sustainability

MDPI

Article

Practical In-Depth Analysis of IDS Alerts for Tracing and Identifying Potential Attackers on Darknet

Jungsuk Song [1], Younsu Lee [1], Jang-Won Choi [1], Joon-Min Gil [2], Jaekyung Han [3] and Sang-Soo Choi [1,*]

1 Department of Advanced KREONET Security Service, Korea Institute of Science and Technology Information, Daejeon 34141, Korea; song@kisti.re.kr (J.S.); zizeaz@kisti.re.kr (Y.L.); jwchoi@kisti.re.kr (J.-W.C.)
2 School of Information Technology Eng., Catholic University of Daegu, Gyeongbuk 38430, Korea; jmgil@cu.ac.kr
3 Department of Construction Legal Affairs, Kwangwoon University, Seoul 01897, Korea; hjk1014@kw.ac.kr
* Correspondence: choiss@kisti.re.kr; Tel.: +82-42-869-0771

Academic Editors: James J. Park and Han-Chieh Chao
Received: 15 December 2016; Accepted: 7 February 2017; Published: 13 February 2017

Abstract: The darknet (i.e., a set of unused IP addresses) is a very useful solution for observing the global trends of cyber threats and analyzing attack activities on the Internet. Since the darknet is not connected with real systems, in most cases, the incoming packets on the darknet ('the darknet traffic') do not contain a payload. This means that we are unable to get real malware from the darknet traffic. This situation makes it difficult for security experts (e.g., academic researchers, engineers, operators, etc.) to identify whether the source hosts of the darknet traffic are infected by real malware or not. In this paper, we present the overall procedure of the in-depth analysis between the darknet traffic and IDS alerts using real data collected at the Science and Technology Cyber Security Center (S&T CSC) in Korea and provide the detailed in-depth analysis results. The ultimate goal of this paper is to provide practical experience, insight and know-how to security experts so that they are able to identify and trace the root cause of the darknet traffic. The experimental results show that correlation analysis between the darknet traffic and IDS alerts is very useful to discover potential attack hosts, especially internal hosts, and to find out what kinds of malware infected them.

Keywords: IDS alerts; darknet traffic; potential attackers; in-depth analysis

1. Introduction

The darknet (i.e., a set of unused IP addresses) is a very useful solution for observing the global trends of cyber threats and analyzing attack activities on the Internet. Since the darknet is not connected with real systems, in most cases, the incoming packets on the darknet do not contain a payload. This means that we are unable to get real malware from the darknet traffic. This situation makes it difficult for security experts (e.g., academic researchers, engineers, operators, etc.) to identify whether the source hosts of the darknet traffic are infected by real malware or not. In this paper, the terms 'the source hosts' and 'the source IP addresses' mean all of the real systems connected to the Internet and do not include the darknet.

In our previous work [1,2], we proposed an advanced incident response framework whose main goal is to identify more dangerous IDS alerts [3–12] using the darknet traffic. In addition, we carried out a practical correlation analysis of IDS alerts and the darknet traffic, focusing on internal hosts that sent packet(s) to the darknet and showed how security operators are able to effectively identify internal attack hosts using the darknet traffic [13]. However, we did not provide any detailed information about the attack activities of the internal attack hosts and did not inspect them using security software.

Therefore, we were unable to identify the root cause of the attack activities, so that security operators cannot make any response against them.

In this paper, as an expansion of [14], in which we only proposed a methodology for conducting correlation analysis between IDS alerts and the darknet traffic, we present the overall procedure of the in-depth analysis between them using real data collected at the Science and Technology Cyber Security Center (S&T CSC) in Korea and provide the detailed in-depth analysis results. To the best of our knowledge, this is the first challenge to carry out the in-depth analysis for the darknet traffic, as well as IDS alerts. The ultimate goal of this paper is to provide practical experience, insight and know-how to security experts (e.g., academic researchers, engineers, operators, etc.) so that they are able to identify and trace the root cause of the darknet traffic.

Especially, we focus on the internal hosts that sent packets to the darknet and analyze IDS alerts related to the internal hosts. Furthermore, since the internal hosts are under the control of the organization, we inspected them using a dedicated anti-virus software, such that it is able to identify whether they are infected by malware or not. The proposed procedure consists of seven main phases, as described in Section 3: collection, extraction, classification, comparison, correlation analysis, identification and tracing.

In our experiments, we used 16*/24 darknet IP addresses for collecting the darknet traffic and a dedicated IDS [15], which is very similar to Snort [16] and is widely used in Korea, for correlation analysis between them. The experimental results show that correlation analysis between darknet traffic and IDS alerts is very useful to discover potential attack hosts, especially internal hosts, and to find out what kinds of malware (e.g., the name of a known virus or worm, unknown malware, etc.) infected them.

The rest of this paper is organized as follows. In Section 2, we give a brief description for existing approaches based on the darknet. In Section 3, we describe the procedure of the in-depth analysis. In Section 4, we provide experimental results obtained from the Science and Technology Security Center. Finally, we present concluding remarks and suggestions for future work in Section 5.

2. Related Work

The darknet is being used for studying and developing the countermeasures against malicious activities on the Internet [17–27]. For example, Bailey et al. introduced the Internet Motion Sensor (IMS), a globally-scoped Internet monitoring system. The goal of the IMS is to measure, characterize and track threats on the Internet [20,22]. Moore et al. introduced a network telescope that is a portion of the routed IP address space [21]. By using the network telescope, in that little or no legitimate traffic exists, they examined its utility and effects for measuring both pandemic incidents (the spread of an Internet worm) and endemic incidents (denial-of-service attacks) on the Internet. Nakao et al. introduced a network incident analysis center for tactical emergency response (nicter), which is monitoring around 300,000 unused IP addresses mainly located in Japan [17–19]. The main objective of the nicter is to carry out correlation analysis between the network threats observed in the darknet and malware executables captured in the various types of honeypots. Most of the existing approaches have mainly focused on only passively observing the darknet traffic to provide statistical information and recent attack trends, such as the rapid change of a certain scanning pattern and the gradual increase of attacks against a certain port, while this paper is aiming at collecting the darknet traffic and carrying out correlation and in-depth analysis with IDS alerts for identifying and tracing the root cause of potential cyber threats.

3. Overall Procedure of Correlation and In-Depth Analysis

Figure 1 shows the procedure of the proposed correlation and in-depth analysis method of IDS alerts for identifying and tracing potential attackers, i.e., attack hosts, that send attack packets to the darknet. Similar to [14], the procedure is composed of seven main phases: collection, extraction, classification, comparison, correlation analysis, identification and tracing. The each phase of the procedure is as follows.

1. Collection: During the first phase, all of the incoming network traffic whose destination IP addresses are the darknet is captured.
2. Extraction: In this phase, all of the source IP addresses that sent attack packets to the darknet are extracted. We call the source IP addresses 'potential attackers'.
3. Classification: The potential attackers are classified into two groups: the internal hosts and the external hosts. The former and the latter mean that they are located inside an outside an organization, respectively.
4. Comparison: The IDS alerts whose source IP addresses are the same as 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).
5. 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 the IP address, port number, protocol, packet size, type of IDS alerts, and so on.
6. Identification: The darknet traffic sent by the internal hosts and the corresponding IDS alerts are investigated by security operators so that they are able to identify internal attack hosts from their historical activities.
7. Tracing: Finally, the internal attack hosts are inspected by a dedicated anti-virus software so that one is able to find malware installed or running on them.

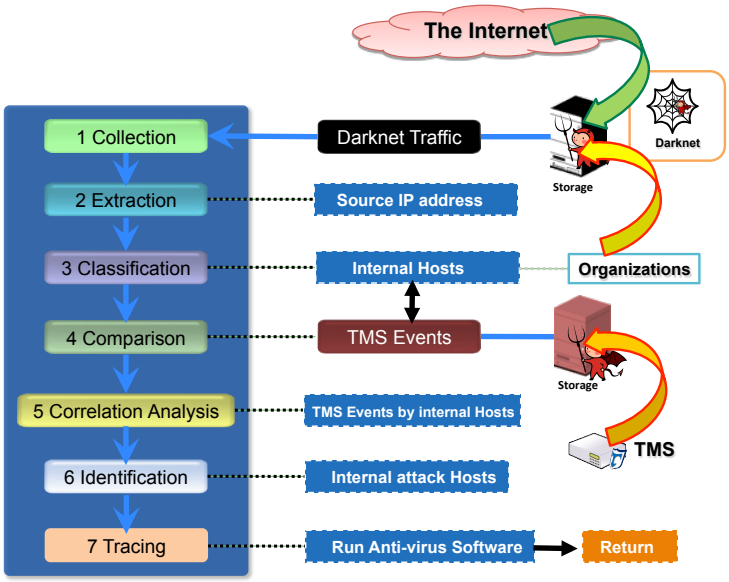

Figure 1. Procedure of the proposed analysis method.

4. Experimental Results

4.1. Correlation Analysis of Darknet Traffic and IDS Alerts

Figure 2 shows the experimental environment. In order to carry out correlation analysis between darknet traffic and IDS alerts, we prepared 16*/24 darknet (i.e., 4080 IP addresses) in Korea and collected all of the darknet traffic during six months (January 2013 to June 2013). Furthermore, we deployed a dedicated IDS in the boundary network of the 16*/24 darknet IP addresses.

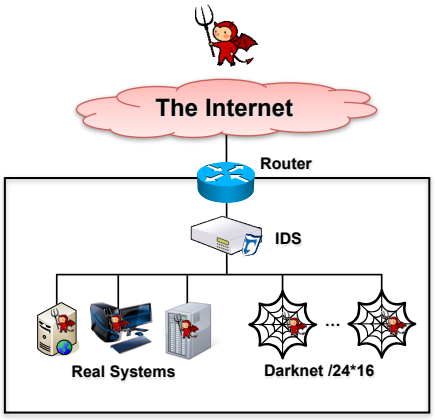

Figure 2. Experimental environment for in-depth analysis.

According to the procedure described in Section 3, we conducted the correlation analysis between all of the incoming darknet traffic and IDS alerts that were raised by a dedicated IDS.

- Extraction: We extracted source IP addresses from the entirety of the darknet traffic. We observed that 300 unique source IP addresses per day sent packets to our darknet on average.
- Classification: We then classified the source IP addresses into the internal hosts and the external hosts. After the classification phase, we observed that only eight internal hosts sent attack packets to our darknet. Table 1 shows the overview of the eight internal hosts observed on our darknet and the number of IDS alerts that were caused by the eight internal hosts. Note that we sanitized the IP addresses of the eight internal hosts and organizations for privacy.
- Comparison: We extracted the IDS alerts whose source IP addresses are matched to the eight internal hosts. In this comparison phase, we set the time interval to one month for comparing the darknet traffic and the IDS alerts. For example, if an internal host sent packets to the darknet on 15 January, we extracted the IDS alerts whose source IP addresses are the same as the internal host from 1 January to 31 January. As a result, as shown in Table 1, among the eight internal hosts, we can see that seven IP addresses also raised one and more IDS alerts during the predefined time interval, i.e., one month.
- Correlation analysis: In our further investigation, we observed that four internal hosts (i.e., the 5th, 6th, 7th and 8th internal hosts in Table 1) raised multiple types (i.e., scanning and web vulnerability) of IDS alerts, while three internal hosts (i.e., the 1st, 2nd and 3rd internal hosts in Table 1) raised a single type of IDS alert (i.e., scanning or web vulnerability).
- Identification: From these results, it could be concluded that seven internal hosts were infected by one and more malware, and consequently, they triggered many IDS alerts with different types; and their malicious activities were also observed on the darknet.

Table 1. Overview of 8 internal hosts observed on the darknet.

Internal Host	Date	IP	Organization	# of the Type of IDS Alerts
1st	15/01/2013	143.x.x.199	K***T	1
2nd	15/01/2013	210.x.x.87	K***T	1
3rd	23/01/2013	203.x.x.165	N*F	1
4th	27/01/2013	110.x.x.184	K***T	0
5th	15/02/2013	143.x.x.91	K***T	4
6th	31/03/2013	143.x.x.192	K***T	7
7th	04/04/2013	143.x.x.136	K***T	4
8th	11/05/2013	143.x.x.164	K***T	6

Figures 3–9 show the IDS alerts related to the seven internal hosts (i.e., the 1st, 2nd, 3rd, 5th, 6th, 7th and 8th) that sent packets to the darknet and also raised one or more IDS alerts. In Figures 3–9, the horizontal axis means the time, and the orange square boxes indicate the detection time of packets observed on the darknet. The Arabic numeral in the colored square boxes (e.g., blue, red, green, purple, etc.) indicates the number of IDS alerts that were triggered by the seven internal hosts, i.e., potential attackers. Furthermore, the color of the square boxes represents the type of IDS alerts. Furthermore, Tables 2–8 show the additional information (i.e., detection time, protocol, source and destination ports, packet size) for the corresponding internal hosts, i.e., the 1st, 2nd, 3rd, 5th, 6th, 7th and 8th, respectively.

From Figure 3, we can see that the first internal host raised one type of IDS alert. The name of the IDS alerts is "netbios xxxx smb Transaction". Note that we sanitized the name of IDS alerts due to security. The first internal host raised 19 IDS alerts before the detection time (i.e., 15 January) of darknet traffic. From Table 2, the first internal host used the TCP protocol, and the darknet traffic was destined to port 1925, while the IDS alerts were destined to many different ports. The packet sizes of darknet traffic and the IDS alerts were 304 and 846 bytes.

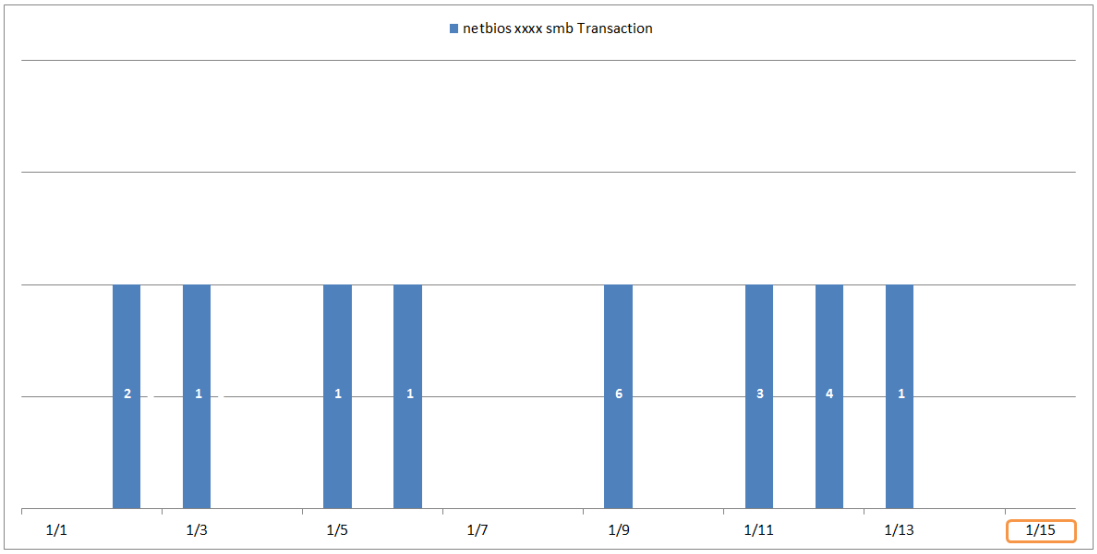

Figure 3. Activities of the first internal host in IDS alerts.

Table 2. Summary of IDS alerts and darknet traffic related to the 1st internal host.

Type	Darknet Traffic	IDS Alert
Detection Time	15/01/2013 00:52:16	Figure 3
Destination Port	1925	Many
Packet Size	304	846
Protocol	TCP	TCP

From Figure 4, we can see that the second internal host raised one type of IDS alert. The name of the IDS alert is "udpflooding". The second internal host raised many IDS alerts constantly before the detection time (i.e., 15 January) of darknet traffic. From Table 3, the second internal host used the UDP protocol, and the darknet traffic was destined to port 34902, while the IDS alerts were destined to many different ports. The packet size of darknet traffic was 352 bytes, while the IDS alerts have many different sizes of packets.

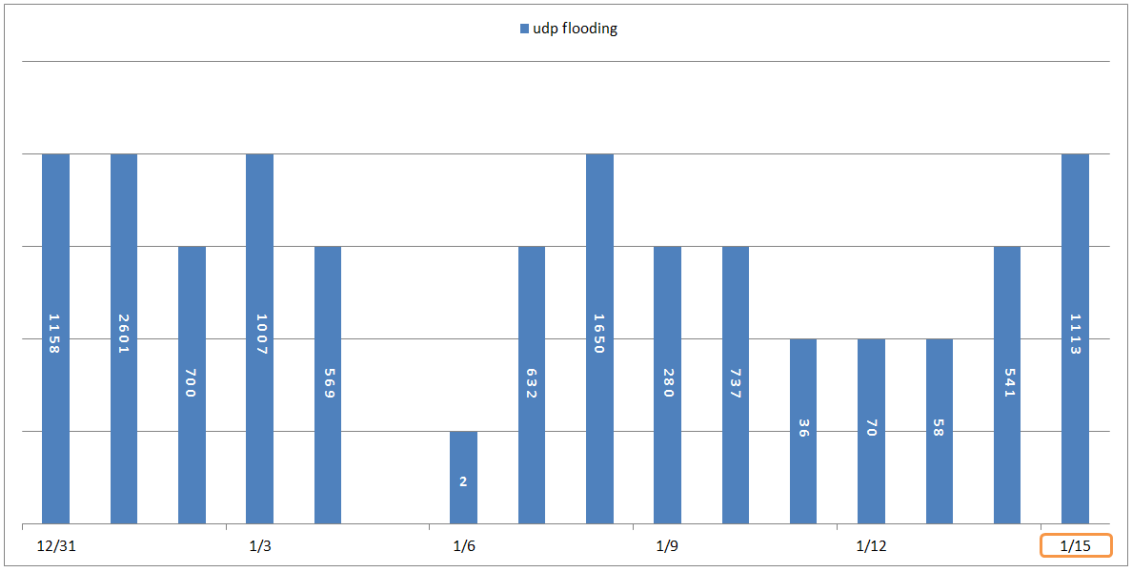

Figure 4. Activities of the second internal host in IDS alerts.

Table 3. Summary of IDS alerts and darknet traffic related to the 2nd internal host.

Type	Darknet Traffic	IDS Alert
Detection Time	15/01/2013 20:10:25	Figure 4
Destination Port	34902	Many (including 34902)
Packet Size	352	Many
Protocol	UDP	UDP

From Figure 5, we can see that the third internal host raised one type of IDS alert. The name of IDS alerts is "udp flooding". The third internal host raised 31 IDS alerts after the detection time (i.e., 23 January) of darknet traffic. From Table 4, the third internal host used the UDP protocol, and the darknet traffic was destined to port 47684, while the IDS alerts were destined to many different ports. The packet size of darknet traffic was 352 bytes, while the IDS alerts have many different sizes of packets.

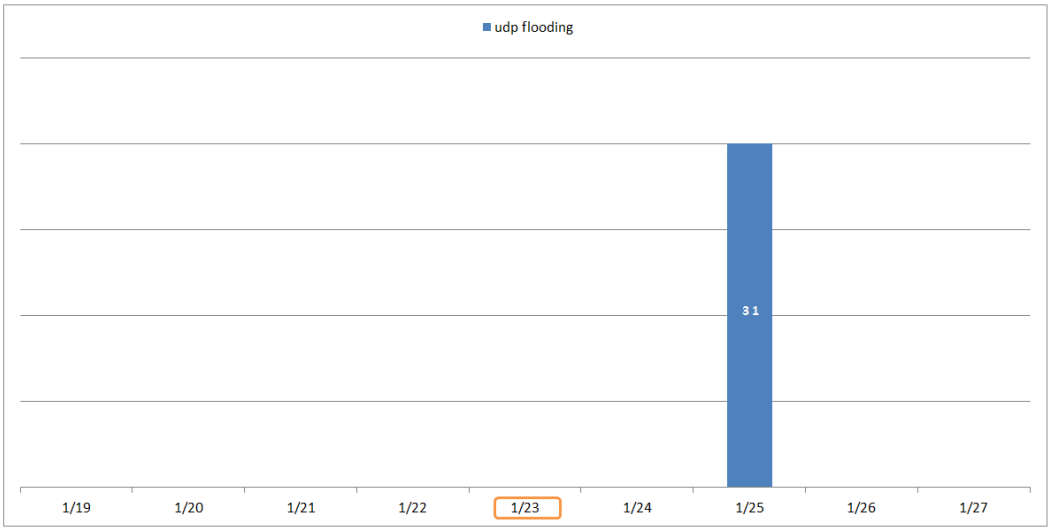

Figure 5. Activities of the third internal host in IDS alerts.

Table 4. Summary of IDS alerts and darknet traffic related to the 3rd internal host.

Type	Darknet Traffic	IDS Alert
Detection Time	23/01/2013 02:12:03	Figure 5
Destination Port	47684	47684
Packet Size	352	Many
Protocol	UDP	UDP

From Figure 6, we can see that the fifth internal host raised four types of IDS alerts. The names of the IDS alerts are "udp flooding", "trojan.xxxx malicious", "MicroSoft (MS)xxxx vulnerability" and "http xxxx remote". The fifth internal host raised 24 IDS alerts before the detection time (i.e., 15 February) of darknet traffic. From Table 5, the fifth internal host used UDP and the TCP protocol, and the darknet traffic was destined to port 16609, while the IDS alerts were destined to many different ports, including 16609. The packet size of darknet traffic was 352 bytes, while the IDS alerts have many different sizes of packets.

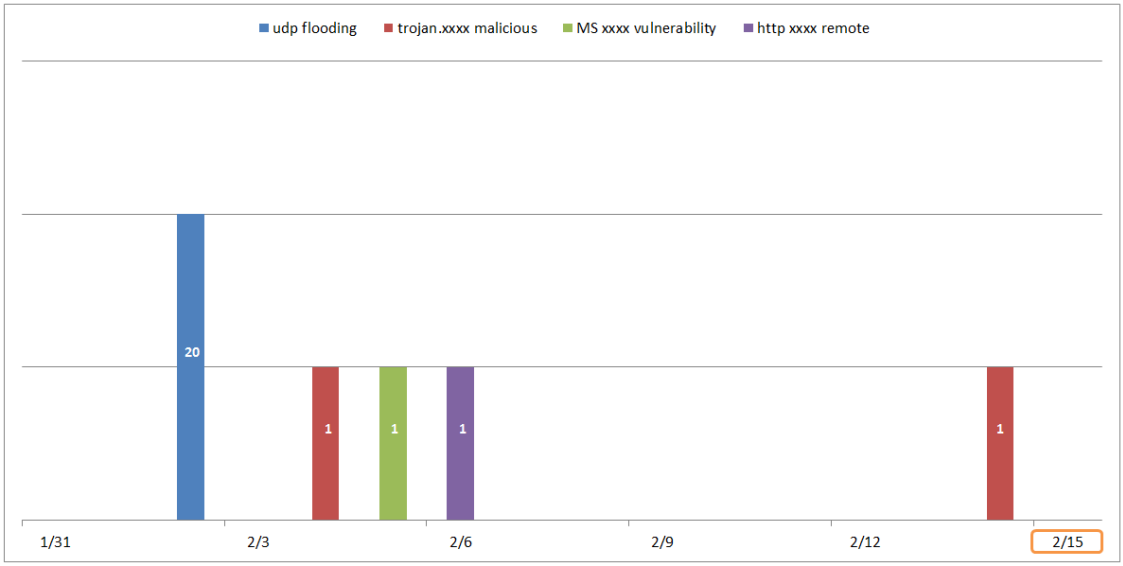

Figure 6. Activities of the fifth internal host in IDS alerts.

Table 5. Summary of IDS alerts and darknet traffic related to the 5th internal host.

Type	Darknet Traffic	IDS Alert
Detection Time	15/02/2013 04:57:23	Figure 6
Destination Port	16609	Many (including 16609)
Packet Size	352	Many
Protocol	UDP	UDP and TCP

From Figure 7, we can easily see that the sixth internal host raised seven different types of IDS alerts. Particularly, two alerts (i.e., "http xxx sqlinjection" and "udp port scan") were recorded before the detection time (i.e., 31 March) of darknet traffic, while four alerts (i.e., "Trojan.xxxx malicious", "MS xxxx vulnerability", "http PHP xxxx SQL Injection" and "dos xxxx agent ping") were raised after the detection time of darknet traffic.

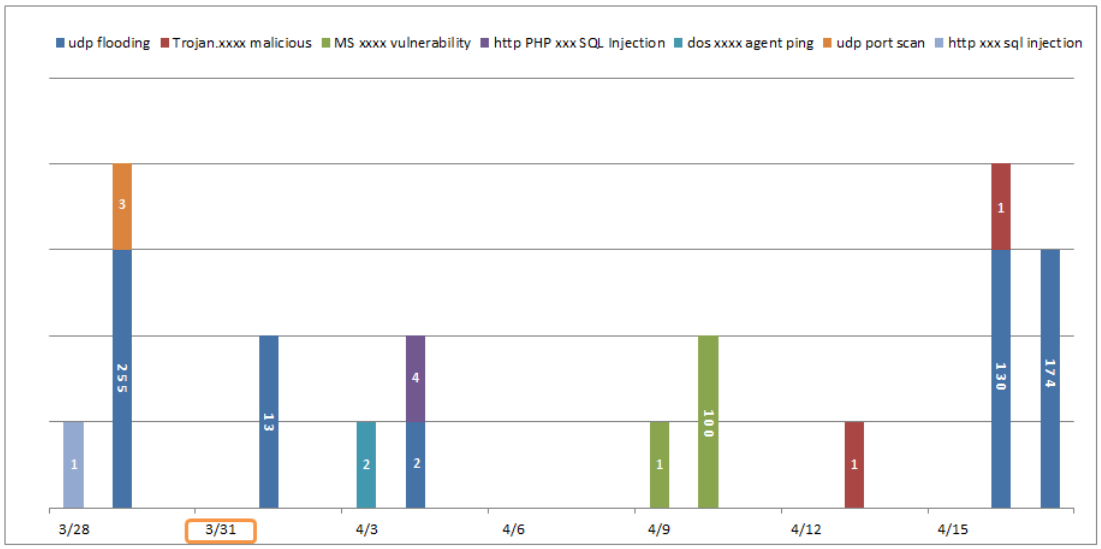

Figure 7. Activities of the sixth internal host in IDS alerts.

From Table 6, the sixth internal host used UDP and the TCP protocol, and the darknet traffic was destined to port 50226, while the IDS alerts were destined to many different ports, including 50226. The packet size of darknet traffic was 352 bytes, while the IDS alerts have many different sizes of packets.

Table 6. Summary of IDS alerts and darknet traffic related to the 6th internal host.

Type	Darknet Traffic	IDS Alert
Detection Time	31/03/2013 05:28:38	Figure 7
Destination Port	50226	Many (including 50226)
Packet Size	352	Many
Protocol	UDP	UDP and TCP

From Figure 8, we can see that the seventh internal host raised four types of IDS alerts. The names of IDS alerts are "udp flooding", "trojan.xxxx malicious", "dos xxxx agent ping" and "udp port scan". The seventh internal host raised many IDS alerts before and after the detection time (i.e., 4 April) of darknet traffic. From Table 7, the seventh internal host used UDP and the TCP protocol, and the darknet traffic was destined to port 15730, while the IDS alerts were destined to many different ports, including 15730. The packet size of darknet traffic was 352 bytes, while the IDS alerts have many different sizes of packets.

Table 7. Summary of IDS alerts and darknet traffic related to the 7th internal host.

Type	Darknet Traffic	IDS Alert
Detection Time	04/04/2013 03:06:54	Figure 8
Destination Port	15730	Many (including 15730)
Packet Size	352	Many
Protocol	UDP	UDP and TCP

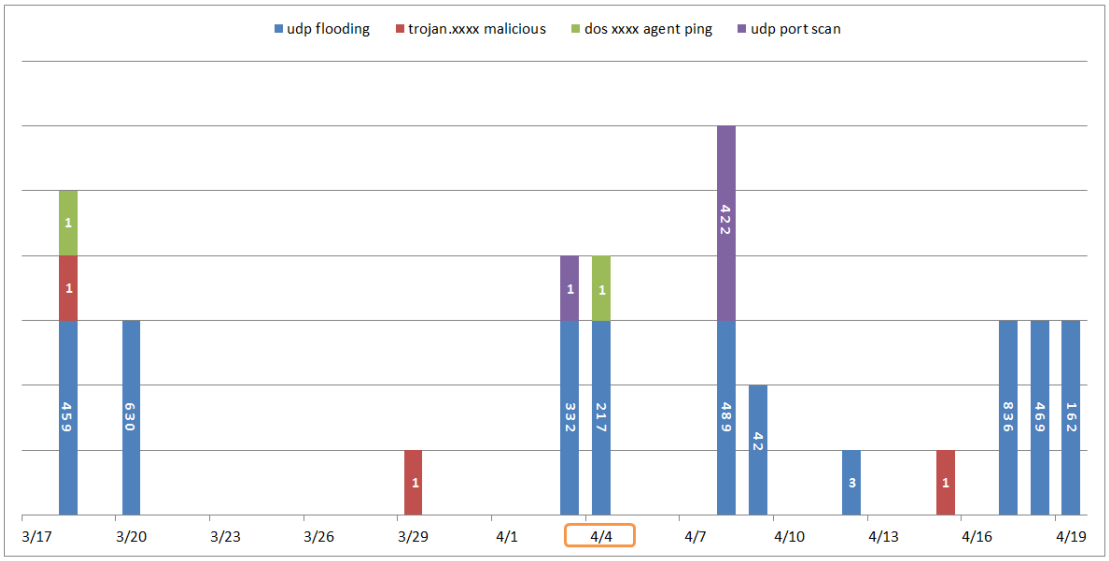

Figure 8. Activities of the seventh internal host in IDS alerts.

From Figure 9, we can see that the eight internal host raised six different types of IDS alerts. Especially, four alerts (i.e., "udp port scan", "dos xxxx agent ping", "dosxxxx agent ping 2" and "malware-hacking-mail") were recorded before the detection time (i.e., 11 May) of darknet traffic, while one alert (i.e., "http web attack tool") was triggered after the detection time of darknet traffic. From Table 8, the eight internal host used UDP and the TCP protocol, and the darknet traffic was destined to port 46201, while the IDS alerts were destined to many different ports, including 46201. The packet size of darknet traffic was 248 bytes, while the IDS alerts have many different sizes of packets.

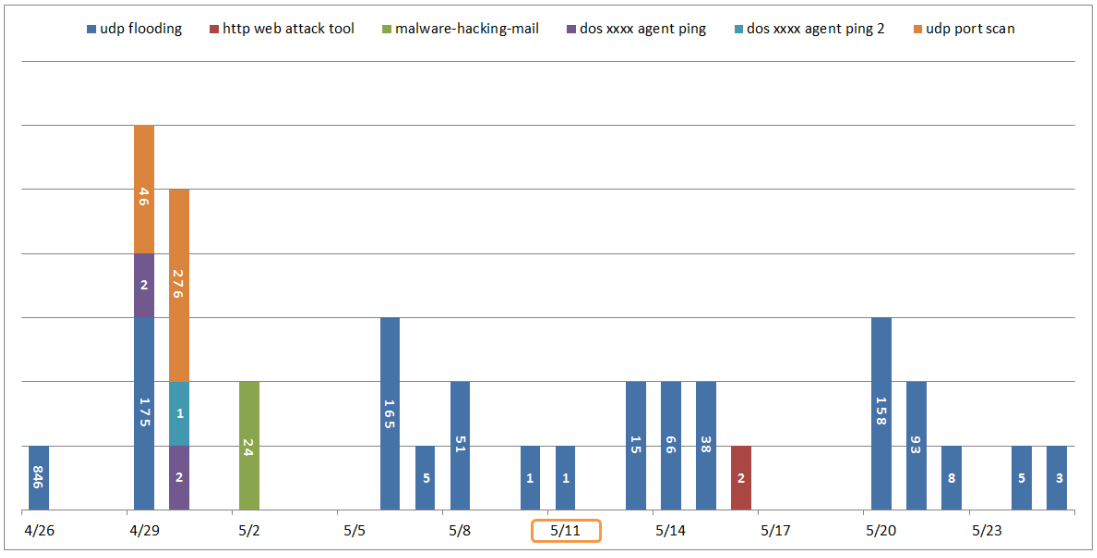

Figure 9. Activities of the eight internal host in IDS alerts.

Table 8. Summary of IDS alerts and darknet traffic related to the 8th internal host.

Type	Darknet Traffic	IDS Alert
Detection Time	05/11/2013 11:27:11	Figure 9
Destination Port	46201	Many (including 46201)
Packet Size	248	Many
Protocol	UDP	UDP and TCP

In addition, from Figures 3, 4 and 7–9, we can easily see that 'udp flooding' IDS alerts were raised during a long period of time. As a result, from these results, we can conclude that if an internal host sends any packet(s) to the darknet, it was already compromised by some malware. Therefore, it is strongly recommended to have a response against the internal host, such as blocking the IP address, removing the malware using security software, and so on.

4.2. Tracing and Identifying Potential Attackers

In order to carry out the in-depth analysis of potential attackers, i.e., attack hosts, that sent packets to the darknet, we prepared more experimental data collected from the same experimental environment in Figure 2. Similar to the correlation analysis in Section 4.1, we also deployed a dedicated IDS in the boundary network of the 16*/24 darknet IP addresses. We used the darknet traffic and IDS alerts of two months (September 2013 to October 2013) for tracing and identifying potential attackers from them.

According to the procedure described in Section 3, we conducted the in-depth analysis between all of the incoming darknet traffic and IDS alerts that were raised by the dedicated IDS.

- Extraction: We extracted source IP addresses from the entire darknet traffic.
- Classification: We then classified the source IP addresses into the internal hosts and the external hosts. After the classification phase, we observed that only 17 internal hosts sent attack packets to our darknet. Table 9 shows the overview of 17 internal hosts observed on our darknet. Note that we sanitized the IP addresses of the 17 internal hosts and organizations for privacy.
- Comparison: We extracted the IDS alerts whose source IP addresses are matched to the 17 internal hosts. In this comparison phase, we set the time interval between darknet traffic and the IDS alerts as one month. For example, if an internal host sent packets to the darknet on 16 September, we extracted the IDS alerts whose source IP addresses are the same as the internal host from 1 September to 1 October. As a result, as shown in Table 10, among the 17 internal hosts, we can see that five IP addresses (i.e., internal attack hosts) also raised one and more IDS alerts during one month.
- Correlation analysis: In our further investigation, we observed that one internal host raised multiple types of IDS alerts, while four internal hosts raised a single type of IDS alerts.
- Identification and tracing: We run anti-virus software to identify and trace malware on the five internal attack hosts. As a result, we observed that two attack hosts (i.e., the third and ninth in Table 9) were infected with 30 and 144 different types of malware; while the anti-virus software could not detect any malware from the other hosts (i.e., the 11th, 12th and 16th in Table 9). From these results, it could be concluded that two internal attack hosts were infected by many malwares, and consequently, they triggered many IDS alerts with different types; and their malicious activities were also observed on the darknet. Furthermore, there is a high possibility that the other three internal hosts were infected by unknown malwares that were not detected by the anti-virus software. Since the darknet traffic itself is caused by malicious activities, if the dedicated IDS records the corresponding security events, they also can be regarded as true positives, not false positives.

Table 9. Overview of 17 internal hosts observed on the darknet.

Internal Host	Date	Organization	IP	Return	Result
1st	16/09/2013	U*T	172.x.x.251	X	-
2nd	16/09/2013	K**T	143.x.x.127	X	-
3rd	**16/09/2013**	**K**M**	**210.x.x.232**	**O**	**30 malwares**
4th	16/09/2013	K**T	143.x.x.192	X	-
5th	16/09/2013	K**T	143.x.x.190	X	-
6th	16/09/2013	K**T	143.x.x.210	X	-
7th	17/09/2013	K***I	150.x.x.135	X	-
8th	25/09/2013	K****H	203.x.x.161	X	-
9th	**30/09/2013**	**K**S**	**134.x.x.63**	**O**	**144 malwares**
10th	03/10/2013	K****H	203.x.x.114	X	-
11th	**08/10/2013**	**K***C**	**210.x.x.172**	**O**	**No malware**
12th	**08/10/2013**	**K*T**	**203.x.x.177**	**O**	**No malware**
13th	08/10/2013	K***T	121.x.x.129	X	-
14th	08/10/2013	K**T	218.x.x.130	X	-
15th	15/10/2013	N**A	119.x.x.31	X	-
16th	**17/10/2013**	**K**S**	**210.x.x.232**	**O**	**No malware**
17th	19/10/2013	K***I	150.x.x.135	X	-

Table 10. Overview of 5 internal attack hosts observed on the darknet.

Attack Host	Date	IP	Organization	# of Types of IDS Alerts
3rd	16/09/2013	210.x.x.232	K**M	1
9th	30/09/2013	134.x.x.63	K**S	1
11th	08/10/2013	210.x.x.172	K***C	1
12th	08/10/2013	203.x.x.177	K*T	3
16th	17/10/2013	210.x.x.232	K**S	1

Figures 10–19 show the IDS alerts related to the five internal attack hosts (i.e., the 3rd, 9th, 11th, 12th and 19th) that sent packets to the darknet and also raised one and more IDS alerts, and the examples of the IDS alerts related to the five internal attack hosts.In Figures 10, 12, 14, 16 and 18, the horizontal axis means the time, and the orange square boxes indicate the detection time of packets observed on the darknet.

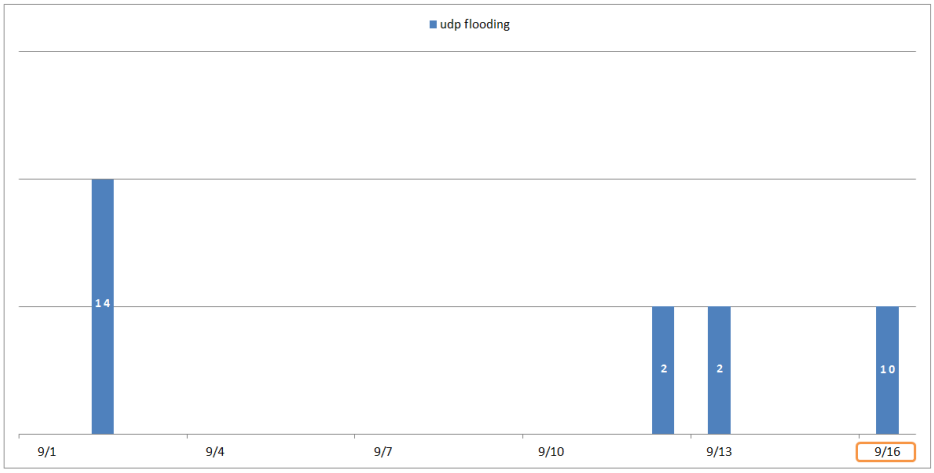

Figure 10. Activities of the third real attack host in IDS alerts.

The Arabic numeral in the colored square boxes (e.g., blue, red, green, purple, etc.) indicates the number of IDS alerts that were triggered by the five internal attack hosts. The color of the square boxes represents the type of IDS alert.

Figure 11. Examples of IDS alerts related to the third real attack host. The Korean means 'attack information'.

Tables 11–15 show the additional information (i.e., detection time, protocol, source and destination ports, packet size) for the corresponding internal attack hosts, i.e., the 3rd, 9th, 11th, 12th and 19th, respectively.

Table 11. Summary of IDS alerts and darknet traffic related to the 3rd real attack host.

Type	Darknet Traffic	IDS Alert
Detection Time	16/09/2013 17:45:00	Figure 10
Destination Port	Many	Many
Packet Size	316	Many
Protocol	UDP	UDP

From Figure 10, we can see that the third internal attack host raised one type of IDS alert. The name of IDS alert is "udp flooding". The third internal attack host raised 28 IDS alerts before the detection time (i.e., 16 September) of darknet traffic. Figure 11 shows the examples of the "udp flooding" alerts. Note that we sanitized the name of the IDS alerts and the IP addresses for security. From Table 11, the third internal attack host used the UDP protocol, and the darknet traffic and the IDS alerts were destined to many different ports. The packet size of darknet traffic was 316 bytes, while the IDS alerts have many different sizes of packets. In addition, as described in Table 9, the anti-virus software detected 30 different types of malware on the third internal attack host.

From Figure 12, we can see that the ninth internal attack host raised one type of IDS alert. The name of IDS alert is "DNS Sinkhole". The ninth internal attack host raised 10 IDS alerts after the detection time (i.e., 30 September) of darknet traffic. Figure 13 shows the examples of the "DNS

Sinkhole" alerts. From Table 12, the ninth internal attack host used TCP protocol, and the darknet traffic was destined to many different ports, while the destination ports of the IDS alerts were 5218 and 217. The packet size of darknet traffic was 264 bytes, while the IDS alerts have many different sizes of packets. In addition, as described in Table 9, the anti-virus software detected 144 different types of malwares on the ninth internal attack host.

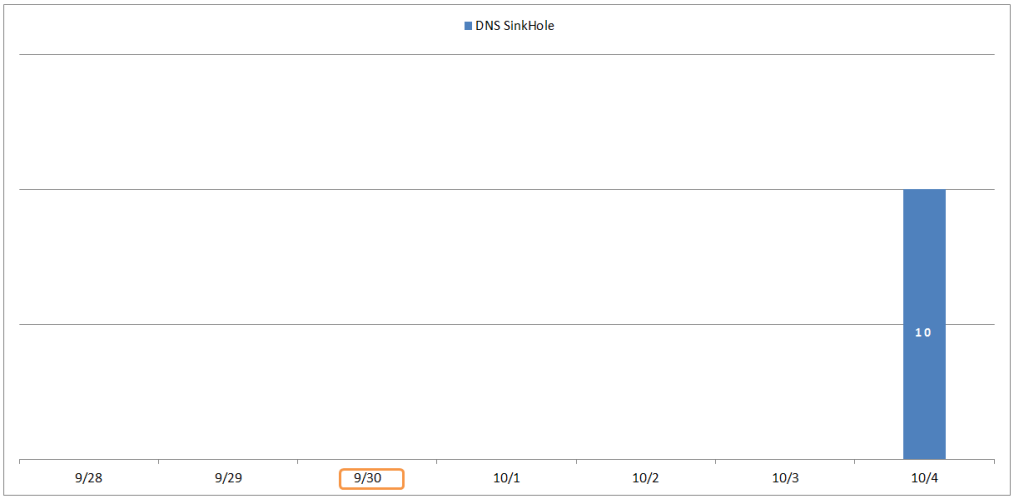

Figure 12. Activities of the ninth real attack host in IDS alerts.

Figure 13. Examples of IDS alerts related to the ninth real attack host. The Korean means 'attack information'.

Table 12. Summary of IDS alerts and darknet traffic related to the 9th real attack host.

Type	Darknet Traffic	IDS Alert
Detection Time	30/09/2013 11:48:00	Figure 12
Destination Port	Many	5218 and 217
Packet Size	264	Many
Protocol	TCP	TCP

From Figure 14, we can see that the 11th internal attack host raised one type of IDS alerts. The name of the IDS alert is "trojan.xxxx malicious". The 11th internal attack host raised six IDS alerts before and after the detection time (i.e., 8 October) of darknet traffic. Figure 15 shows the examples of the "trojan.xxxx malicious" alerts. From Table 13, the 11th internal attack host used UDP and the TCP protocol, and the darknet traffic was destined to port 5489, while IDS alerts were destined

to many different ports. The packet size of darknet traffic was 556 bytes, while the IDS alerts have many different sizes of packets. In addition, as described in Table 9, the anti-virus software could not detect any malware on the 11th internal attack host. This means that the 11th internal attack host was compromised by unknown malware.

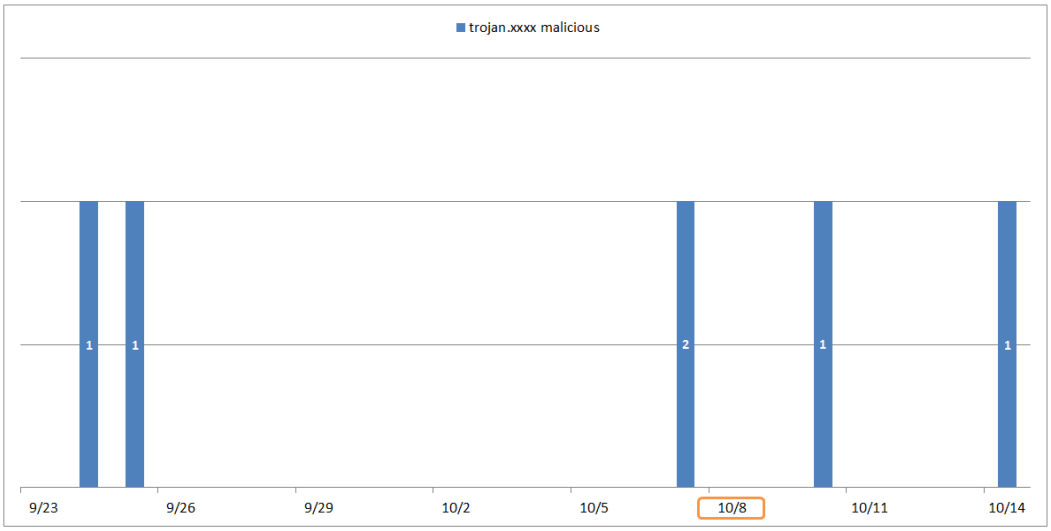

Figure 14. Activities of the 11th real attack host in IDS alerts.

Event Name	S_IP	S_PORT	D_IP	D_PORT		Detection Time
trojan 1	malicious domain	210.1 .172	2566	74.1 8.95	80	460 13-10-14 19:44:38
trojan 1	malicious domain	210.1 .172	4332	74.1 8.95	80	371 13-10-10 09:26:30
trojan 1	malicious domain	210.1 .172	4067	74.1 8.95	80	423 13-10-07 20:50:03
trojan 1	malicious domain	210.1 .172	2293	74.1 8.95	80	354 13-10-07 15:48:26
trojan 1	malicious domain	210.1 .172	1699	74.1 8.95	80	354 13-09-25 17:30:14
trojan 1	malicious domain	210.1 .172	4759	74.1 8.95	80	371 13-09-24 17:07:13

Figure 15. Examples of IDS alerts related to the 11th real attack host. The Korean means 'attack information'.

Table 13. Summary of IDS alerts and darknet traffic related to the 11th real attack host.

Type	Darknet Traffic	IDS Alert
Detection Time	08/10/2013 11:53:00	Figure 14
Destination Port	5489	Many
Packet Size	556	Many
Protocol	UDP	TCP

From Figure 16, we can see that the 12th internal attack host raised three types of IDS alerts. The names of IDS alerts are "udp flooding", "trojan.xxxx malicious" and "http sql injection". The 12th internal attack host raised many IDS alerts before and after the detection time (i.e., 8 October) of darknet traffic. Figure 17 shows the examples of the "udp flooding", "trojan.xxxx malicious" and "http sql injection" alerts. From Table 14, the 12th internal attack host used UDP and the TCP protocol, and the darknet traffic was destined to port 5489, while IDS alerts were destined to many different ports. The packet size of darknet traffic was 556 bytes, while the IDS alerts have many different sizes of packets. In addition, as described in Table 9, the anti-virus software could not detect any

malware on the 12th internal attack host. This means that the 12th internal attack host was infected by unknown malware.

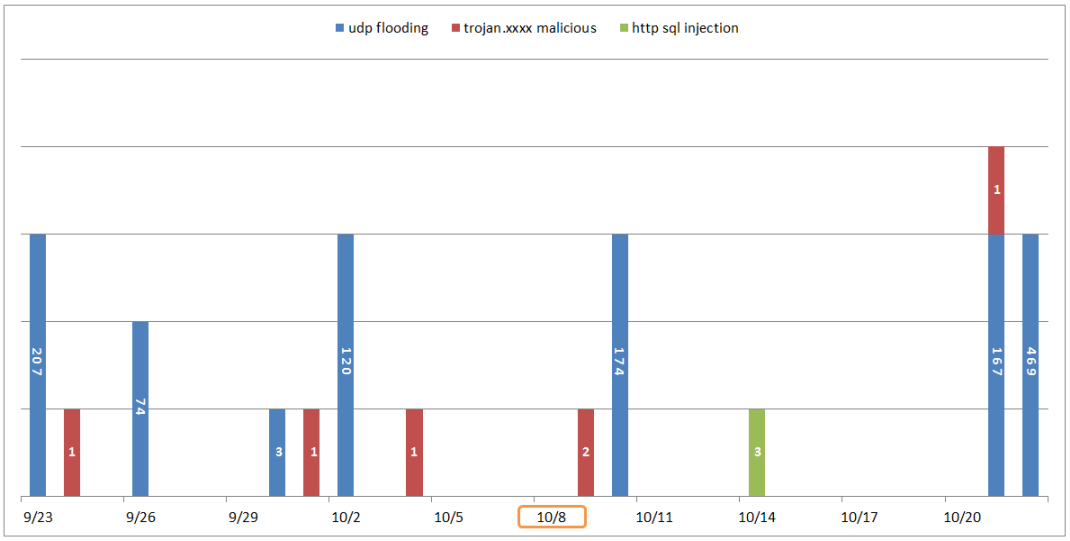

Figure 16. Activities of the 12th real attack host in IDS alerts.

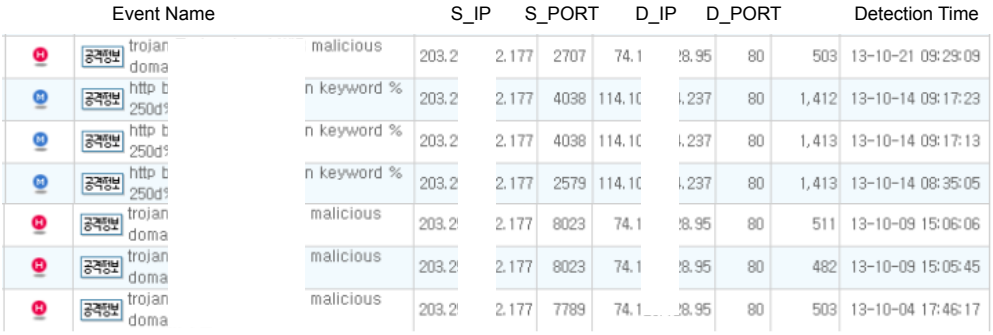

Figure 17. Examples of IDS alerts related to the 12th real attack host. The Korean means 'attack information'.

Table 14. Summary of IDS alerts and darknet traffic related to the 12th real attack host.

Type	Darknet Traffic	IDS Alert
Detection Time	08/10/2013 11:53:00	Figure 16
Destination Port	5489	Many
Packet Size	556	Many
Protocol	UDP	UDP and TCP

From Figure 18, we can see that the 16th internal attack host raised one type of IDS alert. The name of the IDS alert is "trojan.xxxx malicious". The 16th internal attack host raised five IDS alerts before the detection time (i.e., 17 October) of darknet traffic. Figure 19 shows the examples of the "trojan.xxxx malicious" alerts. From Table 15, the 16th internal attack host used the UDP protocol, and the darknet traffic was destined to many different ports, which the IDS alert was destined to port 62181. The packet size of darknet traffic has many different sizes of packets, while the packet size of the IDS alerts was 52,000 bytes. In addition, as described in Table 9, the anti-virus software could not detect any malware on the 16th internal attack host. This means that the 16th internal attack host was infected by unknown malware.

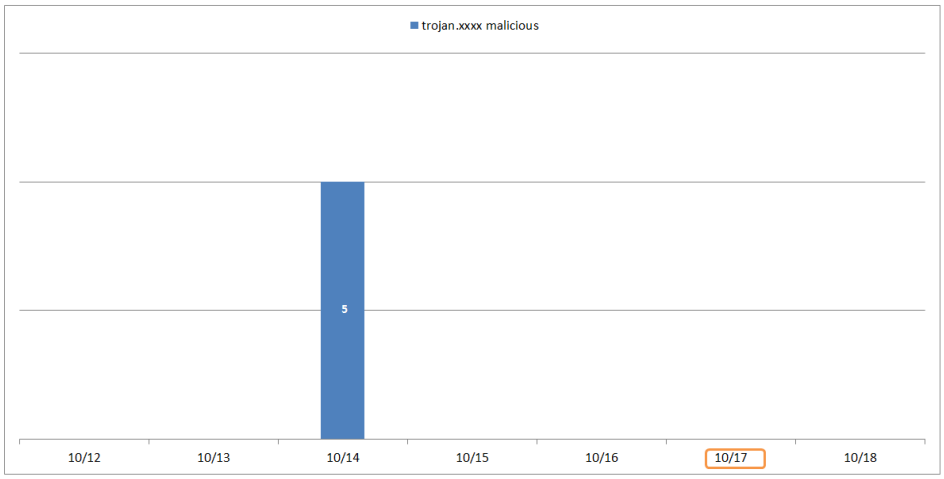

Figure 18. Activities of the 16th real attack host in IDS alerts.

		Event Name	S_IP	S_PORT	D_IP	D_PORT		Detection Time
1		공격정보 udp flooding - same ip	210.9	32	62181	211.2	8.196	6881	52,000	13-10-14 10:25:36
2		공격정보 udp flooding - same ip	210.9	32	62181	211.2	8.196	6881	52,000	13-10-14 10:25:26
3		공격정보 udp flooding - same ip	210.9	32	62181	210	56.68	6881	52,000	13-10-14 10:25:15
4		공격정보 udp flooding - same ip	210.9	32	62181	210	56.68	6881	52,000	13-10-14 10:25:05
5		공격정보 udp flooding - same ip	210.9	32	62181	210.	1.173	6881	52,000	13-10-14 10:24:18

Figure 19. Examples of IDS alerts related to the 16th real attack host. The Korean means 'attack information'.

Table 15. Summary of IDS alerts and darknet traffic related to the 16th real attack host.

Type	Darknet Traffic	IDS Alert
Detection Time	08/10/2013 11:53:00	Figure 18
Destination Port	Many	62181
Packet Size	Many	52,000
Protocol	UDP	UDP

5. Conclusions

In this paper, we have presented the procedure of carrying out the in-depth analysis of IDS alerts and darknet traffic, such that it is able to identify and trace the root cause of the darknet traffic. Especially, we focus on the internal hosts that sent packets to the darknet and analyze IDS alerts related to the internal hosts. Furthermore, we have proposed a method to inspect the internal hosts using a dedicated anti-virus software, so that it is able to identify whether they are infected by some malware or not. The proposed procedure consists of seven main phases, as described in Section 3: collection, extraction, classification, comparison, correlation analysis, identification and tracing.

In our experiments, we used 16*/24 darknet IP addresses for collecting darknet traffic and a dedicated IDS for correlation analysis between them. In the experiments, we detected five internal attack hosts that raised one and more IDS alerts. In addition, we identified that two internal attack hosts were infected by 30 and 144 malwares using the anti-virus software. Furthermore, the anti-virus software could not detect any malwares on the other three internal attack hosts. This means that they were infected by unknown malwares. As a results, it can be concluded that the proposed method for in-depth analysis is very useful to detect internal attack hosts (i.e., potential attackers) in organizations

and to find out malware (e.g., the name of known virus or worm, unknown malware, etc.) running or installed on them.

In the future work, we need to inspect the potential attacks, especially internal hosts infected by unknown malware, using more anti-virus software (e.g., Virustotal [28]) in order to identify them more precisely.

Acknowledgments: This research was supported by the "Building and Services of Information Security System Based on Advanced KREONET (Korea Research Environment Open NETwork)" Program funded by the Ministry of Science, ICT & Future Planning (K-17-L01-C04-S03).

Author Contributions: "Jungsuk Song designed the study, analyzed the data and wrote the manuscript; Younsu Lee and Jang-Won Choi desigend and performed the experiments; Sang-Soo Choi and Joon-Min Gil provided good advice throughout the paper; Jaekyung Han helped revise the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Choi, S.; Kim, S.; Park, H. An Advanced Security Monitoring and Response Framework Using Darknet Traffic. In Proceedings of the 2012 International Workshop on Information & Security, Tenerife, Spain, 2–5 December 2012; pp. 9–10.
2. Choi, S.; Song, J.; Park, H.; Choi, J. An Advanced Incident Response Framework Based on Suspicious Traffic. *J. Future Game Technol.* **2012**, *2*, 171–176.
3. Denning, D.E. An intrusion detection model. *IEEE Trans. Softw. Eng.* **1987**, *2*, 222–232.
4. Lina, W.C.; Keb, S.W.; Tsai, C.F. CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowl.-Based Syst.* **2015**, *78*, 13–21.
5. Kuanga, F.; Xua, W.; Zhang, S. A novel hybrid KPCA and SVM with GA model for intrusion detection. *Appl. Soft Comput.* **2014**, *18*, 178–184.
6. Elhaga, S.; Fernándezb, A.; Bawakidc, A.; Alshomranic, S.; Herrera, F. On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems. *Expert Syst. Appl.* **2015**, *42*, 193–202.
7. Hu, W.; Gao, J.; Wang, Y.; Wu, O.; Maybank, S. Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection. *IEEE Trans. Cybern.* **2014**, *44*, 66–82.
8. El-Semary, A.M.; Mostafa, M.G.M. Distributed and Scalable Intrusion Detection System Based on Agents and Intelligent Techniques. *J. Inf. Process. Syst.* **2010**, *6*, 481–500.
9. Kim, B.J.; Kim, I.K. Robust Real-Time Intrusion Detection System. *J. Inf. Process. Syst.* **2005**, *1*, 9–13.
10. Ponomarchuk, Y.; Seo, D. Intrusion Detection based on Traffic Analysis and Fuzzy Inference System in Wireless Sensor Networks. *J. Converg.* **2010**, *1*, 35–42.
11. Jingle, I.D.J.; Rajsingh, E.B. ColShield: An effective and collaborative protection shield for the detection and prevention of collaborative flooding of DDoS attacks in wireless mesh networks. *Hum.-Centric Comput. Inf. Sci.* **2014**, *4*, 1–19.
12. Song, J.; Takakura, H.; Kwon, Y. A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts. In Proceedings of the International Symposium on Applications and the Internet, Turku, Finland, 28 July–1 August 2008; The IEEE CS Press: Washington, DC, USA, 2008; pp. 51–56.
13. Choi, S.; Song, J.; Kim, S.; Kim, S. A model of analyzing cyber threats trend and tracing potential attackers based on darknet traffic. *Secur. Commun. Netw.* **2014**, *7*, 1612–1621.
14. Song, J.; Lee, Y.; Choi, J.; Gil, J.; Choi, S. An In-Depth Analysis Methodology of IDS Alerts for Identifying Potential Cyber Threats on Darknet. In Proceedings of the International Conference on Future Information Technology, Applications and Services, Seoul, Korea, 20–22 October 2016; pp. 35–37.
15. TMS (Threat Management System). Available online: http://www.kornicglory.co.kr/default/product/security/solution/tess_tms.php (accessed on 10 February 2017).
16. SNORT. Available online: https://www.snort.org (accessed on 10 February 2017).
17. Nakao, K.; Inoue, D.; Eto, M.; Yoshioka, K. Practical Correlation Analysis between Scan and Malware Profiles against Zero-Day Attacks Based on Darknet Monitoring. *IEICE Trans. Inf. Syst.* **2009**, *92*, 787–798.

18. Eto, M.; Inoue, D.; Song, J.; Nakazato, J.; Ohtaka, K.; Nakao, K. nicter: A Large-Scale Network Incident Analysis System. In Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, Salzburg, Austria, 10 April 2011; ACM: New York, NY, USA, 2011; pp. 37–45.
19. Ban, T.; Eto, M.; Guo, S.; Inoue, D.; Nakao, K.; Huang, R. A Study on Association Rule Mining of Darknet Big Data. In Proceedings of the 2015 International Joint Conference on Neural Networks (IJCNN), Killarney, Ireland, 12–17 July 2015.
20. Bailey, M.; Cooke, E.; Jahanian, F.; Nazario, J.; Watson, D. The Internet Motion Sensor: A distributed blackhole monitoring system. In Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security, San Diego, CA, USA, 3–4 February 2005; pp. 67–179.
21. Moore, D.; Shannon, C.; Voelker, G.M.; Savage, S. Network Telescopes: Technical Report. 2004. Available online: http://ants.iis.sinica.edu.tw/3bkmj9ltewxtsrrvnoknfdxrm3zfwrr/17/tr-2004-04.pdf (accessed on 10 February 2017).
22. Bailey, M.; Cooke, E.; Jahanian, F.; Myrick, A.; Sinha, S. Practical darknet measurement. In Proceedings of the 2006 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 22–24 March 2006.
23. Fachkha, C.; Bou-Harb, E.; Debbabi, M. Inferring distributed reflection denial of service attacks from darknet. *Comput. Commun.* **2015**, *62*, 59–71.
24. Bhanu, S.; Khilari, G.; Kumar, V. Analysis of SSH attacks of Darknet using Honeypots. *Int. J. Eng. Dev. Res.* **2014**, *3*, 348–350.
25. Furutani, N.; Ban, T.; Nakazato, J.; Shimamura, J.; Kitazono, J.; Ozawa, S. Detection of DDoS Backscatter Based on Traffic Features of Darknet TCP Packets. In Proceedings of the 9th Asia Joint Conference on Information Security, Wuhan, China, 3–5 September 2014.
26. Pang, S.; Komosny D.; Zhu, L.; Zhang, R.; Sarrafzadeh, A.; Ban, T.; Inoue, D. Malicious Events Grouping via Behavior Based Darknet Traffic Flow Analysis. *Wirel. Pers. Commun.* **2016**, doi:10.1007/s11277-016-3744-4.
27. Liu, J.; Fukuda, K. Towards a taxonomy of darknet traffic. In Proceedings of the International Wireless Communications and Mobile Computing Conference, Nicosia, Cyprus, 4–8 August 2014.
28. Virustotal. Available online: https://www.virustotal.com (accessed on 10 February 2017).