2-3 nicter Report —Transition Analysis of Cyber Attacks Based on Long-term Observation—

NAKAZATO Junji and OHTAKA Kazuhiro

In this report, we provide a statistical data concerning cyber attacks and malwares based on a long-term network monitoring on the nicter. Especially, we show a continuous observation report of Conficker, which is a pandemic malware since November 2008. In addition, we report a transition analysis of the scale of botnet activities.

Keywords
Incident analysis, Darknet, Network monitoring, Malware analysis

1 Introduction

We have been monitoring the IP address space that is reachable and unused on the Internet (i.e. darknets) on a large-scale to understand the overall impact inflicted by infectious activities including malware. This report analyzes the darknet traffic that has been monitored and accumulated over six years by an incident analysis center named the nicter[1][2] to provide changing trends of cyber attacks and fluctuation of attacker host activities as obtained by long-term monitoring. In particular, we focus on Conficker, a worm that has triggered large-scale infections since November 2008, and report its impact on the Internet and its current activities. We also extract the scan of botnets detected through our long-term monitoring and report on the fluctuation of botnet scales over a period.

The nicter places black hole sensors on a darknet to collect and analyze darknet traffic on a large scale. A black hole sensor is a sensor collecting all incoming packets without responding to their source, capable of monitoring the scan tendency of malware and Backscatter (i.e. responses to DDoS attacks based on falsified IP addresses). This report leverages the traffic as detected by the four black hole sensors placed on different network environments as shown by Fig. 1.

- **Sensor I** : Structure where live nets and darknets coexist in a class B network
- **Sensor II** : Structure where only darknets exist in a class B network
- **Sensor III** : Structure where a /24 subnet in a class B network is a darknet*1
- **Sensor IV** : Structure where live nets and darknets coexist in a class B network

The traffic obtained by these four sensors is analyzed by different analysis engines[3][4] provided by the nicter and are stored over a long period of time with their analysis results.

The nicter monitors darknet traffic on a large-scale, while it deploys and operates honeypots collecting malware to identify the malware causing the traffic. Honeypots used by this report are categorized into five groups: Honeypot I deployed on 250 successive IP addresses; Honeypot Ⅱ and Honeypot

*1 There exist darknets other than the monitored /24 network, with the other portions composed of live nets.

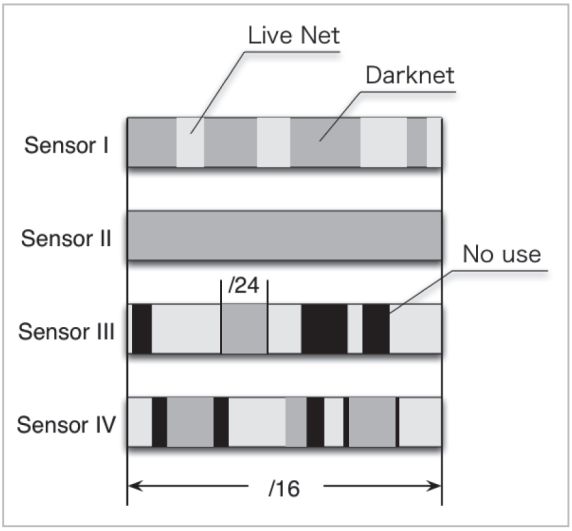


Fig.1 *Summary of monitoring network*

Ⅲ deployed on one IP address; Honeypot Ⅳ deployed on three IP addresses; and Honeypot Ⅴ whose data is provided by external organizations. Honeypots Ⅰ, Ⅱ, and Ⅲ are composed of software emulating general vulnerabilities (i.e. low-interaction honeypot), while Honeypot Ⅳ is set up so that it can rotate different versions of Windows operating systems on real machines and deal with unknown vulnerabilities (i.e. high-interaction honeypot).

The overall trend of the cyber attacks as obtained through our darknet monitoring over six years is reported by Chapter **2**. Chapter **3** shows the statistical data concerning the malware we have collected and analyzed through the honeypots deployed since 2007. Chapter **4** analyzes the fluctuation of botnet scales based on the botnet scans we have monitored over a period. Our final conclusion is summarized by Chapter **5**.

2 Transition of attacks detected on darknets

In the early 2000s, malware that triggered large-scale infections including MSBlaster were rampant on the Internet. On the other hand, the malware detected in the late 2000s have evaded detection through their more sophisticated and subtle mechanisms and enjoyed their covert existence behind the scenes. Large-scale infections could have increased the load and traffic of infected hosts and made users and network administrators more keen on noticing infections, reducing the scale of infectious activities step by step. Furthermore, the emergence of botnets enabled multiple infectious hosts to behave collaboratively so the infectious activities for each host became smaller in their scale. These components made it look highly unlikely in the late 2000s for malware to trigger large-scale infections through networks[5]. In fact, we saw some decrease in the number of detected hosts as we started monitoring through the nicter.

2.1 Transition of the number of unique hosts and packets

Figures 2 and 3 show the transition of the number of unique sender IP addresses (“unique hosts”) and the number of packets included in the traffic detected through the darknet monitoring by the nicter. These two figures illustrate the transition of the moving average of the number of unique hosts and packets detected by each sensor per day (window size: 7 days). The monitoring start date of each sensor is September 5, 2006 for Sensor Ⅰ, December 14, 2004 for Sensor Ⅱ, October 22, 2007 for Sensor Ⅲ, and July 10, 2009 for Sensor Ⅳ. You can see an increase in the number of unique hosts and packets for Sensor Ⅱ at the time when Sensor Ⅰ was added (September 5, 2006). This is because the scale of Sensor Ⅱ was enhanced from a /18 network to a /16 network.

Figure 2 suggests a slight declining in the number of unique hosts between the monitoring start time and late 2008. However, we can see a dramatic increase in the number of detected unique hosts starting in November 2008: a 15-times growth with Sensor Ⅰ and Sensor Ⅱ and about a 10-times increase with Sensor Ⅲ, which covers a smaller scale in monitoring. This increase of unique hosts is impacted by the large-scale infections caused by the Conficker worm[6][7]. The influences inflicted by Conficker worm are explained in Section **2.2**.

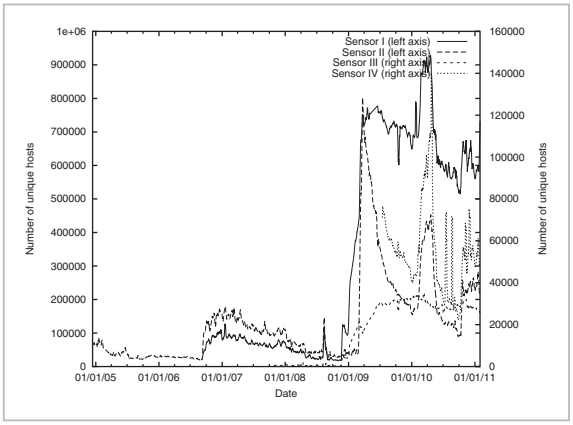


Fig.2 *Number of unique hosts*

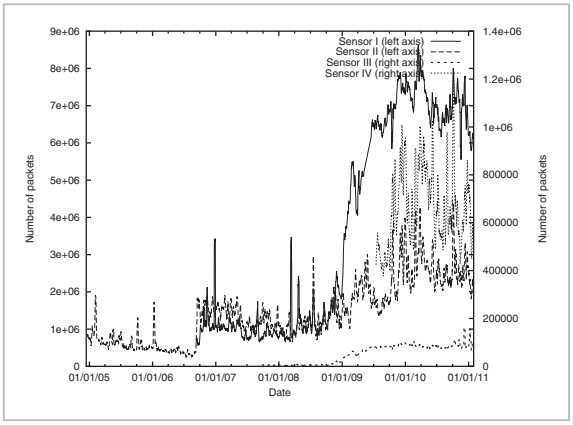


Fig.3 *Number of packets*

Figure 3 shows a dramatic increase in the number of detected packets and unique hosts starting in late 2008, along with the transition of the number of unique hosts. Before November 2008, the number of detected packets was almost flat despite some wild ups and downs. The number of unique hosts was on the decline with the number of packets almost flat, suggesting that the average number of packets transmitted by each host was on the increase. On the other hand, Sensor I, which has detected the largest number of packets, has monitored seven times more packets since November 11 2008. This rate is about half of the growth rate in the number of detected unique hosts (i.e. about 15 times). This means that the average number of packets transmitted by each host has almost halved in comparison with the pre-November 2008 level.

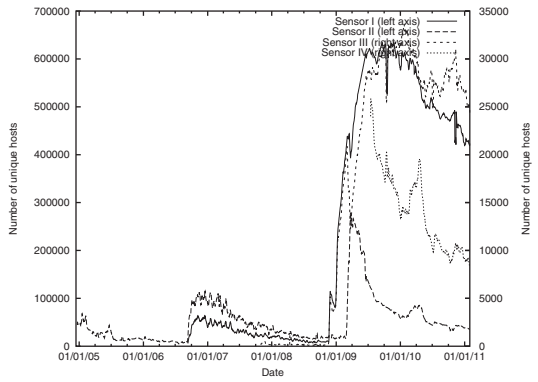
In sum, the number of infected hosts was somewhat declining between the beginning of the late 2000s and November 2008. On the other hand, the number of transmitted packets continued at almost at the same level, placing the average number of packets transmitted by one host on a growth path. Starting in November 2008, when the Conficker worm started its activities, the number of infected hosts began to multiply in a dramatic manner and the average number of packets transmitted by each host dropped to about one half of the previous level.

2.2 Impacts inflicted by the Conficker worm on networks

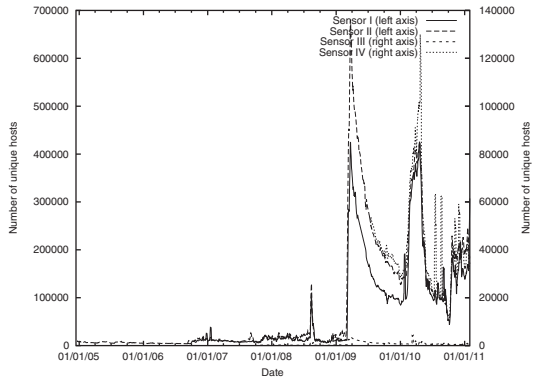
Starting around November 2008, the large-scale infections triggered by Win32/Conficker (also known as Downadup) have become a social problem. This worm is known to leverage vulnerability in Windows Server services (MS08-067). This vulnerability can be attacked through networks, enabling computers (hosts) infected with Conficker to look for another attack target and leading to large-scale scans implemented on networks. We have analyzed the impacts caused by Conficker.A (occurring on November 21, 2008), Conficker.B (occurring on December 29, 2008), Conficker.C (occurring on February 20, 2009), and Conficker.D (occurring on March 4, 2009) based on [6] and [7]. Microsoft has not reported any new varieties of Conficker with the last-detected Conficker.E discovered on April 8, 2009[8].

Figure 4 shows the transition of the number of unique hosts for each protocol (TCP and UDP) and the number of 445/TCP unique hosts used by Conficker worm for infections. Figure 4 (a) and (c) suggest that a vast majority of hosts detected by Sensor I and Sensor Ⅲ as TCP packets are transmitting to the port number 445. On the other hand, we have not detected any impacts on 445/TCP from Sensor Ⅱ and Sensor Ⅳ, with an increase in the number of TCP/UDP unique hosts detected four months later (i.e. around March 2009). Conficker.D discovered on March 4 2009 is reported to have the P2P rendezvous feature,

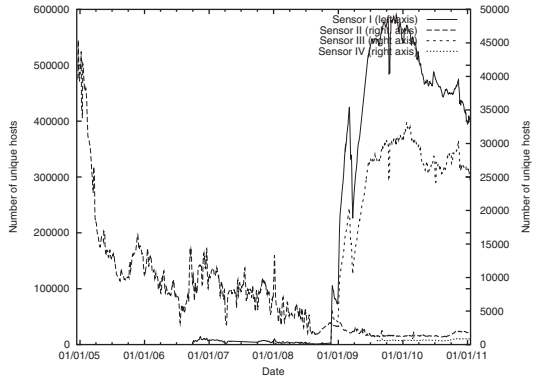
capable of transmitting TCP/UDP scans on a large-scale to high ports (i.e. port numbers higher than 1024)[7]. This is likely to have changed the networks impacted by the scans, changing the trends of Sensor Ⅱ and Sensor Ⅳ. Sensor Ⅱ and Sensor Ⅳ, not impacted by 445/TCP, saw a decrease in the number of unique hosts for both TCP and UDP after the number peaked on March 18. The number of TCP/UDP unique hosts shows a fairly similar pattern of decline. The number of UDP unique hosts also showed a decline for Sensor I, suggesting a decrease in attacks by Conficker.D equipped with the P2P rendezvous feature and scans against high ports. The scans against 445/TCP have decreased about 20% with Sensor I and Sensor Ⅲ in comparison with the peak around February 2010, but were still detected in large numbers as of January 2011. Thus, we can safely say that other varieties of Conficker other than Conficker.D are still infecting many hosts as of now.



(a) Number of unique hosts (TCP)



(b) Number of unique hosts (UDP)



(c) Number of unique hosts (445/TCP)

Fig.4 *Influence of Conficker worm for the Internet*

3 Transition of malware

The nicter has operated honeypots and dynamically analyzed malware since 2007 to detect the root causes of malware scans and come up with countermeasures. To address various types of malware, multiple honeypots with different characteristics and environments (operating systems), including low-interaction honeypots, high-interaction honeypots, and web crawlers, are being operated. We have succeeded in obtaining and analyzing more than 1.6 million malware samples until January 2011. Figure 5 shows the accumulated numbers of malware types*2 obtained by the five honeypots with different characteristics. The

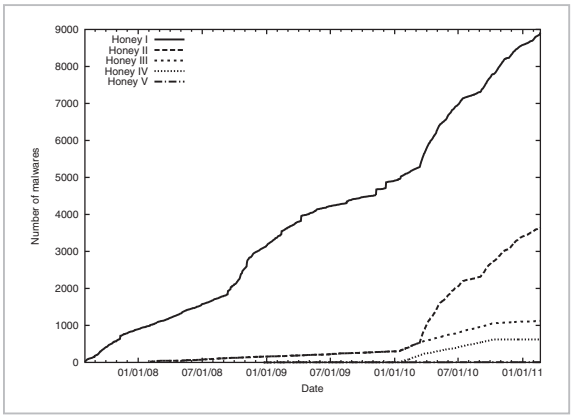


Fig.5 *Number of malwares (accumulation)*

*2 The number of malware with different MD5 hash values obtained by each honeypot.

five honeypots have been in operation during different timeframes but have so far obtained about 9,000 malware samples in total.

Figure 6 illustrates the top 10 malware names. We have obtained the names of malware samples based on antivirus software by Symantec and have not differentiated varieties of each detected malware. For example, we have detected various varieties of W32.Virut including W32.Virut.A and W32.Virut.B, but the number is calculated as W32.Virut. In total, about 350 malware occurrences have been detected, with W32.Virut accounting for about a quarter of them. Such popular malware as W32.Virut, W32.Spybot, and W32.Korgo has been existent for a long time with their first occurrence dating back before 2007 but has accounted for about a half of the total occurrences. In addition, W32.Downadup (also known as Conficker) moved up to number 2 about two years after its first detection, showing its scale of infections. As we focus on the number of obtained malware for one month (i.e. December 2010), 33 samples out of the total 61 are based on W32.Downadup, which signifies how big its threat is in the current environment.

4 Fluctuation of botnet scales

Darknets allow us to monitor large-scale scans used for the detection of vulnerable hosts. Bots receive instructions from C&C servers using IRC etc. and other mechanisms and behave in a collaborative manner. This enables bots connected to the same IRC channel to behave as instructed at the same timing. Therefore, focusing on a rapid increase of unique hosts per a certain time period will allow us to detect the traffic that is scans by bots. In this report, we define the following events as scans by botnets.

1) Multiple hosts behaving in a collaborative manner at the same time
2) Scanning extensively for large-scale infections
3) Searching for specific vulnerabilities

In darknets, we can detect first contacts (i.e. packets used to initiate transmission) targeted for certain vulnerabilities, allowing us to estimate the scale of bonnets based on the transition of the number of unique hosts transmitting TCP/UDP packets. Thus, we have detected an increase of unique hosts beyond a certain threshold based on the transition of unique hosts over a five-minute period to extract scans by botnets. Figures 7 and 8 show the transition of unique hosts transmitting TCP/UDP packets every five minutes. Each of these figures shows a rapid increase of hosts (i.e. a spike) at multiple instances.

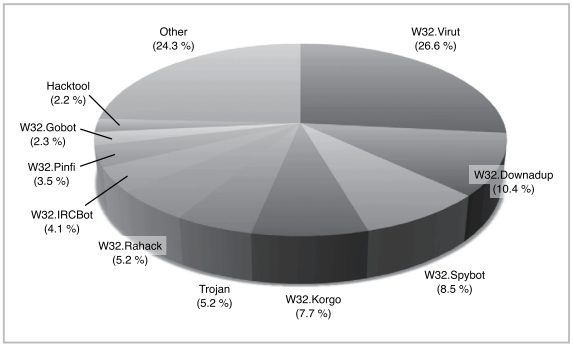


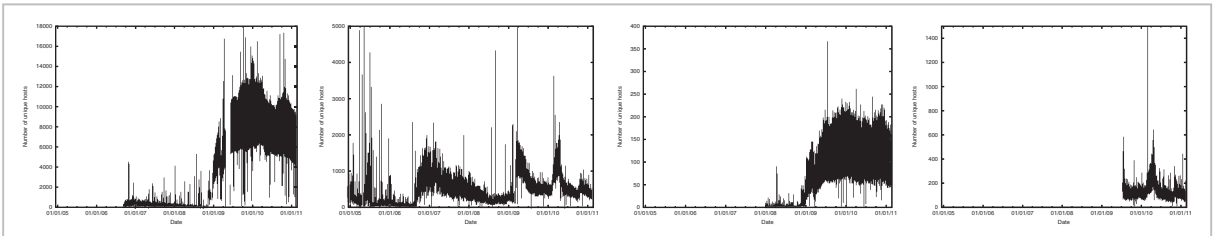
Fig.6 *Type of malware families*

4.1 Methodology to extract bot activity periods

Figures 7 and 8 show how we have detected a rapid increase (i.e. a spike) of unique hosts based on various sensors and protocols. Based on the assumption explained by Chapter **4**, we consider an increase of unique hosts using a specific protocol and detected at the same time as scans by bots. The following shows how we extract scans by bots. First of all, we calculate the moving average of the number of unique hosts h_i detected every five minutes as below.

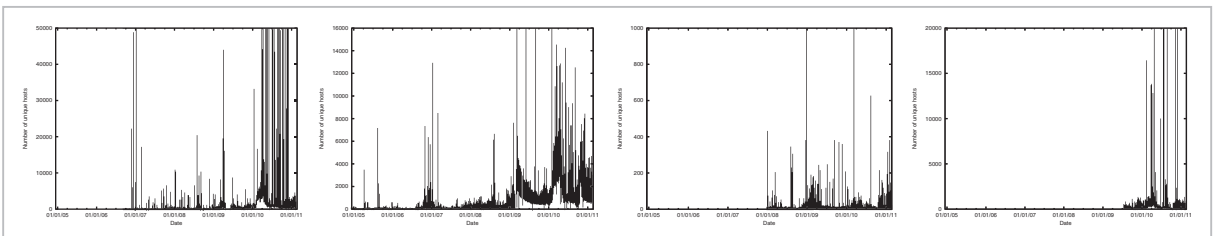
$$a_t = \frac{\sum_{k=t-m}^{t} h_k}{m} \quad (1)$$

m means the number of data points (i.e. a period) used to calculate the moving average. Next, we calculate the variance between the moving average a_t and the number of unique



a) Sensor I b) Sensor Ⅱ c) Sensor Ⅲ d) Sensor Ⅳ

Fig.7 *Number of unique hosts (TCP)*



a) Sensor I b) Sensor Ⅱ c) Sensor Ⅲ d) Sensor Ⅳ

Fig.8 *Number of unique hosts (UDP)*

hosts h_t as below.

$$s_t = \sqrt{\frac{\sum_{k=t-m}^{t}\left(a_k - h_k\right)^2}{m}} \tag{2}$$

Lastly, we calculate the ratio of the difference between the number of unique hosts h_t and the moving average a_t against the last variance value.

$$r_t = \frac{\left(h_t - a_t\right)}{s_{t-1}} \times h_t^{\frac{1}{4}} \tag{3}$$

Since the variance value shows the average difference (i.e. the difference against the average value), calculating the ratio of the last variance value s_{t-1} against the difference from the average value $(h_t - a_t)$ enables us to detect a rapid increase of unique hosts. However, as the variance value tends to become larger based on an increase of the number of unique hosts (i.e. an increase in the moving average) and make the ratio smaller, we use $h_t^{\frac{1}{4}}$ to weight the value. Finally, the spots whose values are larger than the threshold r_t are supposed to include scans by bots.

4.2 Methodology to extract scans by bots

Based on the methodology explained by Section **4.1**, we extract scans by bots (i.e. spike events) from Figs. 7 and 8. Since the monitoring scale is different based on monitoring sensors and protocols, we define a threshold for each scenario and extracted scans. Table 1 shows the results of scans by bots. The period we used for the calculation of the moving average is $m = 288$ (24 hours).

In this report, we set higher thresholds to extract spots where an increase of unique hosts is relatively high. As a result, 631 events have

Table 1 *Number of botnet scans*

Sensor	Protocol	Threshold	# of event
Sensor I	TCP	30	99
	UDP	70	142
Sensor Ⅱ	TCP	30	90
	UDP	80	77
Sensor Ⅲ	TCP	10	66
	UDP	25	108
Sensor Ⅳ	TCP	20	28
	UDP	70	39

been defined as scans by bots. On average, about 100 botnet activities are detected on an annual basis.

4.3 Estimation of botnet scales

Figure 9 shows the number of scans by bots detected each month and the average size of botnets comprising at that time (i.e. the average number of bots comprising detected botnets). We consider the 24-hour moving average as the number of unique hosts in the steady state (i.e. the scans by malware excluding bots) and define the size of botnets as the incremental value against the number of unique hosts in the steady state ($h_j - a_j$).

The number of cases where we detected botnet scans were temporarily on the decline around 2010, but otherwise have been increasing year by year. On the other hand, the size of detected botnets (i.e. the number of bots comprising them) grew rapidly after 2010. The data tells us that the size of each botnet has recently grown larger, making scans more efficient and attacks (e.g. DDoS attacks) and spam transmission larger in scale. In fact, spam transmission using botnets has been very popular, allowing botnet administrators to rent botnets to obtain monetary benefits. It is a well-known fact that the larger the size of botnets is, the higher their prices are for transactions[9].

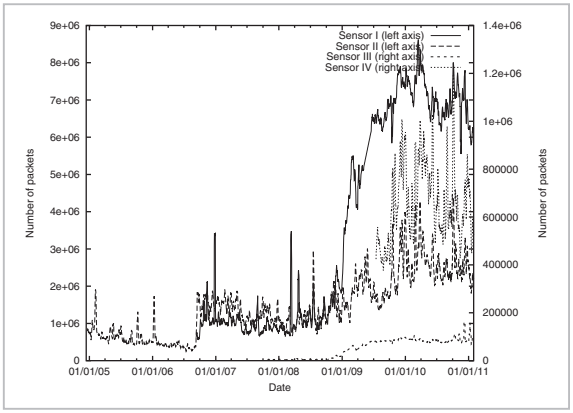


Fig.9 *Change of a size of a botnet*

5 Conclusion

We have obtained and analyzed the results of a long-term network monitoring through the nicter project. Up until early 2008, the number of hosts scanning against darknets was little by little on the decline and some even predicted that no more large-scale infections on networks will occur. However, the emergence of Conficker has drastically changed the situation. The impacts inflicted by Conficker on networks are still underway, accounting for more than half of the detected darknet traffic.

Furthermore, the results of malware collected by honeypots operated by the nicter project clearly showed that the kind of malware that once ran havoc on the Internet, including W32.Virut, W32.Spybot, and W32.Korgo, are still being detected. The phenomenon suggests that malware that has triggered large-scale infections (e.g. Conficker) are still expected to continue to exist going forward, requiring us to monitor their activities on an on-going basis.

We have found out that the number of scans initiated by bots has generally been on the rise with some drop observed around 2010. On the other hand, the scale of botnets has dramatically grown since 2010 with their size continuing to expand. With botnet administrators expected to expand their botnets to extort monetary proceeds, we need to continue to monitor and analyze their activities.

References

1 Koji Nakao, Katsunari Yoshioka, Daisuke Inoue, and Masashi 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.

2 Daisuke Inoue, Masashi Eto, Katsunari Yoshioka, Syunsuke Baba, Kazuya Suzuki, Junji Nakazato, Kazuhiro Ohtaka, and Koji 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.
3 Kazuya Suzuki, Yoshinori Hashimoto, and Shunsuke Baba, "Traffic analysis based on long term trend variations," Symposium on Cryptography and Information Security (SCIS 2007), 1F2-3, 2007. (In Japanese)
4 Daisuke Inoue, Katsunari Yoshioka, Masashi Eto, Yuji Hoshizawa, and Koji Nakao, "Automated Malware Analysis System and its Sandbox for Revealing Malware's Internal and External Activities," IEICE Trans. Information and Systems, Vol. E92-D, No. 5, May 2009.
5 Daisuke Inoue and Koji Nakao, "What's Malware?," IPSJ Magazine, Vol. 51, No. 3, pp. 237–243, 2010. (In Japanese)
6 Junji Nakazato, Kazuhiro Ohtaka, Jumpei Shimamura, and Koji Nakao, "Network Observation and Analysis Report on nicter," IEICE Technical Report, Vol. 109, No. 33, pp. 15–20, 2009. (In Japanese)
7 Junji Nakazato, Kazuhiro Ohtaka, Jumpei Shimamura, and Koji Nakao, "Network Observation and Analysis Report on nicter—Continuous Observation of Conficker and a Primary Example of Macro-Micro Correlation Analysis—," IPSJ SIG Notes, Vol. 2009-CSEC-46, No. 18, 2009. (In Japanese)
8 Microsoft Security TechCenter, "Conficker Worm: Help Protect Windows from Conficker," http://technet.microsoft.com/ja-jp/security/dd452420
9 CNET News, "Botnet services for hire: $8.94 an hour," http://news.cnet.com/8301-1009_3-20005844-83.html

(Accepted June 15, 2011)

NAKAZATO Junji, *Ph.D.*

Expert Researcher, Cybersecurity Laboratory, Network Security Research Institute

Network Security, Malware Analysis, Cryptography, Privacy Preserving

OHTAKA Kazuhiro

Senior Researcher, Cybersecurity Laboratory, Network Security Research Institute

Network Security, Space Weather