# An In-depth Analysis Methodology of IDS Alerts for Identifying Potential Cyber Threats on Darknet

Jungsuk Song[1], Younsu Lee[1], Jang-won Choi[1], Joon-Min Gil[2], Sang-Soo Choi[1]

[1]Department of Advanced KREONET Security Service, KISTI, Daejeon, Korea

[2] School of Information Technology Eng., Catholic University of Daegu, Korea

Emails: {song,zizeaz,jwchoi,choiss}@kisti.re.kr[1], jmgil@cu.ac.kr[2]

**Abstract.** In this paper, we present a methodology of carrying out in-depth analysis of IDS alerts and darknet traffic so that it is able to find out the root cause of the darknet traffic. The proposed procedure consists of seven main phases: Collection, Extraction, Classification, Comparison, Correlation Analysis, Identification and Tracing. The experimental results demonstrate that the proposed method is very useful to detect internal attack and to find out the infected malwares which are running or installed on them.

**Keywords:** In-depth analysis, IDS Alerts, Darknet

## 1 Introduction

Darknet is one of the most powerful technologies for observing a global trend of cyber threats and analyzing their activities [1,2]. Since there are no real systems with the darknet, it has a fatal limitation in that the most incoming packets on darknet do not contain payload. This situation makes security analysts difficult to identify whether the source hosts of the darknet traffic were infected by malware or not.

In our previous work [3], we proposed an advanced incident response framework whose main goal is to identify dangerous IDS alerts using darknet traffic [4]. In addition, we carried out a correlation analysis of IDS alerts and darknet traffic [5].

In this paper, we present a methodology of carrying out in-depth analysis of IDS alerts and darknet traffic so that it can find out the root cause of the darknet traffic. The proposed procedure consists of seven main phases as described in Section 2.

The experimental results showed that the proposed method is very useful to detect internal attack hosts (i.e., potential attackers) and to find out the infected malwares which are running or installed on them.

## 2 Methodology of In-depth Analysis

Figure 1 shows the overall procedure of the proposed analysis method of IDS alerts for identifying and tracing potential attackers that sent attack packets to darknet. The procedure is composed of 7 main phases: Collection, Extraction, Classification,

This research was supported by "Building and Services of Information Security System Based on Advanced KREONET" Program funded by the Ministry of Science, ICT & Future Planning (K-16-L01-C02-S04).

Comparison, Correlation Analysis, Identification and Tracing. The each phase of the procedure is as follows.

- Collection: During this phase, all the incoming network traffic whose destination is the darknet is captured.
- Extraction: In this phase, the entire source IP addresses (i.e., potential attackers) that sent attack packets to the darknet are extracted.
- Classification: The potential attackers are classified into two groups: the internal hosts and the external hosts.
- Comparison: The IDS alerts whose source IP addresses are the same to the internal hosts are extracted by comparing all of the IDS alerts with the internal hosts during the predefined time interval (e.g., one week, one month)
- Correlation Analysis: The extracted IDS alerts are used for correlation analysis in that the activities of the internal hosts are analyzed by using many parameters such as IP address, port number, protocol, and so on.
- Identification: The darknet traffic that was sent by the internal hosts and the corresponding IDS alerts are investigated by security analysts so that they are able to find out potential cyber threats from the their historical activities.
- Tracing: Finally, the internal attack hosts are inspected by anti-virus software so that one can find out the infected malware installed or running on them.

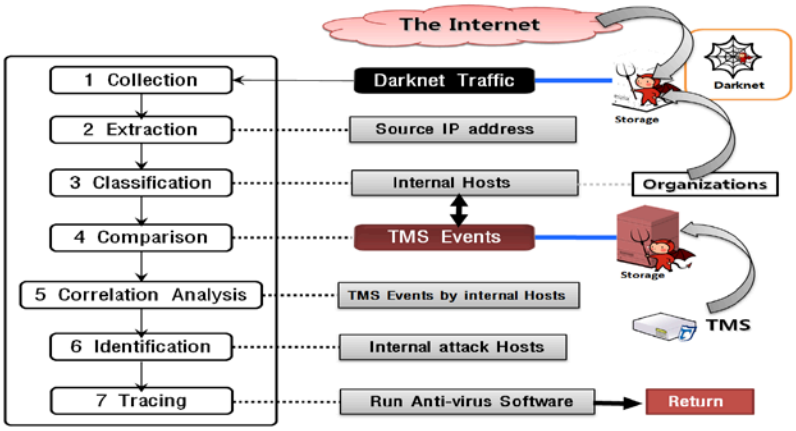


**Fig. 1.** Overall procedure of the proposed methodology for in-depth analysis

## 3 Experimental Results

We prepared 16*/24 darknet space in Korea and collected all the darknet traffic during 2 months (Sep. 2013 - Oct. 2013). Also, we deployed a dedicated IDS into the boundary network of the 16*/24 darknet IP addresses. According to the methodology described in Section 2, we conducted the in-depth analysis between all the incoming darknet traffic and IDS alerts.

Table 1 shows 5 internal attack hosts that raised one and more IDS alerts. Also, we inspected them using anti-virus software to find out hidden malware. We observed that 2 attack hosts (i.e., 1st and 2nd) were infected 30 and 144 different types of malwares. As a result, it could be concluded that 2 internal attack hosts were infected by a lot of malwares and the other 3 internal hosts were infected by unknown malware.

**Table 1.** Experiment results of the in-depth analysis

| Internal Host | Date | Organization | IP | # of type of IDS Alerts (Result of Anti-Virus) |
|---|---|---|---|---|
| 1st | 2013/09/16 | K**M | 210.x.x.232 | 1 (30 malwares) |
| 2nd | 2013/09/30 | K**S | 134.x.x.63 | 1 (144 malwares) |
| 3rd | 2013/10/08 | K***C | 210.x.x.172 | 1 (no malware) |
| 4th | 2013/10/08 | K*T | 203.x.x.177 | 3 (no malware) |
| 5th | 2013/10/17 | K**S | 210.x.x.232 | 1 (no malware) |

## 4 Conclusion

This research aims to present the methodology of carrying out in-depth analysis of IDS alerts and darknet traffic in order to identify and trace the root cause of the darknet traffic. Especially, we have focused on the internal hosts that sent packets to the darknet and analyzed IDS alerts related to the internal hosts.
In the experiments, we detected 5 internal attack hosts that raised one and more IDS alerts. In addition, we identified that 2 internal attack hosts were infected by 30 and 144 malwares by the anti-virus software and the other 3 hosts were not infected by unknown malware.

## References


[1] M. Bailey, E. Cooke, F. Jahanian, A. Myrick, and S. Sinha., Practical darknet measurement. In Information Sciences and Systems, 40th Annual Conference, IEEE (2007) 1496-1501

[2] T. Ban, M. Eto, S. Guo, D. Inoue, K. Nakao, R. Huang, A Study on Association Rule Mining of Darknet Big Data. IJCNN (2015) 1-7

[3] D. E. Denning, An intrusion detection model. IEEE Transactions on Software Engineering, SE-13 (1987) 222-232.

[4] S.S. Choi, J.S. Song, H.S. Park, and J.K. Choi, An Advanced Incident Response Framework Based on Suspicious Traffic. The Journal of Future Game Technology, Vol.2, Issue 2, (2012) 171-176

[5] S.S. Choi, J.S. Song, S.H. Kim, and S.K. Kim, A model of analyzing cyber threats trend and tracing potential attackers based on darknet traffic. Security and Communication Networks, Vol.7, Issue 10, (2014) 1612-1621