Copyright ⓒ 2012 KSII

Detection of Zombie PCs Based on Email Spam Analysis

HyunCheol Jeong[1], Huy Kang Kim[2], Sangjin Lee[2] and Eunjin Kim[3]
[1] Korea Internet & Security Agency
Seoul, Korea
[2] Graduate school of Information Security, Korea University
Seoul, Korea
[3] Kyonggi University, Suwon, Gyeonggi-do, Korea
[e-mail : hcjung@kisa.or.kr, cenda, sangjin@korea.ac.kr, ejkim777@kgu.ac.kr]
*Corresponding author: Huy Kang Kim

Received November 4, 2011; revised February 6, 2012; revised April 20, 2012; accepted April 24, 2012; published May 25, 2012

Abstract

While botnets are used for various malicious activities, it is well known that they are widely used for email spam. Though the spam filtering systems currently in use block IPs that send email spam, simply blocking the IPs of zombie PCs participating in a botnet is not enough to prevent the spamming activities of the botnet because these IPs can easily be changed or manipulated. This IP blocking is also insufficient to prevent crimes other than spamming, as the botnet can be simultaneously used for multiple purposes. For this reason, we propose a system that detects botnets and zombie PCs based on email spam analysis. This study introduces the concept of *"group pollution level"* – the degree to which a certain spam group is suspected of being a botnet – and "*IP pollution level*" – the degree to which a certain IP in the spam group is suspected of being a zombie PC. Such concepts are applied in our system that detects botnets and zombie PCs by grouping spam mails based on the URL links or attachments contained, and by assessing the pollution level of each group and each IP address. For empirical testing, we used email spam data collected in an "email spam trap system" - Korea's national spam collection system. Our proposed system detected 203 botnets and 18,283 zombie PCs in a day and these zombie PCs sent about 70% of all the spam messages in our analysis. This shows the effectiveness of detecting zombie PCs by email spam analysis, and the possibility of a dramatic reduction in email spam by taking countermeasure against these botnets and zombie PCs.

Keywords: Bot-net, internet worm, malware, email spam, zombie PC

"This research was supported by the KCC(Korea Communications Commission), Korea, under the R&D program supervised by the KCA(Korea Communications Agency)"(KCA-2011-10914-06001, The Development of Automatic Analysis and Malicious Site Detection Technology Against Malware

http://dx.doi.org/10.3837/tiis.2012.05.011

1. Introduction

Today, botnets – networks of infected computers or bots – have become one of the key platforms for cyber attacks, such as ransom DDoS (distributed denial of service) attack, personal/financial information theft and illegal email spam. In addition, an attacker does not need to have a high level knowledge in the areas of networks or operating systems to build and operate a botnet. With malware that can easily be found on the internet, attackers can infect unpatched computers and form a botnet. These infected computers (from hundreds of thousands to millions) called Zombie PCs, are remotely controlled by a C&C (Command & Control) Server.

One of the values of botnets comes from their ability to provide anonymity to the attackers through the use of a multi-tier C&C (Command & Control) architecture. Moreover, the individual Zombie PCs or bots are not physically owned by the attackers, and are often located across the globe, which makes it difficult to track botnet activities across international borders [1]. In addition, attackers can also expect to earn money by trading botnets in the underground economy. It is known that a single bot is traded for about $0.03, and a botnet composed of tens of thousands of bots has a value of only several hundred dollars [2]. Due to these benefits of using botnets, these botnets have become more widespread, and are actively being used for various forms of cyber attack.

Among the cyber attacks performed using botnets, email spam is considered the most useful, as it carries a relatively low risk of detection, and requires a little complexity in design and implementation [3][4]. In addition, since spam filtering systems quickly block IPs that send email spam, botnets are preferred by the majority of spammers who require a great number of new mail servers. For these reasons, botnets are widely used for spamming. In a recent survey, it was found that 83.2% of all email spam was sent by botnets [5]. As mentioned previously, spam filtering systems can block the IPs of zombie PCs participating in a spamming botnet. However, this alone does not effectively prevent them spamming, as IPs can easily be changed or manipulated. In addition, IP blocking cannot prevent crimes other than spamming, this is a critical weakness of IP blocking as the same botnet can be simultaneously used for multiple purposes. For these reasons, botnets must be detected and responded to in a more proactive manner.

Botnet detection and tracking, therefore, has become a major research topic in recent years, and several approaches to botnet detection and tracking have been proposed. However, previous studies on botnet detection have many limitations in their implementation.

We can assume that anti-spam solutions are able to detect the spammers' exact location and the PCs involved in sending the spam mail, as such, these things can provide clues for revealing botnets. However, the current spam filtering systems are not effective enough to detect spam mail, this is because spam mail systems have been evolving for two decades and are still evolving to stay ahead of the countermeasure. Besides, even when the spam-sending email servers of botnets are blocked by those systems, the botnet can then be immediately used for other types of attacks, such as DDoS attacks. Hence, simple blocking is not enough to deal with botnets. Early detection and cure of zombie PCs from email spam is therefore required.

This study aims to overcome the increase of spam using botnets and improve upon the limited response provided by just IP blocking. As detecting spam mailers is a good approach to finding the members of a botnet, this study aims to develop a system that detects botnets and zombie PCs based on an analysis of email spam.

In this paper, we compare our work with related works in Section 2. In Section 3, we analyze the characteristics of email spam sent via botnets, and design a system for detecting botnets from spam mails. In Section 4, we test the proposed system using email spam collected in an email spam trap system. In Section 5, we conclude the paper by identifying areas for future research.

2. Related Work

Botnet detection has been a major research topic in recent years. While different approaches have been proposed, there are two main approaches for botnet detection [1]. One approach is based on setting up honeynets [1][6]. Honeynet-based solutions detect malicious bots by statically/dynamically analyzing malware codes found via a honeynet in a virtual host. Many studies [1][7][8] have discussed how to use honeynets for botnet tracking and measurement. However, this approach is not effective when evasion techniques, such as packing, encryption, and non-running in a virtual machine, are used. The other approach for botnet detection is based on passive network traffic monitoring and analysis [1][6]. When the bots communicate with some C&C servers/peers, perform malicious activities, they may do so in a similar or correlated way. These traffic monitoring and analysis method clusters similar communication traffic and similar malicious traffic, and performs cross-cluster correlations to identify the hosts that share similar communication patterns and similar malicious activity patterns [9][10]. However, this method has performance issues and produces a high rate of false positives in large-scale network environments. Normal traffic showing group behavior, such as PMS (Patch Management System) or NMS (Network Monitoring System) traffic, is sometimes falsely detected as botnet traffic.

In our study, the target for analysis is email spam, which is mostly sent via malicious bots. There is a lot of information in the mail header and body of an email that is useful for determining whether the spam mail is sent by a zombie or not. It is hoped that by taking this focus, our study will improve the accuracy of detection, and solve performance issues associated with other methods. We will start by discussing previous research on the detection of botnets using email spam.

Yinglian Xie et al. [11] suggested a framework, known as AutoRE, which automatically creates a URL signature for detecting spam botnets. In Yinglian Xie's study, email spam found via Hotmail was used as simulation data, and spam botnets and zombie IPs were detected by analyzing spam payload and traffic. The criteria used to identify the spam botnets from the data were "distributed," i.e. many different autonomous systems (AS) sent spam, "bursty," i.e. much spam was sent during a very short period, and "specific," i.e. the characteristic of random URL strings. In addition, network traffic, such as network scanning of spam botnets, was used for detecting spam botnets.

Ramachandran et al. [12] presented SpamTracker, which is a spam filtering system that uses a new technique called behavioral blacklisting to classify email senders based on their sending behavior rather than their identity. In Ramachandran's study, email spam found via Hotmail was used as simulation data, and spam botnets and zombie IPs were detected by analyzing spam payload and traffic. SpamTracker clusters the spam with similar patterns and filters spam mail using not only the spammer's IP address but also behavioral characteristics such as mail size, mail arrival time, and spamming interval. However, Ramachandran's study had difficulties in detecting botnets when the botnet sends a small amount of spam mail over long periods of time.

John et al. [13] developed a platform, known as Botlab, which is capable of continuously monitoring and analyzing the behavior of spam-oriented botnets. Botlab detects spam bots through five processes, which are Network Fingerprinting, Execution Engine, DNS Monitoring, Clustering, and Correlation Analysis. Based on the URL of the spam data, Botlab crawls, executes the downloadable files on a virtual machine or bare metal execution engine, and then monitors the behavior. After analyzing the relationship between the monitoring execution engine behavior and the DNS monitoring, spam bots are classified. The platform developed for John's study is quite useful in detecting spam bots designed to spread malicious code, but have limitations in detecting advertising spam bots, because in most cases of advertising spam no malicious executable file is downloaded, even when the selected advertisement URL is checked.

Zhuang et al. [14] conducted research that identifies botnet members by analyzing spam mail found on the MS Hotmail servers. Zhuang's study identified a spam campaign with an approach that involved clustering emails with the same URL, or the same or similar contents. Also, the botnet size and spam sending intervals of each spam campaign were monitored. In Zhuang's study, the URL was selected as a major factor for clustering botnets into the same group. However, this approach lead to a high false positive rate, because all IPs are regarded as a bot, with three exclusions – 1) when the IP address is a known relay IP or proxy IP, 2) when IPs in the spam campaign belong to one C-class, and 3) when the IP belongs to an area less than 3. **Table 1** is a comparison of related works and our proposed model.

Table 1. Comparison of related works and our proposed model

	Goal	Approach	Problem
Yinglian Xie [11]	Design for characterizing spamming botnets by leveraging both payload and spam server traffic properties	Developed a spam signature generation framework called AutoRE	This method has difficulty in detection if there is no URL in the spam mail
Ramachandran [12]	Design for filtering spam mail by using the behavioral characteristics of spam mail	Developed a spam filtering system called SpamTracker	This method has difficulty detecting a botnet when a spam botnet sends a small number of spam mails over a long period of time
John [13]	Design for detecting a spamming botnet by monitoring network behaviors	Developed a platform, known as Botlab, that is capable of monitoring the behavior of spam botnets	This method of detection is limited to spam mail with an executable file attached
Zhuang [14]	Design for identifying a spam botnet by clustering multiple spam campaigns	Group bots in the same spam mail campaign	This method has a high risk of false-positives
Our Proposed Model	Design for detection of spam botnets and internet worms by analyzing spam mail header and payload.	Adapt *IP pollution level* and *group pollution level*	This method can miss spam bot/email worms if the spam mail contains neither a URL nor an attached file.

The above studies were mostly aimed at monitoring or forecasting spam behavior by clustering spam campaigns using URLs in the spam mail. However, these behavior-based methods have a high ratio of false positive detections compared to signature-based methods. In

our study, we use both the behavior method and the signature method to reduce the false positive ratio. The zombie characteristics of a spam-sending host are analyzed using the signature method, and the botnet characteristics of a spam campaign are analyzed using the behavior method. In the following, we outline the differences found in our study compared to previous studies.

First, the characteristics identified when a host is infected by a bot were utilized to detect zombie PCs. Unlike existing studies [14] that determine a botnet based on the analysis of groups' behavioral characteristics, such as dispersion and locality, our study introduced the concept of "*IP pollution level*," which indexes the characteristics that can appear when an IP is infected by a malicious bot and sends spam automatically, such as RBL (Real-time Blackhole List) registration of the spam-sending IP, the number of sent emails**,** MTA (Mail Transfer Agent) status of the sending email server, and the number of "Received From" records.

Second, both the URL and attached file were used for spam group clustering. By looking at previous studies [3][4], we can see most research clusters spam based on the URL. As most spam mails include a URL, the URL is definitely the most important factor in clustering spam. However, the attachment file also seems to be an important factor for spam clustering. Analyzing a group with the same attachment file can be useful in detecting an Internet worm that is spread via email.

Finally, the concept of "group pollution level" is newly introduced, just dealing with single IP address cannot give a big picture to figure out spam delivered and managed by professional group, e.g. professional spammers or botnet. For this, the feedback process that can update the "group pollution level" with the previously driven "IP pollution level" is included.

3. Design of Zombie PC Detection System

3.1 Features of Email Spam Sent by Zombie PCs

There are different ways of sending email spam. Email spam can be sent manually by advertisers, or sent in bulk by using a spam-sending machine. In addition, bulk email spam is often sent via webmail after bots obtain webmail accounts. Email spam can also be sent with an SMTP (Simple Mail Transfer Protocol) engine mounted on the malicious bot itself. Despite these diverse ways of sending email spam, it is reported that 83.2% of all spam is sent via botnets [15].

Spammers usually need a mail server and network bandwidth to send email spam. However, the mail servers that are used to send email spam are easily blacklisted and blocked. This problem can be solved by using a botnet. A botnet is distributed over a large number of hosts, so it is difficult to block. In addition, a botnet also allows spammers to use bandwidth at no cost. These are the characteristics of a botnet that spammers find attractive.

Some spam botnets make the contents for email spam via spam templates, and regularly or randomly fabricate a sender's email address, subject, and payload. The recipients of email spam are determined by receiving a list of email addresses from a bot C&C server, or by collecting email addresses from the email address books or cache files of zombie PCs. SMTP engines in zombie PCs, proxy email addresses, or webmail services such as hotmail are used for sending email spam. Generally, mass MX (Mail Exchanger) queries are requested to check for recipients' email servers when sending email spam.

We performed traffic monitoring for an infected host that was part of the "waledec" botnet. We could see the host generated 227,497 packets (42,252,856 Bytes) in 24 hours. Of those

packets, SMTP traffic was 80.92% (184,084 Packets) and DNS traffic was 11.84% (26,936 Packets). This would be a very large volume of DNS MX queries and SMTP traffic for a normal user.

3.2 Overview of the System

For our proposed system, we introduce the notion of "*pollution level*", which is similar to the concept of "*uncleanliness*" introduced in the Collins' paper [16]. Collins et al. defined a network-based quality of uncleanliness, as an indicator of how likely a network is to contain compromised hosts. In that paper, they used "uncleanliness" to predict future hostile activity from past network activity. However, we used pollution level to detect botnet/internet worm groups and zombie PCs. It is important to increase the detection accuracy, so we tried to use diverse factors when measuring the pollution level. **Fig. 1** is an overview of our proposed system.

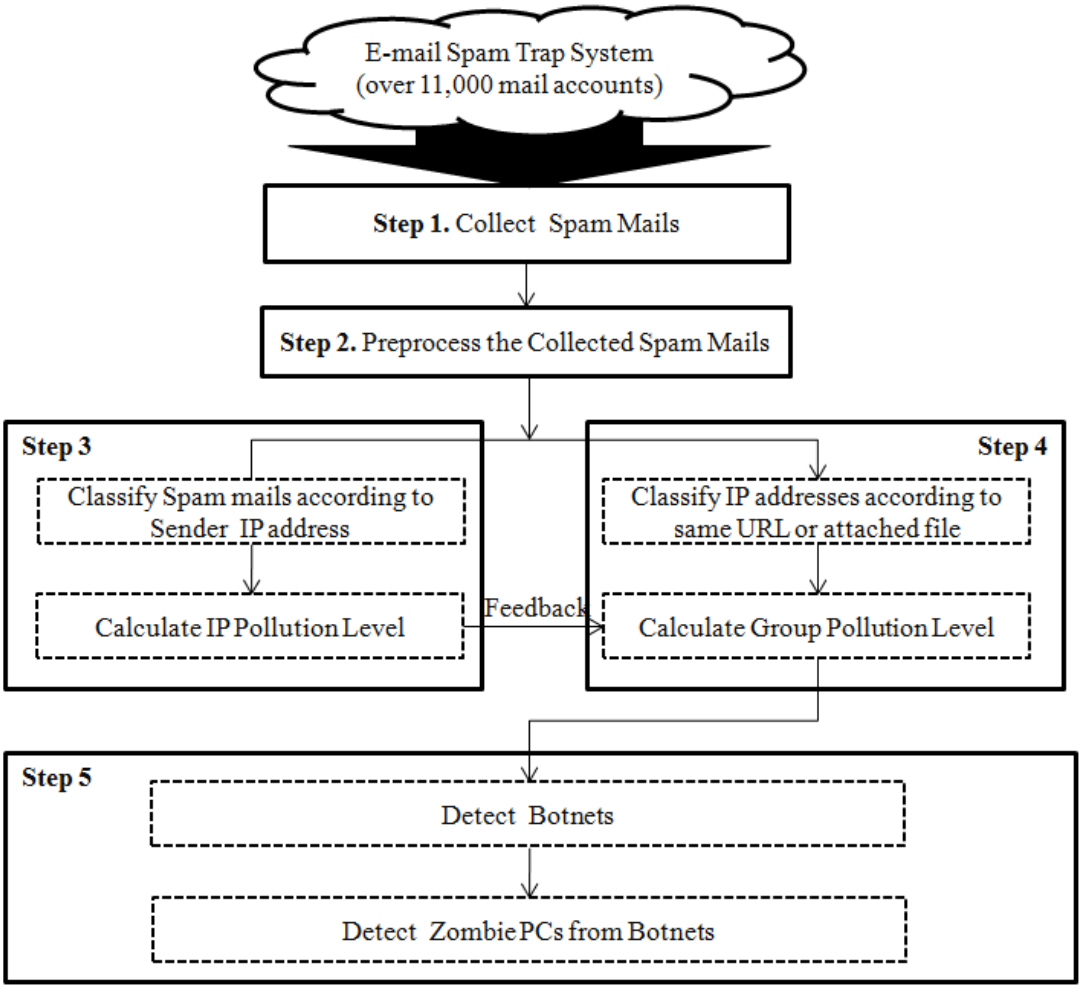


Fig. 1. Overview of Detecting Zombie PCs

In this paper, we introduce two terms: "*IP pollution level*" and "*Group pollution level*." "*IP pollution level*" is an indicator of how likely it is that a host at a certain IP address is a zombie

PC. *IP pollution level* is measured by analyzing the profile of the host and the mail header sent by that host. It is measured based on four factors, including whether or not the host has been registered in the RBL, the number of sent mails, whether or not the host is a real MTA, and the number of "Received From" records. "*Group pollution level*" is an indicator of how likely a group, composed of hosts in the same spam campaign, is a botnet or worm group. It is measured based on three factors, including the number of hosts included in each group, regional diversity, and the average *IP pollution level* of the hosts.

3.3 Design a System for Detecting Zombie PCs

A system for detecting zombie IPs was designed that includes five processes: collecting spam mails, preprocessing the collected spam mails, calculating *IP pollution level*, calculating *Group pollution level*, and finally detecting botnet and zombie PCs.

Step1. Collect Spam Mail

Spam mails are collected in an email spam trap system for a period of time. An email spam trap system, which has been operated by KISA (Korea Internet & Security Agency) since 2008, was the system used to collect, analyze, and retain the evidentiary data of email spam from more than 11,000 virtual email accounts. About 0.5 million spam messages are collected every day. The collected mail was received from the unused email accounts, and most of these can be regarded as bulk email spam.

Step2. Preprocess the Collected Spam Mails

- **Parsing & Regulating mail header/body:** The collected email spam messages are processed by parsing the subject, source IP address, and so on. The source IP address is set as the IP address of the last "*Received From*" record, and embedded URLs are regulated based on the primary domain.
- **Removing White URLs:** If URLs are well-known normal sites, such as portal or internal URLs, they can be deemed as white URLs.
- **Removing White IPs:** Mail server addresses or webmail server addresses applied via SPF (Sender Policy Framework) are removed from the list of IPs to be analyzed.

Step3. Calculate the *IP pollution level*

Spammers can fabricate a great deal of mail information, such as the sender's email address, subjects, transfer route information, sending time and so on. However, we can trust the sender IP address that is stored in the last "*Received From*" record that is written by our spam trap system. This IP address cannot be fabricated by an attacker. We classify spam mails according to sender IP address and make a profile for that IP address, including the number of emails sent, the number of "*Received From*" records in each mail, whether the IP is MTA, and whether the IP has been registered in the RBL. We calculate the *IP pollution level* based on these four factors. The value of each factor is given a real number between 0 and 1. The following are four factors for calculating the *IP pollution level*.

- **IP_POL (RBL) (Registered in RBL or not)**: Zombie PCs that habitually send mass spam mails are likely to be registered on a blacklist. We check whether or not the appropriate IP has already been registered in ten major spam RBLs (Real-time Blackhole List); including kisarbl.or.kr, cbl.abuseat.org, sbl.spamhause.org, xbl.spamhaus.org, list.dsbl.org,

relays.ordb.org, dnsbl.njabl.org, relays.mail-abuse.org, sbl.csma.biz, unconfirmed.dsbl.org, dnsbl.ahbl.org. If the IP address is registered in one or more RBL lists, then IP_POL(RBL) is set to 1.

- **IP_POL (MAIL) (The number of sent mails):** Botnet-infected zombie PCs send many email messages to different recipients in a short period of time. The number of email messages sent from one IP address within a certain period of time is an element that is used to detect zombie PCs. We count the number of emails in h-hours sent from the appropriate IP. If the IP sends more spam mails in a certain period of time, the value of IP_POL (MAIL) goes up.

Table 2. *IP pollution level* by the number of sent mails

For $0 \le i < 10$
If h-hours*i ≤ The number of sent mails < h-hours*(i+1) , *where h-hours is the email collection time*
Then IP_POL(MAIL) = 0.1 * i
If h-hours*10 ≤ The number of sent mails
Then IP_POL(MAIL) = 0.1 * 10

- **IP_POL (MTA) (Normal MTA or not)**: Botnet-infected zombie PCs send email directly, without going through normal mail servers, because each has its own SMTP engine. As a result, the PTR (Pointer DNS Record) information of the mail server cannot be checked, and the domain of the sender's email address does not match the domain where the mail server IP address is included. Thus, we can determine whether email spam has been sent via a botnet by verifying whether the sender's mail server is the one that has been normally registered. We check to determine if the IP address is a normal MTA, and if the MTA has a domain name that is applicable to the appropriate IP. If the IP is a normal MTA, the IP has its PTR record, which matches with the domain of the sender's email address. IP_POL(MTA) is set to 1 in any of the following circumstances.

(1) Case 1 : There is no PTR record for the IP address

(2) Case 2 : PTR record for the IP address ≠ Domain name of sender email address

- **IP_POL (RCV) (The number of "Received From" records):** Many zombie PCs send email spam with their own SMTP engine, which acts as both an MTU (Mail Transfer Unit) and MTA (Mail Transfer Agent) simultaneously. Most spam bots query the MX record to find the receiving mail server, and directly send spam mail to the receiving mail server without relaying it through the local mail server or other relaying server [17]. This is the reason why the mail relaying count sent by a spam bot is usually less that of a normal mail browser. The relay path is checked by using the "Received From" record of the mail header. If the number of the "Received From" record before the recipient's mail server is less than two, the emails may be suspected of being sent by zombie PCs. We calculate the average number of "Received From" records of the emails sent by appropriate IPs. Normal processes of transferring email messages are MUA-MTA-MTA-MUA, so at least two "Received From" records exist. However, many malicious bots have their own SMTP engine, and skip the local MTA. In that case, the "Received From" record for the local MTA is omitted, and

the average number of "Received From" record is less than 2. IP_POL(RCV) is set to 1 in that case.

Based on the profile of each IP address, calculate the pollution level of the IP. The pollution level of an IP is the average of the four factors.

$$IP\_POL = \frac{IP\_POL(RBL) + IP\_POL(MAIL) + IP\_POL(MTA) + IP\_POL(RCV)}{4} \quad (1)$$

Step4. Calculate the *Group pollution level*

Email spam is sent for a range of purposes, including advertising products/services, publicizing pornographic/gambling sites, selling illegal software, and infecting computers with malicious code. To reduce the size of the spam messages, most advertisement spam mail doesn't include all of its contents in the email payload, but includes a URL link that redirects the recipient to an advertising site. It has been reported that 95% of spam mail has a URL that redirects the recipient to an advertising website [18]. On the other hand, attached files are frequently used to propagate malware via internet worms. If identical URLs or attached files are included in a large number of email messages from distributed IP addresses, we suspect that they were sent from zombie PCs. At this point, the criteria for similar email spam should be determined. In this study, the URLs or attached files included in email spam were set as the criteria for determining the spam groups.

We classify IPs with identical URLs or attached files into a group, and use the following three factors for calculating the *Group pollution level*:

- **GR_POL (IP) (The number of IPs in the group):** One of the botnet's most important features is that it is "distributed." When email spam is sent via botnets, the spam mail is sent not from only one IP address but from different distributed IP addresses. The Cutwail botnet, a highly successful spam botnet, had almost 2 million zombie PCs and was the source of almost half of all global spam [15]. In this step, we measure how many IPs are involved in the same spam group.

Table 3. *Group pollution level* by the number of IPs in the group

For $0 \le i < 10$
If h-hours*i ≤ The number of IPs in the group < h-hours* (i+1)
, where h-hours is the email collection time
Then GR_POL(IP) = 0.1 * i
If h-hours*10 ≤ The number of IPs in the group
Then GR_POL(IP) = 0.1 * 10

- **GR_POL (COUNTRY) (Regional distributedness of IPs in the group):** In general, zombie PCs infected by botnets or internet worms have multiple nationalities. For example, if we are to consider a case of 100 IPs in 1 country and a case of 100 IPs in 10 countries, the latter case is much more highly likely to be a botnet or worm group. We check the number of countries in which IPs in the group are located. The higher the number of spam-sending

countries gives the higher the value for GR_POL (COUNTRY). GR_POL(COUNTRY) is set to 0 if spam in a spam campaign is sent from only 1 country, and is set to 0.1 if it is sent from 2 countries, and the value of GR_POL(COUNTRY) is increases when the number of sending countries increases.

- **GR_POL (IP_POL) (Average *IP pollution level* of IPs in the group):** If the hosts in the same group have many characteristics of a zombie PC, this group is likely to be a botnet or internet worm. The *IP pollution level* is used as one factor in calculating the *group pollution level*. Therefore, we calculate the average value of pollution level of the IPs included in the group.

$$GR\_POL(IP\_POL) = \frac{\sum_{i=1}^{i=n} IP\_POL_i}{n} \quad (2)$$

, where IP_POL_i is *IP pollution level* of *i*-th IP in the group

, where n is the number of IPs in the group

Based on these three factors, we calculate the *Group pollution level*, as follows:

$$GR\_POL = \frac{GR\_POL(IP) + GR\_POL(COUNTRY) + GR\_POL(IP\_POL)}{3} \quad (3)$$

Step5. Detect Botnets and Zombie PCs

Someone's private information can be obtained by analyzing the social network he or she has joined, and his or her friends in the social network. Likewise, included spam sender's IP address in a botnet can be used for analyzing the spam group and its members.

In this study, we defined and measured the *IP pollution level* and the g*roup pollution level*. Now, we increase the scope and accuracy of our method for detecting botnets by giving feedback the *IP pollution level* to the *group pollution level*. The *IP pollution level* is used as one factor for calculating the *group pollution level*.

After the feedback between the *IP pollution level* and the *group pollution level* is finished, we detect the suspected botnet groups based on the *group pollution level*. If the *group pollution level* reaches a threshold, we consider the group to be a suspected botnet group. In this study, the threshold for determining a botnet group was set to 0.6 after several simulations and a practical application.

If an appropriate group is judged as a suspected spam botnet group, we consider all IPs belonging to the group to be zombies, regardless of the *IP pollution level* of the individual IP.

4. Experimental Result

Email spam collected via the *email spam trap system* that has more than 11,000 virtual email accounts, was used to verify the efficiency of the proposed methodology. Botnet groups and zombie PCs were detected by applying the proposed methodology to spam mails collected over a period of 72 hours (August 6 ~ August 8, 2011 (KST))

4.1 IP pollution level

In the *email spam trap system*, 1,275,026 emails by 67,856 unique senders IPs were collected over 3 days. The average number of spam mails received from one sender IP in a single day was 19. One sender IP sent as many as 14,678 spam mails in a day. Considering that the *email spam trap system* collects spam mails from a limited number of email accounts, the sender IP actually sent an enormous number of spam mails. **Table 4** shows the statistics of the collected spam mails from the email spam trap system.

Table 4. Statistics of spam mails collected from email spam trap system for 3 days

	Number of Spam Emails	Number of sender IPs	Average Number of Spam Emails per IP	Maximum Number of Spam Emails by one IP
DAY-1	606,381	29,450	20.6	14,678
DAY-2	311,802	18,226	17.1	6,700
DAY-3	411,998	22,338	18.4	10,993
Total	1,330,181	70,014	19.0	14,678

Fig. 2 shows the number of spam emails by time of day. As shown by the graph in **Fig. 2**, there is no regularity in terms of the number of spam messages sent according to time of day.

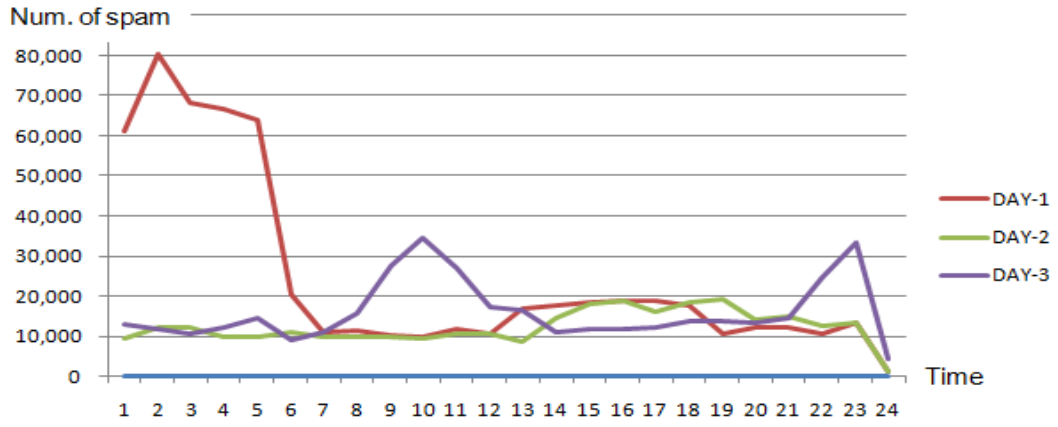


Fig. 2. The amount of Spam against time

It is easy to see that the spam bots are distributed all around the world, and therefore there are many different time zones of origin. However, a sharp increase in the number of spam messages was observed from midnight to 6 o'clock on Day-1. Those spam messages were sent from four Korean IP addresses within a particular C-class IP block (211.119.164.xxx), and the contents were advertisements in Korean language. We assume that spammers in Korea sent a large amount of email spam after midnight, a time at which email administrators are less likely to pay attention. These spam messages had the URLs of "pass.vn" and "tctc52.com" in the email payload. The *IP pollution level* and *group pollution level* calculated by the method proposed in this study were 0.6 and 0.2, respectively, which was quite low, and thus the senders of those spam messages were deemed unlikely to be zombie PCs. By manual

analyzing the header information of the spam messages, it was found that no botnet was being used. It is presumed that dedicated spam senders were used to send massive amounts of spam messages, and the spamming tools were installed on tens of PCs connected via NAT (Network Address Translation).

When we observed the number of spam messages sent by sender IP, most of spam messages were sent by top 20% of IPs. On DAY-1, the top 20% of IPs (5,890 IPs) sent 77.3% of all spam messages (468,492 messages). This implies that spam can be reduced significantly if we concentrate on blocking or disrupting the botnet to which the top spam−sending IPs belong.

The following three factors were measured for each sender IP in order to calculate the *IP pollution level*. By querying ten domestic and overseas RBL sites for spam sender IPs, it was found that 70.9% of IPs (20,879) had already been blacklisted, indicating that the IPs were consistently sending spam messages. By checking whether or not the sender IP was a normal MTA, it was found that 24,696 IPs (83.9%) were abnormal MTAs. The number of IPs with less than two "Received From" records was 16,431 (55.8%). **Table 5** shows the number of IPs that have the value of 1 for IP_POL(RBL), IP_POL(MTA), and IP_POL(RCV) measured by the spam sent proportion per IP.

Table 5. Relationship between number of emails and 3 factors of *IP pollution level* (Result of DAY-1)

Number of emails	IPs		IPs of IP_POL(RBL)=1		IPs of IP_POL(MTA) =1		IPs of IP_POL(RCV) =1	
	Number (T)	%	Number (A)	% (A/T)	Number (B)	% (B/T)	Number (C)	% (C/T)
1~10	18,783	63.8	12,253	65.2	15574	82.9	8372	44.6
11~100	10,300	35.0	8,384	81.4	8784	85.3	7863	76.3
101~1,000	309	1.0	195	63.1	283	91.6	160	51.8
1,001~	58	0.2	47	81.0	55	94.8	36	62.1
Total	29,450	100	20,879	70.9	24,696	83.9	16,431	55.8

Though there were exceptions in some segments, IPs that sent a large amount of spam were more likely to have the value of 1 for IP_POL(RBL), IP_POL(MTA), and IP_POL(RCV). That is, IPs that sent a large amount of spam display similar characteristics to a zombie. Based on these observations, we conclude that many spam messages are sent via zombie PCs, instead of a regular mail browser such as MS Outlook.

The IP pollution level comprises several individual factors. Table 6 shows how many zombies are found by each of these individual factors. It was confirmed that these four factors affect the detection of zombie PCs. In this study, these four factors were considered comprehensively when calculating the IP pollution level to improve detection accuracy.

Table 6. Relationship between number of emails and 3 factors of *IP pollution level*

4 factors of IP pollution level	Zombie	Non-Zombie	Total
# of IP_POL(MAIL) >= 0.5	1,228	501	1,729
# of IP_POL(RBL) = 1	14,057	6,822	20,879
# of IP_POL(MTA) = 1	15,596	9,100	24,696
# of IP_POL(RCV) = 1	11,707	4,724	16,431

Fig. 3 is a Venn diagram that shows what factors are shared, regarding the IPs detected as zombie PCs.

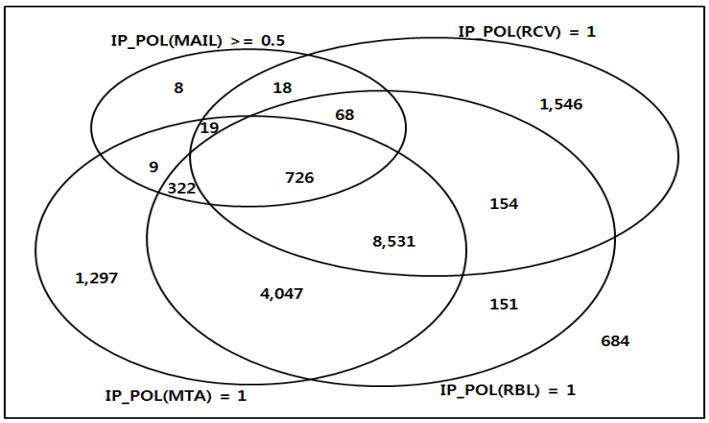
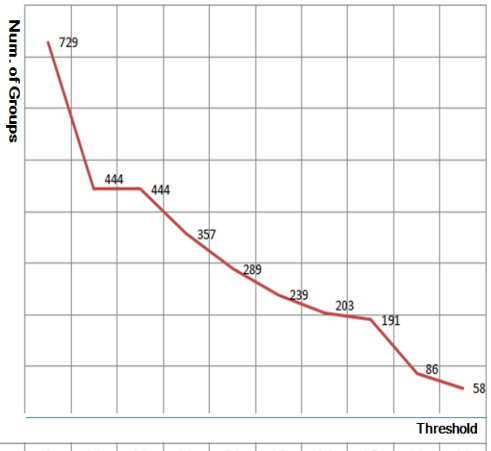


Fig. 3. Venn diagram for 4 factors

4.2 Group Pollution Level

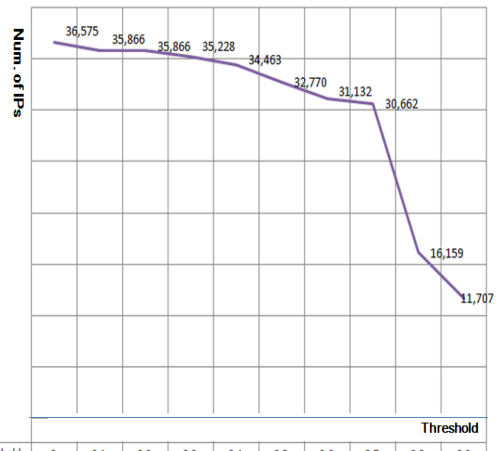
In this study, we used the URLs and attached files as criteria for clustering email spam groups. On DAY-1, 7,017 (23.8%) IPs out of the total of 29,450 senders IPs did not contain any URL or attached file in the email, and were not clustered in the spam group. Emails sent by these IPs contained a particular email address in their email payload for advertisement purposes, or had a particular subject. Therefore, we need to consider using the email subject or the email address in the email payload, in addition to the URL or attached file, as criteria for spam clustering in further work. In total, 22,433 IPs containing a URL or attached file were clustered into 729 groups. Some IPs contained more than two URLs or attached files, and therefore joined more than one group.

The threshold for the *group pollution level* is an important criterion for determining whether the group is a botnet or not. **Fig. 4** and **Fig. 5** show the number of botnets and zombie PCs according to changes of the threshold.



Threshold	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
Num. of Groups	729	444	444	357	289	239	203	191	86	58

Fig. 4. The threshold and number of groups



Threshold	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
Num. of Ips	36,575	35,866	35,866	35,228	34,463	32,770	31,132	30,662	16,159	11,707

Fig. 5. The threshold and number of IPs

If the threshold of the *group pollution level* is set too high, we may miss many botnets and zombie PCs. On the other hand, if the threshold is too low, a high rate of false-positive detection can occur. In this study, the threshold for determining a botnet group was set to 0.6. This value was selected after conducting several simulations and referring to the previous botnet detection experience in the KrCERT/CC.

On DAY-1, 203 groups of the 729 spam groups in total had *group pollution level* of 0.6 or higher. There were 18,283 unique sender IPs belonging to these groups. Some IPs were included in more than two groups, 31,132 sender IPs were duplicated in this way. That is, this study analyzed email spam collected by the spam trap system for one day, and detected 203 botnets, and 18,283 zombie PCs involved in these botnets. The number of email spam messages sent from 18,283 IPs, which are suspected to be the IP addresses of zombie PCs, was 418,840, which amounts to 69.1% of the total spam collected on DAY-1. **Table 7** shows the number of IPs in each group, regional distribution of IPs, and average *IP pollution level* of the top 10 groups with a higher *group pollution level*.

Table 7. Top 10 of *group pollution level*

Rank	Group Name	Number of spam mails	Number of IPs	Number of countries	Avg. IP pollution level	Group pollution level
1	homepharmacydirect.com.ua	12,248	560	37	0.87	0.96
2	instoreinternet.com.ua	11,005	520	37	0.87	0.96
3	celeb-ladymail7.info	1,758	203	20	0.87	0.96
4	canadianrxfish.ru	2,902	174	25	0.85	0.95
5	peniscaresurgy.ru	2,095	142	30	0.85	0.95
6	bigmanpixel.ru	1,546	98	22	0.85	0.95
7	hcgslimauction.ru	2,337	155	27	0.84	0.95
8	cvsdrugstorerx.ru	5,110	338	38	0.84	0.95
9	watchsalesport.ru	1,556	94	21	0.84	0.95
10	internalmedicineweb.com.ua	14,730	685	43	0.84	0.95

The spam group “homepharmacydirect.com.ua,” which recorded the highest *group pollution level*, had 560 PCs from 37 countries and sent 12,248 email spam messages. All spam messages belonging to this group have only one “Received From” record, and a null mailer record. In addition, 673 different sending email addresses and 673 different mail subjects for messages with the same contents were used to avoid filtering. This contextual evidence strongly suggests that a spam bot with an integrated SNMP engine was installed in 560 zombie PCs and these zombie PCs were controlled by the bot master. In addition, not only “homepharmacydirect.com.ua,” but also spam groups with over 0.6 *group pollution level* showed sufficient evidence to be recognized as botnets.

Our proposed system is designed to detect not only botnets but also email internet worms. Email internet worms are propagated through email messages sent by infected PCs located in many different countries. The *group pollution level* of our proposed methodology reflects these characteristics of internet worms and our proposed system can detect internet worms.

Unfortunately, no email worm was detected for the three days of our test. However, a worm propagated by email was detected during a test performed in August 2010 using the proposed methodology. The spam group using an attached file named “report.document.doc.zip” was in fact an internet worm, which was very rapidly propagated all over the world around August 4, 2010 [18]. Even though this group had a relatively low *IP pollution level* of 0.29, the group was identified as a botnet group because the *group pollution level* was as high as 0.76. The worm infected 2,956 PCs in 85 countries, and spread an enormous amount of malicious spam emails that infected other PCs. As such, we can conclude that botnets as well as internet worms spread by email can be detected using the method proposed in this study.

4.3 Detected Botnet And Zombie PCs

In this study, 18,283 zombie PCs from 121 countries were detected by analyzing 606,381 spam messages collected in a spam trap system over one day. 418,840 of spam messages, amounting to 69.1% of all the spam messages, were sent from zombie PCs.

When the zombie PCs were classified by country, the top 10 were ranked IN 2,964 (16.2%), KR 1,620 (8.9%), RU 1,548 (8.5%), VN 1,050 (5.7%), BR 1,003 (5.5%), CN 874 (4.8%), RO 719 (3.9%), ID 693 (3.8%), US 688 (3.8%), and PK 649 (3.5%). This result was very similar with the top 10 spam-relaying countries reported in “Security threat report 2011” released by Sophos [19]. Seven of the top 10 countries in this study were also listed in the report by Sophos.The zombie PCs detected by our proposed system are grouped into two types – ① cases of infection by a malicious bot, ② cases of infection by an internet worm. A host infected by a malicious bot can be controlled by the remote attacker and used continuously for various cyber attacks. On the other hand, a host infected by an internet worm sends a large amount of malicious email to exploit other systems. In this study, the “report.document.doc.zip” group was assumed to be an internet worm and the remaining groups were assumed to be botnet groups. The *IP pollution level* for the “report.document.doc.zip” group members was measured to be significantly lower than that of the botnet groups, this is because the spam mail was not sent by a malicious bot with an SMTP engine, but by a regular email program such as MS Outlook. If someone executes the “report.document.doc.zip” file, it attempts to download two trojan files from different locations.

A spam mail is sent through various methods, such as a botnet, internet worm or dedicated spam sender. **Table 8** summarizes how the *IP pollution level* and *group pollution level*, which are introduced in this paper, are measured in each case.

Table 8. *IP/Group pollution level* of botnet, internet worm, and dedicated spam sender

	Botnet	**Internet worm**	**Dedicated spam sender**
Example group	homepharmacydirect.com.ua	report.document.doc.zip	pass.vn, tctc52.com
IP pollution level (Example group)	High(0.87)	Low (0.29)	Low(0.6)
Group pollution level (Example group)	High(0.96)	High (0.76)	Low(0.2)
Common Characteristics	Using his/her own SMTP engine	Using local mail server	Using local mail server
	Sent from distributed IP blocks	Sent from distributed IP blocks	Sent from limited IP blocks
	Including URL	Including attached file	Including URL

Of course, the above table is not applicable to all cases. For example, botnets can use a local mail server, instead of the internal SMTP engine. However, most spam bots contain an internal SMTP engine in order to send a massive amount of spam quickly and bypass detection by the mail server administrator. On the other hand, an internet worm generally sends malicious emails to infect e-mail users when the users open an attached file via his/her email browser such as MS Outlook. We believe that the concepts of *IP pollution level* and *group pollution level* introduced in this study are useful in analyzing botnet groups, as well as internet worms and dedicated spam senders. As a result, the detailed analysis for classifying the type of sender IP will give a power to response with proper countermeasures against each type of sender. For example, we will take an action to block the botnet C&C (Command & Control) server that controls the zombie PCs when we detect a botnet. We will announce the threat of internet worm when we detect an internet worm propagating fast. Also, we will inform the users immediately if their PCs are infected by bots or internet worms. If we detect a dedicated spam sender, we can arrest him/her cooperating with law enforcement agencies.

5. Conclusions and Future Works

Detecting a botnet is not easy, because botnets are becoming more sophisticated. Botnets are increasingly being used to send massive amounts email spam, as this carries a smaller risk of detection and is more lucrative than other types of attacks.

This study focused on detecting zombie PCs by analyzing email spam collected via an email spam trap system operated by the KISA. In this study, we introduced two new terms: *IP pollution level* and *group pollution level*. We used these measures to detect zombie PCs and botnet groups. Those two concepts were created by analyzing the characteristics of the spam sent by zombie PCs and by looking at the dispersal/collectiveness characteristics of the botnet. These measures are designed to minimize the false-positive rate through a quantitative calculation based on various factors. In addition, we expect that a combination of these two concepts can be utilized to detect internet worms and dedicated spam senders, in addition to botnets.

Through this study, 18,283 zombie PCs in 121 countries were detected from email spam collected in an email spam trap system over a day. The zombie PCs showed sufficient symptoms to determine that they had been infected by malicious code.

Our paper proposes two responses against zombie PCs when they are detected − blocking spam e-mails and removing malicious codes from zombie PCs. First, a list of zombie PCs detected by this study will be registered in KISA-RBL (https://www.kisarbl.or.kr/), which is operated by the KISA, to block spam e-mails. So many mail server administrators in Korea blocks the e-mail from the IPs registered in the list of KISA-RBL. Second, if the zombie PC is found to be located in Korea, the user of the zombie PC will be notified and encouraged to remove the malicious code. The KISA has been operating the system that notified infection to the affected user and encouraging the removal of malicious code together with major ISPs in Korea since 2011.

The proposed system has proved to be useful for detecting botnets, but has some limitations that will be addressed in future study to increase detection accuracy. First, email spam messages without a URL or attached file are not clustered, which means that they are excluded from the analysis. Therefore, the group selection criteria will be diversified to minimize the number of IPs excluded from clustering. Currently, only the presence of a URL or an attached file is used, but the sender email address, email subject or email address in the

payload will be added. Second, it is difficult to verify whether the detected zombie PCs are actually zombie PCs. We are going to observe the changes in the zombie PC list infected by botnet by time, to verify that real zombie PCs are detected. It cannot be regarded as normal e-mail sending behavior, if many PCs distributed among many places send the same spams continuously for a certain period of time. Therefore, the similarity of the same spam campaign group will be measured by time, to prove that the group belongs to a botnet group, and the IPs belonging to that group have a high probability of being a zombie PC.

References

[1] M. Feily, A. Shahrestani and S. Ramadass, “A Survey of Botnet and Botnet detection,” in *Proc. of in Third International Conference on Emerging Security Information, Systems and Technologies*, 2009. Article (CrossRef Link)

[2] Symantec, http://www.symantec.com/

[3] M. Bailey, E. Cooke, F. Jahnian, Y. Xu, and M. Karir, "A survey of botnet technology and defenses," *Cyber-security Applications and Technology Conference for Homeland Security*, pp.299–304, 2009. Article (CrossRef Link)

[4] The Register, "DDoS attacks fall as crackers turn to spam," Article (CrossRef Link)

[5] MessageLabs, http://www.messagelabs.com/

[6] Zhu, Z. Lu, G., Chen, Y., Fu, Z.J., Roberts, P. and Han, K., “Botnet research survey,” *Computer Software and Applications*, 2008. Article (CrossRef Link)

[7] N.C. Paxton, G.J. Ahn, R. Kelly, K. Pearson and B.T. Chu, “Collecting and Analyzing Bots in a Systematic Honeynet-based Testbed Environment,” in *Proc. of the 11th Colloquium for Information Systems Security Education*, 2007. Article (CrossRef Link)

[8] Zhuge, J. and Holz, T. and Han, X. and Guo, J. and Zou, W., “Characterizing the irc-based botnet phenomenon,” *Peking University & University of Mannheim Technical Report*, 2007. Article (CrossRef Link)

[9] G. Gu, R. Perdisci, Z. Zhang and W. Lee, “BotMiner: clustering analysis of network traffic for protocol-and structure-independent botnet detection,” in *Proc. of the 17th conference on Security symposium*, pp.139-154, 2008. Article (CrossRef Link)

[10] Hyunsang Choi, Hanwoo Lee, Heejo Lee and Hyogon Kim, “Botnet detection by monitoring group activities in DNS traffic,” IEEE International Conference Computer and Information Technology(CIT), 2007. Article (CrossRef Link)

[11] Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten and I. Osipkov, "Spamming Botnets: Signatures and characteristics," *SIGCOMM'08*, Aug.2008.

[12] A. Ranachandran, N. Feamster and S. Vempala, "Filtering spam with behavioral blacklisting," *CCS'07*, 2007.

[13] J.P. John, A. Moshchuk, S.D. Gribble and A. Krishnamurthy, "Studying spamming botnets using botlab," *USENIX*, 2009.

[14] L. Zhuang, J. Dunagan, D.R. Simon, H.J. Wang and J.D. Tygar, "Characterizing botnets from email spam records," in *Proc. of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, 2008.

[15] P. Graham, "Different methods of stopping spam," http://www.windowsecurity.com/, 2003

[16] MP Collins, TJ Shimeall, S Faber, J Janies, R Weaver and MD Shon, "Using uncleanliness to predict future botnet addresses," in *Proc. of the 7th ACM SIGCOMM conference on Internet measurement*, 2007.

[17] K.S. Han, Y.H. Shin and E.G. Im, “A study of spam-spread malware analysis and countermeasure framework,” in *Journal of Security Engineering*, 2010.

[18] Hyun Cheol Jeong, Huy Kang Kim, Sangjin Lee, Joo Hyung Oh, “Study for tracing zombie pcs and botnet using an email spam trap,” in *Journal of the Korea Institute of Information Security and Cryptology*, vol.21, no.3, pp.3-188, Jun.2011.

[19] Sophos, “Security threat report 2011,” 2011.

HyunCheol Jeong received his B.S. in Computer & Statistics from Seoul City University, Seoul, Korea in 1989, and his M.S. in Computer Science from KwangWoon University, Seoul, Korea in 1999. He is working for KISA since 1996. He was a senior technical member for KrCERT/CC, and now he is a director for Security R&D Team in KISA(Korea Internet & Security Agency).

Huy Kang Kim received his B.S. in Industrial Management, M.S. and Ph.D. in Industrial Engineering from KAIST(Korea Advanced Institute of Science and Technology) in 1998, 2000 and 2009, respectively. He was a technical director for security division in NCSoft and he is now an assistant professor in Graduate school of Information Security, Korea University.

Sangjin Lee received B.S., M.S. and Ph.D. in Mathematics from Korea University in 1987, 1998 and 1994, respectively. He was a senior researcher in ETRI(Electronics and Telecommunications Research Institute) and he is now a professor in Graduate school of Information Security, Korea University.

Eunjin Kim received her B.S., M.S. and Ph.D degrees in Management from Korea Advanced Institute of Science and Technology (KAIST). She is an assistant professor at Kyonggi University. Her current research interests include economic analysis of digital content, information systems and effects of the digital divide.