Position Paper : Cyberdefense-Oriented Multilayer Threat Analysis

Yuji Sekiya (The University of Tokyo)
Daisuke Miyamoto (The University of Tokyo)
Hajime Tazaki (The University of Tokyo)
Date : Jan. 15th, 2014

1. Introduction

Threat detections and analyses are indispensable processes in today's cyberspace, however, current the state of the art of cyber-defence are still limited to specific aspects of modern malicions activities due to the lack of observation among multiple layers. Measuring and collecting various kinds of data from network traffic, network services, application behaviors, and human behaviors are helpful to inspect malicious behavios of threats multidirectinally. However, such kinds of threat analyses from various data are not easy to implement due to scalability of the amount of data, compatibility of the data formats, and difference of the access policies. It is important for current cyber-security to overcome the issues and make possible to analyze threats multidirectionally from various data.

2. Proposal

We propose the BIG-data analysis system from various datas shown in Fig. 1.

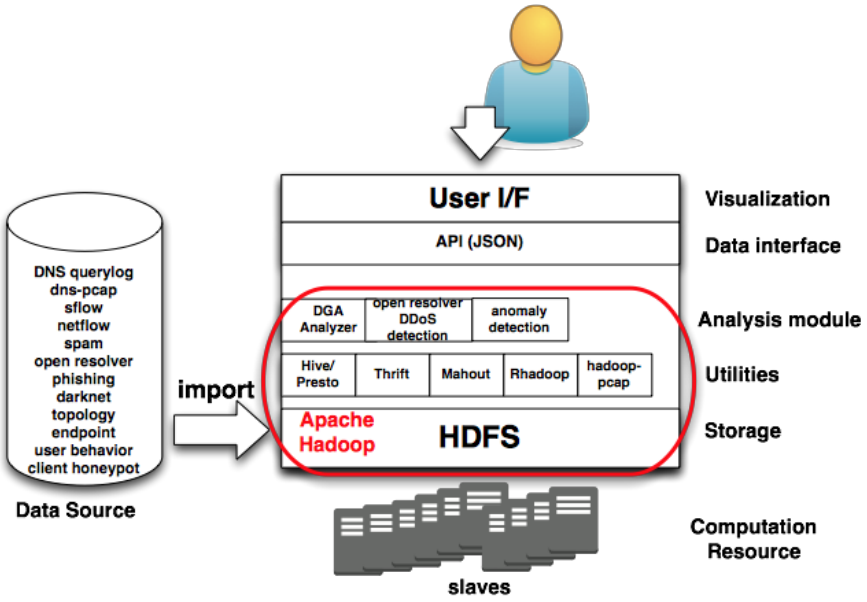

Figure 1 : Threats Analysis System

We build the prototype implementation of our proposed system and try to analyze some kinds of malicious behavios in our university network. At first, we target the analysis of Domain Generation Algorithm (DGA) used by botnets shown in Fig. 2. The system picks up the suspicious DNS queries from DNS service data and network traffic data, and detect the malicious IP addresses in our university, then try to find other suspicious communications from

the IP addresses. Based on the methodlogy, we could find several infected hosts during three months.

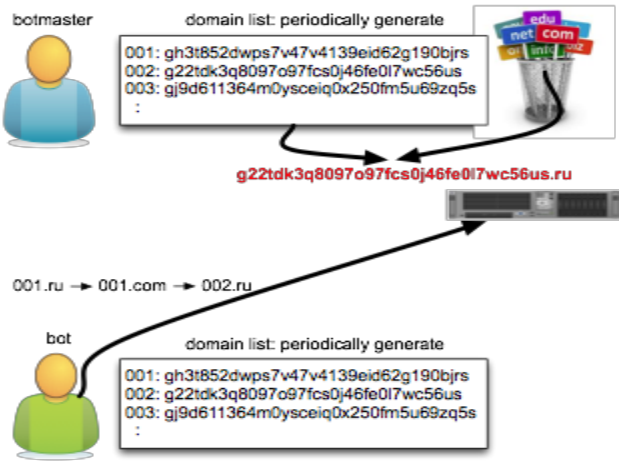

Figure 2 : DGA analysis

3. Conclusion

Analyses from various data are useful for the current threats. From our experiments, we make a point that IETF should propose multidirectional analyses and standardize its framework and dataformat to inter-analyses between organizaitions.