제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

# 인터넷 웜의 확산 모델과 방어 모델 연구

서 동 일*, 김 환 국*, 이 상 호**
* 한국전자통신연구원 네트워크보안구조연구팀
** 충북대학교 컴퓨터공학과

## 요 약

최근에 피해가 보고되고 있는 인터넷 웜은 최초발생 후 단 며칠 만에 전 세계적인 피해를 입히고 있다. 이들 웜들은 메일을 비롯한 기타 여러 가지 경로를 통해 스스로 복제하는 성질을 이용하여 매우 빠른 속도로 전파가 가능하다. 하지만 이를 제대로 막을 수 있는 수단은 마련되지 못하고 있다. 따라서, 인터넷 웜으로부터 네트워크 자산을 보호하기 위해, 체계화되고 자동화된 방지 메카니즘의 인터넷 웜 분야의 연구가 필요하다. 이에, 본 논문에서는 인터넷 웜의 확산과 방어 모델을 기술하고자 한다.

# A Study on the Propagation and Defense Model of Internet Worm

Seo Dong-il*, Kim Hwan-kuk*, Lee Sang-ho**

## ABSTRACT

In these days, many reports noticed that the Internet worms spread out and have done considerable damage to all over the world network within a few days. The worms, which is infected from various route such as e-mail, can spread very fast with common property, self replication. But, there is not prepare for the way effectively to interrupt internet worm. Therefore, to prevent our network resource, internet hosts and user clients, the systemic categorization and automatic defense mechanism is required in the Internet worm research. Hence, in this paper, we describe internet worm propagation and defense model.

## 1. 서 론

일반 PC사용자들의 가장 큰 보안 위협으로 인식되고 있는 바이러스는 빠른 네트워크 환경구축과 인터넷 인구의 증가로 그 피해가 더욱 커지고 있다. 최근 악성프로그램으로 인한 피해의 특징은 네트워크 및 이메일을 비롯한 기타 여러 가지 경로를 통해 스스로 복제하는 성질을 이용하여 매우 빠른 속도로 전파되어 그 확산속도가 급속도로 발전했다는 점과 서비스 거부 공격 등의 해킹공격이 이용되어 최초 발생 후 단 며칠 만에 전 세계적인 피해를 입히고 있다. 하지만 이를 제대로 막을 수 있는 수단은 마련되지 못하고 있다. 따라서 현재 나타나 있는 인터넷 웜 공격 및 각종 해킹 기법을 분석하고, 기존의 인

터넷 웜에 대한 대응 기술을 체계화하여 보다 새롭게 발생하는 웜에 대하여 유연하게 대응할 수 있는 방안을 마련하는 것이 필요하다.

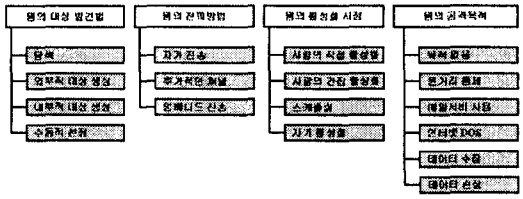
본 논문에서는 인터넷의 발전과 함께 증가하는 인터넷 웜의 발생에 대한 대응 기술을 체계화하여 새롭게 발생하는 웜의 확산을 막기 위한 방안을 마련하기 위해 웜의 확산력과 파급력에 영향을 미치는 요인들을 분류의 기준으로 삼음으로써 인터넷 웜 확산과 방어 모델에 적합한 분류 기준을 제시하였다. 그리고, 인터넷 웜의 특성과 분류에 따른 인터넷 웜 확산 모델을 살펴보고, 마지막에는 웜 확산 방지 모델에 대해 기술하고자 한다.

## 2. 최신 인터넷 웜의 특징 및 분류

### 2.1. 최근 인터넷 웜의 특징

최근에는 새로운 바이러스나 매크로 바이러스, 트로이목마와 같은 유형의 악성프로그램의 출현은 감소하는 반면 웜 유형의 출현 건수는 꾸준히 증가하고 있다. 이러한 웜은 전파속도가 빨라서 단 몇 시간 만에 전 세계적으로 확산되어 엄청난 피해를 일으키고 있으며 바이러스와 해킹의 기법을 덧붙인 변종들의 꾸준히 등장하는 등 날로 지능화되어가고 있다. 해킹기법을 사용하여 다른 시스템에 불법으로 침입하여 바이러스 기법으로 트로이목마 같은 악성 코드를 심어 놓고 나서 전파하는 형태, 바이러스의 전파를 위해 다른 시스템을 검색하거나 서비스 거부 공격을 가하는 형태가 출현하여, 그 구분조차 모호해지고 있는 실정이다. 이러한 다양한 기능을 동시에 사용하는 보다 발전된 웜의 등장은 앞으로도 계속되어 현재에 나타난 이상의 많은 피해가 발생할 것이다.

### 2.2. 인터넷 웜의 분류



(그림 1) 인터넷 웜을 위한 새로운 분류체계

| 이름 | 웜의 대상 발견법 | 웜의 전파방법 | 웜의 활성화 시점 | 웜의 공격목적 |
|---|---|---|---|---|
| 코드 레드 | - 탐색<br>- 내부적 대상 생성 (보안 취약성 공격) | 자가 전송 | 자가 활성화 | -목적 없음 (트래픽 증가)<br>-데이터 손상<br>-HTMP-프록시 서버 |
| 클러즈 | 탐색 | 자가 전송 | 자가 활성화 | -데이터 손상 |
| 멜리사 | 탐색 | 자가 전송 | 사람의 직접 활성화 | -HTMP-프록시 서버<br>-인터넷 DOS |
| 블래스터 | 내부적 대상 생성(취약성 공격) | 추가적인 채널 | 자가 활성화 | -원거리 통제<br>-인터넷 DOS |
| 씨캠 | 탐색 | 자가 전송 | 사람의 직접 활성화 | -목적없음 (트래픽 증가)<br>-원거리 통제<br>-데이터 손상 |

(표 1) 새로운 분류 체계에서의 대표적인 인터넷 웜의 분류

웜은 매우 다양한 유형 및 특성을 갖고 있으며 시간이 흐를수록 점점 복잡하고 교묘한 방법으로 전파하여 우리에게 많은 피해를 준다. 웜의 전파로부터 피해를 줄이기 위해서는 웜의 특성을 알아야하고, 그러기 위해서는 웜의 특성을 몇 개의 기준으로 분류하는 작업이 요구된다. 이러한 분류 기준에 대해 아직 공식적으로 정해진 표준은 없다. 다만 영향력 있는 몇몇 보안업체들의 암묵적인 관습에 따라 [플랫폼],[이름],[변형정

도]등의 형태로 분류를 하여 이름 짓고 있다.

한국정보보호진흥원(KISA)과 국내 백신업계(안철수 연구소, 하우리), 학계 등과 공동으로 작성한 이 분류의 기준은 ▲악성 프로그램 정의에 의한 분류, ▲운영체제에 의한 분류, ▲감염 영역에 따른 분류, ▲감염 경로에 의한 분류, ▲악성 프로그램 증상에 의한 분류 등 5가지로 나누어진다. 기존의 인터넷 웜의 분류 기준은 플랫폼, 이름, 감염영역, 감염 경로, 증상 등에 따른 것이라고 볼 수 있다. 이러한 분류기준들은 기본적으로 바이러스와 함께, 악성 코드를 특성 지을 수 있는 중요한 요소라고 볼 수 있다[1].

그러나 웜의 빠른 전파를 막는 방지모델에서는 웜의 확산력과 파급력에 영향을 미치는 요인들을 분류의 기준으로 정한다면 새로운 웜을 발견하였을 때, 이 웜의 특성을 신속히 파악하여, 최대한 빠르게 전파를 막을 수 있을 것이다. 그 중심적인 내용을 요약한 내용은 그림 1과 같고, 그 분류를 통하여 대표적인 웜을 분류하여 그 효용성을 보였다.(표 1)

## 3. 인터넷 웜 확산 및 방지 모델

### 3.1. 인터넷 웜 확산 모델[2][3][4]

가. 전통적인 전염 모델

생물학의 방역(epidemic)학에서 발전된 모델링으로, 고정된 감염률($\beta$)의 개념을 최초로 소개하고 이를 생물학적인 바이러스에 적용하여, 시간이 지남에 따라서 바이러스의 호스트(인간을 포함한 생물)의 변화의 추이를 수학적으로 모델링한 최초의 시도이며, 기본적인 컴퓨터 바이러스의 전파에 동일하게 적용가능하기 때문에, 현재까지 대부분의 바이러스의 전파분석에서 사용되는 모델이다.

나. Kermack-Mckendrick 모델

Kermack-Mackendrick은 바이러스가 감염되는 이전의 모델이 실제 바이러스의 치료의 효과를 반영하지 못하기 때문에, 적절한 치료율($\gamma$)을 도입하여 바이러스에 감염된 호스트의 치료모델을 추가하였다. 컴퓨터 바이러스에서도 대부분 적용가능 하지만 실제로 사람에 의한 치료를 가정하여 고정된 치료율을 사용하는 것이 대부분이다. 새로운 바이러스에 대한 자동적인 치료가 가능한 모델을 고안하는 것은 여전히 미해결된 문제(open problem)이다.

다. 두요소 모델(Cliff Changchun Zou, Two-factor Model, 2001)[4]

실제 코드레드의 확산을 분석하여 보면, 앞서서 제시한 연구들의 고정된 감염률 및 치료만으로는 해결되지 않는 경우가 많기 때문에, 이에 대한 해결을 위하여 두 가지 새로운 모델이다. 즉, 실제 코드레드의 전파에서 발생한 점은 코드레드가 전 세계적으로 대부분의 네트워크에 감염된 시점에서 네트워크의 병목현상으로 바이러스의 감염율이 시간에 따라서 감소하였기 때문에 감염율이 일정한 상수가 아닌 시간에 따라서 변한다는 사실과, 사람이 감염된 호스트 뿐만 아니라 감염되지 않은 호스트들도 백신을 설치하거나 소프트웨어를 패치 하여 감염대상을 줄이는 사실을 발견할 수 있었다. 이에 따라서 실제 코드레드가 특정 임계시점 이후로는 더 이상 감염이 진행되지 못하고 정체되거나 오히려 줄어드는 현상을 설명할 수 있었다.

라. 격리 모델(Cliff Changchun Zou, Dynamic Quarantine Model, 2003)[5]

인터넷 웜이 웜의 전파에 있어서 특정한 패턴을 가지고 있기 때문에, 새로 발생한 웜이라고 하더라도 호스트의 내부에서 특정한 패턴의 작업을 수행하는 경우에는 인터넷 웜이라고 간주하고, 방화벽과 같이 일정시간동안 전체 네트워크의

다른 호스트에 영향을 미치는 특정 호스트의 웜의 프로그램의 활동을 격리할 수 있다. 이 모델에서는 호스트를 기반으로 하지만 이에 대한 구현은 관심을 가지지 않고, 임의의 바이러스에 감염되었다고 하더라도 이를 고정된 격리률($\lambda$)을 통하여 설명하였다. 그러나, 이는 실제 새로운 인터넷 웜의 경우에도 잘 발견할 수 있는 호스트에 상주하는 프로그램을 구현하는 것이 미해결의 문제이기 때문에 실효성을 담보할 수 없으며, 동시에 구현에 대한 정보가 부족하기 때문에 실질적인 수준의 격리율을 제안하지 못한다는 단점이 있다. 또한, 이 모델은 특정 시간동안에 인터넷 웜에 감염된 프로그램이 사용하는 네트워크 포트 전체를 격리하는 모델을 간주하고 있기 때문에, 웹서버와 메일서버의 경우에는 오류의 상황에서도 서비스가 차단됨으로 인하여 실제 사용에는 힘든 점이 있다.

### 3.2 인터넷 웜 방지모델

현재까지 존재하는 인터넷 웜에 대한 방지 모델은 크게 적극적인 방지모델과 수동적인 방지모델로 나눌 수 있다. 적극적인 방지 모델은 웜이 전파되는 것에서 아이디어를 얻어서, 웜의 전파에 따라서 동적으로 대응하면서 예방 및 치료를 하는 모델과, 이 모델에는 백신 웜, 지뢰의 방식을 사용한 역추적 웜과 스나이퍼 웜 등이 있다. 수동적인 방지 모델은 방화벽 및 라우터 등의 위치에서 작동하며, 주소를 기반으로 차단하는 주소기반 차단 모델과, 내용을 비교분석하여 웜을 차단하는 내용기반 차단 모델 등이 있다. 그러나 적극적인 방지 모델은 모델의 효율성은 좋지만, 아직 실질적인 구현에 관하여는 특별한 대응책이 없다는 단점이 존재하고, 내용기반 차단모델은 웜의 전파속도를 늦추는 것은 분명하지만 결국은 웜의 전파 및 네트워크의 부하를 근본적으로 차단할 수는 없다는 한계점이 존재한다.

## 4. 결론

본 논문에서는 인터넷 웜 확산 및 방지 모델 연구를 위해 인터넷 웜에 해당하는 악성코드들을 분류하는 보다 효율적인 기준을 제시하였다. 이러한 분류는 새로운 인터넷 웜에 대한 신속한 분류 및 대응을 도울 수 있을 것이다.

또한, 인터넷 웜이 어떻게 얼마나 빠르게 전파하고 결과적으로 어느 범위까지 전파할 수 있는지의 인터넷 웜 확산 모델과 인터넷 웜의 확산을 막는 방법을 크게 둘로 나누어서, 적극적인 방법으로 웜과 마찬가지로 동적으로 이동하면서 웜을 치료하거나, 웜이 걸리지 않는 호스트들을 예방하는 것과 수동적인 방법으로 인터넷 라우터의 위치에서 악성적인 코드를 보내는 주소 혹은 내용을 차단함으로서 웜의 확산을 막는 인터넷 방지 모델에 대해 분석하였다.

## 참고문헌

[1] 한국정보보호진흥원, "바이러스 분류안 표준화 추진",http://www.kisa.or.kr/press/2003/press_01_20030116.html

[2] Nicolas Weavor, Vern Paxson, Stuart Stanifod, Robert Cunningham, "A Taxonomy of Computer Worms" , 2003

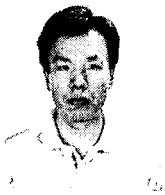
[3] Nicolas Weavor, " Potential Strategies for High Speed Active Worms : A Worst Case Analysis " U.C Berkeley BRASS Group, 2002

[4] Cliff Changchun Zou, Weibo Gong, Don Towsley. "Code Red Worm Propagation Modeling and Analysis". *9th ACM Conference on Computer and Communication Security (CCS'02)*, Nov. 18-22, Washington DC, USA, 2002

[5] Cliff Changchun Zou, Weibo Gong, and Do

n Towsley. "Worm Propagation Modeling a nd Analysis under Dynamic Quarantine De fense". *ACM CCS Workshop on Rapid Ma lcode (WORM'03)*, Oct. 27, Washington D C, USA, 2003

서 동 일



1989년 : 경북대학교 전자공학과 공학사
1994년 : 포항공과대학교 정보통신학과 공학석사
2002년 : 충북대학교 전자계산학과 (박사과정 수료)
1989. 1.~1992. 2. : 삼성전자종합연구소
1994. 3.~현재 한국전자통신연구원 네트워크보안구조연구팀장

김 환 국

1998년 : 한국항공대학교 전자계산학과 이학사
2000년 : 한국항공대학교 컴퓨터공학과 공학석사
2000. 9.~2002. 4. 이레스페이스
2002. 5.~현재 한국전자통신연구원 네트워크보안구조연구팀

이 상 호

1976년 : 숭실대학교 전자계산공학사
1981년 : 숭실대학교 대학원 시뮬레이션 공학석사
1989년 : 숭실대학교 대학원 컴퓨터네트워크 공학박사
1981년 ~ 현재 충북대학교 컴퓨터과학과 교수