MoBots: A New Generation of Botnets on Mobile Devices and Networks

Meisam Eslahi
Computer System and Technology Dept.
University of Malaya
Kuala Lumpur, Malaysia.
Email: meisam_eslahi@um.edu.my

Rosli Salleh
Computer System and Technology Dept.
University of Malaya
Kuala Lumpur, Malaysia.
Email: rosli_salleh@um.edu.my

Nor Badrul Anuar
Computer System and Technology Dept.
University of Malaya
Kuala Lumpur, Malaysia.
Email: badrul@um.edu.my

***Abstract*— Mobile devices are now well integrated with advanced capabilities and technologies such as the Internet. Today, mobile security has become a globally critical issue due to the high usage of mobile devices, their convenience and mobility. However, they are not properly protected compared to computer and computer networks, and the users pay less attention to the security updates. Recently, mobile devices and networks have been targeted by one of the most dangerous cyber threats, known as botnets. Mobile botnets have not yet been fully explored as they have only recently migrated to mobile infrastructures. Therefore, in this paper, we present an overview of mobile botnets including studies on the new command and control mechanisms, actual examples and malicious activities. We also review the current challenges and limitations of botnet detection in mobile environments, as well as existing solutions.**

Keywords*— Mobile Security, Survey, Mobile Botnets, C&C, Botnet Detection.

I. INTRODUCTION

The emergence of new technologies and features of mobile devices makes mobile communication an integral part of every aspect of human activity from education to business and research. Mobile networks are now well integrated with the Internet (e.g. 3G, 4G and LTE technologies); therefore, with the increasing use of these devices on a global scale, mobile security has become a crucial issue [1]. The mobile attacks and threats come in different forms, such as viruses and worms. However, botnets are more dangerous as they pose serious threats to mobile devices and communication networks [2, 3].

A botnet consists of small malicious applications which infect different targets (e.g. computers or mobile devices) without attracting the users' attention, that subsequently communicate with each other by using a command and control (C&C) mechanism [4]. The main difference between botnets and the other threats lies in the fact that they are dynamically controlled by a sophisticated attacker called a botmaster [5]. Regardless of their size, which has a direct link to their complexity and intention, botnets are mainly created to carry out malicious activities in cyberspace. The well managed communication pattern among botnet elements (i.e. bots, C&C servers, and botmasters), and their coordinated attacks have categorised them as an organised form of cybercrime [1].

Botnets are known to have been operating on traditional network infrastructures, with their most common targets being less-monitored computers, computers with high-bandwidth connections, university servers and home computers. Nowadays, mobile devices, and specifically smartphones, are efficient enough to provide environments which attract botmasters [6]. The immense use of them along with the Internet has motivated botmasters to migrate to mobile infrastructures. A series of highly updated reports published by North Carolina State University in collaboration with NQ Mobile [7] has shown that the new generation of botnets and organised C&C based cybercrimes have targeted mobile networks. Since the mobile botnets are newly appeared, the numbers of related studies are relatively low compared to computer-based botnets. Therefore, in this paper we investigate the mobile botnets (MoBots) and present a survey on their characteristics along with detection approaches and challenges. The rest of the paper is organised as follows:

Section II presents current studies on new MoBots' command and control mechanisms. Section III reviews examples of existing botnets in real environments along with their characteristics and malicious activities. The current challenges and limitations in MoBot detection are considered in Section IV, followed by existing solutions in Section V. Finally, Section VI gives the overall conclusions of this paper.

II. COMMAND AND CONTROL MECHANISMS

Command and control (C&C) mechanisms are used as an interface to send botmasters' commands to infected targets (bots) and receive responses from them accordingly [4]. Figure 1 depicts a general view of a botnet C&C scheme.

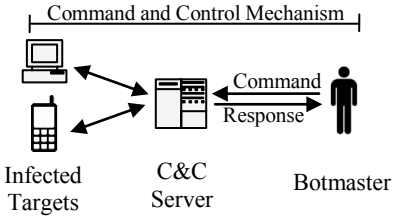

Figure1: A Botnet General Scheme

Botmasters are always attempting different techniques to build fool-proof communication between themselves and bots in a botnet [1, 8]. The first generation of computer-based botnets, were established over IRC servers and their relevant channels, and then evolved to P2P and HTTP mechanisms [9]. In contrast, it is difficult to implement a wide variety of C&C models for MoBots, due to the lack of public IP addresses, the variety of operating systems, different types of connectivity, and the cost of communications [10]. Therefore, a number of studies have been conducted to investigate possibilities of mobile botnets' operations and their countermeasures.

A Short Message Service or SMS is commonly used to propose communication approaches because of the wide range of subscribers, ease of use, and high availability [11]. In a previous study [3], the authors evaluated two peer to peer models called Kademila [12] and Gnutella [13] to implement the SMS-based mobile botnet. However, their model inherited the complexity of the aforementioned peer-to-peer models and required a high number of messages to convey commands to an entire botnet [14]. SMS messages are also not free; thus, costs incurred by the high number of messages required may notify mobile device owners and lead this model to be detected [15]. To overcome this issue, Hua *et al.* [14] proposed a model with a fewer number of messages. They initially sent commands to selected devices and used them to transfer commands from mobile to mobile (i.e. graph structure) by using a flooding algorithm. This model significantly spread a command over an entire botnet containing 20000 members by sending only four messages from each mobile device. However, the main weakness of this model was where the infected mobiles connected to a server over the Internet to get updates and a list of neighbours to form their graph structure. Like a traditional central C&C mechanism, this model comes with a single point of failure [5, 14].

As for computer-based botnets, a hybrid approach was proposed by Singh *et al.* [16], in order to utilise the advantages of different technologies and architectures. They adopted both SMS and Bluetooth to implement a communication model between pre-selected mobiles called updated nodes and the botmaster. Among all of the infected mobiles, those with higher contact with other devices (i.e. over Bluetooth) were selected as update nodes. The authors assumed that these nodes could deliver the commands to others by using Bluetooth when they were in the same frequency range. In addition to the complexity of using Bluetooth, this model comes with traditional P2P botnet drawbacks, which includes the lack of guarantee of message delivery or latency [5]. In addition, the Bluetooth needs permission to receive data and accordingly commands which are sent by the update nodes.

Mulliner *et al.* [10] introduced SMS-only and SMS-HTTP approaches to form another hybrid model. The first approach was designed based on a hierarchical tree structure in which some nodes were placed at the top as a root and others at the bottom as leaves. The botmaster employs the roots to spread commands to the entire tree. As noted by the authors, this model needed a complex procedure to repair and manage any root failure. In fact, all of the sub-nodes would be disconnected from the botnet if their corresponding root node was detected and eliminated. To overcome this problem, they proposed an SMS-HTTP model where the botmaster commands were initially published on a website as a central C&C server, which was received by randomly selected mobiles and forwarded to other bots via SMS. The selected bots periodically connected to the server to receive updates; therefore, this model can be easily detected by cooperative behaviour analysis in large-scale botnets [5]. Finally, the root failure problem was improved in another study [11] by considering broken node's status reports and replacement.

The aforementioned models were mainly designed based on some extent of non-Internet-based technologies like SMS and Bluetooth. Recently, many mobile devices have been connected to the Internet, which provides new opportunities for botmasters to develop IP-based C&C mechanisms (e.g. HTTP-based) [17]. Recently, Knysz *et al.* [18] discovered that mobile botnet activities over WiFi connections are more difficult to monitor and detect compared to other mediums like 3G, SMS and MMS. Thus, they designed a bot which looks for open WiFi networks to connect and receive commands. In addition, they simulated a successful Distributed Denial of Service (DDoS) attack by using their proposed HTTP-based mobile botnet. Finally, like Koobface [19] in computer-based botnets, Faghani *et al.* [20] used online social networking (OSN) as an infrastructure to implement a C&C mechanism for mobile botnets.

This section discussed current studies of new mobile C&C mechanisms. Although, Mulliner *et al.* [10] highlighted several difficulties of designing communication models for mobile botnets, practically they have evolved from day-to-day. The next section provides a few real-world examples of mobile botnets and their malicious activities.

III. MoBots and Malicious activities

Although there have only been anticipations of the existence of mobile botnets [1, 11], one of the first official reports was released by the Damballa Research Laboratory [17]. Based on the report, 40,000 infected mobile devices have been found to be communicating through cybercriminal C&C servers for the first six months of 2011. Moreover, the McAfee research lab predicted that the cyber community (e.g. mobile banking) will face more widely-distributed and more resilient mobile botnets, which are difficult to detect and exterminate [21]. Table 1 shows a number of mobile botnets and their malicious activities.

A. Zeus:

As foreseen by the McAfee research lab, the Zeus botnet migrated from computers to mobile devices and targeted mobile banking. The Zeus in the Mobile or Zitmo uses a social engineering technique in which an SMS is sent to mobile devices with a fake URL that asks users to download a security certificate which is, in fact, the Zitmo bot [22]. It also intercepts messages which are sent by banks to customers and authenticates illegal transactions by stealing mobile Transaction Authentication Numbers (TAC) [23]. One of the

Table 1: Examples of Real Mobile Botnets Characteristics and Attacks

Name	Propagation Method	Attack(s)	Mobile OS	Special Characteristic
Zeus (Zitmo)	• Social Engineering • Infected SMS Messages	• Mobile Banking Attacks • TAC Thefts • Illegal Transactions	• Symbian • Win Mobile • BlackBerry • Android	• Specific Targeted Victims (European Users)
DroidDream	• Exploit Techniques • Trojanised Applications	• Theft of Private Data • Download Malicious Applications	• Android	• Specific Operational Times (11 pm to 8 am)
Android.Bmaster (SmartRoot)	• Exploit Techniques • Trojanised Applications	• Revenue Generation • Theft of Private Data	• Android	• Specific Geographical Distribution (China Boundaries)
AnserverBot	• Social Engineering • Trojanised Applications	• Theft of Private Data	• Android	• Self- Protection • Two Layers C&C
Ikee.B	• Self-Propagation	• Revenue Generation • Theft of Private Data	• iPhone	• Specific Targeted Victims • Specific Geographical Distribution
TigerBot	• Trojanised Applications	• Theft of Private Data • Change Device Settings	• Android	• Self- Protection

notable characteristics of Zitmo is the variety of supported operating systems, such as Symbian, Windows Mobile, BlackBerry, and Android. However, it has recently attacked a smaller group of mobile users, like specific bank users in various European countries [22, 24].

B. DroidDream

The DroidDream MoBot exploits android-based mobile devices to gain root privileges and install another application on infected targets. The second application prevents DroidDream removal, and sends sensitive information to its command and control server, including the user's country, device model and SDK version [25]. Botnets do not make any unusual use of resources or suspicious behaviour on infected targets in order to avoid detection systems. DroidDream is a good example of these silent patterns, since it is activated silently and at night (11pm to 8 am) when the mobile's users are asleep [26].

C. Android.Bmaster

As one of the main differences between botnets and other Internet threats is revenue generation [1], the Android.Bmaster has employed Trojan applications and exploited techniques to infect mobile devices in an attempt to gain money through premium SMS, telephony or video services. Because of the high number of infected devices, millions of dollars have been illegally earned by its botmaster. However, its geographical distribution is small and limited to China [27]. In addition to illegal financial activities, the Android.Bmaster (aka RootSmart) collects a wide range of information on infected devices and records them in its C&C server [28].

D. Ikee.B

Ikee.B is a simple botnet that mostly targets jailbreak iPhones to collect private data. It is considered a proof-of-concept that botnets can be operated on mobile devices with almost the same functionality as computer-based botnets [29]. It dynamically scans the iPhone network IP addresses and attempts a self-propagation technique to infect new devices. An Ikee.B on an infected mobile can propagate itself to other devices located in different countries and deliver private data to its C&C server located in Lithuania [29, 30].

E. AnserverBot

Unlike Ikee.B, the AnserverBot is considered one of the most sophisticated malwares, and was identified by the NetQin research group on the android platform. Besides having a two-layer complex C&C mechanism over public blog services, the botmaster has used different techniques to regularly check its integrity (i.e. verifying its signature) and security. In addition, it detects security managers on infected devices and attempts to disable and remove them [31]. AnserverBot installs a backdoor to infected devices in order to steal private data. It acts like a Trojan by attaching itself to normal applications, and infects victims by sending fake update messages and social engineering techniques [28, 32].

F. TigerBot

On the contrary to most of the existing mobile botnets, TigerBot is fully controlled by SMS instead of the Internet and web technologies. However, it detects the C&C messages and makes them invisible to the mobile device owners [33]. Moreover, it uses popular application names and icons like Google's search application. As reported by the Symantec research lab, it is particularly designed to be spyware. In addition to collecting private data like SMS messages, it has sophisticated capabilities to record voice call conversations and even surrounding sounds [34].

The aforementioned botnets are only a few examples of current mobile botnets to emphasise their existence and their negative impacts on mobile network environments. As suggested by the Nokia Siemens Networks of Germany [6], mobile network operators (MNO) should consider mobile botnet detection approaches in their systems as they will be affected by high losses caused by their malicious activities. However, the characteristics of mobile devices and networks make a set of challenges and limitations which will be discussed in the next section.

IV. DETECTION: CHALLENGES AND LIMITATIONS

There are several methods and techniques that have been used to track botnet activities and detect them in computer networks, including Honeypots and Honeynets, attack's behaviour analysis, monitoring and analysing the DNS,

signature-based botnet detection and behavioural analysis techniques [5]. Regardless of the efficiency and accuracy of these techniques, they are mostly designed based on computer and computer network behaviours and characteristics and may not be directly applicable for mobile devices [3]. In addition, there are some mobile based characteristics that make them different from computers. The current challenges in mobile botnet detection can be summarised as follows:

A. Resource Limitations and Specific Characteristics

Mobile device resources, such as CPU, memory, and battery life, are limited. Therefore, it is difficult to deploy existing botnet detection solutions for mobile botnets [3]. Moreover, there are some mobile-specific characteristics that have differentiated mobile security management to computers [35]. La polla *et al.* [2] summarised them as mobility, strict personalisation, different types of connectivity, technology convergence, and variety of capabilities.

B. Diversity in Infection and Propagation

In a previous study [3], the researchers investigated the potential methods of spreading bots on mobile devices. Infected codes attached to MMS/SMS messages, spam emails, malicious URLs and Bluetooth are listed as vectors of propagating mobile bots. These examples show that, unlike computer-based botnets, the MoBots can use different mediums (e.g. SMS/MMS) along with the Internet to spread. Moreover, this diversity makes it default to detect infection processes using current security systems [2].

C. Self-Protection Techniques

Like any other type of botnets (e.g. Computer-based botnet), MoBots have several characteristics that make them difficult to be detected, such as being developed by proficient developers, having dynamic nature, and being flexible [1, 4]. Moreover, as shown in table 1, botmasters are always trying different techniques to protect their bots from existing detection solutions.

D. Lack of Central Security Management

Mobile devices are not properly protected compared to computer and computer networks, and their users pay less attention to the security updates [36]. Therefore, among all of the aforementioned issues, the main challenge with mobile security is the lack of central security management, as it can track and monitor security threats and update the security policies on mobile devices accordingly [1, 37]. Moreover, as noted by Bailey *et al.* [5], a wide range of current botnet detection methods are designed based on cooperative behaviours posed by bots within the same botnet. As a matter of fact, in mobile devices, there is no centralised security management to analyse these similarities.

These sophisticated characteristics show that mobile botnet detection is a notable challenge in mobile security management, and creative solutions are needed to address the challenges discussed above.

V. CURRENT SOLUTIONS

As suggested by Hua *et al.* [14], one possible solution is to design and develop special security managers (e.g. Honey Phones) based on mobile characteristics. However, in this solution and any other host-based model, the mobile limitations should still be considered. Therefore, a central security management approach over the network infrastructure (e.g. cloud) is proposed [38, 39] as it brings some advantages:

- Shifting the computational and analytical approaches to central management can reduce the processing load and effects on the mobile clients and any other end devices. This method minimises the complexity of computation on the mobile side, in addition to mobile resource consumption.
- From a security point of view, a central management model can record a wide range of information of malicious activities on the same or different infected targets. It provides a rich dataset to enhance the forensic capabilities and retrospective detection.
- Different security analysis models and engines can be employed in central management servers in parallel and independent of clients' specifications and characteristics.

Based on this idea, Kok *et al.* [6] proposed a primitive central management model for MoBot detection called the Anti-Botnet Operation Centre. Anti-Botnet consists of four different modules: analysing, detection, mitigation and prevention. However, they only discuss their model in general instead of providing details on how to detect and respond to mobile botnets. In contrast, Vural *et al.* [40] discussed detailed measurements to distinguish the human and bot activities with respect to the delay, volume, and median of weekly outgoing and incoming SMSs. They also proposed a fuzzy-logic network forensic technique that can be deployed on mobile operator servers to detect SMS-based mobile botnets.

VI. CONCLUSION

This paper presents an overview of the current state of a new generation of botnets called MoBots which operate on mobile devices and mobile networks. As they are newly developed, current studies have been mostly focused on proposing new structures and communication models instead of detecting, mitigating, and responding to them. Real examples of mobile botnets show that botmasters have taken advantage of the lack of security knowledge of mobile users in an attempt to steal private data and earn money illegally. In addition, mobile environments are less protected compare to computers and computer networks and their specific characteristics bring notable challenges to mobile botnet and malware detection.

ACKNOWLEDGMENTS

This work was supported in part by the University of Malaya and the Ministry of Higher Education, Malaysia, under Grant RG086-12ICT and FRGS FP034-2012A. The authors would also like to thank Maryam Var Naseri for her valuable help and support.

REFERENCES

[1] A. Flo and A. Josang, "Consequences of Botnets Spreading to Mobile Devices," in *Proceedings of the 14th Nordic Conference on Secure IT Systems (NordSec)*, 2009, pp. 37-43.

[2] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," *IEEE Communications Surveys & Tutorials,* 2012, doi:10.1109/SURV.2012.013012.00028

[3] Yuanyuan Zeng, X. Hu, and K. G. Shin. (2010). *Design Of SMS Commanded-and-Controlled And P2P-Structured Mobile Botnets* [PDF]. Available: http://www.eecs.umich.edu/techreports/cse/2010/CSE-TR-562-10.pdf

[4] N. Hachem, Y. Ben Mustapha, G. G. Granadillo, and H. Debar, "Botnets: Lifecycle and Taxonomy," in *Proceedings of the Conference on Network and Information Systems Security (SAR-SSI)*, 2011, pp. 1-8.

[5] M. Bailey, E. Cooke, F. Jahanian, X. Yunjing, and M. Karir, "A Survey of Botnet Technology and Defenses," in *Proceedings of the Cybersecurity Applications & Technology Conference for Homeland Security (CATCH)*, 2009, pp. 299-304.

[6] J. Kok and B. Kurz, "Analysis of the BotNet Ecosystem," in *Proceedings of the 10th Conference of Telecommunication, Media and Internet Techno-Economics (CTTE)*, 2011, pp. 1-10.

[7] X. Jiang. (2011). *AnserverBot, New Sophisticated Android Bot Found in Alternative Android Markets* [Online]. Available: http://www.csc.ncsu.edu/faculty/jiang/

[8] MacAfee. (2011). *Threat Predictions 2011* [PDF]. Available: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2011.pdf

[9] L. Jae-Seo, J. HyunCheol, P. Jun-Hyung, K. Minsoo, and N. Bong-Nam, "The Activity Analysis of Malicious HTTP-Based Botnets Using Degree of Periodic Repeatability," in *Proceedings of the International Conference on Security Technology (SECTECH)*, 2008, pp. 83-86.

[10] C. Mulliner and J. P. Seifert, "Rise of the iBots: Owning a telco network," in *Proceedings of the 5th International Conference on Malicious and Unwanted Software*, 2010, pp. 71-80.

[11] G. Guining, X. Guoai, Z. Miao, Y. Yixian, and Y. Guang, "An improved SMS based heterogeneous mobile botnet model," in *Proceedings of the IEEE International Conference on Information and Automation (ICIA)*, 2011, pp. 198-202.

[12] P. Maymounkov and D. Mazires, "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric," in *Proceedings of the First International Workshop on Peer-to-Peer Systems*, 2002, pp. 53-65.

[13] Y. Chawathe, S. Ratnasamy, L. Breslau, N. Lanham, and S. Shenker, "Making Gnutella-like P2P systems scalable," in *Proceedings of the Conference on Applications, technologies, architectures, and protocols for computer communications*, Karlsruhe, Germany, 2003, pp. 407-418.

[14] J. Hua and K. Sakurai, "A SMS-based mobile Botnet using flooding algorithm," in *Proceedings of the 5th International Conference on Information Security Theory and Practice*, Greece, 2011, pp. 264-279.

[15] J. Hua and K. Sakurai, "Botnet command and control based on Short Message Service and Human Mobility," *Computer Networks,* 2012, doi:10.1016/j.comnet.2012.06.007.

[16] K. Singh, S. Sangal, N. Jain, P. Traynor, and W. Lee, "Evaluating Bluetooth as a medium for botnet command and control," in *Proceedings of the 7th international conference on Detection of intrusions and malware, and vulnerability assessment*, Bonn, Germany, 2010, pp. 61-80.

[17] Damballa. (2011). *First Half 2011 Advanced Threat Report* [PDF]. Available: http://www.damballa.com/downloads/r_pubs/Damballa_Threat_Report-First_Half_2011.pdf

[18] M. Knysz, X. Hu, Y. Zeng, and K. G. Shin, "Open WiFi networks: Lethal weapons for botnets?," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, 2012, pp. 2631-2635.

[19] K. Thomas and D. M. Nicol, "The Koobface botnet and the rise of social malware," in *Proceedings of the 5th International Conference on Malicious and Unwanted Software*, 2010, pp. 63-70.

[20] M. R. Faghani and U. T. Nguyen, "SOCELLBOT: A New Botnet Design To Infect Smartphones Via Online Social Networking," Department of Computer Science and Engineering, York University, Toronto,Canada, Tech. , 2012.

[21] MacAfee. (2012). *Threats Predictions 2012* [PDF]. Available: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf

[22] D. Maslennikov. (2011). *ZeuS in the Mobile – Facts and Theories* [Online]. Available: http://www.securelist.com/en/analysis/204792194/ZeuS_in_the_Mobile_Facts_and_Theories

[23] A. Apvrille. (2010). *Zeus In The Mobile (Zitmo) : Online Banking's Two Factor Authentication Defeated* [Online]. Available: http://blog.fortinet.com/zeus-in-the-mobile-zitmo-online-bankings-two-factor-authentication-defeated/

[24] D. Maslennikov. (2012). *New ZitMo for Android and Blackberry* [Online]. Available: http://www.securelist.com/en/blog/208193760/New_ZitMo_for_Android_and_Blackberry

[25] S. Perez. (2011). *More DroidDream Details Emerge: It was Building a Mobile Botnet* [Online]. Available: http://www.readwriteweb.com/archives/droiddream_malware_was_going_to_install_more_apps_on_your_phone.php

[26] T. Strazzere. (2011). *Do Androids Dream…?* [Online]. Available: http://blog.mylookout.com/blog/2011/03/06/do-androids-dream

[27] ThreatPost. (2012). *Researchers Discover Android Mobile Botnet 100k Strong* [Online]. Available: http://threatpost.com/en_us/blogs/researchers-discover-android-mobile-botnet-100k-strong-021012

[28] M. Spreitzenbarth and F. Freiling, "Android Malware on the Rise," University of Erlangen, Germany, Tech.Rep. CS-2012-04, 2012.

[29] P. Porras, H. Saïdi, and V. Yegneswaran, "An Analysis of the iKee. B iPhone Botnet," *Security and Privacy in Mobile Information and Communication Systems,* vol. 47, pp. 141-152, 2010.

[30] M. Postman. (2012). *iPhone Viruses: Ikee.b Worm* [Online]. Available: http://www.letsunlockiphone.com/ios-viruses-iphone-ikee-b-worm

[31] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2012.

[32] Y. Zhou and X. Jiang. (2011). *An Analysis of the AnserverBot Trojan* [PDF]. Available: http://www.csc.ncsu.edu/faculty/jiang/pubs/AnserverBot_Analysis.pdf

[33] X. Jiang. (2012). *New TigerBot Malware Found in Alternative Android Markets* [Online]. Available: http://www.csc.ncsu.edu/faculty/jiang/TigerBot/

[34] A. Yamamoto. (2012). *Android.Tigerbot* [Online]. Available: http://www.symantec.com/security_response/print_writeup.jsp?docid=2012-041010-2221-99

[35] J. Oberheide and F. Jahanian, "When Mobile Is Harder Than Fixed (and vice versa): demystifying security challenges in mobile environments," in *Proceedings of the 11th Workshop on Mobile Computing Systems and Applications*, Annapolis, MD, 2010, pp. 43-48.

[36] E. Yuce, "A Literature Survey About Recent Botnet Trends," GÉANT network, ULAKBIM,Turkey, Rep. JRA2 T4, 2012.

[37] W. Jansen and K. Scarfone, "Guidelines on Cell Phone and PDA Security," National Institute of Standards and Technology, Gaithersburg, MD, Rep. 20899-8930, 2008.

[38] J. Oberheide, E. Cooke, and F. Jahanian, "CloudAV: N-version antivirus in the network cloud," in *Proceedings of the 17th Conference on Security Symposium*, San Jose, CA, 2008, pp. 91-106.

[39] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid Android: versatile protection for smartphones," in *Proceedings of the 26th Annual Computer Security Applications Conference*, Austin, TX, 2010, pp. 347-356.

[40] I. Vural and H. Venter, "Mobile botnet detection using network forensics," in *Proceedings of the 3rd conference on Future Internet*, Berlin, Germany, 2010, pp. 57-67.