情 報 保 護 學 會 誌
第22卷 第8號, 2012. 12

# 이메일 스팸트랩 기반 좀비PC/봇넷그룹 탐지 현황

이 태 진*, 정 현 철*, 이 재 일*

요 약

이메일 스팸메일의 대부분은 악성코드에 감염된 좀비PC에 의해 발송된다. '11년 시만텍 보고서에 따르면 한국발 좀비PC에 의한 스팸메일 발송이 세계 1위를 차지했으며, '12년에도 상위수준을 유지하고 있다. 본 논문에서는 이메일의 패턴 분석을 통해 좀비PC 및 같은 공격명령을 받은 봇넷그룹을 자동으로 탐지하는 시스템을 개발하고, 이를 통해 산출된 다양한 데이터에 대한 분석결과를 제시한다. 좀비PC 및 봇넷그룹 탐지결과는 스팸메일 차단기술로 활용 가능할 뿐 아니라, 악성코드 유포동향 파악 등 다양한 목적의 분석에 활용 가능하다.

## 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 지하경제 세계에서 0.03달러가량에 거래되고 있는데, 수만 대의 봇으로 구성된 봇넷은 수백 달러에 팔리고 있다[1]. 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[2].

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[3]. M. Bailey의 논문에서도 봇의 가장 중요한 사용처 중의 하나가 스팸발송이라고 말하고 있다[4]. 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.

보안업체 MessageLabs社의 조사결과, 전체 스팸메일의 83.2%가 봇넷에 감염된 좀비PC로부터 발송된 것

본 연구는 방송통신위원회의 정보보호원천기술개발 사업의 연구결과로 수행되었음(KCA-2012-(10912-06001))
* 한국인터넷진흥원 (tjlee@kisa.or.kr, hcjung@kisa.or.kr, jilee@kisa.or.kr)

이라고 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[5].

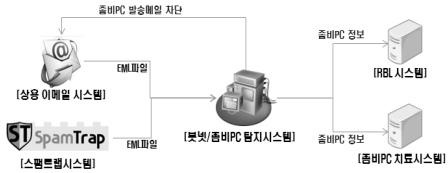
이처럼 봇넷이 스팸메일 발송의 주요 근원지로 부각됨에 따라 스팸대응 국제조직에서도 봇넷에 의한 스팸메일 차단을 위한 노력을 시작하였다. 영국의 OFT (Office of Fair Trading)와 미국의 FTC(Federal Trade Committee) 주도로 운영되고 있는 국제 스팸대응 조직인 LAP(London Action Plan)에서는 국가 간 스팸 전송자에 대한 법적처벌 및 국제 대응조직간 상호협력 등 법·제도 및 정책적인 이슈를 주로 다루어 왔다[6]. 하지만, 최근 LAP에서도 스팸방지를 위한 각국의 정책 및 국경 간 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.

본 논문에서는 스팸메일을 발송시키는 좀비PC 및 봇넷에 대한 탐지 시스템 개발을 통해 산출된 결과 데이터를 검토하고, 그 의미를 분석한다. 2장은 이메일 스팸트랩 시스템과 연동하여 좀비PC 및 봇넷그룹을 탐지하는 기술을 설명하고, 3장에서는 좀비PC 및 봇넷그룹에 대한 탐지결과, 4장에서는 탐지된 정보를 이용한 활용방안 및 의미, 5장에서는 결론을 제시한다.

## Ⅱ. 스팸트랩 기반 좀비PC 및 봇넷그룹 탐지

### 2.1. 시스템 구성

여기서는 이메일 스팸트랩 시스템에 대해 간략히 설명한다. 공격자는 인터넷상에 노출된 이메일 주소를 자동으로 크롤링한후, 스팸 컨텐츠를 받아 자동으로 스팸메일을 발송한다. 이에 따라, 이메일 스팸트랩 시스템은 100개의 가상 메일서버 도메인 및 포털사이트 등에서 확보한 메일계정들을 인터넷 상에 노출시켜서 스팸메일을 보내도록 유도한다. [그림 2]는 이메일 스팸트랩 시스템을 통해 최근30일간(12년10월27일~11월25일)에 수집된 유입IP수, 스팸메일수를 나타낸다. 일평균 약 20여만통 스팸메일, 약 15,000여개 IP에서 스팸메일이 유입되고 있음을 알 수 있다. 이 정보를 기반으로 좀비PC 및 봇넷그룹을 탐지한다.

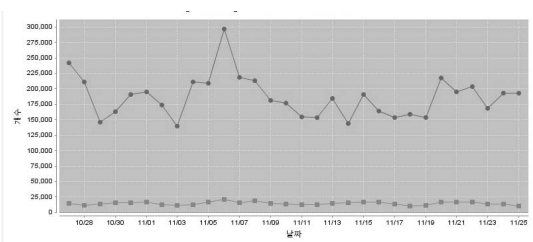



〔그림 1〕 좀비PC/봇넷그룹 탐지기술 구성도

본 논문에서 산출된 데이터는 KISA가 보유한 이메일 스팸트랩 시스템과 연동하여, 좀비PC 및 봇넷 그룹을 탐지하였다. 향후, 상용환경의 이메일 시스템과 연계하여 결과 데이터를 분석할 예정이다.

### 2.2. 이메일 스팸트랩 시스템

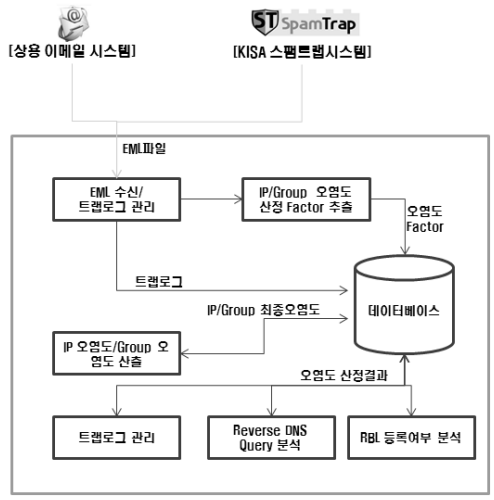
여기서는 이메일 스팸트랩 시스템에 대해 간략히 설명한다. 공격자는 인터넷상에 노출된 이메일 주소를 자동으로 크롤링한후, 스팸 컨텐츠를 받아 자동으로 스팸메일을 발송한다. 이에 따라, 이메일 스팸트랩 시스템은 100개의 가상 메일서버 도메인 및 포털사이트 등에서 확보한 메일계정들을 인터넷 상에 노출시켜서 스팸메일을 보내도록 유도한다. [그림 2]는 이메일 스팸트랩 시스템을 통해 최근30일간(12년10월27일~11월25일)에 수집된 유입IP수, 스팸메일수를 나타낸다. 일평균 약 20여만통 스팸메일, 약 15,000여개 IP에서 스팸메일이 유입되고 있음을 알 수 있다. 이 정보를 기반으로 좀비PC 및 봇넷그룹을 탐지한다.




〔그림 2〕 이메일 스팸트랩 시스템으로 유입된 스팸메일 및 IP수

### 2.3. 좀비PC 및 봇넷그룹 탐지 시스템

상용 이메일 시스템, 스팸트랩 시스템을 통해 유입된 EML 파일을 기반으로 좀비PC 및 봇넷그룹을 탐지하는 시스템 구조는 [그림 3]과 같다. 유입된 EML 파일



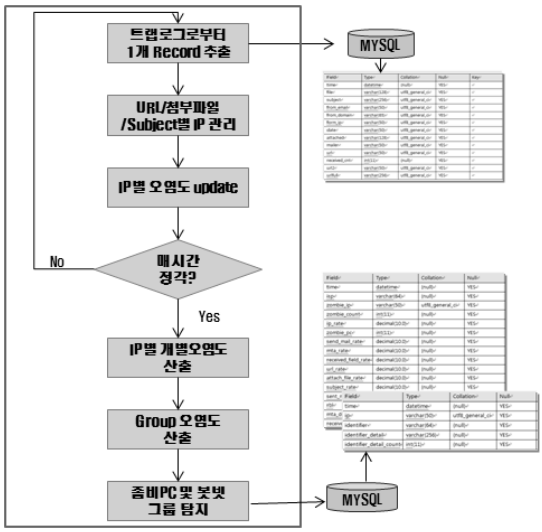

〔그림 3〕 좀비PC/봇넷그룹 탐지시스템 구성도

은 파싱하여, 트랩로그 형태로 관리한다. 트랩로그에서 좀비PC/봇넷그룹 탐지에 필요한 주요 요소들을 식별하고, 이 정보를 기반으로 IP 오염도/Group 오염도를 산출한다. 산출된 정보는 다양한 형태의 통계작성을 위해 데이터베이스에 저장되며, IP 오염도/Group 오염도 산정을 위해 Reverse DNS Query, RBL 등록여부 등을 세부적으로 분석하는 모듈이 사용된다.

[표 1]은 좀비PC 및 봇넷그룹을 탐지하는 위한 주요 요소를 나타낸다. 각 IP가 좀비PC인지 여부를 판단하기 위해 발신메일수, MTA, Received Field, RBL 값들이 사용되고, 봇넷그룹 여부를 판단하기 위해 그룹내 IP수,

〔표 1〕 좀비PC/봇넷그룹 탐지 요소

| 구 분 | 항 목 | 주요 내용 |
|---|---|---|
| IP 오염도 | 발신 메일수 | 시간당 발신메일수가 많을수록 좀비 PC 가능성 높음 |
| | RBL | 스팸발송 IP로 알려져 있는 경우, 좀비 PC 가능성 높음 |
| | MTA | 거쳐온 메일서버 도메인과 IP가 불일치 할 경우, 좀비PC 가능성 높음 |
| | Received Field | 거쳐온 메일서버 개수가 평균 2개 미만일 경우, 좀비PC 가능성 높음 |
| Group 오염도 | IP 분포 | IP 국가가 다양할수록 봇넷 Group 가능성 높음 |
| | IP 개수 | IP 개수가 많을수록 봇넷 Group 가능성 높음 |
| | IP 평균 오염도 | 평균 오염도가 높을수록 봇넷 Group 가능성이 높음 |



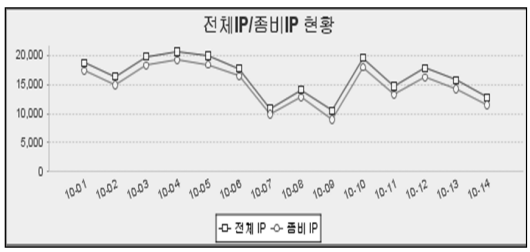

〔그림 4〕 좀비PC/봇넷그룹 탐지 절차

국가 분포수, IP오염도 평균값들이 사용된다.

[그림 4]는 좀비PC/봇넷그룹 탐지 요소를 기준으로 EML 파일 유입시, 처리되는 절차를 나타낸다. 좀비PC 및 봇넷그룹 탐지의 세부 알고리즘은 기 연구한 논문을 참고하면 된다[7].

## Ⅲ. 좀비PC 및 봇넷그룹 탐지 현황

KISA 이메일 스팸트랩 시스템으로 유입된 스팸메일을 분석하여 좀비PC 탐지현황에 대해 소개한다. [그림 5]는 2012년 10월1일부터 14일까지 2주간 유입된 스팸메일에 대한 분석결과를 나타낸다.




〔그림 5〕 전체 유입IP 수 및 좀비IP 수

이메일 스팸트랩 시스템을 통해 유입된 전체IP수는 총 229,170개이며 이중 좀비IP로 판단한 IP수는 209,473개로 91.41% 탐지율을 기록하였다. 날짜별 세

〔표 2〕 유입된 전체IP 및 좀비IP 탐지 현황

| 날짜 | 좀비 IP | 전체 IP | 탐지율 |
|---|---|---|---|
| 10-01 | 17,330 | 18,714 | 92.60% |
| 10-02 | 14,950 | 16,358 | 91.39% |
| 10-03 | 18,296 | 19,786 | 92.47% |
| 10-04 | 19,172 | 20,621 | 92.97% |
| 10-05 | 18,441 | 19,923 | 92.56% |
| 10-06 | 16,435 | 17,741 | 92.64% |
| 10-07 | 9,902 | 10,819 | 91.52% |
| 10-08 | 12,784 | 14,057 | 90.94% |
| 10-09 | 8,985 | 10,507 | 85.51% |
| 10-10 | 17,966 | 19,596 | 91.68% |
| 10-11 | 13,216 | 14,709 | 89.85% |
| 10-12 | 16,227 | 17,822 | 91.05% |
| 10-13 | 14,242 | 15,739 | 90.49% |
| 10-14 | 11,527 | 12,778 | 90.21% |
| **종 합** | **209,473** | **229,170** | **91.41%** |

부 탐지결과는 [표 2]와 같다.

전체 유입된 메일수 대비 좀비PC에서 발송된 메일수를 비교해보면, 총 3,013,130개 메일중 2,896,939개 메일을 스팸메일로 탐지하여 96.14%를 탐지하였다. 이는 좀비PC에서의 메일 발송량이 정상PC보다 많기 때문인 것으로 판단된다. [표 3]는 전체IP/좀비IP에서의 메일발생량을 나타낸다.

[표 4]는 국내 ISP별 좀비PC 분포현황을 나타낸다. ISP별로 탐지된 좀비PC 정보는 ISP 사업자에게 제공하여 조치를 유도하는 등의 정책적 수단을 통해, 좀비PC 치료를 유도할 수 있다.

[표 5]는 유입된 좀비PC의 국내외 분포를 나타낸다. 분석결과를 보면, 약 97%는 해외에서 유입된 것으로 분석되었다.

## Ⅳ. 활용 방안

3장에서는 좀비PC에 대한 탐지결과를 제시하였다. 여기서는 탐지된 좀비PC 정보를 이용한 활용방안 및 그 의미를 제시한다.

〔표 3〕 유입된 전체IP/좀비IP에서의 메일발생 현황

| 날짜 | 좀비IP Mail | 전체 Mail | 탐지율 |
|---|---|---|---|
| 10-01 | 243,445 | 252,662 | 96.35% |
| 10-02 | 215,890 | 225,140 | 95.89% |
| 10-03 | 235,603 | 246,035 | 95.76% |
| 10-04 | 205,967 | 214,652 | 95.95% |
| 10-05 | 224,251 | 233,654 | 95.98% |
| 10-06 | 222,688 | 231,221 | 96.31% |
| 10-07 | 211,020 | 216,378 | 97.52% |
| 10-08 | 192,068 | 198,434 | 96.79% |
| 10-09 | 159,114 | 168,452 | 94.46% |
| 10-10 | 209,830 | 218,370 | 96.09% |
| 10-11 | 226,207 | 233,767 | 96.77% |
| 10-12 | 209,309 | 218,306 | 95.88% |
| 10-13 | 173,281 | 181,280 | 95.59% |
| 10-14 | 168,266 | 174,779 | 96.27% |
| **종합** | **2,896,939** | **3,013,130** | **96.14%** |

### 4.1. 봇넷그룹 탐지

공격자는 다수의 좀비PC를 이용해 자신이 광고하고자 하는 스팸메일을 보낸다. 따라서, 특정 시간에 같은 스팸메일을 전송하는 좀비PC들은 공격자가 보유한 봇넷그룹으로 추정할 수 있다. [그림 6]은 봇넷그룹의 개념적인 동작절차를 나타낸다.

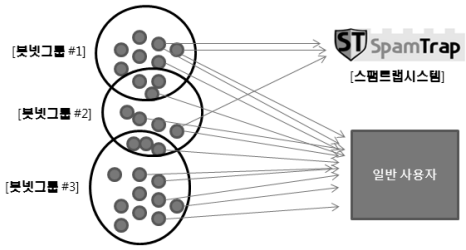
같은 스팸메일임을 판단하는 기준은 동일한 메일제목, 동일한 첨부파일, 이메일 본문에 광고하는 URL이

〔표 5〕 좀비IP의 국내외 현황 비교

| 날짜 | 국외 좀비PC | 국내 좀비PC | 총 계 | 국내 비율 |
|---|---|---|---|---|
| 11-09 | 12,856 | 344 | 13,200 | 2.61% |
| 11-10 | 11,950 | 334 | 12,284 | 2.72% |
| 11-11 | 11,412 | 423 | 11,835 | 3.57% |
| 11-12 | 10,873 | 541 | 11,414 | 4.74% |
| 11-13 | 11,946 | 350 | 12,296 | 2.85% |
| 11-14 | 13,449 | 323 | 13,772 | 2.35% |
| 11-15 | 15,498 | 330 | 15,828 | 2.08% |
| 평균 | 12,569 | 378 | 12,947 | 2.99% |

〔표 4〕 주요 ISP별 좀비PC 탐지 현황

| ISP | 10-01 | 10-02 | 10-03 | 10-04 | 10-05 | 10-06 | 10-07 | 10-08 | 10-09 | 10-10 | 10-11 | 10-12 | 10-13 | 10-14 | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Total | 17,330 | 14,950 | 18,296 | 19,172 | 18,441 | 16,435 | 9,902 | 12,784 | 8,985 | 17,966 | 13,216 | 16,227 | 14,242 | 11,527 | 209,473 |
| [국외 좀비PC] | 16,978 | 14,618 | 17,857 | 18,653 | 17,906 | 15,879 | 9,629 | 12,225 | 8,640 | 17,476 | 12,846 | 15,904 | 14,119 | 11,253 | 203,983 |
| KT | 136 | 117 | 182 | 225 | 224 | 247 | 75 | 262 | 141 | 218 | 163 | 141 | 38 | 66 | 2,235 |
| LG U+ | 88 | 94 | 121 | 124 | 157 | 124 | 74 | 124 | 72 | 105 | 95 | 66 | 19 | 83 | 1,346 |
| SK브로드밴드 | 34 | 27 | 35 | 52 | 42 | 61 | 25 | 51 | 34 | 42 | 26 | 36 | 12 | 20 | 497 |
| KRNIC | 4 | 8 | 7 | 14 | 24 | 25 | 34 | 41 | 46 | 50 | 25 | 39 | 29 | 34 | 380 |
| 티브로드 | 10 | 15 | 13 | 18 | 19 | 21 | 6 | 11 | 5 | 6 | 10 | 8 | 5 | 31 | 178 |
| CJ헬로비전 | 12 | 12 | 13 | 15 | 7 | 16 | 13 | 9 | 9 | 13 | 10 | 5 | 4 | 11 | 149 |
| 씨앤앰 | 5 | 6 | 5 | 9 | 7 | 13 | 12 | 8 | 6 | 7 | 3 | 6 | 4 | 7 | 98 |




〔그림 6〕 봇넷그룹의 개념적인 동작 절차

동일한 경우 등이 가능하다. 여기서는 위 3가지 기준으로, 동일한 스팸메일을 발송한 발신IP들을 그룹핑하고, 이들에 대해 분석한다.

[표 6]는 위에서 분석된 특정 좀비PC와 관련된 봇넷 그룹 탐지결과를 나타낸다. 좀비PC는 37개 국가, 236개 IP에서 동일한 스팸광고(http://gragh.ru)를 동일한 시간에 한 봇넷그룹이다. 여기서 개별IP 오염도는 좀비PC 탐지시스템에서 좀비PC 여부를 산정하는 기준을

〔표 6〕 Case #1 좀비PC가 속한 봇넷그룹 탐지결과

| 국가 | ISP | IP | 개별IP오염도 |
|---|---|---|---|
| KR | KT | 175.199.166.245 | 0.6 |
| IN | | 123.176.36.242 | 0.6 |
| KR | KT | 218.146.62.69 | 0.6 |
| KR | KT | 121.163.78.234 | 0.6 |
| KR | KT | 175.199.166.146 | 0.6 |
| VN | | 123.27.151.58 | 0.6 |
| PL | | 88.199.147.44 | 0.6 |
| VN | | 123.27.158.155 | 0.46 |
| RU | | 88.86.209.179 | 0.6 |
| TW | | 1.165.71.48 | 0.46 |
| KR | CJ헬로비전 | 113.130.182.91 | 0.6 |
| ID | | 118.98.35.92 | 0.6 |
| IN | | 122.176.78.109 | 0.6 |
| CN | | 110.210.94.221 | 0.46 |
| NZ | | 60.234.152.65 | 0.6 |
| IL | | 84.95.112.208 | 0.6 |
| TW | | 219.84.218.6 | 0.46 |
| VN | | 113.167.111.86 | 0.6 |
| VN | | 123.20.70.1 | 0.6 |
| KR | SK브로드밴드 | 221.143.187.185 | 0.6 |
| IN | | 117.218.28.109 | 0.6 |
| KR | ㈜세종텔레콤 | 203.227.210.186 | 0.6 |
| KR | SK브로드밴드 | 211.49.22.207 | 0.6 |
| VN | | 113.167.243.250 | 0.6 |
| KR | KT | 211.226.158.191 | 0.6 |
| RO | | 89.123.13.135 | 0.46 |
| RU | | 94.50.25.119 | 0.6 |
| IN | | 117.213.203.47 | 0.6 |
| VN | | 1.54.78.207 | 0.6 |

| 시간 | 구분 | 식별자 | Group 위협도 | IP수 | 국가수 | IP 평균오염도 |
|---|---|---|---|---|---|---|
| 2012-11-20 23:00 | SUBJECT | Don t forget about me,... | 0.71 | 613 | 87 | 0.59 |
| 2012-11-20 23:00 | ATTACH... | Report.htm | 0.71 | 526 | 81 | 0.59 |
| 2012-11-20 19:00 | SUBJECT | Don t forget about me,... | 0.72 | 462 | 79 | 0.60 |
| 2012-11-20 19:00 | ATTACH... | Report.htm | 0.72 | 406 | 76 | 0.60 |
| 2012-11-20 22:00 | SUBJECT | Don t forget about me,... | 0.71 | 428 | 74 | 0.59 |
| 2012-11-20 22:00 | ATTACH... | Report.htm | 0.71 | 367 | 70 | 0.59 |
| 2012-11-23 00:00 | SUBJECT | You have notifications,... | 0.72 | 308 | 68 | 0.60 |
| 2012-11-21 23:00 | URL | ups.com | 0.72 | 307 | 68 | 0.59 |
| 2012-11-22 05:00 | ATTACH... | Report_T9952.htm | 0.71 | 427 | 68 | 0.59 |
| 2012-11-19 23:00 | ATTACH... | Invoices-1116-2012.htm | 0.71 | 288 | 66 | 0.58 |
| 2012-11-19 22:00 | ATTACH... | Invoices-1119-2012.htm | 0.69 | 220 | 65 | 0.56 |
| 2012-11-22 06:00 | ATTACH... | Report_T9952.htm | 0.71 | 420 | 64 | 0.59 |
| 2012-11-22 21:00 | URL | ups.com | 0.71 | 246 | 64 | 0.59 |
| 2012-11-20 22:00 | SUBJECT | New Russian develop,... | 0.71 | 329 | 62 | 0.58 |
| 2012-11-21 12:00 | ATTACH... | Changelog_11172012,... | 0.71 | 530 | 62 | 0.59 |
| 2012-11-21 22:00 | URL | ups.com | 0.70 | 277 | 62 | 0.57 |
| 2012-11-22 04:00 | ATTACH... | Report_T9952.htm | 0.71 | 385 | 61 | 0.59 |
| 2012-11-20 21:00 | SUBJECT | Don t forget about me,... | 0.71 | 272 | 61 | 0.58 |
| 2012-11-21 07:00 | ATTACH... | Changelog_11172012,... | 0.71 | 346 | 61 | 0.59 |
| 2012-11-21 21:00 | SUBJECT | New Russian develop,... | 0.70 | 244 | 61 | 0.57 |
| 2012-11-20 22:00 | URL | facebook.com | 0.71 | 282 | 60 | 0.59 |
| 2012-11-22 23:00 | SUBJECT | You have notifications,... | 0.71 | 372 | 60 | 0.59 |
| 2012-11-19 23:00 | ATTACH... | Invoices-1119-2012.htm | 0.71 | 259 | 60 | 0.59 |
| 2012-11-21 16:00 | SUBJECT | New Russian develop,... | 0.71 | 329 | 59 | 0.59 |
| 2012-11-20 21:00 | ATTACH... | Report.htm | 0.71 | 236 | 59 | 0.59 |
| 2012-11-22 03:00 | ATTACH... | Report_T9952.htm | 0.71 | 274 | 58 | 0.59 |
| 2012-11-21 18:00 | SUBJECT | New Russian develop,... | 0.71 | 299 | 58 | 0.58 |
| 2012-11-22 00:00 | SUBJECT | New Russian develop,... | 0.71 | 239 | 58 | 0.58 |

〔그림 7〕 봇넷그룹 탐지 결과 예시

의미하는데, 동일 봇넷 그룹에 속해있으므로, 대부분 같은 값을 가지고 있음을 알 수 있다. 또한, 동일 봇넷그룹의 분포를 보면 1개 국가가 아닌, 37개 국가에서 같은 시간에 같은 스팸메일을 발송한 것으로, 같은 봇넷그룹에 속해 있음을 뒷받침한다.

[그림 7]는 11월19일부터 23일까지 탐지된 봇넷그룹에 대한 정보를 나타낸다. 첫 번째 줄에 있는 봇넷그룹은 87개 국가, 613개 IP가 동일 봇넷 그룹을 형성하고 있으며, 두 번째 줄에는 81개 국가, 526개 IP에서 동일한 봇넷 그룹을 형성한 것을 확인할 수 있다. 좀비PC 및 봇넷그룹 탐지 시스템은 이와 같은 봇넷그룹에 대해서도 자동화된 탐지정보를 제공한다.

### 4.2. 봇넷그룹의 특징 분석

봇넷그룹은 특정 시간대에 1번의 스팸메일을 보내고 사라지지는 않는다. 봇넷그룹은 특정 시간동안 일정한 스팸메일을 보내고, 활동하지 않다가 다른 스팸메일을 보내는 등 지속적인 변화가 발생한다. [표 7]은 특정 봇넷그룹의 시간 흐름에 따른 스팸메일 발생패턴을 나타낸다. 10월3일 13시 이전까지는 별다른 활동을 하지 않다가 14시부터 16시까지 집중적인 스펨메일을 보내고 다시 소강상태에 접어들 것을 확인할 수 있다. 봇넷에 속한 IP수를 보더라도 10개 이하로 동작하다가, 특정시간에 200개 이상이 동작하고 있다.

이는 공격자들이 좀비PC들을 활용하는 형태를 짐작할 수 있게 한다. 장시간 스팸메일을 보내기보다 단기간 활동하고 중단하는 등 지속적으로 변경함으로써 탐지를

〔표 7〕 동일 봇넷그룹의 시간대별 동작 패턴

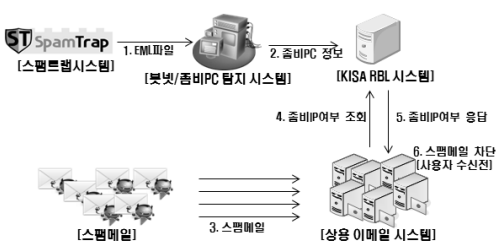
| 시 간 | 구 분 | 식별자 | Group 위험도 | IP수 | 국가수 | IP 평균오염도 | Mail 수 |
|---|---|---|---|---|---|---|---|
| 2012-10-03 05:00 | URL | ridat.ru | 0.57 | 11 | 9 | 0.57 | 28 |
| 2012-10-03 06:00 | URL | ridat.ru | 0.45 | 2 | 2 | 0.6 | 2 |
| 2012-10-03 07:00 | URL | ridat.ru | 0.49 | 5 | 4 | 0.6 | 6 |
| 2012-10-03 08:00 | URL | ridat.ru | 0.56 | 10 | 8 | 0.59 | 11 |
| 2012-10-03 09:00 | URL | ridat.ru | 0.45 | 2 | 1 | 0.6 | 3 |
| 2012-10-03 13:00 | URL | ridat.ru | 0.71 | 242 | 39 | 0.58 | 605 |
| 2012-10-03 14:00 | URL | ridat.ru | 0.71 | 264 | 41 | 0.59 | 940 |
| 2012-10-03 15:00 | URL | ridat.ru | 0.71 | 212 | 39 | 0.58 | 582 |
| 2012-10-03 16:00 | URL | ridat.ru | 0.71 | 166 | 36 | 0.58 | 289 |
| 2012-10-03 17:00 | URL | ridat.ru | 0.46 | 5 | 4 | 0.54 | 10 |
| 2012-10-03 18:00 | URL | ridat.ru | 0.45 | 1 | 1 | 0.6 | 1 |
| 2012-10-03 19:00 | URL | ridat.ru | 0.45 | 2 | 2 | 0.6 | 3 |

회피하는 방식을 취하고 있다. 또한, 좀비PC들은 공격자에게 임대되어 사용되는데, 다수 공격자에게 임대되어 좀비PC들은 동시간대에 다른 피해행위들을 발생시킬 수도 있다. 결국, 탐지된 좀비PC 대응은 적어도 수시간 내에 이루어져야 효과적인 대응이 가능할 것으로 예상된다.

### 4.3. RBL 시스템 연동을 통한 스팸메일 차단

좀비PC 탐지결과는 RBL 시스템과 연동하여 스팸메일 차단에 활용 가능하다. RBL(Realtime Blacklist) 시스템은 스팸메일 발송하는 IP들을 관리하는 시스템이다. 스팸메일 발송IP로 알려진 경우, RBL 시스템에 등록이 되며, 각 메일서버들은 메일을 수신할 때 해당 메일이 RBL 시스템에 등록된 IP인지 query를 통해 조회할 수 있다.

이와 같은 RBL 시스템을 통한 스팸메일 차단은 통상적으로 운영되고 있다. [그림 8]은 좀비PC 탐지정보를 KISA RBL 시스템과 연동된 그림을 나타낸다. 현재, KISA-RBL 시스템은 국내 4,000여개 메일서버와 연동하여 동작하고 있다.




〔그림 8〕 좀비PC 탐지결과 RBL 시스템과 연동

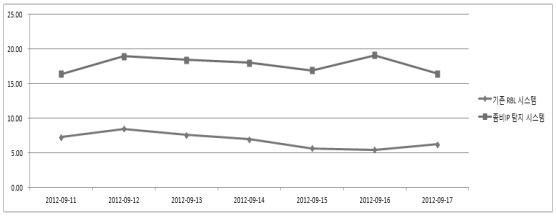
이메일 스팸트랩 시스템을 통해 유입된 이메일 분석을 통해 좀비PC를 탐지하고, 탐지한 좀비PC들은 매시간 KISA-RBL 시스템과 자동으로 연동되도록 구축하였다. 9월11일부터 17일까지 일주일간 시범운영결과, 좀비PC 탐지정보를 받지 않았을 때 스팸메일 차단 건수는 일평균 71,767개였는데, 탐지된 좀비PC 정보를 연동했을 때 일평균 142,726개로 스팸메일 차단율 98.87% 향상되었다. [표 8]은 좀비PC 탐지정보를 RBL 시스템에 적용하기전과 적용 후 추가 차단된 스팸메일 개수를 나타낸다.

또한, 스팸메일 차단에 사용된 좀비IP 정보를 분석한 결과, 기존 RBL 시스템의 경우 스팸발송IP 1개당 스팸메일 발송량은 6.81개인 반면, 좀비IP 탐지시스템의 경우, 좀비IP 1개당 스팸메일 발송량은 17.77개로, 보다 순도 높은 스팸메일을 발송하는 IP임을 확인할 수 있다. [그림 9]은 IP당 평균 스팸메일 발송량 비교결과를 나타낸다.

앞서 기술한 바와 같이, KISA RBL 시스템과 연동한

〔표 8〕 탐지된 좀비PC RBL 시스템 적용결과 비교

| 날 짜 | 기존 스팸메일 차단 건수 | 신규 스팸메일 차단 건수 | 총 합 |
|---|---|---|---|
| 9/11(화) | 70,185 | 66,091 | 136,276 |
| 9/12(수) | 85,763 | 74,418 | 160,181 |
| 9/13(목) | 86,417 | 76,308 | 162,725 |
| 9/14(금) | 76,428 | 78,129 | 154,557 |
| 9/15(토) | 60,402 | 65,532 | 125,934 |
| 9/16(일) | 57,239 | 65,187 | 122,426 |
| 9/17(월) | 65,938 | 71,048 | 136,986 |
| **평 균** | **71,767** | **70,959** | 142,726 |



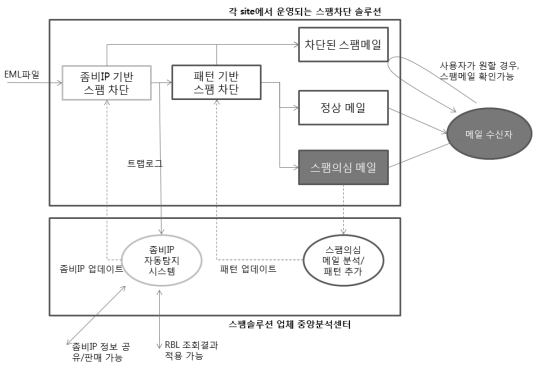

〔그림 9〕 IP당 평균 스팸메일 발송량 비교

결과, 스팸메일 차단율이 약 2배 향상되었다. 결국, RBL 시스템을 통한 스팸메일 차단율은 스팸트랩 시스템에 유입된 IP가 많을수록 높아질 것이다. 이에, 스팸트랩 시스템의 스팸유입 도메인을 확대하고, 홍보를 강화하여 좀비PC 정보를 많이 수집할 수 있도록 환경 구축이 추가로 필요할 것으로 보인다. 또한, 현재 결과물은 KISA 이메일 스팸트랩 시스템과 연동하여 결과를 산출하였는데, 상용 이메일 시스템과 연계하여 동작하면 보다 의미있는 결과물이 나올 것으로 기대된다.

## Ⅵ. 결 론

지금까지 이메일 스팸트랩 시스템과 연동하여 좀비PC 및 봇넷그룹 탐지결과를 제시하고, 탐지된 정보를 활용하여 봇넷그룹 동작 특징, 스팸메일 차단 등에 연동된 결과를 분석하였다. 본 논문에서 제시한 좀비PC 및 봇넷그룹 탐지기술은 스팸메일에 국한되는 것이 아니라, 일반적인 이메일 시스템과 연동하여 똑같은 형태로 동작 가능하다.

본 기술은 대형 포털사이트의 이메일 시스템과 연동하여 좀비PC 및 봇넷그룹을 탐지하고, 이에 대한 검증이 수행되면 다양한 활용방안이 있을 것으로 예상된다.




〔그림 10〕 스팸메일 차단 솔루션과의 연동방안

기존 컨텐츠에 대한 패턴 기반의 스팸메일 차단 솔루션과도 연동하여 동작 가능하다. [그림 10]는 기존 스팸메일 차단 솔루션과의 연동방안을 나타낸다.

기존 스팸메일 차단 솔루션은 스팸메일의 주요 컨텐츠에 대한 패턴을 등록 시킨 뒤, 해당 패턴이 탐지된 스팸메일로 분류하는 방식을 따른다. 이러한 동작방식은 알려진 스팸메일의 경우 효과적으로 동작 가능하나, 알려지지 않은 형태의 스팸메일이나, 동일IP에서 다양한 유형의 스팸메일을 보내는 경우 효과적인 대응에 한계가 있다. [그림 10]는 기존 스팸차단 솔루션과 좀비IP 기반 차단기술이 동시에 사용된 동작 과정을 나타낸다. 스팸메일 차단 솔루션 뿐 아니라, 본 기술은 봇넷그룹을 탐지할 수 있고, 다양한 형태로 악성코드 특징 분석이 가능하다. 추후, 지속적인 운영, 결과 데이터 분석하면서 추가적인 의미를 지속적으로 도출할 예정이다.

## 참고문헌

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

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

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

[4] 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, pages 299‐-304, 2009년

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

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

[7] 정현철, 김휘강, 이상진, 오주형, “이메일 스팸트랩을 이용한 좀비PC 및 봇넷그룹 추적방안 연구”, 한국정보보호학회논문지 제21권 3호, pp. 101-115, 2011년 6월.

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

[9] J.P. John, A. Moshchuk, S.D. Gribble, and A.

Krishnamurthy, "Studying Spamming Botnets Using Botlab", USENIX, 2009년.

[10] 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, 2007년.

[11] 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, 2006년.

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

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

[14] L. Lee, “Measures of distributional similarity”, Proceedings of the 37th annual meeting of the Association for Computational Linguistics on Computational Linguistics, 1999년.

[15] 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, 2008년.

## 〈著者紹介〉

**이 태 진 (Tae-Jin Lee)**
정회원

2003년 2월 : POSTECH 컴퓨터공학과 학사
2008년 2월 : 연세대학교 컴퓨터공학과 석사
2003년 1월~현재 : KISA 선임연구원
<관심분야> 악성코드, 네트워크 보안, 시스템 보안

**정 현 철 (Hyun-Cheol Jeong)**
정회원

1989년 2월 : 서울시립대학교 전산통계학과 학사
1999년 8월 : 광운대학교 전자계산학과 석사
2006년 9월~현재: 고려대학교 정보보호대학원 박사 수료
1996년 7월~현재: KISA IP주소팀장
<관심분야> 침해사고대응, 융합서비스보안, 네트워크보안, IP관리

**이 재 일 (Jae-Il Lee)**
정회원

1986년 2월 : 서울대학교계산통계학과 학사
1988년 2월 : 서울대학교계산통계학과 석사
2006년 2월 : 연세대학교 컴퓨터과학과 박사
현재 : KISA 인터넷침해대응센터장
<관심분야> 침해사고대응, 정보보호기술, 보안정책