# Mobile Botnet Attacks: A Thematic Taxonomy

Ahmad Karim*, Syed Adeel Ali Shah, and Rosli Salleh

Department of Computer Science and Information Technology,
University of Malaya, Malaysia
ahmadkarim@siswa.um.edu.my

**Abstract.** Mobile botnets have recently evolved owing to the rapid growth of smartphone technologies. The implications of botnets have inspired attention from the academia and industry alike, which includes vendors, investors, hackers and researcher community. Above all, the capability of botnets is exploited in a wide range of criminal activities, such as, Distributed Denial of Service (DDoS) attacks, stealing business information, remote access, online/click fraud, phishing, malware distribution, spam emails, and building mobile devices for illegitimate exchange of information/materials. In this paper, we investigate mobile botnet attacks by exploring attack vectors and a subsequent presentation of a well-defined thematic taxonomy. Through identification of significant parameters from the taxonomy, we conduct a comparison to explore effects of existing mobile botnets on commercial as well as open source mobile operating system platforms. The parameters for comparison include mobile botnet architecture, platform, target audience, vulnerabilities/loopholes, operational impact and detection approaches. Related to our findings, we present open research challenges in this domain.

**Keywords:** Mobile botnet, smartphone, attacks, malware.

## 1 Introduction

Mobile attacks are the most critical and emerging threats due to increasing market penetration of smartphones and handheld devices. These smartphones use full-featured operating systems incorporated with powerful hardware that supports manifold interfaces and sensors. At present, personal computers (PCs) have declined as a standout choice of computing. Recent statistics show that global shipments of mobile devices immensely exceeded as compared to personal computers (PCs) since 2011 [4]. Furthermore, in the near future, the wide-scale deployment of 4G technologies e.g LTE and WiMAX will become the major source of broadband Internet access for general public. During 2012-2013, 4G enabled devices represent only 0.9 percent of all global mobile connections and they acquired for 14 percent of mobile data traffic [6]. This technological shift has inspired cyber criminals to exploit the vulnerabilities of smartphone devices through off-the-shelf malware creation tools

* Corresponding author.

Á. Rocha et al. (eds.), *New Perspectives in Information Systems and Technologies, Volume 2*,
Advances in Intelligent Systems and Computing 276,
DOI: 10.1007/978-3-319-05948-8_15, 

[8]. Similarly, the burst of mobile applications have enabled the dissemination of malicious code to potentially wide range of audience. The majority of current mobile threats replicate the behavior of attacks on desktop machines through the Internet. Therefore, many of the existing solutions can be considered applicable to the malicious mobile attacks as well. In spite of that, mobile devices have their own constraints such as limited processing, less data storage capabilities and heterogeneity of operating systems (OS) (Android, Apple, Windows etc.), that restricts the security solutions to be programmed efficiently.

Botnet is a network of compromised machines, aiming to collectively perform some activity on the recommendation of botnet creator (bootmaster). The intentions of botmaster are to disrupt legitimate services over the Internet or deceive the private information. In the similar context, with the rapidly growing mobile computing world, mobile botnets are evolving as a serious threat towards targeting mobile phone devices such as smartphones. The motive of this attack is somewhat similar to that of traditional botnet attacks --- to gain access to the resources, interpret contents of mobile user device and transfer control to the botnet initiator. This only comes true when the hacker takes advantage of the exploited area/loopholes of mobile devices to gain unauthorized access to the compromised mobile devices. Eventually, the hacker's goal is to perform malicious and unauthorized activities including illegal phone calls, accessing control panel, sending emails, initialization of worm code and unauthorized file access or photos [12].

Andbot [12] is a mobile bot which employs URL flux and it is considered as a stealthy, low-cost, and resilient bot, which uses botmaster for illegal activities in mobile environment. This botnet uses microblogs to send malicious commands. It is found that Andbot can be easily 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 mobile environment that uses push-based notification services to disseminate the commands.

Recently, a number of mobile botnets have evolved that can degrade the performance of mobile device. For instance, ZeuS [17] is a botnet that focuses the Blackberry, Symbian and Windows platform users and DreamDroid [19] botnet affects the Android based devices. Similarly, IKee.B [21] is a botnet that is used to scan IP address for iPhones, whereas BMaster and TigerBot specifically target Android application frameworks. Similarly, Epidemic mobile malware is a new terrifying threat for mobile users [22] which disseminates rapidly in smartphones. The malware affects the older version of iOS, however still, epidemic mobile malware is a predominant threat for mobile users. Mobile botnets is a relatively new research domain which constitutes a number of problems. Consequently, the detection, analysis and mitigation have become hot issues nowadays for the industry and research.

To the best of our knowledge, in the existing literature, a comprehensive survey on mobile botnet attacks does not exist. This is the first comprehensive review on mobile botnet attacks exploiting mobile botnet architecture, platform, target audience, vulnerabilities/loopholes, operational impact and detection approaches. Therefore, the

contribution of this review is three fold: (a) from the extensive literature survey we conclude that, in order to comprehend mobile botnet's threatening effect, a comprehensive understanding of the features of malicious mobile attacks is essential, i.e. Type of attack, platform, category, target audience, loopholes, dissemination techniques, operational impact and defensive approaches. Therefore we timeline the mobile botnet/malwares according to the above mentioned properties, (b) we propose thematic taxonomy of state-of-the-art mobile botnet attacks to highlight different aspect of attacks as well as recovery techniques to avoid this growing threating phenomenon(c) further, 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; a thematic taxonomy is presented in section 2 to classify the mobile botnet attack vector; in section 3, we compare the existing mobile botnet attacks based on the significant parameters derived from the taxonomy. Finally, section 4 highlights issues and challenges that require further research in avoiding mobile botnet attacks.

## 2 Thematic Taxonomy Based on Mobile Botnet Attack Vector

In this section, we present a thematic taxonomy of mobile botnets based on the mobile botnet attack vector as shown in Figure 1.

### 2.1 Thematic Taxonomy

In Figure 1, based on the exhaustive survey of botnet attacks, we present a thematic taxonomy on the basis of architecture, platform, attack types, loopholes, target audience, operational impact, and defensive approaches. In the following section, we briefly highlight the existing contributions in mobile botnet attack vector, as well as open areas for research.

**Architecture:** PC based botnet are considered as the most compromised platforms for botnet attacks as compared to the recently evolved mobile botnets due to several reasons: (a) limited battery power (2) resource constraints (3) limited Internet access etc. Mobile botnet architecture has similarities with the traditional PC based botnet architecture. For instance, similarities in the underlying C&C communication protocols exist that includes IRC, HTTP [23], and P2P [24]. These protocols provide coordination between botmaster and bots in a desktop computing environment. In addition to these, SMS [25] [26] [27], Bluetooth [28] or MMS mechanisms have also emerged in mobile botnets

**Loopholes:** Institutions and consumers keep themselves up-to-date about mobile threats because mobile devices are vulnerable to new threats. In particular, Android OS is a victim of malware attacks as reported by[29]. Its increased market share and open source architecture is the enabling factor in the exploitation of various attacks. Although new versions of android operating systems are more resistant against

security vulnerabilities, nevertheless, 44 percent android users do not update and hence compromise their mobile security. SIM cards are the tiny computers inside most mobile devices that allow them to communicate with the service provider. According to one security research [30], flaws in SIM card technology and implementation make hundreds of millions of mobile devices susceptible to being hacked. The root of the problem is the fact that encryption in most SIM cards relies on DES (Data Encryption Standard)- an algorithm created by the US government four decades ago. DES was secure in its day, but the day has long since passed. Now, DES is considered insecure, and is relatively trivial for a skilled hacker or crack.

**Attack Types:** A recent study by Kespersky [15] reported that the most common attacks targeting Android platform are SMS Trojans, adware, viruses, spywares and root exploits. Moreover, mobile botnets are becoming serious threat focusing different mobile platforms that can perform various tasks at the instructions of botmaster. Botnet typically uses DNS to retrieve IP addresses of the servers, therefore targeting DNS service is initial point of attack. It results in activation of incredibly robust and stealthy mobile botnet C&C [31]. 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 call charging detail records (CDR) of the infected mobile systems [4]. Another approach used to reduce such activities is known as the rootkit [32]. It is a type of malicious code specially designed to hide the unwanted activities and virus propagations from the system. In this case, the C&C of a botnet instructs the bots to carry out a malicious activity including, sending spam messages or acquiring authorized control over to smartphone devices and hijack business activities.

**Target Audience:** Mobile botnets are focusing target audience from diverse environments ranging from public audience to government, enterprises and organizations. Profitable organizations like banks (which are shifting majority of their services to the mobile environment e.g. payment of bills, generating account statements and funds transfer). Therefore, the primary focus of mobile botmaster is to gain access to those mobile devices which are dedicated for business activities and tries to launch various activities for instance, DDoS, remote control, and hijacking of private/confidential information. According to Information Week[33], Bank of America, U.S bank, Wells Fargo and JPMorgan Chase were among those U.S banks that were slowed down by DDoS attacks. As a consequence of this attack, thousands of their customers filed complaints for site down and could not access their normal banking activities e.g. account checking, saving, bill payments, mortgage accounts and other similar services through mobile applications.

**Operational Impact:** Overall operational impact of mobile botnet can be seen in two different perspectives: 1) relevant to the host device itself and, 2) relevant to the service provisioning model. The direct impact 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.

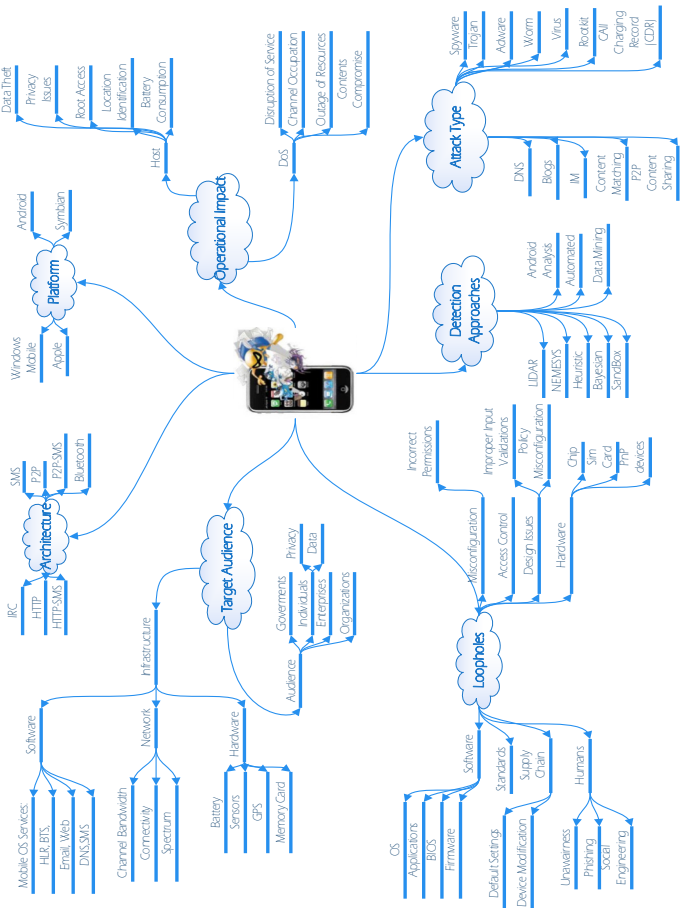


**Fig. 1.** Thematic Taxonomy based on Mobile Botnet Attack Vector

**Detection Approaches:** A mobile botnet detection approach based on "pull" style C&C was presented in [34]. Through investigating flow features (total packets, total bytes) of C&C traffic passing through VPN, the authors investigated the abnormalities of these traffic flows. This approach can also detect mobile botnets residing within signatures, abnormal models and whitelists.

A layered IDS and Remediation framework was proposed by [35] which automatically detects, analyzes, protects and removes security threats in smartphones. This study aims to overcome smartphone vulnerabilities and threat detection in three stages: a) behavioral and threat modeling technique, b) implementation and deployment of stochastic and machine learning techniques to automatically detect intrusion detection that can span among different network layers, applications and social media, and c) builds an automatic threat detection model to lessen or even overcome the security risks.

A behavioral model for the detection of smartphone malwares based on ontology techniques was proposed in [36]. Another approach [4] focused to design a network based anomaly detection method based on analytical modeling, learning and simulating, together with the billing and control-plan data to detect mobile attacks and anomalies. Furthermore, authors in [37] created a virtual lab environment for the purpose of analysis and detection of Android malwares through emulating the environment. In addition to that, a signature based mobile botnet detection algorithm considering Bayesian spam filter mechanism as the key component was proposed in [r10].The authors concluded that this system is capable of identifying 87% of spam message from the dataset.

A prototype named Airmid [29] was designed to automatically identify and respond to malicious mobile applications through analyzing the behavior of the network traffic. It identifies malicious network traffic through the help of cooperation between smartphones and in-network sensors. To detect Android malwares and malicious behavior of applications, a hybrid (static & dynamic) model was proposed in [38] which detects malicious activity through the following stages: a) static analysis --- to parse Manifest file of applications and decompile using reverse engineering tools, and b) dynamic analysis--- execute an application and log all performed actions.

# 3 Comparison of Existing Mobile Botnet Attacks Based on Taxonomy

In this section, we compare the existing mobile botnet attacks based on the significant parameters derived from the taxonomy. Table 1 shows the comparison.

## 3.1 DreamDroid

A mobile botnet based malware DroidDream [16] appeared in spring 2011. The purpose to launch this attack is to gain root access to Android mobile devices in order to acquire unique identification information (model number, product ID, EMI number, provider,

language etc) of the 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. Later, 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 had been malfunctioned by DroidDream malware.

### 3.2 SymbOS.Yxes[2]

This worm targets Symbian mobile devices with OS 9.1S60 3rd Edition, but can also run on wider range of Symbian Operating systems. The potential capabilities of this worm are (a) sending messages to those phone numbers that were harvested from infected devices' SMS inbox. (b) steal information from the victim device e.g. serial number of phone, subscription information and redirect this information to servers controlled by cybercriminals (c) search installed applications from application manager and attempt to kill those tasks or applications. This worm uses valid but revoked certificate, therefore it is required for a device to avoid this attack through enforcing online verification of certificate.

### 3.3 IKee.B

A standalone malicious program that infects iPhone in different ways, such as (a) the device is 'jailbroken'-hacked and installed a software that is not signed by Apple (b) installation of unsigned secured shell (SSH) with remote access enabled capability (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) establish connection with remote server 92.61.38.16 via HTTP and download and install additional components (c) send banking information incorporated in SMS messages to remote server. The only defensive reaction is to reset iPhone and restore all setting to its factory default.

### 3.4 BBproxy

A Trojan malware was detected in blackberry smart phones in Mid-2006, which targeted the enterprise data and network. Initially it creates a trust relationship between a blackberry device and company’s internal server. Once the connection is established, it hijacks and establishes a connection with the company’s internal server. In addition to that, data tunnel established between both entities is based on a secure tunnel. Therefore it is difficult to detect any suspicious activity for intrusion detection system which is installed on the perimeter of the network. The recommendations to avoid this malicious act are: (a) keep blackberry server in demilitarized zone (DMZ) (b) the communication between blackberry server and device should be restricted.

**Table 1.** Mobile Botnet Threat Analysis: A TimeLine

| Botnet/ Malware | Type | Platform | Category | Target Audience | Loophole | Dissemination Technique | Operational Impact | Defensive Reaction |
|---|---|---|---|---|---|---|---|---|
| DroidDream [1] | Root Exploitation | Android | Trojan | Android users | Alter code for Root access | Games | Root access, steal data | Android App Kill switch |
| SymbOS. Yxes[2] | 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 [3] | 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 [5] | Personal Information Theft | Android | Trojan | Android Users | Exploit backdoor | Games | Send private information to C&C via HTTP | Symantec Power Eraser Tool (SPE) |
| RootSMART [7] | 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[9] | Spam, Fraud | Any | Phishing | Any | Phishing to humans | Monetized by signing up | Steal personal information | Educate People |
| Snooping [10] | Privacy/ Snooping | Android <2.3.4 and 3.0 | ftware ult | 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 [11] | Spy Software | Any | Sensors | Any | Phishing to humans | Installation on victim machine | Steal personal information, | Educate People |
| SSL Renegotiation DoS [13] | DoS, Asymmetric Processing | Any | Generic Attack | SSL/TSL servers | TSL Operations | Massive TLS renegotiation requests | Deplete Server resources | Disable SSL/TSL renegotiation |
| BBproxy [14] | Infrastructure | Blackberry/ RIM | Trojan | Enterprise Internal data and network | Exploit the trust relationship | Games, Email | Steal companies' Information | Separate DMZ, limited access |
| Foncy [15] | 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 [15] | SMS Trojan | Android | Trojan | Twitter Users | Posting Message on Twitter | Unknowingly sending SMS to premium users | Information Threat | Antivirus Scanner |
| SpamSold[18] | SMS Spam | Android | Spam | Any | Deceptive Android Permissions | Fee games | Establish connection with C&C | Various Antivirus Software |
| Obad[20] | Admin Exploitation | 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 |

## 4 Issues and Challenges

As a result of exhaustive survey on the existing botnets, we identify open issues for progressive security of mobile devices against botnets. With the proliferation of mobile technology and cloud computing services, the following issues are of concern for academia and industry alike:

- Initially, manifestation of a cross-functional group is essential that involves 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 use must be documented and socialized across the enterprise. Moreover, the public audience should be aware of the means by which mechanisms are designed and developed to overcome mobile botnet threats.
- There is no way for security and risk leaders to ignore the increasing demand and proliferation of mobile into the enterprise at this point. The demand isn't just being driven from by the mass adoption and use consumer devices, but businesses are also leveraging 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 cloud can be implemented to preempt the code or information sharing centers in cooperation with antivirus vendors identify and plan to block the threats. When the malicious code is preempted it may not be possible for providers to predict how devices with more operating platforms receiving the code will behave with traffic. But in case of detection and block management of threats it can be applied in blocking solutions.
- As compared to desktop operating system, smartphone device operating system has less capability in terms of processing, memory and storage, which ultimately restricts the security policy to be implemented at its best.
- Network operators have remarkable control on the software employed for smartphones, which are using their network. The case happens especially when mobile phones are sold as part of wireless subscription. The operators should provide built-in anti-virus scanning facility and should enforce updating and patching in response to any malicious activity.
- User awareness with respect to security threats is a key contribution towards persistent solution of the problem. Therefore, a relevant and determined education and awareness campaign should be introduced that targets mobile users on the risks, policies, and procedures.

## 5 Conclusion

In this survey, 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 and used it to explore the acute features of existing botnet attacks. This review aims to serve as a roadmap for researchers to study and enforce secure communication patterns that are focused at various aspects of attack vectors.

Related to our observations about mobile botnet attacks, we conclude that Android has the minimum resistance against mobile botnets for two main reasons: 1) being open source that makes it a free to contribute digital contribution platform and 2) augmented market penetration that makes it suitable for the spread of botnet.

Addressing mobile botnet attacks have become a challenge for information security professionals and researchers. Therefore, it is necessary that, stakeholders must implement some cooperative and legislative actions to eliminate this hazard. Similarly, it is also important to negotiate on possible international legislative issues and establish global policies to systematically avoid this harmful threat.

## References

1. DroidDream, DroidDream (2012), http://www.webopedia.com/TERM/D/droiddream.html (accessed on: November 30, 2013)
2. Center, F.: SymbOS/Yxes.A!worm!worm (2009), https://www.fortiguard.com/ve?vn=SymbOS/Yxes.A (accessed on: November 30, 2013)
3. Worm: iPhoneOS/Ikee.B, http://www.f-secure.com/v-descs/worm_iphoneos_ikee_b.shtml (accessed on: November 30, 2013)
4. Abdelrahman, O.H., et al.: Mobile Network Anomaly Detection and Mitigation: The NEMESYS Approach. arXiv preprint arXiv:1305.4210 (2013)
5. Android. Geinimi, http://www.symantec.com/security_response/writeup.jsp?docid=2011-010111-5403-99 (accessed on: November 30, 2013)
6. 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
7. Xuxian, J.: Security Alert: New RootSmart Android Malware Utilizes the GingerBreak Root Exploit (2012)
8. Ollmann, G.: The evolution of commercial malware development kits and colour-by-numbers custom malware. Computer Fraud & Security 2008(9), 4–7 (2008)
9. Musthaler, L.: How to avoid becoming a victim of SMiShing (SMS phishing), pp. 10–11 (2013) (accessed on: November 10, 2013)
10. Mills, E.: Report: Android phones vulnerable to snooping attack
11. Kiley, S.: Spy Smartphone Software Tracks Every Move
12. Xiang, C., et al.: Andbot: towards advanced mobile botnets. In: Proceedings of the 4th USENIX Conference on Large-Scale Exploits and Emergent Threats. USENIX Association (2011)
13. Orchilles, J.A.: SSL Renegotiation DOS
14. Zetter, K.: BlackBerry a Juicy Hacker Target

15. SecureList: Mobile Malware Analysis: Part-6, http://www.securelist.com/en/analysis?calendar=2013-02
16. Zhao, S., et al.: Cloud-based push-styled mobile botnets: a case study of exploiting the cloud to device messaging service. In: Proceedings of the 28th Annual Computer Security Applications Conference. ACM (2012)
17. Zeus Botnet Eurograbber Steals $47 Million, http://www.informationweek.com/security/attacks/zeus-botnet-eurograbber-steals-47-millio/240143837 (accessed on: November 19, 2013)
18. Microsoft, Malware Protection Center, Trojan: AndroidOS/SpamSold.A (2013)
19. Android DreamDroid two: rise of laced apps, http://www.itnews.com.au/News/259147,android-dreamdroid-two-rise-of-lacedapps.aspx (accessed on: November 19, 2013)
20. Donovan, F.: Botnet of mobile devices used for first time to distribute Trojan (2013)
21. F.: securel Virus and threat descriptions
22. Szongott, C., Henne, B., Smith, M.: Evaluating the threat of epidemic mobile malware. In: 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE (2012)
23. 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
24. Grizzard, J.B., et al.: Peer-to-peer botnets: Overview and case study. In: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets (2007)
25. Geng, G., et al.: An improved sms based heterogeneous mobile botnet model. In: 2011 IEEE International Conference on Information and Automation (ICIA). IEEE (2011)
26. Hamandi, K., et al.: Android SMS botnet: a new perspective. In: Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access. ACM (2012)
27. Geng, G., et al.: The Design of SMS Based Heterogeneous Mobile Botnet. Journal of Computers 7(1), 235–243 (2012)
28. Singh, K., Sangal, S., Jain, N., Traynor, P., Lee, W.: Evaluating bluetooth as a medium for botnet command and control. In: Kreibich, C., Jahnke, M., et al. (eds.) DIMVA 2010. LNCS, vol. 6201, pp. 61–80. Springer, Heidelberg (2010)
29. Nadji, Y., Giffin, J., Traynor, P.: Automated remote repair for mobile malware. In: Proceedings of the 27th Annual Computer Security Applications Conference. ACM (2011)
30. Forbes, https://viaforensics.com/resources/reports/best-practices-ios-android-secure-mobile-development/mobile-security-primer/
31. Open DNS, security whitepaper, http://info.opendns.com/rs/opendns/images/OpenDNS_SecurityWhitepaper-DNSRoleInBotnets.pdf
32. Rootkit, http://en.wikipedia.org/wiki/Rootkit
33. 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?
34. Choi, B., Choi, S.-K., Cho, K.: Detection of Mobile Botnet Using VPN. In: 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). IEEE (2013)

35. Roshandel, R., Arabshahi, P., Poovendran, R.: LIDAR: a layered intrusion detection and remediationframework for smartphones. In: Proceedings of the 4th International ACM Sigsoft Symposium on Architecting Critical Systems. ACM (2013)
36. Chiang, H.-S., Tsaur, W.-J.: Identifying Smartphone Malware Using Data Mining Technology. In: 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN). IEEE (2011)
37. Andrews, B., Oh, T., Stackpole, W.: Android Malware Analysis Platform. In: 8th Annual Symposium on Information Assurance, ASIA 2013 (2013)
38. Spreitzenbarth, M., et al.: Mobile-sandbox: having a deeper look into android applications. In: Proceedings of the 28th Annual ACM Symposium on Applied Computing. ACM (2013)