스팸메일로 전파되는 악성코드의 분석 및 대응 프레임워크

한경수[1], 신윤호[2], 임을규[3]

A Study of Spam-spread Malware Analysis and Countermeasure Framework

Kyoung-Soo Han[1], Yun-Ho Shin[2], Eul-Gyu Im[3]

요 약

스팸메일은 악성코드를 전파시키는 방법 중의 하나로, 사용자가 스팸메일을 열어보고 첨부파일을 실행하도록 유도하기 위하여 사회공학적인 방법이 주로 사용되고 있다. 본 논문에서는 스팸 메일에 첨부된 악성코드에 대하여 행위 분석과 네트워크 트래픽 분석으로 나누어 분석하고, 분석 결과를 기반으로 대응 프레임워크를 제시한다. 해당 악성코드에 대하여 시스템 내에서의 행위 및 네트워크 트래픽을 분석한 결과, 악성코드에 감염된 시스템 내에서 파일 및 레지스트리를 생성하고 사용자의 키 입력 정보를 파일로 기록(키로깅)하는 것으로 나타났다. 또한 쿠키 파일로부터 추출한 이메일 주소들로 스팸메일을 발송하고, 특정 서버와 지속적인 통신 및 또 다른 악성코드를 다운로드하는 행위를 확인하였다. 또한 분석 결과를 바탕으로 스팸메일을 발송하는 악성코드의 행위와 스팸메일의 특징을 분석함으로써 스팸메일 발송을 탐지하고 차단하기 위한 대응 프레임워크를 제시한다.

핵심어 : 스팸메일, 악성코드, 악성코드 분석, 트래픽 분석

Abstract

Spam is one of the methods to propagate malware, and malware authors mainly use social engineering means in order to get Internet users open spam and execute an attached malware. In this paper, we analyze the malware which is attached in the spam by categorizing them into behavior analysis and network traffic analysis and propose defense mechanisms based on the result. As a results of analyzing the behavior in system and network traffic, it was observed that this malware creates new files, registries, key log files in newly infected machines. Furthermore, we inferred that malware sent spam to user's e-mail addresses from cookie files, communicated with specific server continuously and downloaded other malware. With this analyzed result, we propose the defense mechanism in order to detect sending spam and block it by analyzing the behavior of malware which sends spam and the features of spam.

Keywords : spam, Malware, Malware Analysis, Traffic Analysis

접수일(2010년05월19일), 심사의뢰일(2010년05월20일), 심사완료일(1차:2010년06월09일, 2차:2010년06월21일)

게재일(2010년08월31일)

[1]133-791 서울시 성동구 행당1동 17 한양대학교 전자컴퓨터통신공학과.
email: 1hanasun@hanyang.ac.kr

[2]133-791 서울시 성동구 행당1동 17 한양대학교 전자컴퓨터통신공학과.
email: yhs@hanyang.ac.kr

[3](교신저자) 133-791 서울시 성동구 행당1동 17 한양대학교 컴퓨터공학부 교수.
email: imeg@hanyang.ac.kr

1. 서론

IT 산업의 발전과 인터넷의 대중화로 인해 인터넷 사용자가 급증하고 그 편의성이 증가하고 있다. 또한 개인 및 산업 분야에서도 인터넷 기술의 의존도가 높아지고 있으며, 특히 이메일(E-mail) 서비스는 없어서는 안 될 필수 불가결한 매체로 발전하고 있다[1]. 그러나 이에 따라 사용자의 컴퓨터를 대상으로 한 악성코드 역시 스팸메일을 통해 급격하게 확산되고 있다[2-5]. 스팸메일은 사용자가 수신하기를 원치 않으며 광고, 악성코드 유포, 피싱 공격, 분산서비스거부공격(DDoS Attack: Distributed Denial of Service Attack) 등을 목적으로 하는 이메일을 의미한다[3]. 2008년 12월 불법스팸대응센터(http://www.spamcop.or.kr)로 접수된 스팸메일 신고 현황은 2,894,826건으로 1월 597,550건에 비하여 현저하게 증가하였다[6]. 스팸메일 발송자는 사회공학적인 방법을 이용하여 사용자들로 하여금 수신된 스팸메일의 첨부파일을 실행하도록 유도하고 있으며, 그 예로는 발송자 이름 변조, 법률 관련 제목, 호기심을 자극하는 축하 카드나 이벤트 당첨 관련 제목 등으로 스팸메일을 발송한다. 지난 2009년 12월에는 크리스마스카드로 위장한 스팸메일이 국내에서도 전파되었으며, 이 스팸메일에는 악성코드 실행파일이 'CristmasCard.zip'이라는 압축파일 형태로 첨부되어 있었다. 또한 현재까지도 해당 악성코드에 감염된 수많은 컴퓨터를 통해 구글(Google)을 사칭하거나 친구초대, E-Card 등으로 위장한 스팸메일을 지속적으로 발송하고 있다.

본 논문에서는 해당 악성코드를 시스템 내 행위 분석과 네트워크 트래픽 분석으로 나누어 분석하였으며, 시스템이 악성코드에 감염되었을 때 파일 및 레지스트리를 생성하고, 키보드 입력 정보를 기록하는 것으로 나타났다. 또한 다른 사용자에게 스팸메일을 발송하고 특정 서버와의 지속적인 통신 및 또 다른 악성코드 다운로드 등의 악성행위를 확인하였다. 프로토콜별 발생 패킷량에 대해서는 TCP 전송 프로토콜을 이용한 패킷은 전체 패킷의 93.4%이며, 그중에서도 스팸메일을 전송하기 위한 SMTP 패킷은 44.4%의 비율을 차지하였다.

본 논문의 2장에서는 스팸메일의 전파 과정과 차단 기법, 악성코드의 분석 방법에 대한 관련 연구를 기술한다. 3장에서는 허니넷(Honeynet) 환경을 이용하여 앞서 언급한 악성코드의 행위 분석과 네트워크 트래픽 분석 결과를 기술하고, 4장에서는 분석 결과를 바탕으로 대응방안을 제시한다. 마지막으로 5장에서는 결론과 향후 연구 방향에 대하여 제시하고자 한다.

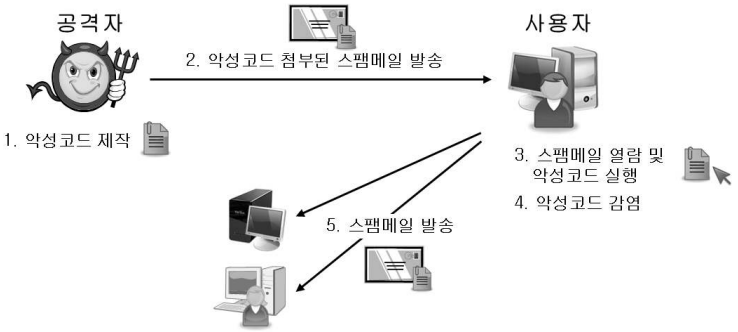
2. 관련연구

2.1. 스팸메일

2.1.1. 스팸메일의 전파 과정

공격자는 악성코드를 작성하고 사회공학적 기법을 이용하여 악성코드를 첨부한 스팸메일을 발송한다. 사용자가 호기심에 의해 수신된 스팸메일을 읽고 첨부파일을 실행시킬 경우, 악성코드는 해당 사용자의 컴퓨터를 감염시키게 된다. 감염된 컴퓨터는 또 다른 사용자들의 이메일 주소를 대

상으로 스팸메일을 발송하고 공격자에게 사용자의 개인정보를 유출시키거나 분산서비스거부공격에 이용되는 등 제 2차 피해로 이어지게 된다. [그림 1]은 스팸메일의 전파 및 악성코드의 감염 과정을 나타낸 것이다.



[그림 1] 스팸메일의 전파 과정
[Fig. 1] Propagation of spam

또한 공격자는 스팸메일을 발송하기 전에 공격 대상자를 선택하기 위해 수많은 홈페이지와 검색엔진 등을 통해 정보를 수집하고 자신의 위치를 숨기기 위한 경유지를 확보한다. 그리고는 이러한 경유지를 악용하여 악성코드를 첨부한 스팸메일을 작성하여 발송하고, 첨부파일의 실행을 통해 감염된 사용자의 컴퓨터에서 각종 정보들을 유출시킨다[7].

2.1.2. 스팸메일 대응 기술

스팸메일에 대응할 수 있는 기술로는 [표 1]에 나타낸 것과 같이 시그니처 기반 필터링, 자동차단, 레퓨테이션(Reputation) 시스템 등이 존재한다.

[표 1] 스팸메일 대응 기술
[Table 1] Anti-spam techniques

유형	방법
시그니처 기반 필터링	컨텐츠 필터링 휴리스틱 필터링 베이지안 필터링
네트워크 필터링	SMTP 연결 차단 트래픽 모니터링 및 속도 제한
자동 차단	대량 메일 발송기를 이용해 전송되는 스팸메일 차단 최초 발송된 이메일 인증 같은 형태의 이메일이 일정 시간 내에 연속적으로 발송될 경우 차단
레퓨테이션 시스템	실시간 스팸 차단 리스트(RBL) SPF(Sender Policy Framework)

가. 시그니처 기반 필터링

시그니처 기반 필터링[19]은 기본적으로 특정 시그니처에 대한 필터를 적용하고 매치 여부를 판단한다. 그중에서도 컨텐츠 필터링은 수신하려는 이메일의 헤더 정보, 본문, 첨부파일의 정보를 읽어 제목 또는 본문 중에 특정 내용, 키워드, 문자열을 포함하고 있거나 발송자의 주소가 특정한 이메일 주소일 경우 컨텐츠 필터가 이러한 스팸메일의 수신을 차단한다.

휴리스틱(Heuristic) 필터링[20]은 스팸메일 차단을 위한 사전 예방적 프레임워크로 활용되며, 수신되는 메시지의 헤더, 본문, 첨부파일을 분석하고 스팸메일의 특성이 존재하는지 확인한다. 예를 들면 느낌표나 점(.), 대문자가 과도하게 사용된 경우 스팸메일 스코어(spam Score)가 높아지게 되고, 이렇게 얻어진 결과를 임계치(Threshold)와 비교하여 스팸메일 여부를 판단한다.

베이지안(Bayesian) 필터링[21-22]은 영국의 수학자 Thomas Bayes의 수학적 원리를 기반으로 동작한다. 이 원리를 텍스트 분류에 적용시켜 개별 단어의 출현 빈도를 기록하고, 비슷한 유형의 텍스트를 샘플 데이터로 추가하여 단어들의 연관을 추적함으로써 임의의 텍스트가 해당 유형으로 분류될 수 있는지 결정한다. 이와 같은 방식으로 스팸메일 필터링에 적용하면, 미리 정의된 규칙이 존재하지 않아도 규칙을 스스로 생성하여 필터링할 수 있다. 즉, 입력되는 스팸메일과 정상메일로부터 각각의 테이블을 생성하고 새로 들어오는 이메일의 각 단어들을 스팸메일 테이블 및 정상메일 테이블과 각각 비교함으로써 특정 단어의 빈도수를 기반으로 스팸메일의 확률을 계산한다.

나. 네트워크 필터링

네트워크 필터링 기술은 네트워크 주변 및 메일 서버에 스팸메일 차단 기능을 제공하도록 구성하고 스팸메일이 네트워크에 진입하기 전에 네트워크 게이트웨이에서 제거함으로써 트래픽 성능을 유지하는 것이다. 이러한 네트워크 필터링의 기술로는 SMTP 연결 차단, 트래픽 모니터링 및 속도 제한 등이 있다.

SMTP 연결 차단은 로컬 네트워크 내에 있는 컴퓨터로부터 외부의 메일 서버로 연결되는 아웃바운드 연결을 차단하는데 주로 이용된다. 이 SMTP 연결 차단에 의해 연결 시도가 차단되면, 스팸메일은 목적지에 도달하지 못하기 때문에 스팸메일로 인한 네트워크상의 트래픽을 감소시킬 수 있다. 그러나 이러한 방법은 정상적인 트래픽마저 차단할 수 있다는 단점이 있다.

트래픽 모니터링 및 속도 제한 방법은 로컬 네트워크 중간에 위치하여 모든 컴퓨터들의 트래픽을 관찰하고 제어한다. 한 대의 컴퓨터가 비정상적인 트래픽 패턴을 생성하면 관리자가 관련 정보를 보고 받고, 현재의 네트워크 대역폭을 감소시키는 등 스팸메일 발송에 필요한 리소스를 제어함으로써 스팸메일을 전송하는 속도를 지연시킬 수 있다.

다. 자동 차단

자동 차단 기술은 스팸메일의 내용이 아니라 이메일의 발송형태와 전송방식을 판단하여 스팸메일의 여부를 판단하는 방법으로써, 개별 이메일 단위의 필터링보다는 대량으로 전송되는 스팸메일에 대응하기 위한 방법이다.

대량 메일 발송기를 통해 전송되는 스팸메일은 a) 표준을 위반한 시간 표기, b) Message-ID 필

드에 'localhost' 포함, c) X-Mailer 필드에 메일 발송기 이름(예: The Bat, eGroups, GoldMine, JiXing 등)을 포함, d) Content-Type과 실제 본문의 불일치와 같은 특징을 이용하여 차단한다. 최초 발송된 이메일 인증은 Challenge-Response 메커니즘을 통해 각 발송자마다 한번만 인증을 수행하며, 스팸메일의 경우 Challenge에 대해 응답하지 못한다는 사실이 전제된 것이다. 또한 같은 형태의 이메일이 일정 시간동안 일정량 이상 반복적으로 발송될 경우 스팸메일로 차단하는 방법도 이용된다.

라. 레퓨테이션 시스템

레퓨테이션 시스템은 블랙리스트나 화이트리스트 등에서 업그레이드된 것으로, 이메일을 보낸 발송자와 그 서버의 환경에 대하여 IP 주소와 같은 정보를 기반으로 스팸메일 여부를 판단하고 차단하는 기술이다.

실시간 스팸 차단 리스트(RBL: Realtime Blocking List)는 스팸메일 발송에 이용되는 IP 주소 리스트로, 이를 통해 해당 IP 주소로부터 수신되는 이메일을 차단할 수 있다. 이용 가능한 RBL로는 KISA(한국인터넷진흥원)-RBL, MAPS(Mail Abuse Prevention System), ORDB(Open-Relay DataBsae), SBL (Spamhous Block List) 등이 존재한다.

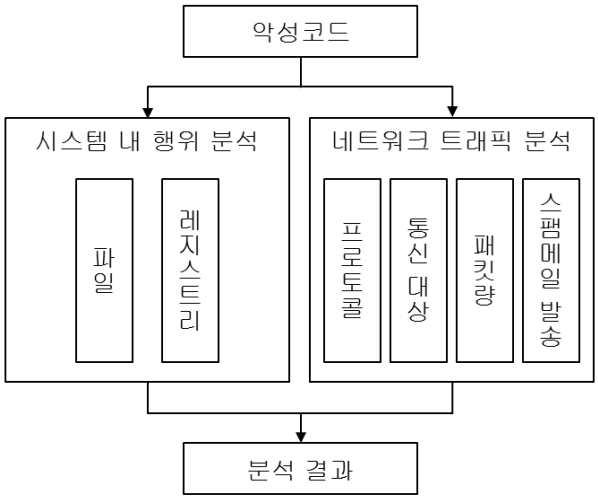
SPF(Sender Policy Framework)는 발송자의 이메일 주소를 분석하여 유효한 사용자가 해당 도메인의 서버를 통해 이메일을 발송한 것인지를 판단하는 것이다. 이는 이메일 수신 측에서 각 이메일이 정단한 DNS를 통해 발송된 것인지 해당 DNS에 직접 질의하여 확인하고, 위조된 이메일로 판단되는 경우 발송을 차단하는 기술이다. 현재 SPF는 발송자 인증 방식으로 사용되고 있는 기술 중의 하나이다.

2.2. 악성코드의 분석 방법

악성코드를 분석하는 방법에는 정적 분석과 동적 분석의 방법이 존재한다. 정적 분석은 시스템의 전체적인 구조와 구성 요소들의 연관성, 호출 관계 등을 분석함으로써 악성코드의 구조를 파악하기 위한 분석을 의미하며, 특히 폴리모픽 악성코드를 탐지하기 위하여 패킷의 페이로드에 대한 바이너리 분석 등이 대표적인 정적 분석이라 할 수 있다[24]. 동적 분석은 시스템을 동작시키면서 원하는 데이터가 산출되는지의 여부 등 시스템의 실행을 통해 결과를 확인하는 분석을 말하며, 위험요소의 실시간 감시 및 데이터 오류 검증의 최적화 등의 장점을 갖고 있다 [8,23]. 또한 역어셈블 방지 기법(Dis-assembly Thwarting Technique), 자기 수정 코드 기법(Self-modifying Code Technique) 등과 같이 정적 분석을 방해하는 기법들이 발전함에 따라 정적 분석을 통한 탐지에 어려움이 있어 동적 분석에 대한 많은 연구가 진행되어왔다[24].

본 논문에서는 [그림 2]에 나타낸 것과 같이 동적 분석을 이용하여 시스템 내 행위 분석과 네트워크 트래픽 분석으로 나누어 악성코드를 분석하였다. 시스템 내 행위 분석은 해당 시스템이 악성코드에 감염이 되었을 때 파일이 새로이 생성되거나, 레지스트리가 변경된다는 특징과 연관 지어

분석한다. 그리고 네트워크 트래픽 분석은 시스템에서 발생하는 트래픽에 대하여 이용되는 프로토콜, 통신 대상과 내용, 각종 패킷량 등 외부와 통신하는 사항들을 분석한다.



[그림 2] 악성코드 분석 방법

[Fig. 2] Method for malware analysis

2.2.1. 시스템 내 행위 분석

가. 파일 생성 및 변경 행위

사용자가 시스템에 응용프로그램을 설치하는 경우 외에 악성코드가 시스템에서 실행되었을 경우에도 파일이 생성 및 변경된다. 이는 기존의 잘 알려진 파일과 유사한 이름으로 파일을 생성하거나, 기존의 파일을 대체하기도 한다. 또한 루트킷(Root-kit)을 먼저 설치하고 이용하여 악성코드의 존재를 은닉하기도 한다. 그러나 이러한 모든 행위는 하드디스크에 새로운 파일을 생성하는 행위이며, 특정 프로세스에 의한 저장매체 사용이나 의심스러운 동작을 분석한다. 악성코드에 의한 파일 생성 및 변경을 분석하기 위해서는 FileMon[9], WinAlysis[10] 등과 같은 도구가 사용될 수 있다.

나. 레지스트리 생성 및 변경 행위

윈도우(Windows)가 부팅되거나 응용프로그램이 실행될 때에는 시스템의 모든 설정이 집결해있는 레지스트리를 바탕으로 동작한다. 악성코드는 이러한 부분을 악용하여 다양한 레지스트리를 조작함으로써 윈도우가 시작될 때 자동으로 악성코드를 실행하도록 하거나 실행 사실을 은닉한다. 따라서 악성코드에 의해 생성 및 변경되는 레지스트리를 분석할 필요가 있으며, 이를 통해서 은닉된 악성코드의 경로나 윈도우 서비스 기능 조작 여부 등에 대하여 확인할 수 있다. 악성코드에 의한 레지스트리 생성 및 변경을 분석하기 위해서는 RegMon[11], RegShot[12], WinAlysis[10] 등과

같은 도구가 사용될 수 있다.

2.2.2. 네트워크 트래픽 분석

최근의 악성코드는 시스템을 감염시키고 파괴하는 것이 아니라, 공격자가 감염된 시스템을 이용할 수 있는 기능을 포함한다. 즉, 악성코드에 감염된 시스템은 공격자와 연결되고, 공격자는 해당 시스템을 모니터링하거나 개인 정보를 유출시킬 수 있으며, 감염된 시스템들을 봇넷(Botnet)으로 구성하여 스팸메일 발송, 분산서비스거부공격 등을 수행할 수도 있다[2]. 따라서 시스템에서 발생하는 네트워크 트래픽을 분석함으로써 이러한 악성행위들을 파악할 수 있다. 네트워크 트래픽을 분석하기 위해서는 실시간으로 관찰할 수 있는 TCPView[13]나 TDIMon[14] 등이 사용될 수 있다. 또한 허니넷을 통해 시스템으로부터 발생하는 트래픽을 수집하고 저장하여 분석할 수 있다. 허니넷은 실제로 악성코드 감염 대상인 허니팟(Honeypot)과 인터넷이 연결된 허니월(Honeywall)을 브릿지(Bridge)로 연결함으로써 허니팟에서 발생하는 트래픽을 허니월에서 수집하여 분석할 수 있는 실험 환경이다.

3. 악성코드의 시스템 내 행위 및 네트워크 트래픽 분석

3.1. 시스템 내 행위 분석

지난 2009년 12월 크리스마스카드로 위장한 스팸메일에 첨부된 악성코드의 실제 파일명은 'Christmas Card.pdf(수십개의 공백).exe'로 되어있지만, 사용자에게는 'Christmas Card.pdf'라는 파일명으로 일반 파일처럼 보임으로써 클릭을 유도하고 있었다. [표 2]는 해당 악성코드에 대한 정보를 나타낸 것이다.

[표 2] 스팸메일에 첨부된 악성코드 정보
[Table 2] Information of malware attached in spam

첨부파일	Christmas Card.pdf(수십개의 공백).exe
파일크기	441,344 bytes
MD5	4B33F1D40C570869276BEBE233FB9635

[표 3]은 허니넷 환경[2]에서 악성코드를 분석한 결과를 나타낸 것으로, 생성된 파일과 그 파일에 대한 정보를 포함한다. 추가적으로 악성코드가 시스템 내에서 실행될 때 상당히 높은 CPU 점유율을 포함하는 것으로 나타났다. 분석 결과 3개의 파일이 생성된 것을 알 수 있다. 첫 번째 'wmimngr.exe'는 처음 첨부파일명 'Christmas Card.pdf(수십개의 공백).exe' 파일과 MD5 값이 일치하기 때문에 자신을 복제하고 파일명을 변경한 것으로 추론할 수 있다. 두 번째 'wpmgr.exe' 파

일은 'C:\Windows\system32' 경로에 생성되며, 키로깅을 수행하는 키로거(Keylogger) 프로그램이다. 키로거는 사용자의 키 입력을 감지하고 기록하는 악성코드로, 웹사이트 접속 ID와 패스워드, 인터넷 뱅킹 거래 시 입력하는 계좌번호와 비밀번호 등 중요한 키 입력을 모두 기록하여 추후 공격자에게 전송하는 역할을 한다[15]. 이 악성코드는 사용자가 입력하는 키보드의 모든 값을 'oracle.ocx'에 저장하고 있음을 확인할 수 있었다. 이와 같이 악성코드는 스팸메일을 보내는 역할뿐만 아니라 사용자의 민감한 정보들까지도 공격자에게 발송되기 때문에 또 다른 피해로 이어질 수 있다.

[표 3] 악성코드의 파일 생성 행위 분석
[Table 3] File creation behavior of malware

파일명	내용	
wmimngr.exe	경 로	C:\Windows\system32
	크 기	441,344 bytes
	목 적	스팸메일 발송
	MD5	4B33F1D40C570869276BEBE233FB9635
	기 타	Christmas Card.pdf(공백).exe 파일의 복제
wpmgr.exe	경 로	C:\Windows\system32
	크 기	239,616 bytes
	목 적	키로깅
	MD5	6CDDFF11CBF7AC159ACC9ACA855F19CA
	기 타	사용자가 입력하는 키로그파일을 oracle.ocx 파일에 저장
oracle.ocx	경 로	C:\Windows
	크 기	variable
	목 적	키로그 정보 저장
	MD5	variable
	기 타	wpmgr.exe에 의해 키로그 정보가 저장되는 파일

감염된 악성코드는 파일 생성 행위 외에도 레지스트리를 변경하는 악성행위를 수행한다. [16]에 따르면 윈도우 비스타(Windows Vista) 이후로 관리자의 허가 없이 어떠한 시스템의 변화도 수용하지 않도록 사용자 계정 컨트롤(UAC, User Account Control)을 도입하여 어떤 프로그램이 시스템을 변화시키려 할 때 사용자에게 확인을 받도록 하였다. 이 악성코드는 악성행위를 수행하기 위해 레지스트리를 변경시켜 사용자 계정 컨트롤의 경고 메시지를 해제하고, EnableLUA(Limited User Account)를 통해 사용자 계정을 제한하도록 변경한다. 또한 Windows Management와 Java micro kernel 레지스트리 변경을 통해 'wmimngr.exe'와 'wpmgr.exe' 악성코드를 시스템 시작과 동시에 실행될 수 있도록 경로를 추가한다. 만약 사용자에게 시스템의 변화에 대한 경고메시지를 보

내지 않도록 레지스트리가 수정된다면, 사용자의 허가 없이 안전하지 않은 프로그램이 실행되고 위와 같이 파일과 레지스트리를 변경시키기 때문에 시스템은 위험에 노출된다. [표 4]는 이 악성코드에 의한 레지스트리 변경에 대하여 나타낸 것이다.

[표 4] 악성코드의 레지스트리 변경 행위 분석
[Table 4] Registry modification behavior of malware

레지스트리	내용	
UACDisableNotify	종 류	REG_DWORD
	데이터	0x00000001 (1)
	경 로	HKLM\SOFTWARE\Microsoft\Security Center
EnableLUA	종 류	REG_DWORD
	데이터	0x00000000 (0)
	경 로	HKLM\SOFTWARE\Microsoft\CurrentVersion\policies\system
Windows Management	종 류	REG_SZ
	데이터	C:\Windows\system32\wmimngr.exe
	경 로	HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Java micro kernel	종 류	REG_SZ
	데이터	C:\Windows\system32\wpmgr.exe
	경 로	HKCU\Software\Microsoft\Windows\CurrentVersion\Run

3.2. 네트워크 트래픽 분석

악성코드를 실행시킨 허니팟에서 악성코드는 다수의 DNS 쿼리(Query)를 이용하여 메일 서버 탐색을 시도하며, 탐색된 메일 서버와 연결되었을 경우 이메일 리스트로 스팸메일을 발송한다. 그리고 스팸메일은 크리스마스카드뿐만 아니라 E-Card 및 친구 초대 등의 제목으로 스팸메일을 발송되며, 공격자의 서버와 지속적인 통신이 이루어지는 것으로 판단된다. 본 절에서는 네트워크 트래픽 분석을 통해 이 악성코드의 스팸메일 발송과정을 기술한다.

3.2.1. 감염된 시스템의 IP 주소 확인

[그림 3]은 감염된 시스템의 IP 주소를 확인하기 위해 www.whatismyip.com(IP 주소 확인 웹사이트)의 도메인네임에 대하여 DNS 쿼리 및 응답을 나타낸 것이며, www.whatismyip.com에 접속하여 automation 디렉토리의 n09230945.asp 페이지로부터 감염된 시스템의 IP 주소 정보를 수신한다.

No.	Timestamp(sec:usec)	Len...	Datalink	Src. IP	Dest. IP	Prot...	Contents
3	1263238448:334800	86	9fef6f 00:13:77:41:bb:45->00:90:1a:a1:20:64 (-...	218.144.99.130	168.126.63.1	DNS	Standard query A www.whatismyip.com
4	1263238448:354094	204	209f4e 00:90:1a:a1:20:64->00:13:77:41:bb:45 (...	168.126.63.1	218.144.99.130	DNS	Standard query response A 72.233.89.200 A 72.233.89.197 A 72.233.89.198 A
5	1263238448:363781	70	1bac748 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	72.233.89.200	TCP	cadkey-tablet > http [SYN] Seq=0 Win=65535 Len=0 MSS=1440
6	1263238448:553102	70	17172ea 00:90:1a:a1:20:64->00:13:77:41:bb:4...	72.233.89.200	218.144.99.130	TCP	http > cadkey-tablet [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1380
7	1263238448:566151	62	12f6684 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	72.233.89.200	TCP	cadkey-tablet > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
8	1263238448:566159	225	f38798 00:13:77:41:bb:45->00:90:1a:a1:20:64 ...	218.144.99.130	72.233.89.200	HTTP	GET /automation/n09230945.asp HTTP/1.1
9	1263238448:786662	318	4b222f 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	72.233.89.200	218.144.99.130	HTTP	HTTP/1.1 200 OK (text/html)
10	1263238449:3621	62	b169f8 00:13:77:41:bb:45->00:90:1a:a1:20:64 ...	218.144.99.130	72.233.89.200	TCP	cadkey-tablet > http [ACK] Seq=164 Ack=257 Win=65279 Len=0

[그림 3] 감염된 시스템의 IP 주소 확인

[Fig. 3] Identifying IP address of infected system

3.2.2. 메일 서버 접속 및 스팸메일 발송 실패

악성코드에 감염된 시스템은 메일 서버에 접속하고, 스팸메일 발송을 위한 정보를 입력한다. 그러나 정상적으로 연결되지 않거나 연결 과정에서 오류가 발생할 경우 해당 메일 서버와의 접속을 종료하고 다른 메일 서버를 탐색한다. [그림 4]는 접속한 메일 서버에서 수신한 이메일 주소 오류(Unrouteable Address)로 인해 스팸메일 발송을 실패하고 접속을 종료한 경우를 나타낸 것이다.

No.	Timestamp(sec:usec)	Len...	Datalink	Src. IP	Dest. IP	Prot...	Contents
11	1263238467:25322	87	1a457b6 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	168.126.63.1	DNS	Standard query MX oriontransfer.co.nz
12	1263238467:45884	188	1855af5 00:90:1a:a1:20:64->00:13:77:41:bb:45...	168.126.63.1	218.144.99.130	DNS	Standard query response MX 0 mail.oriontransfer.org
13	1263238467:55052	90	169e11 00:13:77:41:bb:45->00:90:1a:a1:20:64 ...	218.144.99.130	168.126.63.1	DNS	Standard query A mail.oriontransfer.org
14	1263238467:75177	194	e39a3e 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	168.126.63.1	218.144.99.130	DNS	Standard query response CNAME ayako.oriontransfer.org A 120.138.18.82
15	1263238467:80786	70	a39137 00:13:77:41:bb:45->00:90:1a:a1:20:64 ...	218.144.99.130	120.138.18.82	TCP	goldleaf-licman > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1440
16	1263238467:330884	70	1858610 00:90:1a:a1:20:64->00:13:77:41:bb:4...	120.138.18.82	218.144.99.130	TCP	smtp > goldleaf-licman [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
17	1263238467:345866	62	18e3e60 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	120.138.18.82	TCP	goldleaf-licman > smtp [ACK] Seq=1 Ack=1 Win=65535 Len=0
18	1263238467:596891	82	7259da 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	120.138.18.82	218.144.99.130	TCP	33049 > ident [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=1163483966 TS
19	1263238467:611446	62	16930e2 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	120.138.18.82	TCP	ident > 33049 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	1263238467:867146	139	1add2dd 00:90:1a:a1:20:64->00:13:77:41:bb:4...	120.138.18.82	218.144.99.130	SMTP	S: 220 ayako.oriontransfer.org ESMTP Exim 4.69 Tue, 12 Jan 2010 00:24:37 +1
21	1263238467:878025	85	eee36c 00:13:77:41:bb:45->00:90:1a:a1:20:64 (...	218.144.99.130	120.138.18.82	SMTP	C: EHLO 123greetings.com
22	1263238468:128277	62	194df86 00:90:1a:a1:20:64->00:13:77:41:bb:45...	120.138.18.82	218.144.99.130	TCP	smtp > goldleaf-licman [ACK] Seq=78 Ack=24 Win=5840 Len=0
23	1263238468:128285	190	defa1a 00:90:1a:a1:20:64->00:13:77:41:bb:45 (...	120.138.18.82	218.144.99.130	SMTP	S: 250-ayako.oriontransfer.org Hello 123greetings.com [218.144.99.130] | 250-SIZ
24	1263238468:144105	100	f5da06 00:13:77:41:bb:45->00:90:1a:a1:20:64 (...	218.144.99.130	120.138.18.82	SMTP	C: MAIL FROM:<e-cards@123greetings.com>
25	1263238468:396027	70	bd0108 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	120.138.18.82	218.144.99.130	SMTP	S: 250 OK
26	1263238468:408435	99	8ed465 00:13:77:41:bb:45->00:90:1a:a1:20:64 ...	218.144.99.130	120.138.18.82	SMTP	C: RCPT TO:<sammi@oriontransfer.co.nz>
27	1263238468:664601	87	11a698a 00:90:1a:a1:20:64->00:13:77:41:bb:4...	120.138.18.82	218.144.99.130	SMTP	S: 550 Unrouteable address
28	1263238468:674265	62	107077e 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	120.138.18.82	TCP	goldleaf-licman > smtp [FIN, ACK] Seq=99 Ack=239 Win=65297 Len=0

[그림 4] 메일 서버 접속 및 스팸메일 발송 시도 - 실패(1)

[Fig. 4] Connecting to mail server and attempting to spam - failure(1)

[그림 5]는 접속한 메일 서버에서 SPF(Sender Policy Framework)[17]에 의해 발송이 거부되어 접속을 종료한 것을 나타낸 것이다. 73번 패킷은 앞서 설명한 것처럼 수신측에서 발신 메일의 DNS를 분석하여 발송을 거부한다.

No.	Timestamp(sec:usec)	Len...	Datalink	Src. IP	Dest. IP	Prot...	Contents
63	1263238470:699448	132	126b249 00:90:1a:a1:20:64->00:13:77:41:bb:4...	168.126.63.1	218.144.99.130	DNS	Standard query response A 211.40.221.190
64	1263238470:706463	70	182f0db 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	211.40.221.190	TCP	igi-lm > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1440
65	1263238470:707213	91	192d342 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	168.126.63.1	DNS	Standard query A rmx1.oriontransfer.co.nz
66	1263238470:726371	70	6b97fd 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	211.40.221.190	218.144.99.130	TCP	smtp > igi-lm [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
67	1263238470:736194	62	1c78e57 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.190	TCP	igi-lm > smtp [ACK] Seq=1 Ack=1 Win=65535 Len=0
68	1263238470:761614	100	5224ee 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	211.40.221.190	218.144.99.130	SMTP	S: 220 SmartFilter Build 2.2.2009051816
69	1263238470:767923	85	f6a746 00:13:77:41:bb:45->00:90:1a:a1:20:64 (...	218.144.99.130	211.40.221.190	SMTP	C: EHLO 123greetings.com
70	1263238470:789219	62	15ff48b 00:90:1a:a1:20:64->00:13:77:41:bb:45...	211.40.221.190	218.144.99.130	TCP	smtp > igi-lm [ACK] Seq=39 Ack=24 Win=5840 Len=0
71	1263238470:789226	110	affc70 00:90:1a:a1:20:64->00:13:77:41:bb:45 (...	211.40.221.190	218.144.99.130	SMTP	S: 250-spam3.mailwood.com | 250-8BITMIME | 250 SIZE
72	1263238470:799153	100	1e63e3d 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.190	SMTP	C: MAIL FROM:<e-cards@123greetings.com>
73	1263238470:827590	94	1004901 00:90:1a:a1:20:64->00:13:77:41:bb:4...	211.40.221.190	218.144.99.130	SMTP	S: 550 5.7.1 Access denied by SPF

[그림 5] 메일 서버 접속 및 스팸메일 발송 시도 - 실패(2)

[Fig. 5] Connecting to mail server and attempting to spam - failure(2)

[그림 6]은 스팸메일을 발송하기 위해 접속하려는 메일 서버를 지속적으로 탐색하는 과정을 나타낸 것이다. 101, 103, 106, 113번 패킷에서는 메일을 발송하기 위해 메일 서버가 있는지를 지속적으로 확인하고 메일 서버 주소를 정확히 알지 못하기 때문에 프리픽스(Prefix)를 변경하면서 메일 서버를 탐색함을 볼 수 있다.

No.	Timestamp(sec:usec)	Len...	Datalink	Src. IP	Dest. IP	Prot...	Contents
100	1263238471:294682	146	1fc4bec 00:90:1a:a1:20:64->00:13:77:41:bb:4...	168.126.63.1	218.144.99.130	DNS	Standard query response, No such name
101	1263238471:300582	90	dc8569 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	168.126.63.1	DNS	Standard query A ns.oriontransfer.co.nz
102	1263238471:554066	143	1bab50a 00:90:1a:a1:20:64->00:13:77:41:bb:4...	168.126.63.1	218.144.99.130	DNS	Standard query response, No such name
103	1263238471:566162	92	c3c749 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	168.126.63.1	DNS	Standard query A gate.oriontransfer.co.nz
104	1263238471:820445	145	150bd4d 00:90:1a:a1:20:64->00:13:77:41:bb:...	168.126.63.1	218.144.99.130	DNS	Standard query response, No such name
105	1263238472:282953	70	1bc4459 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	210.91.16.23	TCP	prm-nm-np > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1440
106	1263238472:722171	77	12b6651 00:13:77:41:bb:45->00:90:1a:a1:20:...	218.144.99.130	168.126.63.1	DNS	Standard query A mx.belkin
107	1263238472:934974	152	4a5ab2 00:90:1a:a1:20:64->00:13:77:41:bb:45...	168.126.63.1	218.144.99.130	DNS	Standard query response, No such name
108	1263238472:939532	92	6e1408 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (2048)	192.168.0.100	192.168.0.255	NBNS	Name query NB MX.BELKIN<00>
109	1263238473:689052	92	e53108 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (2048)	192.168.0.100	192.168.0.255	NBNS	Name query NB MX.BELKIN<00>
110	1263238473:923401	70	f62373 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	211.119.128.196	TCP	ibm-res > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1440
111	1263238474:32831	70	19189e1 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.119.128.196	TCP	dbsa-lm > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1440
112	1263238474:439071	92	1690726 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (20...	192.168.0.100	192.168.0.255	NBNS	Name query NB MX.BELKIN<00>
113	1263238475:190840	79	9931f5 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	168.126.63.1	DNS	Standard query A mail.belkin
114	1263238475:214015	154	19ee1ac 00:90:1a:a1:20:64->00:13:77:41:bb:4...	168.126.63.1	218.144.99.130	DNS	Standard query response, No such name
115	1263238475:220570	92	1f1fba0 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (2048)	192.168.0.100	192.168.0.255	NBNS	Name query NB MAIL.BELKIN<00>
116	1263238475:970090	92	1befab0 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (2048)	192.168.0.100	192.168.0.255	NBNS	Name query NB MAIL.BELKIN<00>
117	1263238476:720110	92	13c5982 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (20...	192.168.0.100	192.168.0.255	NBNS	Name query NB MAIL.BELKIN<00>
118	1263238477:473627	79	1186fab 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	168.126.63.1	DNS	Standard query A smtp.belkin
119	1263238477:668915	154	14b7453 00:90:1a:a1:20:64->00:13:77:41:bb:...	168.126.63.1	218.144.99.130	DNS	Standard query response, No such name
120	1263238477:673501	92	c21495 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (2048)	192.168.0.100	192.168.0.255	NBNS	Name query NB SMTP.BELKIN<00>
121	1263238478:298099	70	1d5550d 00:13:77:41:bb:45->00:90:1a:a1:20:...	218.144.99.130	210.91.16.23	TCP	prm-nm-np > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1440
122	1263238478:423019	92	c2ea3f 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (2048)	192.168.0.100	192.168.0.255	NBNS	Name query NB SMTP.BELKIN<00>
123	1263238479:173037	92	a0dcd9 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (2048)	192.168.0.100	192.168.0.255	NBNS	Name query NB SMTP.BELKIN<00>
124	1263238479:924806	78	1034bb5 00:13:77:41:bb:45->00:90:1a:a1:20:...	218.144.99.130	168.126.63.1	DNS	Standard query A mx1.belkin
125	1263238479:938547	70	15f5897 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.119.128.196	TCP	ibm-res > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1440
126	1263238479:946989	153	b162d5 00:90:1a:a1:20:64->00:13:77:41:bb:4...	168.126.63.1	218.144.99.130	DNS	Standard query response, No such name
127	1263238479:954287	92	1cfb549 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (204...	192.168.0.100	192.168.0.255	NBNS	Name query NB MX1.BELKIN<00>
128	1263238480:47977	70	186d4c1 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.119.128.196	TCP	dbsa-lm > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1440

[그림 6] 지속적인 메일 서버 탐색

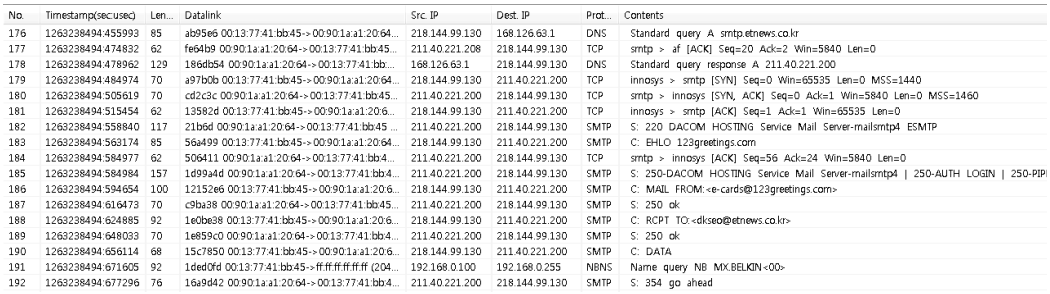
[Fig. 6] Continuously searching the mail server

3.2.3. 메일 서버 접속 및 스팸메일 발송 성공

악성코드에 감염된 시스템은 메일 서버에 접속하고, 스팸메일 발송을 위해 수신자 및 발송자 이메일 주소를 입력한다. 만약 메일 서버와 연결이 성립되면 앞서 언급했듯이 사회공학적인 방법을 이용한 본문에 파일을 첨부하여 스팸메일을 발송한다. 다음은 스팸메일 발송 시도 중, 메일 서버 접속 및 스팸메일 발송이 성공했을 경우의 동작 순서이다.

- 메일 서버 DNS 쿼리 및 응답
- 스팸메일 발송을 위한 정보 입력
- 연결 성립
- 스팸메일 발송
- 연결 종료

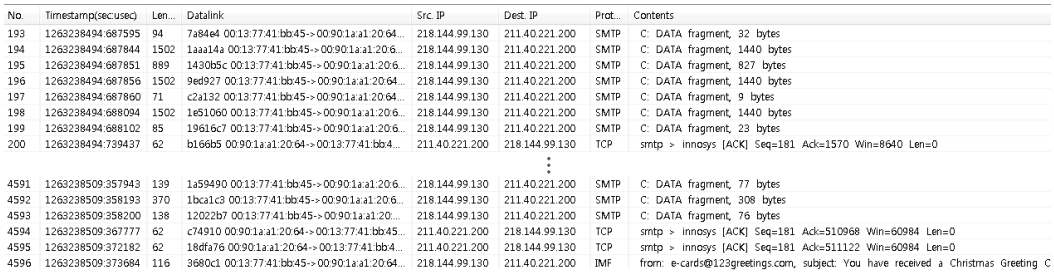
[그림 7]은 메일 서버(smtp.etnews.co.kr)와 연결이 설정되어 이메일 발송 준비가 된 것을 나타낸 것이고, [그림 8]은 메일 서버와의 연결 성립 후, 이메일을 발송하는 과정을 나타낸 것이다. 이 때 송신 포트 번호는 innosys(1412)이고 수신 포트 번호는 SMTP(25)로, 약 4300개의 패킷으로 나누어 데이터를 전송한다. 또한 스팸메일을 보낼 때마다 송신 포트 번호는 변경된다.



No.	Timestamp(sec:usec)	Len...	Datalink	Src. IP	Dest. IP	Prot...	Contents
176	1263238494:455993	85	ab95e6 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	168.126.63.1	DNS	Standard query A smtp.etnews.co.kr
177	1263238494:474832	62	fe64b9 00:90:1a:a1:20:64->00:13:77:41:bb:45...	211.40.221.208	218.144.99.130	TCP	smtp > af [ACK] Seq=20 Ack=2 Win=5840 Len=0
178	1263238494:478962	129	186db54 00:90:1a:a1:20:64->00:13:77:41:bb:...	168.126.63.1	218.144.99.130	DNS	Standard query response A 211.40.221.200
179	1263238494:484974	70	a97b0b 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	211.40.221.200	TCP	innosys > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1440
180	1263238494:505619	70	cd2c3c 00:90:1a:a1:20:64->00:13:77:41:bb:45...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
181	1263238494:515454	62	13582d 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	TCP	innosys > smtp [ACK] Seq=1 Ack=1 Win=65535 Len=0
182	1263238494:558840	117	21b6d 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	211.40.221.200	218.144.99.130	SMTP	S: 220 DACOM HOSTING Service Mail Server-mailsmtp4 ESMTP
183	1263238494:563174	85	56a499 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	211.40.221.200	SMTP	C: EHLO 123greetings.com
184	1263238494:584977	62	506411 00:90:1a:a1:20:64->00:13:77:41:bb:4...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=56 Ack=24 Win=5840 Len=0
185	1263238494:584984	157	1d99a4d 00:90:1a:a1:20:64->00:13:77:41:bb:4...	211.40.221.200	218.144.99.130	SMTP	S: 250-DACOM HOSTING Service Mail Server-mailsmtp4 | 250-AUTH LOGIN | 250-PIPI
186	1263238494:594654	100	12152e6 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	SMTP	C: MAIL FROM:<e-cards@123greetings.com>
187	1263238494:616473	70	c9ba38 00:90:1a:a1:20:64->00:13:77:41:bb:45...	211.40.221.200	218.144.99.130	SMTP	S: 250 ok
188	1263238494:624885	92	1e0be38 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	SMTP	C: RCPT TO:<dkseo@etnews.co.kr>
189	1263238494:648033	70	1e859c0 00:90:1a:a1:20:64->00:13:77:41:bb:4...	211.40.221.200	218.144.99.130	SMTP	S: 250 ok
190	1263238494:656114	68	15c7850 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	SMTP	C: DATA
191	1263238494:671605	92	1ded0fd 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (204...	192.168.0.100	192.168.0.255	NBNS	Name query NB IMX.BELKIN<00>
192	1263238494:677296	76	16a9d42 00:90:1a:a1:20:64->00:13:77:41:bb:4...	211.40.221.200	218.144.99.130	SMTP	S: 354 go ahead

[그림 7] 메일 서버와의 연결 성공

[Fig. 7] Successful connection with mail server

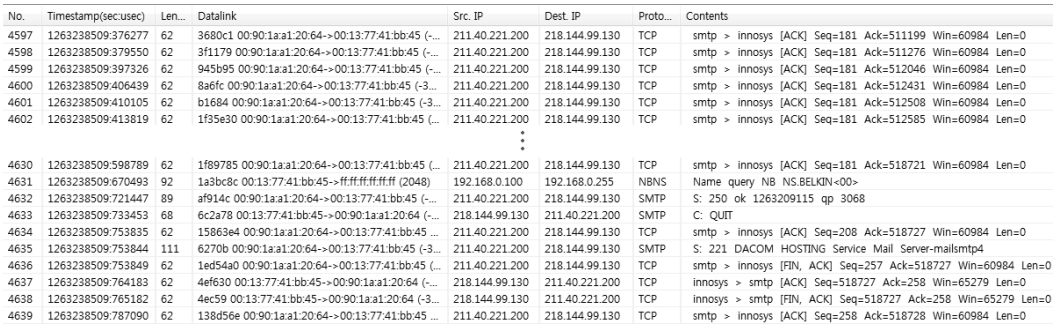


No.	Timestamp(sec:usec)	Len...	Datalink	Src. IP	Dest. IP	Prot...	Contents
193	1263238494:687595	94	7a84e4 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 32 bytes
194	1263238494:687844	1502	1aaa14a 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 1440 bytes
195	1263238494:687851	889	1430b5c 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 827 bytes
196	1263238494:687856	1502	9ed927 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 1440 bytes
197	1263238494:687860	71	c2a132 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 9 bytes
198	1263238494:688094	1502	1e51060 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 1440 bytes
199	1263238494:688102	85	19616c7 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 23 bytes
200	1263238494:739437	62	b166b5 00:90:1a:a1:20:64->00:13:77:41:bb:4...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=1570 Win=8640 Len=0
⋮							
4591	1263238509:357943	139	1a59490 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 77 bytes
4592	1263238509:358193	370	1bca1c3 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 308 bytes
4593	1263238509:358200	138	12022b7 00:13:77:41:bb:45->00:90:1a:a1:20:...	218.144.99.130	211.40.221.200	SMTP	C: DATA fragment, 76 bytes
4594	1263238509:367777	62	c74910 00:90:1a:a1:20:64->00:13:77:41:bb:45...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=510968 Win=60984 Len=0
4595	1263238509:372182	62	18dfa76 00:90:1a:a1:20:64->00:13:77:41:bb:4...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=511122 Win=60984 Len=0
4596	1263238509:373684	116	3680c1 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	211.40.221.200	IMF	from: e-cards@123greetings.com, subject: You have received a Christmas Greeting C

[그림 8] 이메일 본문 및 첨부파일 전송

[Fig. 8] Sending email body and attachment

[그림 9]는 이메일 본문 및 첨부파일 발송 후, 데이터 전송에 대한 ACK를 수신하고 메일 서버와의 연결을 종료하는 과정을 나타낸 것이다.

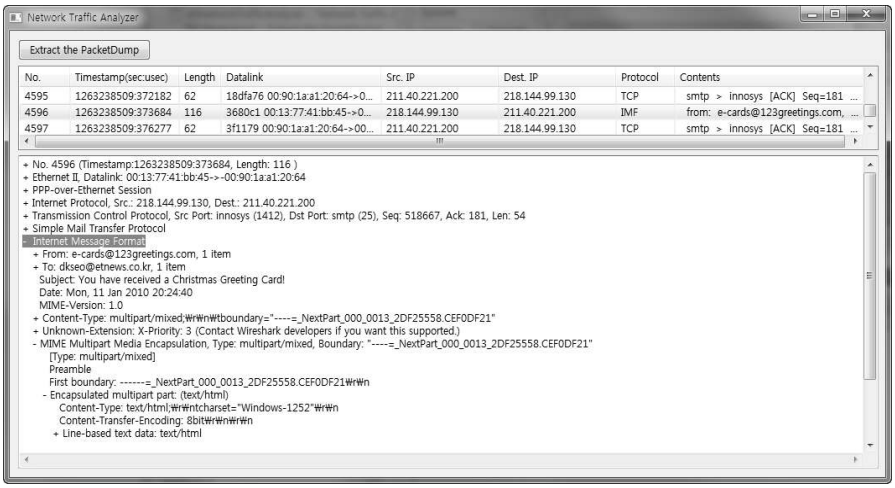


No.	Timestamp(sec:usec)	Len...	Datalink	Src. IP	Dest. IP	Proto...	Contents
4597	1263238509:376277	62	3680c1 00:90:1a:a1:20:64->00:13:77:41:bb:45 (-...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=511199 Win=60984 Len=0
4598	1263238509:379550	62	3f1179 00:90:1a:a1:20:64->00:13:77:41:bb:45 (-...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=511276 Win=60984 Len=0
4599	1263238509:397326	62	945b95 00:90:1a:a1:20:64->00:13:77:41:bb:45 (-...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=512046 Win=60984 Len=0
4600	1263238509:406439	62	8a6fc 00:90:1a:a1:20:64->00:13:77:41:bb:45 (-3...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=512431 Win=60984 Len=0
4601	1263238509:410105	62	b1684 00:90:1a:a1:20:64->00:13:77:41:bb:45 (-3...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=512508 Win=60984 Len=0
4602	1263238509:413819	62	1f35e30 00:90:1a:a1:20:64->00:13:77:41:bb:45 (...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=512585 Win=60984 Len=0
⋮							
4630	1263238509:598789	62	1f89785 00:90:1a:a1:20:64->00:13:77:41:bb:45 (...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=181 Ack=518721 Win=60984 Len=0
4631	1263238509:670493	92	1a3bc8c 00:13:77:41:bb:45->ff:ff:ff:ff:ff:ff (2048)	192.168.0.100	192.168.0.255	NBNS	Name query NB NS.BELKIN<00>
4632	1263238509:721447	89	af914c 00:90:1a:a1:20:64->00:13:77:41:bb:45 (-...	211.40.221.200	218.144.99.130	SMTP	S: 250 ok 1263209115 qp 3068
4633	1263238509:733453	68	6c2a78 00:13:77:41:bb:45->00:90:1a:a1:20:64 (-...	218.144.99.130	211.40.221.200	SMTP	C: QUIT
4634	1263238509:753835	62	15863e4 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=208 Ack=518727 Win=60984 Len=0
4635	1263238509:753844	111	6270b 00:90:1a:a1:20:64->00:13:77:41:bb:45 (-3...	211.40.221.200	218.144.99.130	SMTP	S: 221 DACOM HOSTING Service Mail Server-mailsmtp4
4636	1263238509:753849	62	1ed54a0 00:90:1a:a1:20:64->00:13:77:41:bb:45 (...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [FIN, ACK] Seq=257 Ack=518727 Win=60984 Len=0
4637	1263238509:764183	62	4ef630 00:13:77:41:bb:45->00:90:1a:a1:20:64 (-...	218.144.99.130	211.40.221.200	TCP	innosys > smtp [ACK] Seq=518727 Ack=258 Win=65279 Len=0
4638	1263238509:765182	62	4ec59 00:13:77:41:bb:45->00:90:1a:a1:20:64 (-3...	218.144.99.130	211.40.221.200	TCP	innosys > smtp [FIN, ACK] Seq=518727 Ack=258 Win=65279 Len=0
4639	1263238509:787090	62	138d56e 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	211.40.221.200	218.144.99.130	TCP	smtp > innosys [ACK] Seq=258 Ack=518728 Win=60984 Len=0

[그림 9] 전송 ACK 및 연결 종료

[Fig. 9] ACK and close connection

[그림 10]은 발송자 이메일 주소, 수신자 이메일 주소, 제목, 날짜, 컨텐츠 유형, 본문에 포함된 HTML 태그, 첨부파일 등 실제로 발송된 스팸메일에 대한 정보를 확인할 수 있다.



[그림 10] 발송된 스팸메일의 정보

[Fig. 10] Information of sent spam

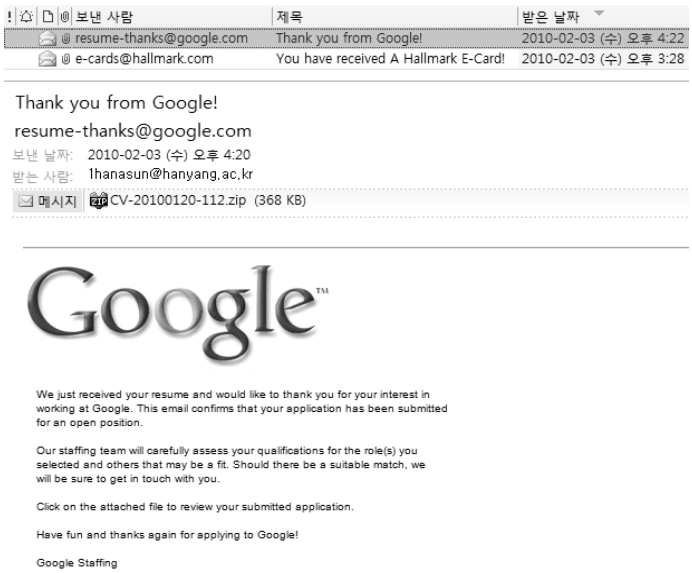
위와 같은 과정으로 허니팟에서 발생하는 네트워크 트래픽을 분석한 결과, [표 5]와 같이 악성코드가 각각 발송자 이메일 주소, 제목, 본문, 첨부파일 이름을 변경하여 스팸메일을 발송하는 것으로 나타났다.

[표 5] 발송한 스팸메일과 내용

[Table 5] Sent spam and contents

스팸메일	내용	
스팸메일 1	발송자	e-cards@123greetings.com
	수신자	(삭제)@etnews.co.kr
	제 목	You have received a Christmas Greeting Card!
	첨부파일	Christmas Card.zip
스팸메일 2	발송자	e-cards@hallmark.com
	수신자	(삭제)@segye.com
	제 목	You have received A Hallmark E-Card!
	첨부파일	Postcard.zip
스팸메일 3	발송자	invitations@hi5.com
	수신자	(삭제)@etnews.co.kr
	제 목	Jessica would like to be your friend on hi5!
	첨부파일	Invitation Card.zip

[그림 11]은 실제로 수신한 스팸메일을 나타낸 것이다. [표 5]에 나타낸 'Hallmark E-Card' 스팸메일 외에도 구글(Google)을 사칭하여 'Thank you from Google!' 이라는 제목 및 첨부파일을 검토해달라는 내용이 포함되어 있다.



[그림 11] 실제 수신된 스팸메일

[Fig. 11] Actual received spam

3.2.4. 특정 서버와 지속적인 통신

감염된 시스템은 [그림 12]와 같이 60초마다 ciscotunnel.webhop.net에 대한 DNS 쿼리를 발생시키고 소스 포트 번호를 1씩 증가시켜 DNS 서버로부터 받은 응답 IP 주소인 204.13.248.126의 443번 포트(https)를 대상으로 SYN 패킷을 3개씩 전송한다. 해당 도메인은 DynDNS.com에서 제공하는 서비스를 이용하여 악성코드 제작자가 IP 주소를 맵핑(Mapping)한 것이다. 이는 감염된 시스템이 악성코드 제작자의 서버에 접속하여 지속적인 통신이 이루어지는 것으로 판단된다.

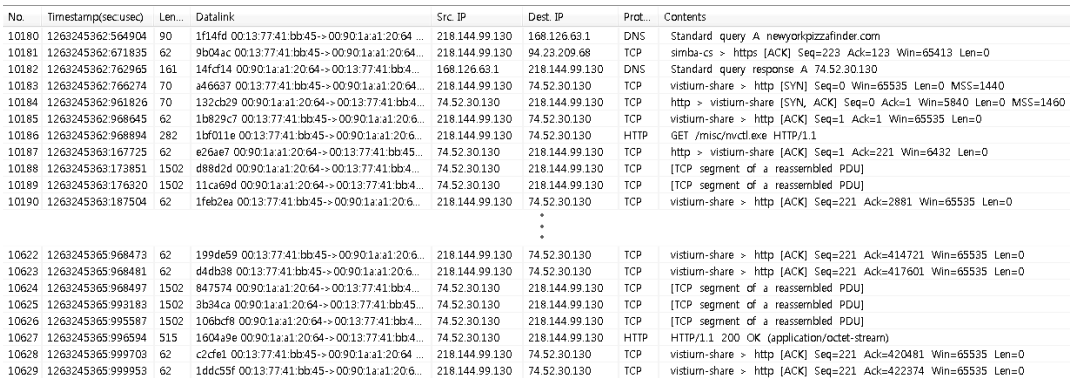
No.	Timestamp(sec:usec)	Len...	Datalink	Src. IP	Dest. IP	Prot...	Contents
8953	1263238826:897958	90	10cecb2 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	168.126.63.1	DNS	Standard query A ciscotunnel.webhop.net
8954	1263238827:212145	222	187d20c 00:90:1a:a1:20:64->00:13:77:41:bb:4...	168.126.63.1	218.144.99.130	DNS	Standard query response A 204.13.248.126
8955	1263238827:223749	70	1ef48fb 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	204.13.248.126	TCP	saism > https [SYN] Seq=0 Win=65535 Len=0 MSS=1440
8956	1263238827:438767	62	a06824 00:90:1a:a1:20:64->00:13:77:41:bb:45...	204.13.248.126	218.144.99.130	TCP	https > saism [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8957	1263238827:832109	70	1154718 00:13:77:41:bb:45->00:90:1a:a1:20:...	218.144.99.130	204.13.248.126	TCP	saism > https [SYN] Seq=0 Win=65535 Len=0 MSS=1440
8958	1263238833:956436	70	1eea96c 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	204.13.248.126	TCP	saism > https [SYN] Seq=0 Win=65535 Len=0 MSS=1440
8959	1263238875:606756	60	1b529d6 00:90:1a:a1:20:64->00:13:77:41:bb:...	Unispher_a1:20...	SamsungE_41:b...	PPP	LCP Echo Request
8960	1263238875:609744	60	cdc97b 00:13:77:41:bb:45->00:90:1a:a1:20:64...	SamsungE_41:...	Unispher_a1:20:...	PPP	LCP Echo Reply
8961	1263238886:891515	90	66eb46 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	168.126.63.1	DNS	Standard query A ciscotunnel.webhop.net
8962	1263238887:94059	222	e07e6b 00:90:1a:a1:20:64->00:13:77:41:bb:45...	168.126.63.1	218.144.99.130	DNS	Standard query response A 204.13.248.126
8963	1263238887:109375	70	8bb9d1 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	204.13.248.126	TCP	tabula > https [SYN] Seq=0 Win=65535 Len=0 MSS=1440
8964	1263238890:61236	70	1546c85 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	204.13.248.126	TCP	tabula > https [SYN] Seq=0 Win=65535 Len=0 MSS=1440
8965	1263238896:185811	70	1a0d111 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	204.13.248.126	TCP	tabula > https [SYN] Seq=0 Win=65535 Len=0 MSS=1440
8966	1263238935:803213	60	fdf48d 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	Unispher_a1:20...	SamsungE_41:b...	PPP	LCP Echo Request
8967	1263238935:807670	60	c260c5 00:13:77:41:bb:45->00:90:1a:a1:20:64...	SamsungE_41:...	Unispher_a1:20:...	PPP	LCP Echo Reply
8968	1263238946:886821	90	15f6479 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	168.126.63.1	DNS	Standard query A ciscotunnel.webhop.net
8969	1263238946:906577	206	1bd7d0e 00:90:1a:a1:20:64->00:13:77:41:bb:4...	168.126.63.1	218.144.99.130	DNS	Standard query response A 204.13.248.126
8970	1263238946:917051	70	15d533d 00:13:77:41:bb:45->00:90:1a:a1:20:...	218.144.99.130	204.13.248.126	TCP	eicon-server > https [SYN] Seq=0 Win=65535 Len=0 MSS=1440
8971	1263238949:884651	70	3d2b3 00:13:77:41:bb:45->00:90:1a:a1:20:64 ...	218.144.99.130	204.13.248.126	TCP	eicon-server > https [SYN] Seq=0 Win=65535 Len=0 MSS=1440
8972	1263238950:100537	62	fde8da 00:90:1a:a1:20:64->00:13:77:41:bb:45 ...	204.13.248.126	218.144.99.130	TCP	https > eicon-server [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8973	1263238950:431302	70	1c27402 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	204.13.248.126	TCP	eicon-server > https [SYN] Seq=0 Win=65535 Len=0 MSS=1440

[그림 12] 지속적인 DNS 쿼리 발생 및 SYN 전송

[Fig. 12] Continuous DNS query and SYN

3.2.5. 다른 악성코드 다운로드

감염된 시스템은 [그림 13]과 같이 newyorkpizzafider.com에 대한 DNS 쿼리를 요청하여 접속하고 misc 디렉토리의 nvctl.exe라는 이름의 파일을 약 450개의 패킷으로 나누어 다운로드한다.



No.	Timestamp(sec:usec)	Len...	Datalink	Src. IP	Dest. IP	Prot...	Contents
10180	1263245362:564904	90	1f14fd 00:13:77:41:bb:45->00:90:1a:a1:20:64 ...	218.144.99.130	168.126.63.1	DNS	Standard query A newyorkpizzafinder.com
10181	1263245362:671835	62	9b04ac 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	94.23.209.68	TCP	simba-cs > https [ACK] Seq=223 Ack=123 Win=65413 Len=0
10182	1263245362:762965	161	14fcf14 00:90:1a:a1:20:64->00:13:77:41:bb:4...	168.126.63.1	218.144.99.130	DNS	Standard query response A 74.52.30.130
10183	1263245362:766274	70	a46637 00:13:77:41:bb:45->00:90:1a:a1:20:64...	218.144.99.130	74.52.30.130	TCP	vistium-share > http [SYN] Seq=0 Win=65535 Len=0 MSS=1440
10184	1263245362:961826	70	132cb29 00:90:1a:a1:20:64->00:13:77:41:bb:4...	74.52.30.130	218.144.99.130	TCP	http > vistium-share [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
10185	1263245362:968645	62	1b829c7 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	74.52.30.130	TCP	vistium-share > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
10186	1263245362:968894	282	1bf011e 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	74.52.30.130	HTTP	GET /misc/nvctl.exe HTTP/1.1
10187	1263245363:167725	62	e26ae7 00:90:1a:a1:20:64->00:13:77:41:bb:45...	74.52.30.130	218.144.99.130	TCP	http > vistium-share [ACK] Seq=1 Ack=221 Win=6432 Len=0
10188	1263245363:173851	1502	d88d2d 00:90:1a:a1:20:64->00:13:77:41:bb:4...	74.52.30.130	218.144.99.130	TCP	[TCP segment of a reassembled PDU]
10189	1263245363:176320	1502	11ca69d 00:90:1a:a1:20:64->00:13:77:41:bb:4...	74.52.30.130	218.144.99.130	TCP	[TCP segment of a reassembled PDU]
10190	1263245363:187504	62	1feb2ea 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	74.52.30.130	TCP	vistium-share > http [ACK] Seq=221 Ack=2881 Win=65535 Len=0
			⋮				
10622	1263245365:968473	62	199de59 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	74.52.30.130	TCP	vistium-share > http [ACK] Seq=221 Ack=414721 Win=65535 Len=0
10623	1263245365:968481	62	d4db38 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	74.52.30.130	TCP	vistium-share > http [ACK] Seq=221 Ack=417601 Win=65535 Len=0
10624	1263245365:968497	1502	847574 00:90:1a:a1:20:64->00:13:77:41:bb:4...	74.52.30.130	218.144.99.130	TCP	[TCP segment of a reassembled PDU]
10625	1263245365:993183	1502	3b34ca 00:90:1a:a1:20:64->00:13:77:41:bb:45...	74.52.30.130	218.144.99.130	TCP	[TCP segment of a reassembled PDU]
10626	1263245365:995587	1502	106bcf8 00:90:1a:a1:20:64->00:13:77:41:bb:4...	74.52.30.130	218.144.99.130	TCP	[TCP segment of a reassembled PDU]
10627	1263245365:996594	515	1604a9e 00:90:1a:a1:20:64->00:13:77:41:bb:4...	74.52.30.130	218.144.99.130	HTTP	HTTP/1.1 200 OK (application/octet-stream)
10628	1263245365:999703	62	c2cfe1 00:13:77:41:bb:45->00:90:1a:a1:20:64 ...	218.144.99.130	74.52.30.130	TCP	vistium-share > http [ACK] Seq=221 Ack=420481 Win=65535 Len=0
10629	1263245365:999953	62	1ddc55f 00:13:77:41:bb:45->00:90:1a:a1:20:6...	218.144.99.130	74.52.30.130	TCP	vistium-share > http [ACK] Seq=221 Ack=422374 Win=65535 Len=0

[그림 13] 다른 악성코드 다운로드

[Fig. 13] Download of another malware

3.3. 네트워크 트래픽 통계

본 장에서는 시스템에 악성코드를 감염시킨 후 악성코드에 의해 발생한 트래픽에 대하여 통계를 산출하여 시각화한다. 스팸메일 발송 기록을 포함할 수 있도록 2시간동안 발생한 트래픽에 대한 통계를 산출하였다. [표 6]은 2시간동안 발생한 트래픽에 대한 정보를 나타낸 것이다. 전체 14,968 개의 패킷이 3,444,323 바이트만큼 발생하였고, 평균 패킷 사이즈는 230 바이트 정도이며, 초당 평균 480.5 바이트이다.

[표 6] 2시간동안 발생한 트래픽

[Table 6] Generated traffic for 2 hours

네트워크 트래픽의 속성	수치
총 패킷 수	14,968 Packets
총 패킷의 크기	3,444,323 Bytes
평균 패킷 사이즈	230.112 Bytes
평균 초당 바이트수	480.555 Bytes/sec

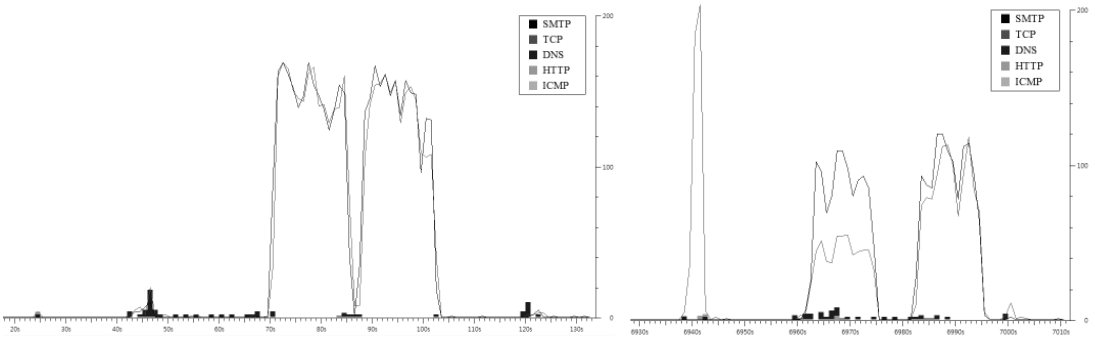
[표 7]은 프로토콜별 패킷량에 대하여 나타낸 것이다. PPP Link Protocol은 감염시킨 허니팟 시

스템이 ADSL 연결이기 때문에 연결을 지속하기 위해 발생하는 패킷으로 판단되고, NetBIOS Name Service는 네트워크 리소스에 대한 명칭의 등록, 검색, 해제 등을 수행하는 서비스를 일컫는다. 전체 발생 패킷의 약 93%가 TCP 패킷임을 알 수 있으며, 그 밖에도 UDP, ICMP 등을 포함한다.

[표 7] 프로토콜별 패킷량
[Table 7] Packet statistics for each protocol

프로토콜		패킷량	비율(%)
PPP Link Control Protocol		148	0.98878
UDP	DNS	521	3.48076
TCP	TCP	7325	48.93773
	SMTP	6645	44.39471
	HTTP	6	0.04009
	SSL	6	0.04009
ICMP		6	0.04009
Etc(NetBIOS Name Service)		311	2.07777
Total		14,986	100

[그림 14]는 시간 흐름에 따른 프로토콜별 패킷량을 나타낸 것이다. 2시간동안 발생한 트래픽 중에서 초반 40초~110초 사이에서 2개의 스팸메일을 발송하기 때문에 트래픽량이 급증한다. 후반 6940초를 전후에서는 다른 악성코드를 다운로드하기 때문에 TCP 트래픽량이 증가하고, 이후 2개의 스팸메일을 발송하기 때문에 또다시 트래픽량이 급증한 것을 볼 수 있다.



[그림 14] 시간 흐름에 따른 프로토콜별 패킷량
[Fig. 14] Number of packets for each protocol according to time

4. 대응방안

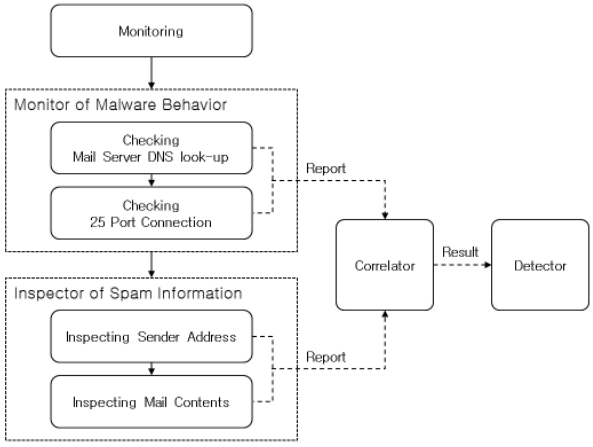
4.1 스팸메일을 발송하는 악성코드의 특징

보안이 취약한 메일 서버가 허가되지 않은 사용자들의 메일 전송을 허용할 경우 스패머들은 스팸메일을 발송하기 위해 이를 악용하게 되며, 이를 스팸메일 릴레이라 한다. 또한 스팸메일 릴레이를 이용하지 않고 직접 메일 서버에 접속하여 스팸메일을 전송하는 것도 가능하다. 다음은 스팸메일 릴레이를 이용하지 않고 스팸메일을 발송하는 악성코드의 특징을 나타낸 것이다.

- 수신 메일 서버에 직접 접속하여 스팸메일을 전송하기 위해 메일 서버 탐색을 수행
- 메일을 전송할 때 임의의 포트 번호를 통해 수신 메일 서버의 25번 포트로 접속
- 자신을 복제한 파일을 첨부하여 전송
- 탐색한 수신 메일 서버로 직접 접속하여 스팸메일을 전송

4.2 제안하는 프레임워크

본 논문에서 제시하는 스팸메일 발송 탐지 및 차단 프레임워크는 앞서 기술한 악성코드 특징을 바탕으로 감염된 시스템에서 악성코드가 비정상적으로 스팸메일을 발송할 때 이를 탐지하고 차단하는 것이다. [그림 15]는 악성코드가 발송한 스팸메일을 탐지하고 차단하는 과정을 나타낸 것으로, 스팸메일 발송 행위에 대한 최초 탐지 시점은 시스템이 메일을 전송하기 위해 메일 서버의 25번 포트에 접속할 때이다.



[그림 15] 스팸메일 발송 탐지 시스템의 프레임워크

[Fig. 15] Framework for outbound spam detection system

본 논문에서 제안하는 시스템은 악성코드의 행위 탐지와 스팸메일 특징 탐지 두 가지로 구성되어 있다. 악성코드의 행위 탐지에서는, 메일 서버 탐색을 수행하는 행위에 대한 네트워크 트래픽을 모니터링하며, 호스트 내에서 이루어진다. 악성코드가 수신 메일 서버로 직접 접속하기 위해 가능한 메일 서버를 수시로 찾는 DNS look-up의 유무를 검사하는 Checking Mail Server DNS look-up 과정이 있다. 악성코드가 주기적으로 탐색하는 메일 서버에는 smtp.server.com, mail.server.com, ns.server.com, mx1.server.com 등이 있다. 두 번째로 탐색한 수신 메일 서버에 접속할 때 25번 포트를 사용하기 때문에 25번 포트에 접속하는지를 탐지하는 Checking 25 Port Connection 과정이 있다. 이렇게 악성코드가 DNS look-up을 사용하여 메일 서버를 탐색하고 25번 포트에 접속하는 행위가 탐지되면 코릴레이터(Correlator)로 보고하게 된다.

악성코드의 행위 탐지 이외에도, 스팸메일 특징 탐지는 다음과 같은 스팸메일의 특징에 기반을 두고 실행된다.

- 같은 내용의 이메일을 반복하여 발송
- 발송자 이메일 주소를 위조 및 변조하여 이메일 발송

본 논문에서의 스팸메일로 전파되는 악성코드는 항상 같은 내용의 이메일을 반복하여 발송하며 한정된 종류의 발송자 이메일 주소로 변조하여 이메일을 발송하고 있기 때문에 제안하는 시스템은 이메일의 내용과 변조된 발송자의 주소를 검사하여 스팸메일 탐지와 차단을 돕는 Inspecting Sender Address 과정과 Inspecting Mail Contents 과정을 포함한다.

앞서 설명한 바와 같이 악성코드의 행위와 스팸메일의 특징을 검사하여 결과값을 코릴레이터에 보고하면, 코릴레이터는 이를 바탕으로 데이터베이스 비교와 확률 계산을 수행한다. 이를 통해 임계치(Threshold)와 비교하여 산출된 값이 임계치를 넘어서는 경우 감지기(Detector)로 결과를 전송함으로써 스팸메일 발송을 탐지하고 네트워크 단, 즉 방화벽에서 스팸메일을 차단한다.

5. 결론 및 향후 연구

본 논문에서는 동적 분석을 이용하여 스팸메일에 첨부되어 전파되는 악성코드가 시스템 내에서 동작하는 행위를 분석하였다. 시스템 내 행위 분석을 통해 파일, 레지스트리의 변화를 관찰 및 분석할 수 있었고, 네트워크 트래픽 분석은 시스템에서 발생하는 트래픽에 대하여 이용되는 프로토콜, 통신 대상과 내용, 각종 패킷량 등 외부와 통신하는 사항들을 분석하였다. 결과적으로 악성코드가 시스템에서 실행되면 스팸메일 발송을 위하여 시스템의 파일, 레지스트리 등을 변경시키고 메일 서버에 주기적으로 접속을 시도하면서 스팸메일을 발송하는 것을 알 수 있었다. 따라서 본 논문에서 제안하는 시스템은 악성코드가 스팸메일을 발송하기 위해 수행하는 행위들을 분석하는 악성코드 행위 탐지와 스팸메일에 내포된 특징을 통해 탐지하는 스팸메일 특징 탐지로 이루어져 있으며, 만약 악성코드가 비정상적으로 스팸메일을 발송할 때 미리 설정한 기준에 따라 임계치(Threshold)를 넘는 비정상 행위와 트래픽이 발생하였을 경우 이를 탐지하고 경고함으로써 차단한

다. 향후에는 스팸메일 릴레이를 사용하는 스팸메일 발송 악성코드에 대하여 분석하고, 이 역시 탐지할 수 있도록 시스템을 확장한 후 실제로 구현하고자 한다.

5. 사사

본 연구는 지식경제부 및 한국산업기술평가관리원의 IT산업원천기술개발사업의 일환으로 수행하였음.[KI001862, 자가복구형 네트워크 보안품질 보장 기술 개발]

참고문헌

[1] 유진호, 임종인, “스팸메일 관리지표 개선에 관한 연구”, 정보보호학회논문지, 제19권 제3호, pp. 133-142, 2009년 6월.

[2] 한경수, 임광혁, 임을규, “허니넷을 이용한 P2P 기반 Storm 봇넷의 트래픽 분석”, 정보보호학회논문지, 제19권 제4호, pp. 51-61, 2009년 8월.

[3] K. Saraubon and B. Limthanmaphon, “Fast Effective Botnet Spam Detection”, 4th IEEE International Conference of Computer Science and Convergence Information Technology, pp. 1066-1070, November 2009.

[4] C. P. Fuhrman, “Forensic Value of Backscatter from Email Spma”, 3rd IEEE International Annual Workshop on Digital Forensics and Incident Analysis, pp. 46-52, October 2008.

[5] Y. H. Shin and E. G. Im, “A Survey of Botnet: Consequences, Dfenses and Challenges”, Joint Workshop on Information Security, August 2009.

[6] 국가정보원, 방송통신위원회, 국가정보보호백서, pp. 154-158, 2009년 2월.

[7] 양경철, 이수연, 박원형, 박광철, 임종인, “전자우편을 이용한 악성코드 유포방법 분석 및 탐지에 관한 연구”, 정보보호학회논문지, 제19권 제1호, pp. 93-101, 2009년 2월.

[8] 송승화, 김윤관, 장천현, “소프트웨어 정적 분석의 가시적 표현 모델”, 한국컴퓨터종합학술대회 논문집, 한국정보과학회, 제34권 제1호(B), pp. 117-122, 2007년 6월.

[9] Filemon, http://technet.microsoft.com/en-us/sysinternals/bb896642.aspx

[10] Winalysis, http://www.winalysis.com/

[11] Regmon, http://technet.microsoft.com/en-us/sysinternals/bb896652.aspx

[12] Regshot, http://www.sourceforge.net/projects/regshot/

[13] TCPView, http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx

[14] TDImon, http://www.sysinternals.com/Utilities/TdiMon.html

[15] 서희석, 최중섭, 주필환, “윈도우 악성코드 분류 방법론의 설계”, 정보보호학회논문지, 제19권 제2호, pp. 83-92, 2009년 4월.

[16] N. J. Rubenking, “Does Windows 7’s version of User Account Control improve on the infamous feature

Vista introduced?", Article, PC Magazine, November 2009.

[17] M. Wong and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail", RFC 4408, April 2006.

[18] 권영관, 염홍열, "스팸메일 현황과 대응에 관한 고찰", 정보보호학회지, 제17권 제2호, pp. 66-79, 2007년 4월.

[19] 공미경, 이경순, "스팸성 자질과 URL 자질을 이용한 최대엔트로피모델 기반 스팸메일 필터 시스템", 한국정보과학회 언어공학연구회 학술발표 논문집, 한국정보과학회, pp. 213-219, 2006년 10월.

[20] 강승식, "메일 주소 유효성과 제목-내용 가중치 기법에 의한 스팸 메일 필터링", 한국멀티미디어학회 논문지, 제9권 제2호, pp. 255-263, 2006년 2월.

[21] 김현준, 정재은, 조근식, "가중치가 부여된 베이지안 분류자를 이용한 스팸 메일 필터링 시스템", 정보과학회논문지, 제31권 제8호, pp. 1092-1100, 2004년 8월.

[22] 이호섭, 조재익, 정만현, 문종섭, "비정상 문자 조합으로 구성된 스팸 메일의 탐지 방법", 정보보호학회논문지, 제18권 제6호(A), pp. 129-137, 2008년 12월.

[23] 박남열, 김용민, 노봉남, "우회기법을 이용하는 악성코드 행위기반 탐지 방법", 정보보호학회논문지, 제16권 제3호, pp. 17-28, 2006년 6월.

[24] 오진태, 김대원, 김익균, 장종수, 전용희, "고속 정적 분석 방법을 이용한 폴리모픽 웜 탐지", 정보보호학회논문지, 제19권 제4호, pp. 29-39, 2009년 8월.

저자 소개

한경수 (Kyoung-Soo Han)

2008년 상지대학교 컴퓨터정보공학부 학사
2010년 한양대학교 전자컴퓨터통신공학과 석사
2010년 8월 현재 한양대학교 전자컴퓨터통신공학과 박사과정
관심분야 : 악성코드 분석, 네트워크 보안, 정보보호

신윤호 (Yun-Ho Shin)

2009년 경원대학교 IT대학 전자거래학과 학사
2010년 8월 현재 한양대학교 전자컴퓨터통신공학과 석사과정
관심분야 : 악성코드 분석, 네트워크 보안, SCADA 보안

임을규 (Eul-Gyu Im)

1992년 서울대학교 컴퓨터공학과 학사
1994년 서울대학교 컴퓨터공학과 석사
2002년 University of Southern California 컴퓨터과학과 박사
2010년 8월 현재 한양대학교 컴퓨터공학부 조교수
관심분야 : 네트워크 보안, 악성 프로그램 분석, RFID 보안, SCADA 보안