# Mobile Botnet Attacks – an Emerging Threat: Classification, Review and Open Issues

**Ahmad Karim[*], Syed Adeel Ali Shah,Rosli Bin Salleh, Muhammad Arif, Rafidah Md Noor, Shahaboddin Shamshirband**
Faculty of Computer Science and Information Technology, University of Malaya, Malaysia
[e-mail: ahmadkarim@um.edu.my]
[*]Corresponding author: Ahmad Karim

*Received July 21, 2014; revised October 2, 2014; accepted March 4, 2015;*
*published April 30, 2015*

## Abstract

The rapid development of smartphone technologies have resulted in the evolution of mobile botnets. The implications of botnets have inspired attention from the academia and the industry alike, which includes vendors, investors, hackers, and researcher community. Above all, the capability of botnets is uncovered through a wide range of malicious activities, such as distributed denial of service (DDoS), theft of business information, remote access, online or click fraud, phishing, malware distribution, spam emails, and building mobile devices for the illegitimate exchange of information and materials. In this study, we investigate mobile botnet attacks by exploring attack vectors and subsequently present a well-defined thematic taxonomy. By identifying the significant parameters from the taxonomy, we compared the effects of existing mobile botnets on commercial platforms as well as open source mobile operating system platforms. The parameters for review include mobile botnet architecture, platform, target audience, vulnerabilities or loopholes, operational impact, and detection approaches. In relation to our findings, research challenges are then presented in this domain.

***Keywords:*** Attacks, malware, mobile botnet, smartphone, DDoS

This version extends our previous work, which appeared in WorldCIST'14 (World Conference on Information Systems and Technologies) 2014, April 15-18, Madeira, Portugal. This research was supported by a research grant from the R&Dprogram (IPPP) of the University of Malaya [Project No. FP034-2012A].

**http://dx.doi.org/10.3837/tiis.2015.04.012** **ISSN : 1976-7277**

# 1. Introduction

Mobile attacks are the most critical among the emerging threats from the increasing market penetration of smartphones and handheld devices. Smartphones use full-featured operating systems (OS) incorporated with powerful hardware that supports manifold interfaces and sensors. At present, personal computers (PCs) have declined as the primary choice of computing. Recent statistics show that global shipments of mobile devices have immensely exceeded those of PCs since 2011 [1]. In the near future, the wide-scale deployment of 4G technologies,such as LTE and WiMAX, will become the major source of broadband Internet access for the general public. From 2012 to 2013, 4G-enabled devices represent only 0.9 percent of all global mobile connections,accounting for 14 percent of all mobile data traffic [2].

This technological shift has motivated cyber criminals to exploit the vulnerabilities of smartphone devices through off-the-shelf malware creation tools [3]. Similarly, the spread of mobile applications have enabled the dissemination of malicious code to a wide range of potential audience. Through the Internet, the majority of current mobile threats replicate the behavior of attacks on desktop machines. Therefore, many of the existing solutions can also be considered applicable to the malicious mobile attacks. Nevertheless, mobile devices have their own constraints, such as limited processing, less data storage capabilities, and heterogeneity of OS (e.g., Android, iOS, and Windows), that restricts the security solutions to be efficiently programmed.

## 1.1 Anatomy of Mobile Botnets

Mobile botnet [4] refers to a group of affected mobile phone/smartphones that are remotely controlled and administered by botmasters through the C&C architecture. **Fig. 1** shows the default working environment of a mobile botnet[5]. The network (botnet) of compromised computers or hand-held devices comprises abotmaster (a person who hinders the usual network traffic flow), a command and control (C&C) architecture (designed to implement malicious activities instructed by the botmaster), provoked mobile or stationary computing resources called bots, and a target victim.

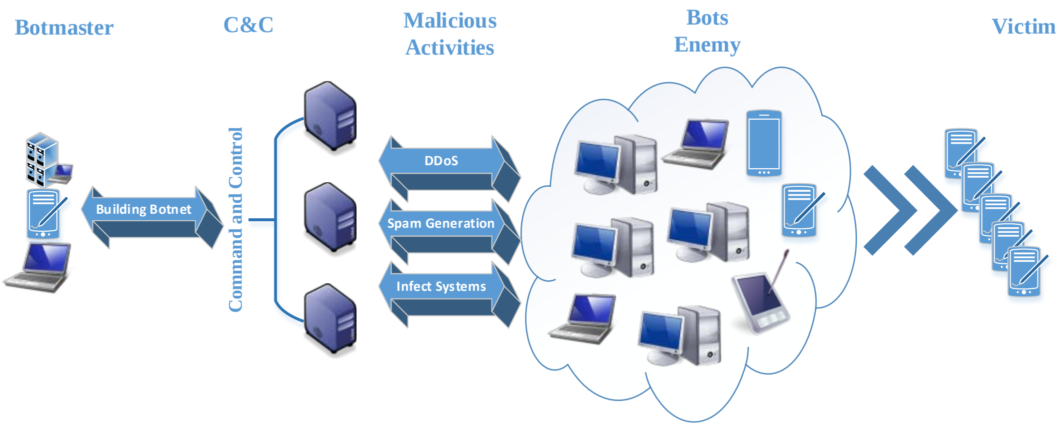

**Fig. 1.** Anatomy of Mobile Botnets

**Table 1** highlights possible mobile botnet attacks. These activities include propagation of viruses and worms, theft of private and confidential information, spam generation, unauthorized root access, access to control panel, illegal phone calls, unauthorized file and photo access, service disruption (also known as DDoS), power outage, and memory consumption. In addition, as mobile botnet operations can be implemented by disseminating malicious applications to mobile subscribers, both concepts are therefore interrelated.

**Table 1.** Possible Mobile Botnet Attacks

| Attack type | Description |
|---|---|
| Sending Email | A mobile bot Weldac was designed to send emails without being noticed by mobile user. |
| Sending MMS/SMS | An infected mobile device may send an MMS/SMS to service providers or to a wide range of subscribers. An SMS-based heterogeneous mobile botnet [6] was created to perform a similar task. |
| Victim Selection | Victims/bot enemies can be selected by botmaster from the contact list or address book of infected mobile devices. |
| Mobile Voting System | A botmaster can dismiss recently evolved mobile voting services. |
| Charity Services | Giving money to charity organizations using mobile services may exploit by mobile botnet. |
| Spyware | Infected mobiles can be treated as spyware to collect personal information of subscribers. |
| Privacy Issues | Privacy issues may arise in mobile networks for stealing personal information. For instance credit card number or financial information, while interacting with response servers. |

The latest statistics show that in the smartphone industry, Android has captured a record 81% of the global market share from 2012 to 2013 [7]. **Table 2** [8] shows the market share of different smartphone vendors. Overall, the market grew by 45.5%, relatively faster than the rate in 2012, which is 44%. Android's market share jumped to 81.3% from 75% last year, which alsoincreased from last quarter,whereasApple slid from 15.6 % in Quarter3 of 2012 to 13.4% this year. Moreover, BlackBerry lost over 75% of its market share, dropping to a single digit 1%. Consequently, during the same period, Android is affected most in comparison with other platforms. As a result, the Android platform is currently at high risk of malwareattacks.**Table3** shows the total number of modifications and families of mobile malware with their infection ratio.

**Table 2.** Global smartphone OS market share

| Platform | Quarter 3, 2012 | Quarter 3, 2013 | Quarter 1,2014 |
|---|---|---|---|
| Android | 75.0% | 81.3% | 30.8% |
| Apple | 15.6% | 13.4% | 15.2% |
| Microsoft | 2.1% | 4.1% | 4.7% |
| BlackBerry | 4.3% | 1.0% | 4.4% |
| Others | 3.0% | 0.2% | 4.3% |
| **Total** | **44.0%** | **45.5%** | **40.7%** |

Recently, a number of mobile botnets have evolved to degrade the performance of mobile devices. For example, ZeuS [9] is a botnet that focuses onBlackberry, Symbian, and Windows platform users, and DroidDream [10] botnet affects Android-based devices. Similarly, IKee.B [11] is a botnet that is used to scan IP addressesiniPhones, whereas BMaster and TigerBot specifically target Android application frameworks.

**Table 3.** The total amount of modifications and families of mobile malware along with their infection ratios, updated as of January 1, 2014 [12]

| Platform | Modification | Family | Infection Ratio |
|---|---|---|---|
| Android | 43600 | 255 | **65%** |
| J2ME | 2257 | 64 | **2%** |
| Symbian | 445 | 113 | **32%** |
| Windows Mobile | 85 | 27 | **< 1%** |
| Others | 28 | 10 | **1%** |
| **Total** | **46415** | **469** | **100%** |

### 1.2 Contribution

This review serves as a roadmap for the researcher community to study and enforce secure communication patterns that are focused on various aspects of mobile botnet attack vectors. Consequently, this article analyzes the prospective threats and vulnerabilities of botnets based on mobile networks.

To the best of our knowledge, a comprehensive survey on mobile botnet attacks has yet to be made. In our previous work [13], we have discussed mobile botnet attack vector classes. The present study is a more compact and comprehensive review on mobile botnet attacks exploiting mobile botnet architecture, platform, target audience, vulnerabilities/loopholes, operational influence, and detailed detection approaches. Therefore, the contribution of this review is three-fold. First, from the extensive literature survey, we conclude that to understand the threat of a mobile botnet, the features of malicious mobile attacks should be comprehended(e.g.,typeof attack, platform, category, target audience, loopholes, dissemination techniques, operational influence, and defensive approaches). Therefore, we set the timeline for the mobile botnet/malwares according to the aforementioned properties.Second, weproposetaxonomy of state-of-the-art mobile botnet attacks to highlight different aspects of the attacks as well as to identify recovery techniques to avoid this growing threat. Third, we highlight open challenges and issues pertaining to the dissemination of these malicious mobile botnet threats.

The rest of the paper is organized as follows.Section2 discusses a brief background with respect to mobile malware and differentiates between interchangeably used terms,such as mobile malwares and mobile botnets.Section 3 presents taxonomy to characterize the mobile botnet attack vectors. Section 4 compares the existing mobile botnet attacks based on the significantly derived parameters from the taxonomy. Finally, Section 5 highlights issues and challenges that require further scrutiny to avoid mobile botnet attacks.

## 2. Background

In the rapidly growing world of mobile computing, mobile botnets that target mobile phone devices such as smartphones have emerged as a serious threat. The aim of such an attack is to gain access to the resources and content of a mobile user device and transfer control to the botnet initiator. Hackers take advantage of the exploited area/loopholes of mobile devices to gain unauthorized access to the compromised mobile devices. Eventually, the hackers aim to perform malicious and unauthorized activities, including making illegal phone calls, accessing the control panel, sending emails, initializingaworm code, and accessing unauthorized files or photos [14, 15].

A mobile bot that employs URL flux, Andbot [14] is a stealthy, low-cost, and resilient bot that uses a botmaster for illegal activities in a mobile environment. This botnet uses microblogs to send malicious commands. Andbotwaseasily implemented on smartphones for longer durations without being noticed or detected. Andbot integrates several other schemes to make it efficient and stealthy. Cloud-Based Push-Styled Mobile Botnets [16] is a new type of botnet in the mobile environment that uses push-based notification services to disseminate the commands. A novel C&C channel is presented using the Cloud-to-Device Messaging (C2DM) service, which is provided by Google for Android platforms. This channel shows that C2DM is stealthy in terms of command traffic, power consumption, bandwidth utilization, and transformation of commands to all bots. Likewise, Epidemic mobile malware is a new, terrifying threat for mobile users [17] thatdisseminates rapidly in smartphones. The malware affects older versions of iOS,butit is still a predominant threat for mobile users. The Kaspersky research lab report [12] on the total number of families and modifications of mobile malware was presented on January 1, 2013 (**Table 2**). According to this report, the substantial growth of the Android platform has made it the major target of malware programmers and botnet creators.

Previous generations of botnets have predominantly targeted either the most vulnerable systems or highly utilized computer systems in terms of user requests or bandwidth. However, the recent consideration of botmaster has shifted to mobile devices, as these devices are well-equipped with latest developments in technology. Moreover, the high degree of Internet usage, convenience of use, and their mobility are sufficient factors to capture the attention of a botmaster. **Fig. 2** shows the evolution of challenges and properties inherited from traditional botnets to more recent mobile botnets.

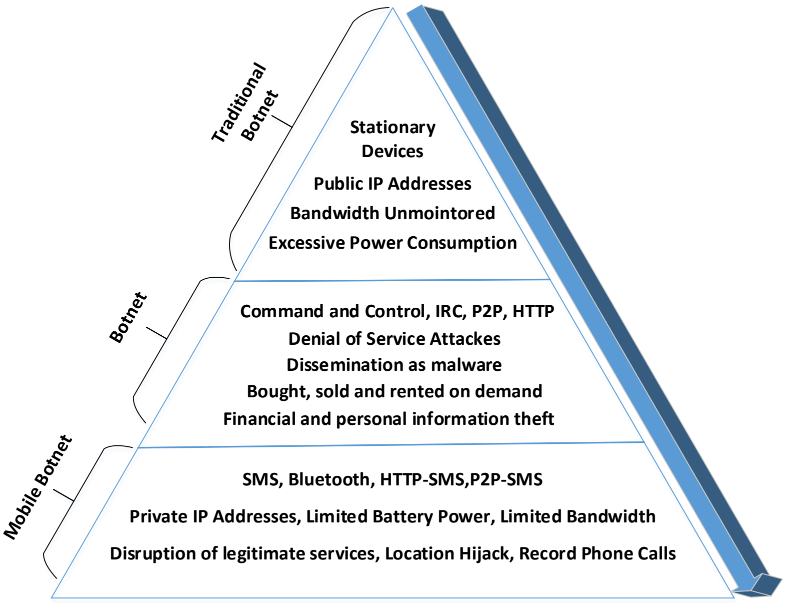
Traditional Botnet
Stationary Devices
Public IP Addresses
Bandwidth Unmointored
Excessive Power Consumption
Botnet
Command and Control, IRC, P2P, HTTP
Denial of Service Attackes
Dissemination as malware
Bought, sold and rented on demand
Financial and personal information theft
Mobile Botnet
SMS, Bluetooth, HTTP-SMS,P2P-SMS
Private IP Addresses, Limited Battery Power, Limited Bandwidth
Disruption of legitimate services, Location Hijack, Record Phone Calls

**Fig. 2.** Challenges inherited from traditional botnets to mobile botnets

### 2.1 Mobile Malware vs. Mobile Botnet

Although the terms mobile malware, adware, spyware, viruses, and botnets are used interchangeably, their activities distinguish them from one another [18].

A mobile botnet is a network that is formed and controlled remotely by criminals using mobile devices and smartphones --contaminatedby malware (e.g., computer virus, key loggers, and other malicious software). Once these devices become registered with a botnet, they are able to communicate with a device located somewhere in the C&C architecture. These devices receive instructions from C&C and perform them accordingly. To bring about control over these devices, the criminals may have different intentions of either gaining financial benefits or launching attacks on websites or networks. Their actions may harvest user data, including passwords, social security numbers, credit card numbers, addresses, telephone numbers, and other personal information without the user's knowledge. Data can then be unethically used to attempt identity theft, credit card fraud, spamming (i.e., sending junk email), website attacks, and malware distribution.

In contrast, a malware is a contentious, intrusive, malevolent, or annoying program segment (e.g.,rootkit, Trojan, or backdoor) intended to manipulate a device without the owner's knowledge [19]. A malware is often distributed as spam within a malicious attachment or link in an infected website. Manipulation by a remote C&C is not necessarily required for a malware program. Hence, the main difference between mobile malware and mobile botnet is the unconditional control of a remote machine over the mobile botnet. This article discusses mobile botnets and investigates its attack vector in particular. In addition, previous studies have discussedmobilemalware,which is outside the scope of the present study.

### 2.2 Mobile Botnet Constraints:

As compared with PC-based botnets, mobile botnets have relatively less penetration ratio in smartphones because ofseveralconstraints that allows for easy bot detection. The constraints can be specified as resource-based and communication-based. As a result, the implementation of mobile botnet attacks is still limited in scope. According to [20], the constraints are identifiedasfollows: 1) battery power, 2) application usage cost, 3) communication cost, and 4) communication complexity.

The battery power of smartphones is limited as compared with PCs. The excessive battery power usage may be an indication of superficial activity and make bots sensitive to detection. The application usage is also a constraint in easy bot detection under situations in which the application usage cost exceedsthenormal cost experienced by the user. Similarly, communication cost of smartphone applications can be monitored to detect potential botnet attack. Therefore,if C&C utilizes an excessive amount of network traffic, this abnormal network behavior may signify a possible bot. Finally, communication complexity is defined by the mobility of smartphones and the dynamic network topology, which makes it difficult for the bots to operate with persistence [14].

## 3. Taxonomy of Mobile Botnet Attach Vector

In this section, we present a thematic taxonomy of mobile botnets based on the mobile botnet attack vector (**Fig. 3**).

### 3.1 Taxonomy

Nowadays, mobile devices are capable of using Internet connection [21, 22] through different IP-based technologies that evolved within the mobile network and wireless network (WLAN) such as High-Speed Downlink Packet Access (HSDPA), Universal Mobile Telecommunication System (UMTS), Evolution-Data Optimized (EVDO), Enhanced Data Rates for GSM Evolution (EDGE), and General Packet Radio Service (GPRS). As previously discussed, mobile botnet refers to a group of compromised smartphones that are remotely controlled by a cybercriminal or a botmaster through some C&C channels [14]. Nevertheless, this trend is changing rapidly with the growing usage and popularity of smartphones, which have become powerful handheld devicesthathaveenhanced computing and processing capabilities alongwith Internet accessibility. In addition to these capabilities, a large amount of sensitive personal data can be stored in smartphones, and these devices are often used in online payment and banking transactions.

Therefore, smartphones have become one of the most attractive targets for malware and botnet creators [23]. As a result, the research community has to study the possible areas where attackers may exploit technological loopholes in the attempt to harvest information from the mobile device.

From the same motivation and the exhaustive survey of botnet attacks, we present a thematic taxonomy as shown in **Fig. 3**, based on architecture, platform, attack types, loopholes, target audience, and operational influence. In addition, we outline the defensive approaches contributed by researchers up to this point. In the following sections, we highlight the existing contributions in the mobile botnet attack vectors as well as open areas for research.

**3.1.1 Architecture:** The widespread implementation of mobile botnets is restricted as compared with legacy, computer-based botnets for the following reasons: (a) limited battery power, (2) resource constraints, (3) limited Internet access, and other constraints. The mobile botnet architecture has similarities with existing botnet architectures. For instance, similarities in the underlying C&C communication protocols exist, which includes Internet Relay Chat, Hypertext Transfer Protocol (HTTP) [18], and Peer-to-Peer (P2P) networks [24]. In addition to these, mechanisms based on Short Messaging System (SMS) [6][25][26], Bluetooth [27], or Multimedia Messaging System (MMS) [28] have also emerged to disseminate and control botnet traffic. **Fig. 4** shows the basic architecture of a mobile botnet, with the basic assumption of a connection of mobile nodes and C&C through an IP network (Internet). Initially, the botmaster creates a malicious application (based on the vulnerabilities of Application Programming Interfaces or APIs) and publishes it through an online application portal (e.g., APP Engine for Android applications). The mobile user downloads the application, which in turn affects the mobile device. The infected application leaks the private information from the victim's device and may cause service disruption.

An SMS-P2P based mobile botnet architecture is proposed by [29], that uses different mobile services and is resilient to detection. The architecture of SMS-P2P is shown in **Fig. 5**. The SMS messages are used to coordinate the devices and the C&C in a P2P topology. The authors proposed countermeasures to defeat an SMS-P2P attack.

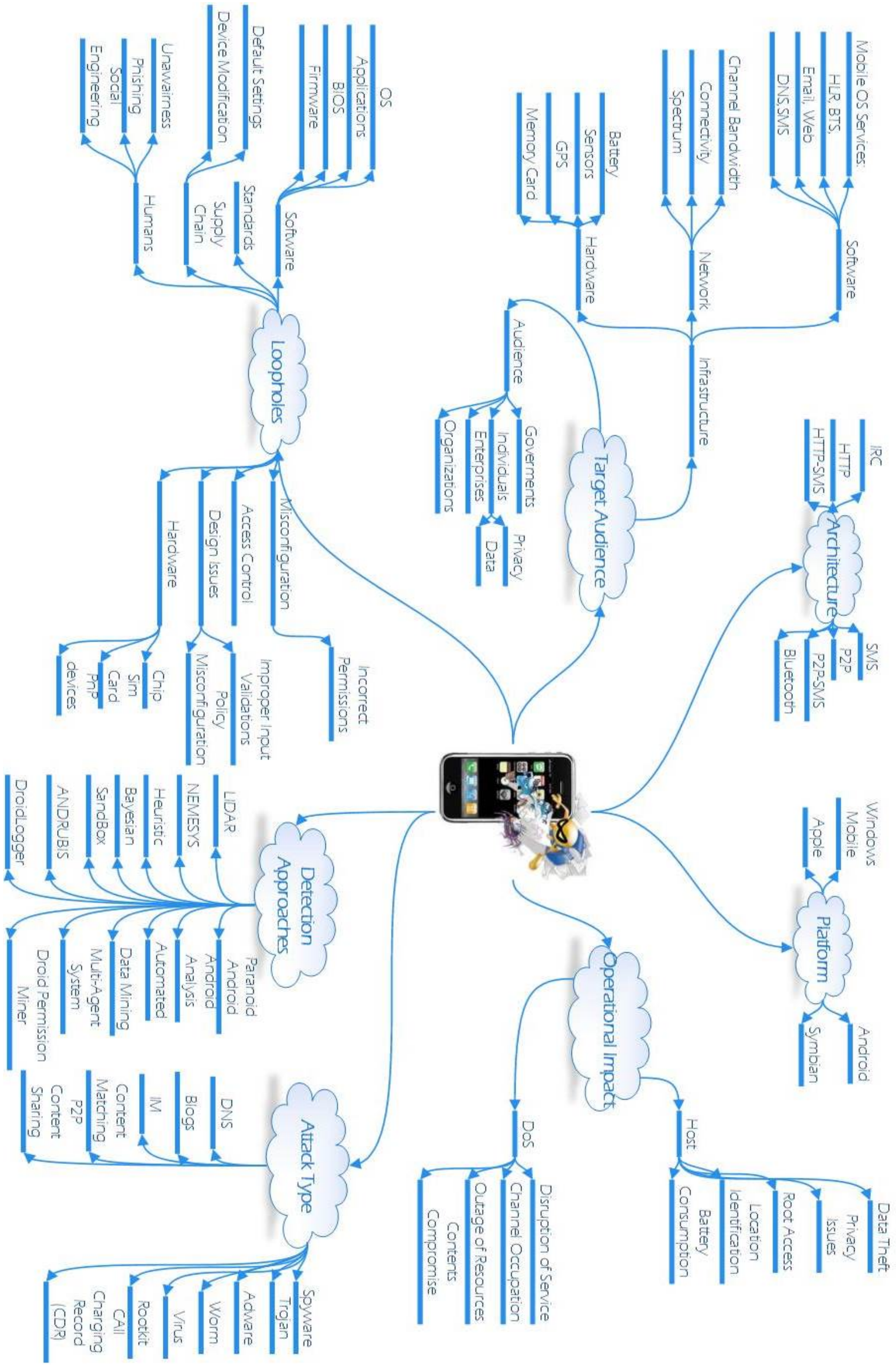

**Fig. 3.** Taxonomy of Mobile Botnets

A C&C architecture based on Bluetooth technology was evaluated in [27], as shown in **Fig. 6** Bluetooth architecture utilizes near-field communication channels. Therefore, underlying botnet architecture cannot reach a wide range. The authors evaluate and investigate the challenges of mobile botnet creation and maintenance via Bluetooth. In addition, the behavior of a mobile botnet is investigated using Bluetooth technology in a large-scale simulated environment. Such a malicious infrastructure was concluded to be possible in various scenarios because of the largely repetitive nature of daily user routines.

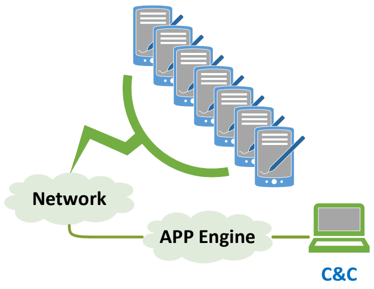

**Fig. 4.** Basic Architecture of Mobile Botnet

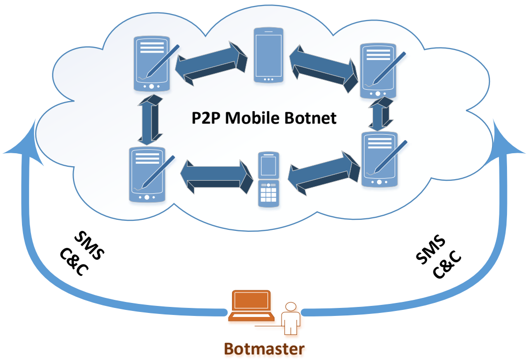

**Fig. 5.** P2P- and SMS-based Mobile Botnet

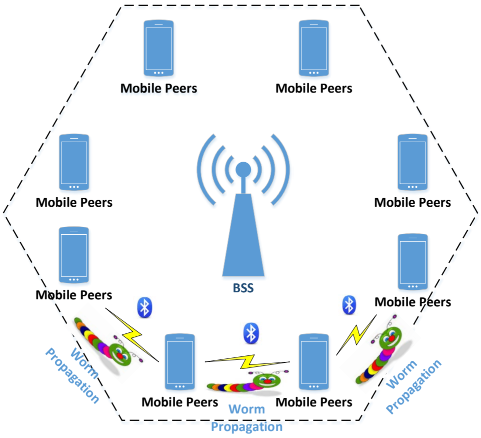

**Fig. 6.** Bluetooth-P2P C&C Architecture

A more recent real-world scenario is presented in [30] to understand Bluetooth-based C&C channel development mechanism.In this study, a Bluetooth C&C channel is deployed in a controlledenvironment using Android OS as a development platform. The strengths and weaknesses of the proposed architecture are then identified. Finally, a physical Bluetooth channel governing C&C isproven to be possible in a controlled environment.

**3.1.2 Platform:**In consideration of the technological advancements in mobile computing, smartphone vendors are introducing OS that offer competitive features with respect to the traditional desktop OS. **Table 4**presents the evaluation of mobile OS platforms from 2000 to 2013, whereas **Fig.7** shows the total infection ratio for each platform.

**Table 4.** Mobile Platform Evolution from 2000 to 2013

| Year | 2000 | 2001 | 2002 | 2005 | 2007 | 2008 |
|---|---|---|---|---|---|---|
| OS | Symbian | Palm OS | Windows CE | Maemo OS | iOS | Android 1.0 |
| Model | Ericsson R380 | Kyocera 6035 | Pocket PC | Tablet N770 | Apple iPhone | HTC Dream |
| OS | | | Black Berry OS | | Open Handheld Alliance (OHA) | |
| Model | | | Black Berry Phone | | Google, HTC, Sony,Intel, Motorola | |

| Year | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|
| OS | Web OS | Windows Phone OS | MeeGo | FireFox OS | Ubuntu Touch |
| Model | Palm Pre | | Nokia N9 | | |
| OS | Bada OS | | | | Black Berry 10 |
| Model | Samsung S8500 | | | | Black Berry |

**Fig.7** depicts that Android is the most affected platform with a 65% infection ratio. The reasons for this high ratio are as follows: Android has a leading market position, third party application stores are easily introduced due tothe open source architecture of the OS, andprograming the malware is easy. After Android, the most affected platforms are Symbian and J2ME with 32% and 2% infection ratios, respectively [31].

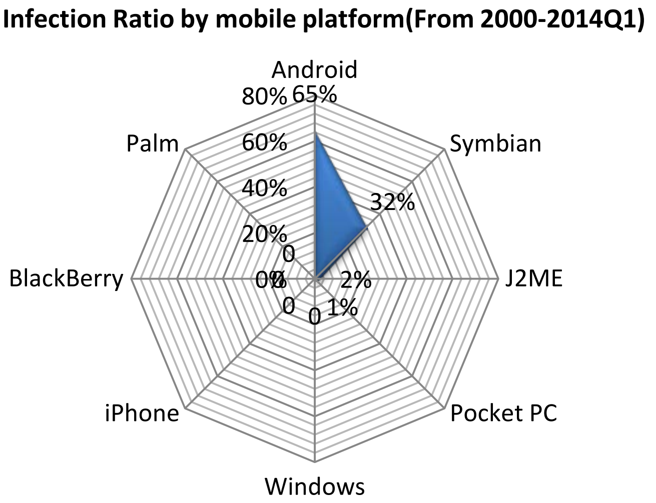

**Fig. 7.** The total infection ratio for each mobile platform from 2000 to 2014 (Q1)

**3.1.3 Loopholes:**Considering the vulnerability of mobile devices to new threats, institutions and consumers keep themselves updated about mobile. In particular, the Android OS is a victim of malware attacks as reported by [32]. Android's increased market share and open-source architecture are factors that enable the exploitation of various attacks. Although new versions of the Android OS are more resistant against security vulnerabilities, 44% of Android users do not update their systems, and hence compromise their mobile security. Having an updated version of a mobile OS is desirable,particularlyfor federal, state, and local authorities, to optimize secure solutionsformobile technologies.

Unified Extended Firmware Interface (UEFI) [33] provides specifications for boot loaders with the capability of launching various OS. According to the Advanced RISC Machine architectures, UEFI boot loaders should be preferably adopted by 64-bit processors. Mark Doran, president of the UEFI Forum, argues that UEFI Secure Boot should be used apart from the Windows platform to enable protection in mobile devices [34]. When platform vendors do not implement Secure Boot properly, they face two major challenges in execution: 1) attackers gain privilege either to modify the code that contains the Secure Boot call, and 2) attackers execute their own code in the system. Vendors face these vulnerabilities, which are not inherent to the Secure Boot itself, because of implementation errors.

Another serious problem faced by software manufactures is the human knowledge in terms of software usage. In general, humans are not aware of the possible consequences caused by the misuse of mobile applications. For this reason, social engineering and phishing tools and techniques are considered as the two most common mechanisms that are effective for capturing personal information of a lame user. Similarly, default settings (default usernames and passwords) of various smartphone device vendors often open a gate for attackers to gain unauthorized access.

Vulnerabilities can sometimes be uncovered by monitoring the communication between a mobile device and the web server to find weaknesses in the protocol or access controls. Many Web services blindly trust input coming from mobile applications, relying on the application to validate the data provided by the end user. However, attackers can forge their own communication to the web server or bypass the application logic checks entirely, allowing them to take advantage of missing validation logic on the server to perform unauthorized actions [35].

Subscriber Information Module (SIM) cards are tiny memory units inside most mobile devices that allow such devices to communicate with the service provider. According to a security research [36], flaws in SIM card technology and implementation make hundreds of millions of mobile devices susceptible to hacking. The root of the problem lies in the fact that encryption in most SIM cards relies on Data Encryption Standard (DES), which is an algorithm created by the US government four decades ago. DES was secure in its day, but that day has long passed. At present, DES is considered to be insecure and is relatively trivial for a skilled hacker or crack.

**3.1.4 Attack Types:**A recent study by Kaspersky [12] reported that the most common attacks targeting the Android platform are SMS Trojans, adware, viruses, spywares, and root exploits. Moreover, mobile botnets are becoming a dangerous threat that target different mobile platforms that can perform malicious tasks at the instructions of the botmaster. Typically, botnets usetheDomain Name System (DNS) to retrieve the IP addresses of the servers; therefore, targeting DNS service is the initial point of attack. This results in the activation of an incredibly robust and stealthy mobile botnet C&C [37]. Moreover, the key feature of mobile communication relates to the exchange of traffic load and its constant observation for billing and accounting. Consequently, mobile botnets have the potential to affect the infected mobile system's call charging detail records (CDR) [1]. Another approach used to reduce malicious activities is known as the rootkit [38], which is a malicious code that is especially designed to hide unwanted/malicious activities and virus propagations in the system. In this case, the C&C of a botnet instructs the bots to carry out a malicious activity, which mayinclude sending spam messages, acquiring authorized control over smartphone devices, and hijacking business activities.

**3.1.5 Target Audience:**Mobile botnets affectadiverse audience ranging fromthegeneralpublic to government institutions, enterprises, and organizations. Profitable organizations such as banks are shifting the majority of their services to the mobile environment (e.g., payment of bills, generating account statements, and funds transfer). Therefore, the primary focus of the mobile botmaster is to gain access to such mobile devices that are dedicated for business activities andtoattemptto launch different malicious activities such as DDoS, remote control, and service disruption. According to Information Week [39], Bank of America, U.S bank, Wells Fargo, and JPMorgan Chase are among those U.S banks that were slowed down by DDoS attacks. Consequently, thousands of customers filed complaints for the banks' websites being down that result in their inability to access their normal banking services (e.g. account checking, savings, bill payments, mortgage accounts, and other similar services through mobile applications).

**3.1.6 Operational Influence:**The overall operational influence of mobile botnets can be viewed from two different perspectives: 1) relevant to the host device itself and, 2) relevant to the service provisioning model. The direct influence related to the host mobile device includes privacy violation, data theft, root access, location identification, and battery consumption. Similarly, the concept related to service provisioning model includes, disruption of services, channel occupation, outage of resources, and content compromise.

**3.1.7 Detection Approaches:**A mobile botnet detection approach based on "pull" style C&C was presented in [40]. Through investigating flow features (total packets and total bytes) of C&C traffic passing through a Virtual Private Network (VPN), the authors investigated the abnormalities of these traffic flows. Likewise, this approach can detect mobile botnets residing within signatures, abnormal models, and whitelists.

A layered intrusion detection system and remediation framework, which automatically detects, analyzes, protects, and removes security threats in smartphones, was proposed by [41]. This study aims to overcome smartphone vulnerabilities and to detect threats in three stages: a) behavioral and threat modeling technique; b) implementation and deployment of stochastic and machine learning techniques to automatically detect intrusion that can span among different network layers, applications, and social media; and c) building an automatic threat detection model to lessen or even overcome the security risks.

A behavioral model was proposed in [42] for the detection of smartphone malware based on ontology techniques. Another approach presented in [1] focused on the design of a method for network-based anomaly detection based on analytical modeling, learning, and simulating, together with the billing and control-plan data to detect mobile attacks and anomalies. Furthermore, authors in [43] created a virtual lab environment for the purpose of analysis and detection of Android malware through emulating the environment. In addition to this method, a signature-based mobile botnet detection algorithm that considered Bayesian spam filter mechanism as the key component was proposed in [44].The authors concluded that this system is capable of identifying 87% of spam message from the dataset.

A prototype called Airmid [32] was designed to automatically identify and respond to malicious mobile applications by analyzing the behavior of the network traffic. Airmididentifies malicious network traffic through the cooperation between smartphones and in-network sensors. To detect Android malware and the malicious application behaviors, a hybrid (static and dynamic) model was proposed in [45], which detects malicious activity through the following stages: a) static analysis – to parse the manifest file of applications and decompile them using reverse engineering tools, and b) dynamic analysis – execute an application and log all performed actions.

An adaptive hybrid multi-agent system for SMS-based mobile botnet detection is proposed in [46]. The approach employs signature-based and anomaly–based analysis systems to detect SMS-based mobile botnets. Detection is achieved by applying behavioral analysis that includes correlating suspicious SMS messages with a generated profile. This system is still in the development phase.

Droid Permission Miner [47] specifies a mechanism for static analysis of the Android platform to detect possible malicious activity by analyzing permissions of the applications. The authors analyzed 436 APK files and extracted specific features that are relevant to malicious activities. The proposed model is then classified based on machine learning classifiers. By contrast, this model can be considered as an initial classifier to measure benign and malware specimens.

Recently, the authors in [48] devise a fully automated and comprehensive analysis system for Android applications. The approach combines static and dynamic malware analysis techniques at both Delvik VM and system level. To the best of our knowledge, this dataset consists of 1,000,000 applications, which is the largest dataset ever analyzed for malware behavior measurement. Another system named DroidLogger [49]identifies suspicious behavior of applications via instrumentation. A lightweight method is proposed to understand the dynamic behavior of an application by logging program APIs and system calls alongwith their detailed arguments.

From various constraints imposed by cellphone technologies (e.g., resources, memory, processing, and storage), a concept of remote server utilization is introduced for the first timein application scanning in [50],which is known as “Paranoid Android”. The authors investigate recording and replaying concepts during application execution. While an application executes, acomplete replica of the system runs in parallel on a remotevirtual machine. Apart fromlocal security measures on the mobile device, the device records a minimal execution trace and sends it to the security server.The server then replays the execution traces to detect any potential malware.

In thefollowingsection, we will review and discuss the most popular mobile botnet attacks evolved to date, with consideration of the following distinctions: type of attack, platform being compromised, category, target audience, vulnerability/loopholes in technology, dissemination method, overall operational influence, and defensive approaches carried out to undermine each mobile botnets.

## 4. Review of Existing Mobile Botnets based on the Proposed Taxonomy

In this section, we review the existing mobile botnet attacks based on the significant derived parameters from the taxonomy. **Table 5** shows the comparative study of these mobile botnets/malwares. In the following subsections, we will briefly describeeach botnet with respect to the attack vectors specified in the previous section.

**4.1 DroidDream:**A mobile botnet-based malwarecalledDroidDream appeared in the spring of 2011. The purpose of launching this attack was to gain root access to Android mobile devices and acquire unique identification information (model number, product ID, EMI number, provider, language, etc.) of a mobile phone. Moreover, after infection, the compromised device could also download and install additional executable programs and features without being noticed by the user, while providing a backdoor root access for attacker. The DroidDream's major focus was to infect mobile devices running Android v2.2 and earlier versions. More than 50 malware-infected applications were identified; however, what was alarming is that such applications were available on the official Android market place. Afterwards, Google managed to remove the effected applications from its official marketplace and had implemented a "kill switch" mechanism to remotely clear Android handheld devices that have been malfunctioned bytheDroidDream malware.

**4.2 SymbOS.Yxes:** This worm targets Symbian mobile devices with OS 9.1S60 3rd Edition, but can also run on a wider range of Symbian OS. The potential capabilities of this worm are the following: (a) sending messages to those phone numbers that were harvested from infected devices' SMS inbox, (b) stealing information from the victim's device (e.g., serial number of phone and subscription information) and redirecting this information to servers controlled by cybercriminals, and (c) searching for installed applications from the application manager and attempting to kill those tasks or applications. This worm uses a valid but revoked certificate; therefore, it is required for a device to avoid this attack through enforcing online verification of the certificate. Moreover, FortiGate Systems and FortiClient Systems can also be used to avoid or even eliminate this attack.

**4.3 IKee.B:**This malware is a standalone malicious program that infects iPhone in different ways, such as the following: (a) the device is "jailbroken" and installed with a software that is not signed by Apple, (b) installation of unsigned secured shell (SSH) with remote access enabled capability,and(c) default root password("alpine") has not been changed from the default factory setting. Similarly, this worm can infect other vulnerable iPhones by scanning over 3g or Wi-Fi networks. Moreover, its dispersion takes place in three stages when active on the iPhone: (a) changes default password, (b) establishes connection with remote server with address 92.61.38.16 via HTTP and downloads and installs additional components, and (c) send banking information incorporated in SMS messages to a remote server. The only defensive reaction is to reset the iPhone and to restore all settings to their factory defaults.

**4.4 Geinimi:**Anotherthreatening Trojan that infects Android devices with the aim to steal information appeared in the middle of 2011. Users unknowingly install applications that are repackaged versions of legitimate applications, which can be downloaded from third-party application stores. When the application is launched, the Trojan starts in the background. Meanwhile, the Trojan collects the user's private information, such as location identification, list of installed applications, and IMEI and SIM identifiers of the particular phone. Afterward, Geinimi attempts to connect to a remote server to transmit collected data as a payload for the remote server. The Geinimi Trojan can be avoided by resetting the registry information of the phone. To hide its functionality, the Trojan canemploy two anti-analysis functions called encryption and obfuscation.

**4.5 RootSmart:**Inthe same year, another Android malware GingerMaster [51] exploitation is further strengthened bytheRootSmart [52] malware. Unlike GingerMaster, it does not directly embed a root exploitation code into the application; it rather fetches the GingerMaster root exploitation logic from a remote server and executes it to gain root access into device. After gaining root access to device, this malwaredownloads and installs other malware applications without being noticed by the user. The motivation is to steal private information and send ittoaremotely managed C&C. In addition to this operation, stealth is provided by encrypting the C&C server URL inside a raw resource file.

**4.6SMiShing:** In the middle of 2012, SMS phishing evolved as a means to target lame mobile users. In computing terminology, phishing is a form of criminal actthat acquirespersonal information by exploiting the ignorance of a user. The attacker must first establish trust with the victim by masquerading as a trustworthy entity in a mobile communication system. The only meansto combat such a malicious act is to educate users on how to reduce the likelihood of becoming a victim.

**4.7Android Snooping:** Android snooping vulnerability is discovered in the Android platform version 2.3.4, particularly in Google's ClientLogin protocol such as Google Calendar provider and contacts sync service. Not only did this problem affect the standard Android applications, but it also affected those that used Google services throughtheClientLogin protocol via HTTP. The vulnerability was diagnosed from the disclosure to steal personal data from the Calendar Control object. Apart from information theft of personal interest, the adversary could perform substantial changes to the user's profile data without being noticed by the user. For example, the adversary can change the victim's personal phone book data (e.g., changing the email address of his/her boss), hoping to capture sensitive and confidential data related to some business activity. To counter this attack, one must (a) limit the time of AuthToken and (b) enforce secure HTTP (HTTPS) for authentication. Google has fixed the problem in its subsequent Android releases.

**4.8 BBproxy:**A Trojan malware was detected in Blackberry smart phones in the middle of 2006.It targeted the enterprise data and network. Initially, it creates a trusting relationship between a Blackberry device and a company's internal server. Once the connection is established, it hijacks and establishes a connection with the company's internal server. In addition to this intrusion, the data tunnel established between both entities is based on a secure tunnel. Therefore, detecting any malicious activity by an intrusion detection system, which is installed on the perimeter of the network, is difficult. Moreover, the Trojan is bundled with the most popular games and can also disseminate through email. Once installed, it tries to acquire and steal a company's personal informationwhile scanning for more vulnerability. The recommendations to avoid this malicious act are the following: (a) the Blackberry server should be kept in a demilitarized zone (DMZ), and (b) the communication betweentheBlackberry server and the device should be restricted.

**4.9 SSL Renegotiation DoS:** A generic OS was discovered during 2011, which lies in the category of DoS attack based on asymmetric processing. This OS can target secure socket layer/ transport layer security (SSL/TLS) servers, because the basic TLS operations increase the load on the processing of the server rather than on the client side. The attacker attempts to exhaust the server resources by initiating large numbers of TLS renegotiation requests. The following precautions can be made to avoid the above-stated problem: (a) disable SSL/TLS renegotiation, (b) impose a time limit between both incoming and renegotiation SSL/TLS requests, and (c) offload processing by applying SSL accelerator.

**4.10 Obad.**Until now, Obad malware [63] has a sophisticated design that exploits several unexplored vulnerabilities. Furthermore, it uses SMS, fake Google Play stores, and untrustworthy third party Android application portals as a means of initiating the attack. The Obad.a malware is distributed along with another Trojan called SMS.AndroidOS.Opfake.a to capitalize the infection ratio.

**Table 5.** Review of Existing Mobile Botnets based on Taxonomy

| Mobile Botnet | Type | Platform | Category | Target Audience | Loophole | Dissemination Technique | Operational Impact | Defensive Reaction |
|---|---|---|---|---|---|---|---|---|
| DroidDream[53] | Root Exploitation | Android | Trojan | Android users | Alter code for Root access | Games | Root access, steal data | Android App Kill switch |
| SymbOS. Yxes[x2] | Service disruption | Symbian OS 9.1 | Worm | Symbian Users | Invalid certificate registration | Sending SMS, Redirect to cybercriminal website | Abnormally high phone bills, battery power loss | FortiGate Systems, FortiClient Systems |
| IKee.B[54] | Root Access | Apple | Worm | Systems and Networks, iPhone users | Unapproved SSH, setting default SSH password | scan and infect other iPhones by Wi-Fi or 3G Networks | Stole financial sensitive information | Restore firmware via Apple iTunes |
| Geinimi[55] | Personal Information Theft | Android | Trojan | Android Users | Exploit backdoor | Games | Send private information to C&C via HTTP | Symantec Power Eraser Tool (SPE) |
| RootSMART[52] | Root Exploitation | Android | Malware | Android <2.3 or 3.0 | GingerBreak Root Exploit | Through two Helper-Scripts | Establish connection with C&C | Use reputable app store |
| SMiShing[56] | Spam, Fraud | Any | Phishing | Any | Phishing to humans | Monetized by signing up | Steal personal information | Educate People |
| Snooping [57] | Privacy/ Snooping | Android <2.3.4 and 3.0 | Software Fault | Users using synchronization services | Misusing Google's ClientLogin Protocol | Attacker snoops AuthToken in clear text | Impersonate user to change his personal info | Minimize timeout of AuthToken |
| SpySmart Phone [58] | Spy Software | Any | Sensors | Any | Phishing to humans | Installation on victim machine | Steal personal information, | Educate People |
| SSL Renegotiation DoS[59] | DoS, Asymmetric Processing | Any | Generic Attack | SSL/TSL servers | TSL Operations | Massive TLS renegotiation requests | Deplete Server resources | Disable SSL/TSL renegotiation |
| BBproxy[60] | Infrastructure | Blackberry/ RIM | Trojan | Enterprise Internal data and network | Exploit the trust relationship | Games, Email | Steal companies' Information | Separate DMZ, limited access |
| Foncy[12] | SMS Trojan | Android | Trojan | Any | Sending random messages to victims | Working with IRC bot and a root exploit | Malicious activates initiated by C&C | Already Dead |
| Cawitt[12] | SMS Trojan | Android | Trojan | Twitter Users | Posting Message on Twitter | Unknowingly sending SMS to premium users | Information Threat | Antivirus Scanner |
| SpamSold[61] | SMS Spam | Android | Spam | Any | Deceptive Android Permissions | Fee games | Establish connection with C&C | Various Antivirus Software |
| Obad[62] | Admi Explotation | Android <v4.3 | Trojan | Android cell holders | Google Play fake stores | Spam text messages | Attain admin rights to hack a firm | Patch in v4.3 |

In the first step, Obad.a sends a message (“MMS Message has been delivered, download from www.otkroi.com”) to the user device through Google’s GCM (Google Cloud Messaging) service. When a user clicks on the link in the message, a file called “mms.apk” that contains “Opfake.a” is loaded in the active memory of the mobile device. If a user proceeds to install the program, then the C&C is activated, and the Trojan sends a message to the victim’s contact list. this encourages the receivers to download an MMS message from the URL http://oktroi.net/12. By following the link, the recipients are also infected by Obad.a. Similarly, the Obad botnet is capable of providing high levels of code obfuscation for stealth and hiding malicious routines from known anti-virus software programs. Furthermore, Obad.a can spread its malicious files, such as opfake.a and obad.a, very quickly. Despite of its sophisticated technique to hide and propagate, the threat has been recognized by Google, and the company has disabled the security holes related to Obad.a found in Android 4.3.

## 5. Issues and Challenges

As a result of the exhaustive survey on the existing botnets, we identify open issues for the progressive security of mobile devices against botnets. With the proliferation of mobile cloud computing [64] platforms, the following issues with respect to mobile botnets are of concern for the academia and industry alike:

- Initially, the manifestation of a cross-functional group is essential.Itinvolves researchers and the stakeholders (e.g. enterprises, governments, networks, and ISPs) for identification and effective confiscation of botnets. A clear and transparent policy on mobile equipment and usagemust be documented and socialized across the enterprise. Moreover, the public should be informed of the means by which mobile botnet threats can be overcome.
- At this point, security and risk leaders cannot ignore the increasing demand and proliferation of mobile devicesinenterprises. Not only is the demand driven by the mass adoption and use of consumer devices, but businesses also leverage on the power of mobile computing to strengthen their value to their clients and customers, making them more agile, relevant, and able to respond to the needs of their customers.
- Scanning and blocking of malicious code in the cloud can be implemented to preempt the code or information sharing centers in cooperation with antivirus vendors in identifying and planningto block threats. When the malicious code is preempted, it may not be possible for providers to predict the way that devices with more operating platforms receiving the code behave with traffic. However, in case of detection and block management of threats, it can be applied in blocking solutions.
- As compared to desktop OS, smartphone device OS has less capabilities in terms of processing, memory and storage, which ultimately restricts the best security policies to be implemented.
- Network operators have remarkable control on the software employed by smartphones that use their network. In particular, this happens when mobile phones are sold as part of a wireless subscription. The operators should provide built-in anti-virus scanning facilities and should enforce updating and patching in response to any malicious activity.
- User awareness with respect to security threats is a key contribution toward a persistent solution of the problem. Therefore, a specific and dedicated education and awareness campaign that targets mobile users on the risks, policies, and procedures should be introduced.

## 6. Conclusion

Smartphones have become similar to desktop computers nowadays because of the rapid development of computational and storage capabilities of such devices. Mobile devices are usually connected to the Internet all the time because of its always-on facility. Consequently, new security threats are becoming the interest for malware writers. Similarly, this interest opens the door for botnet creators to mold their intentions to this new technological arena. Moreover, through the emergence of mobile devices in general-purpose computing and communication platforms, new security vulnerabilities have evolved. Therefore, users have to be aware about the vulnerability of mobile devices to malware infection, and can thus be turned into a botclient as part of a botnet.

In this review, we have conducted an exhaustive survey of existing botnet attacks on mobile devices. Through an investigation of botnet attack vectors, we have presented a well-defined taxonomy which we used to explore the acute features of existing botnet attacks. This review serves as a roadmap for researchers to study and enforce secure communication patterns that are focused on various aspects of mobile botnet attack vectors.

Related to our observations about mobile botnet attacks, Android is concluded to have the least resistance against mobile botnets for the following reasons. First, Android is open-source, making it free to contribute in a digital contribution platform. Second, Android has an augmented market penetration makes it suitable for the spread of botnets.

Addressing mobile botnet attacks have become a challenge for information security professionals and researchers. Therefore, stakeholders must implement cooperative and legislative actions to eliminate this hazard. Furthermore, negotiating possible international legislative issues and establishing global policies are important to systematically avoid suchharmful threats.

## References

[1] Abdelrahman, O.H., E. Gelenbe, G. Görbil, and B. Oklander, “Mobile Network Anomaly Detection and Mitigation: The NEMESYS Approach,”*Information Sciences and Systems 2013 Lecture Notes in Electrical Engineering*, vol. 264, pp.429-438, 2013. Article (CrossRef Link)

[2] Arbor Networks: Worldwide Infrastructure Security Report (2012), https://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/4737-the-arbor-networks-8th-annual-worldwide-infrastructure-security-report-finds-ddos-has-become-part-of-advanced-threat-landscape

[3] Ollmann, G., “The evolution of commercial malware development kits and colour-by-numbers custom malware,”*Computer Fraud & Security*, vol. 9, pp. 4-7, 2008.Article (CrossRef Link)

[4] Flo, A. and A. Josang, “Consequences of botnets spreading to mobile devices,” in *Short-Paper Proc. of ofthe 14th Nordic Conference on Secure IT Systems*, 2009.

[5] KARIM, A., R.B. SALLEH, M. SHIRAZ, S.A.A. SHAH, I. AWAN, and N.B. ANUAR, “Botnet detection techniques:review, future trends and issues,”*Journal of Zhejiang University SCIENCE C*, 2014.Article (CrossRef Link)

[6] Geng, G., G. Xu, M. Zhang, Y. Yang, and G. Yang., “An improved sms based heterogeneous mobile botnet model,”in *Proc. ofInformation and Automation (ICIA), 2011 IEEE International Conference*, 2011.

[7] VentureBeat,“News about Tech, money and innovation / Mobile,” http://venturebeat.com/2013/10/31/android-captures-record-81-global-market-share-windows-phone-is-fastest-growing/

[8] Smartphone Vendor Market Share, http://www.idc.com/prodserv/smartphone-market-share.jsp, 2014 [Accessed on : 20-06-2014]

[9] Zeus Botnet Eurograbber Steals $47 Million, http://www.informationweek.com/security/attacks/zeus-botnet-eurograbber-steals-47-millio/240143837

[10] Android DreamDroid two: rise of laced apps, http://www.itnews.com.au/News/259147,android-dreamdroid-two-rise-of-lacedapps.aspx/

[11] F-Secure, F- secure| Virus and threat descriptions, http://www.f-secure.com/v-descs/worm_iphoneos_ikee_b.shtml

[12] Maslennikov, D., SecureList: Mobile Malware Analysis: Part-6, http://www.securelist.com/en/analysis?calendar=2013-02

[13] Karim, A., S.A.A. Shah, and R. Salleh, "Mobile Botnet Attacks: A Thematic Taxonomy,"*New Perspectives in Information Systems and Technologies*, vol. 2, pp. 153-164, 2014. Article (CrossRef Link)

[14] Xiang, C., F. Binxing, Y. Lihua, L. Xiaoyi, and Z. Tianning,"Andbot: towards advanced mobile botnets," in *Proc. of the 4th USENIX conference on Large-scale exploits and emergent threats*, 2011.

[15] Qi, H., M. Shiraz, A. Gani, M. Whaiduzzaman, and S. Khan, "Sierpinski triangle based data centerarchitecture in cloud computing,"*The Journal of Supercomputing*, pp. 1-21, 2014. Article (CrossRef Link)

[16] Zhao, S., P.P. Lee, J. Lui, X. Guan, X. Ma, and J. Tao,"Cloud-based push-styled mobile botnets: a case study of exploiting the cloud to device messaging service," in *Proc. of the 28th Annual Computer Security, Applications Conference,ACM*, 2012. Article (CrossRef Link)

[17] Szongott, C., B. Henne, and M. Smith.,"Evaluating the threat of epidemic mobile malware," in *Proc. of Wireless andMobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on*, 2012. Article (CrossRef Link)

[18] Paganinip, HTTP-Botnets: The Dark Side of an Standard Protocol!, http://securityaffairs.co/wordpress/13747/cyber-crime/http-botnets-the-dark-side-of-an-standard-protocol.html

[19] La Polla, M., F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 1, pp. 446-471. Article (CrossRef Link)

[20] Pieterse, H. and M. Olivier, "Design of a hybrid command and control mobile botnet," in *Proc. of Academic Conferences and Publishing International Ltd*,2013. Article (CrossRef Link)

[21] Kasera, S. and N. Narang, "3G mobile networks: architecture, protocols and procedures based on 3GPP specifications for UMTS WCDMA networks,"*McGraw-Hill Professional*,2005.

[22] Mishra, A.R., "Advanced cellular network planning and optimisation: 2G/2.5 G/3G... evolution to 4G," *John Wiley & Sons*, 2007.

[23] Gani, A., G.M. Nayeem, M Shiraz, M. Sookhak, M. Whaiduzzaman, and S. Khan, "A review on interworking and mobility Techniques for seamless connectivity In Mobile Cloud Computing,"*Journal of Network and Computer Applications*, pp. 84-102,2014. Article (CrossRef Link)

[24] Grizzard, J.B., V. Sharma, C. Nunnery, B.B. Kang, and D. Dagon,"Peer-to-peer botnets: Overview and case study,"in *Proc. of the first conference on First Workshop on Hot Topics in Understanding Botnets*, 2007.Article (CrossRef Link)

[25] Hamandi, K., I.H. Elhajj, A. Chehab, and A. Kayssi, "Android SMS botnet: a new perspective," in *Proc. of the 10th ACM international symposium on Mobility management and wireless access*, 2012.Article (CrossRef Link)

[26] Geng, G., G. Xu, M. Zhang, Y. Guo, G. Yang, and C. Wei, "The Design of SMS Based Heterogeneous Mobile Botnet," *Journal of Computers*, vol. 7, no.1, pp. 235-243, 2012. Article (CrossRef Link)

[27] Singh, K., S. Sangal, N. Jain, P. Traynor, and W. Lee, "Evaluating bluetooth as a medium for botnet command and control," in *Proc. of Detection of Intrusions and Malware, and Vulnerability Assessment*,pp. 61-80, 2010. Article (CrossRef Link)

[28] Adeel, M., L. Tokarchuk, and M. Awais Azam,"Classification of Mobile P2P Malware Based

on Propagation Behaviour," in *Proc. of The Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, 2010.Article (CrossRef Link)

[29] Zeng, Y., K.G. Shin, and X. Hu,"Design of SMS commanded-and-controlled and P2P-structured mobile botnets,"in *Proc. of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, 2012.Article (CrossRef Link)

[30] Pieterse, H. and M.S. Olivier, "Bluetooth Command and Control Channel," *Computers & Security*, 2014.Article (CrossRef Link)

[31] Protalinski, E., "F-Secure: Android accounted for 97% of all mobile malware in 2013, but only 0.1% of those were on Google Play", 2013.

[32] Nadji, Y., J. Giffin, and P. Traynor.,"Automated remote repair for mobile malware," in *Proc. of the 27th Annual Computer Security Applications Conference*, 2011.Article (CrossRef Link)

[33] Unified Extensible Firmware Interface, http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

[34] UEFI Technology Expands in Mobile Devices and Other Non-PC Market Segments, http://www.uefi.org/sites/default/files/press_releases/UEFI_Specifications_Expand_in_Mobile_Devices_and_Non-PC_Markets_May_8_2013.pdf

[35] Mobile Security Primer, https://viaforensics.com/resources/reports/best-practices-ios-android-secure-mobile-development/mobile-security-primer/

[36] Forbes, Secure mobile development best practices, https://viaforensics.com/resources/reports/best-practices-ios-android-secure-mobile-development/mobile-security-primer/

[37] Open DNS, security whitepaper, http://info.opendns.com/rs/opendns/images/OpenDNS_SecurityWhitepaper-DNSRoleInBotnets.pdf

[38] Rootkit, http://en.wikipedia.org/wiki/Rootkit

[39] Bank Site Attacks Trigger Ongoing Outages, Customer Anger, http://www.informationweek.com/attacks/bank-site-attacks-trigger-ongoing-outages-customer-anger/d/d-id/1106615?

[40] Choi, B., S.-K. Choi, and K. Cho, "Detection of Mobile Botnet Using VPN," in*Proc. of Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on*, 2013.Article (CrossRef Link)

[41] Roshandel, R., P. Arabshahi, and R. Poovendran, "LIDAR: a layered intrusion detection and remediationframework for smartphones," in *Proc. of the 4th international ACM Sigsoft symposium on Architecting critical systems*, 2013.Article (CrossRef Link)

[42] Chiang, H.-S. and W.-J. Tsaur, "Identifying Smartphone Malware Using Data Mining Technology," in *Proc of Computer Communications and Networks (ICCCN), 20th International Conference on*, 2011. Article (CrossRef Link)

[43] Andrews, B., T. Oh, and W. Stackpole,"Android Malware Analysis Platform," in *Proc. of 8th Annual Symposium on Information Assurance (ASIA'13)*, 2013. Article (CrossRef Link)

[44] Vural, I. and H. Venter, "Combating Spamming Mobile Botnets through Bayesian Spam Filtering,"

[45] Spreitzenbarth, M., F. Freiling, F. Echtler, T. Schreck, and J. Hoffmann,"Mobile-sandbox: having a deeper look into android applications,"in *Proc. of the 28th Annual ACM Symposium on Applied Computing*, 2013. Article (CrossRef Link)

[46] Alzahrani, A.J. and A.A. Ghorbani,"SMS mobile botnet detection using a multi-agent system: research in progress," in *Proc. of the 1st International Workshop on Agents and CyberSecurity*, 2014. Article (CrossRef Link)

[47] Aswini, A. and P. Vinod,"Droid permission miner: Mining prominent permissions for Android malware analysis," in *Proc. of Applications of Digital Information and Web Technologies (ICADIWT), 2014 Fifth International Conference on the*, 2014. Article (CrossRef Link)

[48] Weichselbaum, L., M. Neugschwandtner, M. Lindorfer, Y. Fratantonio, V. van der Veen, and C. Platzer, "Andrubis: Android Malware Under The Magnifying Glass,"*Vienna University of*

*Technology, Tech. Rep*,2014. Article (CrossRef Link)

[49] Dai, S., T. Wei, and W. Zou.,“DroidLogger: Reveal suspicious behavior of Android applications via instrumentation,” in *Proc. of Computing and Convergence Technology (ICCCT), 2012 7th International Conference on*, 2012.

[50] Portokalidis, G., P. Homburg, K. Anagnostakis, and H. Bos,“Paranoid Android: versatile protection forsmartphones,”in *Proc. of the 26th Annual Computer Security Applications Conference*, 2010. Article (CrossRef Link)

[51] X. Jiang, “GingerMaster: First Android Malware Utilizing a Root Exploit on Android 2.3 (Gingerbread)”, 2011.

[52] Xuxian, J., “Security Alert: New RootSmart Android Malware Utilizes the GingerBreak Root Exploit,” 2012.

[53] DroidDream, DroidDream, http://www.webopedia.com/TERM/D/droiddream.html

[54] Worm:iPhoneOS/Ikee.B, http://www.f-secure.com/v-descs/worm_iphoneos_ikee_b.shtml

[55] Android.Geinimi, http://www.symantec.com/security_response/writeup.jsp?docid=2011-010111-5403-99

[56] Musthaler, L., “How to avoid becoming a victim of SMiShing (SMS phishing)”

[57] Mills, E., Report: Android phones vulnerable to snooping attack, http://news.cnet.com/8301-27080_3-20063646-245.html

[58] Kiley, S., “Spy Smartphone Software Tracks Every Move,”

[59] Orchilles, J.A., "SSL Renegotiation DOS, 2011, http://permalink.gmane.org/gmane.ietf.tls/8335

[60] Zetter, K., BlackBerry a Juicy Hacker Target, 2006, http://www.wired.com/science/discoveries/news/2006/08/71548

[61] Microsoft, Microsoft, Malware Protection Center, Trojan:AndroidOS/SpamSold.A, http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan%3AAndroidOS%2FSpamSold.A#tab=2

[62] Donovan, F., “Botnet of mobile devices used for first time to distribute Trojan,” 2013.

[63] Unuchek, R., Obad.a Trojan Now Being Distributed via Mobile Botnets, http://securelist.com/blog/mobile/57453/obad-a-trojan-now-being-distributed-via-mobile-botnets/

[64] Shiraz, M., A. Gani, R.W. Ahmad, S.A.A. Shah, A. Karim, and Z.A. Rahman, “A Lightweight DistributedFramework for Computational Offloading in Mobile Cloud Computing,”*PloS one*, vol.9, vo.8,2014. Article (CrossRef Link)

**Ahmad Karim** has distinctively received his MIT (Masters of Information Technology) and MS (CS) degrees from Bahauddin Zakariya University Multan, Pakistan. He has also achieved Cisco International Certifications (CCNA, CCNP, CCAI). He is currently pursuing his PhD from University of Malaya, Malaysia. His area of research includes Botnet Detection, Mobile Cloud Computing, Computer Networks and Mobile Computing.

**Syed Adeel Ali Shah**received his M.Sc. in computer & information networks from the University of Essex, United Kindom. Currently, he is a research scholar working towards his PhD degree in computer science at the Mobile Ad hoc networking group, University of Malaya, Malaysia. His PhD is funded by the Higher Education Commission (HEC) Pakistan under the approved project of Jalozai campus for UET Peshawar. His research interests include data dissemination aspects in vehicular networks, in particular, adaptive control mechanisms for awareness and congestion management and security aspects in ad hoc broadcast communications.

**Rosli Bin Salleh**is an Associate Professor and Deputy Dean of Research in Faculty of Computer Science and Information Technology, University of Malaya, Malaysia. He has obtained his bachelor degree from University of Malaya, Malaysia and later Masters and PhD degree from Salford University, UK. He has a good profile of publications in renowned Journals and Proceedings. He is actively supervising students at Master and PhD level. His interests of research include Mobile IPv6, Wireless Handoff and Botnet Phenomenon. He is also an associate member of Cisco Systems, Inc. 2008-2016. He has been serving for different administrative duties since 2002 in University of Malaya.

**Muhammad Arif**is a PhD student at Faculty of CS and IT, University of Malaya. He joined UM as a Bright Spark Scholar in September 2013. Before this he has completed masters (MS) and bachelor (BS) degrees fromCOMSATS Institute of Information Technology, Pakistanand University of Sargodha Pakistan respectively. His research interests include image processing, E-Learning, Artificial intelligence, Networking, and data mining.

**Rafidah Md Noor**received her BIT from University Utara Malaysia in 1998, and MSc in Computer Science from University Technology Malaysia in 2000, and PhD in Computing from Lancaster University, United Kingdom in 2010. She is currently a Deputy Dean of Undergraduates and Quality Manager at the Faculty of Computer Science and Information Technology, University of Malaya. She has more than 20 Master Degree and PhD students supervised since 2004. She also serve as technical reviewer and track chair for International conferences and journals. Her research interests include network mobility, vehicular networks, mobile IP, Quality of Service and Quality of Experience.

**Shahaboddin Shamshirband**is a research fellow at the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia.His academic qualifications were obtained from the Islamic Azad University, Sari and Mashhad for bachelor and master degrees, and the University of Malaya (2014), Malaysia for PhD. His interest of research includes game theory, reinforcement learning, and wireless-related networks. He is an editorial board and act as a reviewer for various top journals with ISI indexed. He is a member of IEEE.