# OutBound 트래픽을 이용한 인터넷 웜 탐지 및 대응 방안 연구

이 상 훈*

요 약

인터넷 웜은 1.25 인터넷 대란의 경우에서도 알 수 있듯이 네트워크를 마비시키고, 정보를 유출 하는 등 여러 가지 피해를 준다. 본 논문에서는 이를 예방하기 위하여 자신의 PC에서 인터넷 웜을 탐지하고 자동 대응을 수행할 수 있는 방안을 제시하였다. 인터넷 웜의 특징인 트래픽 기반 네트워크 스캐닝을 탐지하여 이에 대한 대응을 수행하며, 웜에 감염된 프로세스를 중단시키고, 해당 트래픽이 외부로 유출되는 것을 방지하며, 웜에 감염된 실행파일을 고립시키고 특정 위치에 이동함으로써, 사후에 웜에 대한 조사를 원활히 수행할 수 있도록 구성하였다. 이런 방식은 알려지지 않은 웜의 탐지에도 유용하며, 이를 통해 안정적인 네트워크 운영이 가능할 것이다.

# A Study of Internet Worm Detection & Response Method Using Outbound Traffic

Sang Hun Lee*

**ABSTRACT**

Internet worm gives various while we paralyze the network and flow the information out damages. In this paper, I suggest the method to prevent this. This method detect internet worm in PC first. and present the method to do an automatic confrontation. This method detect a traffic foundation network scanning of internet worm which is the feature and accomplish the confrontation. This method stop the process to be infected at the internet worm and prevent that traffic is flowed out to the outside. and This method isolate the execution file to be infected at the internet worm and move at a specific location for organizing at the postmortem so that we could accomplish the investigation about internet worm. Such method is useful to the radiation detection indication and computation of unknown internet worm. therefore, Stable network operation is possible through this method.

Key words : Network, Internet Warm, Outbound Traffic

* 국가보안기술연구소

## 1. 서 론

정보통신 기술의 발달로 인해 인터넷은 자료의 공유, 업무 지속성 유지, 간편한 상거래 등의 여러 가지 기능을 수행하고 있으며, 이는 우리 생활에 필수불가결한 요소기술로 자리매김하고 있다. 그러나, 이러한 인터넷의 순기능과 더불어 이의 악용으로 인해 발생하는 여러 가지 역기능이 존재하는데, 그 중 대표적인 것이 인터넷 웜이다. 인터넷 웜은 2004년에 발생한 1.25 인터넷 대란으로 알 수 있듯이, 각 기관 및 주요 네트워크를 마비시켜 인터넷의 순기능을 이행할 수 없도록 한다. 따라서, 이러한 인터넷 웜의 확산을 방지하는 것은 안정적인 인터넷의 사용을 위해 반드시 필요하다. 인터넷 순기능의 안정적 제공을 위해 침입차단시스템, 침입탐지시스템, 유해트래픽 차단 시스템, 바이러스 방역 시스템, 스팸 메일 필터링 시스템, 통합보안관리 시스템 등 여러 가지 정보보호시스템들이 각 단위 네트워크 및 대규모 네트워크에 적용되어 사용되고 있다.

정보보호시스템 중 침입탐지시스템은 네트워크 상의 비정상적인 트래픽 흐름, 공격 시도 등을 탐지하고 이를 관리자에게 통보함으로써, 안정적인 네트워크를 유지시키기 위한 기능을 수행한다. 침입탐지시스템은 크게 사용자 및 네트워크 트래픽의 행위를 기반으로 침입을 탐지하는 행위기반 침입탐지시스템과 침입에 해당하는 규칙을 미리 정의하고 이에 대한 탐지를 수행하는 오용탐지 기반의 침입탐지시스템으로 나눌 수 있다[1]. 또한, 탐지 대상에 따라 네트워크 기반, 호스트 기반, 하이브리드 형태의 침입탐지시스템으로 분류할 수 있다. 이러한 침입탐지시스템들은 모두 네트워크로 유입되는 패킷을 분석하여 공격 여부를 탐지한다. 현재 가장 많이 사용되고 있는 침입탐지시스템은 네트워크 기반의 오용탐지 기반 시스템이다. 그러나, 기존의 오용탐지 기반 네트워크 침입탐지시스템들이 유입되는 패킷만을 기반으로 침입탐지를 수행하고, 규칙 기반의 침입탐지를 수행하기 때문에 새로운 인터넷 웜 또는 스캐닝 등 대규모 패킷의 발생에 대해 적절히 탐지를 수행하지 못하는 경우가 존재한다. 또한, 관리자에게 송출된 경보메시지를 관리자가 인지하고 대응을 수행하기 위해서는 많은 시간이 요구된다. 따라서, 본 논문에서는 이를 보완하기 위해 Outbound 트래픽을 대상으로 침입탐지를 수행할 수 있는 방안에 대해 논한다.

Outbound 트래픽을 대상으로 침입탐지를 수행하는 시스템은 개인 시스템에서 외부로 발생하는 트래픽을 점검하여 이 중 스캐닝 시도를 탐지하고 이를 차단하는 기능을 수행한다. 즉, Outbound 트래픽을 기준으로 흐름 기반 스캐닝 탐지 기법을 이용하여 스캐닝을 탐지하고, 탐지된 해당 IP 및 포트에 대해서 패킷 유출을 차단시키는 기능을 수행한다. 이러한 기능은 알려지지 않은 인터넷 웜에 개인 시스템이 감염되었을 경우에도 이를 미연에 차단하는 기능을 수행하므로, 전체 네트워크를 안정적으로 유지시켜줄 수 있는 기능을 수행할 수 있다. 또한, 차단 사실을 개인 및 관리자에게 전송하여 감염 초기에 신속한 조치를 취할 수 있도록 한다.

본 논문은 다음과 같이 구성되어 있다. 먼저 제 2장에서 본 논문을 작성하기 위한 관련 연구 내용을 기술하고, 제 3장에서는 Outbound 트래픽을 이용한 인터넷 웜 탐지 및 대응 방안의 연구 내용을 기술한다. 그리고, 제 4장에서는 제안하는 방식의 설계에 대해 이야기하고, 제 5장에서는 제안하는 방식을 적용한 결과와 일반적인 패킷 유출량을 비교하여 평가에 가름하였다. 제 6장에서는 결론을 이야기하고, 마지막으로 이 논문을 작성하기 위한 참고문헌에 대해 기술하였다.

## 2. 관련 연구

Outbound 트래픽을 기준을 침입을 탐지하기 위

해 필요한 관련 연구는 침입탐지시스템에 대한 연구, 스캐닝 기법에 대한 연구 등이다. 다음은 이에 대한 기술이다.

## 2.1 침입탐지시스템

일반적으로 침입탐지시스템은 컴퓨터가 사용하는 자원의 무결성과 비밀성, 가용성을 저해하는 행위를 가능한 실시간으로 탐지하는 시스템을 의미한다. 최근에 빈번히 발생하고 있는 주요 인터넷 사이트들의 해킹으로 인해 네트워크 보안이 중요한 문제로 대두되면서 침입탐지시스템의 중요도는 점점 높아지는 추세이다[2, 3].

### 2.1.1 구성요소

침입탐지시스템은 데이터 수집 단계, 데이터 가공 및 축약 단계, 침입분석 및 탐지단계, 그리고 보고 및 대응단계의 4단계 구성요소를 가진다[4].

데이터 수집 단계는 침입탐지시스템이 대상 시스템에서 제공하는 시스템 사용 내역, 컴퓨터 통신에 사용되는 패킷 등과 같은 탐지 대상으로부터 생성되는 데이터를 수집하는 감사 데이터 수집 단계이다.

데이터 가공 및 축약 단계는 수집된 감사 데이터가 침입 판정이 가능할 수 있도록 의미 있는 정보로 전환하는 단계이다.

분석 및 침입탐지 단계에서는 의미 있는 정보로 전환된 감사 데이터를 분석하여 침입 여부를 판정하며, 이는 침입탐지시스템의 핵심 단계이며, 시스템의 비정상적인 사용에 대한 탐지를 목적으로 하는지 또는, 시스템의 취약점이나 응용 프로그램의 버그를 이용한 침입에 대한 탐지를 목적으로 하는지에 따라 비정상적 행위 탐지 기술과 오용 탐지 기술로 분류할 수 있다.

보고 및 대응 단계에서는 침입탐지시스템이 감시 대상 시스템 또는 네트워크에 대한 침입 여부 판정 결과를 이용하여 적절한 대응을 수행하거나 관리자에게 통보하여 조치를 취할 수 있도록 하는 단계이다.

최근에는 침입탐지 및 대응에 대한 요구가 증가되고 있으며, 침입을 추적하는 기능에 대한 연구도 활발히 진행되고 있다[5, 6].

### 2.1.2 침입 탐지 방법

침입탐지에는 공격에 관한 축적된 지식을 이용하여 공격을 수행하고 있다는 증거를 찾는 방식과 감시중인 시스템의 정상행위에 관한 참조모델을 생성한 후 정상행위에서 벗어나는 경우를 찾는 두 가지 방식이 존재한다.

지식기반 침입탐지 방법은 알려진 침입 행위를 이용하여 침입을 탐지하고, 정해진 모델과 일치하는 경우를 침입으로 간주한다. 이러한 방법에는 전문가 시스템, 규칙 분석, 페트리넷, 상태전이 분석, 신경망, 유전 알고리즘 등이 있다.

행위기반 침입탐지 방법은 사용자의 패턴 분석 후, 입력 패턴과 비교하여 침입을 탐지하며, 통계적 방법, 전문가 시스템, 신경망, 컴퓨터 면역학, 데이터마이닝, 기계 학습 방법 등이 존재한다. 또한, 침입탐지를 위한 분석을 수행하는 방식에 따라 정적 및 동적 침입탐지로 나눌 수 있다. 동적 침입탐지시스템은 시스템에 영향을 미치는 이벤트가 발생하는 즉시 획득함으로써, 실시간 분석을 수행하며, 정적 침입탐지시스템은 시스템의 스냅샷을 이용하여 분석한 후 취약한 소프트웨어나 구성 오류 등을 찾는다.

### 2.1.3 침입 대응 방법

침입에 대한 대응 형태에 따라 수동적 대응과 능동적 대응으로 구분되는데, 대부분의 침입탐지시스템은 수동적으로 공격이 발견되면 경보가 생성되지만 공격을 방어하기 위한 능동적 대응을 수행하지 않는다. 이는 침입탐지시스템이 많은 수의 잘못된 경보를 발생시켜 시스템의 가용성을 떨어

뜨릴 수 있으므로 일면 타당할 수 있다. 주기적인 분석에 기반을 둔 다수의 침입탐지시스템에는 시스템의 구성에 보안 문제가 발생하는 경우 능동적으로 대처할 수 있는 능력이 추가되었고, 이러한 시스템들은 취약점을 탐지하고 시스템을 이전 상태로 되돌리는 스크립트들을 생성한다.

침입탐지시스템들의 도래와 함께 대응 요소들도 현저하게 증가했는데, RealSecure, Net-Ranger, WebStalker 등은 공격애 행해지고 있는 연결을 단절시키고 공격이 시작된 호스트로부터의 트래픽을 차단하거나 방화벽이나 라우터 등의 설정 변경 기능을 포함하고 있다.

### 2.1.4 침입탐지시스템의 한계

현재까지 가장 널리 사용되는 침입탐지시스템은 오용탐지 방법을 이용한 침입탐지시스템이다. 이 시스템은 알려진 공격 패턴을 이용하여 침입을 탐지하는 시스템으로, 침입탐지시스템의 안전성, 성능 등의 이유로 가장 널리 사용되고 있다. 그러나, 오용탐지의 방식은 알려진 공격을 탐지하기에는 적합하나 그렇지 않은 경우는 탐지할 수 없다는 한계점을 가진다. 또한, 정해진 패턴에서 벗어나는 변종 인터넷 웜의 경우는 탐지할 수 없다. 그리고, 대응 기능을 가지지 못하기 때문에 침입에 대한 발견과 이에 대한 대응을 수행하는데 걸리는 시간이 길어 웜 등 네트워크에 신속하게 대량으로 영향을 미치는 공격의 경우 적절한 대응을 수행할 수 없다는 한계점을 가진다. 따라서, 본 논문에서는 이러한 한계점들을 극복할 수 있는 방안을 제시한다.

## 2.2 포트스캐닝

### 2.2.1 정의

포트스캐닝이란, 포트 스캔 도구에 의한 목적지 시스템에 대하여 접속 가능한 포트를 찾기 위한 행위이다. 공격자들은 목적지 시스템이 동작하고 있는지 확인하고, 열려진 포트를 탐색한 후 취약점 스캔 도구(Nessus, Internet Scanner 등)를 이용하여 취약점 분석을 수행한다. 취약점 분석 후 알려진 취약점이 존재할 경우 해당 취약점을 이용하여 공격을 수행한다. Footprinting이 DNS 정보나 whois 정보와 같은 공개된 정보를 수집하는 단계라고 한다면 포트 스캐닝은 시스템의 동작여부 검사 후 실질적인 최초의 시스템 분석 시도이다[7].

### 2.2.2 종류

(1) TCP Connect() 스캔

이 기법은 3-Way handshaking을 이용한 스캐닝이다. 완전한 TCP 연결을 수행하여 포트의 open/close 상태를 확인하기 때문에 시스템에서 쉽게 탐지가 될 수 있다.

(2) TCP SYN 스캔

Half-open 스캔 또는 stealth 스캔으로 불리기도 하며, 완전한 TCP 연결을 맺지 않고 대상 포트로 SYN 패킷을 전송하여 SYN/ACK를 받으면 open 상태, RST/ACK를 받으면 close 상태로 판단한다.

SYN 스캔은 half-open 연결을 통하여 포트의 open/close 상태를 확인하기 때문에 TCP connect() 스캔에 비하여 비밀스러운 연결로 시스템에 로그가 기록되지 않는다. TCP를 이용한 스캔 방법 중 스캔 속도가 TCP connect() 스캔 보다 빠르기 때문에 가장 많이 사용된다.

(3) TCP FIN, Xmas Tree, Null 스캔

TCP FIN, Xmas Tree, Null 스캔은 steal 스캔이라고 불리기도 하며 UNIX 계열 시스템에 대해서만 사용할 수 있다. 만약 TCP FIN, Xmas Tree, NULL 스캔으로 스캔을 수행하여 결과가 없다면 해당 시스템은 windows 계열의 시스템이라고 판단할 수 있다.

TCP FIN 스캔은 TCP flag의 FIN을 활성화하여 대상 포트로 패킷을 전송하고, Xman Tree 스캔은 TCP flag의 FIN, URG, PUSH를 활성화하여 대상 포트로 패킷을 전송한다. NULL 스캔은 TCP flag를 모두 비활성화하여 대상 포트로 패킷을 전송한다. 세 가지의 스캔 방법 모두 포트가 close 상태이면 RST 패킷을 전송하며, open 상태이면 패킷을 무시한다.

(4) UDP 스캔

UDP 스캔은 UDP를 사용하는 열린 포트를 찾기 위한 스캐 기법이다. 대상 포트로 UDP 패킷을 전송하고 대상 포트로부터 "ICMP Port Unreachable" 메시지를 받으면 close 상태이며, 메시지가 오지 않는 경우 open 상태이다.

UDP 스캔은 정확도가 떨어지기 때문에 결과에 대해서 신뢰를 할 수 없는 스캔 기법이다. close 상태는 명확하게 포트가 닫혀 있다는 것을 알 수 있지만 open 상태는 UDP 프로토콜의 특성상 네트워크의 상태나 라우터, 스위치 등에 의한 필터링에 의해서 응답이 없을 수 있기 때문에 open 상태는 정확도가 떨어진다고 할 수 있다.

# 3. Outbound 트래픽을 이용한 인터넷 웜 탐지 및 대응 방안

Outbound 트래픽을 이용하여 인터넷 웜을 탐지하고, 이에 대한 자동적인 대응을 수행하기 위해서는 두 가지 형태의 기능이 존재하여야 한다. 첫 번째 기능은 Outbound 트래픽을 대상으로 스캐닝을 수행하는 프로세스를 탐지하는 것이고, 두 번째의 경우는 탐지된 내용을 이용하여 해당 프로세스를 삭제하고, 프로세스의 실행 파일을 향후 분석을 위해 특정 위치에 저장하며, 스캐닝 패킷을 네트워크로 분출하지 못하게 하기 위하여 패킷 Drop 정책을 설정하는 것이다. 스캐닝을 탐지하기 위한 기법은 Traffic Flow 기반의 기법을 사용하며, 프로세스의 삭제 및 패킷 Drop 정책을 수행하기 위해서는 Windows 또는 Unix 계열의 시스템에서 제공하는 침입차단 기능(iptables, windows 방화벽, iptrap 등)을 사용한다.

## 3.1 Traffic Flow 기반 스캐닝 탐지 기법

### 3.1.1 개요

인터넷 웜의 특징 중 하나는 시스템이 감염되었을 경우 다른 시스템으로의 전의를 위해 네트워크를 대상으로 스캐닝을 수행하는 것이다. 이때, 네트워크로의 패킷 유입/유출이 증가하는 패턴을 파악하고 분석하여 스캐닝을 탐지하는 방법이 Traffic Flow를 이용한 네트워크 스캐닝 탐지 기법이다. 이 기법은 일정기간의 학습을 통해 정상 상태의 트래픽 수치를 저장하고 이에 대한 이상 상태를 파악하여 네트워크 스캐닝 수행 여부를 판단하는 기법이며, 출발지주소, 목적지주소, 프로토콜, 목적지포트 등의 분포 및 시간 단위를 기본으로 한다. 그러나, 현재 제안하는 인터넷 웜에서의 스캐닝은 그 특성상 무작위 IP를 대상으로 스캐닝을 수행하는 경우가 많고, 취약점이 존재하는 시스템을 찾는 형태가 많으므로 목적지 주소와 포트, 프로토콜, 패킷의 양을 계산하기 위한 단위 시간의 4가지 요소를 이용하여 판단한다.

### 3.1.2 탐지 요소

스캐닝을 탐지하기 위해서는 목적지 주소, 포트, 프로토콜에 대한 통계를 이용하며, 통계를 유지하는 시간을 단위 시간으로 수행한다.

| | |
|---|---|
| $D_A$ | : *Destination Address Count* |
| $D_P$ | : *Destination Port Count* |
| $P$ | : *Protocol Count* |
| $SP$ | : *Process created packet* |
| $sp$ | : *Each Process created packet* |
| $\triangle T$ | : *Unit Time(5Sec)* |
| $F1(SP, D_A)$ | : *Destination Address Distribution Rate* |

$F2(SP, D_p, P)$ : *An Everage of Service Count and Protocol on Unit Time*

$D_A$는 단위 시간동안 유출되는 패킷의 목적지 주소별 통계치를 나타내며, $D_P$는 단위 시간동안 유출되는 패킷의 서비스별 통계치를 나타낸다. 그리고, P는 단위 시간동안 유출되는 패킷의 프로토콜별 통계치를 나타내며, $SP$는 패킷을 발생시킨 프로세스를 나타낸다. $\Delta T$는 가장 각종 통계치를 생성하기 위한 가장 기본이 되는 시간 단위이다.

인터넷 웜에서 수행하는 네트워크 스캔인 경우 대다수의 불특정 IP 또는 감염된 시스템이 존재하는 네트워크에 동일한 서비스가 존재하는지 스캔을 수행하는 것이 일반적이므로, $F1(SP, D_A)$인 경우에는 표준 분포 형태가 스캔 여부를 결정하는 중요한 요소이다. 따라서, 동일 IP를 대상으로 수행하는 스캔인 경우 스캔이 아니라 정상적인 웹 연결 등의 요소일 가능성이 존재한다. 그러므로, 각 프로세스에서 발생하는 네트워크 패킷 중 목적지 IP 별 통계치의 분포로 웜에 의한 스캔을 수행하는지 그렇지 않은지를 결정한다. 또한, IP 별 통계와 상호 관계가 존재하여 유기적으로 연결되어 있는 부분은 각 프로세스가 생성하는 패킷에 대한 네트워크 포트 및 프로토콜별 통계이다. 이 통계 정보는 $F2(SP, D_p, P)$의 함수에 의해 계산한다.

### 3.1.3 스캐닝 탐지 방법

스캐닝 수행 상태를 판단하기 위해 정상상태의 트래픽 흐름을 판단하여야 한다. 그 판단은 F1과 F2의 유기적 관계에서 판단을 수행한다. 즉, F1의 흐름이 정규분포를 따르는 형태이고, F2에서 정상이 아닌 대량의 트래픽이 발생하였을 경우 스캐닝이라 간주할 수 있다. 이를 위해 정상 상태의 트래픽 흐름을 계산하여 이를 저장하여야 하며, 이에 대한 비교 및 임계치 설정을 통해 스캐닝을 판별하게 된다. 계산을 위한 수식은 다음과 같다.

$$E(D_A)=\frac{\sum_{i=0}^{\Delta T} F1_i}{\Delta T},\ E(D_P)=\frac{\sum_{i=0}^{\Delta T} F2_i}{\Delta T},$$

$$T=(1-p)E(D_A)+pE(D_P)$$

식에서 구해진 평균치와 두 식 사이의 연계성을 이용하여 임계치 T를 구한다. 이때, 확률 p는 동일한 IP에서 패킷이 발생할 확률이며, $D_A$는 동일하지 않은 목적지IP, $D_P$는 동일한 서비스 및 프로토콜에 대한 확률 분포로 동일하지 않은 무작위 IP를 대상으로 동일 서비스로의 취약점을 이용한 스캐닝을 탐지할 수 있다. 이렇게 정해진 임계치와 확률치를 이용하여 스캐닝 판단을 수행하게 되며, 그 탐지 수식은 다음과 같다.

스캐닝공격 : $ST \geq \Delta + T$
($\Delta$ = 적정임계치기준값)

적정 임계치 기준값에 평균값으로 구해진 임계치를 더한 값보다 단위 시간의 통계치가 더 클 경우 이를 스캐닝 공격으로 판단하고 이에 대한 대응을 수행한다. 이러한 네트워크 스캐닝의 경우 일반적인 인터넷 웜의 특성에 해당되므로 해당 트래픽을 유발하는 프로세스를 인터넷 웜 유발 프로세스로 판단할 수 있다.

### 3.2 침입 대응

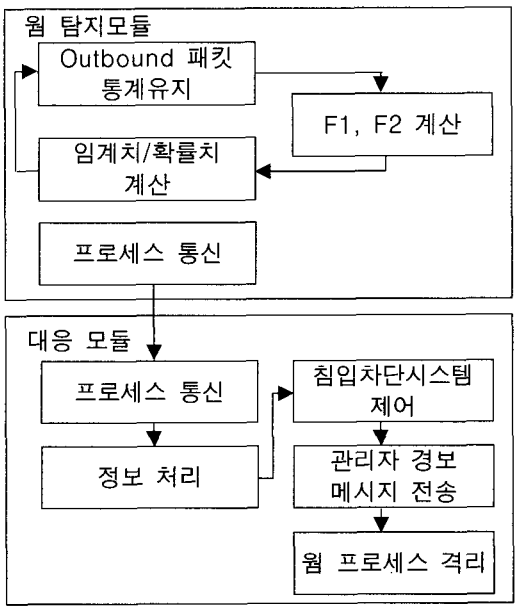
침입에 대응하기 위해서는 Windows 시스템의 패킷 필터링 API 또는 Unix 계열 시스템의 침입 차단기능인 iptables, iptrap을 연계하여 침입에 대응한다. 그리고, 웜에 대한 사후 조사를 위해 웜 트래픽을 유발시키는 프로세스를 프로세스 리스트에서 확인한 후 이에 대한 동작을 중지시키고, 다음으로 이를 특정 위치로 이동한다. 이렇게 대응을 수행할 경우 네트워크에 웜에 의한 패킷 유발을 중단시킬 수 있어 안정적으로 네트워크를 유지할 수 있으며, 또한, 웜의 전파를 사전 차단하고,

이에 대한 사후 조사를 위하여 웜 프로그램을 보관하므로 사후 감염원인 분석에도 유용하다[8, 9, 10].

### 3.3 탐지 및 대응 방안 설계

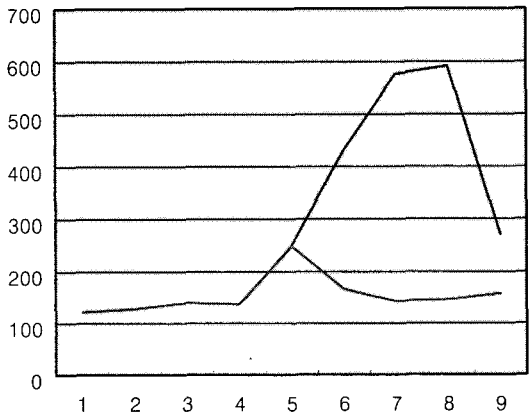
(그림 1)은 Traffic Flow 기반 인터넷 웜 탐지 및 대응 방안에 대한 설계 내용이다.

먼저 인터넷 웜의 탐지 수식 계산을 위해 목적지 포트, 주소 등의 통계를 유지하기 위한 Outbound 패킷 통계 유지 모듈과 임계치 계산의 기본이 되는 통계치 계산을 위한 F1, F2 계산 모듈, 이를 이용하는 임계치/확률치 계산 모듈이 존재한다. 또한, 프로세스간 통신 모듈을 이용하여 대응 모듈로 탐지 사실을 전송하며, 대응 모듈에서는 정보처리 모듈을 통하여 적절한 형태로 전송 정보를 가공하고, 침입차단시스템 제어 모듈을 통해 인터넷 웜에 의한 패킷을 차단한다. 또한, 웜 프로세스 격리 모듈을 통해 웜에 감염된 프로세스를 찾고, 이를 특정 위치에 격리시키며, 관리자 경보 메시지 전송 모듈을 통해 관리자에게 웜 감염 사실 및 프로세스 격리 내용을 전송한다.




(그림 1) Traffic Flow 기반 인터넷 웜 탐지 및 대응 방법

## 4. 패킷 유출량 비교




(그림 2) 웜 감염 시 패킷 유출 분포 및 제안 사항 적용 시 패킷 유출 분포도

(그림 2)는 일반적인 PC에서 스캔을 수행하였을 때 Outbound로 유출되는 패킷에 대한 통계 그래프와 제안하는 탐지 및 대응 방안을 적용하였을 경우 Outbound로 유출되는 패킷에 대한 통계를 나타내는 그래프이다. 그래프에서 알 수 있듯이 일반적인 PC에서 스캐닝을 수행하였을 경우는 순간적으로 Outbound로 유출되는 패킷의 양이 급증하였다가 스캐닝이 끝난 후 다시 원래대로 되돌아온다. 그러나, 제안하는 방식을 적용한 PC에서는 패킷이 임계치가 넘어가므로 스캐닝을 수행하는 프로세스를 종료시키고 격리시키기 때문에 스캐닝에 의한 패킷 증가가 거의 없다. 따라서, 네트워크에 유출되는 패킷이 정상 패킷이므로 안정적으로 네트워크를 운영할 수 있다.

## 6. 결 론

본 논문에서는 Outbound 트래픽을 이용하여 인터넷 웜을 탐지하고 이에 대응할 수 있는 방안에 대해 기술하였다. 본 방안은 트래픽 흐름 기반 스캐닝을 탐지하는 방식으로 각 개인의 PC에서 유출되는 인터넷 웜 패킷을 근본적으로 차단하고, 이를 통하여 안전한 네트워크 운영을 보장할 수 있도록 구성하였다. 또한, 인터넷 웜에 감염된 프로세스에 대한 격리 및 이동을 통하여 사후 웜의 분석에 도움을 줄 수 있도록 구성하였다. 향후 연구 방향은 설계된 내용의 구현을 통해 인터넷 웜에 대한 피해를 얼마나 줄일 수 있는지 확인할 것이며, 제안된 방안의 미비점을 보완하여 정교한 인터넷 웜 탐지 및 대응 방안을 마련할 것이다.

## 참 고 문 헌

[1] Dorothy, E. Denning, "An Intrusion Detection Model", IEEE Transactions on software engineering, Vol. SE-13, No. 2, FEB, 1987.

[2] Bishop, Matt, S. Cheung, C. Wee, "The Threat from the Net", IEEE Spectrum 34, 1997.

[3] Hebelin, L. T, "A Network Security Monitor", Proceedings of the 1990 IEEE Symposium, 1990.

[4] Steven, R. Snapp, "DIDS-Motivation, Architecture, and an Early Prototype", Proceedings of the Fifteen.

[5] D. Anderson, T. Frivold, and A. Valdes, "Next generation intrusion detection expert system(NIDES)", Technical Report SRI-CLS-95-07, 1995.

[6] Dan Gorton, "Extending Intrusion Detection with Alert Correlation and Intrusion Tolerance", Technical Report NO.27L at Chalmers University, 2003.

[7] Stuart McClure, Joel Scambray, and George Kurtz, "Hacking Exposed 4th edition", Found stone company, 2003.

[8] Richard Stones and Neil Matthew, "Beginning Linux Programming", Wrox press Ltd., 1999.

[9] Sang Hun Lee, "A Design and Implementation of Spam Mail Relay Prevention System in Linux Environment", 3rd EALPIIT2003 conference, 2003.

[10] 이상훈, 김우년, 이도훈, 박응기, "리눅스 환경에서의 침입방지시스템(IPS) 설계", 한국정보보증학회 정보보증논문지, Vol. 4, No 2, 2004.

### 이 상 훈

2000년 성균관대학교 정보공학과(공학사)
2002년 성균관대학교 전기 전자 및 컴퓨터 공학부(공학석사)
2002년~현재 국가보안기술연구소(연구원)