Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Mobile Botnet: A Threat to User Privacy

Mrs. Sonali Tidke
Computer Science and Engineering,
Shreeyash College of Engineering and Technology,
Aurangabad, *Maharashtra, India*

Abstract— Botnet is emerged as threat for cyber world. Cellular botnet is becoming new threat for network security professionals and researchers. Cellular botnet works like PC-based botnet but its detection is much more difficult than PC-based botnet because of various reasons like lack of public IP address, limited resources and battery life and varying operating system. Cellular botnet can infect smart devices using common communication medium like SMS/MMS, Bluetooth etc. This paper focus on architecture of botnet, why cyber criminals are focusing on smart devices for spreading botnet attacks and how to protect smart devices from such attacks.

Keywords— Botmasters, Botnet, Cellular botnet, command and control server, mobile malware

I. INTRODUCTION

Remarkable development in the features offered thru Internet, many users are connected to Internet day and night. With the abilities and facilities offered over cellular devices like smart phones, tablets, PDAs users are accessing them without any security. In the field of network security, main focus is given over PC-based network and their security. The latest research has reported that on average people own three smart-devices connected thru Internet [1]. This is a good reason to include smart devices in botnet attacks. A botnet consists of small malicious applications which infect different targets without attracting the users attention that subsequently communicate with each other by using command and control (C & C) servers[2]. The main difference between botnets and the other threats lies in the fact that they are dynamically controlled by a sophisticated attacker called botmaster [2]. Various elements of botnet include bots, C & C server and botmaster. All these components communicate with each other in a well organized format makes them difficult to identify and detect.

Cellular botnet, also known as mobile botnet, is a group of comprised smart devices which is controlled thru C & C server by botmaster. Cellular botnets are considered as less threatened of botnet compared to its counterpart PC – based botnet. The obvious reason is limited battery power, limited resources and different communication medium and not much research and development has been done on this field till last few years. This makes smart devices vulnerable for development of cellular botnet. Smart devices are now widely used by billions of users due to their enhanced computing ability, practicality and efficient internet access [3]. Smart devices are used to store and access personal and sensitive data like bank account details, net banking password management, online payment details etc. Also availability of free applications over smart devices makes them lucrative targets for cybercriminals and malware creators.

This paper mainly focuses on how to detect and avoid botnet infection on smart devices. Section II gives basics of various types of botnet architectures. In section III, paper gives relation between smart devices and botnet while section IV focus on detecting botnet and possible solutions over controlling them.

II. BASICS OF BOTNET

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

1. Centralized architecture is the oldest botnet and easiest to manage for botmaster. As name suggests, complete network is controlled from a central place and makes them easy to detect and stop.

2. Peer to Peer (P2P) removes this drawback of centralized architecture. P2P is hard to manage for botmaster but also hard to detect. P2P uses various C & C control servers. Botmaster sends various commands to various bots and bots acts as C&C server for forwarding various commands.

3. Hybrid is combination of P2P and centralized architecture. Botmaster sends commands to C&C servers which acts like P2P and communicate various commands amongst themselves. C&C also forwards commands to various bots under its control. Botmaster controls various C&C centrally. Data mining offers various techniques to extract, analyze, recognize and discover normal and abnormal patterns. Methods like correlation, classification, clustering, statistical analysis and aggregation techniques can be used for botnet detection [4].

III. SMART DEVICES AND BOTNET

One of the major problems in today's Internet is malware. Amongst these malware, botnet is a big challenge for network security provider and security researchers. Various malicious activities can be carried out thru botnet like Distributed Denial of Service (DDoS) attack, spam mails, hosting of malware 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, limited storage capacity and high communication cost.

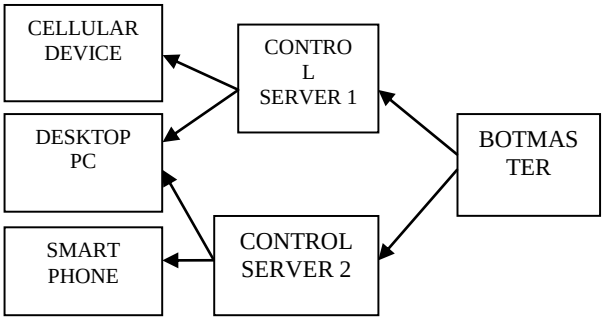

Fig. 1: Centralized Botnet

The first generation of computer based botnets were established over 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 [3]. Although existence of mobile botnets is anticipated, one of the first official report was released by the Damballa Research Laboratory [6]. According to report, more than 40000 mobile devices were infected and were communicating thru C & C servers for first six months of 2011. McAfee research lab predicted that cyber world (eg. Mobile banking, social networking sites) will face more widely distributed cellular botnets which are difficult to detect and exterminate [7]. In [3], it is mentioned that first mobile malware, known as Cabir, was discovered in 2004. The first mobile botnet was discovered around July 2009, when a security researcher found SymbOx.Yxes or SymbOS.Exy.C targeting Symbian devices using simple HTTP based C & C [8]. Later the same year, a security researcher discovered Ikee.B [9] which targets jailbroken iphones using similar mechanism to SymbOS.Yxes. Gemini was first discovered in China in December 2010 and considered as first Android botnet [3]. 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 few reasons why cellular bots are attracting cyber criminals [3]:

1. Increasing features and computational power of smart devices
2. Lack of awareness in end user about threats and risk attached to smart devices
3. Availability and use of free applications amongst end users
4. Each smart device helps to track activities of its user
5. Most smart devices operate on an open platform such as Android which encourages cyber criminals to develop malware

IV. DETECTION AND POSSIBLE SOLUTION

Various techniques are proposed and developed to identify botnet attacks. Botnet detection can be broadly classified into two categories like Structured Based and Behavior Based identification.

Structured Based Identification is divided into:

1. Signature Based Detection which is successful only for known botnets. Some authors used the list of IRC nicknames an applied n-gram analysis for detecting that whether it is from an infected bot or not [10].
2. In DNS Based Detection, bots use to send DNS queries to C&C. so DNS botnet can be detected by examining DNS traffic.

Behavior Based Detection is categorized into Anomaly Based Detection and Communication Pattern of Botnet.

The same techniques discussed above for PC based Botnet detection are not directly applicable to cellular botnets as there is much difference between development, spreading and implantation pattern of PC-based and Cellular botnets. Following can be considered as challenges in cellular botnet detection:

1. Botnet development topology: Cybercriminals are trying different techniques for developing botnet. Botmasters are employing various techniques for protecting bots from current botnet detection solutions.
2. Cellular botnets are dynamic in nature, difficult to detect and flexible to update [11,12].
3. Botnets can be spread thru MMS/SMS, spam mails, Bluetooth or thru other HTTP activities. This shows that botnet can be spread thru common communication medium like SMS/Bluetooth which makes them difficult to detect using current PC-based solution.
4. Limited cellular resources like CPU, memory, battery life impose another challenge for applying current botnet detection techniques on cellular botnets.

5. Compared to PC-based networks, smart devices are not properly protected by owners and no central security can be applied to them in current situation.

In view of above mentioned trends and challenges, a security solution is required specifically for smart/ cellular devices. As suggested by Hua et al. [13], a possible solution is design and development of special security managers like Honeyphones which are designed considering various characteristics of smart devices. Also Kok et al. [14] proposed a primitive central management model for cellular botnet detection called Anti-Botnet operation center. It consists of 4 different modules: analyzing, detection, mitigation and prevention. Also Vural et al. [15] discussed details about differentiating human and bot activities based on 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 serves to detect SMS- based mobile botnets [16].

For providing security to Android market applications, Google has added one layer of security by scanning applications before uploading. Google market can add certification process for applications which is currently not available. But still End users are required to decide whether an application is safe or not before downloading it. End users can take preventive measured like mentioned below:

1. Users should not rely only on operating system to protect themselves from attacks. Owners are supposed to use antivirus and anti- malware software on smart devices too.
2. They should install applications only from trusted sources developed by trusted developers.
3. Read and check default permission required by the application before installing.
4. Use up-to-date software and operating system.
5. Avoid accessing sensitive information over public networks which are not having password or encryption strategy.

Along with end users, Mobile Network Operators and service providers should also maintain some security policy for their customers. They can create a secure environment for customers by using proper and sufficient preventive measured to protect their users. Simultaneously, cellular app developers should take care while creating apps to use proper channels for communication between application and device related data. Also Android market/ Apple store should rigorously screen and review code before making them available for user.

V. CONCLUSION

This paper presents an overview of new threat for cellular world known as cellular botnet. Cellular botnet 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. The reason lies in the lack of knowledge about threats and risks by the end users, negligence of mobile network operators in providing security to its consumers and insufficient efforts by application developers and providers in providing security against malware development and detection. In this paper we are trying to provide information about risks of cellular botnet and basics of how to keep smart devices safe from cellular attacks.

REFERENCES

[1] Juniper, "Trusted Mobility Index," Juniper, http://www.juniper.net/us/en/local/pdf/additional-resources/7100155-en.pdf 27/02/2013 2012.

[2] 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.

[3] Abdullahi Arabo & Bernardi Praggono, "Mobile Malware & Smart Devices Security : Trends, Challenges and Solutions", 19th International Conferences on Control System and Computer Science, 2013, pp 526-531.

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

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

[6] Damballa. (2011). *First Half 2011 Advanced Threat Report*[PDF]. Available: http://www.damballa.com /downloads/ r_pubs /Damballa_Threat_Report_First_Half_2011.pdf

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

[8] A. Apvrille, "Symbian worm Yxes: Towards mobile botnets?," presented at 19th EICAR Annual Conference, Paris, France, 2010.

[9] P. A. Porras, H. Saidi, and V. Yegneswaran, "An Analysis of the iKee.B iPhone Botnet," presented at 2nd International ICST Conference on Security and Privacy on Mobile Information and Communications Systems (Mobisec), 2010.

[10] Jan Goebel, Thorsten Holz, "Rishi : Identify Bot Contaminated Hosts by IRC Nickname Evolution", Hotbots' 07 Proceedings of the first conference on First workshop on Hot topics in understanding botnets, ACM.

[11] Juniper, "Trusted Mobility Index," Juniper,http://www.juniper.net/us/en/local/pdf/additional-resources/7100155-en.pdf 27/02/2013 2012.

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

[13] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, T. L. Porta, and P. McDaniel, "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core," presented at ACM Conference on Computer and Communications Security (CCS), 2009.

[14] TrendMicro, "Security in the Age of Mobility," Trend Micro 2012.

[15] 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.

[16] Meisam Eslahi, Rosli Salleh, Nor Badrul Anuar, " MoBots : A New Generation of Botnets on Mobile Devices and Network", 2012 International Symposium on Computer Applications and Industrial Electronics (ISCAIE 2012), December 2012, pp. 262-266

