Poster: Towards a framework for Network-based Malware detection System

Abimael Carrasquillo[†]
abimael.carrasquillo@upr.edu
Student

Albert E. Maldonado[†]
albert.e1992@gmail.com
Student

Eric Santos[†]
eric.santos1@upr.edu
Student

José Ortiz-Ubarri[†]
jose.ortiz23@upr.edu
Assistant Professor

[†]Department of Computer Science
University of Puerto Rico, Río Piedras Campus
San Juan, Puerto Rico

***Abstract*— It is known that the major threat on mobile devices is malware. In this work we present a Network-based Malware detection System to provide situational awareness of mobile devices connected through a VPN network. Our goal is to combine network traffic analysis with signature-based IDS to provide both the mobile user and the network administrators with alarms of anomalous behavior and means for visualization analytics of mobile devices. In this work we evaluated the effectiveness of our framework to provide the mobile user with malware alarms detected by the signature-based IDS.**

Keywords—Android; malware

I. INTRODUCTION

As mobile devices plays an important role in todays life, also does malware protection. For instance, the major threat on the Android operating system is malware and adware infection via Android markets[1]. There are two approaches to mobile Malware detection: host-based malware detection and network-based malware detection. The host-based malware detection uses the limited resources of the mobile devices and is prone to drain the battery power of the mobile devices. The network-based malware detection delegates the analysis of the network behavior to a back-end server to detect malware based on the traffic generated by the mobile device, but is unable to detect malware that does not generate network traffic[2]. Our framework is a network-based malware detection system that will combine network flows analysis and signature-based traffic analysis of a virtual private network (VPN)[3] of mobile devices. Similar to the approach proposed by Parrizas et al. in[4], we utilize Snort[5] for the signature-based traffic analysis. However, in our work, we provide both the mobile device user and the system administrator of the VPN network with the alarms generated. For the network flows analysis, the framework uses NetFlow, a network protocol developed by Cisco[6] for traffic monitoring. One NetFlow is a record representing an unidirectional sequence of packets that contains information on the source Internet Protocol address (IP), the destination IP, the source port, destination port, the sum of the payload size of the packets, a timestamp, among others. A NetFlow generator will run on the VPN server to collect aggregated information of the network traffic. The collected data will be analyzed to detect network anomalous behavior, per mobile device, and will be represented in charts for situational awareness and visualization analytics.

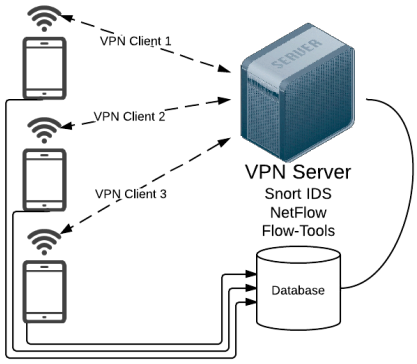

Figure 1: VPN Client/Server Diagram

II. METHOD

To create the framework we need to: 1) configure mobile devices to connect to the VPN, 2) install and configure Snort IDS to monitor the VPN server virtual interface with signatures for malware detection, 3) install and configure a NetFlow generator (flow probe) to generate NetFlow data of the VPN, 4) collect the NetFlow data for analysis, 5) analyze the NetFlow data and the IDS alerts per mobile device, 6) generate charts per mobile devices for situational awareness and visualization analytics, 7) implement the framework interface to provide the users with their mobile device alarms and charts.

III. RESULTS

We implemented Snort signatures to match specific network traffic and generate alerts. The network traffic was generated with Android devices and were successfully assigned to each VPN mobile device; i.e, the alerts are reported only in the device that generated the network signature. Besides the alerts, the users can also display traffic charts generated from the NetFlow data.

IV. FUTURE WORK

In the current stage of the work we have implemented the signature-based part of the framework with its user interface. We are also generating NetFlow traffic charts for each mobile device registered in the VPN and presenting them in the user interface. Currently we are working on the generation of traffic charts per network service (ssh, http and others). We will add the capacity to push notifications in the mobile devices, such that the user is alerted with the alarms generated by the framework, instead of relying on the user to access the framework interface to check for the alarms. Finally we will study different algorithms for anomalous network traffic analysis and study its performance.

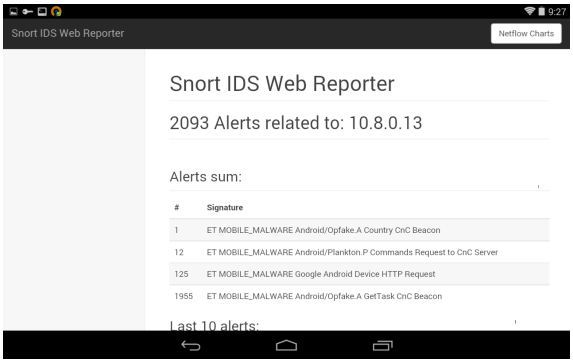

Figure 2: Interface displaying Snort alerts

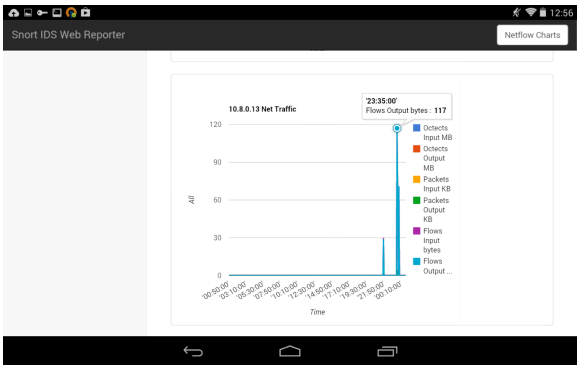

Figure 3: Interface displaying Netflow graphs

REFERENCES

[1] T. Isohara, K. Takemori, and Ayumu Kubota, "Kernel-based Behavior Analysis for Android Malware Detection", In Proceedings of the 2011 Seventh International Conference on Computational Intelligence and Security(CIS '11), IEEE Computer Society, Washington, DC, USA, 1011-1015,DOI=10.1109/CIS.2011.226 http://dx.doi.org/10.1109/CIS.2011.226

[2] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss. "Andromaly: a behavioral malware detection framework for android devices", Journal of Intelligent Information Systems, 2011, 10.1007/s10844-010-0148-x

[3] OpenVPN, HOWTO, available from:http://goo.gl/wT095i

[4] A. Parrizas, and D. Adriyanto Monitoring network traffic for Android devices, January-16-2013, retrieved from: http://goo.gl/5IyaCB.

[5] Source Fire, Inc. , Snort, Web page: http://www.snort.org/

[6] D. Kerr and B. Bruins, "Network flow switching and flow data export", June 5 2001, US Patent 6,243,667