences of bots awaiting instructions.

Malware Detection Technique

A. Static Analysis

Static analysis is a quick, not costing a deal to find malicious characteristics or bad segments in an application without executing them. These techniques are used in a preceding analysis, when introductory applications are for at evaluated to detect any security threats. Static analysis examines downloaded app by inspecting its software properties and source code

B. Dynamic Analysis

Dynamic analysis involves execution of application is separated from other environment to track its execution behavior. In contrast to static analysis, dynamic analysis, dynamic analysis enables to open up natural behavior of malware as executed code is analyzed, therefore immune to obfuscation attempts.

C. Permission based analysis

With the help of listed permissions in manifest.xml, various researchers are able to detect applications malicious behavior. These permissions have the ability to limit application behavior by controlling over privacy and reducing bugs and vulnerabilities.

V. CONCLUSION

Smart phones are becoming popular in terms of power, sensor and communication. Modem, smart phones provides some of the services like messaging, browsing internet, emailing, playing games. Due to its multi-functionality, new security threats are occurred for mobile devices. In this paper, we discussed some of the examples of malware was to show how rapidly the threat is developing along with the architecture of malware. And we have categorized various mobile malware detections.

REFERENCES

[1] Mobile Application for Malware Detection, Pranjali Deshmukh, Pankaj Agarwal- International Research Journal of Engineering and Technology.
[2] Detect and prevent the mobile malware, Abdullah Mohammed Rashid & Ali Taha Al-Oqaily.
[3] An analysis of Mobile malware and detection technique, Aswathy Dinesh
[4] Mobile malware Dr. Alexander Pons
[5] Review on Mobile threats and detection techniques By Lovi Dua and Divya Bansal.