3-4 DAEDALUS: Practical Alert System Based on Large-scale Darknet Monitoring for Protecting Live Networks

Mio SUZUKI, Koei SUZUKI, Yaichiro TAKAGI, and Ryoichi ISAWA

In a regular organization, major approach of detecting cyber-attack is "perimeter defense" between the internal network of the organization and the Internet. However, the perimeter defense approach cannot prevent all infections of recent targeted malwares through email attachment files, USB memories, and PCs that are brought in. These infections show rapidly increasing of the importance of security strategies that complement perimeter defense. We have been conducting research and development on the practical alert system called DAEDALUS (Direct Alert Environment for Darknet And Livenet Unified Security) based on the ideological premise that it is difficult to completely protect against malware infection. This report gives the status of DAEDALUS and its deployment in society.

1 Background

In a regular organization, in order to protect its own network from cyber-attack, there are many security devices such as Intrusion Detection System (IDS) or Intrusion Protection System (IPS). These types of security technology are referred to as "perimeter defense," and they mainly operate to detect and protect from external cyber-attacks on the perimeter of the organization's internal network and the Internet. However, there are many cases where malware infections start inside the organization through email attachment files, USB memories, and PCs that are bought in. As many of these examples of infection are mediated by people inside the organization, it becomes difficult to completely protect from new cyber-attacks through perimeter defence, and it is becoming increasingly important to have security strategies that complement perimeter defenses.

We the current authors have been conducting research and development on the practical alert system DAEDALUS based on the ideological premise that it is difficult to completely protect against malware infection [1]–[3]. DAEDALUS, as a post-infection measure, is a system that detects organization-internal malware-infected terminals (particularly worm-type malware that has self-propagating properties), and issues an alert to that organization. Additionally, it can also detect special-type outside cyber-attacks, such as DDoS (Distributed Denial of Service) attacks.

This report gives an update on the status of DAEDALUS system and its deployment in society. Below, in Section **2**, the structure of DAEDALUS is explained, in Section **3**, there is a discussion of DAEDALUS-VIZ, the visualization system of DAEDALUS, Section **4** deals with the status of its implementation into society, and Section **5** provides a summary.

2 Issuing of cyber-attack detection alert

2.1 The structure of DAEDALUS

The structure that allows DAEDALUS to detect attacks and issue warnings is extremely simple, as is explained below.

> When a packet from a specified organization arrives at the darknet, an alert is issued to that organization

Here, "darknet" refers to spaces throughout the Internet with unused IP addresses. It is hard to believe that, in the context of regular transmissions, a packet (the smallest unit of Internet transmission) would arrive at an unused IP address, but when the darknet is actually monitored it can be seen that a large volume of packets do arrive there. Most of these packets are referred to as "scans," which are packets that terminals infected with worm-type malware use to scatter through the Internet in order to seek out the next target of infection. For example, as in the way only junk mail is delivered to the mailbox of a vacant apartment, the majority of packets that arrive at the darknet are unauthor-

ized transmissions deriving from malware, and one can very reasonably suspect that the source of that transmission is also infected with malware. Thus, an alert is issued to the organization that is using that source IP address, and this allows for a swift trigger against an incident.

The attacks that can be detected by DAEDALUS are divided into three cases, as in Figure 1. The "NICTER" in Figure 1 is the incident analysis system, which includes a large scale darknet monitoring system, on which DAEDALUS is based, and which monitors over 300,000 (as of March, 2016) unused IP addresses distributed through Japan and the world in real time [4]–[6].

- Case 1: Organization-internal Infection

Infection working in the organization through a terminal infected with malware (local scan)

- Case 2: Organization-external Focused Attack

Infection working outward from an organization through a terminal infected with malware (global scan)

- Case 3: Backscatter of DoS Attack

A Backscatter of DDoS attack directed toward a specified organization from an external attacker (backscatter)

Further, in order to monitor Case 1, it is necessary to implement a darknet monitoring sensor into the organization-internal network. For Cases 2 and 3, external monitoring is possible through the large scale darknet monitoring system of NICTER, and by simply registering the network address range being used in the organization in DAEDALUS, the implementation of a sensor becomes unnecessary.

2.2 Alert types

DAEDALUS alerts do not send an email for each of the packets (alert packet) that reach the darknet and trigger the issuing of an alert, but aggregate packets that are the focus of an alert coming from a given source IP address (alert packets) in a given grouped unit before sending an alert mail. Further, those alerts are also classified as either urgent or not or as new or continuing. For each alert the monitoring timing interval is set and when an alert packet is generated, and alert information is sent (alert issuing) at the end of the monitoring timing interval. Listed below are the generation conditions for each of the alerts.

- New alert

When an alert packet from a given source IP address is detected, alert packets from the corresponding source IP address from the monitoring timing interval (13 seconds) are aggregated and an alert is issued. When the below conditions are both met a new alert is issued.

1. An alert packet from the corresponding source IP address has not been observed in the past week.
2. One or more alert packets have been observed from the corresponding source IP address during the

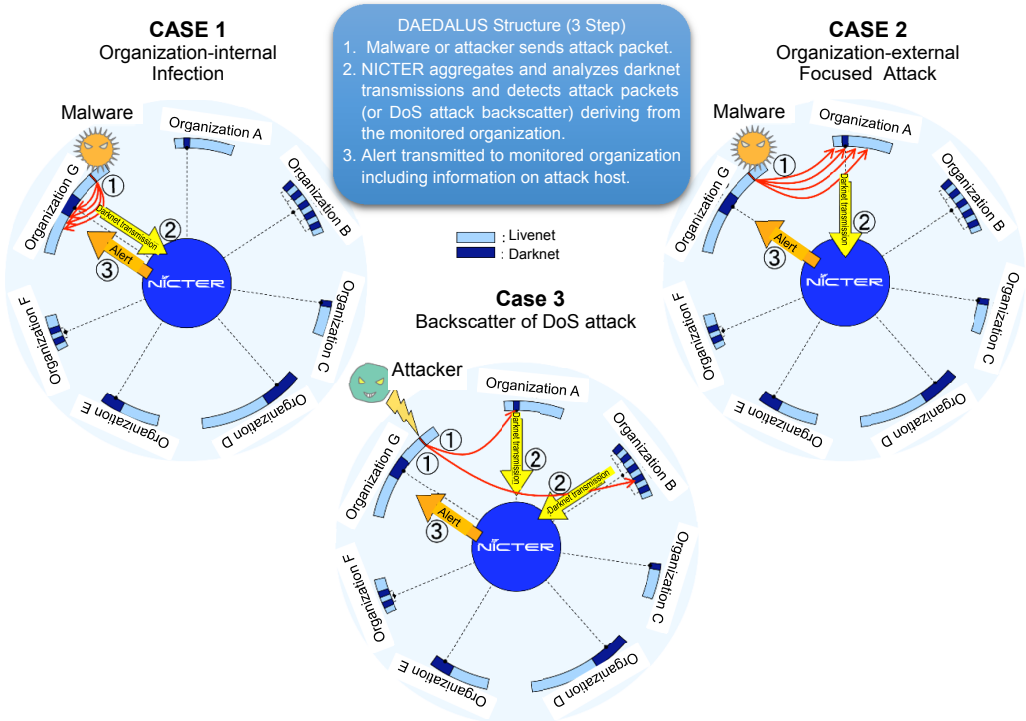

Fig. 1 Cases 1-3 of DAEDALUS attack detection

monitoring timing interval (13 seconds).

- Continued regular alert

When an alert packet from a given source IP address is detected, alert packets from the corresponding source IP address from the monitoring timing interval (60 minutes) are aggregated and an alert is issued. When the condition below is met a continued regular alert is issued.

- One or more alert packets have been observed from the corresponding source IP address during the monitoring timing interval (60 minutes).
- Urgent alert

When an alert packet from a given source IP address is detected, alert packets from the corresponding source IP address from the monitoring timing interval (15 minutes) are aggregated and an alert is issued. When the condition below is met an urgent alert is issued.

- 1,000 or more alert packets have been observed from the corresponding source IP address during the monitoring timing interval (1 minute).

2.3 Alert emails

Attacks detected by DAEDALUS are sent (issued) as alerts by email to the registered organization. Outlined in the alert emails is information including receipt time of packets arriving at the darknet, source address (registered organization IP address), transmission source port number, intended recipient port number, protocol type (TCP or UDP, etc.), and protocol flag (if TDP, SYN/ACK, etc.).

2.4 Alerts other than malware infection

When a network application (especially P2P software) installed on a PC of the registered organization sends a packet to the darknet, an alert is issued (alert sent) to the corresponding organization in the same manner as in Case 2.

Again, when there is an open resolver in the network of the registered organization and an attacker performs a scan on the DNS server with a spoofed source IP address, there is the case in which a DNS response is sent from the registered organization to the darknet. In that case, an alert is issued to the corresponding organization in the same manner as in Case 3 (Fig. 1).

3 The DAEDALUS alert visualization engine

DAEDALUS is a system that issues alerts to multiple organizations based on information obtained from a monitoring network spread out across multiple organizations, and ascertaining the status of alert issuing has be-

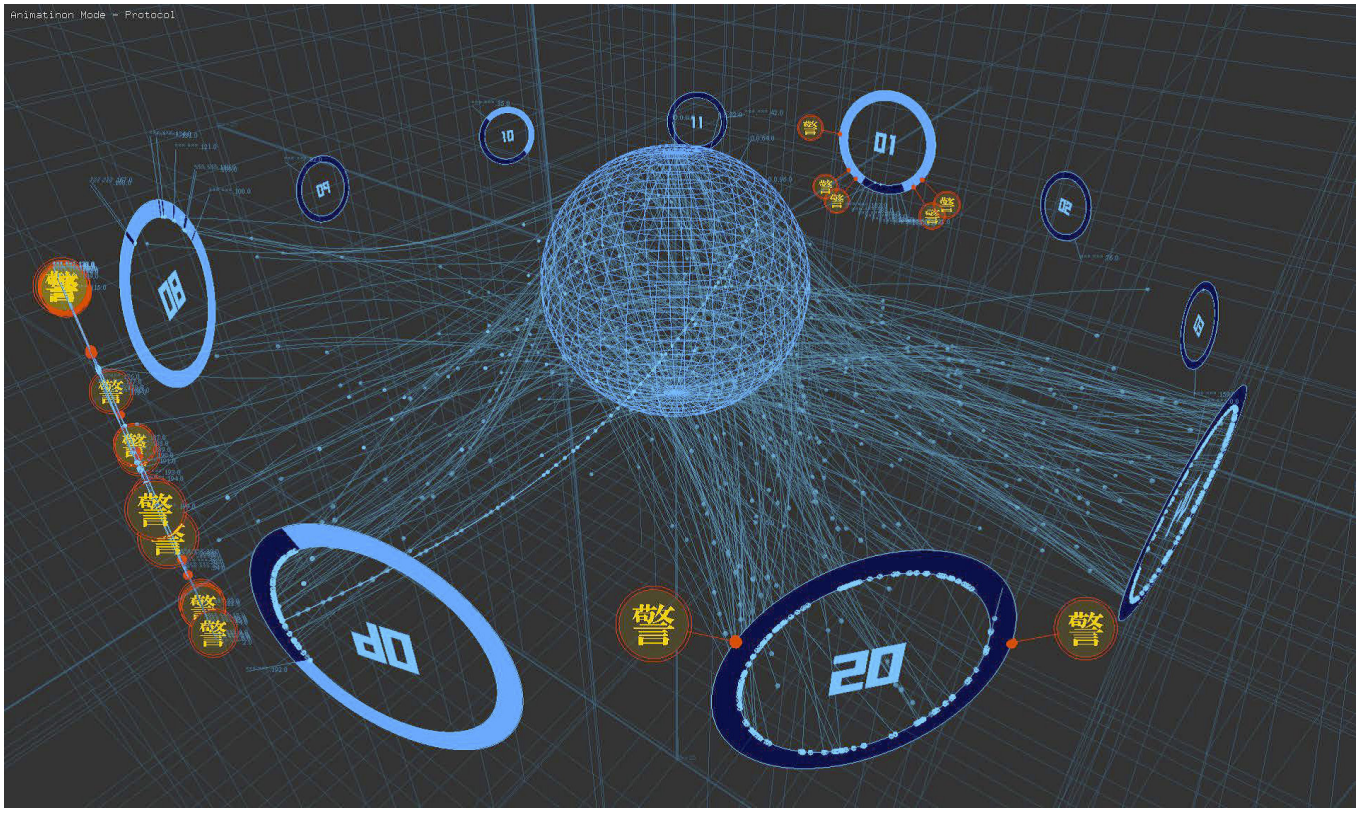

Fig. 2 DAEDALUS-VIZ visualization screen

come a larger issue as alert issuing numbers have been increasing. For this reason, the current authors developed the visualization engine "DAEDALUS-VIZ" in order to broadly ascertain the status of alert issuing. Figure 2 shows the DAEDALUS-VIZ screen. On this screen, the Internet is represented by the sphere in the center and the individual organization networks are represented by the rings around the outside. In each of the rings, the bright light blue parts are the livenet (used IP address blocks) and the dark parts are the darknet. The transmissions to the darknet by each of the organizations that are being monitored by DAEDALUS are represented by the objects that flow between the sphere and the rings. When a new alert is issued to an organization, this is represented by the symbol "警" filling up the entire screen as in Fig. 3, and after that at fixed times it continues to be represented as a "警" symbol around the outside of the ring. As an example of the actual issuing of an alert, Fig. 4 shows what happens when a malware infected terminal carries out malware activities within the organization, and Fig. 5 shows what happens when a DDoS attack is carried out on a given organization server and that backscatter (reflected packets due to the TCP structure) is observed. In both examples, the curved yellow lines represent packets related to the attack.

4 The status of DAEDALUS deployment into society

The current authors have worked to accelerate the deployment of DAEDALUS into society in Japan and overseas. Domestically in Japan, darknet monitoring sensors and visualization engines have been deployed into, and alert issuing through DAEDALUS has been provided for educational institutes and, for regular businesses, while working with the recipients of technology transfer, an alert issuing service based on DAEDALUS has been provided. Further, DAEDALUS alert issuing has been provided for local governmental bodies since November 2013 through cooperation with J-LIS (Japan Agency for Local Authority Information Systems/former incorporated foundation Local Authorities Systems Development Center). The 47 local governments for which this was provided as of November 2013, had increased to 598 as of August 2016.

As for those directed overseas—as a part of the comprehensive cooperative technology project related to the security measures of the Ministry of Internal Affairs and Communications concerning the various ASEAN countries (JAPSER: Japan ASEAN Security Partnership)—DAEDALUS alert issuing is being provided for the various countries of ASEAN.

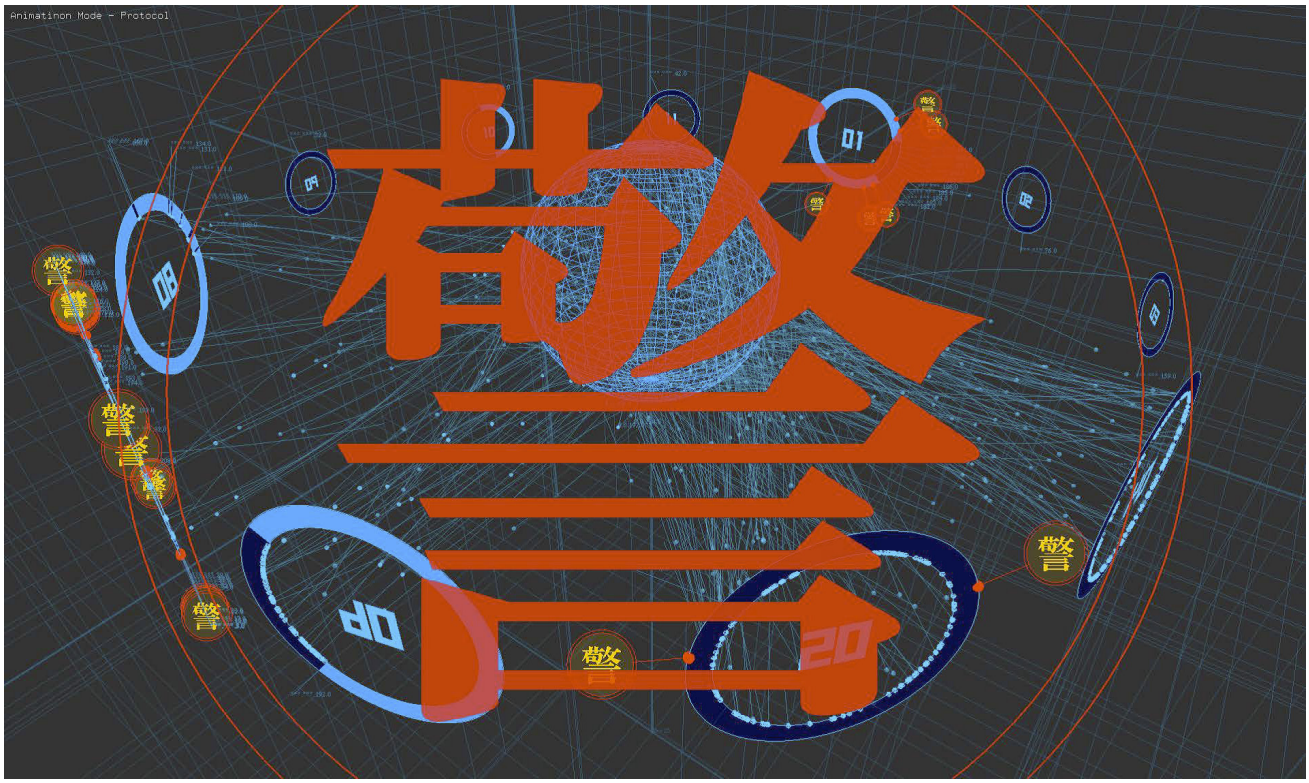

Fig. 3 DAEDALUS-VIZ new alert issuing screen

5 Summary

The current authors have worked until now to research and develop DAEDALUS, one of the security methods for complementing structure perimeter defense. As discussed above, DAEDALUS is based on the monitored results of a large scale darknet monitoring net, and has a structure through which alerts issuing is provided to participating organizations. As the number of organizations included in the scope of darknet monitoring increases, DAEDALUS has such characteristics as to allow its overall detection abilities to improve, and based on a win-win balance of the imple-

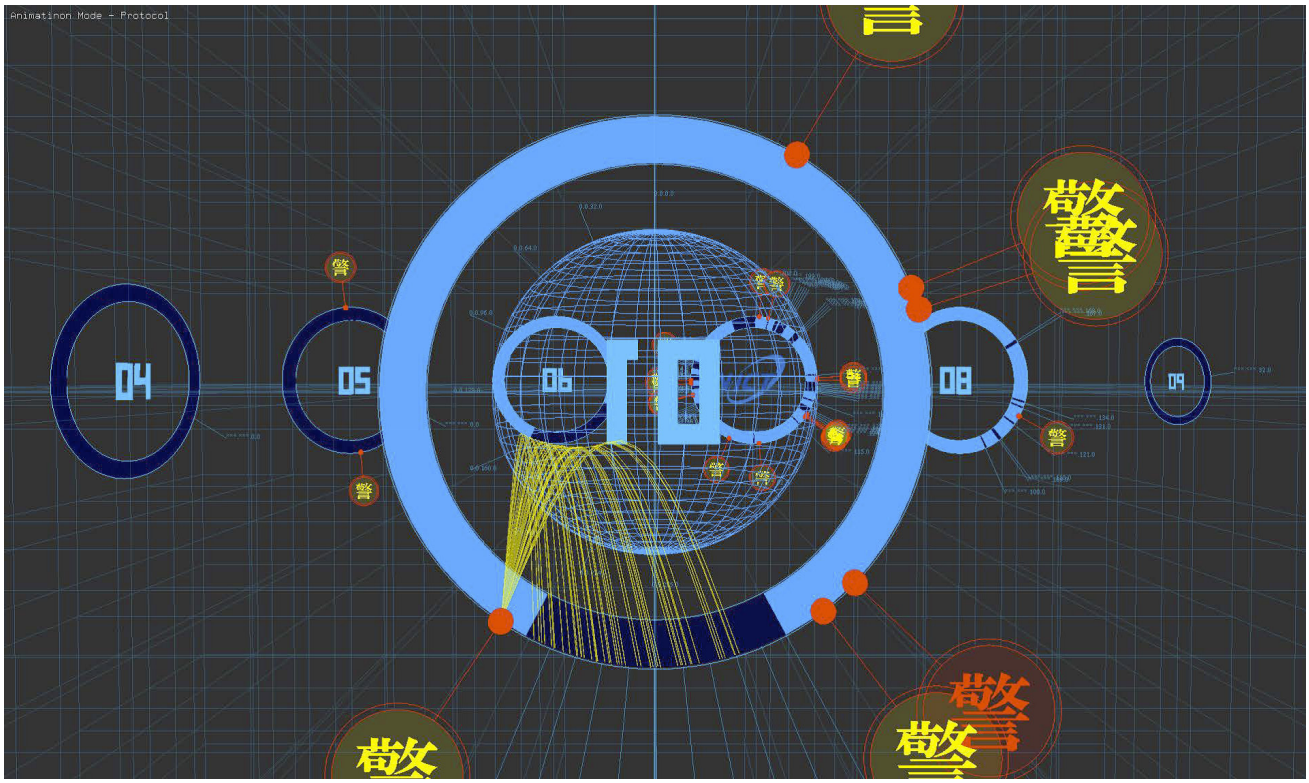

Fig. 4 Actual example of local scan from malware

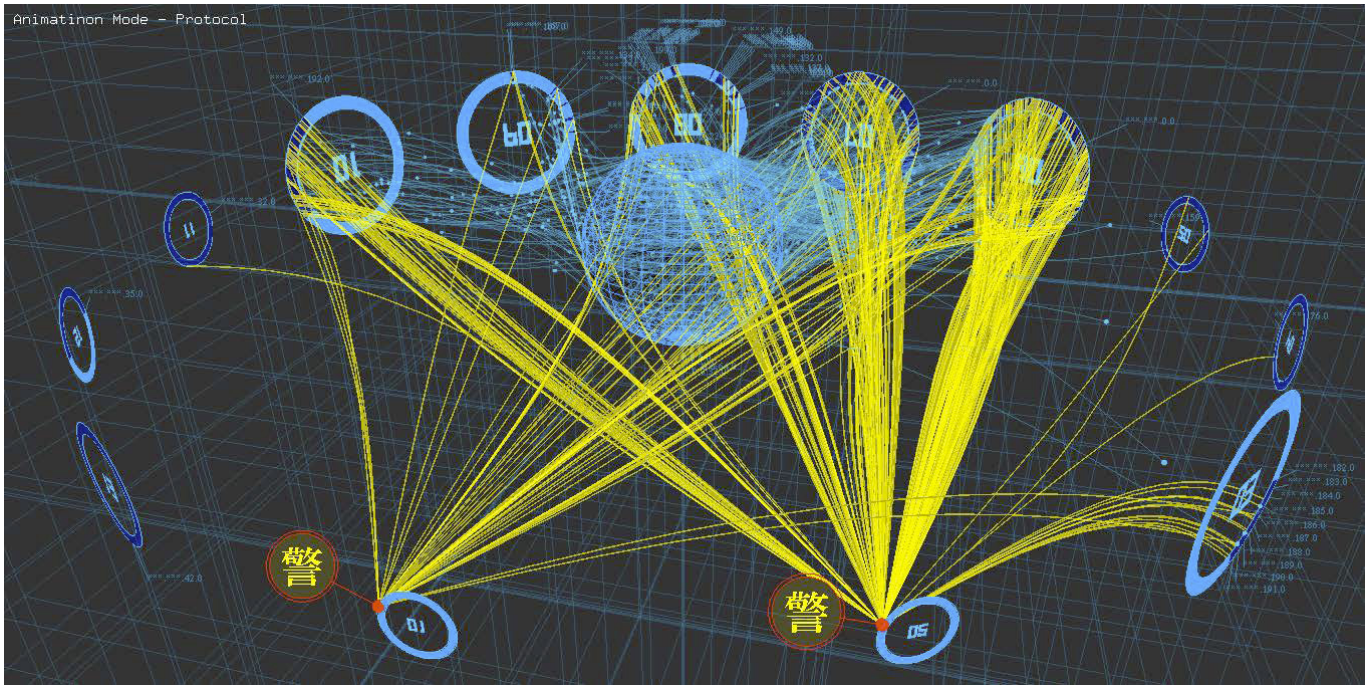

Fig. 5 Actual example of Backscatter from DDoS

mentation of darknet monitoring sensors in collaborating facilities with the provision of alert issuing from DAEDALUS, the current authors will continue to promote its development in industry, academia, and government.

References

1 D. Inoue, M. Eto, K. Nakao, "Practical Alert System Based on Large-scale Darknet Monitoring for Protecting Live Networks, " ICSS2008, 2008. (in Japanese)

2 D. Inoue, M. Suzuki, M. Eto, K. Yoshioka, and K. Nakao, "DAEDALUS: Novel Application of Large-scale Darknet Monitoring for Practical Protection of Live Networks, " 12th International Symposium On Recent Advances In Intrusion Detection (RAID 2009), Poster Session, 2009.

3 D. Inoue, M. Eto, K. Suzuki, M. Suzuki, and K. Nakao, "DAEDALUS-VIZ: novel real-time 3D visualization for darknet monitoring-based alert system, " 9th International Symposium on Visualization for Cyber Security (VizSec '12), pp.72–79, 2012.

4 K. Nakao, K. Yoshioka, D. Inoue, and M. Eto, "A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities," The 2nd Joint Workshop on Information Security (JWIS07), pp.267–279, 2007.

5 D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J.Nakazato, K. Ohtaka, and K. Nakao,"nicter: An Incident Analysis System toward Binding Network Monitoring with Malware Analysis," WOMBATWorkshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp.58–66, 2008.

6 Koji Nakao, Daisuke Inoue, Masashi Eto, and Katsunari Yoshioka, "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.

Mio SUZUKI, Ph.D.

Researcher, Cybersecurity Laboratory, Cybersecurity Research Institute
Network Security, Network Operation

Koei SUZUKI

Senior Technical Researcher, Cybersecurity Laboratory, Cybersecurity Research Institute
Cybersecurity

Yaichiro TAKAGI

Technical Researcher, Cybersecurity Laboratory, Cybersecurity Research Institute
Cybersecurity

Ryoichi ISAWA, Ph.D.

Senior Researcher, Cybersecurity Laboratory, Cybersecurity Research Institute
Malware Analysis, Network Security