

National Spam Threat Management:

With Case Studies of Spam Incidents Analysis

Hyukjoon Kim, Spam Response Team at Korea Information Security Agency

joonkim@kisa.or.kr

Abstract

Spam in today's globally interconnected world has gone far beyond the nuisance in end users' mailboxes. It consumes significant network bandwidth, server resources, and management man power, raising many other complex problems. It is increasingly used as an infection vector for malware and social engineering attacks. This paper introduces the national spam threat management system operated by Korea Information Security Agency along with the current achievements gained by the system. It comprises three subsystems: KISARBL, Email Spam Trap, and APRBL. KISARBL (Korea Information Security Agency Real time Block List) generates spam IP blocking lists and manages the reputation of the mail sender. Spam Trap actively collects and analyzes .4 million spam messages every day. Lastly APRBL, a cross-border spam information sharing system in the Asia Pacific region, facilitates the cross-border spam information exchange process. Once the threat management system analyzes the threat type and level, it issues an alert through the alert network maintained by the system. The process includes distribution of a confirmed list of spam IP in the form of a real-time blocking list. Those lists are used by various organizations in Korea, such as Korea Telecom, and by other major portals to reduce the number of spam messages within and outside of Korea.

After describing the systems' roles and capabilities, recent cases of managing two major spam incidents will be presented. The first case illustrates the process of managing a domestic spammer who used 15,809 vulnerable mail servers around world to send billions of spam messages to Korean networks, giving pointers to Korean spammers' current status and recent developments. The second case is about the notorious Storm worm identified by the systems as having compromised more than 2.2 million hosts around world, including a significant number of Korean ones, illustrating the trend of Korean networks being abused as the infrastructure for malevolent operations affecting the world.

1 Introduction

Korea has made rapid development in information and telecommunication technology over the last 40 years. In its infancy in the 1960s, it had only 0.36% telephone penetration rate, which was lower than 10% of the world average. However, in 2002, Korea became a leader in world broadband internet access. But like other developing countries, Korea did not pay enough attention to building an IT security infrastructure that corresponded to its superb high speed networks.

Advanced countries had relatively enough time to develop consensus among various social entities in the public and private sectors about the needs for implementing security in their information and telecommunication infrastructure. Countries like Korea did not have enough time for that model, so they need a steering body to facilitate building security in their information and telecommunication infrastructures.

To answer this need, KISA (Korea Information Security Agency) was created in 1997 to develop a secure information and telecommunication infrastructure in the private sector. The KISA Spam

Response Team (KSRT) is responsible for building a secure email infrastructure in Korea. KSRT's efforts to control spam problems have come together in the National Spam Threat Management System. The system consists of four phases: Threat Modeling, Data Collection, Threat Analysis, and Threat Management. The goal of having the system is to break away from a continuous wheel of response without improvement. It measures the threat level and the performance of the spam response process. The three subsystems, KISARBL, Email Spam Trap, and APRBL, support the collection, analysis, and escalation processes of the management system. KISARBL is not limited by its nomenclature. It collects secondary spam data from major Korean email service providers, processes the data with respect to its source IP and the filtering rules, and then hands it to the threat management system for further analysis.

Email Spam Trap is a system that started its service in early 2008. It is an active spam and related information gathering system with hundreds of mx domains and more individual accounts that lure spammers to send spam to the trap account. The Storm analysis presented

at the end of this paper was made available through this system, which allowed us to collect original spam messages sent by Storm agent, information about the operating system that was used to harbor the Storm malware, and the email agent's signature. These components identified both the high and low profile activity of Storm's mass-mailing operation.

APRBL, the latest addition to the system, copes with the growing need for timely cross-border spam responses. As more and more spammers use compromised hosts as their attack and binary distribution points, traditional ways of handling such problems produce no results. Once the message gets to the other party, there may be no trace of spammers in the IP or domain information. APRBL provides a means of automated spam information exchange among signatory countries who signed the Seoul-Melbourne MoU. Later on, this system could accommodate more parties who can gain benefits and contribute to the members of the system.

The data collected by the systems is granulized and then stored in the main processing system. The threat management system analyzes and classifies it based on the level of threat. The system uses the classification to determine the corresponding escalation process. The details of the process are described in section 4.

The case studies depicting the results of the National Spam Threat Management System were carefully chosen from the many spam incidents to which KSRT responded. Because the current threats imposed by spammers include compromising hosts, building attack networks, sending spam, launching DDoS attacks, and more, defenders should break the boundaries to handle the ever growing adversaries. The Storm case demonstrates that the capability of the system is not limited by traditional boundaries. It includes identification of compromised botnet IPs, fast-flux networks, and polymorphic binaries. Moreover, the trend of using Korean networks as their fast-flux and binary repository infrastructure rather than a spam-sending agent are also recognized. The second case is recent case of a domestic spammer whose characteristics are closer to those of advanced spammers on the other hemisphere. The case illustrates how the domestic spammer used thousands of vulnerable mail servers around world, and, more significantly, it shows the characteristics of having intermediary pseudo-botnet command and control structure, which were first observed in Korea.

2 Threat Modeling

The first and foremost phase of the National Spam Threat Management System is Threat Modeling. Spam

is a bigger threat than it appears to be. On the surface, it causes minor annoyance to end users who did not expect to receive such email, but underneath the simple nuisance, there are shadows of organized crime large and small spreading worms, compromising hosts, and clogging network connections either intentionally or unintentionally. To model such complex threat effectively, the scope cannot be limited to traditional spammers because spammers today are able to launch host-based attacks as well as network-based attacks using highly sophisticated botnet operations. Rather, in KSRT's jurisdictional point of view, the attacker is modeled to either domestic spammers or overseas ones in terms of their target recipients. Overseas spammers are modeled as fully fledged organized crime groups with the financial and technological capability to compromise millions of hosts, launch various network-based attacks such as DDoS and spam, and operate botnet and fast-fluxing networks to evade countermeasures. Moreover, as shown from the emerging pump-and-dump stock scam, the spammer is not working for the payer but is creating its own market.

Domestic spammers are modeled as copycats of overseas spammers. Although they are not highly organized and are not financially independent, there are many signs of them adopting advanced skills from the internet. As they impose direct threats to Korean email services and internet users, higher level of severities are assigned.

In the modeling process, assets that need to be protected are defined in two groups. One includes assets that are directly wasted, such as network bandwidth, mail servers for handling flooding spam messages, and man power to deal with various problems caused by them. The other group includes assets that are not directly wasted but are considered to be more significant, such as trust in email systems and control, which are being lost because of insidious spammers.

3 Data Collection

The objective of the data collection process is to have a reasonable number of sensors to collect statistically representative spam information in the form of either a digested summary of spam or full messages. The former type of data is collected from major Korean email service providers who voluntarily provide spam digests that are filtered at their SMTP gateway and are not delivered to the intended destination. There are 20 million lines of data gathered on a daily basis in the following format: time stamp, source IP, sensor name, spam type, sender, and subject of the filtered spam messages. The last two entries are optional because the

information may not be available depending on the way it is filtered. Although it is believed to cover more than 80% of domestic email traffic, there are shortcomings of the data because it only gathers a digest of the original message.

To compensate for the limitation of the data from KISARBL, KISA has deployed Email Spam Trap to actively collect original data as well as the invaluable data from transmission of the message. It has more than 100 mx domains, and the trap accepts any messages arrived at the gateway. It collects email messages destined for the account, openrelay attempts, and even the one who tries to carry out joejobs in the application layer. The system also performs passive IP stack fingerprinting to identify the operation system of the spamming host. Since most of the compromised spam agents reside in MS Windows systems, the operating system information can be used to identify types of spam agent.

The trap system can see more than digests of spam messages, so it also collects URL information in the spam messages and then recursively collects URLs that are linked to the initial one. It is necessary to follow the URL link since many spam filtering software programs use the URL in the spam message to filter out the spam messages, and spammers use free URL redirection services to avoid the filtering. The number of spam messages collected through the system is on the rise since the initial operation in September 2007; currently, the system receives .4 million spam messages.

The systems described above are mainly designed to collect domestic data; thus, their scope is limited to internal and inbound spam messages. If it is possible to collect outbound spam messages, the information will help to identify compromised hosts within the networks. So far, such ideas are honored among many countries, and data exchanges were made either by phone or by written requests. There were neither agreements nor procedures for timely processing of the data exchange. Delays were also caused by geographical distances and lack of trust among parties involved in the data exchange. Moreover, recently spammers have tended to move fast from one domain or IP to another, and the delays give them enough time to cleanse evidence that may expose their activity. To deal with such problems effectively, KISA initially suggested APRBL to the members of the Seoul-Melbourne Multilateral MoU in 2006 to facilitate the data exchange via a standardized process defining protocols for automated exchange and the format of the data. KISA began developing the system in 2007, and the system is currently in the alpha test phase. It is expected to be launched at the end of 2008. The system

will eventually serve as repository of compromised host IP information along with enough evidential information to convince other parties to take necessary measures. It will also enforce timely response to cross-border spam by tracking histories of member activities. When the system is up and running, KISA will correlate the information it gathers with information from other systems and actively use it all to identify and take necessary countermeasures against compromised resources in Korean networks. Data collection is an essential phase because it lays the foundation for the threat analysis and management phases.

4 Threat Analysis

Data collected from the previous phase is deposited into central database. Each analysis is defined as a process or a series of processes of correlating data gathered from the described data sources. While the threats imposed by domestic spammers are lower in technical and financial aptitude, they have more severe impacts on domestic users, networks, and computer resources. Korean domestic spammers are thought to be in final stage of Phase II.

Phase I refers to an early stage of spammers, which is often seen in developing countries. There are little or no regulatory measures, and spamming is not thought to be a serious offense. Spammers usually work individually with their own resources, such as a PC and a low-speed connection. They are not professional, have regular jobs, and send less serious spam. Their techniques for sending spam are simple and symmetric in bandwidth because they are bound by the bandwidth they have.

In Phase II, spammers are starting to organize and specialize in terms of their separate roles as spam senders, content providers who sit between mail senders and advertisers, and the advertisers who fund the whole operation. Regulatory bodies are aware of severe side effects caused by spammers and are trying to raise the regulatory bars. Less serious spammers decide not to take the risk to be a 'spammer,' but serious ones become so-called professional full-time spammers. Underground social networks start to build between the entities described above. In this phase, spammers gain better technical skills by mimicking the more advanced skills through the internet to evade the regulatory measures. They start to use overseas domain/hosting service providers and/or send spam messages through resources that do not legally belong to them. In this phase, spammers send spam behind open relays and open proxies to hide their location, but, as in Phase I, their bandwidth stays symmetric.

In Phase III, there is a fine line between spammers who are thriving and those who are not. The ones with high technical skills tend to make much more profit than others. They have enough money to develop highly sophisticated malware and build global networks to evade investigators and regulators. They eventually create a market as seen from the pump-and-dump scam. What is significant in this phase is that spammers are not bound by their bandwidth anymore. They can easily amplify the number of spam messages in one-to-many relationships by using botnets. In this phase, spammers can easily clog SMTP transactions; it is reported that Storm once created up to 90% of the transactions. Moreover, they also have ability to launch DDoS attacks, phishing attacks, and many other types of attacks they could imagine.

Defining the phase is important in threat analysis since there are quite a few differences in countermeasure strategy from one phase to the next. For the threat imposed by foreign spammers, KISA has little control but deals with problems such as finding and quarantining infected computers and exchanging related information with other foreign authorities. But the activity of domestic spammers is still within the jurisdictional boundaries and has a direct impact on the Korean networks and end users. Threat analysis depends on quite a bit of information gathered from the data.

Analysis techniques include magnitude analysis, frequency analysis, duration analysis, spam agent analysis, and operation system analysis. Most of those analysis techniques are self-explanatory and used in many other organizations. However, the spam agent signature detection is solely developed by KISA, and it is worth introducing in this paper. The idea of a signature detection engine came from the fact that there are no strict standards in composing email headers. Because each email client composes its mail header uniquely, we need to divide variant and invariant components in mail headers and take signatures of how those invariants are composed. The idea worked well and is deployed in the Email Spam Trap, where we can get original spam messages intact. If a spammer uses a unique agent like a botnet, it would be very useful to identify the types of agent used to send spam. If we correlate the information with the passive operating system detection technique, the results are more than expected and will be presented in the case study.

At the very top of the threat analysis, we correlate secondary information from the described analysis techniques. The top-level threat analysis includes reputation analysis, domestic spam activity profiling, cross-border threat analysis, and related threat analysis.

Once the threat types and levels are identified, the process moves to the Threat Management System.

5 Threat Management

The Threat Management system controls overall threat level, escalation path, and alert network management. After all, these steps boil down to threat identification and the mitigation process. Identification of threats uses the previously analyzed values to determine the severity and type of them. It uses jurisdictional factor, magnitude, and type of attack. If it is considered to be a well-known attack, then the level goes down, but if it is novel and not known to public, then the level goes up. Depending on the level and type, the escalation path to mitigate the threats varies widely. The mitigation process is divided into generating a real-time block list, initiating a domestic and international alert network, and launching an investigation if it is jurisdictionally enforceable.

Real-time block list generation is the basic level of the mitigation process. It aggregates spam asset information from various sources and then generates the list that follows a time decay function with a two-tiered memory structure. The active set on the list is maintained at a fixed size, reflecting currently active spam IPs. The size of passive set on the list is much larger than the active one. If certain IP is detected and hibernates, it won't be in the active list. However, if it shows up again, the stay time becomes exponential. This way, the list can stay a manageable size and reflect both previous and new resources used in spamming operations. Outside users can only access the active set on the list on an hourly basis either by using rsync to download the bulk list or by throwing a direct query to spamlist.or.kr. Currently, thousands of organizations, including Korea Telecom and most of major Korean email service providers, use the list in the way it is convenient to them to reduce the number of spam messages from and to the SMTP gateway.

Although applying the real-time block list helps relieve organizations from the burden of processing unnecessary spam mail filtering by terminating the connection before it sends data, it often cause problems with false positives. As more spammers send spam mail through otherwise benign IPs, such as vulnerable SMTP servers or compromised PCs, the rate of false positives and resulting complaints are increasing. To reduce such side effects, KISA maintains a voluntarily registered list of mail servers.

WHITEDOMAIN is a subsystem of the KISARBL through which organizations can register their sending address by publishing SPF (Sender Policy Framework) records. Because their records are automatically

queried on a daily basis, registrants do not need to worry about sending environment changes but can update their own SPF record. KISARBL compares its block list with the one queried on IPs each day then alerts the domain administrators about their IPs being listed in the block list before they are actually included. This strategy was successful in regaining domestic users' trust in the email system. However, there are still problems with accommodating international mail domains in the list.

Tracking domestic spammers and prosecuting them for their wrongdoings is also considered a major response strategy. Since 2006, we have launched more than twenty investigations of domestic spammers who were either prosecuted or penalized. In 2006, a spammer who distributed open proxy malware that opened port 50050 and 50033 for SOCKS and HTTP proxy disturbed Korea, infecting thousands of personal computers via an anonymous open proxy server. KISA has launched investigations with law enforcement authorities, and the person who was responsible for the wrongdoings was prosecuted for sending spam messages and compromising computers. In 2007, a man who was responsible for running a spam contents server connecting the advertiser and the spam sender was also investigated. He actually revealed a lot of useful information about spammers. Many of them were penalized for sending spam messages. Currently, we are tracking a spammer who abused more than 15 thousand mail servers from 140 countries. This case will be presented as a case study later in this paper.

6 Conclusion

In this paper, we showed the process of a nation-wide spam threat management system in Korea. The internet was not designed with security in mind. It was a research network built upon the implicit trust between members. As it grew into a commercial network, the trust model showed many flaws. For example, the original SMTP had no built-in authentication features. While there are many people working very hard to make the internet secure, another group of people tries to exploit the inherited vulnerabilities. Email spam seems a small problem at a glance, but a closer look reveals more than a person can imagine. On one side, the spammers just send spam emails but on the other side, they compromise innocuous computers, launching DDoS and social engineering attacks. Although it poses many different forms of threats, it can be managed by implementing a nation-wide spam threat management system. It does not necessarily replace the private sectors' work in areas such as developing anti-spam products and providing customized filtering services. Its role is to keep the national security baseline and

facilitate the security process until it reaches certain degrees. We believe such work will eventually benefit internet users worldwide.

Case Study

1 Storm Worm Analysis

1.1 Introduction

This case study analyzes the case of the Storm worm that flooded internet with spam and DDoS attack traffic in 2007. All of the data used here was solely collected and analyzed by KISA's Spam Threat Management System. This analysis is based on the data collected from October 2007 to January 2008.

While Storm was on high-profile activity, it tried to widen its P2P network using email as an infection vector. In this period, Storm used social engineering techniques to trick users who received the spam mail into clicking on the embedded link which caused the Storm bootstrap agent to download and install. This analysis was performed to verify claims that Korean networks were used as an infrastructure for malicious activity because of their reliable high-speed internet connections. Since the active response against the outbound spam traffic at the international gateway, the overall amount of spam from Korea has shown a decreasing tendency. This does not necessarily mean the number of botnet-infected hosts in Korea are decreasing. Although the SMTP traffic from botnets is decreasing, they can launch DDoS attacks and be used as attack infrastructures such as fast-flux DNS servers and malware repositories.

Because the Storm worm's activity can be easily identified during the high-profile period, several emails sent by the Storm worm were collected by Email Spam Trap. A sample message is shown in Figure 1.

```
MAIL FROM: ibarrarubiojuan@genisystems.ca
ORG RCPT TO: fullbackgenitrfies@casillas.co.kr
RCPT TO: fullbackgenitrfies@casillas.co.kr
X-SPAM-TYPE: SPAM
X-HELO: helo 244-240-231-201.fibertel.com.ar
X-RECEIVED-IP: 201.231.240.244
Received: from 201.231.240.244(201.231.240.244)
    at Tue, 25 Dec 2007 12:48:19 +0900
    by mail.com with ESMTIP CrediShield
X-MAIL-FROM: ibarrarubiojuan@genisystems.ca
Received: from ynd ([177.76.169.234])
    by 244-240-231-201.fibertel.com.ar (8.13.3/8.13.3) with SMTD id 18P3uoP8007560;
    Tue, 25 Dec 2007 00:56:50 -0300
Message-ID: <47707E5B.2020102@genisystems.ca>
Date: Tue, 25 Dec 2007 00:51:55 -0300
From: <ibarrarubiojuan@genisystems.ca>
User-Agent: Thunderbird 2.0.0.6 (Windows/20070728)
MIME-Version: 1.0
To: fullbackgenitrfies@casillas.co.kr
Subject: Find Some Christmas Tail
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

Hey nan,

I know you hate these kind of emails but this one is different. Forget
all the stress for two min and feast your eyes on these. :-))
http://merrychristmasdude.com/
```

Figure 1 Trapped Email from the Storm Worm

From the sample email, we have generated the email agent's signature. By painstakingly verifying the signatures with its well-known subject in high profile activity and the URL in the spam messages, we have confirmed that only two signatures are there for the worm. After isolating the signatures and corresponding subjects, we compared the subject with the data collected by KISARBL. Following the mythologies, we have identified 2 million Storm-infected IPs from 200 countries. Moreover, by launching an investigation on its malware repository and fast-flux network, we also have identified 9,000 malware repository IPs and 2,000 fast-flux IPs from hundreds of countries. It is also shown that Korea is now used by attacks as their infrastructures rather than spam shooters.

1.2 Evidence collection

The Storm worm mail sample and SMTP traffic information was collected by Email Spam Trap, and the majority of IP information was collected by KISARBL. These act as a national spam sensor network. The fast-flux and malware repository domain information is collected by DNS querying of the URL in the spam messages.

1.3 Evidence Analysis

When Storm sends email to spread malware, the email contains a malware repository URL within the body. By looking at the URL, it can be easily identified that the mail is from the worm. In December 2007, the worm used merrychristmasdude.com as a pointer to the repository. Among those spam mails trapped in the Email Spam Trap System, we collected the message that contained the URL then generated spam agent signatures from the messages. We used hundreds of messages to generate the signatures, and only two unique ones out of all the messages were produced. With the signature handy, we extracted a total of 5,987 emails. In the body of those emails, there are linked URLs that lead to known name and IP of the Storm repositories (Figure 2).

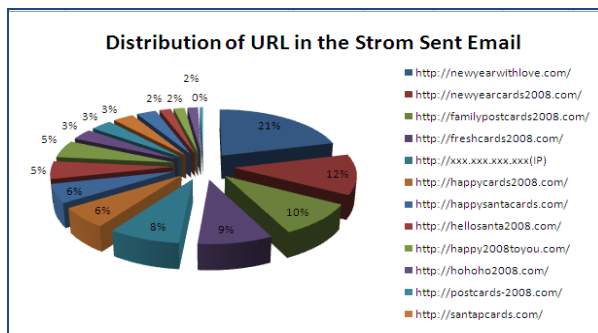


Figure 2 URL in the Storm sent email

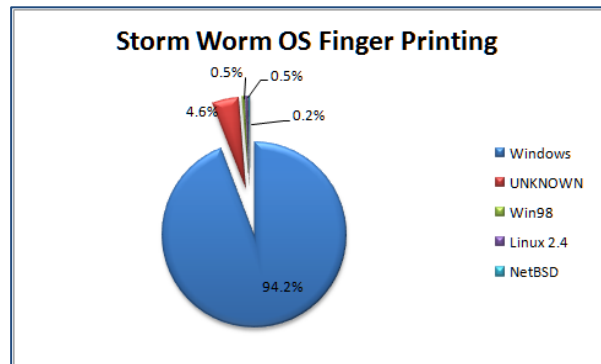


Figure 3 The Storm OS Fingerprinting

Also, more than 94.7% of the network traffic initiated by the Storm worm was identified as Windows operating systems.

1.4 Further Analysis

The goal of our analysis is to figure out whether Korean networks are used as spammers' network infrastructures. To analyze the location of fast-flux DNS servers, we threw 76,213 DNS queries. Results show that Storm uses 2,110 IP addresses from 61 countries with name server switching periods of 20 minute on average. And 9,383 malware repository IP addresses from 101 countries are also identified. The results from the analysis show that Korea ranked 5th in spamming IP count (3.77%) and 2nd both for number of the fast-flux DNS servers and malware repositories.

1.5 Conclusions

The analysis that was made available by these systems verified that the Korean networks are still highly vulnerable to being abused by outside attackers. As shown by the analysis, spammers have many faces. Attackers are now aggregating their skills for financial gains while defenders are split in term of their specialties. To deal with such converged threat, defenders in each field should think about how to cooperate effectively.

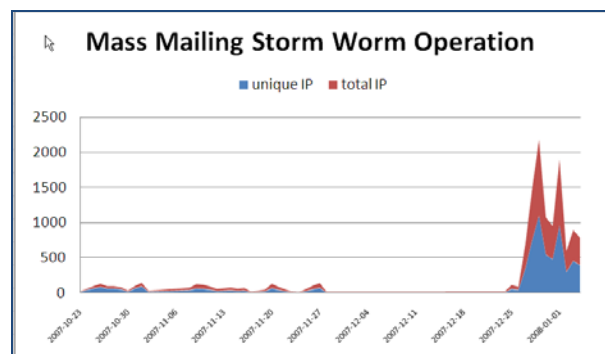


Figure 4 Low and High Profile Operation

2 Forging MAIL FROM Relay Analysis

2.1 Introduction

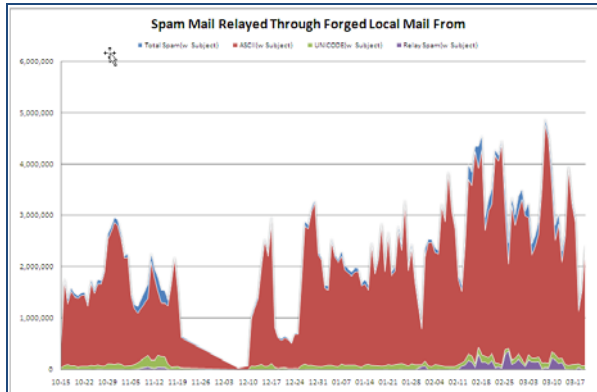


Figure 5 Forging MAIL FROM Relay Spam

Korean spammers are believed to be in the second phase of the development, and the operation of botnets to amplify the number of spam mails sent by their agents is thought to be only from advanced spammers on the other hemisphere. Forging MAIL FROM Relay Spam reflects the current state of Korean spammers and how they will evolve. Although they are now staying in between phases II and III, they will eventually move to the next stage if necessary counter measures are not taken.

2.2 Alert form Spam Threat Management System

In March 2008, KISA's Spam Threat Management System issued an alert for Korean spam surge in a short period time from a wide range of IP address spaces. In Figure 5, the top blue color represents total spam with subject collected in KISARBL; the red color is for email encoded in ASCII (English spam); the green color is for UNICODE spam, including Korean spam; and last, the purple color shows the abrupt increase of the same type of Korean spam messages from hundreds of different countries. KSRT (KISA Spam Response Team) launched an investigation on that matter immediately.

2.3 Initial Analysis

The amount of spam the spammer sent reaches up to 80% of total Unicode spam messages collected in KISARBL. It was a surprising fact since such dominant domestic players haven't been identified. At first, the attacker seemed to be running large globally distributed botnets, but it turns out that the spammer exploited the vulnerability of SMTP servers that selectively relayed email as long as the email address of the MAIL FROM commands was active and existed in the domain. This fact was identified since most of the spam messages have forged MAIL FROM values with seemingly

existing accounts such as abuse, admin, contact, help, info, postmaster, and root. To verify that hypothesis, a hotmail email account was set up, and test mails were sent. We used the Expect script language to write an automated interactive check script. Among those mail servers, 5,046 mail servers were confirmed as being vulnerable to such attacks as shown in Figure 6.

2.4 Evidence Collection for Digital Investigation

Among those 15,062 unique IP addresses that were used for sending the spam email, 5,046 identified vulnerable mail servers were initially selected for on-site examination. It turns out that 35 mail servers were located in Korea, and the administrators were willing to help the investigation. By analyzing the network traffic to the server with the relaying requests, it turned out that all of the 38 IP addresses were located in Korea. We are currently working to determine who is behind the IP addresses that were used as intermediary stepping stones. Once that is identified, the case will be turned over to a corresponding law enforcement agent.

2.5 Vulnerable Mail Servers

By profiling the vulnerable mail servers, it was revealed that most of the servers are installed on a MS Windows GUI configuration environment. Because MDAemon and Mercury mail servers were the majority, we downloaded those two mail servers and identified that the default configuration allows outside users who claim to be local users to relay mail to anywhere they want.

2.6 Conclusion

Although such vulnerabilities were repeated over and over during that period of time, they are still around us. From this incident, we have learned the need for continuous threat management since such basic vulnerabilities are repeating and the level of technical aptitude of domestic spammers is growing. This incident is still under investigation, and further contact for this matter will be mainly handled by the Spam Response Team at KISA.

보낸 사람	제목	날짜
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25
RELAY TESTER	KSRT Openrelay Test Mail	2008-03-25

Figure 6 Confirmed Relay Servers