IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. II (May – Jun. 2015), PP 69-72
www.iosrjournals.org

Botnet Attack: Is it a risk for Smart Phones?

Sonali Tidke[1], Dr. Pravin Karde[2]
1Research Scholar, Sant Gadge Baba Amravati University, Maharashtra, India
2IT Department, Government Polytechnic College, Amravati, Maharashtra, India

Abstract: *With immense use of internet over smartphones, it is being a matter of concern for cyber security experts to provide security from ever growing threat of cyber attacks. The motivation of hackers behind developing malware is shifted from joy to a profit earning market. Amongst various forms of malware, mobile based botnet is emerged as a new threat for cyber security experts. Mobile based botnet attacks are increasing day by day and smartphone users are unaware about the harm it can cause. Considering this, the paper gives an overview of working and propagation of mobile based botnet attacks. Common propagation medium of smartphone based botnet are SMS, Bluetooth, NFC and WiFi. The paper proposed a hybrid P2P system for creating botnet using WiFi.*

Keywords: *Botmaster, C & C server, NFC, Hybrid P2P*

I. Introduction

As smartphones become powerful, they are being appealing target for cyber attackers. Most of the top selling smartphone platforms are based on common PC based operating systems. This makes transition of PC based malware to smartphone based malware easy. Though smartphone malwares are not very common, in near future, it will be as common as PC based malware.

A study shows that on an average, each user is having three smart devices. Users are storing sensitive information like bank account numbers, passwords, credit card details or other personal details on smart devices. Besides this, corporate users are storing corporate details too on smart devices. All this information is usually used for making online transactions or other sensitive transactions. The wide spread use of open-source operating platforms and availability of third-party applications also provides more opportunities and attractions for malware developers.

Typical botnet consists of three main elements - Bots, Command & Control (C & C) servers and Botmaster. Once botmaster get access of a device, it can control all its activities using C & C server without knowledge of user. C & C server spreads attacks to different devices and creates network of bots. Like parasite, botnet works on computing power and bandwidth available on infected hosts [1].

Users generally assume that everything related to smartphone will work just as it should and relies on a device's default settings. It makes them weakest link in security and easy target for cyber criminals. The use of mobile devices by health care professionals (HCP) is increasing day by day. Numerous apps are available now-a-days to support HCP. HCPs require access to many types of resources in a clinical setting, including voice calling, video conferencing, text, and e-mail, maintaining electronic health records, electronic medical records, clinical decision support systems, picture archiving and communication systems etc. If these devices are compromised not only will the information and privacy of the user of the device be compromised, but the attacker can even change the settings of the devices, which could lead to harmful consequences. It has been shown that hackers can hack wireless pacemaker and read the details of data stored in the device or make changes in them to harm patient.

Botnet can be implemented using various sizes or architecture with same stages of lifecycle like Infection and Propagation, Rallying, Commands and Reports, Abandon, Securing the Botnet [2,3].

II. History Of Mobile Botnet

The first generation of computer-based botnets, were established over IRCs and then evolved to P2P and HTTP mechanisms. While it is difficult to implement a wide variety of C&C models for mobile based botnets due to the lack of public IP addresses, availability of variety of operating systems, different types of connectivity mediums and the cost of communication.

Cabir [4, 5, 6, 7] was the world's first mobile worm appeared in 2004. Cabir was designed to infect the Nokia Series 60. Its attack resulted in the word "Caribe" appearing on the screen of infected phones. Fortinet discovered SymbOs.Exy.A/Yxes [2, 4, 6], appeared in early 2009, is a piece of malware behind the seemingly legitimate "Sexy View" application. DroidKungFu/DroidDream [4, 8], emerged with several unique

characteristics, and even today is considered one of the most technologically advanced viruses in existence. This is activated silently and at night (11 P.M. to 8 A.M.) when the mobile's users are asleep [8].

Plankton[9] discovered in 2011 and is still one of the most widespread Android malware. 2013 marked the arrival of FakeDefend, the first ransom ware for Android mobile phones. This malware works in a similar way to that of fake antivirus. It locks the phone and requires the victim to pay a ransom in order to retrieve the contents of the device. The year 2014 starts with the formation of new mobile malware like 'Android.HeHe', with the ability to steal text messages, intercept phone calls, and other malware such as 'XXXX.apk' uses WiFi networks or hotspots to steal information, infected more than 24,000 Devices.

In 2010, Internet crime loss by individuals totaled $560 million. Phishing alone resulted in $120 million per quarter. A Symantec-commissioned StrategyOne report found that 65 percent of computer users have spent 28 hours and $300 dealing with cybercrime; McAfee estimated a $1 trillion global cost. A single botnet ring took $100 million before the FBI managed to stop it. The UK government estimates that each year the country loses 27 billion to cybercrime, which extrapolated to the US population and converted to dollars would be approximately $210 billion. The UK's response will be 650 million for cyber security. A few years ago, Consumer Reports gave a relatively low number for US cybercrime loss-$7 billion over two years, whereas The Washington Post suggested a cost of $105 billion per year. Another large study estimated that cyber fraud and the like cost between 0.2 percent and 0.4 percent of global GDP, or approximately $100 to $200 billion [10].

III. Mode of communication and propagation

Botnet uses various types of architectures to control network and to be invisible from detection i.e. Centralized Botnet Architecture, Peer to Peer Botnet Architecture (P2P), Hybrid, and Combination of Hyper Text Transfer Protocol with Peer to Peer (HttP2P). The first architecture is not very secure but easy to implement while the second architecture is hard to detect as well as hard to manage, whereas Hybrid and HttP2P are combination of first two and used for bypassing firewalls and intrusion detection mechanism.

There are several methods and techniques that have been used to track botnet activities and detect them such as signature-based detection, honeypots, analyzing the DNS traffic and behavioral analysis (e.g. active and passive).Various Tools available for Botnet detection includes DE – Cleaner by Kaspersky, Avira DE-Cleaner, RuBotted, Norton Power Eraser. Several communication medium for spreading Botnet command includes:

Bluetooth: Amongst various devices, Bluetooth is a way to send or receive data between two or more devices. Bluetooth device ask for permission before connecting with other Bluetooth device. For spreading botnet commands through Bluetooth, it is necessary to connect Bluetooth without asking for permission. This can be achieved by Bluetooth hacking. Su et. al highlighted the presence of a diverse set of known security vulnerabilities in the Bluetooth protocol's implementation [11]. Botnets like Cabir,Mabir and CommWarrior have already exploited vulnerabilities available in Bluetooth Protocol.

SMS: Similarly, SMS can be used as communication medium for spreading Botnet attack. SMS is a very common medium used to propagate bot commands because of wide range of subscribers, ease of use, and high availability. Kademila and Gnutella are two peer to peer models where SMS is used as mode of propagation for mobile botnet. Singh et al.[8] has adopted both SMS and Bluetooth to implement a communication model between pre-selected mobiles and the botmaster. But the failure point of this model lies with Bluetooth requirement. Bluetooth needs permission to receive data and accordingly commands which are sent by the update nodes [8].

NFC (Near Field Communication) : It is a set of standards for mobile devices designed to establish radio communication with each other by being touched together or brought within a short distance. Although the communication range of NFC is limited to few centimeters, it can be used as medium of attack propagation.

WiFi: WiFi gives several advantages over other communication mediums available to mobile botnets. As compared to cellular communication channels like 3G/4G or SMS/MMS, botnet activities over WiFi network are difficult to detect and more discrete. Mobile devices connect to cellular network through non spoofable mobile ID which makes them easy to detect and shutdown if they participate in bot network. This is in contrast to a WiFi botnet where IPs can be spoofed and malicious activity hidden behind many different open networks and NAT routers, where it is difficult to mitigate.

IV. Motivation

Mobile botnet attacks on cellular networks and devices have recently grown in number and sophistication. With the rapidly-growing popularity of smartphones, such as the iPhone and Android-based phones, there has been a drastic increase in downloading and sharing of third-party applications and user-generated content, making smartphones vulnerable to various types of malware. Security wise and financial charge wise, lots of research is required in this field.

So the main aim of the proposed research work is to enhance the security of mobile services by analyzing several security issues in accessing mobile services. This research work is mainly focused on safeguarding mobile phones from ever growing and varying technologies of botnet attack.

V. Proposed Methodology

PC based botnet attacks are now known to the world and like other malware and spam activities, anti malwares are available to monitor and detect them. But considering the scenario of mobile based botnet attacks, it is still very new and unknown to the world of cyber users. Smart phone users still blindly trust on applications and default settings of smart devices and are using them without knowledge of risk associated with it.

Though mobile botnet is a pretty new concept for users, it is not much known to cyber researchers too. Research work on mobile botnet is still in the initial stages of detecting and stopping them from propagation. Though researchers are developing various ways for detecting botnet, not a guaranteed technique is provided to stop propagation.

Botmaster can be either a smart phone or a PC.

1) Hybrid P2P Architecture for C & C Server: Centralized architecture is easy to implement and detect while P2P is difficult to detect and implement too. In this research we are using Hybrid architecture for developing botnet. Following figure shows architecture of botnet. Here botmaster can be either a smart device or a desktop PC which will work in isolation to avoid detection. Botmaster maintains a list of C & C servers and gives commands to propagate to bots. Botmaster need not required to be infected device.

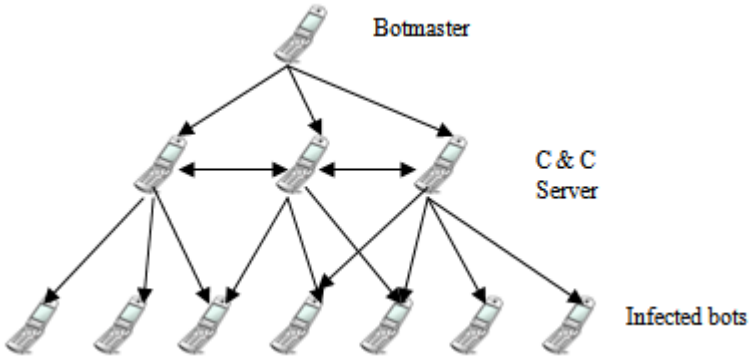

Figure 1 : Hybrid P2P architecture for C & C Server

C & C servers gets commands from Botmaster or from peer C & C server and maintains a list of infected devices. After a particular duration, Botmaster can remove C & C server from its list of servers to avoid detection. Infected bots can also work as C & C server if required.

2) WiFi as medium of propagation: SMS and/or Bluetooth are commonly used as medium of propagation of bot attacks. Bluetooth can provide the necessary stealth required for developing C&C server but it cannot function as a medium for other botnet activities like DDoS attacks. Furthermore, due to its limited range and transmission rates, a large number of identically infected, slowly moving, devices must continuously come in close proximity to one another to be effective. This is not suitable for newly emerging botnets, where infected devices may be few and geographically dispersed. Similarly, SMS can be detected early as each SMS carries carrier charge. Though researchers were using SMS as medium of propagation, its use is very limited and can be detected during early stage of propagation.

In contrast, WiFi botnets can achieve faster transfer speeds, support multiple botnet activities, and be incrementally deployed with less effort; a small WiFi botnet, even when spread across multiple cities, can immediately contributes to an existing botnet, unlike Bluetooth. In WiFi IPs can be spoofed and malicious activity can hide behind many different open networks which makes them difficult to detect.

APPLICATION LAYER
BOT
MODEM DRIVER SERIAL LINE
GSM MODEM

Figure 2: BOT implementation

3) Implementation of Bot: The telephony stack of a smartphone handles communications between the GSM modem an the application processor. Naming conventions and implementation differ from platform to plaform

but usually a multiplexing serial line modem driver that translates instructions between application API calls and GSM modem AT commands[12]. The Bot layer can be inserted between application layer and modem driver serial line layer as shown in figure 2.

VI. Conclusion

With extensive use of smart devices, security is being a major concern for cyber researchers and security experts. Mobile attacks are tough to detect as compared to desktop computers because of variety of mobile architectures. There are many security threats to smart phones from the data arriving via SMS, MMS, downloaded executable files or over Bluetooth, NFC, WiFi etc. The botmasters are designing bot commands considering all this along with special characteristics of mobile phones like limited memory, limited battery life and low security. Botmasters are changing methods used for creating network attacks making them more challenging for detection.

Mobile phones are used everywhere from trading on financial markets and mobile banking to carrying medical records, providing health treatments, in weather forecasting to educational institutes etc. Though, every sector is not in need of strict security but every application needs security up to some extent. Many users are using online banking through mobile applications while based on mobile medical diagnosis, patients are treated. If bot attacks on such mobile devices, it can create severe threats for the users and service providers. Considering all these applications, securing mobile phones is a challenging job for researchers.

References

[1]. Suresh Ramasubramanian, "ITU Botnet Mitigation Toolkit Background Information", ICT Applications and Cybersecurity Division, Policies and Strategies Department, International Telecommunication Union, Geneva, Switzerland, January 2008.
[2]. Meisam Eslahi, Rosli Salleh and Nor Badrul Anuar,"Bots and Botnets: An Overview of Characteristics, Detection and Challenges", IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, pp. 349-354, 23 – 25 November 2012.
[3]. Ihsan Ullah, Naveed Khan and Hatim A. Aboalsamh, "Survey on botnet: its architecture, detection, prevention and mitigation", IEEE Transactions, pp. 660 -665, 2013.
[4]. Abdullahi Arabo and Bernardi Pranggono, "Mobile Malware and Smart Device Security: Trends, Challenges and Solutions", 19th International Conference on Control Systems and Computer Science, IEEE Computer Society, pp. 526-531, 10 – 11 September 2013.
[5]. Joany Boutet and Lori Homsher, "Malicious Android Applications: Risks and Exploitation, How I Met All Your Friends, A Spyware story about Android Application and Reverse Engineering", Information Security Reading Room, The SANS Institute, pp. 1 – 5, 2 March 2010.
[6]. Phillip Porras, Hassen Saidi and Vinod Yegneswaran, "An Analysis of the iKee.B iPhone Botnet", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 141- 152, 2010.
[7]. Guining Geng, Guoai Xu, Miao Zhang and Yixian Yang Guang Yang , "An improved SMS based heterogeneous mobile botnet model", Proceedings of the IEEE International Conference on Information and Automation, Shenzhen, China, pp. 198-202, June 2011.
[8]. Meisam Eslahi, Rosli Salleh and Nor Badrul Anuar, "MoBots: A New Generation of Botnets on Mobile Devices and Networks", International Symposium on Computer Applications and Industrial Electronics (ISCAIE 2012), IEEE, pp. 262-266, 3 – 4 December, 2012.
[9]. Jing Liu, Yang Xiao, Kaveh Ghaboosi, Hongmei Deng and Jingyuan Zhang, "Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures", Hindawi Publishing Corporation, EURASIP Journal on Wireless Communications and Networking, 19 July 2009.
[10]. H Pieterse and M Olivier, "Design of a hybrid command and control mobile botnet", International Journal of Information Warfare, Vol. 12, Issue 1, May 2013.
[11]. J. Su, K. Chan, A. Miklas, K. Po, A. Akhavan, S. Saroiu, E. Lara, and A. Goel. A Preliminary Investigation of Worm Infections in a Bluetooth Environment. In ACM Workshop onRecurring Malcode (WORM), Alexandria, VA, Nov. 2006.
[12]. Transparent Botnet Command and Control for Smartphones over SMS,Shmoocon 2011,Georgia Weidman.