The Research of Control Mechanism in Mobile Botnet

Tao Liu [a], Kai Zhu [b]

School of Electrical and Electronic Engineering, North China Electric Power University, Baoding 071000, China

[a] ltwin211@126.com, [b] kaigev520@163.com

Keywords: mobile botnet, CCC, attack models, control commands.

Abstract. With the rapid development of mobile communication technology, mobile botnet comes into being which gives mobile users a great threat. The botnet hacker issue orders through the command and control channel to let the bots launch attacks to gain significant economic benefits. Based on this, this paper puts forward three kinds of SMS-HTTP -based mobile botnet attack models, including bots automatically dial telephone, stealing messages, telephone DDOS attacks. At the same the article also designs the appropriate control commands and makes a detailed specification. In the end we discuss the corresponding defense against mobile botnet.

1. Introduction

With the rapid development of the mobile communication technology, mobile terminal technology and mobile operating system, mobile Internet[1], smartphones have more powerful computing ability, easier ways to access network and larger storage, which creates conditions for the emergence of mobile botnets. So far, there have been multiple rudiments of mobile botnets, which cover current popular platforms. In 2009, SymbOS. Yxes [2] Trojans found on the Symbian operating system have similar behavior patterns like the computer platform, mobile botnets Ikee B[3] for the jailbreak iPhone also appears in people's vision, Schmidt[4] puts forward the feasibility of constructing Android platform for mobile botnet. Reference [5] predicts that Android will most likely become the target of large-scale mobile botnet.

Unlike traditional botnets, whose bots are mainly PCs, mobile botnets [6-9] are composed of various mobile terminals, such as smartphones and tablets. Botmasters establish a controllable smartphones group by propagating malware and then publish commands to control them to launch a series of attacks, which poses serious threats to the privacy and property security of smartphone users.

Based on the research of botnet control pattern, we study the propagation, control and attack of botnet spreading on the smart phone platform. The second chapter focuses on the overview and analysis for control command mechanism in mobile botnets; the third chapter we design three mobile botnet simulated attack models combining with botnet features; In the end, we give the corresponding defense strategies against mobile botnet.

2. Control command mechanism in mobile botnet

2.1 mobile botnet control flow

In order to make people clearly know how botmaster control bots remotely. We first introduce mobile botnet integral control process as Figure 1 shown below:

In the control terminal, Botmasters accomplish the deployment of control command by controlling the terminal interface, then transmit commands through the command and control channel (C&C) to the compromised bots. After receiving the control commands, they will parse out the control commands right away and execute malicious attacks that Botmaster gives. In the end, bots deliver the information of data and device to the Botmaster through the recovery channel, the Botmaster will see the corresponding information at the terminal interface.

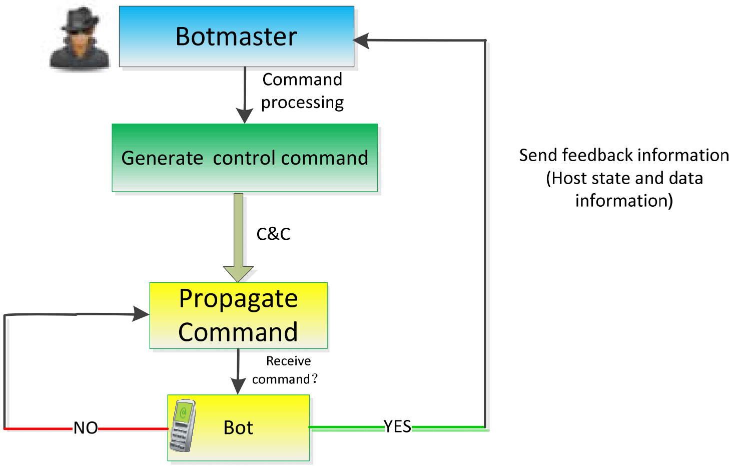

Fig. 1 mobile botnet control flow

2.2 Control command generation

With the growing popularity of smart phone applications, text messaging has become an important part of our daily lives, as a voice communication complement, short message service (SMS) has quick, clear, low-cost, reliable features. With the further development of messaging applications, adding control command information in a text message quietly becomes a trend.

Let us put an SMS message containing control command called control messages, which uses SMS to control the phone. Currently it's a popular method to hide the control command into text or picture, then send to the controlled phones. After verification, they parse the control command, and then start the appropriate processing module implementing the specified function. We design three mobile botnet simulated attack models such as automatically dialing the telephone, SMS steal, phone DDOS attack to allow people to well understand the process of botnet attacks.

Based on this, we propose a method to generate strong robustness control messages, the main idea is to give control command plaintext many complex processing, making it difficult to be analyzed and finally sent to bots via SMS. To achieve the goal, we take the following approaches to generate a control command.

Encryption you can achieve the purpose of hiding commands through encryption and you can use a variety of encryption methods, here we use symmetric encryption algorithms-DES algorithm. In order to increase the difficulty of cracking, we have adopted a one-time pad method, encrypt keys are randomly generated each encryption and join them into a text message.

Encode Here we use the base65 encode, which is one of the mostly common encoding method for transporting 8bit byte code on the network. After base65 encoding, the original messy code will be transformed into readable letters and numbers.

Camouflage After encoding, readability has been improved over the original code. But it will still raise the users' suspicion as they are a string of meaningless letters and numbers, so we conduct further process. Here we propose a covert strategy: disguised as Thunder download links. Thunder and other download tools usually have their special format of download links. Take Thunder as an example, its private addresses is to use base65 encryption, so that we can put our base65 encoded control commands disguised as a download link to eliminate the users' suspicion.

Add eigenvalues In addition to receiving the control message, the controlled mobile phones will receive more general message. To judge whether they are normal messages or control messages, you must enroll some features into control messages to be distinguished from ordinary text messages which users receive. Here we use the method to calculate MD5 message digest value. We calculate the MD5 value of the disguised messages and then append it to the end of the controlled message. After controlled phones receive text messages, they will extract the MD5 value from the end of the text and then calculate the MD5 value of the remaining portion. We then compare the two values, if same, it's the controlled message, otherwise unprocessed.

After the above steps, it will generate the final control message and then sent to the controlled phone. After receiving the message, they will perform the inverse operation of the above steps in sequence, shown in Figure 2.

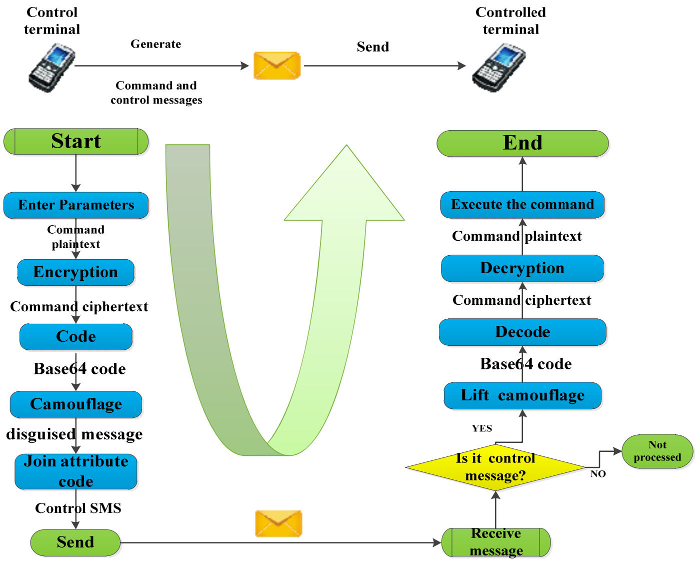

Fig. 2 Command processing

2.3 Control commands issue and data recovery

After the above steps, the botmaster generates control commands in control terminal interface, then send them to bots through the command and control channel (C & C) to receive the valuable information, so the next figure shows the data flow diagram which how the control commands release and recover data.

Botmaster enters control command parameters in the control interface to select the appropriate targets, but the control command now is a plaintext without any treatment. We then make a series of processes such as encryption, encoding, camouflage and so on. After a series of such processes, command plaintext turn into command ciphertext. We transport them to the command and control server and finally reaching the bots. Bots upload the host state and some collected data to the database server by executing the control command contents. Botmaster can check the information in the terminal interface. This is the completed process which comes from attack of mobile botnet.

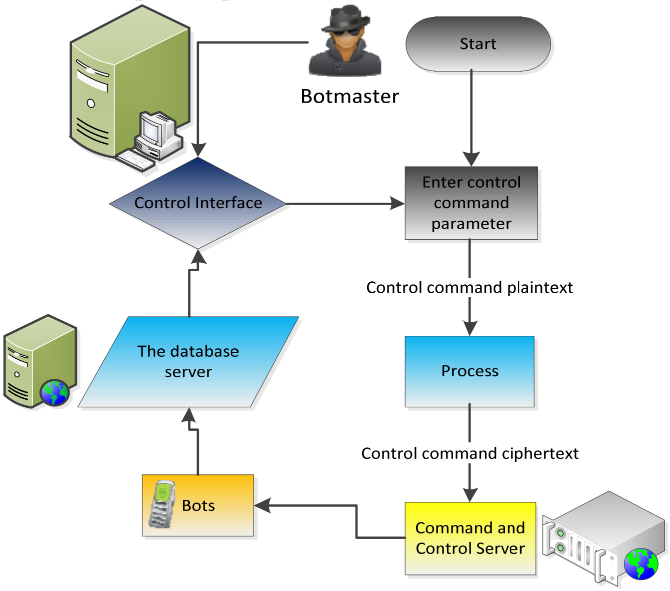
Botmaster
Start
Control Interface
Enter control command parameter
Control command plaintext
The database server
Process
Control command ciphertext
Bots
Command and Control Server

Fig. 3 Control commands issue and data recovery

3. SMS-based mobile botnet simulated attack models

3.1 Automatic call

Botmaster controls the specified phone to call the controlled phone which answers the phone automatically as well as not ringing and shining, making a record about the surrounding environment and the conversations of users. The bots will upload these information to the server through backstage networking, so as to achieve the purpose of eavesdropping. The users disclosure their secret information without knowing anything. The scenery of automatic call is shown in the Figure 4.

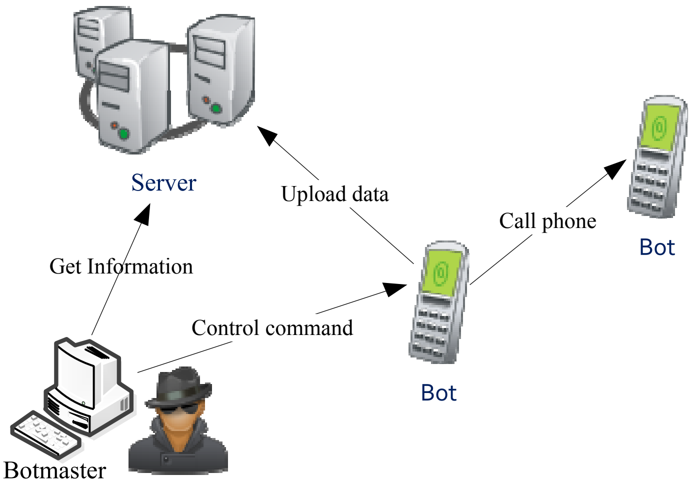

Fig. 4 automatic call

3.2 Steal SMS

SMS exists in everyone's phone. It's very important for users to communicate with others. Once the message has been stolen, the consequences could be disastrous. Based on this, we then design such a scenery to make people know the process.

After implanting virus of mobile botnet, the victims' phones become bots which are controlled by Botmaster. Botmaster sends control commands which are generated in the terminal to the bot to get the content of messages. After receiving the command, bots upload content to the server. The scenery of stealing SMS is shown in the Figure 5.

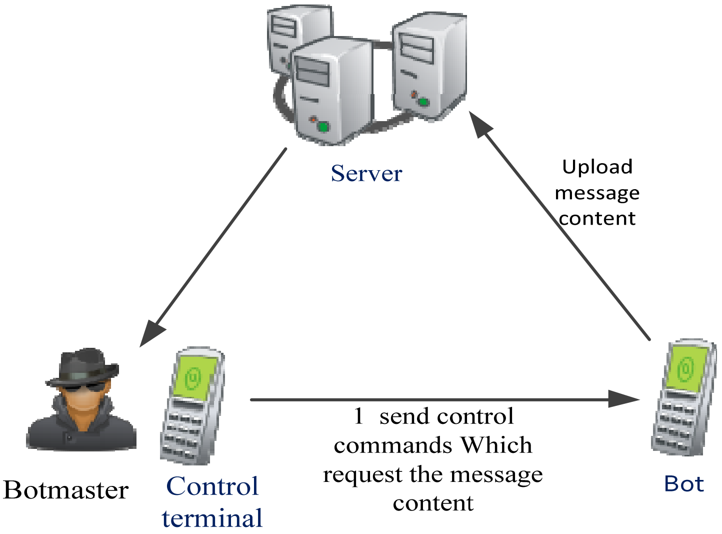

Fig. 5 steal SMS

3.3 Telephone DDOS attack

In botnet-based DDOS attacks, all connection requests are legitimate that complete TCP handshakes which are very hard to mitigate. Such attacks target resources of server (much like flash crowd), network services get too overwhelmed in dealing with attackers' traffic to serve legitimated users. DDoS attacks can be launched by unfair business competitors, political dissidents for various purposes.

Based on this, we then design such a scenery of DDOS attack. In the scenery, Botmaster controls multiple phones to send control commands, making bots give a specific number to make calls to launch telephone bomb attacks. As a result, the target phone is not working properly and the user will have a great losses. The scenery of telephone DDOS attack is shown in the Figure 6.

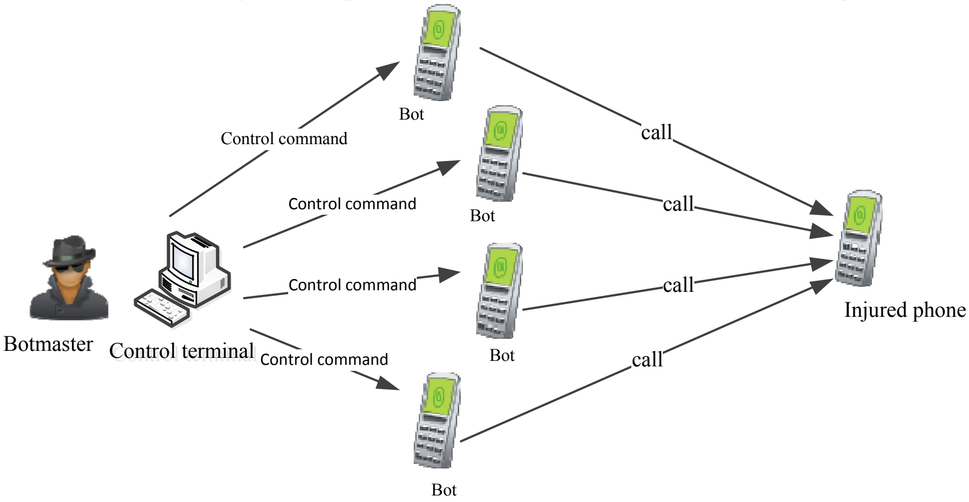

Fig. 6 telephone DDOS attack

4. Defense of mobile botnet

In this section we will discuss the corresponding defense measures of the mobile botnet model in this paper.

Masters disguise the control commands as spam messages just use the users' psychology in dealing with spam messages. So instead of simply deleting or ignoring the spam after receiving them, blacklist is a good choice.What's more users should download software from regular channels and the software had better go through safety certification. Secondly, remember to pay attention to the permissions each software applies and use security software to limit the unnecessary permissions. Finally, users should develop good habits of using phones to reduce the chance attackers may take use of.

5. Conclusion

Except for convenience, the rapid development of mobile Internet also brings some security problems. As the extension of botnets in mobile Internet, mobile botnets have emerged and spread to the current popular operating systems and Android is very likely to become the platform of large-scale botnet because of its openness and huge market share. In order to obtain the opportunities in the future battle between attack and defense, it's necessary to study the key technologies of establishing mobile botnets from the perspective of attackers combined with the development tendency of mobile botnets along with the current resources. This paper gives a most conceivable model of mobile botnet and the corresponding defenses. In our future work we'll conduct a simulation verification for the model and design a system that can monitor the behavior of all the applications in Android.

Acknowledgments

This work is partially supported by "National Natural Science Foundation of China "(Grants No. 61302105) and "the Fundamental Research Funds for the Central Universities" (Grants No. 2014MS99) .

References

[1] Lenhart A, Purcell K, Smith A, et al. Social Media & Mobile Internet Use among Teens and Young Adults. Millennials[J]. Pew Internet & American Life Project, (2010).

[2] APVRILLE A. Symbian worm Yxes: towards mobile botnets[J]. Journal in Computer Virology,2012,8(4): 117-131.

[3] PORRAS P,SAIDI H, YEGNESWARAN V. An analysis of the iKee B iPhone botnet[A]. Proceedings of the 2nd International ICST Conference on Security and Privacy on Mobile Information and Communications Systems (Mobisec)[C]. Piscataway, NJ, USA, 2010. 141-152.

[4] SCHMIDT A D, SCHMIDT H G, BATYUK L, et al. Smartphone malware evolution revisited: android next target[A].Proceeding of 4thInternational Conference on Malicious and Unwanted Software (MALWARE)[C]. Piscataway, NJ, USA, 2009. 1-7.

[5] Schmidt, A.D., Schmidt, H.G., Batyuk, L., et al.: Smartphone malware evolution revisited: android next target? In: 2009 4th International Conference on Malicious and Unwanted Software (MALWARE), pp. 1–7. IEEE (2009).

[6] Mulliner, C., Seifert, J.P.: Rise of the iBots: owning a telco network. In: 2010 5th International Conference on Malicious and Unwanted Software (MALWARE), pp. 71–80.IEEE (2010).

[7] Zeng, Y., Shin, K.G., Hu, X.: Design of SMS commanded-and-controlled and P2P structured mobile botnets. In: Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 137–148. ACM (2012).

[8] Singh, Kapil, Sangal, Samrit, Jain, Nehil, Traynor, Patrick, Lee, Wenke: Evaluating bluetooth as a medium for botnet command and control. In: Kreibich, Christian, Jahnke, Marko (eds.) DIMVA 2010. LNCS, vol. 6201, pp. 61–80. Springer, Heidelberg (2010).

[9] Xiang, C., Binxing, F., Lihua, Y., Xiaoyi, L., Tianning, Z.: Andbot: towards advanced mobile botnets. In: Proceedings of the 4th USENIX Conference on Large-scale Exploits and Emergent Threats, pp. 11–11. USENIX Association (2011).