Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 3, pp: (17-22), Month: September - December 2016, Available at: www.noveltyjournals.com

Research of the Command and Control Based on Mobile Botnet

Gao Jian

People's Public Security University of China, China, BeiJing

Abstract: **This paper describes the current status and trends of the development of mobile botnet. Mainly on mobile botnet functionality and harm are summarized. The detection method from the type of attack, attack target, operation platform, communication mechanism, exploits and other aspects of the classification, at the same time the mobile botnet command and control channel was studied, focusing on the SMS, SMS-HTTP and SNS types of communication are analyzed.**

Keywords: **Mobile Botnet; Command and Control; DDoS; Detection; Malware; Bot.**

I. INTRODUCTION

In recent years, the rapid development of the field of mobile Internet technology, smart mobile devices due to the growing popularity of the price trend. Since the date of the birth of smart phones, not only with the amazing speed of development of a long time to go through a long time of the traditional computer software and hardware upgrades, but also has been in the rapid development of. All the signs indicate that the mobile terminal thanks to its perfect function and portability of the obvious advantages, and gradually replace the traditional computer, has become the daily life of ordinary users of the center. On the basis of the thirty-fifth "China Internet Network Information Center in February 3, 2015 released by the development of Chinese Internet Statistics Report" statistics, until the end of 2014, the use of mobile devices for Internet network connection has now reached 557 million people, compared with the end of 2013, an increase of 56 million 720 thousand. Among Internet users, the number of people who choose to use mobile phones to surf the Internet has increased from 81% in 2013 to 85.8%. Mobile network's influence is evident, but it should be noted that it is not only a more convenient network of life, as there are serious challenges from the mobile security.

In the threat of these mobile security areas, mobile botnet brings a great security threat. Compared with the traditional computer, the use of mobile devices closer to the user's daily life, mobile devices to store a large number of communications, transaction records and other users of personal privacy information. In addition, mobile devices, touch screen, motion sensor, optical sensor in the process of operation is also stored in the fingerprint, location information, health and many other traditional computer to obtain personal information, these sensitive information can not only be used as advertisers directional on the advertising reference, can also be used as criminals for tracking crime support. By selling personal information, the attacker will get a huge mobile botnet investment returns. In view of the above reasons, the mobile botnet to mobile users of personal privacy security will pose a greater threat and harm. At the same time, the DDos attacks based on mobile botnet are more subtle and great social harm to the key components of telecommunication network and the call center.

II. MOBILE BOTNET FUNCTION STRUCTURE AND WORKING MECHANISM

With the market share of smart phones and handheld devices continue to rise, attacks against mobile terminals in an endless stream. At present, the purchase amount of PC computer is declining year by year, the latest statistics, since 2011, the global mobile phone shipments have been greatly exceeded the [1] computer PC. In the near future, 4G and 5G mobile communication technology in the growing popularity of mobile communications will become the main way of public broadband Internet access. From 2012 to 2013, 4G mobile devices accounted for only 0.9% of the global mobile device connectivity, and its traffic data accounted for 14%[2] of all traffic data.

The transformation of this technology, so that the attacker began to exploit the vulnerability of intelligent devices to develop malicious software tools to conduct cyber crime. However, the mobile terminal based malware also encountered in the development of the platform of their own restrictions, such as limited processing ability, limited memory function, heterogeneous and operating system (such as: IOS, Android and Windows Phone).

Table I describes some of the common features of the mobile botnet. These include the spread of worms and viruses, stealing confidential and private information, sending spam, unauthorized root access, illegal telephone broadcast, unauthorized access, DDoS, power consumption and memory consumption, etc..

TABLE: I Mobile Botnet Attacks

Attack Type	Description
Sending Emails	Mobile Bot Send a large number of spam to other terminal
Sending MMS/SMS	Mobile Bot Send a large number of MMS/SMS to other phone
Spyware	Mobile Bot can collect personal information
Privacy Issues	Privacy information can be leakage.such as credit card number,phone number list.
DDoS	Mobile Bot can be used to send a large number of stream to target website.

The latest data statistics, in the smart phone industry, Android operating system has accounted for 84.8% of the world's share from 2012 to 2014. Data in Table II shows that by August 2015, the market share of the smart phone system. From the table can be seen that more than 80% of the mobile phone using the Android operating system, and the current mobile phone malware is mostly targeted at the platform.

TABLE: II Mainstream Platform Market Share

Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%
2014Q2	84.8%	11.6%	2.5%	0.5%	0.7%
2013Q2	79.8%	12.9%	3.4%	2.8%	1.2%
2012Q2	69.3%	16.6%	3.1%	4.9%	6.1%

III. THE DIFFERENCE BETWEEN PC AND MOBILE BOTNET

Compared with the traditional PC Botnet, the design of mobile botnet has many limitations, and it is easy to be detected. Mainly embodied in two aspects of resources and communication, according to the description of the document [3], the main constraints are:

1) Power consumption;

2) The application of the cost of the application;

3) Communication costs;

4) Communication complexity.

Battery energy consumption is one of the biggest characteristics of the mobile terminal[4], when the program running on the phone power consumption is too much, it is easy to be found by the user or the detection software. The same traffic flow is also an important part of the detection of mobile zombies, if the use of excessive network traffic zombies, this abnormal behavior will be detected. There is a big difference between the topology of the mobile botnet and the traditional Botnet, and it is also a hot spot to maintain the persistence of communication.

Mobile botnet communication architecture and traditional botnet is similar, including IRC based, HTTP based and P2P based network, communication also includes SMS, Bluetooth, MMS, etc.. Figure 1 shows the basic architecture of a mobile botnet. First, the attacker to create malicious mobile APP, and released to the APP market through the network, when the mobile users to download and install these applications, they were infected and joined the botnet.

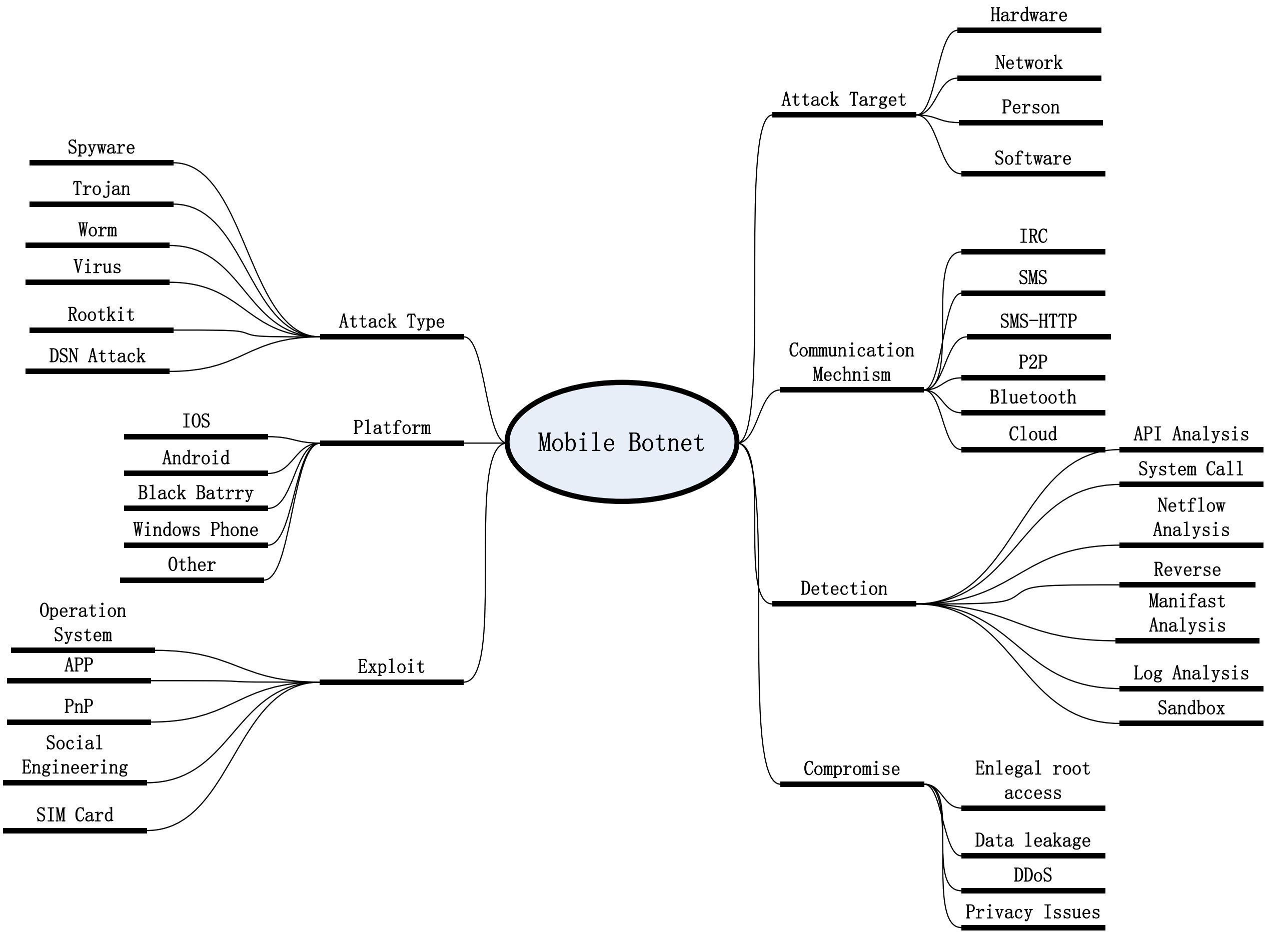

FIGURE I: Mobile Botnet Feature Classification

IV. MOBILE BOTNET COMMAND AND CONTROL MECHANISM

Different mobile bots and ordinary mobile virus is his remote control features, and command and control mechanism, but also can be said to be CCC (Command&amp;Control Channel, the command and control channel), is the key part to realize the remote control of mobile Botnet[5][6], its concealment, connectivity and robustness for the zombie network availability is crucial. It includes the topology of command control mechanism, the network communication protocol and communication algorithm, and the various software and hardware resources used by the attackers.The following will introduce the three main types of command control mechanism.

A. Command and Control Mechanism Based on SMS:

Short Message service (Short Message Service, referred to as SMS), is a text or digital message to mobile users using a mobile phone or other communication devices directly sending or receiving the mobile users a SMS message to receive and send messages to the number of characters, must be less than or equal to 160 English character or numeric characters or 70 characters Chinese. SMS is a kind of storage and forwarding service. This means that the SMS message is not sent directly from the SMS message to the SMS message receiving end, and need to be forwarded through the SMS service center. If the SMS message receiving end is offline (it may be a mobile device shutdown), the message will be sent on the receiving end of the line. In addition to mobile devices such as mobile phones, there are other ways to send SMS messages, for example by extending the Short Message Entity ESME (External). Short message value-added service, which is used by telecom operators, is a kind of ESME, which uses EMSE to send messages to mobile devices through the SMS service of the network.

Different from the traditional Botnet, mobile equipment can not be sustained and stable access to the Internet, so Short Message service as the communication mode of mobile terminal specific, SMS message can delay the reception characteristics of zombie hosts in order to maintain good connectivity between the control and the zombie host, so it is widely used in mobile botnet the command and control channel. For example, Geng Guining et al proposed a heterogeneous mobile botnet model based on SMS, using the SMS device of infected bots with broadcast command control messages, and by the features of mobile cellular network to launch DDos attacks, affecting normal mobile services.

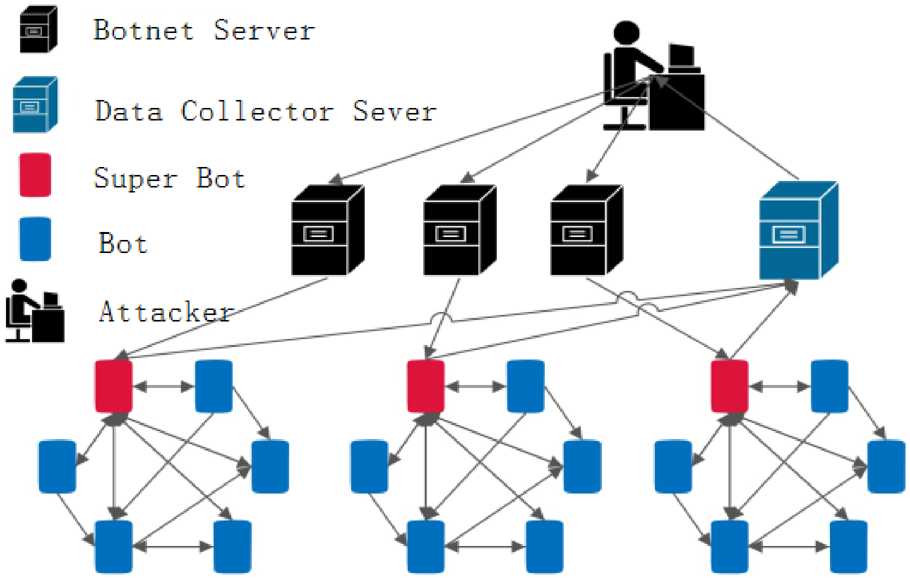

FIGURE II: Mobile Botnet Model Based on SMS

The topology of mobile botnet model SMS as shown in Figure II based on it by an attacker, the attacker node and node directly connected to a plurality of Botnet server nodes, an information collection node and uses the P2P structure to connect a plurality of regional network server nodes and zombie zombie nodes.

When the attacker sends control command message, the message is first disguised, hidden in the user easily overlooked spam and advertising SMS messages. And then broadcast the way through the server to send and zombie nodes sent each other way to send to the zombie node. Installed in the zombie nodes of the zombie program will scan SMS messages, and find the attacker to send commands to control the message, the attacker expected to attack, upload and download data, etc.. Lost in the server node, the botnet attacker can delete node failure, and specify another zombie node to the server, this move to ensure the zombie network connectivity, improves the robustness of the botnet.

B. Command and Control Mechanism Based on SMS-HTTP:

SMS-HTTP mobile botnet model is based on the SMS, the use of HTTP services for data upload and download. Hypertext Transfer Protocol (HyperText, Transfer Protocol HTTP) is the most widely used network protocol on the traditional Internet. All WWW files must comply with this standard. With the rapid development of mobile network technology, the HTTP protocol and other traditional computer network protocol support is increasing, in the WiFi environment, the mobile terminal is equivalent to the traditional computer. At the April 14, 2015 meeting, Li Keqiang put forward to increase the construction of mobile information infrastructure, improve the bandwidth of mobile internet. With the development of the attention of government departments and 4G network technology, mobile network communication ability will be more and more close to the traditional computer, in the user experience at the same time, BOT command and control messages to upload and download data will also be hidden in a large number of data packets in the network, it is difficult to trace, greatly enhance the mobile botnet concealment. For example, Mulliner et al. Proposed a command control channel based on SMS-HTTP hybrid protocol. The basic principle is that the control will be encrypted and signed by processing the file containing the control command upload to the web server, and then through the SMS to send the URL containing the corresponding file to the zombie phone.

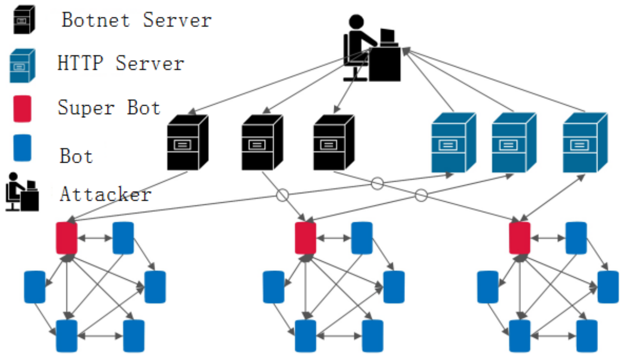

FIGURE III:　Mobile Botnet Model Based on SMS-HTTP

The topology of mobile botnet model SMS-HTTP as shown in Figure III based on it, in addition to SMS based mobile botnet model structure of the same node, and the attacker attacker nodes directly connected a plurality of Botnet server nodes, using P2P structure for connecting a plurality of regional botnet server nodes and the zombie nodes, and HTTP server as a zombie node node upload and download data.

In the execution of a command control message, the attacker first will command control information hidden in the HTTP page, and then URL hidden in the text messages sent by SMS to the zombie node. Zombie node of the zombie program to complete the interception of information, read, scan the HTTP page in the command and control messages and the implementation of the corresponding operation. After the completion of the instruction, the zombie node will complete the deletion of information, to avoid tracking anti-virus software. In addition, the same as the SMS based mobile botnet is, when the server nodes lose their role, but also the way to ensure the connectivity of the node to ensure the connectivity of the botnet.

C. Command and Control Mechanism Based on SNS:

Social network services (SNS, Social, Network, Service) is developed on the theoretical basis of six degrees of separation theory. Mainly based on the Internet, to provide personal data recording and communication links between users, the user retrieval service for a group of like-minded people, for social communication, contact activity platform. Through SNS, users can easily get to know new friends, and even international friends, to expand the communication network. SNS users can also through the release of micro-blog, log and so on, and like-minded friends to maintain a more long-term, direct contact. From the early start of the online chat room, the major SNS platform in recent years, rapid development, and excellent adaptation to the mobile network and mobile devices, the development of a stable, functional and perfect APP products. Today's social network mainstream SNS platform mainly domestic micro-blog, sina renren.com, Tencent QQ, WeChat and foreign Facebook, Twitter.

In SNS rich user's social life, but also brings personal information security risk of damage and personal privacy leak. SNS based mobile botnet is on the basis of HTTP connection, take the command control mechanism based on SNS. Because there is a high degree of trust between SNS users, SNS users are not infected with the SNS friends have been infected with the zombie program to deceive the friends of the poison, such as the operation of the toxic connection, so as to infect zombies.

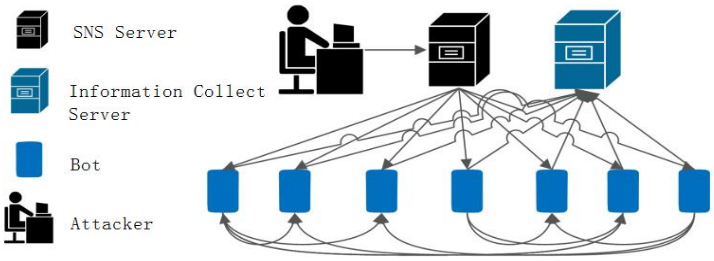

FIGURE IV:　Mobile Botnet Model Based on SNS

The topology of mobile botnet based on Figure IV is shown in figure SNS, which is mainly composed of an attacker node, a social application server, an information gathering node and a number of zombie nodes. Overall, it uses SNS communication as the main command control channel, and SMS communication to ensure the connectivity and robustness of the botnet.

The attacker first set up a SNS server or on the existing SNS server attack control, and then use the proprietary command control server SNS server control[7], control commands generated information hidden in the information network communication with SNS users, SNS users to send fraudulent information, control the upload and download of data such as operation to SNS friends.

V. CONCLUSION

Botnet is a very serious security problem in the traditional Internet industry, the mobile terminal to expand it to make it more flexible and hidden. At the same time, the characteristics of remote control also make the mobile botnet is different from ordinary mobile viruses, compared with them, mobile botnet has a higher operating efficiency and greater social harm. In this paper, the definition of mobile botnet and the command control mechanism are studied, and three kinds of mainstream mobile botnet are studied, and their topology structure and working mechanism are analyzed.

Mobile botnet is gradually becoming the biggest security threat to the mobile terminal, which needs more and deeper research. At the present stage, the research of mobile botnet is still a lot of research on the control command mechanism. Because of the characteristics of mobile Botnet, it is difficult to study and test the scale, makes the research on mobile botnet propagation model and the transmission characteristics of small, lack of detection, timely and effective countermeasures and the appraisal rating of the reasonable plan, the situation is still very passive defense. Future research in the field of mobile zombies should pay attention to the above issues, the problem of mobile botnet to put forward a better solution.

REFERENCES

[1] Abdelrahman O H, Gelenbe E, Görbil G, et al. Mobile Network Anomaly Detection and Mitigation: The NEMESYS Approach[J]. Lecture Notes in Electrical Engineering, 2013, 264(8):429-438.

[2] Arbor Networks: Worldwide Infrastructure Security Report (2012), https://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/4737-the-arbor-networks-8th-annual-worldwide-infrastructure-security-report-finds-ddos-has-become-part-of-advanced-threat-landscape

[3] Google Inc. Android Cloud to Device Messaging Framework.http://code.google.com/android/c2dm.

[4] Apple Inc. Local and Push Notification Programming Guide.http://developer.apple.com/library/mac/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/RemoteNotificationsPG.pdf, 2011.

[5] Microsoft Inc. Push Notifications Overview for Windows Phone.http://msdn.microsoft.com/en-us/library/ff402558(v=vs.92).aspx.

[6] Reserach In Motion Inc. Blackberry push service.http://http://us.blackberry.com/developers/platform/pushapi.jsp.

[7] Zhao S, Lee P P, Lui J, et al. Cloud-based push-styled mobile botnets: a case study of exploiting the cloud to device messaging service[C]//Proceedings of the 28th Annual Computer Security Applications Conference, 2012: 119-128.