ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY
TECHNOLOGY

Malicious Codes in Mobile Phones

Ankur Singh Bist
Govind Ballabh Pant University of Agriculture and Technology, India
ankur1990bist@gmail.com

Abstract

In this paper a survey study is made on various issues of mobile malicious codes. Spreading pattern of different mobile viruses is discussed to make a collective analysis of concerned problem and various approaches are also discussed to solve those problems.

Keywords: Mobile viruses, operating system.

Introduction

The first instance of a mobile virus occurred in June 2004 when it was discovered that a company called Ojam had engineered an anti-piracy Trojan virus in older versions of their mobile phone game Mosquito [1]. This virus sent SMS text messages to the company without the user's knowledge. This virus was removed from more recent versions of the game; however it still exists on older, unlicensed versions [1]. These older versions may still be distributed on file-sharing networks and free software download web sites [1].

Issues of Mobile Malwares

Trojan: SymbOS/Skulls is distributed in a malicious SIS file named "Extended theme.SIS", allegedly a theme manager for Nokia 7610 smart phone (authored by "Tee-222") [2]. Skulls.A and other Skulls Trojans are targeted against Symbian Series 60 devices, but can also affect other Symbian devices, for example Nokia 9500, which is a Series 80 device[2]. However when trying to install Skulls Trojan on Nokia 9500, the user will get a warning that the SIS file is not intended for the device, so risk of accidental infection is low[2].

On installation, the Trojan will replace the system applications with non-functional versions, so that all but the phone functionality will be disabled [2]. It will also cause all application icons to be replaced with picture of skull and cross bones; the icons don't refer to the actual applications anymore so none of the phone's normal applications will be able to start [2].

Figure 1[2]

This basically means that if Skulls is installed, only calling from the phone and answering calls works. All functions which need some system application, such as SMS and MMS messaging, web browsing and camera no longer function [2].

If you have installed Skulls, the most important thing is: do not reboot the phone**.**

Process of Installation

Skulls SIS file does not contain any malicious code as such, it is just a Symbian Installation file that installs critical System ROM binaries into C: drive in with exact same names and locations as in the ROM drive [2].

The application files installed by Skulls are normal Symbian OS files extracted from the phone ROM. However due to feature in Symbian OS, copying them into correct locations in the device C: drive, causes critical system applications fail to function [2].

ISSN: 2277-9655
Impact Factor: 1.852

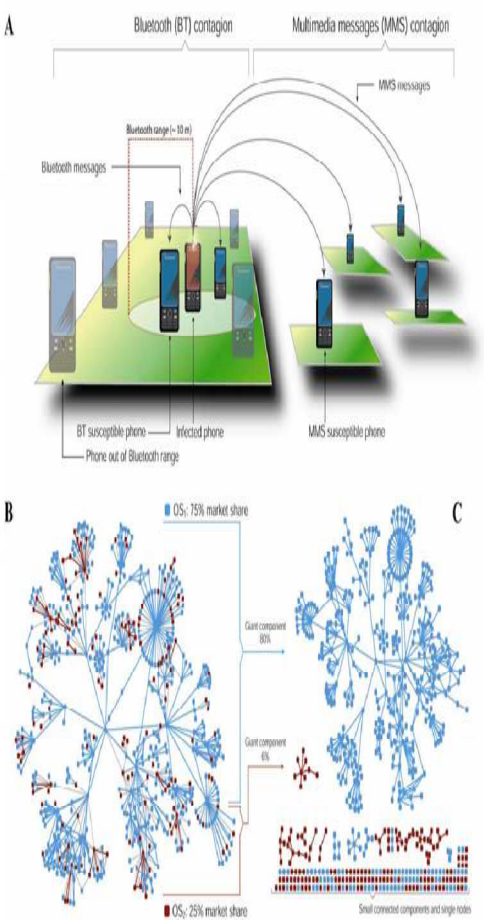

FIGURE 2[3]

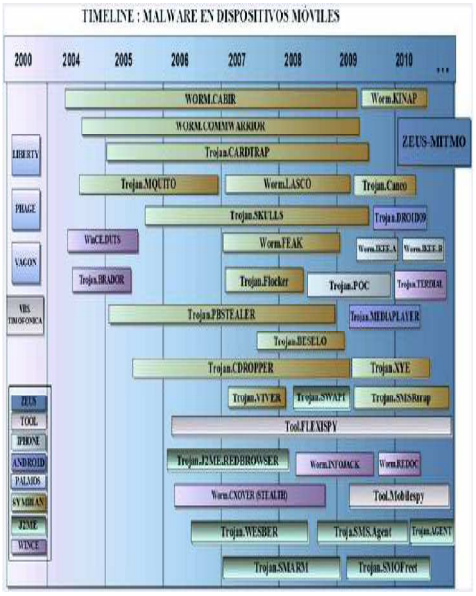

Figure 4[5]

AN OVERVIEW OF EXISTING ANDROID MALWARE (PART I: INSTALLATION AND ACTIVATION)

	Installation				Activation								
	Repackaging	Update	Drive-by Download	Standalone	BOOT	SMS	NET	CALL	USE	PKG	BATT	SYS	MAIN
ADRD	√				√		√	√					
Anserverbot	√	√			√	√	√		√		√	√	
Asroot				√									
BaseBridge	√	√			√	√	√				√	√	
BeanBot	√					√		√					
Bgserv	√				√	√							√
CoinPirate	√				√	√							
Crusewin				√	√	√							
DogWars	√												
DroidCoupon	√				√		√	√		√			
DroidDeluxe				√									
DroidDream	√												√
DroidDreamLight	√				√			√					
DroidKungFu1	√				√						√	√	
DroidKungFu2	√				√						√	√	
DroidKungFu3	√				√						√	√	
DroidKungFu4	√				√						√	√	
DroidKungFuSapp	√				√						√	√	
DroidKungFuUpdate	√	√											
EndOfDay	√				√	√							
FakeNetflix				√									
FakePlayer				√									
GamblerSMS				√	√								
Geinimi	√				√	√							
GGTracker			√	√	√	√					√		
GingerMaster	√				√								
GoldDream	√			√	√	√		√					
Gone60				√									
GPSSMSSpy				√		√							
HippoSMS	√				√	√							√
Ikee	√		√										
JSMSHider	√									√			√
KMin				√	√								
Lovetrap				√	√	√							
NickyBot				√	√	√							
Nickyspy				√	√								
Pjapps	√				√	√						√	
Plankton		√		√									
RogueLemon				√		√							
RogueSPPush				√		√							
SMSReplicator				√		√							
SndApps				√	√								
Spitmo			√	√		√		√					
TapSnake				√	√								
Walkinwat				√									
YZHC				√	√								
zHash				√	√								
Zitmo			√	√		√							
Zsone	√					√							√
number of families:	25	4	4	25	29	23	4	6	1	2	8	8	5
number of samples:	1083	85	4	177	1050	398	288	112	187	17	725	782	36

Table-1 [4]

There are various techniques adopted by different authors to prevent virus on mobile devices .Bayesian decision theory using heuristic rules are used on virus samples. Viruses are detected on the basis of DLL usage of a program. This technique proves itself very useful in detection of unknown viruses [6].

Many of the security measures that apply to PCs also apply to smartphones. These are some best practices we recommend to help you protect your cell phone [5]:

- Enable access protection measures such as a PIN or password (if possible).
- Configure the smartphone to automatically lock after a minute or so being idle.
- Before installing or using new smartphone apps or services, check their reputation. Only install applications from trusted sources [5].
- Pay attention to the security permissions requested by every application and service you install.
- Keep your operating system and software applications up to date.
- Disable features not in use: Bluetooth, infrared or Wi-Fi.
- If you have Bluetooth enabled, set your device to be hidden and password-protect it [5].
- Make regular backup copies of your important files.

ISSN: 2277-9655
Impact Factor: 1.852

- Encrypt sensitive information whenever possible.
- Use call and SMS encryption software.
- whenever possible, do not store sensitive information on the smartphone. Make sure it is not cached locally [5].

Conclusion

In this paper we reviewed approaches and methods that are given by various authors to explain different issues of mobile malwares .The purpose of this collective analysis is to present the solution set for mobile virus detection and prevention and try to evolve some more efficient approaches for the concerned problem. This study will make vision clear to all those working in this area.

References

[1] www.wikipedia.com.
[2] www.fsecure.com.
[3] Pu wang ,"Understanding the patterns of mobile phone viruses."
[4] Yajin Zhou," Dissecting Android Malware: Characterization and Evolution"
[5] Consejo Nacional Consultivo de Cyber-Seguridad , Smartphone malware. Deepak Venugopal ,"Intelligent virus detection on mobile devices"