스팸 메일 차단을 위한 RBL개념의 확장에 관한 연구

김종민* · 김형근** · 김봉기***

Studying on Expansion of Realtime Blocking List Conception for Spam E-mail Filtering

Jong-Min Kim* · Hion-Gun Kim** · Bong-Gi Kim***

요 약

본 논문에서는 스팸 차단을 위해서 사용되고 있는 RBL의 기능에 더하여, 최근 유행하는 스팸 형태에 효과적으로 대응할 수 있는 방법으로 메일원문에 포함된 URL을 추출하여 RBL에 적용하여 확장할 수 있는 방법을 제안한다. 최근 스팸 메일발송에 많이 사용되고 있는 봇넷은 이메일 스팸에서 메일 발송 주소분포로 해결할 수 없는 문제점을 가지고 있다. 일반적으로 이러한 스팸 메일은 각 개인의 감염된 좀비 PC에서 발송되므로, 발송 주소 자체가 RBL에서 사용하기에 효율성이 떨어지고 무의미 하다. 따라서 봇넷에 의해 발송되는 스팸 메일을 효과적으로 차단하기 위한 방법으로써, 스팸 메일의 원문에 포함된 URL을 분석하고, 사용자를 유인하는 URL 사이트에 대한 분포자료를 바탕으로 효과적으로 차단률을 향상 시킬 수 있는 방법을 제안한다. 본 논문에서는 봇넷에서의 스팸메일 발송 메커니즘과, 이러한 유형의 스팸메일을 판단하기 위하여 사용할 수 있는 방법을 제안하고 분석 가능한 스팸메일의 수집을 위하여 이메일 스팸 트랩 시스템을 구성하여 실험한다. 일정한 실험 기간 동안 수신된 스팸메일의 분석을 통하여 스팸메일에 포함된 URL을 이용한 확장된 RBL기법이 스팸메일의 검출 분포를 높이는데 효과적임을 보여준다.은 요약문 입니다.

ABSTRACT

In addition to RBL function, which is used to applying for spam e-mail filtering, as an effective way to deal with the recently widespread spam types, this paper proposes how to extract URL that was comprised in the original e-mail, apply it to RBL, and expand it. The BotNet, which is used to using for sending spam mails these days, has a problem that it is not able to solve with the distributed addresses of sent mails in spam e-mails. In general, as these spam e-mails are sent from the infected Zombi PC of individual user, the sent address itself is not efficient and is meaningless to use in RBL. As an effective way to filter spam e-mail sent by BotNet, this paper analyzes URLs that contained in the original spam e-mail and proposes how to effectively improve filter rate, based on the distribution data of URL site tempting users. This paper proposes the sending mechanism of spam e-mails from BotNet and the methods to realize those types of spam e-mails. In order to gather analyzable spam e-mails, this paper also carries out an experiment by configuring trap system of spam e-mail. By analyzing spam e-mails, which have been received during the certain period of experiment, this paper shows that the expanded RBL method, using URLs that contained in spam e-mails, is effective way to improve the filter distribution of spam e-mail. Key words: Spam, RBL(Real-Time Blocking List), Spam URL, BotNet, Trap system of spam e-mail, Zombi PC.

키워드

스팸, RBL(Real-Time Blocking List), 스팸URL, 봇넷, 이메일 스팸 트랩 시스템, 좀비PC

* (주)모비젠 기술연구소 선임연구원
** (주)모비젠 기술연구소 연구소장 재임
*** 현재 진주산업대학교 컴퓨터공학부 부교수

접수일자 2008. 05. 23

Ⅰ. 서 론

이메일 스팸 차단 방법에 대해서 논의 된지도 몇 년이 지났다. 정보기술의 기술적 패턴이나 라이프 패턴은 점점 진화하고 있으며, 스팸발송의 유형과 형태 또한 계속적으로 변화한다. 스팸은 기술적 문제라기보다는 인간 행동의 변화를 그대로 반영하고 있으며 사회, 경제적인 문제와 밀접한 관계가 있다. 스패머는 여러 다양한 이유가 있겠지만, 주로 금전적인 취득을 위한 목적으로 스팸메일을 발송하며, 목적을 달성하기 위해서 수신자가 원하지 않는 메일을 수신자의 메일함에 안전하게 전송하기 위해서 노력한다. 스팸 차단 시스템은 그 반대로 스팸메일이 메일 수신함에 들어오지 못하도록 노력하는 시스템이다. 스팸 메일은 개인 메일함을 어지럽히고, 혼란스럽게 만들며, 스팸 메일인지 아닌지를 판단하고 정리, 삭제함으로써 메일 수신함을 깨끗하게 유지하는데 비용이 들게 한다.

스팸 메일을 탐지하기 위한 여러 가지 방법 중 가장 대표적인 방법으로 SPF(Sender Privacy Framework)[1] 와 RBL(Realtime Blocking List)이 있으며, SPF는 발송 주소와 발송도메인에 대해서 유효성을 검사하는 것이며, RBL은 스팸 메일을 많이 보내는 발송 주소의 분포를 리스트화 한 것이다. 세계적으로 다수의 RBL 사이트가 존재하며, 약간씩 다른 방법으로 리스트를 생성하지만, 기본적으로 많이 발송된 스팸 주소가 좀 더 악성 주소라는 개념은 동일하며, 확률적인 분포를 통하여 생성함으로 RBL을 참조하는 메일 서버는 수신되는 이메일에 대해서 발송 주소를 추출하고, 이 발송 주소를 공인된 RBL 사이트에 DNS 질의, 검사하여 스팸의 진위를 판단한다. 최근 몇 년간 RBL은 많은 효과를 거두어 왔다. RBL서버는 전 지구상에서 발생할 수 있는 스팸 정보를 수집하고 발송 주소를 추출하고 정제하여 양질의 블랙 IP 차단 리스트를 만들어낸다.

본 논문에서는 최근 발생하는 여러 유형의 스팸메일 중에서 주로 봇넷[2, 3]에서 발송되는 이메일 스팸에 대한 효과적인 탐지 방법을 제안한다. 기존의 스팸차단을 위해서 널리 사용되었던 RBL 기법을 개선하여 새로운 스팸 차단방법을 제시하며, 그에 대한 효과를 측정해본다. 이를 위해서 최근에 발생하는 스팸 메일에 대한 특성을 살펴볼 필요가 있다. 최근 출현하는 스팸 메일 중에서 스팸 차단에 어려움을 겪는 경우는 크게 이미지 스팸과 봇넷[2, 3] 에서 발송하는 스팸으로 구분할 수 있다. 전자는 컨텐츠 필터링으로 해결할 수 없는 어려움이 존재하며, 후자는 RBL등의 발송 주소 분포를 사용하는 필터링 기법으로써 해결 할 수 없는 어려움이 있다. 본 논문에서 제안하는 것은 후자의 경우에 대한 것이며, 봇넷의 특성을 정의하고 그 스팸 발송 패턴을 분석함으로써, 봇넷에서 발송되는 스팸의 특성을 파악하고 이것을 RBL의 개념에서 확장하여 스팸 차단률을 향상시키는 것에 대해서 연구해 본다. 봇넷에서 발송되는 메일은 대부분 봇넷 스패머에 의해서 광고주의 광고 타깃이 되는 서버의 URL을 보내는 방식으로 구성되므로, 본 논문에서는 이러한 URL을 추출하여 이용하는 방법을 제시할 것이다.

이 논문의 구성은 다음과 같다. 2장에서는 RBL에 의한 스팸 필터링 메커니즘에 대해서 간략히 설명하고, 3장에서는 봇넷의 기본적인 특성과 봇넷에서 발송되는 스팸메일의 구조에 대해서 알아 볼 것이다. 4장에서는 스팸메일의 원문에서 URL을 정보를 추출하여 활용하는 방안과 확장 가능한 RBL을 어떻게 구성할 것인지에 대해서 논의할 것이며, 5장에서는 이메일 스팸 트랩 시스템[1]을 사용하여 허니팟[1] 을 구성하고 이메일 스팸메일로 수집된 메일을 분석하여 그 결과를 보여줌으로써 스팸 발송 패턴에 대해서 URL을 RBL에 확장, 적용하는 것이 봇넷에서 발송된 스팸을 검출하는 효과적인 방법임을 제시할 것이다. 그리고 마지막으로 6장에서는 결론과 향후 연구방향에 대해서 논의한다.

Ⅱ. RBL에 의한 스팸 필터링

RBL(Realtime Blocking List)은 크게 3가지 방법으로 생성된다. 첫째 실시간으로 메일 릴레이가 가능한 IP주소만을 수집하고 공개하는 DB, 둘째 실시간으로 해킹에 도용될 수 있는 Proxy의 IP 주소만을 수집하고 공개하는 DB 그리고 마지막으로 실시간으로 불량소프트웨어에 감염된 좀비 PC의 주소만을 수집하고 공개하는 DB로 나누어진다.

기존 RBL에 등재된 IP 리스트의 신뢰도의 증가는 지구상에 존재하는 메일 서버가 스팸메일을 효과적으로 판단하는데 큰 도움을 주며, 이를 위해서는 다수의 스팸 발송 주소 탐지 장치가 필요하다. 따라서 RBL간의 정보 공유와 스팸 발송 주소 탐지 장치의 지속적인 증가가 필

요 하다. 그림1.은 일반적으로 RBL 시스템에 의해서 스팸이 필터링 되는 메커니즘을 그림으로 나타낸 것이다. 최종 메일 수신단계에서 메일 서버는 RBL 시스템에 메일 발송 주소의 등록 유무를 조사함으로써 스팸 메일인지 확인할 수 있다.

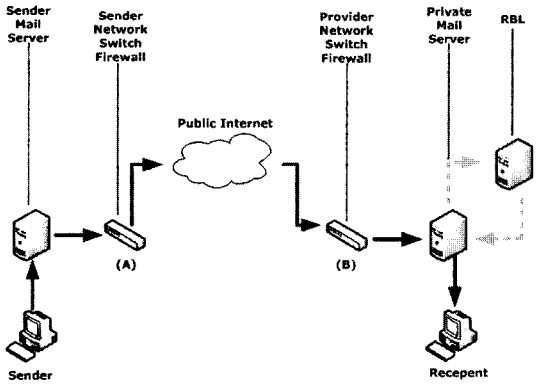

그림 1. RBL을 사용하는 일반적인 메일 송수신 흐름
Fig. 1. A general flow of the sending and receiving e-mail used in RBL

Ⅲ. 봇넷에서의 스팸 발송

봇과 봇넷은 여러 가지 동작을 수행하지만, 가장 많이 사용되는 것이 스팸 메일의 발송이다. 좀비에 감염된 PC들은 봇 컨트롤러와 좀비 아미 또는 봇넷으로 참조되는 형태의 다른 봇들과 통신한다[2, 3].

극히 빈도가 낮은 좀비PC의 주소가 모두 리스트에서 존재할 경우에 그 리스트를 유지하는 비용이 많이 든다. 결국, 효율적으로 해결 할 수 있는 다른 대안이 필요하며, 봇넷에서 보내는 스팸의 특성을 잘 살펴볼 필요가 있다. 봇넷에서 발송되는 스팸은 특별한 목적 즉, 금전적인 이득을 목적으로 원하는 대상서버로의 방문을 유도하는 특성을 가진다. 즉, 일반적인 내용기반 스팸 필터링보다, 방문되기를 원하는 URL에 대한 적극적인 방어가 필요하다.

3.1 봇넷의 기본 구조

앞에서 설명한 봇넷의 기본적인 메커니즘에 대해서 그림으로 표현하면 그림 2.와 같다. 일반적으로 감염된 좀비 PC에서 스팸이 발송되며, 컨트롤러를 통해서 명령이 하달된다. 좀 더 지능적인 봇넷 에서는 좀비간의 통신도 수행한다. 봇넷에서 좀비는 서로 간에 P2P로 통신 하는데, 컨트롤러와 좀비들 간의 통신이 두절되었을 경우 자립성을 실현하는 봇넷들도 존재한다. 점점 고도로 지능화된 봇넷을 근본적으로 차단하기는 상당히 어려운 점이 많다. 봇넷의 검출에 관련된 연구도 활발하게 진행중이다. 그림 2.는 일반적인 IRC(Internet Relay Chat) 기반의 봇넷에서의 DDOS 공격에 대한 그림이다.

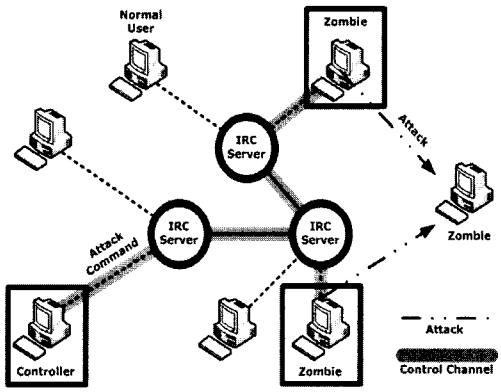

그림 2. IRC기반의 봇넷 DDOS
Fig. 2. IRC-based BotNot DDOS

3.2 봇넷에서의 스팸 발송

최근 스팸 유형 중에 봇넷을 이용해서 스팸메일을 보내는 경우를 많이 볼 수 있다. 최근에 구성된 봇넷들은 매우 지능적이며, 봇넷은 마스터와 컨트롤러라는 구성원에 의해서 자율적이며 협동적인 행동을 수행한다[3]. 이것은 웹의 악성 코드 등에 의해서 감염된 개인의 PC에서 마스터의 명령에 따라서 스팸을 발송한다. 스팸 발송이 실패 했을때 이웃하는 좀비 또는 마스터와의 통신을 통해서 발송의 확장 또한 가능하다.

이에 따라서 봇넷과 각 개인 PC에 설치된 좀비를 이용한 스팸 메일의 발송 메커니즘은 단일 메일 발송 주소가 아닌 광범위한 발송주소 범위에서 검출되므로, 새로운 방법이 제시 되지 않는다면 스팸 검출이 쉽지 않다. 봇넷의 발송 주소 대역이 몇 개로 제한된다면 발송 주소 클래스에 부가적으로 신뢰도를 부여하여, RBL 리스트를 생성하는 방법을 사용할 수 도 있다.극적인 방어가 필요하다.

Ⅳ. URL정보를 확장한 RBL 시스템 구성

본 논문에서는 스팸메일의 원문에서 URL 추출하여 그 URL을 이용하여 RBL 시스템의 확장을 제안한다. 따라서 기존의 RBL 룩업에서 스팸 URL 룩업을 추가하면 된다. 시스템의 구성에 있어 특별히 어려운 점은 없다. 본 논문에서 제안하고자하는 것은 이러한 메커니즘의 타당성이다. 기존의 발송 주소 리스트를 사용 하던 것에 더해서 URL 리스트를 추가적으로 사용하면 되는 것이다. 다음의 그림3.은 간단히 스팸 발송 주소에 더해서 스팸 URL을 추가한 시스템의 구성도를 나타낸 것이다.

이미 몇 가지 사이트들[5, 6]에서 이러한 스팸 URL을 가지고 RBL 확장 구성을 시도하고 있지만, 봇넷에 대한 검출과 URL추출을 수행 하는 것에 대해서는 아직 미미하다.

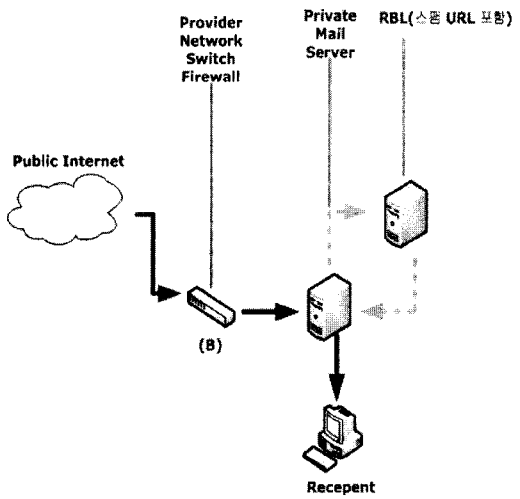

그림 3. URL 정보를 확장한 RBL 시스템 구성도
Fig. 3. RBL system configuration extending URL information

Ⅴ. 실험 및 결과

5.1 이메일 스팸 트랩 시스템 구성

본 논문에서 제안된 내용에 대해 실험을 위해서 이메일 스팸 트랩 시스템(honeypot)을 구성한다. 이것은 능동적으로 스팸메일을 수집하고 스팸 메일의 원문에서 발송 IP와 본문에 포함된 URL의 추출 및 통계, 분포 그리고 최종적으로 URL의 IP등을 분석하고자 하는 것이 그 목적이다.

먼저 이메일 스팸 트랩 시스템에 대해서 간단히 정의하도록 한다. 이 시스템은 실제로 사용되지 않는 메일서버를 이용하여, 스패머들에게 스팸 발송을 유인함으로서 분석 가능한 샘플메일을 얻고자 함이 그 목적이다. 메일을 한번 도 발송한 적이 없는 계정들이 존재하는 이메일 시스템이기 때문에 수신된 메일들에 대해서 스팸메일로 가정할 수 있다. 일반적인 명칭으로 이메일 허니팟이라고도 부르며, 봇넷 검출[7], 악성코드 검출 등 여러 가지 용도로 사용된다. 본 논문에서는 다음과 같이 이메일을 수신하는 부분과 메일을 분석하고 발송 주소와 URL을 추출하는 부분 그리고 통계를 분석하는 시스템으로 구성된다. 이메일 스팸 트랩 계정을 이용하기 위해서는 이메일 트랩 계정 생성 서버에서 생성하고 이를 인터넷에 공표한다. 본 논문의 실험에서 필요한 시스템을 다음과 같이 구성한다.

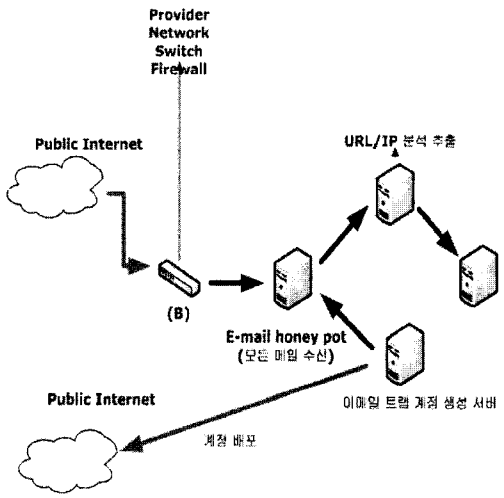

그림 4. 스팸메일을 수신하기 위한 이메일 스팸 트랩 시스템 구성도
Fig. 4. System configuration of e-mail spam trap to receive e-mail spam

5.2 실험 결과 및 통계

이메일 스팸 트랩 시스템으로 수신된 메일의 발송 IP의 빈도를 분석함으로써 기존의 RBL 의해서 스팸 필터링 될 수 있는 여지가 있는지에 대해서 알아볼 것이다. 표.1은 약 열흘간 메일 스팸 트랩 시스템으로 입수된 스

팸메일의 발송주소를 표로 정리한 것이다. 왼쪽 칸에는 스팸 발송 IP 주소 빈도수를 오른쪽은 그 빈도가 나타난 IP의 개수이다. 총 수집된 스팸 메일은 796,339개이다. 왼쪽 빈도수는 스팸메일의 발송 IP를 모두 분석한 결과 1회 출현한 IP가 총 28,739개라는 것이다. 그리고 10~100은 내용의 구성상 하나로 정리하였다. 이 표에서 알 수 있듯이, 한 개의 IP가 435,557 개 나타난 경우도 보인다.

RBL을 구성하는 가장 단순한 알고리즘 형태로 봤을 때, 가장 하단의 435,557개의 스팸 메일을 발송한 한 개의 IP는 가장 악성 IP로 분류 될 수 있다. 즉, 가장 많이 나타난 IP는 실제로 RBL등에서 잘 필터링 될 것이다. 발송 IP 주소의 분포를 통해서 생성되는 RBL 리스트에는 빈도수에 따라서 435,557번 나타난 1개의 IP 주소가 가장 악성 IP 주소이며 그 이후로 순서대로 RBL에 등재될 확률이 높다. 한 번의 스팸 발송 빈도를 가지는 형태로 많이 나타난 IP는 분명히 어떤 RBL에 등재되어 있을 것이다. 그러나 한 개씩 나타는 많은 스팸발송주소는 RBL에 등재될 확률이 낮다.

실제로 이 많은 스팸 발송 IP가 서로 연관이 없다면 상관없다. 고의든 실수이든 스팸메일을 한번 발송하고 RBL에 의해서 등재된다면 RBL 리스트는 너무 많은 IP를 유지 하고 있어야 하며, RBL 시스템의 성능 또한 영향을 받는다.

표 1. 이메일 스팸 트랩 시스템에 나타난 스팸 발송 IP 빈도수별 IP개수

Table 1. The number of IP per IP frequency sending spam, which was shown on the e-mail spam trap system

스팸 발송 IP 주소 빈도수	IP 개수
1	28,739
2	5,038
3	1,306
4	807
5	478
6	587
7	320
8	305
9	278
10	247
10~100	5,868
100~2000	297
435,557	1

그러나, 한 번씩 또는 소수의 빈도수를 나타내는 발송 주소들이 봇넷에 의해서 발송된 스팸메일들이라면 기존의 RBL에 의해서 차단될 가능성이 낮아진다. 적극적이고 효과적인 대응 없이는 봇넷에서 발송되는 스팸메일에 대해서 속수무책일 수밖에 없으며, 기존의 RBL에 의한 방법에 추가적으로 새로운 스팸 차단 방법이 요구된다. 기존의 방법에서 모든 스팸 발송 주소를 유지하는 것은 시스템의 성능 저하와 부하를 높게 유지하기 때문이다. 실험결과 표.1에서 '스팸 발송 IP 주소 빈도수' 가 낮을 경우인 한번 발송된 스팸 메일 28,739개의 스팸 메일에 대해서 원문을 분석해 본다. 물론, 소수의 빈도를 모두 대상(가령 2번, 3번)으로 포함시킬 수도 있으나, 여기서는 한번 씩 발송된 스팸 발송 주소로 제한한다. 표.2는 한 번씩 발송된 28,739개의 발송주소 메일에 대해서 원문 분석을 수행한 결과이며, 한 번씩 발송된 IP에 대해서 본문에 스팸URL이 포함된 메일 중에서 본문 링크의 통계를 1위부터 10위까지만 추출한 것이다.

본문에 링크가 포함된 메일은 총 8558개이며, 각 URL에 대한 링크별 순위를 나타낸다. 결국 이 분포를 리스트로 만들어내면 확장 가능한 URL을 가진 RBL시스템을 구성할 수 있는 것이다. 표.2의 결과는 표에서도 나타나듯이 서로 다른 발송 주소에서 발송된 메일들의 원문에서 같은 URL이 추출됨으로써, 봇넷에서 발송된 스팸 메일은 하나의 발송주소에서 같은 메일이 발송되는 것이 아니라, 수평적으로 넓게 퍼진 발송주소 영역에서 스팸메일이 발송됨을 알 수 있다.

이러한 시스템에서는 기존의 알고리즘이나 랭크 시스템으로 RBL을 만들기에 충분한 요건을 만족하지 못한다. 그러나 다른 예를 들어보자, 모든 스팸메일에 포함된 URL의 링크를 분석해 보기로 한다. 스팸 URL은 충분히 가능한 몇 개로 수렴되고 있다. 이것은 봇넷의 특성을 만족한다. 봇넷은 서로 다른 널리 퍼져있는 자원을 이용하여 메일을 발송하지만, 시간대 유사 분포도에서는 같은 봇넷에서 발송된 메일일 확률이 높다. 이것은 몇 개의 단어가 다르거나 파라미터가 다른 URL로 연결되며, 페이지에서 다른 페이지도 리다이렉트[4]되는 경우도 많다. 스팸메일에 의해서 개인이 최종적으로 방문하는 곳에 입력된 개인정보가 저장되거나, URL의 IP를 추적해보면 결국 몇 개의 IP로 수렴된다. 이것은 광고주가 여러 명의 스패머에게 스팸 발송을 의뢰하기 때문이기도 하다.

표 2. 스팸 발송 주소가 한 개씩만 수집된 것에 대한 본문 포함 링크 분석 통계
Table 2. Link analysis statistics containing e-mail body, which was collected only one spam address

Hostname	Count
www.21springshoe.com	793
www.wouldmillion.com	488
www.shoes1you2.com	208
www.stringcolony.com	177
animalrain.com	107
minetold.com	106
exampleopposite.com	96
teethexperiment.com	95
cellgentle.com	90
filltown.com	88

VI. 결론 및 향후 연구

기존의 RBL 시스템들은 과거 수 년 동안 스팸 메일 차단에 있어서 많은 효과를 거두어 왔다. 하지만 최근의 스팸메일들이 다량의 발송주소를 소유한 스패머 또는 봇넷을 이용한 스팸 발송에 대처하기에는 비효율적이다. 따라서 스팸메일에 포함된 URL등의 분포를 이용하는 것은 합리적인 대안이 될 수 있다. 다양한 스팸메일에 대해서 스팸 필터링을 효과적으로 수행하기 위해서는 스팸 발송 메커니즘의 정확한 이해를 바탕으로 분석을 통하여 그 효과를 증대시킬 있다. 스패머의 의도를 충분히 이해하는 것이야 말로 스팸 필터링 대책을 세우는데 최고의 지름길이다.

본 논문에서는 봇넷을 통해서 보내는 스팸메일에 대해서 효과적으로 차단률을 높이는 방법을 RBL을 확장하는 개념에서 접근해 보았다. 봇넷을 의해서 발송되는 스팸 메일에 대해서 RBL에 등재하는 효과적인 방법으로 스팸 발송 주소의 대역별 클래스 단위로 등재하는 것도 그 대안이 될 수 있다. 클래스 단위의 신뢰도를 설정하여 스팸 발송 주소의 빈도를 클래스별로 할당할 수도 있을 것이다. 다수의 IP를 보유한 전문 발송인으로 추정되는 발송자에 의해 대량으로 발생하고 있는 현재의 상태에서의 적극적인 대응은 아직 미미한 수준이며, 좀 더 다양한 방법으로의 접근이 필요하다. 스팸 필터링 자체의 연구뿐만 아니라, 봇넷의 적극적인 대응도 필요하며, 이러한 연구는 다른 여러 연구기관과 공동으로 협조적인 대책이 필요하다.

참고문헌

[1] M.W. Wong and M. Lentczner. "Sender Policy Framework(SPF): A Convention to Describe Hosts authorized to Send SMTP Traffic," May 2004

[2] G. S. Mullane, "Spambot Beware", Website, 2003, http://www.turnstep.com/Spambot/inde- x.html.

[3] Cooke E, Jahanian F, Mcpherson D, The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets, Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI) (June 2005.)

[4] S.Webb, J.Caverlee, C.Pu, Characterizing Web Spam Using Content and HTTP Session Analysis, In Proceedings of the Fourth Conference on Email and Antispam CEAS 2007.

[5] Realtime URI Blacklist, http://www.uribl. com, March 2008.

[6] SURBL, http://www.surbl.org, March 2008.

[7] The Honeypot Project and Research Alliance Know Your Enemy, Tracking Botnets. http://honeynet.org /papers/bots, March 2005.

저자소개

김종민 (kim jong min)

1997 동국대학교 전자계산학과 졸업
2000 동국대학교 대학원 전자계산학 석사
2000 ~ 2005 코리아링크 기술연구소
현재 (주)모비젠 기술연구소 선임연구원
※관심분야 : 스팸메일 유형 분석 및 차단 알고리즘 연구

김형근 kim hion gun

1993 KAIST 전자계산학과 졸업
1995 KAIST 전자계산학 석사
1995 ~ 2000 한국통신 연구소 연구원
현재 (주)모비젠 기술연구소 연구소장 재임
※ 관심분야 : 자연어 처리 및 검색엔진, 웹문서 수집로봇

김봉기(Bong-Gi Kim)

1987년 숭실대학교 전자계산학과 공학사
1989년 숭실대학교 전자계산학과 공학석사
1999년 숭실대학교 전자계산학과 공학박사
1994년 3월 ~ 1999년 2월 한림성심대학 컴퓨터응용과 조교수
1999년 3월 ~ 현재 진주산업대학교 컴퓨터공학부 부교수
※관심분야 : 지능형 홈, 지능형 제어, 멀티미디어 시스템