Cross-Organizational Incident Information Sharing using a Darknet Monitoring System

Mio Suzuki*, Daisuke Inoue*, Takeshi Takahashi*
*National Institute of Information and Communications Technology, Tokyo Japan
E-mail: mio@nict.go.jp

***Abstract*—Security-related information needs to be shared to cope with increasing amount of cyber attacks. We introduce a system, called DAEDALUS (Direct Alert Environment for Darknet And Livenet Unified Security), that monitors a large-scale darknet to secure live networks. It uses a large-scale distributed darknet consisting of several organizations, with which we can mutually observe outgoing malicious packets among one another. This paper presents the overview of the system, current status of this work toward practical deployment, and consideration on the usefulness of related standards.**

I. Introduction

We have been working on monitoring a large-scale darknet (a set of globally announced unused IP addresses) [2] [4] to grasp the global trends of malicious activities, such as world-wide pandemic of malwares. However, there have been a gap between the darknet monitoring and actual security operations on the live network (livenet) that contains legitimate hosts, servers and network devices. For instance, the darknet monitoring can inform network operators about a global increase of scan on 80/tcp, but it is a mere reference and may not lead to any concrete security operations on their livenets. It means that the results of the darknet monitoring have less direct contribution to protect the livenet. We thus propose an alert system, called DAEDALUS (Direct Alert Environment for Darknet And Livenet Unified Security)[3] [1], which monitors a large-scale darknet and contributes to securing the livenet directly. Note that the darknet consists of several organizations, with which we can mutually observe outgoing malicious packets among one another.

II. Architecture Overview

Figure 1 illustrates DAEDALUS' architecture overview. The system consists of an analysis center and subscribing organizations. Each of the organizations establishes a secure channel with the analysis center and continuously forwards darknet traffic to the center. In addition, each organization registers the IP address range of its livenet to the center beforehand[1]. Here we divide the darknet into two types: internal and external darknet. From the viewpoint of an organization, darknet in the organization is the internal darknet, and darknet in other organizations are the external darknet.

[1]Subscribing organizations usually set up a sensor that communicates with the center in their internal networks. We also have subscribing organizations that only registers their IP address ranges without setting up such a sensor, but the detection we can do for them is limited.

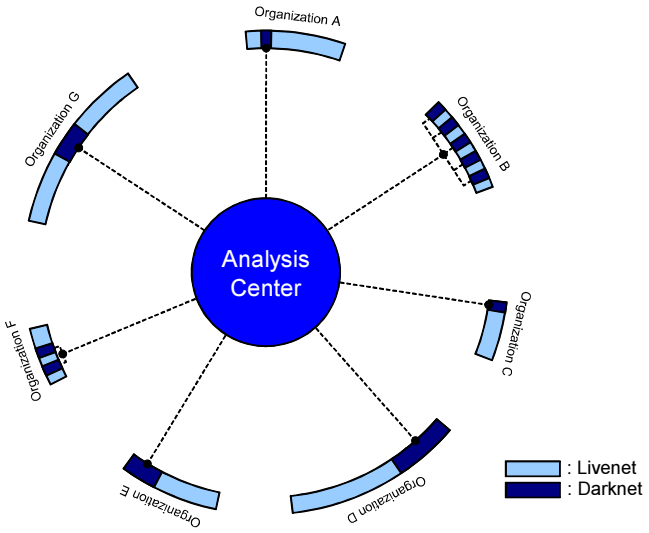

Fig. 1. DAEDALUS Architecture

When a host is infected by malware and starts scanning to the network within the organization including darknet, the analysis center detects the host because a source IP address of darknet traffic matches a preregistered livenet IP address. The analysis center then sends an internal darknet alert to the organization. When the infected host starts scanning to the external networks that belongs to the subscribing organizations, including darknet, the analysis center can also detect the infection with the same manner. The analysis center then sends an external darknet alert to the organization of the infected host. The alerts include at least an IP address of infected host, protocol, source/destination ports, duration of attack, and analysis results if any. Figure 2 shows an example of the alert.

III. Tailored Communication

We also put emphasis on visualization so that an operator receiving the alerts can instantly grasp the security situation. The alerts are often sent in the form of email, but it is not always the best form for all the receivers. Some organizations, such as security operation centers, need to watch wide range of IP address space, thus receiving and analyzing lots of alerts are cumbersome. We developed a visualization module that shows the overview of the current situation in order to facilitate such organizations. Figure 3 provides the snapshot of the system.

```
<?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>
```

Fig. 2. Example of a DAEDALUS Alert

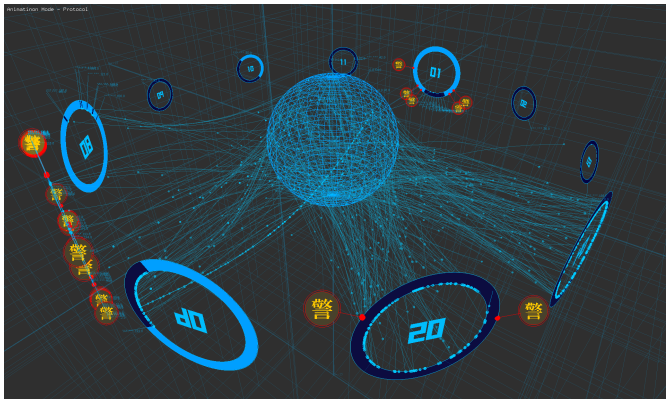

Fig. 3. Screen shot

On the other hand, we need to cope with organizations that do not have technical experts. There are non-trivial number of organizations that lack staffs with sufficient technical knowledge and skills and that cannot understand the implication of the alerts, thus they always need to contact our support desk. This situation could be alleviated by developing tailored communication methods, and we are currently working on this.

IV. Coping with Standard Methodologies

We have been working on detection of incident-related activities and collecting information on them. Currently, we are focusing on automated mitigations using the collected information. For that, we need to share these information to the other parties, including network devices such as firewalls and switches. We already have several experimental tools that run on routers and switches and that change their filtering rules in real time using the information received from the DAEDALUS system. Though the details of this issue is outside the scope of this paper, we consider using IODEF, IPFIX, and NETCONF. IODEF is attractive since its data model covers necessary information we need to share with the corresponding parties and since it is extensible, though we do not need to use all of the fields it defines. From the standpoint of system implementation, these are just output format of the system and do not affect the architecture of the system at all. One of the most important issue here is that the stakeholders agree upon the common schema for describing and sharing such information, and the selection of actual transport protocol is rather a trivial issue. The transport protocol can be defined simply based on which protocols are supported by network devices we use for information exchange. We are thus hoping to see that the standardization activities in this field could develop schemata and stakeholders can agree upon that.

V. Substantiative Experiment

We have deployed DAEDALUS by use of NICTER's darknet resources [2] within a pilot project. The project involved a /16 network consisting of livenet and darknet (= preregistered livenet and internal darknet) and other darknets (= external darknet), and more than 2,700 alerts were issued in August 2010 – January 2011, 20 of which triggered actual security operations in the organization that owns the livenet.

References

[1] D. Inoue, K. Suzuki, M. Suzuki et al. DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System. In *International Symposium on Visualization for Cyber Security*, 2012.

[2] D. Inoue, M. Eto, K. Yoshioka, et al. nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis. In *WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, 2008.

[3] D. Inoue, M. Suzuki, M. Eto, et al. DAEDALUS: Novel Application of Large-Scale Darknet Monitoring for Practical Protection of Live Networks. In *International Symposium on Recent Advances in Intrusion Detection Poster Session*, 2009.

[4] K. Nakao, D. Inoue, M. Eto, and K. Yoshioka. Practical Correlation Analysis between Scan and Malware Profiles against Zero-Day Attacks based on Darknet Monitoring. *IEICE Transactions on Information and Systems*, 2009.