2-5 DAEDALUS: Practical Alert System Based on Large-scale Darknet Monitoring for Protecting Live Networks

SUZUKI Mio and INOUE Daisuke

A darknet is a set of globally announced unused IP addresses and using it is a good way to monitor network attacks such as malware's scans. However, large-scale darknet monitoring systems had two problems: 1) the systems have less direct contribution to protect the live networks; 2) the systems provide less incentive to organizations that will deploy a sensor on their darknet. In this paper, we describe a novel darknet monitoring architecture to solve the above two problems. Based on the architecture, we designed, implemented, and conducted trial operations of an alert system named DAEDALUS. The DAEDALUS enables us to detect malicious hosts in an internal network of an organization, and to send alerts to an operator of the organization. After the trial operations, we have confirmed that the DAEDALUS is effective to detect malicious hosts and misconfigured hosts in the internal networks.

Keywords
Darknet monitoring, Black hole sensor, Live network protection, Alert

1 Introduction

A darknet means IP address space that is both unused and reachable on the Internet[1]-[3]. It is less likely for unused IP addresses to receive packets based on the usual use of the Internet, but a large volume of packets are actually reaching darknets. Many of these packets are triggered by malicious activities on the Internet, including scans or exploit codes remotely transmitted by malware and Backscatter responding to SYN flood attacks with spoofed source IP addresses. This means that monitoring packets received by darknets will allow us to grasp the trend of malicious activities occurring on the Internet. The greatest advantage of darknet monitoring lies in the fact that we do not have to distinguish the validity of the traffic and can construe the vast majority of packets as malicious.

Darknet monitoring requires the setup of sensors, which are server machines collecting and responding to packets. Sensors are categorized as follows based on how they respond to packet sources.

- **Black hole sensors:** Sensors that do not respond at all to packet sources. Quite easy to maintain, they are a perfect fit for large-scale darknet monitoring. Not responding to packets makes it very difficult for them to be detected by external devices, which is also an advantage of these sensors. They can detect scans that occur at the initial stage of infectious activities triggered by malware but cannot detect subsequent activities.
- **Low-interaction sensors:** Sensors that somewhat respond to packet sources. They include sensors that return SYN-ACK packets to TCP SYN packets and low-interaction honeypots that emulate known OS vulnerabilities. They tend to be detected based on the trend of ports they listen to,

making them unsuitable for large-scale darknets with successive addresses.

- **High-interaction sensors:** Live hosts or sensors that similarly respond to packet sources (i.e. so-called high-interaction honeypots). They can detect various information including behaviors at the time of malware infection and keystrokes by attackers. However, the high cost required to operate them in a safe manner make them inappropriate for large-scale operations.

We have deployed black hole sensors on multiple darknets located within Japan for continuous monitoring based on the nicter, an incident analysis center developed by us[4]-[6]. This continuous monitoring of darknets has allowed us to face the following two challenges.

(1) Protection of live networks

Darknet monitoring is quite useful to enable us to monitor the trends of malicious activities on the Internet but has not directly led to the protection of organizational live networks where servers and hosts are located.

(2) Large-scale implementation of sensors

The accuracy of darknet monitoring is improved depending on the number of addresses to be monitored, making it critical for us to implement sensors on a large scale. We have faced the challenge to offer incentives so that various organizations can feel motivated to offer their darknets and implement sensors.

This paper explains a new darknet monitoring architecture that solves the above two challenges at the same time and reports how the alert system that enables this architecture, named DAEDALUS (Direct Alert Environment for Darknet And Livenet Unified Security), has been designed, developed, and operated on a trial basis. DAEDALUS has closely integrated darknet monitoring and live network protection, both of which had rarely been linked to each other. What is more, it has expanded the potentials of darknet monitoring and enabled the implementation of nicter sensors on a large scale.

This paper explains related work in Chapter **2** below, followed by our proposed architecture in Chapter **3**. Chapter **4** shows the design and deployment of DAEDALUS alert system, with Chapters **5** and **6** referring to the results of its trial operations. Finally, Chapter **7** sums up the findings and future challenges related to this system.

2 Related work

We provide the overview of major network monitoring projects carried out by Japan and other countries in Chapter **2**.

- Network Telescope[2]

  A darknet monitoring project by the Cooperative Association for Internet Data Analysis (CAIDA) in the U.S. It monitors darknets containing more than 160,000 addresses and publishes data sets concerning traffic by Backscatter and worms.
- Internet Motion Sensor (IMS)[3]

  A large-scale darknet monitoring project by University of Michigan in the U.S. covering more than 17 million addresses including /8 networks. Its sensors return SYN-ACK to some of the observed TCP SYN packets to attempt to establish TCP connections so that the payload of the first packet after the established connection can be collected and analyzed.
- Leurre.com[9][10]

  An information collection and analysis project by Eurecom of France using distributed honeypots. The number of IP addresses to monitor is relatively small but the areas to be monitored are distributed worldwide. The first generation project (Leurre.com v1.0) used to use low-interaction sensors called Honeyd[11], but the second generation project (Leurre.com v2.0) leverages SGNET[12] to improve its information collection capabilities.
- REN-ISAC[13]

  A project by the Research and Education Networking (REN) of the U.S. to share and analyze security information. It analyzes traffic obtained through Internet2 and publishes monitoring results.

- Internet Storm Center (ISC)[14]

  A project by the SysAdmin, Audit, Networking, and Security (SANS) of the U.S. to collect and analyze security information. It integrates firewall logs from more than 500,000 addresses into its system called DShield[15] to publish statistical data or analysis reports created by volunteers.

In Japan, the following network monitoring projects are currently underway: ISDAS[16], @police[17], MUSTAN[18], and WCLSCAN[19].

Each of these projects focuses on detecting trends of malicious traffic on the Internet. In contrast, the architecture proposed by us in this paper aims to directly link darknet monitoring with the protection of live networks.

3 Our proposed architecture

This chapter describes our proposed architecture enabling the protection of live networks based on the results of darknet monitoring. The traditional darknet monitoring based on black hole sensors was designed to detect trends of malicious traffic on the Internet, transferring the traffic reaching internal darknets (“darknet traffic”) to internally deployed sensors, which in turn transmit the darknet traffic to the central analysis center. Basically, the analysis center analyzes the darknet traffic collected from sensors managed by each organization and reports the statistical and other information related to the traffic.

Our proposed architecture leverages the basic structure of traditional darknet monitoring and does not require any changes to be made to sensors deployed by each organization. This allows the continued utilization of the large-scale darknet monitoring networks created by the nicter and enables us to detect malware infections and misconfigured network devices on live networks. Our proposed architecture is illustrated below.

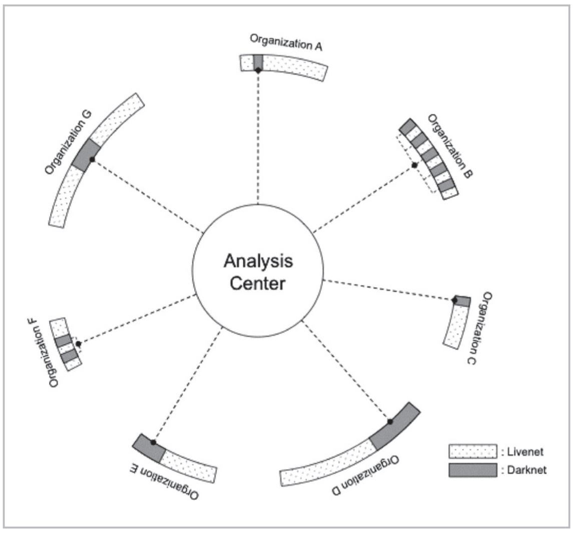


Fig.1 *Proposed architecture*

3.1 Assumed environment

Figure 1 shows the assumed environment of our proposed architecture. Organizations A–G providing darknets set up black hole sensors within their organizations and forward their darknet traffic to sensors. Unlike conventional darknet monitoring, this mechanism enables each organization to register the range of IP addresses used as live networks (“livenets”) in the analysis center.

The analysis center monitors the darknets in a conventional manner as well as detecting in darknet traffic the packets containing source IP addresses registered by each organization as its livenets. The detection of those packets will issue alerts to the point of contact (POC) of the packet source organization.

3.2 Detecting malicious hosts within internal darknets

An organization has darknets contained in the range of IP addresses managed by it. We call them “internal darknets”. As hosts infected with malware in each organization run local scans (typically scans run against /24 or /16 networks including infected hosts) and the scans reach internal darknets, they are detected by the analysis center, which issues alerts to the appropriate organization. As shown by the example in Fig. 2, hosts infected with malware within Organization G run local

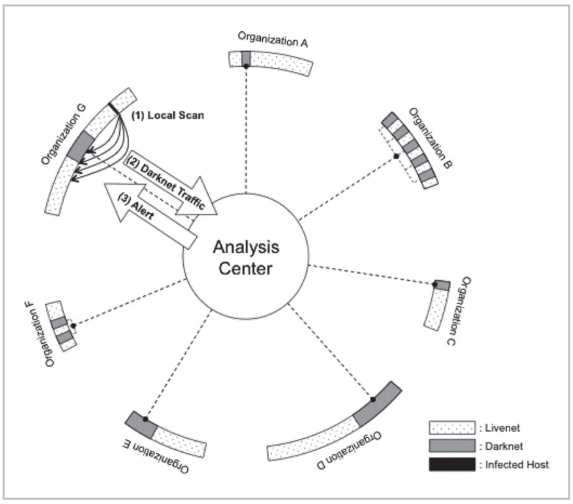


Fig.2 Detection of malicious hosts by observing internal darknet

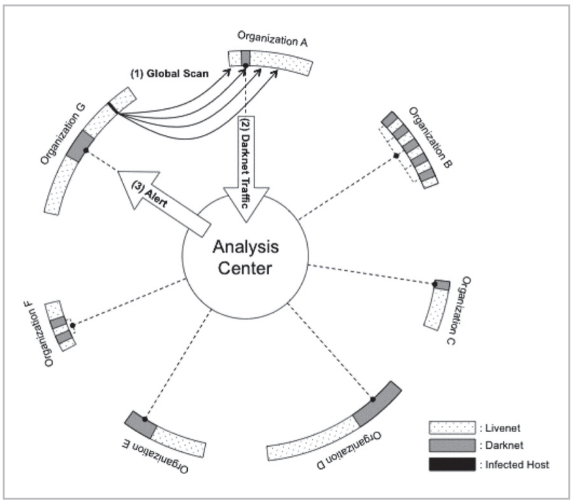


Fig.3 Detection of malicious hosts by observing external darknet

scans, causing the analysis center to issue alerts to Organization G. Within internal darknets, the detection of packets from inside the organization can be triggered by network misconfiguration and other anomalies in addition to local scans. However, we can safely say they are malicious packets either way and use alerts as valid information to manage networks.

3.3 Detecting malicious hosts within external darknets

Darknets outside the range of IP addresses managed by an organization are called "external darknets". As hosts infected with malware in each organization run global scans (scans run outside the organization of infected hosts) and the scans reach external darknets, they are detected by the analysis center, which issues alerts to the organization with the host that has initiated the scans. As shown by the example in Fig. 3, hosts infected with malware within Organization G run global scans and the scans reach a darknet of Organization A, causing the analysis center to issue alerts to Organization G. Within external darknets, alerts can be issued based on the detection of global scans as well as Backscatter from the livenets as registered in the analysis center. The situation suggests the possibility of internal servers being attacked by some malware and can provide valuable information for the sake of security management.

4 Designing and deploying the alert system based on DAEDALUS

In this chapter, we describe how we have designed and deployed DAEDALUS, the alert system based on our proposed architecture explained in Chapter **3**.

4.1 Designing DAEDALUS

DAEDALUS is designed to link traditional darknet monitoring with the protection of live networks. As we defined the design requirements of DAEDALUS, we focused on the feature that retained affinity with the existing nicter system and allowed us to leverage the data and analysis results as obtained by the nicter.

4.1.1 Structure of DAEDALUS

Figure 4 illustrates the structure and the data flow of DAEDALUS designed in line with the previous requirements. As explained by Chapter **3**, DAEDALUS is composed of multiple organizations providing darknets and the analysis center. Each organization is equipped with black hole sensors to collect darknet traffic. The collected traffic is transferred to the analysis center via VPN as summary data only containing what is required for the analysis by the sensor. The summary data comprises sen-

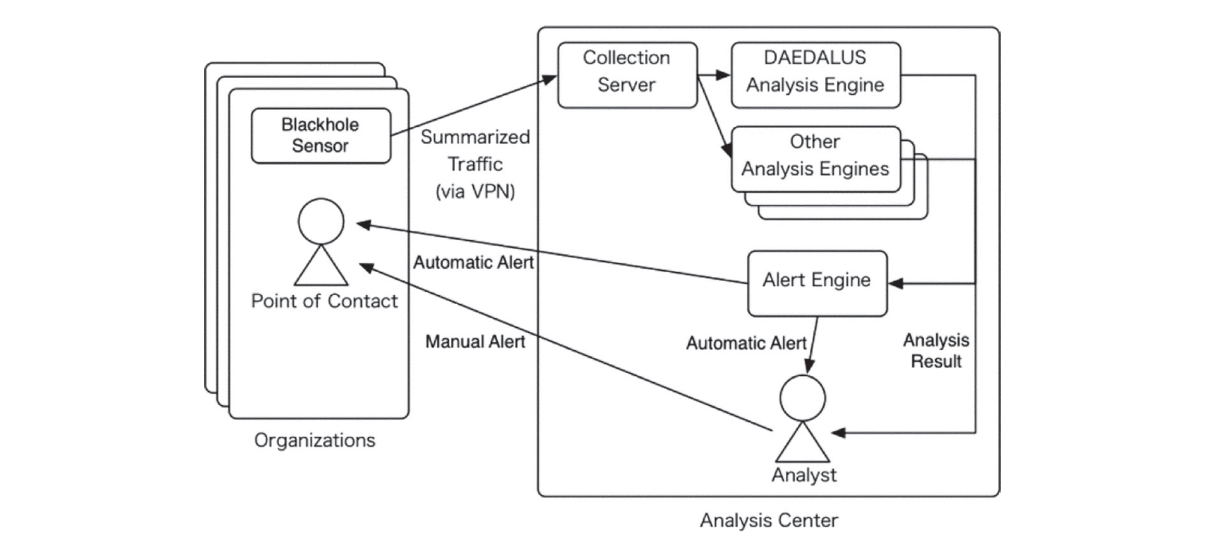


Fig.4 Data flow of DAEDALUS

sor IDs, collected time, packet IDs, IP headers, transport protocol headers, and hash values for the payload part. The collection server within the analysis center receives the summary data transmitted by each organization, distributing it to the DAEDALUS and other existing analysis engines. This mechanism basically leverages the basic structure of the existing nicter system[20] the way it is, except for the DAEDALUS analysis engine.

The DAEDALUS analysis engine has both the IP address ranges used by each organization (i.e. livenets) and the unused IP address ranges (i.e. darknets) registered. As the sensor detects packets containing IP address ranges of livenets as source IP addresses, it analyzes their frequency and other information and transmits the analysis results to the alert engine and analysts. The alert engine evaluates the severity of the analysis results based on frequency and other information, sending automatic alerts to the POC or analysts of the appropriate organization. In addition, the analysts who have received analysis results or alerts further select critical information to report it to the POC of their organization as a manual alert.

4.1.2 Automatic alerts

This section explains how the DAEDALUS alert engine issues automatic alerts. DAEDALUS is designed to detect malicious traffic, and eventually malicious hosts. This has made us focus on the source IP addresses included in malicious traffic and culminated in the design to aggregate the number of detected packets per source IP address for a certain unit of time. Aggregating the number for each source IP address enables us to understand the behaviors of a specific host by taking a look at one alert. Also, aggregation per unit time period can reduce the number of issued alerts. We have come up with three types of alerts to be issued after the aggregation: new alerts, continual alerts, and emergency alerts. We will refer to a specific example to explain each alert. Imaging one source IP address initiates sequential scans for darknets. Once the alert engine first detects a packet with its destination address specified as a darknet, a new alert is issued per unit time period. Then, as the packet is continually detected by the engine, a continual alert is issued. In case the engine detects a packet that goes beyond a certain threshold for each unit time period, an emergency alert is issued. These alerts are automatically issued by DAEDALUS to the POC or analysts almost in real time.

4.2 Implementing DAEDALUS

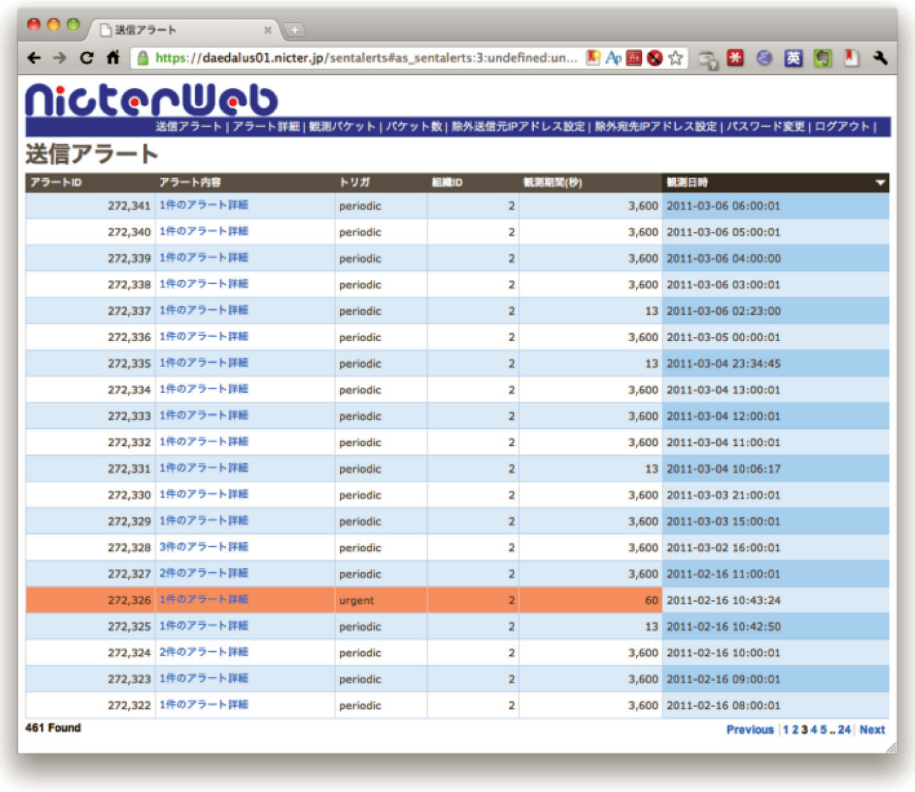
This section explains how we have implemented DAEDALUS based on the previous design. Figure 4 includes black hole sensors, a collection server, and existing analysis engines as they are used by the existing nicter system. The DAEDALUS analysis engine and alert engine have been implemented using Ruby on FreeBSD 7.3. This is because we have adopted Ruby on Rails[21], an open-source web application framework, so that we can efficiently implement the system to create the web interface enabling the POCs to view detailed alert information. We have also used MySQL as the backend database for the system. Patricia Trie libraries have been used to determine whether source IP addresses and destination IP addresses are included in the registered livenets or darknets.

Alerts are issued to POCs in such a way as the overview can be sent by email and details can be viewed through a web interface. The system has been designed this way so that we can increase visibility by showing the data in an interactive manner through a web interface instead of bundling a large volume of information in email. Figure 5 shows the screen of the web interface. This web interface enables users to view detailed alert information as well as to edit the whitelists of source and destination IP addresses.

The unit time period to issue a continual alert is set for one hour. Also, an emergency alert is issued in case at least 1,000 packets containing source certain addresses are detected during one minute period. We can easily change this threshold in the current implementation. The threshold of 1,000 packets has been decided based on the number of packets generated by CodeRed[22] and Slammer[23], which caused large-scale infections in the past.

5 Operational results observed by an organization with sensors

This chapter describes how we have deployed DAEDALUS in a domestic organiza-


送信アラート
NicterWeb
送信アラート | アラート詳細 | 観測パケット | パケット数 | 除外送信元IPアドレス設定 | 除外宛先IPアドレス設定 | パスワード変更 | ログアウト |
Previous | 1 2 3 4 5 .. 24 | Next

https://daedalus01.nicter.jp/sentalerts#as_sentalerts:3:undefined:un...

送信アラート

アラートID	アラート内容	トリガ	組織ID	観測期間(秒)	観測日時
272,341	1件のアラート詳細	periodic	2	3,600	2011-03-06 06:00:01
272,340	1件のアラート詳細	periodic	2	3,600	2011-03-06 05:00:01
272,339	1件のアラート詳細	periodic	2	3,600	2011-03-06 04:00:00
272,338	1件のアラート詳細	periodic	2	3,600	2011-03-06 03:00:01
272,337	1件のアラート詳細	periodic	2	13	2011-03-06 02:23:00
272,336	1件のアラート詳細	periodic	2	3,600	2011-03-05 00:00:01
272,335	1件のアラート詳細	periodic	2	13	2011-03-04 23:34:45
272,334	1件のアラート詳細	periodic	2	3,600	2011-03-04 13:00:01
272,333	1件のアラート詳細	periodic	2	3,600	2011-03-04 12:00:01
272,332	1件のアラート詳細	periodic	2	3,600	2011-03-04 11:00:01
272,331	1件のアラート詳細	periodic	2	13	2011-03-04 10:06:17
272,330	1件のアラート詳細	periodic	2	3,600	2011-03-03 21:00:01
272,329	1件のアラート詳細	periodic	2	3,600	2011-03-03 15:00:01
272,328	3件のアラート詳細	periodic	2	3,600	2011-03-02 16:00:01
272,327	2件のアラート詳細	periodic	2	3,600	2011-02-16 11:00:01
272,326	1件のアラート詳細	urgent	2	60	2011-02-16 10:43:24
272,325	1件のアラート詳細	periodic	2	13	2011-02-16 10:42:50
272,324	2件のアラート詳細	periodic	2	3,600	2011-02-16 10:00:01
272,323	1件のアラート詳細	periodic	2	3,600	2011-02-16 09:00:01
272,322	1件のアラート詳細	periodic	2	3,600	2011-02-16 08:00:01

461 Found

Fig.5 *Web interface provided by DAEDALUS*

tion (Organization X) with a black hole sensor for the nicter and operated the system on a trial basis. Organization X has a network structure where /16 networks contain both darknets and livenets (similar to Organization B in Fig. 1). We have designated the livenets of Organization X as the IP addresses to be registered on DAEDALUS and construed the darknets of Organization X as internal darknets. On the other hand, we have construed the darknets held by other organizations as external darknets. The system was operated between August 1, 2010 and January 31, 2011.

5.1 Number of detected packets and issued alerts

Table 1 contains the number of unique hosts detected across all the darknets, the number of total packets detected across all the darknets, the number of packets with Organization X's source addresses as detected by DAEDALUS, the number of automatic alerts issued by DAEDALUS, and the number of alerts nicter analysts extracted as malware-induced alerts, all calculated for each month of the operation period. The number of automatic alerts has reached 452 on an average for each month, with 15.1 alerts issued per day. Based on the investigation by us, a vast majority of these automatic alerts were caused by misconfigured devices or obsolete configuration remaining in devices. On the other hand, we have also found that some alerts were triggered by malware infecting internal PCs and other devices. These alerts triggered by malware require rapid actions to rein in the further propagation of infections. Thus, we have focused on alerts likely to have been caused by malware out of all automatic alerts in the trial operation of the system, implementing the workflow allowing nicter analysts to extract such alerts and requesting the POC of Organization X to work on them (the manual alert process made by analysts as illustrated by Fig. 4).

The nicter analysts have reported a total of 20 incidents to the POC of Organization X during the trial operation period. Based on this number, local operators have confirmed six incidents with actual malware infections on appropriate hosts.

5.2 Detected incidents

This section describes some incidents detected during the trial operation period

5.2.1 Incidents related to malware

- **Incident 1:** On September 10, 2010, we detected a sequential scan made by an IP address against the TCP port number 445. The number of packets per destination address was two or three, with one packet transmitted on an average every three seconds. nicter analysts contacted the POC of Organization X to request further investigations and received the report that the host was infected with such malware as W32.Downadup.B, W32.Downadup!autorun, and Trackware.Rewardnet.
- **Incident 2:** On December 14, 2010, we detected a random scan made by an IP address against the TCP port number 445.

Table 1 *Alerts issued for each month*

Date	Num. of unique hosts	Num. of total packets	Num. of packets detected	Num. of alerts sent automatically	Num. of alerts sent by our analyst
2010/8	23,685,324	306,523,808	562,532	712	0
2010/9	21,240,024	290,529,367	703,055	952	3
2010/10	22,659,297	309,694,496	787,756	227	5
2010/11	28,562,141	296,772,713	1,450,179	113	0
2010/12	29,126,062	324,485,640	2,475,351	352	7
2011/1	28,863,449	276,093,022	2,111,713	358	5

The number of packets per destination address was one, with one packet transmitted on an average every three seconds. We requested further investigations of this incident and received the report that the host was infected with such malware as Backdoor.Graybird, Trojan.Gen, Trojan.ADH, and Trojan.ADH.2.

5.2.2 Other incidents

- **Incident 3:** On January 18, 2011, we detected a sequential scan made by an IP address against the UDP port number 137. The number of packets per destination address was one, with 93 packets transmitted on an average every second. We requested further investigations of this incident and received the report that this was a regular behavior by Android terminals. As we further investigated, we confirmed that this behavior was triggered since Android terminals speed up the connection to network shared disks.
- **Incident 4:** On January 21, 2011, we detected a sequential scan made by an IP address against the UDP port number 137. The number of packets per destination address was one, with 56 packets transmitted on an average every second. We requested further investigations of this incident and received the report that this was caused by the software called IP Scanner Pro[24] operating on the host. IP Scanner Pro is a scan tool for Mac, capable of detecting device types or operating systems.

6 Operational results by NICT

This chapter discusses how DAEDALUS was deployed and operated by the information system team (current Information System Office) of National Institute of Information and Communications Technology (NICT), which is responsible for managing NICT networks. NICT's networks have a structure where /16 networks include both darknets and livenets (similar to Organization B of Fig. 1). Thus, we have designated the livenets of NICT as the IP addresses to be registered on DAEDALUS and construed the darknets of NICT as internal darknets. On the other hand, we have construed the darknets held by other organizations as external darknets. The POC was operated by the staff of the information system team. The system was in operation between January 13, 2011 and March 31, 2011. Out of all the alerts issued during this period, one alert was useful in analyzing the actual situation. The report made by the information system team is described in the following section.

6.1 Alert incident

- **Incident 1:** We detected the transmission of ICMP packets from an internal darknet address to another internal darknet address. The behavior was detected eight times between January 13 and January 16. This phenomenon is likely to have been observed since the ingress filter was not set up in the BGP router used for external connections and some packets were created with their source spoofed. Based on this incident, the information system team decided to set up the ingress filter for both IPv4 and IPv6.

7 Conclusion

DAEDALUS leverages large-scale darknet monitoring networks based on the nicter to protect live networks. The traditional use of darknets used to allow us to monitor malicious packets received from external sources, meaning we used to capture the access from outside. In contrast, DAEDALUS monitors malicious packets transmitted internally based on distributed darknets. It shows a new way to use darknets by capturing the access from inside to outside (or within inside).

Based on the DAEDALUS mechanism, the analysis center detects malware infections and other anomalies within an organization and sends alerts to an appropriate organization so that darknet monitoring results can trigger security operations of live networks. This provides a solution to one of the two challenges (i.e. the protection of live networks) as mentioned by Chapter **1**.

From the perspective of organizations offering darknets, offering a part of their unused IP addresses and setting up black hole sensors enable them to obtain direct feedback in the form of alerts from large-scale darknet monitoring networks, leading to the rapid detection of unauthorized access to external destinations from their internal hosts. This is expected to create incentives for organizations to deploy sensors on a large scale, solving the second challenge faced by darknet monitoring. Furthermore, we can expect to enhance positive effects based on this step, by further expanding darknet monitoring networks, improving the accuracy of analysis, and growing the number of participating organizations.

Incidents mentioned by Chapters **5** and **6** clearly show that DAEDALUS is instrumental in detecting malicious hosts caused by malware and misconfiguration of devices. Based on the trial operation of the system, nicter analysts manually extracted alerts possibly triggered by malware from automatic alerts and communicated with the POC of the appropriate organization. This flow requires the intervention of analysts, causing bottlenecks in terms of operational timeliness and performance. Going forward, we will leverage the nicter system to develop a mechanism that will complete the whole workflow without the intervention of analysts. Specifically, we will utilize the correlation analysis technology [4]-[6] of the nicter to automatically estimate the root causes for alerts based on the patterns of the destination addresses, port numbers, and arrival intervals of detected packets and map priority to those root causes so that only the alerts required by the POC of each organization can be automatically issued.

References

1 D. Song, R. Malan, and R. Stone, “A Snapshot of Global Internet Worm Activity,” The 14th Annual FIRST Conference on Computer Security Incident Handling and Response, 2002.

2 D. Moore, “Network Telescopes: Tracking Denial-of-Service Attacks and Internet Worms around the Globe,” The 17th Large Installation Systems Administration Conference (LISA ’03), USENIX, 2003.

3 M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, “The Internet Motion Sensor: A Distributed Blackhole Monitoring System,” The 12th Annual Network and Distributed System Security Symposium (NDSS05), 2005.

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,” WOMBAT Workshop 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.

7 D. Inoue, M. Eto, and K. Nakao, “A Protection Architecture for Live Networks Based on Darknet Monitoring,” The 5th workshop of Information and Communication System Security (ICSS2008), 2008.

8 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.

9 F. Pouget, M. Dacier, and V. H. Pham, “Leurre.com: On the Advantages of Deploying a Large Scale Distributed Honeypot Platform,” E-Crime and Computer Conference (ECCE’05), 2005.

10 C. Leita, V. H. Pham, O. Thonnard, E. Ramirez-Silva, F. Pouget, E. Kirda, and M. Dacier, “The Leurre.com Project: Collecting Threats Information using a Worldwide Distributed Honeynet,” WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp. 40–57, 2008.

11 N. Provos, “A Virtual Honeypot Framework,” The 13th USENIX Security Symposium, 2004. http://www.honeyd.org/

12 C. Leita and M. Dacier, “SGNET: A Worldwide Deployable Framework to Support the Analysis of Malware Threat Models,” The 7th European Dependable Computing Conference (EDCC 2008), 2008.

13 REN-ISAC, http://www.ren-isac.net/

14 M. V. Horenbeeck, “The SANS Internet Storm Center,” WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp. 17–23, 2008. http://isc.sans.org/

15 DShield, http://www.dshield.org/

16 JPCERT/CC ISDAS, http://www.jpcert.or.jp/isdas/

17 @police, http://www.cyberpolice.go.jp/detect/observation.html

18 MUSTAN, http://mustan.ipa.go.jp/mustan web/

19 WCLSCAN, http://www.wclscan.org/

20 K. Suzuki, S. Baba, H. Wada, K. Nakao, H. Takakura, and Y. Okabe, “Implementation and Evaluation of a Traffic Data Delivery System for Executing Realtime Analysis by Multiple Methods,” IEICE Trans. Information and Systems, Vol. J92-B, No. 10, pp. 1619–1630, 2009.

21 Ruby On Rails, http://rubyonrails.org/

22 C. Zou, W. Gong, and D. Towsley, “Code Red Worm Propagation Modeling and Analysis,” 9th ACM Conference on Computer and Communications Security (CCS '02), 2002.

23 D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, “Inside the SlammerWorm,” IEEE Security and Privacy, Vol. 1, No. 4, pp. 33–39, 2003.

24 IP Scanner Pro, http://10base-t.com/macintosh-software/ip-scanner/

(Accepted June 15, 2011)

SUZUKI Mio, *Ph.D.*

Technical Expert, Cybersecurity Laboratory, Network Security Research Institute

Network Security, IPv6 Security, Network Emulation

INOUE Daisuke, *Ph.D.*

Director, Cybersecurity Laboratory, Network Security Research Institute

Network Security, Information Security