情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

이메일 스팸트랩을 이용한 좀비 PC 및 봇넷 추적 방안 연구*

정 현 철[1†], 김 휘 강[2‡], 이 상 진[2], 오 주 형[1]
[1]한국인터넷진흥원, [2]고려대학교

Study for Tracing Zombie PCs and Botnet Using an Email Spam Trap*

HyunCheol Jeong[1†], Huy Kang Kim[2‡], Sangjin Lee[2], Joo Hyung Oh[1]
[1]Korea Internet & Security Agency, [2]Korea University

요 약

봇넷(Botnet)은 이미 해킹당한 좀비 PC들로 구성된 거대한 네트워크이다. 본 논문에서는 대다수의 스팸이 봇넷에 의해 발송되고 있다는 점에 착안하여 스팸메일을 분석하여 봇넷과 좀비PC들을 탐지할 수 있는 시스템을 설계하고 이를 검증하였다. 특히, 본 논문에서는 국가차원에서 스팸 수집·분석·증거물 확보를 목적으로 KISA에서 운영하고 있는 이메일 스팸 트랩 시스템에서 수집된 방대한 스팸 메일을 분석에 활용하였다. 본 논문에서는 동일한 URL이나 첨부파일을 가진 스팸을 하나의 그룹으로 분류하고, 각 그룹의 전체 IP들이 어느 정도 봇넷의 특징을 가지고 있는지와 그룹 내의 각각의 IP들이 어느 정도 좀비 PC의 특징을 가지고 있는지를 측정하여 봇넷 그룹과 좀비 PC를 판별할 수 있도록 설계하였다. 제안된 시스템의 시뮬레이션 결과 1시간동안 16,030개의 좀비 의심 PC를 추출할 수 있었으며, 이메일 스팸이 좀비 PC를 추적하는데 상당히 유용한 정보를 제공해 줄 수 있음을 확인할 수 있었다.

ABSTRACT

A botnet is a huge network of hacked zombie PCs. Recognizing the fact that the majority of email spam is sent out by botnets, a system that is capable of detecting botnets and zombie PCs will be designed in this study by analyzing email spam. In this study, spam data collected in "an email spam trap system", Korea's national spam collection system, were used for analysis.

In this study, we classified the spam groups by the URLs or attached files, and we measured how much the group has the characteristics of botnet and how much the IPs have the characteristics of zombie PC. Through the simulation result in this study, we could extract 16,030 zombie suspected PCs for one hours and it was verified that email spam can provide considerably useful information in tracing zombie PCs.

Keywords: Botnet, Zombie PC, Spam botnet

I. 서 론

봇넷(Botnet)은 이미 해킹당한 좀비 PC들로 구성된 거대한 네트워크이다. 봇넷은 일반적으로 C&C (Command & Control) 서버를 통해 수백 대에서 수십만 대에 이르는 좀비 PC들을 원격에서 제어함으로써 공격자가 원하는 행위를 하게끔 한다. 1대의 봇(Bot)이 지하 경제 세계에서 0.03달러가량에 거래되

접수일(2010년 10월 13일), 게재확정일(2010년 12월 30일)
* 본 연구는 방송통신위원회의 정보보호원천기술개발사업의 연구결과(KCA-2011-10914-06001, 지능형 악성코드 자동분석 및 경유·유포지 탐지기술)와 지식경제부 및 정보통신산업진흥원의 "대학 IT연구센터 육성·지원사업 (NIPA-2011-C1090-1001-0004)"의 연구결과로 수행되었음
† 주저자, hcjung@kisa.or.kr
‡ 교신저자, cenda@korea.ac.kr

고 있는데, 수만 대의 봇으로 구성된 봇넷은 수백 달러에 팔리고 있다[12]. 지하 경제에서 거래된 봇넷은 DDoS 공격, 개인/금융정보 유출, 불법 스팸메일 발송, 온라인 사기 등 불법적인 방법으로 금전적 이득을 취하는데 악용되고 있다.

봇넷이 공격자에 의해 범죄에 악용되고 그들에게 부를 축적할 수 있는 수단이 되어줌에 따라 봇넷은 지속적으로 진화하고 있고 봇에 감염되어 좀비 PC로 전락하는 PC의 수 또한 증가하고 있다. TCP/IP 프로토콜의 공동 창시자인 Vint Cerf는 인터넷에 연결된 컴퓨터 중 4분의 1 이상에 해당하는 컴퓨터(전 세계 약 6억대의 컴퓨터의 중 1억~1억5천대의 컴퓨터)가 이미 악성 봇에 감염되어 봇넷의 일원으로 악용되고 있다고 하며, 이러한 상황에서 인터넷이 아직 작동하고 있다는 사실 자체가 놀라울 정도라며 봇넷의 위협을 강력히 경고하였다[13].

봇넷은 금품 갈취를 위한 협박성 DDoS 공격, 개인/금융정보 유출, 불법 스팸메일 발송, 온라인 사기 등 다양한 목적으로 사용되고 있다. 대부분의 DDoS 공격에는 악성봇에 감염된 좀비 PC들이 악용되고 있으며, 봇넷을 이용한 범죄행위 중 우리가 가장 쉽게 탐지할 수 있는 공격 또한 DDoS 공격이다. 하지만 DDoS 공격에 이용되는 좀비 PC들은 ISP 사업자들에 의해 쉽게 발각되고 차단될 수 있으며, DDoS 공격을 하는 봇 master는 자신의 봇넷을 잃어버릴 수 있는 위험을 감수해야만 한다. 이러한 이유에서 최근 DDoS 공격보다 훨씬 많은 돈을 벌 수 있고, 발견될 위험성도 적은 스팸 발송에 봇넷을 이용하는 경우가 증가하고 있다[14]. M. Bailey의 논문에서도 봇의 가장 중요한 사용처 중의 하나가 스팸 발송이라고 말하고 있다[9]. 스팸발송 메일서버는 RBL(Real-time Black List) 등 스팸차단 정책에 의해 차단되고 있어 스팸 발송을 위해서는 많은 수의 새로운 메일서버들을 필요로 하는데, 봇에 감염된 호스트들은 스팸발송을 위한 훌륭한 수단을 제공해 주고 있다. M. Bailey의 논문에서 봇넷을 이용한 5가지 공격(Single Host DDoS, Multi Host DDoS, Identity Theft, Spam, Phishing) 중 스팸의 공격 가치가 가장 높고, 발견 위험성 및 설계 복잡성은 상대적으로 낮은 것으로 평가하였다[9].

보안업체 MessageLabs社의 조사결과, 전체 스팸메일의 83.2%가 봇넷에 감염된 좀비PC로부터 발송된 것이라고 밝혔다. Cutwail, Mega-D, Grum, Rustock 등 많은 대규모 봇넷들이 스팸발송에 사용되고 있으며, 특히 Cutwail 봇넷은 150만대에서 200만 대에 이르는 거대한 좀비PC들을 이용하여 전체 스팸의 35% 이상을 발송하기도 했다[15].

이처럼 봇넷이 스팸메일 발송의 주요 근원지로 부각됨에 따라 스팸대응 국제조직에서도 봇넷에 의한 스팸메일 차단을 위한 노력을 시작하였다. 영국의 OFT (Office of Fair Trading)와 미국의 FTC(Federal Trade Committee) 주도로 운영되고 있는 국제 스팸대응 조직인 LAP(London Action Plan)에서는 국가 간 스팸 전송자에 대한 법적처벌 및 국제대응조직간 상호협력 등 법·제도 및 정책적인 이슈를 주로 다루어 왔다[16]. 하지만, 최근 LAP에서도 스팸방지를 위한 각국의 정책 및 국경 간 공조 프레임워크 논의에 그치지 않고 실질적 스팸대응을 위해 악성코드, 봇넷 등 스팸발생의 근원적인 위협에 대한 이해가 선행되어야 함을 인식하고 기술적인 부분에 대한 연구를 확대하고 있다[16].

본 논문에서는 대다수의 스팸이 봇넷에 의해 발송되고 있다는 점에 착안하여 스팸메일을 분석하여 봇넷과 좀비PC들을 탐지할 수 있는 시스템을 설계하고자 한다. DDoS, 개인/금융정보 유출 등 봇넷을 이용한 다른 공격에 비해 공격 결과물인 스팸메일을 쉽게 수집할 수 있고, 공격이 발생되고 있는 순간이 아닌 공격 이후에도 증거물이 남아 있어, 실시간 분석 뿐 아니라 사후분석도 가능하다는 장점이 있다. 전체 스팸메일의 80% 이상이 좀비 PC로부터 발송되었으므로 스팸메일의 헤더정보와 페이로드(Payload) 분석은 좀비 PC 추적에 결정적인 단서를 제공해 줄 것으로 생각한다.

본 논문의 2장에서는 스팸 메일 분석을 통해 좀비 PC를 확인하는 기존의 연구동향을 살펴보았고, 3장에서는 봇넷에 의해 발송된 스팸메일의 특징과 봇넷 탐지의 개념을 소개하였으며, 4장에서는 이를 시스템으로 구현할 수 있도록 설계하였다. 5장에서는 이메일 스팸트랩에서 수집된 스팸메일을 샘플로 하여 제안한 시스템을 시뮬레이션하여 보았으며, 6장에서는 결론 및 향후 연구과제를 언급하였다.

II. 기존 연구 동향

봇넷은 다양한 사이버범죄의 수단으로 사용되고 있기 때문에 침해사고대응팀(CSIRT, Computer Security Incident Response Team)이나 사이버보안 연구자들의 주요 관심사가 되고 있다.

봇넷 탐지 기술은 네트워크 기반 분석과 호스트 기반 분석으로 나눌 수 있다.

네트워크 기반 분석은 악성봇 전파, DDoS/스팸발송 등 공격행위, 악성 봇 성능 업그레이드 등 네트워크 트래픽 모니터링을 통해 봇넷의 행위를 분석하여 봇 C&C를 탐지하는 방법이다. 하지만, 이 방법은 많은 정상적인 트래픽이 봇넷 트래픽으로 잘못 탐지 될 수 있으며, 대규모 네트워크에서 적용할 경우 성능 문제가 발생할 수 있다. 호스트 기반 분석은 허니넷을 통해 수집된 악성코드를 리얼 머신 또는 가상머신에서 정적/동적 분석하여 악성봇을 탐지하는 기술로 최근 packing, 암호화, 가상머신 확인기술 등 다양한 분석 회피 기술들이 사용되고 있어 분석의 어려움이 있다.

본 논문에서는 대용량의 정상/비정상 트래픽이 섞여 있는 네트워크 트래픽을 분석대상으로 삼지 않고, 80% 이상이 악성봇에 의해 발송되고 있는 스팸메일을 분석대상으로 삼음으로써 성능 및 탐지 정확성을 높이고자 한다. 본 논문에서 분석 대상으로 삼고 있는 스팸메일을 이용한 봇넷 탐지 연구동향을 살펴보도록 한다.

MIT 대학에서는 로컬 메일서버에 수집된 스팸 트래픽을 기반으로 스패머들의 클러스터링 구조를 조사하였다[4]. 이 연구에서는 스패머들은 스팸메일에 포함된 URL 그룹에 기반한 클러스터링 구조와 상당히 높은 연관관계가 있음을 보여주었다. 동일한 스패머 그룹의 스팸 발송간격 등 집단적인 행동패턴을 분석함으로써 해당 그룹에 의한 스팸발송을 예측하는 연구를 하였다. 하지만, 이 연구에서는 URL을 포함하고 있지 않은 스팸메일은 클러스터링할 수 없다는 한계가 있고, 단축 URL을 사용하여 실제 동일한 목적지 사이트이지만 웹사이트 주소를 서로 다르게 사용하는 등 URL 은닉수법에 대한 대응 연구가 필요하다.

MS에서는 스팸 봇넷을 탐지하기 위한 URL 시그니쳐를 자동 생성해 주는 AutoRE라고 하는 프레임워크를 제안하였다[1]. 이 연구에서는 Hotmail에서 수집한 스팸메일을 실험 데이터로 사용하였으며, 스팸의 페이로드와 트래픽을 분석하여 스팸봇넷 및 좀비 IP를 탐지하였다. 스팸 봇넷으로 탐지하는 기준으로 얼마나 많은 서로 다른 AS(Autonomous System)에서 스팸이 발송되었는지 하는 "분산성(distributed)", 아주 짧은 기간에 많은 스팸이 발송되었는지 하는 "집중성(bursty)", random URL 스트링의 특징을 추출하는 "특이성(specific)"을 삼았다. 또한, 스팸 봇넷의 네트워크 스캐닝 행위 등 네트워크 트래픽도 스팸 봇넷 탐지에 활용하였다. 하지만 탐지를 회피하기 위해 장기간에 걸쳐 적은 량의 스팸을 발송하는 봇넷 등 탐지회피 기술이 결합된 최근의 봇넷을 탐지하는데 한계를 보이고 있다.

Washington 대학에서는 스팸기반 봇넷의 행위를 지속적으로 모니터링하고 분석할 수 있는 Botlab 이라는 플랫폼을 개발하였다[2]. Botlab은 Network Fingerprinting, Execution Engine, DNS Monitoring, Clustering, Correlation Analysis의 5가지 과정을 통해 스팸봇을 탐지한다. Botlab은 스팸 데이터의 URL을 바탕으로 Crawling하여 다운로드 가능한 실행파일을 가상 머신 또는 실 서버(Bare-metal) 기반의 실행 엔진에서 실행하여 그 행위를 모니터링한다. 실행엔진의 행위 모니터링 결과는 DNS 모니터링 결과와 연관관계 분석하여 최종적으로 스팸봇을 분류한다. 이 연구는 악성코드를 유포하기 위한 스팸봇을 탐지하기에는 상당히 유용하지만, 단순 광고성 스팸을 전파하기 위한 봇넷의 경우 해당 URL을 Crawling하더라도 악성 실행파일이 다운로드 되지 않는 경우가 대부분으로 광고성 스팸봇을 탐지하기에 한계를 가진다.

UC Berkeley 대학에서는 MS사의 Hotmail 서버의 스팸메일을 분석하여 봇넷 멤버를 찾아내는 연구를 진행하였다[20]. 이 연구에서는 동일한 URL이나 동일하거나 거의 중복되는 콘텐츠를 가진 이메일을 클러스터링하여 스팸 캠페인을 찾아내고 있으며, 각 스팸 캠페인을 구성하고 있는 봇넷의 규모, 스팸발송주기 등을 모니터링하였다. 이 연구에서도 동일한 봇넷 그룹으로 클러스터링하는 가장 주요 인자를 URL로 삼았다. 하지만, 이 연구에서는 IP주소가 알려진 relay IP 또는 Proxy IP인 경우, 스팸캠페인의 IP들이 1개의 C-class에 속하는 경우, 3개 미만의 지역에 속하는 경우 등 3가지 경우를 제외하고 모두 봇으로 간주하고 있어 오탐(False-Positive)이 발생될 수 있는 가능성이 높다.

III. 스팸메일의 특징 및 스팸봇넷 탐지 개념

3.1 봇넷에 의해 발송된 스팸메일의 특징

스패머들은 스팸 발송을 위해 메일서버와 네트워크 대역폭이 필요한데, 지속적으로 스팸메일을 발송하는 메일서버들은 블랙리스트에 등록되어 메일발송이 차단되기 쉽다. 이러한 문제를 해결해 줄 수 있는 수단

이 봇넷인데, 봇넷은 거대한 분산 호스트를 거느리고 있어 차단이 어렵고, 아무런 비용없이 네트워크 대역폭을 마음대로 사용할 수 있어 스패머들에게 매력적인 스팸발송 수단이 되어주고 있다.

봇넷에 따라 상이할 수 있지만 많은 스팸봇넷은 일반적으로 다음과 같은 과정을 통해 스팸메일을 발송한다. 첫째, 스팸 템플릿 서버를 통해 발송할 스팸메일의 콘텐츠를 작성하고, 발송자 메일주소, subject, 페이로드 등은 일정한 규칙에 따르거나 무작위로 조작한다. 둘째, 스팸 수신자는 봇 C&C 서버에서 메일주소 리스트를 전송받거나 좀비 PC의 메일 주소록 또는 캐쉬 파일에서 메일 주소를 수집함으로써 결정한다. 셋째, 스팸메일 발송은 좀비 PC 자체에 SMTP 엔진을 가지고 발송하거나, 오픈된 메일 Proxy를 이용하거나 Hotmail과 같은 웹메일 서비스를 이용하기도 한다. 넷째, 스팸메일 발송시 수신자의 메일서버를 확인하기 위해 대량의 MX query를 생성하기도 한다.

위와 같은 발송과정을 거친 스팸봇넷에 의해 발송된 스팸메일은 일반적으로 다음과 같은 특징을 가지고 있다.

- 발송자 IP 주소의 분산성 : 봇넷의 가장 큰 특징은 분산성인데, 봇넷에 의해 발송된 스팸메일들의 특징도 1개의 IP에서 발송되지 않고 수많은 분산된 IP에서 동일한 스팸이 발송된다는 것이 특징이다. 또한 IP들이 속한 AS와 지리적 위치도 분산되어 있다. 대표적인 스팸봇넷인 Cutwail 봇넷은 210만대에 달하는 많은 좀비 PC를 이용하여 전체 스팸의 35%에 해당하는 스팸메일을 발송하였다[15].
- 발송자 이메일 주소의 분산성 : 일반적으로 봇넷에 의한 스팸메일 발송시 스팸 발송자의 이메일 주소를 신뢰할 수 있는 메일 주소로 위장하거나 실제 존재하지 않는 주소를 사용한다. 동일한 발송자 IP를 가지고 있다고 하더라도 발송자 이메일 주소가 다수개로 위장되는 경우가 많다. 동일한 페이로드를 가진 이메일들의 발송자 이메일 주소가 상당 수준이상 분산되어 있을 경우 봇넷에 의해 발송된 것으로 의심할 수 있다.
- 수신자 이메일 주소의 분산성 : 봇넷에 감염된 좀비 PC는 짧은 시간에 많은 메일을 여러 수신자에게 보낸다. 하나의 IP에서 일정 기간 내에 발송한 메일의 수나 메일 수신자의 수도 좀비 PC 탐지의 한 요소가 될 수 있다.
- 스팸메일 내의 URL과 첨부파일의 유사성 : 스팸메일은 제품/서비스 광고, 음란/도박 사이트 홍보, 불법 S/W 판매, 악성코드 감염 등을 위해 전송된다. 광고성 스팸의 경우 적은 사이즈의 스팸을 발송하기 위해 메일 페이로드에 모든 내용을 포함하지 않고, 관련된 URL을 링크시키는 경우가 많다. 악성코드 감염을 목적으로 한 스팸의 경우는 메일 수신자를 감염시킬 수 있는 악성코드 파일을 첨부하는 경우도 흔히 볼 수 있다. 이처럼 다수의 메일에 동일한 URL이나 첨부파일이 포함되어 있을 경우 다수의 좀비 PC로부터 발송되었다고 의심할 수 있다.
- 비정상적인 메일서버를 이용한 메일 발송 : 봇넷에 감염된 많은 좀비 PC들은 자체 SMTP 엔진을 가지고 있어 정상적인 로컬 메일서버를 거치지 않고 직접 메일을 발송한다. 이 경우 메일발송 서버의 PTR(Pointer DNS Record) 정보를 확인할 수 없고, 발송자 E-mail 주소의 도메인과 메일서버 IP가 속한 도메인이 일치하지 않는다. 발송자 메일서버가 정상적으로 등록된 메일서버인지 검증함으로써 봇넷에 의해 발송된 스팸인지 확인할 수 있다.
- 적은 수의 Received 필드 개수 : 자체 SMTP 엔진을 사용하여 스팸메일을 보내는 좀비 PC의 경우 MTU(Mail Transfer Unit) 역할과 로컬 MTA(Mail Transfer Agent) 역할을 동시에 하게 된다. 봇넷은 로컬 메일서버를 거치지 않고 수신자 메일서버에 스팸메일을 직접 전달해 주게 되므로, 정상적인 메일 발송과정에 비해 메일이 전달되는 hop이 훨씬 줄어든다. 메일이 전달되어 온 경로는 메일 헤드의 Received 필드를 통해 확인할 수 있으며, 수신자 메일서버 이전의 Received 필드 수가 2개 미만인 경우 좀비에 의한 스팸메일을 의심할 수 있다.

위에서 언급된 특징들은 환경에 따라 정상적인 메일에서도 발생될 수 있으므로, 한 가지 특징만으로 봇넷을 단정하지 말고, 여러 가지 특징을 복합적으로 고려하여 봇넷을 추출함으로써 오탐률(False-Positive Rate)을 줄일 필요가 있다.

3.2 스팸 봇넷의 노드와 그룹

본 논문에서는 스팸메일에 포함되어 있는 URL과 메일 첨부파일을 통해 각 스팸 발송 IP들 간의 링크를

형성하고, 각 그룹의 IP들의 지리적 위치, MTA 여부, 블랙리스트 포함 여부 등 공개된 정보를 최대한 활용하여 공개되지 않은 정보, 즉 좀비 PC인지 여부를 분석할 수 있도록 한다. 본 논문에서는 각 IP들이 얼마나 좀비 IP의 특성을 지녔는지와 이 IP들로 구성된 그룹이 얼마나 스팸 봇넷의 특성을 지녔는지 측정하고 그 결과를 서로 feedback하여 탐지 범위와 정확도를 높이고자 한다.

3.2.1 발신자 IP 주소

스패머는 스팸 발송자 IP 주소를 포함하여 발송자 이메일 주소, 발송시간 등 많은 정보를 조작할 수 있다. 하지만, 수신자 메일서버의 바로 전 단계의 발송자 IP 정보는 수신자 메일서버에 의해 Received 필드에 기록되기 때문에 공격자에 의해 조작이 불가능하다. 많은 스팸 봇들은 자체 SMTP 엔진을 가지고 있는데, 이 경우 수신자 메일서버 바로 전단계의 발송자 IP 정보는 바로 좀비 PC의 IP주소이다.

각 발신자 IP는 좀비 PC로 의심되는 알려진 특성들을 얼마나 많이 가지고 있느냐를 기준으로 IP별 오염도를 측정한다. 각각의 IP별로 RBL 등록 여부, 발송한 메일의 수, 발송 메일서버의 MTA 여부, Received 필드 수가 기본적인 판단기준이 되고, IP가 속해 있는 그룹의 오염도 값도 추후 반영시켜서 각 IP별 오염도를 계산한다.

3.2.2 동일 스팸그룹 결정

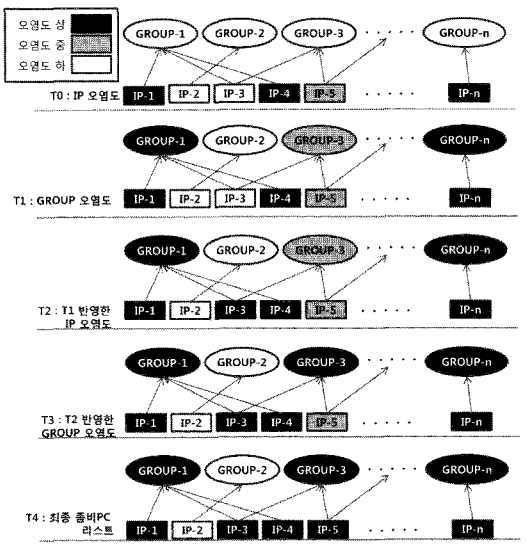
유사한 스팸메일이 분산된 다수의 IP로부터 발송되었다면 스팸 봇넷을 의심해 볼 필요가 있다. 이때 유사한 스팸메일의 기준을 무엇으로 할 것인지를 결정해야 한다. 본 논문에서는 스팸 메일 내에 포함되어 있는 URL과 첨부파일을 스팸 그룹을 결정짓는 기준으로 삼고자 한다.

스팸메일은 광고나 malware 전파 등을 목적으로 전송되는데, 페이로드에 text 형태로 전달하기 보다는 URL이나 첨부파일에 전달하고자 하는 내용을 포함하는 경우가 대부분이다. 한 보고서에서는 스팸메일의 95%가 URL을 가지고 있다고 밝혔다[18]. 스패머들이 URL을 선호하는 이유는 전달하고자 하는 모든 정보를 스팸메일 페이로드에 담을 경우 스팸메일의 사이즈가 커져 네트워크 리소스를 많이 소비하고, 메일 차단시스템에 의해 차단될 가능성이 높아지기 때문이다. 첨부파일은 malware 전파 목적으로 많이 사용되고 있는데, 실행파일 뿐만 아니라 문서파일이나 그림파일 등으로도 수신자 PC를 감염시킬 수 있다.

동일한 URL이나 첨부파일을 가진 스팸메일들을 그룹으로 분류하고, 각 그룹이 얼마나 봇넷의 속성을 많이 가지고 있는지를 측정한다. 봇넷 그룹의 속성은 그룹내 IP들의 분산성, IP들의 지리적 다양성, 그리고, 각 IP들의 오염도 값이 기준이 된다. 동일한 스팸을 여러 국가의 여러 IP 주소에서 발송하였고, 발송한 IP들이 좀비로 의심되는 정도가 높을 경우 해당 스팸 그룹을 봇넷 그룹으로 유추할 수 있을 것이다.

3.3 스팸봇넷 탐지 개념

본 논문에서는 각 스팸 발송 IP들과 이들이 속해 있는 스팸 그룹을 분석하여 봇넷과 좀비 PC 여부를 판단한다. 개별 스팸 발신자 IP와 스팸 그룹에 봇넷 의심정도를 나타내는 오염도를 측정하고, IP의 오염도를 그룹 오염도에 feedback하고 그룹 오염도 결과를 다시 그룹에 속한 IP들에게 feedback 함으로써 탐지 범위와 정확도를 높이고자 하였다. 그룹 오염도를 측정하는 이유는 개별적으로는 좀비로 의심되는 항목이 낮지만, 동일 스팸을 발송한 전체를 대상으로 판단했을 때 봇일 가능성이 높을 수 있기 때문이다. 예를 들어 1개의 좀비 IP에서 소수의 스팸메일만 발송할 경우 좀비라고 판단하기 어려우나, 이런 형태로 동



[그림 1] IP 오염도와 GROUP 오염도 계산 과정

일한 스팸을 보내는 IP들이 다수개일 경우 스팸 봇넷이라고 판단할 수 있다.

〔그림 1〕은 시간의 흐름에 따라 T0, T1, T2, T3, T4 각 단계에서 계산된 오염도 값을 다음 단계에 반영시켜 탐지 범위와 정확도를 높이는 과정을 보여주고 있다.

- T0 : 각 IP의 RBL 등록여부, 메일 발송수, MTA 여부, Received 필드 수 등 4가지 속성에 의해 IP 오염도 측정 (IP-1, IP-4, IP-n의 오염도가 high)
- T1 : 각 GROUP에 속한 IP들의 분산성, 지역적 다양성과 T0에서 계산된 IP 오염도를 기반으로 GROUP 오염도 측정 (GROUP-1, GROUP-n의 GROUP 오염도가 high)
- T2 : T1에서 측정한 GROUP 오염도를 각 그룹에 속한 IP들에게 상속시켜 IP별 오염도 재측정 (오염도가 높은 GROUP-1 그룹에 있던 IP-3의 오염도가 low에서 high로 변경)
- T3 : T2에서 측정한 IP 오염도를 관련 GROUP에 반영하여 GROUP 오염도 재측정 (IP-3가 포함되어 있던 GROUP-3도 오염도가 middle에서 high로 변경)
- T4 : T3 결과 오염도가 high인 GROUP을 스팸 그룹으로 결정하고, 해당 GROUP에 속해 있는 IP들을 IP오염도와 무관하게 모두 좀비 IP로 결정 (IP-5의 오염도가 middle이었으나, 스팸 그룹으로 결정된 GROUP-3에 속해 좀비 IP로 결정)

각 과정을 거치면서 IP 오염도와 GROUP 오염도의 변화는 아래 〔표 1〕에서 확인할 수 있다.

〔표 1〕 시간흐름별 IP 오염도와 GROUP 오염도 변화

시간	IP 오염도 high (좀비PC 의심 IP)	GROUP 오염도 high (봇넷 의심 GROUP)
T0	IP-1,IP-4,IP-n	-
T1	IP-1,IP-4,IP-n	GROUP-1,GROUP-n
T2	IP-1,IP-3,IP-4, IP-n	GROUP-1,GROUP-n
T3	IP-1,IP-3,IP-4, IP-n	GROUP-1,GROUP-3, GROUP-n
T4	IP-1,IP-4,IP-3, IP-5, IP-n	GROUP-1,GROUP-3, GROUP-n

본 논문에서는 프로토타입 형태로 개발하여 IP 오염도와 GROUP 오염도를 각각 1회에 한해 feedback하여 T4 단계에서 최종적으로 봇넷 그룹을 판단하도록 하였다. 하지만 향후 이 과정을 계속 반복하여 GROUP 오염도 값이 일정수준에서 안정화될 때 까지 반복하게 하여 feedback 횟수가 유동적으로 결정되어질 수 있도록 할 예정이다. 물론 이 과정에서 시스템의 성능이슈도 고려하여 feedback 횟수가 정해질 필요가 있다.

IV. 스팸트랩을 이용한 좀비 IP 추적 시스템 설계

2장에서 살펴본 기존의 연구들은 스팸봇넷을 탐지하여 행위를 모니터링하거나 예측하는 것을 주목적으로 연구되었으나, 본 연구에서는 탐지된 좀비 PC들을 치료 또는 네트워크 차단 등 직접적인 대응에 활용할 목적으로 연구하였다. 이 때문에 오탐을 최소화하는 것이 무엇보다 중요하여 다양한 탐지 요소들을 복합적으로 사용하고 봇넷 및 좀비 가능성을 정량화하였다. 앞서 2장에서 살펴 본 기존연구들과는 다음과 같이 차별화된 특성이 있다.

첫째, 각 IP들이 봇에 감염되었을 때 나타날 수 있는 특성들을 좀비 PC 탐지에 활용하였다. 기존의 연구들은 분산성, 지역성 등 그룹의 행위특성 분석을 통해 봇넷을 판정한 반면, 본 연구에서는 스팸을 발송한 IP의 RBL 등록 여부, 발송한 메일의 수, 발송 메일 서버의 MTA 여부, Received 필드 수 등 해당 IP 자체가 악성봇에 감염되어 자동으로 스팸을 발송하였을 때 나타날 수 있는 특성들을 측정하여 봇 탐지에 활용하였다.

둘째, 스팸그룹 클러스터링에 URL 뿐만 아니라 첨부파일도 사용하였다. 앞서 2장의 기존 연구들이 URL을 기반으로 스팸 그룹을 클러스터링하고 있는 것을 확인할 수 있었다. 대다수의 스팸메일이 URL을 포함하고 있어 스팸 그룹을 클러스터링하는데 가장 중요한 요인이 되는 것은 사실이지만, 실제 Cutwail, Bredolab 등 많은 봇넷들은 악성코드를 전파하기 위해 첨부파일을 포함하고 있어 이메일의 첨부파일도 스팸 그룹 클러스터링에 빠질 수 없는 중요한 요인이라고 생각한다.

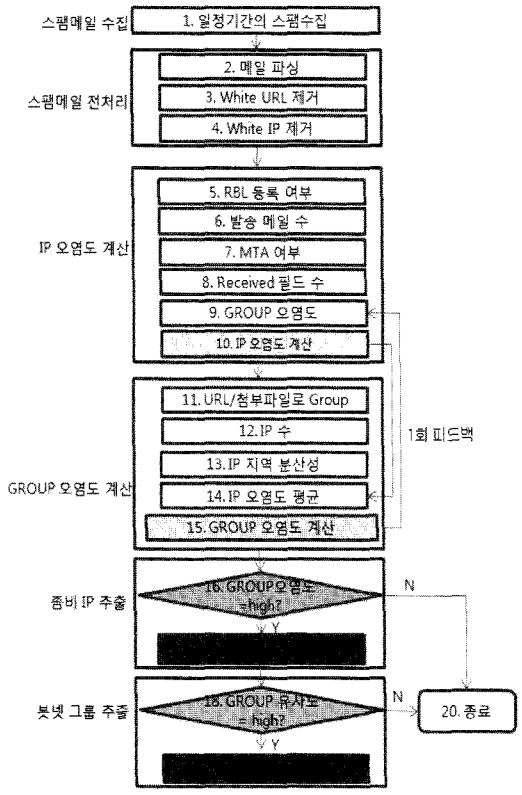
셋째, IP 오염도와 GROUP 오염도 결과를 상호 feedback하는 새로운 아이디어를 추가하였다. 본 연구에서는 기존의 연구와 달리 IP별 개별적인 봇의 특성과 스팸 그룹의 그룹 특성을 모두 이용하고, 그 결

과를 서로 feedback하게 하여 탐지 결과의 정확성을 높이고자 하였다.

이러한 특성을 반영하여 3장에서 제안한 기본 개념을 시스템으로 구현하기 위해 스팸메일 수집, 스팸메일 전처리, IP 오염도 측정, GROUP 오염도 측정, 좀비 IP 추출, 봇넷그룹 추출의 6개 과정을 거치도록 시스템을 설계하였다.

4.1 스팸메일 수집

- Step1. 일정기간의 스팸 수집 : 이메일 스팸트랩에 수집된 스팸을 실시간이 아닌 일정기간 동안 수집하여 batch 작업으로 수행한다. 이메일 스팸트랩 시스템은 스팸메일의 수집·분석·증거자료 보존을 위한 시스템으로 2008년부터 KISA에서 운영하고 있다. 9개 포털사의 1,000 여개 이상의 웹메일 계정과, 독자적으로 구축한 100개의 메일서버에 각각 1,000개의 이메일 주소를 설치하여 총 1만1천개 이상의 메일계정을 확보하여 스팸메일을 수집하고 있으며, 일일 100만~150만통 가량의 스팸메일이 수집되고 있다. 이메일 스팸트랩 시스템에서 사용되는 1만1천개 이상의 메일계정은 실제 사용자가 사용하고 있지 않은 가상의 메일계정으로, 이들 주소로 유입되는 메일은 대부분 Junk성 스팸메일로 볼 수 있다.



[그림 2] 스팸트랩에서 좀비 PC 및 봇넷 그룹 추출 절차

4.2 스팸메일 전처리

- Step2. 메일 헤더/Body 파싱 및 정규화 : 수집된 스팸메일들을 Subject, Source IP 주소, From 메일 주소, To 메일 주소, Time Stamp, Embedded URLs, Received 필드 수, 첨부파일명으로 파싱한다. Source IP 주소는 마지막 Received 필드의 IP 주소로 하고, Embedded URL은 1차 도메인을 기준으로 정규화한다.
- Step3. White URL 제거 : Body에 포함된 URL 중 포털, 내부 URL 등 정상 URL이 명확한 경우 White URL에 포함시키고, 그룹결정시 제외함으로써 False-Positive를 줄이고, 불필요한 연산을 막을 수 있도록 한다.
- Step4. White IP 제거 : SPF(Sender Policy Framework)에 의해 인가된 메일서버의 주소 또는 웹메일 서버 주소 등은 분석대상 IP 목록에서 제거하여 역시 False-Positive를 줄이고, 불필요한 연산을 막는다.

4.3 IP 오염도 계산

마지막 Received 필드의 IP 주소, 즉 스팸트랩에 최종적으로 메일을 전송한 IP 주소가 얼마나 좀비 PC의 성향을 띄고 있는지를 측정하는 단계이다. 각 IP별 오염도를 측정하기 위해 RBL 등록 여부, 해당 IP에서 발송된 메일의 수, MTA 여부, Received 필드 수, 포함되어 있는 그룹의 평균 오염도 등 5가지 속성을 기준을 사용하였다.

- Step5. RBL 등록 여부 : 해당 IP가 이미 스팸 RBL에 등록되어 있는지 확인한다. kisarbl.or.kr, sbl.spamhaus.org, list.dsbl.org 등 국내외 10개 RBL 사이트에게 블랙리스트 등록 여부를 질의하여 1개의 RBL 사이트에라도 등록되어 있을 경우 값을 1로 한다.
- Step6. 발송 메일 수 : 해당 IP에 의해 발송된

메일의 수를 카운트한다. 동일한 IP에서 발송된 메일의 수가 1개일 경우 0, 2개~10개일 경우 0.1, 11~20개일 경우 0.2, ..., 81~90개일 경우 0.9, 91개 이상일 경우 1로 한다.

- Step7. MTA 여부 : 최종 received 필드의 발송지 IP가 정상적인 MTA인지 확인하기 위해 해당 IP의 Reverse DNS 조회(PTR 조회)를 통해 해당 IP에 일치하는 도메인네임이 부여되어 있는지 검사한다. 정상적인 MTA를 거치지 않고 좀비 PC에서 직접 발송되었을 경우 PTR이 존재하지 않거나, 발송자 이메일 주소를 속이는 경우 IP주소와 도메인이 일치하지 않는 결과가 나오며 이 경우 값을 1로 한다.
- Step8. Received 필드 수 : 해당 IP에서 발송된 메일들의 Received from 필드 수의 평균값을 구한다. 일반적으로 아웃룩과 같은 MUA에서 메일을 작성하여 "전송" 버튼을 누르면 로컬 메일 서버인 MTA에게로 보내지고, 로컬 MTA는 수신자 측 MTA를 찾아 메일을 전송하고, 수신자는 수신자의 MUA를 통해 Pop3나 IMAP 프로토콜을 이용하여 수신자 MTA로부터 메일을 받아와 읽는 과정을 거친다[7]. 즉, 일반적인 메일 전송과정은 MUA-MTA-MTA-MUA의 전달과정을 거치게 되며 로컬 MTA와 수신자측 MTA에서 Received 필드를 추가하여 최소 2개 이상의 Received 필드가 존재하게 된다. 그러나 악성봇은 로컬 MTA를 통하지 않고 자체 SMTP 엔진을 가지고 보내는 경우가 많은데, 이 경우 로컬 MTA에서 기록되는 Received 필드가 생략된다. 해당 IP에서 발송한 메일들의 Received 필드 수의 평균이 2 미만일 경우 값을 1로 하고, 2 이상인 경우 0으로 한다.
- Step9. GROUP 오염도 : 해당 IP가 포함하고 있는 GROUP의 오염도 정도를 반영한다. 최초에는 GROUP 오염도 정보가 없으므로 0으로 계산하고 이후 Step15를 통해 GROUP 오염도가 산출되면 그 결과를 피드백 받아 IP 오염도 계산에 반영한다. 각 IP가 발송한 메일들에 다수개의 URL이나 첨부파일이 포함되어 있을 경우 각 GROUP의 오염도 평균값을 계산한다.
- Step10. IP 오염도 계산 : 앞서 Step 5~9의 결과를 토대로 IP의 오염도를 계산한다. IP 오염도는 각 Step의 오염도 결과값의 평균으로 한다. 즉, (Step5의 오염도 + Step6의 오염도 + Step7의 오염도 + Step8의 오염도 + Step9의 오염도) / 5 로 하고 결과값은 0에서 1 사이의 값을 가진다.

4.4 GROUP 오염도 계산

GROUP 오염도 계산 단계는 동일한 URL 또는 첨부파일을 포함하는 IP 그룹들이 얼마나 스팸 봇넷의 성향을 띄고 있는지를 측정하는 단계이다. GROUP 오염도 계산을 위해서 그룹내의 IP들의 다양성, IP들의 지역적 분산성, IP 오염도 평균 등 3가지 항목을 사용하였다.

- Step11. URL/첨부파일별 IP 그룹 분류 : 동일한 URL이나 첨부파일을 가진 IP들을 하나의 그룹으로 분류한다.
- Step12. 그룹내 IP 수 : 동일한 스팸메일이 얼마나 다양한 IP에서 발송되어졌는지를 측정하는 항목으로 1개의 IP에서 보냈을 경우 0, 2개~10개일 경우 0.1, 11~20개일 경우 0.2, ..., 81~90개일 경우 0.9, 91개 이상일 경우 1로 한다.
- Step13. 그룹내 IP들의 지역적 분산성 : URL 그룹내의 IP들이 지리적으로 위치한 국가를 확인하여 1개 국가에서 발송된 경우 0, 2개 국가의 경우 0.1, ..., 10개 국가의 경우 0.9, 11개 이상의 국가에서 발송된 경우 1로 한다.
- Step14. 그룹내 IP들의 오염도 평균 : 그룹내에 속해 있는 다수개의 IP들의 오염도 평균값을 구한다.
- Step15. GROUP 오염도 계산 : GROUP 내의 IP 수, IP의 지역적 분산성, IP 오염도 평균을 기반으로 해당 GROUP이 봇넷 그룹으로 의심되는 정도를 계산한다. 즉 GROUP 오염도는 (IP 다양성 + IP 지역적 분산성 + IP 오염도 평균) / 3 로 한다. GROUP 오염도가 계산되면 그 결과를 Step9로 전달하여 IP 오염도 계산에 반영하도록 한다. 단, GROUP 오염도 결과를 IP 오염도에 피드백하는 과정은 1회만 수행하도록 한다.

4.5 좀비 IP 추출

- Step16. 봇넷 의심 그룹 판별 : Step15를 통해 계산된 GROUP 오염도가 일정 수준 이상일 경

우 봇넷 그룹으로 간주한다. 단, GROUP 오염도가 어느 수준 이상인 경우를 봇넷으로 볼 수 있을지는 충분한 시뮬레이션을 거쳐야만 정확도를 높일 수 있는데, 본 논문에서는 몇 차례의 시뮬레이션 결과를 토대로 0.6 이상일 경우 봇넷 의심 그룹으로 간주하기로 한다.

- Step17. 좀비 List 추출 : Step16에 의해 해당 그룹이 스팸 봇넷으로 판정될 경우 IP 오염도와는 상관없이 그 GROUP에 속해 있는 모든 IP를 좀비 의심 IP DB에 추가한다.

4.6 봇넷 그룹 추출

- Step18. GROUP 유사도 측정 : 하나의 봇넷에서 동일한 좀비 PC들을 이용하여 다수개의 URL이나 첨부파일을 가진 스팸메일을 발송할 수 있다. Step16 과정에서 추출된 봇넷 의심 그룹들 간의 상호연관성을 알아보기 위해 두 그룹의 교집합과 합집합의 크기를 통해 샘플 집합의 유사도를 측정하는 자카드 계수(jaccard coefficient)[19]를 사용한다. 두 그룹에 공통적으로 속한 좀비 PC들의 수가 많을수록 두 그룹은 유사하고 상호연관성이 높다고 판단할 수 있다.

$$J(A,B)=\frac{|A\cap B|}{|A\cup B|}$$

- Step19. 봇넷 그룹 추출 : Step18의 GROUP 간 유사도 측정 결과 0.8 이상일 경우 이 두 그룹이 동일한 봇넷 그룹이라고 판단한다.
- Step20. 종료 : Step16에서 GROUP 오염도가 높지 않거나, Step19에서 GROUP간 유사도가 높지 않을 경우 종료한다.

V. 시뮬레이션 결과

4장에서 제안한 시스템을 검증하기 위해 이메일 스팸 트랩시스템에 2010년 8월 4일 오전 12시부터 오전 01시 까지 수집된 스팸메일을 대상으로 시뮬레이션하였다.

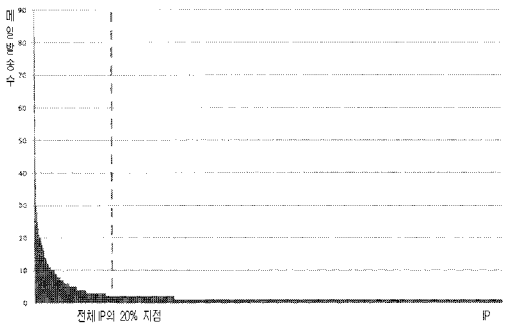
5.1 IP 오염도 결과

이메일 트랩시스템에 1시간 동안 수집된 스팸메일은 총 57,200통이었으며, 25,975개의 고유한 IP에서 발송되어 1개의 IP로부터 평균 2.2통의 스팸이 수신되었다. [표 2]는 IP들의 메일 발송 분포를 나타낸 것이다.

[표 2] 스팸 발송량 분포

스팸 발송량 (통/1hour)	1	2~10	11~20	21~30	31~40	41~50
IP 수	18,247	6,888	629	147	39	15
스팸 발송량 (통/1hour)	51~60	61~70	71~80	81~90	91~	합계
IP 수	6	2	0	2	0	25,975

가장 많은 스팸을 발송한 IP는 190.252.177.199로 1시간 동안 82통의 스팸을 발송하였다. 이 IP에서 발송된 스팸은 'Hello'라는 제목과 'report.document.doc.zip'라는 첨부파일을 가지고 있었다. report.document.doc.zip은 8월 3일을 전후하여 이메일을 통해 전 세계적으로 전파된 인터넷 웜으로써 실행시 트로이목마 프로그램에 감염된다. 단 1통의 스팸 메일을 보낸 IP도 전체의 70.2%인 18,247개나 되었다. [그림 3]은 스팸 발송 IP와 발송한 메일의 수를 그래프로 나타낸 것으로 X축의 왼쪽으로 갈수록 스팸발송이 많은 IP주소들이며, Y축은 각 IP에서 발송한 스팸메일의 수이다. 이 그래프는 거듭제곱법칙(Power Law)을 따르는 그래프와 유사한 형태를 띄고 있으며, 스팸 메일 발송량 상위 20%인 5,195개의 IP에서 전체 스팸의 59.24%에 해당하는 33,885통의 스팸메일이 발송되었다.



[그림 3] IP별 스팸발송량 그래프

스팸 발송자 IP를 국내외 10개의 RBL 사이트에 조회해 본 결과 82개 IP를 제외한 대부분의 IP가 이미 블랙리스트에 등록되어 있어 상습적으로 스팸을 발송하고 있는 IP들임을 알 수 있었다. 하지만, 샘플 스

팸을 분석한 시점이 스팸 수신 후 10여일이 지난 시점이었기 때문에 RBL 등록률이 높았을 수 있으며, 만약 스팸 수신 당일에 조회하였다면 결과가 달랐을 수도 있을 것으로 생각된다.

또한, 발송자 IP가 정상적인 MTA인지 확인한 결과 8,739개의 IP가 비정상적인 MTA로 추정된다. 전체 IP 중 Received 필드의 수가 2개 미만인 것은 20,201개였다. 그룹 오염도를 반영하기 이전에 IP 오염도를 결정하는 4가지 속성인 RBL 등록, 메일 발송수, MTA 유무, Received 필드수 등 각 속성의 오염도 수치가 높은 IP의 수는 다음과 같았다.

〔표 3〕 IP 오염도 속성별 IP 현황

구분	IP 수	전체 IP 대비 비율
RBL 등록 IP	25,893	99.7%
메일발송량 상위 20% IP	5,195	20.0%
MTA가 아닌 IP	8,739	33.6%
Received 필드 2개 미만 IP	20,201	77.8%

위의 4가지 속성값을 기준으로 계산한 평균 IP 오염도는 0.54였으며, GROUP 오염도 결과를 반영한 후에는 0.52로 약간 감소하였다.

5.2 GROUP 오염도 결과

앞서 스팸메일들을 분류하는 기준을 URL과 첨부파일로 결정하였다. 이렇게 분류된 그룹 중 어떤 그룹이 스팸봇넷 그룹인지를 결정하는 것은 GROUP 오염도이다. GROUP 오염도의 임계값을 높게 정할 경우 False-Positive는 낮아지나, False-Negative는 높아질 것이고, 임계값을 낮출 경우 그 반대의 현상이 발생하여 False-Positive와 False-Negative 모두를 적절한 수준으로 낮출 수 있는 임계값을 결정하는 것은 대단히 중요하다. 본 논문에서는 봇넷 그룹으로 판정하는 GROUP 오염도의 임계값을 수차례의 시뮬레이션을 통해 0.6으로 결정하였다.

시험에 사용된 총 57,200통의 스팸메일 중 URL을 포함하고 있는 스팸메일은 22,925통이었으며, 첨부파일을 가지고 있는 메일은 21,002통이었다. URL이나 첨부파일을 가지고 있지 않은 13,272통(23.2%)의 메일들은 그룹으로 분류되지 않아 분석대상에서 제외되었다.

URL과 첨부파일에 의해 분류된 고유한 그룹은 총 86개였으며, 이 그룹들의 평균 GROUP 오염도는 0.34였다. 86개의 그룹 중 봇넷그룹으로 판단하는 임계값인 0.6 이상의 GROUP 오염도를 보인 그룹은 17개로 이 그룹에 속한 IP는 총 16,030개였다. 이 좀비 PC로 의심스러운 IP에서 발송된 스팸은 총 43,694통으로 전체 스팸의 76.4%에 달했다. GROUP 오염도가 높은 Top 10 그룹의 IP 다양성, 지역(국가)분산성, IP들의 평균오염도는 〔표 4〕와 같았다.

〔표 4〕 GROUP 오염도 상위 Top 10

Group 오염도 순위	그룹명 (URL or attached file)	IP수	국가수	IP 평균 오염도	Group 오염도
1	picturewater.com	378	39	0.68	0.89
2	fastcola.com	991	52	0.68	0.89
3	colaocean.com	791	63	0.67	0.89
4	colaloud.com	2,342	69	0.67	0.89
5	listsound.com	1,675	66	0.67	0.89
6	ratherwent.com	1,697	79	0.51	0.84
7	elasticbuy.ru	137	31	0.48	0.83
8	report.document.doc.zip	2,956	85	0.29	0.76
9	vulturemix.ru	127	27	0.28	0.76
10	termtv.ru	133	36	0.28	0.76

이 외에도 shrimpfemale.ru, gotchaic.ru, twimg.com, rushguy.ru, tablepig.ru, utespace.ru, splateffect.ru 이 GROUP 오염도 0.6 이상인 것으로 측정되었다.

전체 스팸의 평균 IP 오염도가 0.52 이고, 평균 GROUP 오염도가 0.34 였는데, 봇넷 의심 그룹으로 탐지된 상위 5개 그룹은 이 평균을 훨씬 상회하는 것을 확인할 수 있다. 하지만, 8, 9, 10번째 그룹의 IP 오염도는 평균 IP 오염도에도 못 미치고 있지만, 최종적으로 봇넷 그룹으로 판정되었다. 이는 개별 IP에서는 좀비 PC의 특성을 적게 가지고 있지만 해당 그룹의 전체 IP들을 종합적으로 평가했을 때 봇넷에서 나올 수 있는 특징들을 강하게 가지고 있기 때문이었다.

예를 들어, report.document.doc.zip 라는 첨부파일을 가진 스팸 그룹은 정상적인 MTA를 통해 메일이 전송되었고, Received 필드 수도 2개 이상으로 IP 오염도 계산 결과 평균 0.29 밖에 되지 않았다. 하지만, 85개 국가의 2,956개 IP로부터 동일한 제목과 동일한 첨부파일을 가진 스팸 21,000통을 1시간 동안 발송하여 GROUP 오염도가 상당히 높게 계산되어

최종적으로 봇넷 의심 그룹으로 판별되었다. 이 그룹에서 발송된 스팸메일은 2010년 8월 3일을 전후하여 전세계적으로 급속하게 전파된 인터넷 웜으로 첨부파일은 트로이목마 기능을 가진 악성코드였다. report.document.doc.zip 메일은 모두 Received 필드가 2개 이상이었으며, 대부분 아웃룩이나 야후 메일과 같은 정상적인 mailer에서 발송되었다. 즉, 봇넷처럼 공격자의 명령에 의해 언제든 스팸을 보낼 수 있는 자체 SMTP 엔진을 가지지 않고, 사용자가 E-mail에 첨부된 파일을 실행하여 전파되는 웜 형태의 악성코드로 짐작할 수 있다. 이처럼 제안된 시스템은 개별 PC는 별로 의심의 여지가 없는 건전한 PC로 보이지만, 동일한 패턴을 가지는 IP들을 한데 모아 종합적으로 분석함으로써 비정상적인 그룹임을 판별할 수 있음을 확인할 수 있었다.

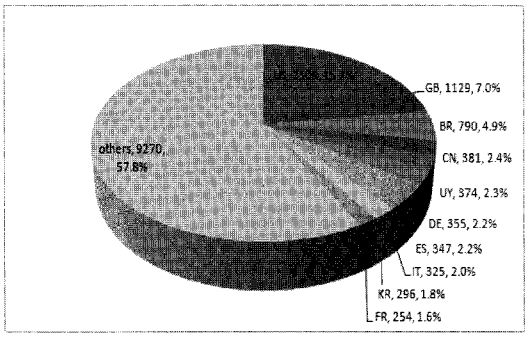
GROUP 오염도가 가장 높은 picturewater.com은 39개 국가의 378개 IP에서 61개의 서로 다른 선정적인 메일제목을 사용하여 389통의 스팸을 보냈으며, 성기능 강화 약품을 광고하는 사이트를 홍보하고 있었다. 이 그룹에서 보낸 모든 스팸메일은 Received 필드가 1개였으며, 특이하게도 mailer 필드가 모두 '0'으로 표시되어 있어 사람에 의한 발송보다는 기계에 의해 인위적으로 제작된 메일로 보여진다.

또, ratherwent.com라는 URL을 포함한 그룹은 service.ratherwent.com, room.ratherwent.com, show.ratherwent.com 등 수십 개의 서로 다른 2차 도메인을 사용하여 탐지를 회피하려는 시도가 있었다. 이처럼 2차 도메인을 random하게 바꾸지만 모두 동일한 사이트로 연결되는 경우를 자주 발견할 수 있었는데 제안한 시스템은 전처리 과정에서 URL을 모두 1차 도메인을 기준으로 분류함으로써 random한 2차 도메인을 사용한 우회시도를 차단할 수 있었다.

5.3 좀비 IP 추출 결과

본 연구에서는 제안한 시스템을 통해 1시간 동안 스팸트랩 시스템에서 수집된 57,200통의 스팸을 분석하여 좀비 PC로 의심스러운 105개국의 16,030개의 IP를 추출하였다. 이 좀비 의심 IP에서 전체 스팸의 76.4%에 해당하는 43,694통의 스팸이 발송되었다. 이 스팸 중에는 상업적 광고를 목적으로 한 것도 있었고, 악성코드를 감염시키기 위한 메일도 포함되어 있었다.

추출된 좀비 의심 IP를 국가별로 분류하면 미국, 영국, 브라질, 중국, 우크라이나 순이었으며, Top 10 국가 중 6개국은 『Symantec Global Internet Security Threat Report -Trends for 2009』의 Malicious Activity Top 10 국가에도 포함되어 있다.



〔그림 4〕 좀비 의심 IP Top 10 국가

5.4 탐지율 측정

제안한 시스템의 좀비 PC 탐지율과 미탐율을 측정하기 위해 KISA에서 운영하고 있는 DNS 싱크홀 시스템을 통해 이미 확보한 좀비 PC의 IP 리스트와 본 연구에서 사용한 샘플 스팸의 발신자 IP와 비교하였다.

DNS 싱크홀 시스템은 국내 주요 ISP/IDC/포털 DNS 서버에서 봇넷 C&C 서버의 RR(Resource Record) 정보를 변경하여 C&C 서버와 좀비 PC간의 채널을 차단하기 위한 시스템으로 KISA에서 운영하고 있다. 이 DNS 싱크홀 서버는 좀비PC가 C&C 서버로 연결을 시도할 때, KISA에서 운영하고 싱크홀 서버로 접속하도록 함으로써 좀비PC가 해커로부터 악용되는 것을 차단하고, 유입되는 좀비 PC들의 트래픽을 모니터링하여 좀비 PC의 IP 리스트를 DB화하고, 해당 좀비 IP가 속한 AS의 관리자에게 통보하거나 일반인에게 "악성 봇 감염 확인" 서비스를 제공해 주고 있다. 본 연구에서는 2010년 8월 4일 하루 동안 DNS 싱크홀에 유입된 트래픽에서 추출한 73,075개의 좀비 PC IP를 스팸메일 발송 IP와 비교하였다.

〔표 5〕 좀비 PC DB와 좀비 의심 IP 비교 결과

구분	DNS 싱크홀 서버의 좀비IP수(A)	스팸트랩 시스템		Num of A∩B	Num of A∩C
		총 IP수(B)	좀비의심 IP수(C)		
IP 수	73,075	25,975	16,030	5	4

DNS 싱크홀을 통해 보유하고 있는 좀비PC DB의 IP와 본 연구에서 사용했던 스팸의 전체 발송자 IP와 비교한 결과 5개의 IP가 일치하였으며, 이 IP들 중 4개의 IP는 제안한 시스템에서 좀비 의심 IP로 판정하였다. 충분한 량의 시험데이터는 아니었지만 주어진 데이터를 기반으로 한 탐지율 측정결과 80%의 탐지율을 보였다.

본 연구에서 샘플 스팸으로 삼았던 57,200통의 스팸 중 좀비PC DB에 등록되어 있는 IP에서 발송한 스팸은 〔표 6〕과 같았으며, 이들은 제안한 시스템에서 좀비 의심 IP로 판정되었다.

〔표 6〕 좀비 PC DB 중 좀비 의심 IP로 추출된 4개의 IP

IP	Subject	GROUP 명 (attached file or URL)
122.34.229.142	Hello	report.document.doc.zip
125.242.13.186	Armani bangle will surely raise your status and make you look rich. 이하생략	shrimpfemale.ru
	Upgrade to Microsoft Office 2008 Standart Edition now for less than $200.	s.twimg.com
211.173.128.20	Have an upgraded Adobe Acrobat 9 Pro for MAC for only $59.95.	s.twimg.com
	Once you see our watches you will dispose your old ones.	gotchaic.ru
59.27.18.81	Gucci wallets are known to be most qualitative and fashionable. 이하생략	tablepig.ru

〔표 7〕 4개 IP가 속한 스팸봇넷 그룹 및 IP 수

그룹명	포함 IP 수	GROUP 오염도
report.document.doc.zip	2,956	0.76
shrimpfemale.ru	183	0.76
gotchaic.ru	136	0.76
twimg.com	250	0.76
tablepig.ru	51	0.62

4개의 IP가 속해 있었던 5개 그룹의 GROUP 오염도가 모두 0.6을 초과하는 것으로 계산되었었다. 본 연구의 결과로 DNS 싱크홀 시스템에 의해 이미 좀비 PC로 알려진 4개의 좀비 IP 이외에도 이들이 속해 있는 스팸 봇넷의 수많은 알려지지 않은 좀비 IP들이 탐지될 수 있음을 확인할 수 있었다.

좀비 DB에는 있었으나 본 연구 결과 좀비 의심 IP로 탐지되지 않은 1개의 IP는 210.118.228.3이었다. 이 IP는 "Affordable advertising?"이라는 제목으로 단 1개의 메일을 발송하였으며, URL이나 첨부파일이 없어 그룹으로 조차 설정되지 않아 분석대상에서 제외되었었다.

5.5 그룹 유사도 측정 결과

URL과 첨부파일에 의해 분류한 총 86개의 그룹들 간의 유사도를 측정한 결과 상위인 경우도 2~8% 정도의 낮은 유사도가 측정되었다.

〔표 8〕 그룹 유사도 측정 결과(Top 10)

번호	그룹 A	그룹 B	Num of A	Num of B	유사도 (A∩B) / (A∪B)
1	viagra-gogo.com	anshindou.biz	3	1	0.333
2	appledvd.me	viagra-gogo.com	2	3	0.25
3	colaocean.com	colaloud.com	4285	3907	0.08
4	fastcola.com	listsound.com	991	1675	0.072
5	picturewater.com	fastcola.com	378	991	0.034
6	picturewater.com	listsound.com	378	1675	0.03
7	twimg.com	vulturemix.ru	250	127	0.027
8	rushguy.ru	utespace.ru	79	44	0.025
9	shrimpfemale.ru	twimg.com	183	250	0.024
10	vulturemix.ru	gotchaic.ru	127	136	0.019

그룹 구성원 수가 상당히 적은 1, 2번째 그룹을 제외하고 3번째로 높은 그룹 유사도를 보인 colaocean.com과 colaloud.com의 경우 606개의 IP가 두 그룹에 공통적으로 존재하고 있고, URL 이름에서도 유사성을 보여 동일한 봇넷이거나 봇넷 소유자가 동일할 가능성이 있는 등 상당히 연관성이 높은 그룹들로 추정할 수 있다.

하지만 전반적으로 그룹간 동일한 좀비 PC를 포함하는 비율이 상당히 낮으며, 동일한 그룹에서 2개 이상의 서로 다른 종류의 스팸메일을 발송하는 경우가 많지 않은 것으로 나타나고 있다. 이러한 결과는 본 연구에서 사용한 샘플 스팸의 수집기간이 1시간으로 하나의 봇넷 그룹이 2개 이상의 서로 다른 종류의 스팸을 발송하기에는 상당히 짧은 기간이었기 때문일 수

도 있을 것으로 생각된다. 향후 스팸 수집 기간을 1시간이 아닌 1일 이상으로 늘일 경우 그룹간 유사도가 높은 그룹들이 나타날 수 있을 것으로 예측한다.

VI. 결론 및 향후 연구 방향

6.1 결론

본 연구에서는 KISA에서 운영하고 있는 이메일 트랩 시스템에서 수집된 스팸메일을 분석하여 좀비 PC 및 봇넷을 추출하는 연구를 진행하였다. 본 연구에서는 스팸메일을 분류하기 위해 스팸메일 내의 URL 또는 첨부파일을 사용하였다. 스팸메일은 광고하고자 하는 URL이나 악성코드 전파를 위한 첨부파일을 통해 응집력을 가진 스팸 그룹으로 분류가 가능하며 이 스팸그룹은 동일한 봇넷에 의해 발송된 스팸메일들일 가능성이 높다. 또한, 각 스팸 그룹이 어느 정도 봇넷 그룹의 특징을 가지는지를 측정하는 GROUP 오염도와 그룹을 구성하는 각각의 IP들이 좀비 PC의 특성을 얼마나 가졌는지를 측정하는 IP 오염도라는 개념을 도입하고 이 두개 오염도의 결과값을 서로 feedback하여 봇넷 탐지범위와 탐지 정확도를 높이고자 하였다.

본 연구에서 제안한 시스템을 이메일 스팸트랩 시스템에 1시간 동안 수집된 스팸메일에 적용한 결과, 105개국 16,030개의 좀비 의심 IP를 추출하는 성과를 얻었다. 이 좀비 의심 IP들은 악성코드에 감염되었을 것으로 보여지는 상당 수준의 징후를 가지고 있었다. 봇넷은 각종 사이버범죄에 사용되면서 갈수록 지능화되고 은닉성이 높아지고 있어 탐지가 쉽지 않다. 본 연구는 국가 차원의 이메일 스팸 수집 시스템인 스팸트랩 시스템을 활용하여 상시적으로 봇에 감염된 좀비 PC를 추출하여 조치하도록 함으로써 봇넷에 의한 다양한 사이버 범죄를 사전에 예방하는데 기여할 수 있을 것으로 생각된다.

6.2 향후 연구 방향

본 연구에서는 스팸메일 분석을 통해 스팸봇넷을 추적하는 시스템을 설계하고 이를 검증하였다. 향후 연구에서는 아래의 몇 가지 사항을 개선함으로써 탐지 정확도를 높이고, 타 시스템과의 연동을 통하여 종합적인 봇넷 탐지·대응이 가능한 시스템으로 발전시킬 예정이다.

첫째, 스팸 그룹을 클러스터링할 수 있는 요소를 확대할 예정이다. 본 연구에서는 URL이나 첨부파일을 통해 클러스터링하였으나, 이 2가지 요소가 없는 스팸메일은 클러스터링이 불가능하다. 따라서 URL이나 첨부파일이 없는 경우 스팸메일의 파일사이즈, 해쉬값 등 좀 더 다양한 요소를 활용하여 클러스터링하는 방안을 고려할 예정이다.

둘째, 학습에 의한 동적 가중치와 임계값을 구할 수 있도록 할 예정이다. 본 연구에서는 IP 오염도와 GROUP 오염도 계산에 사용한 각 항목의 가중치와 봇넷 의심그룹 판별 임계값을 정적인 값으로 주었으나, 향후 다수의 시뮬레이션 결과에 따라 이 값을 최적화 시키고 나아가 학습에 의해 동적으로 가중치와 임계값이 계산되게 하여 탐지 정확도를 향상시킬 예정이다.

셋째, 호스트기반 봇넷 탐지시스템과 연동시킬 예정이다. 스팸메일에 포함된 URL과 첨부파일의 행위를 모니터링하여 스팸메일 발송의도를 파악할 수 있도록 할 예정이다. 스팸메일은 광고 목적뿐만 아니라 악성코드를 감염시키기 위한 용도로도 사용되고 있다. 스팸메일에 포함된 URL을 방문하거나 첨부파일을 실행함으로써 악성 봇, 트로이목마, 스파이웨어 등 다양한 악성코드에 감염될 수 있다. 스팸메일의 이러한 행위를 탐지하기 위하여 URL과 첨부파일을 호스트기반 행위 분석 시스템에 전달하여 해당 스팸의 악성행위 여부를 판별할 수 있도록 할 예정이다.

넷째, 네트워크기반 봇넷 탐지시스템과 연동시킬 예정이다. 본 연구를 통해 확보한 좀비 의심 IP들의 네트워크 트래픽을 모니터링하여 이들 IP로 송수신되는 명령전달이나 악성행위가 포착되는지 확인함으로써 좀비 의심 IP를 좀비 IP로 확신할 수 있도록 할 예정이다. 또한 이들 좀비 IP들이 어떤 C&C 서버로부터 명령을 전달받고, 어떤 다운로드서버로부터 악성코드를 업데이트 받는지 등 좀비 IP와 연관되어 있는 모든 서버들을 추적할 수 있도록 시스템을 확장할 예정이다.

참고문헌

[1] Y. Xie, F. Yu, K. Achan, R. Panigrahy, G. Hulten, and I. Osipkov, "Spamming Botnets: Signatures and Characteristics," SIGCOMM'08, pp.17-22, Aug. 2008

[2] J.P. John, A. Moshchuk, S.D. Gribble, and A. Krishnamurthy, "Studying Spam-

ming Botnets Using Botlab," USENIX, 2009

[3] A. Mislove, M. Marcon, K.P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and Analysis of Online Social Networks," Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, 2007

[4] F. Li, and M.H. Hsieh, "An Empirical Study of Clustering Behavior of Spammers and Group-based Anti-Spam Strategies," CEAS 2006-3rd Conference on Email and Anti-Spam, 2006

[5] A. Ranachandran, N. Feamster, and S. Vempala, "Filtering Spam with Behavioral Blacklisting," CCS'07, 2007

[6] L.H. Gomes, C. Cazita, and W. Meira, "Characterizing a Spam Traffic," IMC'04, 2004

[7] A. Ranmachandran and N. Feamaster, "Understanding the Network-Level Behavior of Spammers," SIGGOMM'06, 2006

[8] H. Husna, S. Phithakkinukoon,A. Palla, and R. Dantu, "Behavioral Blacklisting," CCS'07, 2007

[9] M. Bailey, E. Cooke, F. Jahnian, Y. Xu, and M. Karir. "A survey of botnet technology and defenses," In 2009 Cybersecurity Applications and Technology Conference for Homeland Security, pp. 299-304, 2009

[10] 정현철, 이상진, "국가 봇넷 대응 프레임워크 제안," 2009년도 정보보호학회 동계학술발표대회 논문집, KIISC, 19(2) pp. 193-197, 2009년 12월.

[11] Wikipedia, http://en.wikipedia.org/wiki/E-mail

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

[13] BBC News, Criminals 'may overwhelm the web', http://news.bbc.co.uk/2/hi/business/6298641.stm, 2007

[14] The Register, "DDoS attacks fall as crackers turn to spam," http://www.theregister.co.uk/2007/05/02/dos_trends_symantec/, 2007.

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

[16] London Action Plan, http://www.londonactionplan.com/

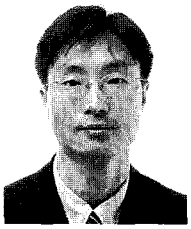
[17] 조선일보, http://biz.chosun.com/site/data/html_dir/2010/06/11/2010061101547.html, 2010

[18] P. Graham, "Different Methods of Stopping Spam," http://www.windowsecurity.com/, 2003

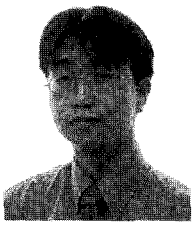
[19] L. Lee, "Measures of distributional similarity," Proceedings of the 37th annual meeting of the Association for Computational Linguistics on Computational Linguistics, 1999

[20] L. Zhuang, J. Dunagan, D.R. Simon, H.J. Wang, and J.D. Tygar, "Characterizing Botnets From Email Spam Records," LEET'08 Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, 2008

〈著者紹介〉



정 현 철 (HyunCheol Jeong) 종신회원
1989년 2월: 서울시립대학교 전산통계학과 졸업
1999년 8월: 광운대학교 전자계산학과 석사
2006년 9월~2008년 8월: 고려대학교 정보보호대학원 박사과정 수료
1996년 7월~현재: 한국인터넷진흥원 인터넷침해대응센터 연구개발팀장
〈관심분야〉 침해사고대응, 융합서비스보안, 네트워크보안, 컴퓨터 포렌식



김 휘 강 (Huy Kang Kim) 정회원
1998년2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년5월~2010년2월: 엔씨소프트 정보보안실장, Technical Director
2010년3월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직

이 상 진 (Sangjin Lee) 종신회원
1987년 2월: 고려대학교 수학과 이학사
1989년 2월: 고려대학교 수학과 이학석사
1994년 2월: 고려대학교 수학과 이학박사
1989년 2월~1999년 2월: 한국전자통신연구원 선임연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 부채널 공격, 대칭키 암호의 분석 및 설계, 정보은닉이론, 컴퓨터 포렌식

오 주 형 (Oh-Joo Hyung) 정회원
2005년 2월: 인제대학교 컴퓨터과학과 졸업(학사)
2008년 2월 성균관대학교 전자전기 및 컴퓨터공학과 졸업(석사)
2008년~ 한국인터넷진흥원 주임연구원
〈관심분야〉악성코드 분석, 네트워크 보안, 침해사고 분석