Network Traffic Analysis of Android Malware

Myeong-jae. Seong*, TaeGuen Kim, Eul-gyu im*
*Dept. of Computer and Software
Hanyang University, Korea,
E-mail : {mjseong, cloudio17, imeg}@hanyang.ac.kr

1. Introduction

Android malwares can transmit data over the network, and the data which most malware transmit is sensitive information of normal user. We performed research in order to prevent this kind of sensitive information leakage. In our research, we analyzed malicious android application's network traffic and figured out how to distinguish benign app and malware using it. In fact, it is very difficult to monitor the network packet payload which real malware generate. Therefore, we analyzed network traffic rather than real network packet payload.

In this paper, we collected the network traffic which is generated by android malwares, and extracted network protocol information and transmission pattern from the network traffic. Finally, we could find common transmission patterns of android malwares.

2. Background

2.1. Android malware

Trojan is the most popular type of android malware and it takes more than 49% of the total android malware.[1] Most of the Trojan transmit sensitive data like Phone number, IMEI, SMS information, etc. to certain server. And Trojan also can send SMS message to the other user. This SMS message can be used to do phishing attack and to install another android malware. Infection of Trojan can cause additional attack on android system or phone user.

2.2. Android packet capture method

To analyze the network traffic of malware, we should know how to capture packet on android system. Simple description of packet capture method is explained in this section.

There are two packet capture methods which can used in android environment. Firstly, it is possible to capture the packet by sniffing AP(Access Point). Secondly, it is possible to capture the packet by using tcpdump which is provided by android basic service.

In this paper, we could collect packets of android malware using the android application called tPacketcapture[3]. tPacketCapture does packet capturing without using any root permissions. tPacketCapture uses VpnService provided by Android OS.

3. Android malware packet feature

3.1. Android packet pattern

We found that android malware has distinguishable packet transmission pattern through our experiment.

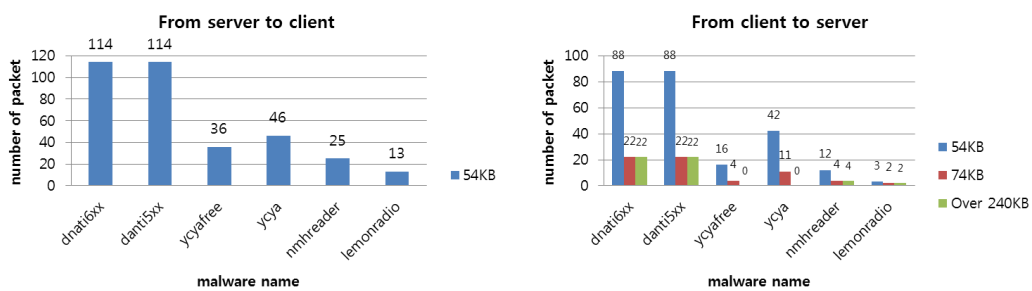

Figure 1. The difference of TCP packets between ingoing packets and outgoing packets

Firstly, we learned that most android malware used TCP protocol to communicate. We also could observe that many android malware prefer to transmit the packet using HTTP protocol after the network connection is established using 3-way handshake.

Secondly, we could learn that outgoing packets outnumber the ingoing packets and outgoing packet and ingoing packets have difference. Communication of android malware observe detailedly, Every ingoing packets which direct to client from server were TCP response packets such as "ACK", "SYN + ACK", "FIN + ACK". Meanwhile, outgoing packets which direct to server from client consist of TCP request packets such as "SYN", TCP response packets, and other packets contain real message data like HTTP message.

There is the method using Size of packet among approaches which distinguish Android malware using Network packet. This method, when using feature of packet size, packet size must be change. Therefore, It can not be a using feature because packet size be transmitted packet of the certain size from server to client. However, packet size be transmitted various size from client to server. So it can be using feature. Figure 1 is collected packet which communicated each malwares, Packets in transmitted from the server to the client was found packet of certain size, and packets in transmitted from the server to the client was found packet of various sizes.

3.2. Communication protocol of android malware

In this section, we will explain about android malware's communication patterns which we found in experiment. We observed that most of android malwares do not communicate directly, using IP address. All of android malwares request IP address to DNS server and then DNS server notify the IP address to the malwares. It also use DNS in order to evasion to method that separate whether malware or not and block IP address, using IP address. also, observed android malwares communicated using TCP than to use the UDP protocol. Because data need not transmission at high speed and it also used in order to delivery user information of used Android OS without loss, we think that Android malware use TCP protocol. thus, many android malwares communicate using TCP protocol and this result is shown in figure2.

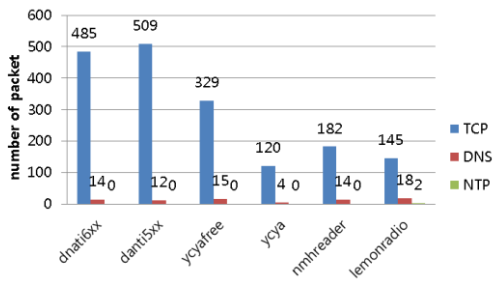

Figure 2. protocol number of captured packet

4. Conclusion

In this paper, we captured many packets which were generated by android malicious application, and analyzed them to learn the property of malicious packets.

As a result, we could find that size of packet in received from the server to the client can not be used feature, and size of packet in sent from the client to the server can be used feature. and we also observed that most of communication protocol which android malware used was TCP protocol. And we could observe that malware use DNS server to gain IP address it wants to communicate.

In the future, we have a plan to find more feature in the future. That features will be help to distinguish benign traffics and malicious traffics.

5. Acknowledgments

This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2014-H0301-14-1022) supervised by the NIPA(National IT Industry Promotion Agency).

6. References

[1] Ahnlab Smartphone malware 2014 1Q, http://blog.ahnlab.com/ahnlab/1912.
[2] TCPdump, http://www.tcpdump.org/
[3] tPacketcapture, http://www.taosoftware.co.jp/en/android/packetcapture