DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System

Daisuke Inoue
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795 Japan
dai@nict.go.jp

Koei Suzuki
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795 Japan
koei@nict.go.jp

Mio Suzuki
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795 Japan
mio@nict.go.jp

Masashi Eto
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795 Japan
eto@nict.go.jp

Koji Nakao
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795 Japan
ko-nakao@nict.go.jp

ABSTRACT
A darknet is a set of unused IP addresses whose monitoring is an effective way of detecting malicious activities on the Internet. We have developed an alert system called DAEDALUS (direct alert environment for darknet and livenet unified security), which is based on large-scale darknet monitoring. This paper presents a novel real-time 3D visualization engine called DAEDALUS-VIZ that enables operators to grasp visually and in real time a complete overview of alert circumstances and provides highly flexible and tangible interactivity. We describe some case studies and evaluate the performance of DAEDALUS-VIZ.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – *Security and protection*;
C.2.3 [**Computer-Communication Networks**]: Network Operations – *Network monitoring*;
H.5.2 [**Information Interfaces and Presentation**]: User Interface – *Graphical user interfaces (GUI)*, *Screen design*

General Terms
Design, Experimentation, Security

Keywords
Darknet monitoring, alert system, real-time visualization

VizSec '12, October 15 2012, Seattle, WA, USA

1. INTRODUCTION
A darknet is a set of globally announced unused IP addresses, the monitoring of which is an effective way of detecting a global trend in malicious activities on the Internet. We have been developing the nicter[1] system [1][2] that consists of a large-scale darknet monitoring facility, using which we can observe approximately 190,000 unused IPv4 addresses. In order to protect live networks (hereafter, livenets) by means of darknet monitoring, we have developed an alert system called DAEDALUS[2] [3]. It has been operating in collaboration with many organizations, and therefore, enormous numbers of alerts are sent to operators at the nicter center.

In this paper, we introduce DAEDALUS-VIZ, which enables operators to grasp visually and in real time a complete overview of alert circumstances. It also provides highly flexible and tangible interactivity with the alerts as well as darknet traffic.

In Section 2, we mention some related works. In Section 3, an overview of DAEDALUS is presented. Then we introduce DAEDALUS-VIZ in Section 4. Sections 5 and 6 provide some case studies and evaluations, respectively. Finally, we present our conclusions in Section 7.

2. RELATED WORKS
Over the past several years, a number of visualization technologies have been proposed to monitor and analyze network traffic and alerts of intrusion detection system (IDS) [4].

2.1 Alert Visualization
Some of the above-mentioned technologies visualize IDS alerts to support network operators in order to intuitively detect underlying anomalies from a large number of alerts [5]-[8].

IDS RainStorm [5] visualizes IDS alerts over time and incorporates flexible options of zooming and drilling down to

[1] network incident analysis center for tactical emergency response

[2] direct alert environment for darknet and livenet unified security

details. By plotting IDS alerts on a chart, where the x- and y-axes denote their time and location (i.e., local IP address), respectively, IDS RainStorm allows operators to easily understand trends in the alerts. However, since IDS RainStorm focuses on the visualization of only an overview of numerous IDS alerts over a long time, it is not adequate for attracting the operators' attention to the latest alerts to which they have to respond.

VisAlert [8] reveals the correlation between multiple data sources, such as IDS alerts and system log files based on the What, When, and Where attributes of the source data. In VisAlert views, alerts are depicted along outer rings that denote the type (What) of the alerts. In the center of the view, network topology is drawn to indicate the locations (Where) of the alerts. The time (When) attribute is represented by the distance between the center of the ring and the alert sign.

Itoh et al. proposed an IDS alert visualization tool that employs a hierarchical data visualization technique [6]. Their proposed tool efficiently utilizes a 2D display field by visualizing thousands of hierarchical leaf nodes and alerts in a network equally in one display space.

VisAlert and the technique described in [6] are novel visualization technologies that efficiently integrate multiple attributes (e.g., network nodes and data sources) within a single 2D display field.

2.2 Traffic Visualization

In addition to the research on alert visualization, there have been several studies on the visualization of network traffic for detecting anomalous activities in the network [9]-[14].

Rumint [9] is a packet-level visualization engine that employs a novel visualization technique called binary rainfall, where each packet is plotted, one per row, and where each pixel represents a bit in the packet. Since detailed packet data (i.e., header and payload data) are depicted in one view, operators can obtain a quick overview of the current network traffic and understand its characteristics. In terms of real-time visualization of raw packet data, our motivation behind the present study falls into the same category as that of Rumint; however, our motivation includes providing a view that explains the semantics of the traffic data, such as the logical geography (location of IP address) of nodes and the connectivity among them.

NVisionIP [14] visualizes the current status of a class-B network based on the NetFlow data collected from routers in the network. The galaxy view of the NVisionIP gives an operator the broadest view of his/her network by means of a chart in which the network and host addresses are respectively assigned to the x- and y-axes. Using this tool, the operator can grasp the current status of the network. Since NVisionIP can depict only one class-B network, it is not suitable for analysts monitoring multiple networks by distributed sensors.

In summary, there have been several related works that tried to efficiently integrate many attributes under the physical restriction of a 2D display space. In order to incorporate more extensive information within a display, we believe a 3D display space (as mentioned in [15]), is a better solution for a novel visualization technology. Moreover, there have been few studies on the simultaneous real-time visualization of raw network traffic (packet data) and alert information. Our goal is to develop a novel visualization engine that depicts alert information as well as packet data in real time in a 3D display space.

3. OVERVIEW OF DAEDALUS

DAEDALUS is a real-time alert system based on a large-scale darknet monitoring facility that has been deployed as a part of the nicter system. Large-scale darknet monitoring is an effective approach to detecting a global trend in malicious activities on the Internet, such as a worldwide spread of malwares. There is, however, a gap between darknet monitoring and actual security operations on livenets: monitoring the global trend does not make a very direct contribution toward livenet protection.

DEADALUS is a novel application of large-scale darknet monitoring whose objective is to bridge this gap, thereby contributing significantly to the security of livenets. In contrast to conventional methods, wherein only the packets received from outside the organization are observed, we employ a large-scale distributed darknet that consists of several organizations that mutually observe the malicious packets transmitted from inside the organizations.

DAEDALUS consists of an analysis center (i.e., nicter) and several organizations. Each organization installs a darknet sensor and establishes a secure channel between it and the analysis center, and continuously forwards darknet traffic toward the center. In addition, each organization registers the IP address range of its livenet at the center in advance. Figure 1 illustrates the overall architecture of DAEDALUS.

We divide the darknet into two types: internal and external. From the viewpoint of an organization, the darknet within its own organization is an internal darknet, and the darknets in other organizations are external darknets.

3.1 Internal Darknet Alert (Local Scan)

As shown in Figure 2, when a malware infection occurs in organization G and the infected host starts scanning the inside of the organization, including the internal darknet, the analysis center can detect the infection on the basis of the match between the source IP address of the darknet traffic from organization G and the preregistered livenet IP address. The analysis center then sends an alert to organization G.

3.2 External Darknet Alert (Global Scan)

When the infected host starts scanning outside the organization, including the external darknet in organization A in Figure 3, the analysis center detects the infection as described in Section 3.1. It then sends an alert to organization G.

3.3 External Darknet Alert (Backscatter)

When a host in organization G in Figure 4 is under a distributed denial of service (DDoS) attack from many spoofed IP addresses, the host sends backscatter (TCP SYN-ACK) packets to a wide area, including the external darknets in organizations A and B. The analysis center detects the backscatter as described in Section 3.1. It then sends an alert to organization G.

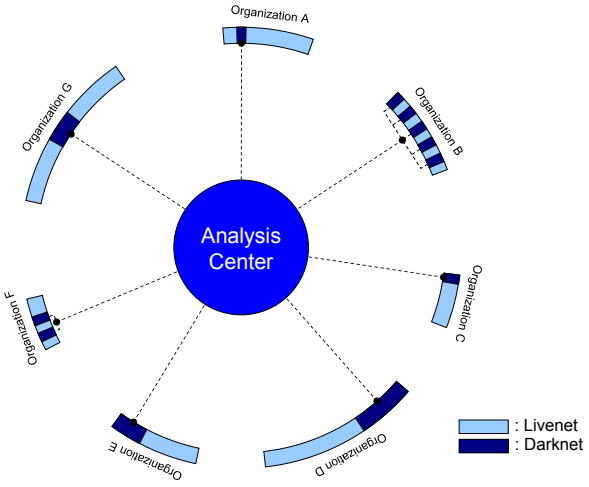

Figure 1. DAEDALUS Architecture

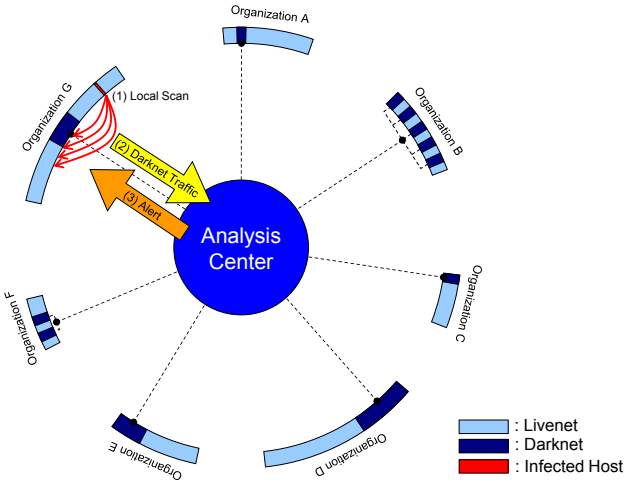

Figure 2. Internal Darknet Alert (Local Scan)

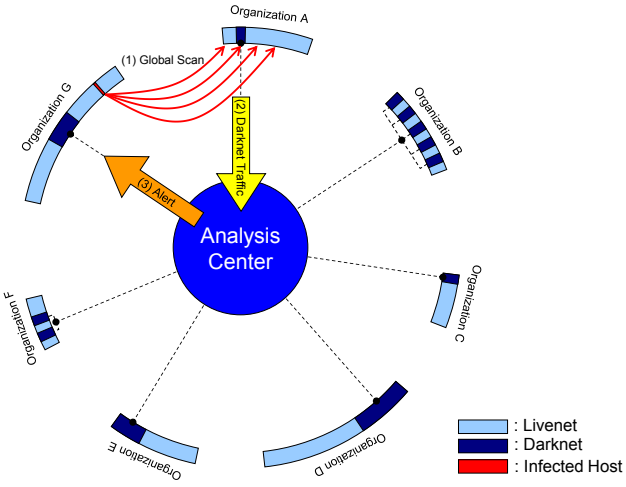

Figure 3. External Darknet Alert (Global Scan)

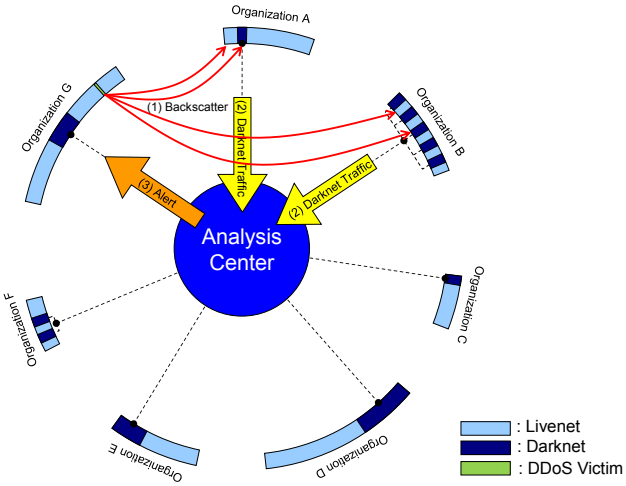

Figure 4. External Darknet Alert (Backscatter)

```
<?xml version="1.0"?>
 <NicterEvent>
  <Header>
   <EventType>DaedalusAlert</EventType>
   <CreateTime>2011-12-19 11:00:45</CreateTime>
  </Header>
  <DaedalusAlertHeader>
   <AlertID>277761</AlertID>
   <OrgID>2</OrgID>
   <Trigger>Periodic</Trigger>
   <Duration>3600</Duration>
  </DaedalusAlertHeader>
  <AlertData EventTime="2011-12-19 11:00:39" EventID="1096117" SrcIP="xxx.yyy.236.116" SrcCC="JP" TotalPacketCount="878" DisplayedPacketCount="878" Type="Continued">
   <Packet PacketTime="2011-12-19 10:01:21" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:31" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:33" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:35" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="445" SrcPort="3580" Protocol="6" Flag="2" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:38" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="445" SrcPort="3580" Protocol="6" Flag="2" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:42" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:44" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="" SrcPort="" Protocol="1" Flag="8" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:45" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="445" SrcPort="3580" Protocol="6" Flag="2" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:47" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="137" SrcPort="137" Protocol="17" Flag="" DarknetType="internal"/>
   <Packet PacketTime="2011-12-19 10:01:48" DstIP="xxx.yyy.241.101" DstCC="JP" DstPort="137" SrcPort="137" Protocol="17" Flag="" DarknetType="internal"/>
   <!– SNIP -->
  </AlertData>
 </NicterEvent>
```

Figure 5. Example of a DAEDALUS Alert

3.4 Alert Format

Figure 5 shows a real example of a DAEDALUS alert in XML format. The alert is generated for each source IP address (xxx.yyy.236.116 in this case) that accessed the darknet. The alert includes several types of meta data, e.g., creation time of the alert, alert ID, organization ID, trigger of the alert (periodic or urgent), duration of the alert in seconds. The alert also includes a summary of an event, which is the cause of the alert, that shows the event ID, source IP address, source country code, number of packets in the event, and event type (new or continued). The latter part of the alert describes the details of the event, i.e., information on each packet, including arrival time, destination IP address, destination country code, source/destination port, protocol, TCP flag, and type of the accessed darknet (internal or external).

4. DAEDALUS-VIZ

4.1 Motivation

DAEDALUS-VIZ is a real-time 3D visualization engine for DAEDALUS alerts as well as darknet traffic. Herein we describe our motivation behind developing DAEDALUS-VIZ.

We have been operating DAEDALUS for several years in collaboration with many organizations where darknet sensors have been installed. DAEDALUS automatically emails XML-based alerts to the corresponding organizations according to the alert mechanisms described in Section 3. At the same time, all alerts are sent to operators at the nicter center as well. The operators are now accustomed to receiving an enormous number of alerts every day; consequently, they find checking the alerts cumbersome, and sometimes they overlook critical incidents.

Although this problem is a generic issue for every alert system, we believe that the visualization technology for the alert system could ameliorate it. This practical issue motivated us to develop DAEDALUS-VIZ.

4.2 Contributions

The contributions of DAEDALUS-VIZ can be listed as follows:

- **Novelty**: It provides novel visualization methodologies, such as a mechanism for mapping IPv4 addresses on a sphere, darknet and livenet representation in a ring, packets with a comet shape, etc.
- **Real-timeness**: It makes possible the animation of the DAEDALUS alerts sent to all the cooperating organizations, as well as large-scale darknet traffic in true real-time.
- **Bird's-eye view and deep dive**: It allows the operator to see an overview of all the alert circumstances and to drill down into packet-by-packet information with a continuous view.
- **Interactivity**: It provides a highly interactive user interface, with facilities such as flexible viewpoint change, smooth magnification and minimization, tangible 3D objects including alerts and packets, any-time pause and resume, etc.
- **Customizability**: It enables the operator to flexibly customize almost all the parameters related to the visualization (e.g., color, shape, size, position, duration of all 3D objects) through a graphical user interface (GUI). It also provides a fine-grained packet filtering function.

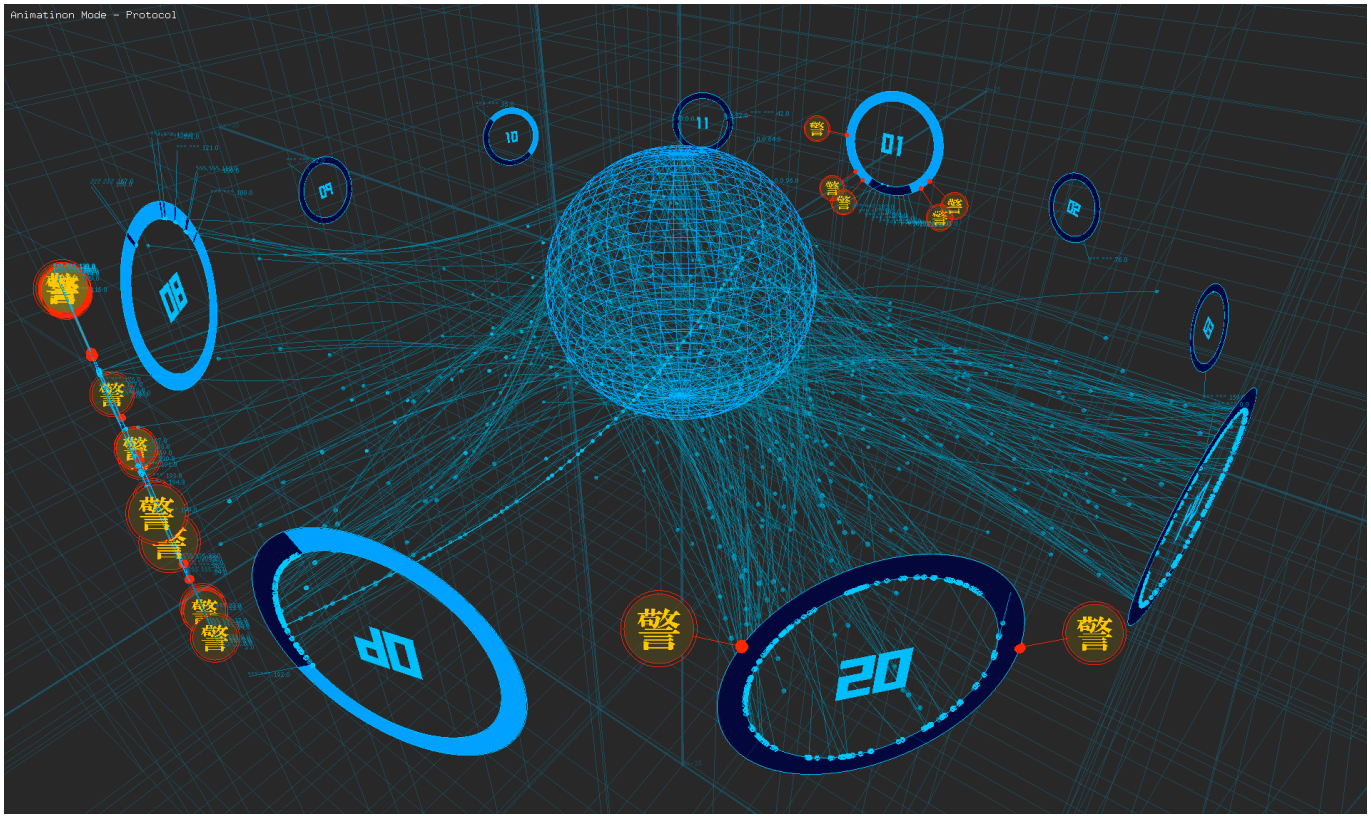

Figure 6. Overview of DAEDALUS-VIZ

4.3 Overview

DAEDALUS-VIZ, as illustrated in Figure 6, has two components: a central sphere with a wireframe, and several rings around the sphere. The sphere represents the Internet, and the rings represent the organizations that are the subjects for the DAEDALUS alert system (i.e., monitored organizations). In between the sphere and rings, hundreds of comet-shaped darknet packets continuously drift from the sphere to the rings in real time.

4.3.1 Sphere

The sphere, as illustrated in Figure 7, represents a complete IPv4 address space on the Internet. A /16 network (i.e., 2^{16} = 65,536 addresses) sequentially maps on to a meridian from the North Pole to the South Pole. In total, 65,536 meridians (representing from 0.0.0.0/16 to 255.255.0.0/16, respectively) are placed around the surface of the sphere in order. The IP addresses that are assigned to the monitored organizations are excluded from the mapping on the sphere since they are on the rings.

4.3.2 Ring and alerts

A ring, as illustrated in Figure 8, represents an organization monitored by DAEDALUS. The IP addresses assigned to the organization are on the periphery of the ring in a sequential manner. The lite blue parts of the ring are mapped livenets, and the dark blue parts are mapped darknets in the organization. The ring revolves around the sphere and rotates clockwise. The purpose of this self-rotation is to hide the start and end address of the organization since the location of the darknet should be kept secret. The number in the center of the ring indicates the unique identifier of the organization.

The icons showing Chinese characters (indicating "caution") around the ring are DAEDALUS alerts. Each alert indicates an IP address in the livenet that has sent some packets to internal and/or external darknet(s). The color of the Chinese character signifies a trigger and the type of the alert (as mentioned in Section 3.4). In Figure 8, all alerts are yellow, which means they are continued and periodic alerts. If an IP address in the livenet starts anew to send packets to some darknet, a red alert will be immediately displayed on the entire screen, as shown in Figure 9, in order to emphasize it to the operators; and the address will be indicated on the ring. If an operator clicks or double-clicks on an alert icon, its meta data or the details of the darknet packets can be displayed, respectively.

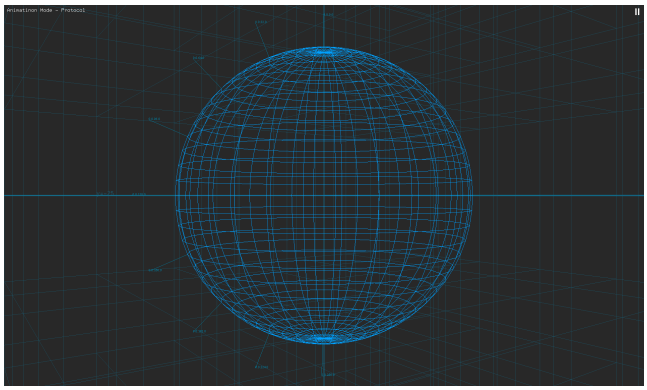

Figure 7. Sphere

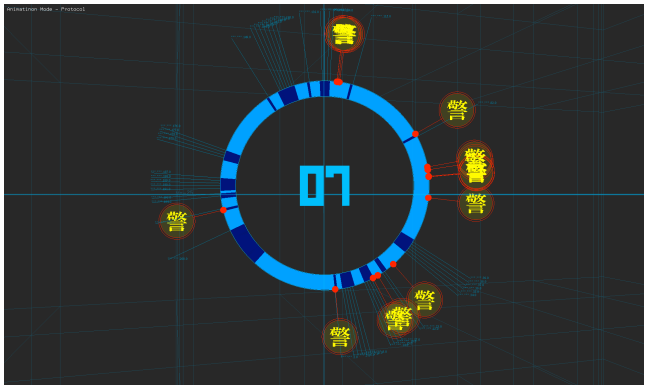

Figure 8. Ring and Alerts

Figure 9. New Alert

4.4 Filtering Function

DAEDALUS-VIZ provides a highly flexible filtering function for darknet traffic. The following parameters and their combinations can be used to determine filtering rules.

- Source and destination IP addresses and network address represented in the CIDR[3] notation (Figure 10)
- Protocols (TCP/UDP/ICMP) and TCP flags (Figure 11)
- Source and destination port numbers (Figure 12)
- Sensor ID (Figure 13)

In each figure, the filtering function is utilized to assign different colors to the darknet packets according to specified rules. The function can also render specific packets invisible (or visible) by using the settings console as shown in Figure 14.

4.5 Deep Dive

DAEDALUS-VIZ assigns the mouse wheel event to magnify and minimize the screen in order to conduct a deep dive. Figure 15 shows a magnified screen where many small spheres are drifting outward from the large sphere. The small spheres represent the darknet packets that are capable of providing detailed information when clicked. In Figure 15, one of the darknet packets is clicked, and then detailed information such as time, source/destination IP addresses and port numbers, and sensor ID are displayed on a pop-up panel.

[3] Classless Inter-Domain Routing (RFC 4632)

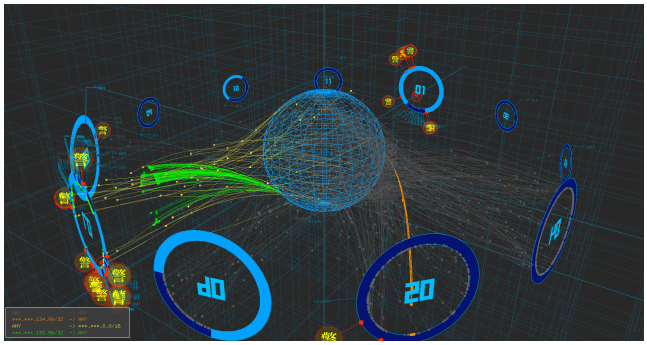

Figure 10. IP/Network Address Filter

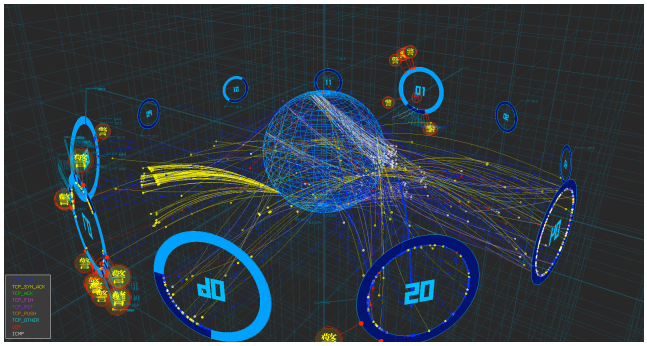

Figure 11. Protocol Filter

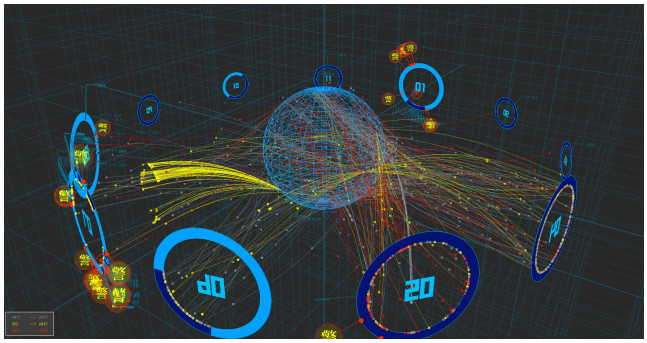

Figure 12. Port Filter

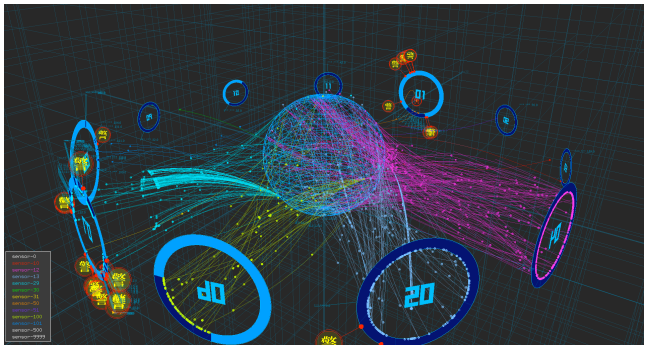

Figure 13. Sensor ID Filter

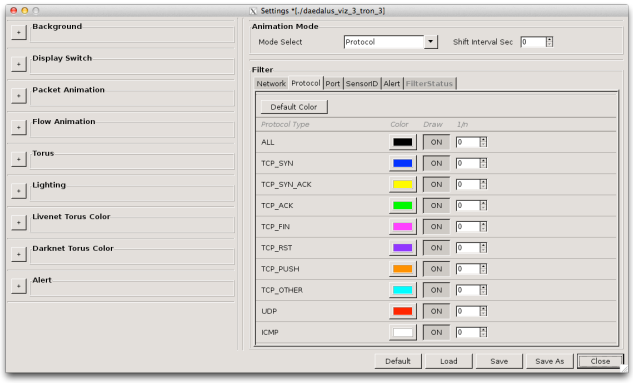

Figure 14. Settings Console

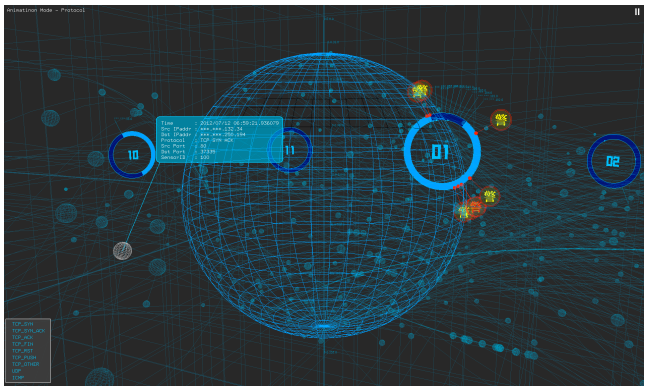

Figure 15. Deep Dive View

4.6 Flow Mode

DAEDALUS-VIZ includes another visualization method called flow mode. Although the packet-by-packet visualization is useful for observing the detailed behavior of the darknet traffic, it is difficult to measure the volume of the traffic. The flow mode helps the user find the relative traffic volume by means of the color temperature, as shown in Figure 16. The volume, which is based on the number of packets or the amount of data being sent, is calculated on each source IP address. In Figure 16, a red flow and a yellow flow can be seen whose source hosts on the sphere are conducting massive scans.

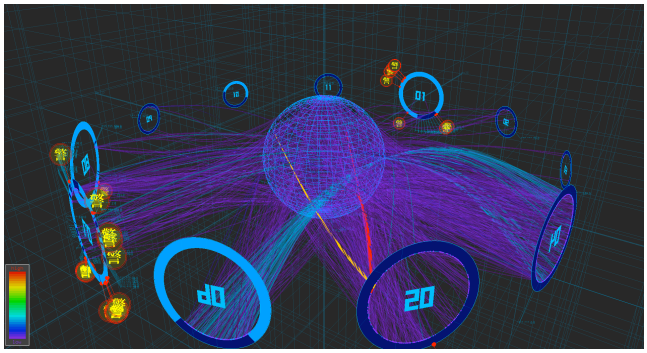

Figure 16. Flow Mode

5. CASE STUDY

This section presents two case studies that are based on real monitoring results on the nicter system. In both cases, an operator could easily grasp the overview of alerts and promptly understand the reason why each alert was generated.

5.1 Internal Malware Infection

The ring illustrated in Figure 17 represents an organization where many malware infections are observed. The organization has approximately 14,000 IP addresses for livenet and 2,500 IP addresses for darknet. At around 18:00 on July 10, 2012, we could see five continued alerts (the yellow ones) and one new alert (the red one). By clicking on the root of an alert icon (red point), we could see quite a few tracks of packets from a certain host to a wide range of the internal darknet. The destination port of the packets is 445/tcp, which is a typical scanning behavior of a malware-infected host that spreads the infection.

5.2 DDoS Backscatter

On June 16, 2012, Anonymous announced that they had initiated OperationJapan against the Anti-Counterfeiting Trade Agreement (ACTA). From June 26 to 30, the Web site of the Democratic Party Japan (DPJ) was under a DDoS attack by Anonymous. At that time, we set two IP addresses of the DPJ's site as subjects for the DAEDALUS alert. Although the DDoS campaign did not eventually increase in size, we observed several backscatter packets from the Web site on June 28, 2012. In Figure 18, the two small rings at the bottom are the IP addresses of the DPJ. We could find that the tracks of the backscatter packets were distributed to many organizations, which is a typical behavior reflective of a DDoS attack with random IP spoofing.

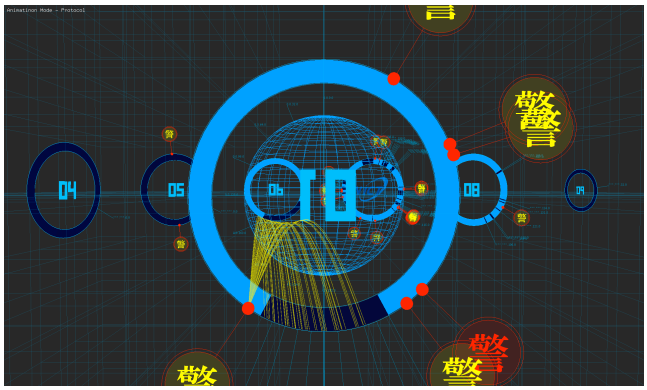

Figure 17. Internal Infection

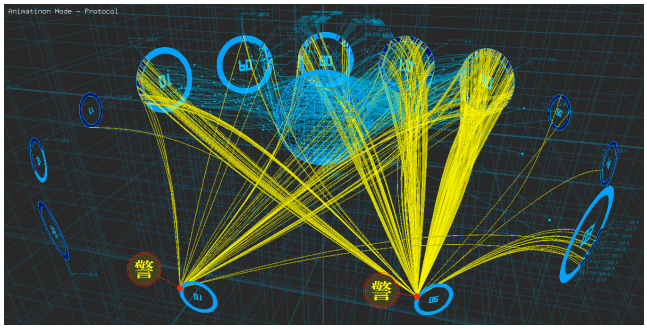

Figure 18. Backscatter from DPJ

6. EVALUATIONS

This section evaluates the graphic performance of DAEDALUS-VIZ. For the evaluations, we used the following hardware and software specifications.

Table 1. HW and SW Specifications

CPU	Intel Core i7-2600, 3.4 GHz, 8 MB cache
Memory	12 GB DDR2 SDRAM 1333 MHz
HDD	1 TB SATA HDD (7200 rpm)
Graphic Card	NVIDIA GeForce GT 545 1 GB GDDR5
OS	CentOS 5.8 x86_64
kernel	2.6.18-308.4.1.el5
Language	C/C++
GUI	gtk2
Graphic	OpenGL

6.1 Number of Alerts

There seems to be a tradeoff relationship between the number of alerts displayed on a screen and the frames per second. Therefore, we evaluated the graphic performance using various numbers of artificially generated alerts. Figure 19 shows the results. We conducted each evaluation three times and calculated the average. According to the results, DAEDALUS-VIZ maintained over 34 fps even when the number of alerts reached 1000. In June 2012, an organization that has a /16 network (including approximately 35,000 IP addresses for darknet) was sent 25.6 alerts per day on average. Consequently, we found that the performance of DAEDALUS-VIZ was sufficiently good against this number of alerts.

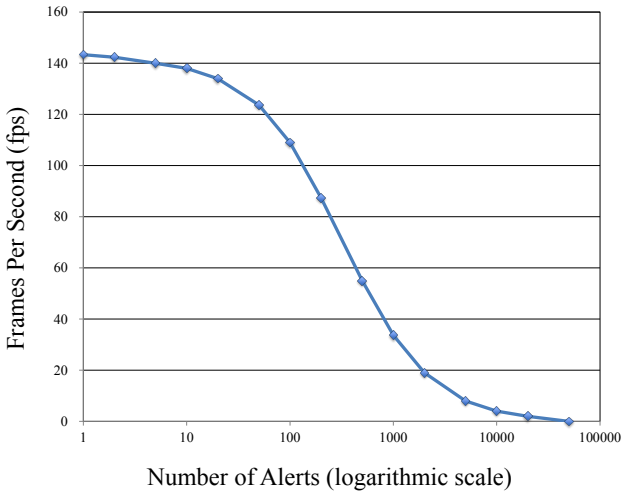

Figure 19. Number of Alerts vs. FPS

6.2 Number of Packets

There also seems to be a tradeoff relationship between the number of packets displayed on a screen and the frames per second. Therefore, we evaluated the graphic performance with various numbers of packets that were generated by a traffic generator called Spirent TestCenter. Figure 20 shows the results (the average of three evaluations) with or without a line after each packet object. Since we displayed each packet for 4 s on the screen, the actual number of displayed packets was about four times higher than that shown on the horizontal axis. According to the results, DAEDALUS-VIZ maintained 26 fps even when the number of packets with lines reached 2000 (500 packets × 4). In June 2012, the nicter received 227 packets per second on average. Consequently, we found that the performance of DAEDALUS-VIZ was sufficiently good against this number of packets.

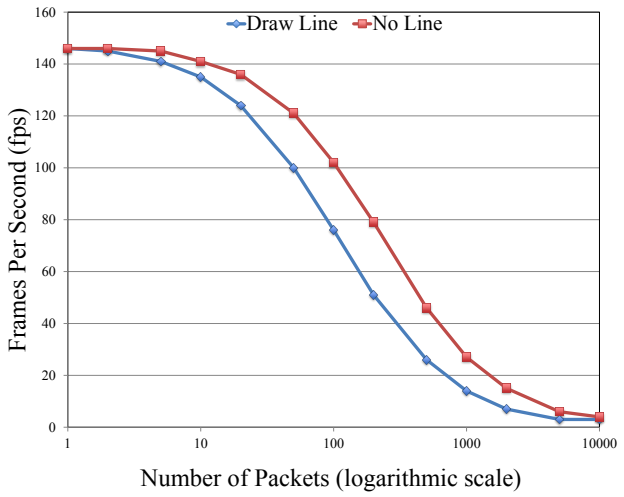

Figure 20. Number of Packets vs. FPS

7. CONCLUSIONS

In this paper, we presented a novel real-time 3D visualization engine called DAEDALUS-VIZ that allows operators to grasp visually and in real-time an overview of alert circumstances, and provides highly flexible and tangible interactivity. Our future works include solving occlusion problems of 3D representations and evaluating the usability of DAEDALUS-VIZ in order to improve its design and utility.

8. REFERENCES

[1] Inoue, D., Eto, M., Yoshioka, K., Baba, S., Suzuki, K., Nakazato, J., Ohtaka, K., Nakao, K., nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis. WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp. 58–66, 2008.

[2] 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. Information and Systems, Vol.E92-D, No.5, pp. 787–798, 2009.

[3] Inoue, D., Suzuki, M., Eto, M., Yoshioka, K., Nakao, K., DAEDALUS: Novel Application of Large-scale Darknet Monitoring for Practical Protection of Live Networks. 12th International Symposium on Recent Advances in Intrusion Detection, pp. 381–382, 2009.

[4] Goodall, J., Introduction to Visualization for Computer Security. VizSEC 2007, pp. 1–17, 2008.

[5] Abdullah, K., Lee, C., Conti, G., Copeland, J., and Stasko, J., IDS RainStorm: Visualizing IDS Alarms. IEEE Workshop on Visualization for Computer Security, pp. 1–10, 2005.

[6] Itoh, T., Takakura, H., Sawada, A., and Koyamada, K., Hierarchical Visualization of Network Intrusion Detection Data. IEEE Computer Graphics and Applications, Vol. 26, Issue 2, pp. 40–47, 2006.

[7] Koike, H., and Ohno, K., Snortview: Visualization System of Snort Logs. 2004 ACM Workshop on Visualization and Data Mining for Computer Security, pp. 143–147, 2004.

[8] Livnat, Y., Agutter, J., Moon, S., Erbacher, R., Foresti, S., A Visualization Paradigm for Network Intrusion Detection. 6th Ann. IEEE SMC Information Assurance Workshop, pp. 92–99, 2005.

[9] Conti, G., Abdullah, K., Grizzard, J., Stasko, J., Copeland, J., Ahamad, M., Owen, H., Lee, C., Countering Security Information Overload through Alert and Packet Visualization. IEEE Computer Graphics and Applications, Vol. 26, Issue 2, pp. 60–70, 2006.

[10] Kintzel, C., Fuchs, J., and Mansmann, F., Monitoring Large IP Spaces with Clockview. 8th International Symposium on Visualization for Cyber Security, Article No. 2, 2011.

[11] Krasser, S., Conti, G., Grizzard, J., Gribschaw, J., Owen, H., Real-time and Forensic Network Data Analysis Using Animated and Coordinated Visualization. 6th Ann. IEEE SMC Information Assurance Workshop, pp. 42–49, 2005.

[12] Nyarko, K., Capers, T., Scott, C., Ladeji-Osias, K., Network Intrusion Visualization with NIVA, an Intrusion Detection Visual Analyzer with Haptic Integration. 10th Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems, pp. 277–284, 2002.

[13] Nurbol, Xu, H., Yang, H., Meng, F., Hu, L., A Real-time Intrusion Detection Security Visualization Framework based on Planner-scheduler. 4th International Conference on Innovative Computing, Information and Control, pp. 784–788, 2009.

[14] Lakkaraju, K., Yurcik, W., Lee, A., NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness. 2004 ACM Workshop on Visualization and Data Mining for Computer Security, pp. 65–72, 2004.

[15] Lau, S., The Spinning Cube of Potential Doom. Communications of the ACM, Volume 47, Issue 6, pp. 25–26, 2004.