Generating a Rich Mobile Dataset Using a Central Management Approach

Khelwa Fariza Binti Mohd Sakroni, Assoc. Prof. Dr. Habibah Binti Hashim
Faculty of Electrical Engineering,
Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia
khelwafariza@yahoo.com

***Abstract* – Bots are small-size malwares that infect computers or mobile network, which can join with other bots via the Internet to form a network of bots called Botnet. The Botmasters, who control the Botnets, update the bots and change their codes day by day to avoid the traditional detection methods such as signature-based anti-viruses. Mobile environment is less protected and botmasters have taken advantage of the lack of security knowledge of mobile users in an attempt to steal private data and earn money illegally. Many techniques are employed by Botmasters to make their Botnets undetectable for as long as possible. This paper presents a method to produce rich mobile datasets for mobile security researchers. Project development is carried out using tPacketCapture application which been installed in the Android Smartphone and the collected mobile data been analyzed using a network protocol software, named Wireshark. The valid mobile dataset can be utilized for future mobile security study.**

***Index Term* – Botnets, Bots on Smart Phones, Mobile Dataset, Mobile Botnets, Wireshark**

I. INTRODUCTION

Mobile devices are everywhere and the Smartphone usage has dramatic growth in the mobile network. It is beyond just simply making phone calls. Among the mobile's operating systems, Android is very popular owing to availability as an open source operating system. Due to the proliferation of Android malwares, it is crucial to study the best classifiers to detect them effectively and accurately.

Internet is most vulnerable to attacks due to its public nature and virtually without centralized control. With the growing financial dealings and business dependence on Internet, these attacks have increased. Whereas previously hackers would satisfy themselves by breaking into someone's system, in today's world hackers' work under an organized crime plan to obtain illicit financial gains or profits.

Among all these threats, Botnet is considered the most dangerous and biggest threat to cyber security. A Botnet is a linked group of infected networks (termed as Bots). Bot is a computer program installed on a compromised machine which allows an attacker to execute arbitrary commands on the infected machine. When a large number of Bots spread to different mobile devices and connect to each other through the Internet, they form a network of Bots called Botnets. Bots communicate with each other and get their commands from a controller, named with Botmaster, as shows in Fig. 1.1.

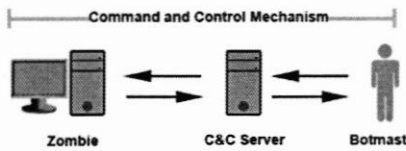

Fig. 1.1. General schema of Botnets C&C mechanism

The Botmaster has a mechanism to control their Botnets by sending commands to the bots and receiving response from them. Different command and control mechanisms (e.g. IRC, HTTP, and P2P) are used by Botmasters to achieve this goal. In general, Fig. 1.2. shows Botnets phases in their life cycle.

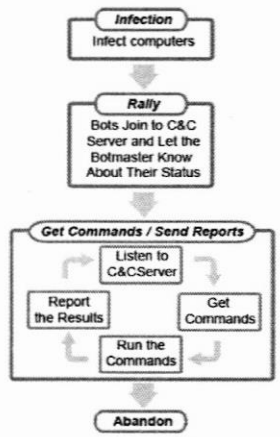

Fig.1.2. Botnet life cycle

The objective of this paper is to study and gain an insight overview of the mobile threats that users of Internet are facing from hackers by the use of malicious mobile Botnets. The contribution of this paper is the mobile data collection with normal traffic and the traffic with the existence of Botnets. Next, execute the offline client server system to collect the file of mobile data (PCAP file). The goal is to identify possible infection of malware or malicious activity in the captured PCAP files using the Wireshark tool. Hence, these valid data can be apply for mobile security researchers and become the base line for mobile forensics analysis.

The rest of this paper organized as follows: Section II provides background of the Botnet system. Section III provides the research methodology of creating the mobile dataset on Android smart phone. In Section IV, presents the result and discussion on the collected mobile data. Last but not least, the conclusion and future works of this paper is been presented in Section V.

II. BACKGROUND

Botnet threat comes from three main elements - the bots, the Command and Control (C&C) servers, and the Botmasters. Bots infect the devices, and C&C servers distribute the Botmasters' order to the bots in infected devices. The Command and Control mechanism creates an interface between the bots, C&C servers and the Botmasters, to transmit data between them. Fig. 2.1. shows the logical relationship between these three elements.

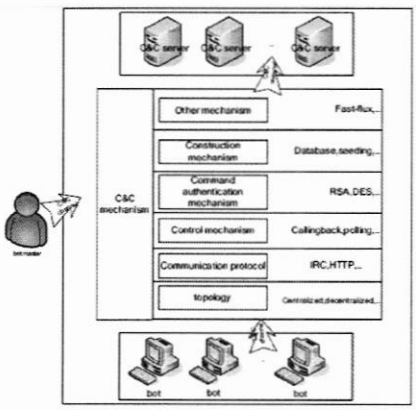

Fig. 2.1. General framework for Botnets

Nowadays, Botmasters prime targets are computer and mobile devices especially when they are connected to Internet using broadband connection. These users usually have low awareness or lack knowledge of network security. Botmasters take advantage of this to gain unauthorized access into the devices without being detected. Botnets are expected to be activated to distribute spam, steal private info, and install other malware. Botmaster can design a botnet to perform certain actions, such as information stealing or launching a denial of service, and issues commands to the bot clients from a command and control server.

Since mobile networks are now well integrated with the Internet, it can potentially be utilized like any other computer while maintaining all of their functionality within a mobile network. Mobile applications, commonly called apps, provide enhanced convenience and functionality. Anyone can potentially develop and distribute mobile applications with little oversight, making apps a potential attack vector for cyber criminals. Several major banking institutions provide legitimate mobile applications that allow customers to conveniently check balances, pay bills, transfer funds, or locate automated teller machines (ATMs) and banking centers.

Android is an open platform, which enforces security by sandboxing applications, where it provides the users with the opportunity to install applications from various untrusted sources. Therefore, fooling a user into installing malicious content is an important attack strategy. Considering Internet connection as the delivery path for malware, example scenario for delivery of malicious content to Android devices via Internet is presented in Fig. 2.2.

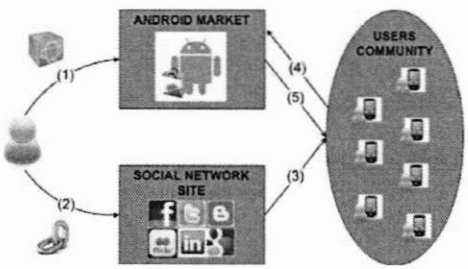

Fig. 2.2. Malicious content delivery scenario for Android

However, such an application, when installed, gets all the permissions on a mobile device. Application might access local camera, 3G/4G, Wi-Fi or GPS module without user's knowledge.

III. METHODOLOGY

This section describes the procedures that have been conducted during the project implementation. From the gathered information, the previous literature about mobile data collection is studied.

The research has been performed by doing the simulation process using Google Application (tPacketCapture). The mobile data is executed on Android Smart Phones (model Samsung Galaxy Pocket Neo S5310) to get the expected result. Data capturing activity was carried out in 4 to 5 days duration and this step been executed repetitively to get the best result. Testing for more than that duration will affect the performance, speed and space storage of the phone. The process of mobile data capture was running on WiFi Network and 3G Network which using local mobile service provider, Celcom. It accesses the normal mobile traffic; such as internet data browsing (using Google and Firefox), login to multiple emails account, social network media (eg. Instagram, Facebook, etc), joins chats group and make a video calls (via Whatsapp, Viber and Sype), and login into local financial account to perform some financial transaction via e-banking systems such as Maybank2U and CimbClicks.

When the mobile data is obtained by transferring the dataset to PC (act as a server), the next step is to analyze the datasets via the powerful software, Wireshark. This network analyzer is use as a monitoring tool for exploring the characteristics of the Bots in mobile network. Detail flowchart of the project studied is presented in Fig. 3.1.

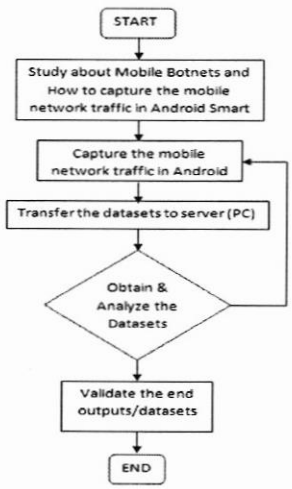

Fig.3.1.Flowchart of collecting the mobile data and analyzing the mobile dataset.

IV. RESULT AND DISCUSSION

The analysis was made on the virtual smart phone or devices and the captured data is transferred to Windows 7 machine (PC). Each captured mobile data was subjected to the same Wireshark analysis to cross-reference the results.

The main goal of the test result is to identify possible infection of malware in the Wireshark captured PCAP file. Additional, analysis section explained the techniques, filters tools, gathers knowledge and information, where Malware or malicious behavior are described and summarizes the end result.

A. Mobile data traffic in Wireshark

The Wireshark tool helps in examining the recorded mobile data by inspecting and monitoring the data packets and its protocol. The main purpose for Wireshark software is to analysis the network protocols and monitor problems in the network traffic from the captured mobile file. Fig. 4.1. shows the sample Graphic Interface of mobile data containing different protocols such as HTTP, TCP, TLSv1 and UDP.

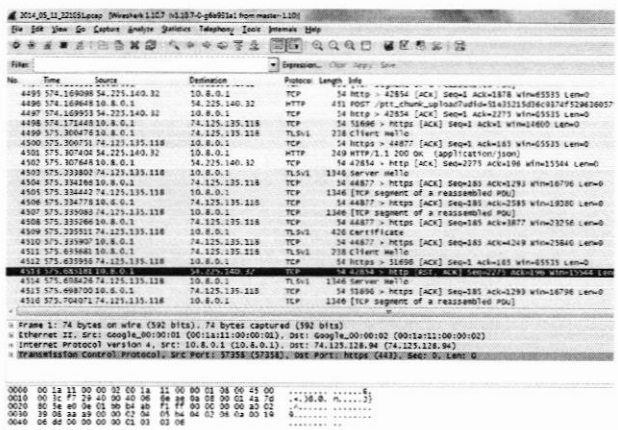

Fig. 4.1 Wireshark graphic interface of captured mobile data.

Wireshark uses display filters for general packet filtering while viewing the file. When needs a display filter for a specific protocol, example HTTP, below **http** syntax need to be entered at "Filter" field as shown at Fig. 4.2.

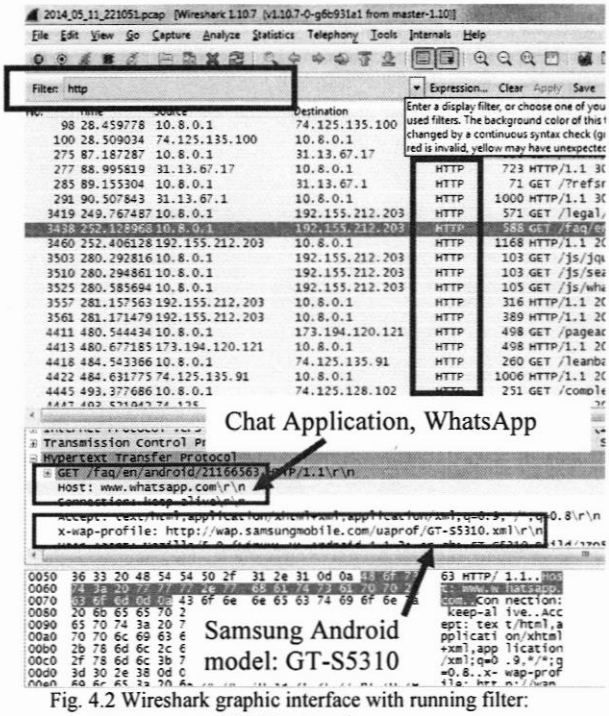

Fig. 4.2 Wireshark graphic interface with running filter: HTTP protocol.

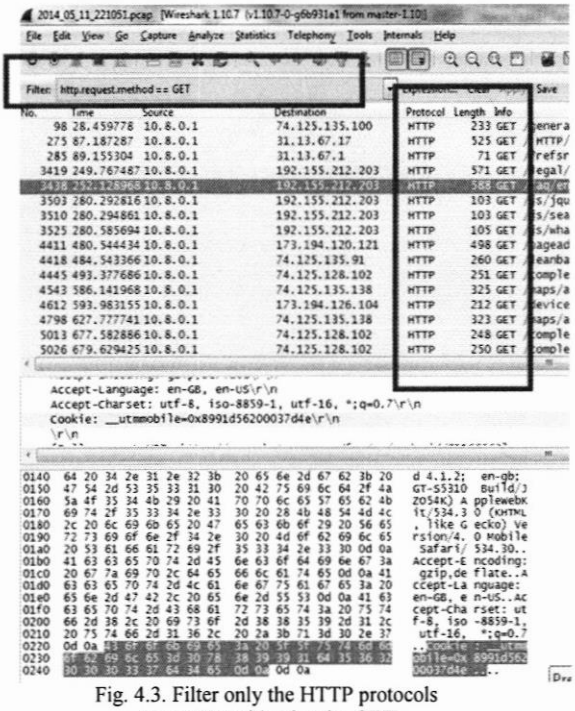

Fig. 4.3. Filter only the HTTP protocols on port 80 with a header GET

From Fig. 4.2., we can see that one of the hosts stated on the Wireshark graphic interface is www.whatsapps.com. It tells that the Chat Application, named WhatsApp has been accessed by the mobile user. On top of that, it is also displays the information of the Android smart phone model used in this project as shown at the same graphic interface, Fig.4.2.

However, from the Fig.4.2 we can see that there is a lot of traffic generated by the mobile user. Therefore we have to apply an additional filter rule, which will help and guide user for better and easy analysis. As we go through each generated HTTP protocol traffic, we can conclude that the user has been visiting different sources, which can be a potential threat for the network and personal use with a different malicious code.

To be able to filter only the HTTP protocols on port 80 with a header GET, use the following filter: **http.request.method == GET**. This filter will narrow down the results that are presented into the captured file. See Fig. 4.3.

B. Mobile data malware detection in Wireshark

Another extremely useful feature in Wireshark is the detail analyzer communication from menu path Analyze → Follow TCP Stream. Step is shown in Fig.4.4.(a).

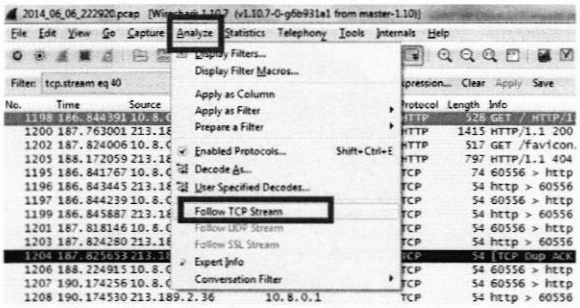

Figure 4.4. (a) Useful steps to display the detail communication information

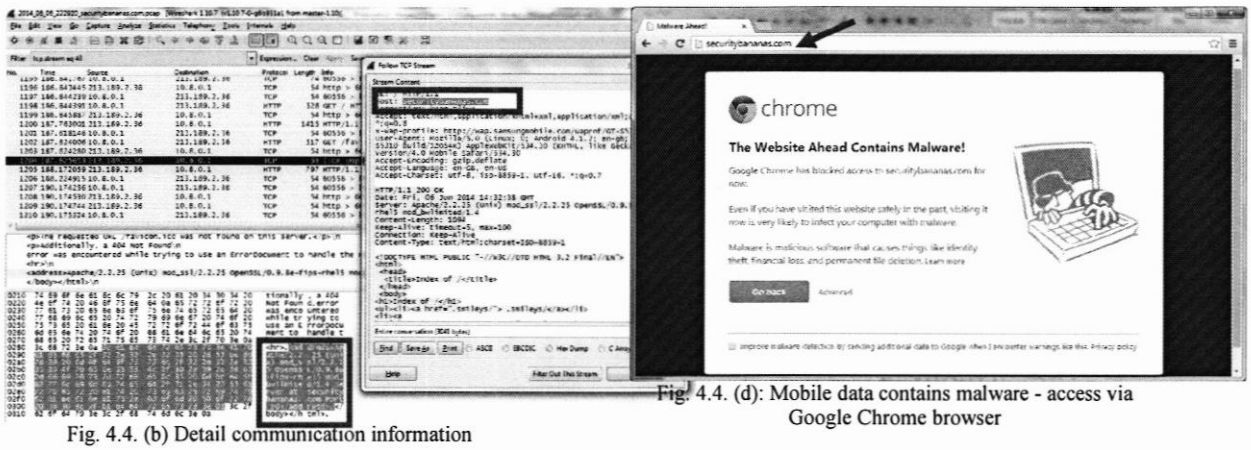

Fig. 4.4. (b) Detail communication information

Fig. 4.4. (d): Mobile data contains malware - access via Google Chrome browser

The above steps, as shown at Fig. 4.4.(b), display the communication between IP addresses in more readable and useful way. It shows the DNS name for the IP and if file was downloaded, it gives filetype and name. From Fig. 4.4.(b), it discovered that IP address 213.186.2.36 belongs to *securitybananas.com*.

If we run or analyze the above domain names into Internet browser, automatically it indicated that the *securitybananas.com* is reported as a malware site. When try to access the site with various web browsers, all of them showed that it contained malicious behavior. The access from Mozilla Firefox and Google Chrome was shown in Fig. 4.4.(c) and Fig 4.5.(d):

Fig. 4.4 (c): Mobile data contains malware – access via Mozilla Firefox browser

C. Summary of mobile data collection and malware detection in Wireshark

Nowadays malicious behavior and malware infection in the mobile network is the highest vector of production work every day. The malware universe is infinite and is in constant evolution. There are always cases where malware can escape from the antivirus systems and reaches the end mobile user and manages to execute their malicious activity. Once a device or smart phone is infected, it is essential and very crucial to identify what type of threat it is and eliminate it.

Therefore, different approaches, troubleshooting and advance analysis have to be applied to detect these malicious activities in the frequent usage of mobile data. Leaking of data, information, and access of network (internal and external) can be very harmful for any mobile users. Thus, this project main aim is to produce the valid mobile dataset to be able to use in future advance analysis of the identification of infection within the Wireshark tool.

Concluding, as there are many different ways, tools and process for analyzing the malicious behaviors in mobile network, the result of this project is to supply the reader and researcher with advance and stepwise solution for identifying the malicious activity in the mobile data within the Wireshark network analysis.

V. CONCLUSION

Overall, this paper successfully describes a mobile data collection to become a valid mobile dataset for future mobile security research. Analysis on mobile data on normal traffic and the traffic with the existence of malware or malicious behavior was also executed. The discussion on the result was obtained based on the analysis. It is anticipated that the level of findings to emerge where malware detection in mobile network can be performed by using Wireshark tool. The paper only concentrates on producing a rich mobile datasets which been implemented at Android Smartphone. This paper not presents any solution for reducing the mobile botnets or develop any mobile security but hopefully will generate an intense interest among researchers to undertake research in this area.

REFERENCES

[1] Niko Kiukkonen, Jan Blom, Olivier Dousse, Daniel Gatica-Perez and Juha Laurila, "Towards rich mobile phone datasets: Lausanne data collection campaign", *Nokia Research Center, PSE-C, 1015 Lausanne EPFL, Switzerland, Nokia Research Center, Itamerenkatu 11-13, 00180 Helsinki, Finland, IDIAP Research Institute, Rue Marconi 19, CP 592, 1920 Martigny, Switzerland*

[2] M. Eslahi, R. Salleh and N. B. Anuar, "Bots and Botnets: An Overview of Characteristics, Detection and Challenges," presented at the IEEE International Conference on Control System, Computing and Engineering, Penang,Malaysia, 2012., DOI 10.1109/ICCSCE.2012.6487169 pp.349-354, IEEE 2012

[3] Eslahi, M. Hashim, H., and Tahir, N.M., "An efficient false alarm reduction approach in HTTP-based botnet detection", *IEEE Symposium,* DOI 10.1109/ISCI.2013.6612403 pp.201-205, IEEE 2013

[4] Martini P., "Botnets - Detection, classification and countermeasures", *IEEE 36th Conference,* DOI 10.1109/LCN.2011.6115152 , IEEE 2011

[5] M. Eslahi, R. Salleh and N. B. Anuar, "MoBots: A New Generation of Botnets on Mobile Devices and Networks," presented at the IEEE International Symposium on Computer Applications and Industrial Electronics (ISCAIE), Kota Kinabalu Malaysia, 2012, DOI 10.1109/ISCAIE.2012.6482109 pp. 262 - 266, IEEE 2012

[6] Khosroshahy, M. ; Dongyu Qiu ; Mehmet Ali, M.K., "Botnets in 4G Cellular Networks: Platforms to launch DDoS attacks against the air interface", *IEEE International Conference* DOI 10.1109/MoWNet.2013.6613793, pp. 30 - 35, IEEE 2013

[7] Leavitt, N., "Mobile Security: Finally a Serious Problem?", *IEEE Journals and Magazine, Volume 44, Issue 6*, DOI 10.1109/MC.2011.184 , pp. 14 - 14, 2011

[8] C.Mulliner and C.Miller, "Fuzzing the phone in your phone," in *Security Conference,* 2009.

[9] P.Traynor, M.Lin, M.Ongtang, V.Rao, T.Jaeger, P.McDaniel, and T.L.Porta, "On cellular Botnets: Measuring the impact of malicious devices on a cellular network core," in *Proceedings of the 12th ACM Conference on Computer and Communications Security* (CCS'09).

[10] Pieterse, H. and Olivier, M.S., "Android Botnets on the Rise: Trends and Characteristics", Information Security for South Africa (ISSA), pp 1-5, IEEE 2012

[11] Collin Mulliner, "Smartphone Botnets", *Berlin Institute of Technology, FG Security in Telecommunications*, July 7th 2010

[12] Georgia Weidman "Transparent Botnet Control for Smartphones over SMS", 2011,

[13] "Cyber Threats to Mobile Devices", US-CERT Technical Information Paper – Cyber Security TIP-10-105-01 April 15, 2010

[14] Yajin Zhou, Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution," *in Proceedings of the 33rd IEEE Symposium on Security and Privacy, San Francisco, CA*, May 2012

[15] Vinit B. Mohata,, Dhananjay M. Dakhane, Ravindra L.Pardhi, "Mobile Malware Detection Techniques", *International Journal of Computer Science & Engineering Technology (IJCSET)*, ISSN : 2229-3345, Vol. 4 No. 04 Apr 2013

[16] Chris Greer, "*Top 10 Wireshark Filters*", April 2010, http://www.lovemytool.com/blog/2010/04/top-10-wireshark-filters-by-chris-greer.html

[17] Russ McRe, "*Security Analysis with Wireshark*", November 2006

[18] David Barrera, Jeremy Clark, Daniel McCarney, "Understanding and Improving App Installation Security Mechanisms through Empirical Analysis of Android", 2012