情 報 保 護 學 會 誌
第18卷 第1號, 2008. 2

분석 사례를 통해 본 네트워크 포렌식의 동향과 기술

김 혁 준*, 이 상 진*

요 약

최근 인터넷의 가용성을 위협하는 대형 침해사고는 줄어들고 있으나 스팸, 피싱, 금전적 이익을 위한 분산서비스거부공격 등 악성행위의 양상은 더욱 정교하고 교묘해지고 있다. 이러한 변화는 인터넷 이용에 수반되는 잠재적인 위협을 크게 증가시켰으며 악성행위자와 이에 대응하는 보안전문가 간의 비대칭성을 크게 증가시키고 있다. 네트워크 포렌식은 보호하고자 하는 자산에 대한 직접적인 위협과 잠재 위협을 정확히 산정할 수 있는 수단을 제공하여 기존의 대응 방법에서 발생하는 비대칭성을 상쇄시킬 수 있는 수단을 제공해준다. 본 논문에서는 네트워크 포렌식의 동향과 기술에 대해 설명하고 이를 이용한 분석 사례를 통해 네트워크 포렌식의 효용을 설명하였다.

Ⅰ. 서 론

네트워크 포렌식의 효용이 세상에 알려지게 된 최초의 계기 중 하나는 1991년 걸프전 당시 네덜란드 해커에 의해 일어난 PACFLEETCOM컴퓨터 침해사고일 것이다. 당시 공격자는 자신의 행위가 관찰되고 있는 것을 모르고 해당 컴퓨터에 비인가 접근하여 미 해군의 이메일을 열람하는 동안 미국 Los Alamos 연구실에서는 그 모든 행위가 조용히 기록되고 있었으며 이후 이 사실은 Tsutomu Shimoura의 저서 "Take down"[1]을 통해 자세히 소개되었다.

1991년 당시와 현재의 인터넷 상황을 비교해보면 네트워크를 통해 소통되는 정보의 양 및 사용 행태에 많은 변화가 있었지만 기간망을 구성하는 TCP/IP의 기술적 내용은 크게 변화하지 않았다. 그러나 지속적으로 발생하고 있는 네트워크 침해사고의 양상은 '03년 슬래머 웜(slammer worm)에 의한 인터넷 대란과 같은 인터넷의 가용성에 대한 화려하고, 단발적인 위협에서 봇넷을 이용한 피싱, 스팸 혹은 금적전인 대가를 요구하는 분산서비스거부공격[2] 등 은밀하고, 지속적 위협으로 변화하고 있으며 불특정 다수를 대상으로 하는 인터넷 망에서 대형사고의 수는 줄어들고 있으나 특정그룹을 대상으로 한 공격 및 인터넷 내부의 잠재적인 위협은 크게 증가하고 있다.

이러한 위협의 도구로 사용되는 악성코드들은 자신의 생존시간을 증가시키기 위해 암호화, 다단계 패킹, 루트킷 혹은 폴리몰피즘(polymorphism) 등을 자유자제로 구사하여 분석에 복잡성을 더하고 있으며 이와 동시에 목표물이 되는 컴퓨터 운영체제 및 버전별 또는 패치수준 별 등에서 기인한 복잡성은 공격자와 방어자 간의 비대칭성을 크게 증가시켜 효과적인 침해대응 및 잠재위협에 대한 분석을 점점 더 어렵게 하고 있다.

이러한 복잡성의 문제는 네트워크 웜 등 자동화된 공격도구가 사용될 때 더 큰 힘을 발휘하는데 대개 공격자에 의한 한 번의 초기공격이 셀 수 없이 많은 추가공격을 동시 다발적으로 생성하며 이로 인한 감염여부를 호스트 수준에서 파악하고 대응하기 위해서는 침해사고 대응자의 많은 노력과 시간이 소요된다. 이러한 경우 네트워크 포렌식을 통해 네트워크 인입선(choke point)에서 입·출입 트래픽을 분석하여 효과적으로 침해상황을 파악할 수 있으며 이를 통해 침해사고가 일어난 호스트를 생산 네트워크에서 격리하여 피해의 확산을 방지할 수 있다. 또한 네트워크 포렌식 워크스테이션 구성을 통해 추가공격에 사용될 수 있는 악성자원을 분석할 수 있는 수단을 제공하여 공격자와 방어자간 발생하는 비대칭성을 상쇄시킬 수 있다.

* 고려대학교 정보경영공학전문대학원 (joonkim@kisa.or.kr, sangjin@korea.ac.kr)

Ⅱ. 네트워크 포렌식

디지털 포렌식은 크게 서버, PC 등 컴퓨터에 대한 분석하는 호스트 기반 포렌식과 네트워크상의 정보를 수집 분석하는 네트워크 기반의 포렌식으로 나눠지는데 일반적으로 디지털 포렌식은 기술적인 증거자료 수집, 분석 이외에 법정에서 증거로 인정받을 수 있는 요건을 충족시키는 법적인 증거수집 방식 및 처리절차 등을 포괄적으로 정의한다. 아직 국내에는 이에 대한 명확한 정의가 내려져 있지 않으며 본 문서에서는 네트워크 포렌식에서의 기술적인 부분만을 논한다.

2.1. 개요

본 논문에서 다루어지는 네트워크 포렌식을 이용한 분석은 침해위협 분석과 잠재위협 분석으로 나누어진다. 침해위협 분석은 네트워크 트래픽 분석을 통해 실재 네트워크에서 발생하고 있는 침해시도 및 사실을 빠르게 인지하여 이에 효과적으로 대응할 수 있는 방법을 제시하며 잠재위협 분석을 통해 공격자의 잠재적 가용자원에 대한 능동적 분석 방법을 제시하고 이를 통해 향후 발생할 수 있는 공격의 범위 및 내용을 파악하여 대응할 수 있도록 한다.

2.2. 침해위협 분석

침해위협 분석을 위해서는 분석을 위한 증거자료를 수집하는 과정과 이를 분석하는 과정으로 나누어진다. 증거수집 과정에는 증거수집 장치의 위치와 종류 선정 및 해당 장치에 대한 접근제어가 포함되며 증거자료 분석과정에는 수집된 증거를 체계적으로 분석할 수 있는 방법이 제시된다.

2.2.1. 증거수집 장치

침해위협 분석을 위한 네트워크 트래픽 정보를 수집하기 위한 장치로는 수집 장치의 위치와 수집목적에 따라 다양한 장비를 선택하여 사용할 수 있으며 사용될 수 있는 장치에는 Network Hub, Switch Mirroring Port, Network Bridge 및 Network Tap 등이 있다.

2.2.1.1. 네트워크 허브(Network Hub)

네트워크 허브는 트래픽이 수신되는 포트를 제외한 모든 포트에 동일한 네트워크 트래픽 정보를 발생시키는 물리층(Physical Layer) 네트워크 장치로 반이중(half-duplex) 모드로 동작한다. 이를 사용한 네트워크 트래픽 수집 시 수집 장치가 네트워크 트래픽을 유발시키면 모니터링하고자 하는 네트워크 트래픽과 충돌을 일으킬 수 있고 이로 인해 네트워크전반의 성능(Performance)을 저하시킬 수 있어 가급적 수집 장치 수집 인터페이스에서 네트워크 패킷을 전혀 발신하지 않는 수동모드(Passive Mode)로 동작하도록 하여야 한다.

2.2.1.2. 스위치 미러링 포트

네트워크 스위치(Network Siwtch)는 데이터 연결계층(Network Link Layer) 간 통신 시 상호 충돌 없이 사용할 수 있도록 하는 전양방 방식(full duplex)의 네트워크 장치이다. 주로 고성능 스위치 장치에 설치된 미러링 포트(Mirroring Port) 혹은 SPAN 포트는 시스템 관리자의 설정에 의해 수집 장치가 연결된 포트를 제외한 스위치 장치의 다른 포트에서 수신된 모든 네트워크 트래픽 정보를 미러링 포트로 복사하여 전송한다. 이를 이용하면 라우터에서 스위치 혹은 방화벽에서 스위치 간의 네트워크 통신을 자료를 수집할 수 있다.

2.2.1.3. 네트워크 탭(Network Tab)

네트워크 탭은 네트워크 트래픽 모니터링을 위해 수동모드(Passive Mode)로 Physical Layer에서 동작하는 장치로 어떤 형태의 네트워크 장치 간의 통신도 쉽게 모니터링할 수 있으며 일반적으로 탭장비에 전원공급이 없더라고 증거를 수집하고자 하는 네트워크의 단절(Network Failure)을 유발하지 않는 안정성 있는 수집 장치로 가용성이 보장되어야 하는 기업환경에서 널리 사용되고 있다.

2.2.1.4. 네트워크 브릿지(Nettwork Bridge)

네트워크 브릿지(network bridge)는 일반적으로 Layer 2 네트워크 세그먼트를 연결하는데 사용되며 세

그먼트간의 통신을 MAC 주소 필터링을 통해 처리한다. 네트워크 브릿지는 수동모드(Passive mode) 설치를 통해 Layer 3 이상의 통신을 하는 공격자에게 투명하게 동작하며 또한 네트워크 필터 및 방화벽 차단 스크립트 등을 이용한 Active Response 기능설정으로 선택적인 네트워크 수신을 할 수 있다.

2.2.2. 증거수집 위치

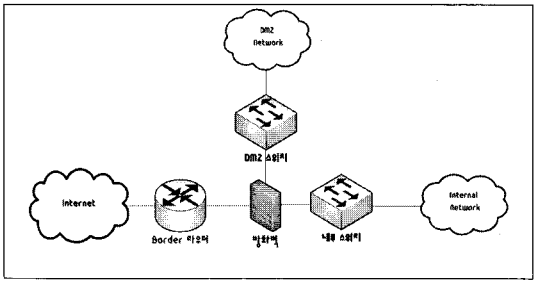
침해위협 분석을 위한 증거수집 장치의 위치는 공격자의 유형에 따라 달라진다. 이를 위해 공격자의 유형을 외부공격자와 내부공격자로 분류하고 각 유형별 공격대상이 관리 네트워크의 내부와 외부 중 어느 곳에 위치하고 있는지를 구분하여 효과적인 증거자료 수집위치를 선정할 수 있다. 이때 공격자의 유형에는 인적 공격자원 및 네트워크 웜과 트로이안 등의 자동화된 공격자원을 포함한다.

2.2.2.1. 외부 공격자의 내부망 침해

[그림 1]에 표시된 네트워크에서 공격자가 관리네트워크의 외부에 위치해 있고 공격대상이 내부 네트워크인 경우 증거수집 장치의 위치는 수집대상 트래픽의 종류에 따라 방화벽 외부 혹은 내부에 위치할 수 있는데 방화벽 외부에 위치한 경우 모든 공격 시도 트래픽을 분석할 수 있는 장점이 있으나 많은 양의 증거자료 저장 공간이 필요하며 방화벽 내부에 위치한 경우 실제 데이터 전송이 이루어진 네트워크 트래픽에 대한 정보를 선택적으로 수집할 수 있는 장점이 있다. 외부공격자의 내부 네트워크공격은 가장 일반적인 네트워크 공격 유형이며 방화벽을 사용하고 있는 사이트에서는 위의 방법을 통해 Layer 3,4 방화벽의 정책에 위배되지 않는 HTTP, SMTP, DNS 등의 Application layer 공격정보를 수집할 수 있다.

2.2.2.2. 내부 공격자의 외부망 침해

관리 네트워크 내부에 위치한 호스트에서 관리자가 인지하지 못한 침해사고 발생 시 침해사고가 발생한 호스트는 일반적으로 외부에 위치한 공격자로부터 2차 공격에 대한 정보를 수신하기 위해 외부접근을 시도하는데 이러한 비정상 접근시도를 통해 내부망의 침해사실을 빠르게 파악할 수 있다.[3] 여기에서 증거수집을 위한



[그림 1]. 참고 네트워크 구성도

위치는 2.2.1.1의 경우와 동일한 위치에서 증거자료 수집이 가능하나 방화벽에서 NAT(Network Address Translation) 정책을 사용하는 경우 공격자의 사설 IP가 공용 IP로 변환되기 전에 증거자료를 수집하는 것이 바람직하다.

2.2.2.3. 내부 공격자의 내부망 침해

자동화된 공격도구인 네트워크 웜 또는 봇넷에 감염된 경우나 1차 침해를 당한 내부 호스트를 통한 2차 침해시도는 내부 네트워크에 위치한 스위치([그림 1]에서 내부 스위치)의 미러링 포트를 통해 증거자료를 수집 분석할 수 있으며 이를 통해 내부에 위치한 공격자의 내부망 침해시도를 탐지할 수 있다

2.2.3. 증거 자료 분석

침해위협 분석을 위한 증거자료 분석은 패킷 수집 장치에 의해 수집된 네트워크 트레이스(Network trace) 파일을 통해 이루어진다. 네트워크 기능을 제외한 컴퓨터를 생각하기 힘든 현대사회에서는 일반 사용자 PC에서 발생하는 트래픽 량이 대략 수십 메가에서 수십 기가바이트에 이르며 기업환경에서는 더욱 많은 트래픽 데이터가 발생한다. 이때 발생하는 네트워크 데이터에서 분석하고자 하는 대상을 분리해 내는 것은 쉽지 않은 일이다. 네트워크에서 발생하는 대용량 데이터를 효율적으로 분석하기 위해서는 먼저 통계적 데이터와 세션데이터를 생성하고 이의 분석을 통해 정상트래픽과 비정상트래픽을 분리한 뒤 비정상 트래픽에 대한 선택적 전수조사 통해 대응하여야 한다.

2.3. 잠재위협 분석

공격자의 잠재위협을 분석하기 위해서는 침해위협 분석을 통해 얻어진 공격자의 자산에 대한 분석을 실시하여야 한다. 이를 위해서는 네트워크 포렌식 워크스테이션을 통한 능동적인 증거수집 활동을 수행하여야 하는데 자신의 자산에 대한 증거수집활동을 인지한 악성행위자의 공격에 대응하기 위한 조치를 하여야 한다. 이를 위해서는 공격자가 수행할 수 있는 분산서비스공격이 분석가가 위치한 네트워크의 가용성을 위협할 수 있으므로 증거 수집을 위한 네트워크는 생산네트워크와 분리하여야 하며 방화벽을 통해 QoS 및 세션제한 등의 조치를 취하여야 한다. 잠재위협을 분석하기 위해 사용되는 정보에는 WHOIS정보, DNS정보, 운영체제정보, 서비스 소프트웨어정보, 라우팅정보 등의 정보와 악성코드, 악성스크립트 등의 정보를 포함하는데 분석가는 자신의 행위가 반드시 적법한 범위 내에서 수행되도록 하여야 한다.

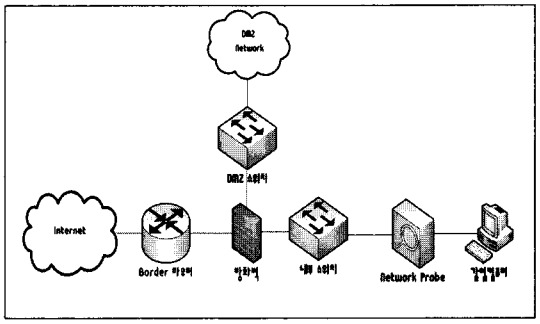
Ⅲ. 네트워크 포렌식 분석사례

이번 장에서는 앞에서 소개된 방법을 통해 악성행위자를 실재 검거한 사례와 현재 인터넷의 가장 큰 잠재위협으로 평가받고 있는 봇넷의 Fast-flux[4]기법을 분석한 사례소개를 통해 네트워크 포렌식의 동향과 효용을 제시한다.

앞에서 기술한 네트워크 포렌식의 기법이 실재 침해사고 분석에 사용된 예는 국내·외에서 적지 않게 보고되고 있다. 본 논문에서는 한국정보보호진흥원에서 2006년 네트워크 트레이스 분석을 통해 관련자 검거에 결정적 기여를 한 오픈프락시 감염 대응사례와 인터넷 망에 위치한 서버에 대한 적극적 네트워크 포렌식[5]을 통해 2007년 전 세계적으로 많은 피해를 유발하고 있는 대표적인 봇넷(Botnet)인 Storm worm의 Fast-flux 도메인 전환기법을 분석한 사례를 소개한다.

3.1. 오픈프락시 분석

네트워크 프락시서버는 HTTP, SMTP 등 Application Layer 프로토콜 통신을 중계해주는 네트워크 프로그램으로 일반적으로 SOCK 혹은 HTTP Connect 방식으로 동작한다. 오픈프락시 서버는 인증을 거치지 않고 누구나 사용할 수 있도록 설정된 프락시 서버로서 최종 접속지에서는 최초 접속자의 IP 정보를 알 수 없어 악성행위자들의 IP 세탁을 위한 용도로 널리 사용된다.



〔그림 2〕. 오픈프락시 증거수집

3.1.1. 개 요

2006년 2월 국내 인터넷 망에 50050/50033 포트에 과도한 트래픽이 집중되는 이상 징후를 파악하여 해당 IP에 대한 원격점검을 실시한 결과 오픈프락시로 확인되어 위치가 파악된 2곳에 현장점검을 통해 오픈프락시 감염사실을 발견하였으며 감염 PC 사용자의 동의를 거쳐 네트워크 브릿지[6]를 설치를 통해 네트워크 트레이스를 수집하여 분석하였다.

3.1.2. 증거수집

오픈프락시서버를 통한 악성행위에 대한 증거 수집을 위해 인라인 네트워크 브릿지를 설정하였다. 이때 불필요한 패킷전송을 통해 공격자에게 수집 장치가 노출되는 것을 방지하기 위해 STP(Spanning Tree Protocol) 및 ARP 정보 전송을 억제하였으며 수집 장치의 위치는 감염 PC와 인터넷 연결단자 중간에 설치되었다. 이를 통해 두 곳의 감염지에서 5일 동안 각각 4 Gbyte 와 8Gbyte의 네트워크 트레이스 파일이 수집되었다.

3.1.3. 네트워크 트레이스 분석

수집된 데이터의 통계 및 네트워크 세션 데이터를 분석을 통해 사용된 세션 중 다수가 SMTP 및 HTTP 데이터 전송에 사용된 것을 확인하였으며 이후 추출된 SMTP 트레이스에 대한 네트워크 전수데이터 분석을 통해 악성코드 전파에 사용된 스팸메일이 복구되었으며 이를 통해 악성코드 저장서버의 URL을 확보하여 해당

사이트에서 악성코드를 다운로드 받아 분석하였다.[7] 분석 결과 피해자 PC에서 수집된 것과 동일한 오픈프락시 파일이 해당 서버에 저장되어 있음을 확인한 후 네트워크 세션데이터 분석을 통해 관련 행위가 발생한 최초 접속지 IP를 추출하였다.

3.1.4. 증거자료 이관 및 수사의뢰

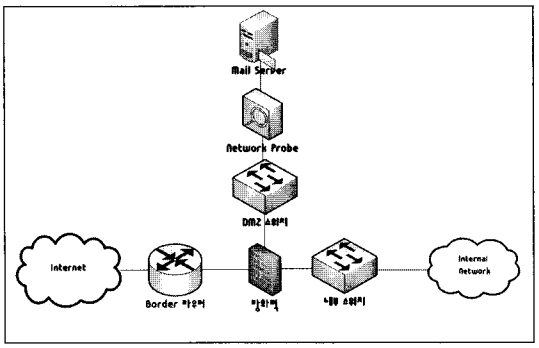
네트워크 포렌식을 통해 수집된 증거자료와 분석보고서는 모두 읽기전용 DVD ROM에 저장하였으며 위변조를 방지하기 위하여 모든 제출 자료의 해쉬값을 구하여 관계기관에 수사의뢰하였으며 관련 내용을 접수한 수사기관은 작성된 보고서에 명시된 최초접속 IP에 대한 소유자 조회를 통해 관련자를 검거하였으며 해당 악성행위자는 스팸발송, 악성코드 유포 등의 혐의로 검찰에 기소되었다.

3.2. Fast-flux 네임서버 분석

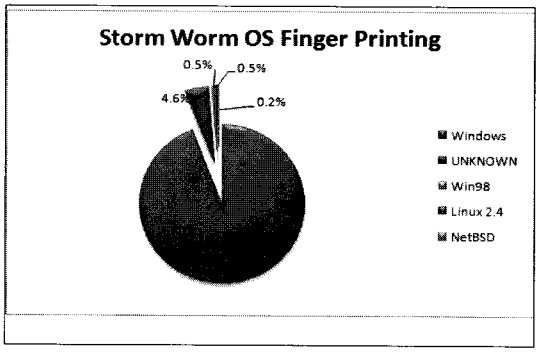
지금까지의 스패머는 광고주와 계약을 통해 이메일을 이용하여 상품 광고를 대행하고 이에 대한 수익을 배분받는 광고 대행자의 역할을 수행하였으나 대규모 봇넷의 출현은 스패머 스스로 시장을 창출할 수 있는 구조적인 여건을 제공하였다. Pump and Dump 라고 불리는 주식사기스팸이 그 전형적인 예로, 스패머가 특정주식을 구입한 뒤 이에 투자를 유도하는 사기성 스팸메일을 전송하여 수신자로 하여금 관련 주식을 매수하게 하고 그 가격이 상승하였을 때 되파는 수법을 통해 금전적인 이익을 발생시킨다. 이러한 방법을 통해 자본을 축적한 스패머는 더욱 정교한 봇넷을 구성하게 되며 이는 기존 IRC 봇넷의 단일화된 Command and Control 채널의 취약점을 개선한 P2P 방식의 봇넷을 출현시켰다.[8] P2P 방식의 봇넷은 봇넷 명령구조를 변경하고 통신채널을 암호화하여 자신이 구성한 봇넷군단의 평균 생존시간을 크게 증가시켰다. 또한 P2P방식의 봇넷과 함께 소개된 Fast-flux 네임서버기법은 DNS 레코드의 캐쉬 저장시간(TTL)을 매우 짧게 설정하고 봇넷전파를 위한 악성코드 저장서버의 Authoritative DNS IP를 매우 짧은 시간간격으로 전 세계의 다양한 IP 대역을 넘나들며 계속 변화시켜 대응에 큰 어려움을 주고 있으며 기존의 봇넷 대응 전략에 근본적인 변화를 요구하고 있다.

3.2.1. 개요

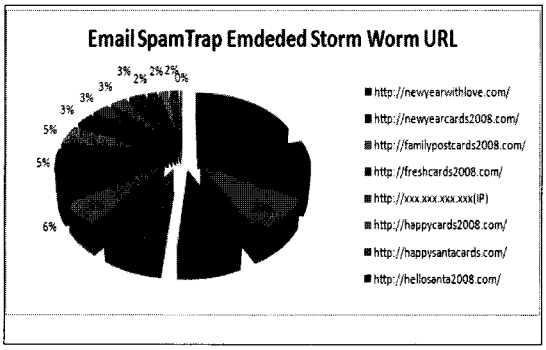
본 분석 사례는 '07년 전 세계적으로 수많은 스팸메일을 발송하고, 분산 서비스거부공격 등을 수행한 Storm worm의 Fast-flux 도메인 변환 기법을 분석한 것이다. 본 분석은 '07년 12월부터 '08년 1월까지 계속된 Storm worm의 감염 시도 이메일을 분석하여 관련 URL과 스팸메일을 발송한 스팸발송 소프트웨어의 특성값을 추출하여 이를 국내 주요포탈의 스팸 차단로그와 비교분석한 결과 스팸메일전송에 약 200여 개국 2백만 개의 IP가 사용된 것으로 나타났으며 또한 인터넷 포렌식을 통해, 악성코드 저장에 100여 개국의 약 9천여 개, Fast-flux 네임서버에 약 60여 개국 2천여 개의 IP가 사용 된 것으로 나타났다. 일반적으로 봇넷 운영자들은 자신의 IP가 Spamhaus, DNSBL 등에서 관리하는 차단리스트(Real Time Blocking List)에 등재되어 있지 않은 것을 확인한 뒤 해당 봇넷을 스팸발송에 사용하며 스팸발송 사실이 노출된 후에는 스팸발송 보다는 주로 분산 서비스 공격에 사용하는 것으로 알려져 있다.[9] 분산 서비스거부 공격 시에는 공격자의 주소지가 대부분 위조(spoofing) 되며 국경 간 대응의 어려움을 이용하여 피공격지를 선정하여 공격 근원지를 찾기가 매우 어렵다. 그러나 앞에서 기술한 것과 같이 이러한 공격의 전 단계에 일어나는 봇넷을 이용한 스팸메일 전송 시 TCP full connection을 통해 짧은 시간에 많은 메시지를 발송하는데 이러한 환경 하에서 발송 IP가 위변조될 가능성은 매우 희박하다. 만약 전송된 스팸메일이 봇넷에서 발송된 것이 확인된다면 이를 통해 봇넷감염지의 IP를 알아낼 수 있으며 이를 이용하여 봇넷을 이용한 2차 공격을 미연에 방지할 수 있다.



〔그림 3〕. Fast-flux 도메인 분석용 네트워크 증거수집



〔그림 4〕. Storm Worm 감염 운영체제 분포



〔그림 5〕. Storm worm 발송 스팸 내 URL 분포

3.2.2. 증거수집 및 보존

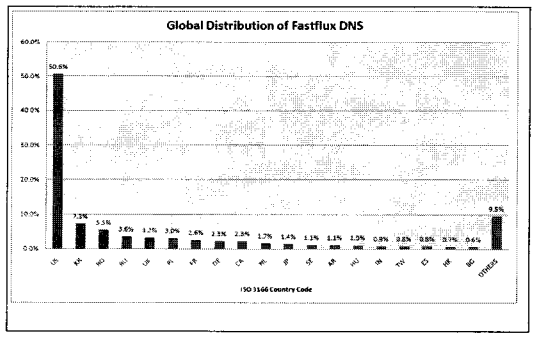
Fast-flux 네임서버 분석을 위해 수집될 증거에는 네트워크 탭을 통해 수집된 SMTP 트래픽 정보와 인터넷 포렌식을 통해 수집된 DNS 정보가 포함된다. SMTP 트래픽 정보는 [그림 3]에서 Network Probe로 표시된 증거자료 수집 장치를 통해 '07년 10월 23일부터 '08년 1월 4일까지 수집되었으며, 분석을 통해 얻어진 Storm worm 전파용 이메일에 포함되어 있는 도메인명을 사용하여 '07년 12월 24일부터 '08년 1월 1일까지의 DNS 질의를 통해 수집되었다.

3.2.3. 증거 자료 분석

Storm worm의 활동은 이메일을 통한 봇넷 감염시도와 봇넷을 통한 스팸메일전송으로 크게 나뉜다. 이중 감염 시도 스팸은 본문에 악성코드 저장서버의 URL이 포함되어 있어 해당 스팸이 Storm worm에서 발생한 것인지 여부를 쉽게 확인할 수 있다. '07년 12월 감염 시도 이메일에 포함된 merrychristmasdude.com[10] 도메인명이 포함되어 있는데 수집된 메일 중 해당 URL이 포함되어 있는 이메일을 추출하여 발송 소프트웨어의 특성값을 추출한 뒤 이를 통해 수집 장치를 통해 수집된 기간 중에 수신된 모든 Storm worm 추정 이메일을 추출하였다. 동일한 특성값을 가지고 있는 이메일은 총 5,987개이며 해당 메일에 포함된 URL을 분석한 결과 99.5%가 storm worm 감염파일을 포함한 사이트임이 확인되었다.([그림 5] 참조) 또한 동일한 특성값을 가지는 이메일 발송에 사용된 TCP SYN 패킷에 대한 운영체제검사(OS Fingerprint)를 통해 스팸메일발송 호스트 운영체제의 총 94.7% 가 윈도우 계열로 분석되어 봇넷에 감염된 윈도우즈 계열의 컴퓨터가 스팸발송에 사용된 것이 확인되었다.([그림 4] 참조)

3.2.4. 심층 분석

Fast-flux 네임서버 분석을 위해 수집된 DNS 증거자료는 총 76,213건의 DNS질의가 사용되었으며 이를 통해 전 세계 61개국 2,110개의 IP가 약 20분 간격으로 네임서버를 변경하는 것으로 분석되었고([그림 6] 참조) 또한 전 세계 101개국 9,383개의 봇넷 전파를 위한 악성코드 저장사이트 IP가 확인되었다. 앞의 두 경우 모두 한국은 미국에 이어 두 번째로 많은 Fast-flux 네임서버와([그림 7] 참조) 악성코드 전파 사이트 수를 가지고 있는 것으로 분석되었다. 또한 분석 기간 중 Storm 봇넷을 통해 발송된 스팸메일의 IP를 분석한 결과 전 세계 130개국 5,987개의 IP가 스팸발송에 사용된 것으로 확인되었는데 이중 한국은 총 발송 IP의 3.77%를 차지해 미국, 인디아, 페루, 터키에 이은 5위로 나타났다.



〔그림 7〕. Fast-flux 도메인서버 국가별 분포

위의 분석결과에 의하면 한국에 위치한 Storm 봇넷은 스팸발송 보다는 Fast-flux DNS 및 악성코드 저장소로 더 많이 사용되는데 이는 상대적으로 보안수준이 취약한 국내 초고속 인터 망이 해외 봇넷 운영자에게 오, 남용되는 현상을 나타내고 있는 것으로 생각된다.

Ⅳ. 결 론

1969년 미국 국방성의 실험 망에서 시작한 인터넷은 이제 명실공히 전 세계를 연결하는 상업망으로 성장하였지만 그 보안성은 아직 초기단계의 수준을 크게 넘어서지 못하고 있다. 또한 최근 들어 인터넷을 통해 적법하지 않은 이익을 추구하려는 경향이 두드러지고 있는데 이들은 개인적 흥미나 명성을 위해 인터넷의 취약점을 들어내던 초기의 해커와는 달리 금전적 이익을 추구를 위한 조직범죄 집단화 되어 많은 고도의 기술력을 가지고 많은 자본과 인력을 투입하여 인터넷을 악용하기 위한 수단을 개발하고 있다. 이들은 인터넷 침해사고에 대한 국경 간 공조의 어려움, 개인사용자 PC의 보안취약점 등을 악용하여 대규모의 봇넷 등을 구성하여 스팸, 피싱, 및 금전적 대가를 위한 분산서비스거부공격 등을 수행하고 있으며 이에 대응하는 보안전문가의 노력을 저지하기 위해 다양한 기술적인 수단을 강구하고 있다. 네트워크 포렌식은 공격자의 행위가 노출되는 관리네트워크의 주요지점에 증거수집 장치를 설치하여 이를 통해 내부망에 대한 침해시도를 탐지하고 이미 침해사고가 일어난 후에는 이러한 침해사실을 빠르게 파악하여 대응할 수 있는 방법을 제공해 주며 능동적인 분석기법을 통해 공격자의 잠재위협을 효과적으로 평가할 수 있는 방법을 제공해 준다.

참고문헌

[1] Shimoura, T. (1996). Takedown. New York, Hyperion Press.

[2] Whitcomb, D. (2006). Botmaster pleads guilty to computer crime. Reuters. LOS ANGELES.

[3] Bejtlich, R. (2005). Extrusion Detection: Security Monitoring for Internal Intrusions, p. 83-84 Addison-Wesley Professional.

[4] The Honeynet Project & Research Alliance (2007) Fast-Flux Service Networks. Know Your Enemy

[5] Robert, J. (2005). Internet Forensics, p. 1-8 O'Reilly Media, Inc.

[6] Bejtlich, R. (2004). The Tao Of Network Security Monitoring: Beyond Intrusion Detection, p. 76-83 Addison-Wesley Professional.

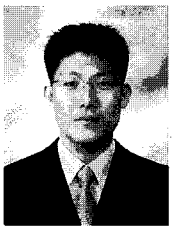
[7] Jones, K. J., R. Bejtlich, et al. (2005). Real Digital Forensics: Computer Security and Incident Response, p. 597-607 Addison-Wesley Professional.

[8] Porras, P., H. Saidi, et al. (2007). A Multi-perspective Analysis of the Storm (Peacomm)Worm.

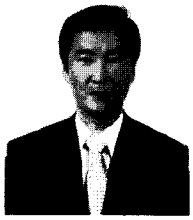
[9] Ramachandran, A., N. Feamster, et al. (2006). Revealing botnet membership using DNSBL counter-intelligence. Proceedings of the 2nd conference on Steps to Reducing Unwanted Traffic on the Internet - Volume 2. San Jose, CA, USENIX Association

[10] Nazario, J. (2007). "Storm is Back, Dude!" ARBOR Security Engineering & Rerponse Tt, from http://asert.arbornetworks.com/2007/12/storm-is-back-dude/.

〈著者紹介〉



김 혁 준 (Hyukjoon Kim)
2004년 5월: 캐나다 알버타 주립 대학교 컴퓨터공학과 졸업
2005년 5월 : 캐나다 Random-Knowledge사 IDS/IPS 개발팀
2005년 5월~현재 : 한국정보보호진흥원 스팸대응팀
2006년 3월~현재 : 고려대학교 정보경영공학전문대학원
<관심분야> 네트워크 포렌식, 디지털 분석, 침해사고대응, 봇넷대응, 스팸대응



이 상 진 (Sangjin Lee)
1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임 연구원,
1999년 2월~2001년 8월 : 고려대학교 자연과학대학 조교수,
2001년 9월~현재 : 고려대학교 정보경영공학 대학원 교수
<관심분야> 대칭키 암호, 정보은닉이론, 디지털 포렌식