International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 16 (2015) pp 36494-36497

A Survey On Mobile Botnet

Birundha S
PG Student, Department Of Computer Science and Engineering,
Kumaraguru College of Technology, Saravanampatti, Coimbatore District
mailtobrindha@gmail.com

Vanitha V
Professor, Department Of Computer Science and Engineering,
Kumaraguru College of Technology, Saravanampatti, Coimbatore District
vanitha.v.cse@kct.ac.in

Ilakkiya B
PG Student Department Of Computer Science and Engineering,
Kumaraguru College of Technology, Saravanampatti, Coimbatore District
ilakkiyaboopathy@gmail.com

Abstract
A botnet is a collection of compromised nodes, due to mobile malware they are able to perform coordinated attacks. Mobile networks have been relatively isolated from the Internet, so there has been need for protecting against botnets. With the rapid development of computing and Internet access (i.e., Wi-Fi, GPRS and 3G) capabilities of smart phones, constructing practical mobile botnets have become underlying trend. This paper presents a comprehensive review that discusses the botnet problem, summarizes the previously published studies and provides these with a wide ranging discussion of recent works and solution proposals in the entire botnet research field. This paper also presents and also discusses a list of the prominent and persistant research problems that remain open.

Keywords: Botnet, Mobile Security, C&C Server, VPN, P2P

Introduction

A Botnets [1] is a set of computers that are infected by specific bot virus which gives an attacker (Botmaster) the ability to remotely control that set of computers. Most botnets are developed for an organized crime where doing targeted attack to gain money. The word Bot means that those victims controlled by coordinated attacker, and it derives from the word "robot". The figure 1 shows the basic architecture of mobile botnet. The attacks and threats on mobile devices come in various forms, such as viruses, Trojans, worms and mobile botnet [2].However; mobile botnets are more dangerous as they pose serious threats to mobile devices and mobile networks. In this research, [3] had defined a mobile botnets as a set of mobile devices that are infected by a specific malware or software without user knowledge. These infected devices communicate with each other by using a Command and Control(C&C) mechanism and controlled by an attacker called bot master. The botmaster controls a large scale of bots at different locations to initiate attack, and due to the complexity of internet, it can be hardly trace back. The infected mobile devices then can be used by botmaster to do a cyber-crimes or cyber attacks, such as sending spam message, interruption, Denial of Service (DoS) and collecting sensitive information which can be exploited for illegal purposes.

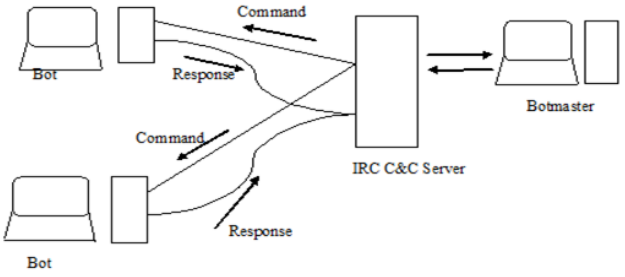

Fig 1: Mobile botnet architecture.

Basics of botnet

Botnet is available in different architectures like centralized, peer to peer, hybrid etc.

- Centralized architecture is the oldest botnet architecture and easiest to manage for botmaster. As name implies, the complete network is controlled from a central place and makes them easy to detect and stop.
- Peer to Peer (P2P) removes this drawback of centralized architecture. P2P architecture is difficult for bot master to manage but also hard to detect. It uses various C & C control servers. Bot master sends several commands to various bots and bots acts as C&C server for forwarding commands.
- Hybrid architecture is the combination of P2P and centralized architecture. In this architecture botmaster sends commands to the C&C servers which acts like P2P and communicate various commands amongst themselves .It also forwards commands to various bots under its control. Botmaster controls various C&C servers centrally. Data mining offers various techniques to extract, analyze, recognize and discover normal and abnormal patterns.,

- Correlation, classification, clustering, statistical analysis and aggregation techniques can be used for the detection of botnet [4].

Smart devices and botnet

One of the major problems that are faced in internet is malware. Amongst these malware, botnet acts as a big challenge for network security provider and security researchers. Various mischievous activities can be carried out by botnet like Distributed Denial of Service (DDoS) attack, spam mails and phishing websites. For smart devices spreading botnet is difficult as compared to PC-based network because of lack of public IP address, different types of connectivity, variety of operating system being used, availability of limited storage capacity and high communication cost.

The first generation of computer based botnets were established over Internet Relay Chat (IRC) servers and their relevant channels and then evolved to P2P and HTTP mechanisms [5].A Short Message Service (SMS) is commonly used to propose communication approaches because of the wide range of subscribers, ease of use, high availability. Although the existence of mobile botnet is expected, one of the first official report was released by the Damballa Research Laboratory. According to report, more than 40000 mobile devices were infected and were communicating through C & C servers for first six months of 2011. McAfee research lab determined that the cyber world (e.g. Mobile banking, social networking sites) will face more widely distributed cellular botnets which are difficult to detect and exterminate .The first mobile malware, called as Cabir, and was discovered in 2004. The first mobile botnet was discovered around July 2009, by a security researcher who found SymbOx. Yxes or SymbOS.Exy.C targeting Symbian devices using simple HTTP based C &C. Later the same year, a security researcher discovered Ikee.B which targets jail broken iphones by using a similar mechanism to SymbOS.Yxes. Gemini was first explored in China in December 2010 and considered as first Android botnet. Gemini steals the device's International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), GPS coordinates, SMS, contact list etc. and forward it to the botmaster. Following are the few reasons why cellular bots are attracting cyber criminals:

- There is increase in features and computational power of smart devices
- End users are not that much conscious about threats and risks involved in smart devices
- Use of applications that are available for free amongst end users
- Smart device helps to track the activities of its user
- Smart devices mostly operate on an open platform such as Android that encourages the cyber criminals to develop malware.

Characteristics of Android botnet

Mobile Botnet has the following characteristics. Due to the lack of IP addresses, mobile devices are connected mostly and are not directly reachable. These characteristics are used to detect botnets on android devices.

Repackaged Application

These applications are well known and legitimate but an attacker repackaged the original code with additional malicious code. A user installs the application without the awareness of additional configuration taking place on the device. This character is similar to that of Trojan horse and is the most common method to distribute botnet code.

Receiving Commands

An important characteristic of any bot is the ability to either receive command automatically or to prompt a remote server for the commands. The first option is to send the commands directly from a C&C server to the Android bots as needed. The other option is to allow the Android bot to contact the C&C server at regular intervals and ask whether new commands are available. This contact with a remote server is an absolute indication of an Android botnet.

Messaging

Current Android botnets are utilize SMS messages to gather money by sending messages to phone numbers at regular intervals.

Steal Information

Android botnets not only receive information from C&C server but also upload information about the infected device to the server.

Third Party Application Markets

Recently, Droid Dream Malware is an example for malicious application appeared for Android Markets.

Additional Content Downloaded

The latest characteristic of Android botnets is the ability to download additional content. This content, usually harmful in nature, aids and improves the performance of the botnet .The additional content is either downloaded dynamically by the application or a prompt asks the user to perform the necessary download.

AndroidManifest.xml File:Features and Permissions

Androidmanifest.xml File presents essential information about the particular application to the Android system [6].

Mobile botnet challenges

Following are considered as challenges in cellular botnet detection

- Cyber criminals are trying different techniques for developing botnet. Bot masters are employing various techniques for protecting bots from current botnet detection solutions.
- Cellular botnets are dynamic in nature, difficult to detect and flexible to update [7].
- Botnets can be spread through MMS /SMS, spam mails, Bluetooth or through other HTTP activities. This shows that botnet can be spread through

common communication medium like SMS/Bluetooth which makes them difficult to detect using current PC –Based solution.

- Cellular resources like CPU, battery life are limited on smart phones when compared with PC's. If the battery power consumption speed exceeds user expectations, the battery exhaustion is likely to be noticed by the user, leaving the bot opened to detection.[8]
- 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 smart phones.

Mobile botnet detection techniques

Push-Styled C&C Mechanism

The mobile bot is a general term of malicious software specifically for mobile communication devices. When it is infected by malware, a Smartphone becomes a mobile bot, and it connects to bot masters by sending the messages or links via Internet. These infected mobile bots are controlled by bot master to form a mobile botnet. In this, Push-Styled C&C is introduced, which utilizes Google Cloud Messaging (GCM) service as the botnet C&C channel .To reduce the cost and traffic consumption, an adaptive network connection strategy is applied in Push-Styled C&C mechanism, which use 3G cellular network and Wi-Fi and this is divided into four parts: concealing commands by the botmaster, pushing commands by GCM, adaptive network connection and command extraction by the bot .First, botmaster conceals commands for bots in the specific image with the information hiding technology. Then, bot master uploads the picture in the micro-blog or blog and record the URL of the image. Botmaster adds the specific flag at the end of URL of the image and pushes the processed URL to the corresponding mobile devices by GCM. Bot reads the message pushed by GCM and take appropriate adaptive procession.

VPN Mechanism

The authors have proposed the following requirement for an improved mobile botnet detection scheme

- Botnet detection scheme can detect botnet from various attack vectors.
- Botnet detection scheme can run without OS dependency.
- Botnet detection scheme can reuse the existing approaches.

To fulfill the requirements, the following three design goals are used in detecting mobile botnets.

Most mobile botnets have centralized architecture. The C&C channel link between bots and the C&C server is a unique link in the centralized botnet. We build a VPN between a mobile device and an IDS and it works in the same way as the wired network. That is, VPN provides the shared path for 3/4G and Wi-Fi traffic. It is almost impossible to inspect all attack vectors all the time because various attack vectors such as 3/4G, WiFi, Bluetooth and SMS are used for attacks. However, packets are periodically send while bots request commands to the C&C server. Their proposed scheme tries to detect botnet during the communication between bots and the C&C server.

C&C channel in centralized botnets has "pull" style control in HTTP or "push" style control in IRC. However, in mobile botnet, "push" style control is not useful because IP address of a mobile device changes repeatedly and "push" style control requires contiguous connection. Thus, they have detected botnet in the C&C channel which has "Pull" style control over HTTP traffic through 3/4G or Wi-Fi.

Design of SMS Commanded-and-Controlled and P2P-Structured Mobile Botnets

Host-based approaches that detect malware at runtime could also serve as a solution. Signature-based detection is effective but cannot handle unknown malware. They prefer use of behavior-based detection. Since bots send SMS messages stealthily without the user's involvement the detector could first utilize the normal process of sending SMS messages by a system call state-diagram and then keep monitoring the system calls that generate outgoing messages to see if there is any deviation from the usual behavior. In order to detect the incoming C&C messages, the detector needs to know the encoding scheme probably through binary analysis so that it can intercept and delete malicious messages before any application's access. However, the botmaster can apply advanced packing techniques to make the binary analysis harder, and periodically update the spam templates as well as the mapping between them and corresponding commands. In addition, host-level detection is susceptible to compromise by the malware, and consumes much resource. Deploying detection schemes at the SMSC is another possible solution. Compared to the host-level detection, this centralized approach can acquire a global view of all phones' SMS activities, although the information of each phone might be limited. As mentioned before, simply filtering out spam will not effectively cut off the botnet's C&C. The reason is that even if carriers dump spam-like SMS messages into a spam folder like email service providers do, spam messages will still reach target phones, stay at a less noticeable place, the spam folder and get commands executed.

Black-listing and SMS sending/receiving rate-limiting may be difficult because the design attempts to minimize the total number of messages sent/received and to balance the load on each bot. As always, matching signatures extracted from known bots' messages can be bypassed by malicious messages with completely new formats or contents. To differentiate between mobile bots and normal phones, the detector at the SMSC needs to extract more distinctive features from SMS traffic patterns. For example, normal phones may have regularities in whom they send messages to and the sending frequency [9]. The detector can therefore build normal profiles and identify anomalies accordingly. The detector may also adopt a high-level view for detection. As our botnet utilizes a P2P architecture [10], the resultant network topology stemmed from SMS activities may be different from that formed by benign phones, given the fact that P2P applications are rare in today's mobile phone networks.

Conclusion

Mobile devices are used by billions of people around the world. Sensitive data is stored on such devices, from contact lists, to passwords and credit card numbers. This paper presents an overview about mobile botnet, which can lift information from smart devices without knowledge of its users. In current situation , it is easy to infect smart devices than PC-based network. Mobile devices normally stay connected online all the time because of their default characteristics and user behavior. Thus, security threats on one network will affect the other network and this makes smart phones attractive targets to hackers. In this paper we have shown that there are potential profitable business model for exploiting mobile botnets .It is therefore necessary to start thinking about methods for reducing the threat of botnets on mobile networks. Future research includes the advance study of internal workings of current Android botnets and malware. The purpose of this survey is to explore the development and underlying structure of android botnets to aid the discovery process of such botnets.

References

[1] Norton. Bots and Botnets- A Growing Threat .Internet: http://us.norton.com/botnet/ , read: 01.01.2012.

[2] Eslahi,M., Salleh,R and Anuar,N.B., Nov, 2012, "Bots and botnets: An overview of characteristics, detection and challenges,"2012 IEEE Int. Conf. Control.Syst. Comput. Eng., pp. 349-354.

[3] LaPolla ,M., Martinelli,F and Sgandurra,D.,Jan.2012., "A survey on security for mobile devices, "IEEE Commun. Surv. Tutorials, vol. 15, no. 1,pp. 446 -471.

[4] IhsanUllah., Naveed Khan., Hatim A. Aboalsamh.,2013"Survey on Botnet: Its Architecture, Detection, Prevention and Mitigation", IEEE, pp 660-665.

[5] Auriemma,L.,"Samsung devices with support for remote controllers," http://aluigi.org/adv/samsux_1-adv.txt,26/04/2012.

[6] The Android Manifest .xml file, Android Developers, [online] 2012,http://developer.android.com/guide/topics/manifest-intro.html (Accessed: 19 March 2012).

[7] Juniper,2012.,"Trusted Mobility Index, " .

[8] GraigA.Schiller .,Jim Binkluy with GadiEvron, Carsten Williems, Tony Bradley, David Harley, and Michael Cross. Botnets: The Killer Web App. Andrew Williams, Syngress, 2007.

[9] Yan,G.,Eidenbenz,S., and Galli,E., "Sms-watchdog: Profiling social behaviors of sms users for anomaly detection," in Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID'09).

[10] Dittrich,D and Dietrich,S., P2p as botnet command and control: a deeper insight. In Proceedings of the 2008 3rd International Conference on Malicious and Unwanted Software (Malware 2008), Alexandria, VA, Oct 2008.