# MOBILE BOTNETS

**What is a botnet?**

A botnet is a network of private computers infected with malicious software and controlled as a group without the owner's knowledge. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks.

**What is a mobile botnet?**

A botnet in mobile networks is a collection of compromised nodes due to mobile malware, which are able to perform coordinated attacks. Mobile botnets take advantage of unpatched exploits to provide hackers with root permissions over the compromised mobile device, enabling hackers to send e-mail or text messages, make phone calls, access contacts and photos, and more. Most mobile botnets go undetected and are able to spread by sending copies of themselves from compromised devices to other devices via text messages or e-mail messages. Different from Internet botnets, mobile botnets do not need to propagate using centralized infrastructures, but can keep compromising vulnerable nodes in close proximity and evolving organically via data forwarding.

**Components of a mobile botnet:**

1. Botmaster: A botmaster controls all the nodes of the mobile botnet. The botmaster has direct contact with bot servers.
2. Bot: Bot is the compromised mobile device. It receives commands from region bot server, and executes the commands.
3. C&C Server: A command and control server (C&C server) is the centralized computer that issues commands to a botnet and reports back from the infected computers.

**Some mobile botnet attacks:**

- A mobile bot Waledac was designed to send emails without being noticed by mobile users. Waledac is a plug-in based botnet and it is easy to add plug-ins to extend functionality.
- An infected mobile device may send an SMS/MMS to service providers or to a wide range of subscribers.
- Victims or bot enemies can be selected by botmaster from the contact list or address book of infected mobile devices.
- A botmaster can dismiss recently evolved mobile voting services. Instead of using the voting application, a DDOS attack against core of the mobile network can be done to stop people voting by making the voting system unavailable during the voting period.
- Giving money to charity organizations using mobile services can be exploited by mobile botnets. A botherder can create his own service number and programs all his botclients to call that number. The price should be low so the subscribers would not notice and be suspicious about the extra charges
- Infected mobile devices can be treated as spyware to collect personal information of subscribers.

**Challenges in the construction of mobile botnets:**

1. The battery power is rather limited on smartphones when compared with PCs. If the battery power consumption speed exceeds user expectations, the battery exhaustion is likely to be noticed by the user, leaving the bot open to detection.
2. The cost of smartphones is an extremely sensitive area for many users. If data costs begin to exceed the amount that the user had expected or agreed to pay, the bot could also be detected.
3. If C&C consumes an abnormal amount of network traffic, the abnormity is likely to be noticed.
4. The absence of public IP addresses and a constant change in network connectivity makes the robust P2P-based C&C in PC-based botnets impractical, and potentially impossible, in smartphones.

**Factors that make detecting mobile botnets difficult:**

- It is developed by skillful developers who use various strategies to keep the bots safe and uncovered, as long as possible.
- Having Dynamic and Flexible Nature: Bot and botnets are continuously being updated and their codes change from day to day.
- Using Standard Protocols: Some botnets are using standard protocols to establish their communication infrastructure. For instance, one of the latest generations of botnet, called HTTP-based, uses the standard HTTP protocol to impersonate normal web traffic and bypass the current network security systems.
- Working in Silent Mode: The bots on infected targets try to avoid any unusual or suspicious use of the CPU, memory, or other computer resources, which may uncover their presence.
- Lack of Protection and User Awareness
- Resource Limitations: 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.
- MoBots can use different mediums (e.g. SMS/MMS/Bluetooth) along with the Internet to spread.
- Lack of Central Security Management: With the help of central security management we can track and monitor security threats and update the security policies on mobile devices accordingly.

**Mobile botnet detection:**

**(1) Detection of Mobile Botnet Using VPN [4]**

Their proposed solution is a network-based scheme that detects botnets by inspecting abnormal flow features of C&C traffic traveling through VPN which provides a shared path for both 3/4G and WiFi. Through the verification analysis under real botnet attacks, we show that our proposed scheme provides high detection rate by using abnormal models as well as low FP rate by adding white list and signatures.

**(2) SMS mobile botnet detection using a multi-agent system: research in progress [6]**

This paper proposes a SMS botnet detection framework that uses multi-agent technology based on observations of SMS and Android smartphone features. This system detects SMS botnets and identifies ways to block the attacks in order to prevent damage caused by these attacks. An adaptive hybrid model of SMS botnet detectors is being developed by using a combination of signature-based and anomaly-based methods. The model is designed to recognize malicious SMS messages by applying

behavioural analysis to find the correlation between suspicious SMS messages and reported profiling. Behaviour profiles of Android smartphones are being created to carry out robust and efficient anomaly detection. A multi-agent system technology was selected to perform light-weight detection without exhausting smartphone resources such as battery and memory.

**(3) MoBots: A New Generation of Botnets on Mobile Devices and Networks [7]**

This paper cites a few proposed current solutions like the following.

- One proposed solution is to design and develop special security managers 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 is proposed.
- Another solution was to use 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.

**Defense mechanisms that can be used against mobile botnets:**

- Antivirus Scanning
- Intrusion Detection System (IDS)
- Firewalls
- Packet Filtering
- Monitoring at SMSC
- Infiltration
- Building International Co-ordinated Mechanism

**Conclusion:**

With the research I had done to write up this article I have understood that mobile botnets are a serious threat and shouldn't be taken lightly. As you may have noticed from reading this article that it is very easy to form mobile botnets without the mobile phone user ever noticing the fact that their phone has been compromised and also it is still a challenge to find an efficient way of detecting these botnets. A variety of attacks can be carried out through the use of mobile botnets and there are still many undiscovered possible ways that these botnets can be used. There are many aspects of mobile botnets that are unexplored and hence, it is an interesting research area for those interested in doing some form of research in mobile security.

**References:**


1. http://www.kpubs.org/article/articleMain.kpubs?articleANo=E1KOBZ_2015_v9n4_1471
2. Study of Mobile Botnets: An Analysis from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices. (Authors - Rizwan Ahmed and Dr. Rajiv V. Dharaskar)
3. http://www.cyberdefensemagazine.com/mobile-botnets-are-all-around-us-by-meisam-eslahi/
4. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6603663&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6603663
5. http://link.springer.com/chapter/10.1007%2F978-3-642-15877-3_7
6. http://dl.acm.org/citation.cfm?id=2602950

7. https://www.academia.edu/7704856/MoBots_A_New_Generation_of_Botnets_on_Mobile_Devices_and_Networks
8. http://www.darkreading.com/cloud/the-rise-of-the-resilient-mobile-botnet/d/d-id/1317593
9. https://www.eecs.umich.edu/techreports/cse/2010/CSE-TR-562-10.pdf
10. http://www.webopedia.com/TERM/M/mobile_botnet.html