情報保護學會論文誌
第16卷 第3號, 2006. 6

시간적인 행동 패턴을 고려한 웜의 정형 표현 기법 연구*

이 민 수[1†], 손 태 식[2], 조 상 현[1], 문 종 섭[1‡], 김 동 수[3], 서 정 택[3], 손 기 욱[3]
[1]고려대학교, [2]삼성전자, [3]국가 보안 기술 연구소

A Study of Formalized Presentation of Worm based on time-based Behavioral sequences.*

Min-Soo Lee[1†], Tae-Shik Shon[2], Sang-Hyun Cho[1], Jong-Sub Moon[1‡]
Dong-Soo Kim[3], Jung-Taek Seo[3], Ki-Wook Sohn[3]
[1]Korea University, [2]Samsung Electronics, [3]National Security research institute

요 약

현재 안티 바이러스 회사들을 중심으로 제작되는 웜의 분석 보고서는 기존의 바이러스 보고서의 형태를 가지고 있어, 웜의 특성들을 제대로 표현하지 못한다. 이에 본 논문에서는 웜의 특성을 표현 할 수 있도록 시간적인 행동 순서를 고려한 정형화 된 표현기법을 제안한다.

이를 위해 감염된 호스트와 감염 대상이 되는 호스트 사이의 발생하는 웜의 행동 패턴과, 통신 메시지들을 중심으로 정형화 된 양식을 정의한다. 앞서 정의된 양식을 중심으로 웜의 분석된 데이터를 표현 할 수 있는 방안에 대해서 제안하고, 검증을 위해 시만텍에서 제공하는 분석 데이터와 비교하였다.

ABSTRACT

Worm analysis report currently produced by anti-virus companies closely resemble those of virus report and do not properly characterize the specific attributes of worms. In this paper, we propose formalized presentation method based on time-based behavioral sequences to more accurately characterize worms. we define a format based on the behavior and communication patterns that occur between an infected host and a target host. we also propose a method for presently worm analysis data with that format. we also compare our framework with analysis data provided by Symantec

Keywords : *Worm, Worm Behavioral Sequences, Taxonomy of Worm*

Ⅰ. 서 론

인터넷 웜은 컴퓨터 바이러스와 매우 유사한 의미로 사용되며, 이에 대한 연구 또한 많은 부분이 바이러스 분석기술의 연장선상에서 연구가 진행되었다. 인터넷 웜은 바이러스와는 달리, 네트워크를 통하여 스스로 전파되는 특성을 갖는다.

따라서 기존의 바이러스 분석 보고서 형태의 표현 방식을 그대로 웜의 분석 보고서의 표현 방식으로 활용하기에는 웜의 동적인 특성을 표현하는 점에서 한

접수일: 2006년 1월 25일; 채택일: 2006년 6월 8일
* 본 연구는 국가보안기술 연구소 연구과제 지원 사업에 연구결과로 수행하였습니다.
† 주저자, leesle@korea.ac.kr
‡ 교신저자, jsmoon@korea.ac.kr

계를 갖는다. 따라서 본 논문에서는 웜의 동적인 특성을 표현 할 수 있도록 시간의 흐름에 따라 웜의 행동패턴을 표현 할 수 있는 방안에 대해서 제안한다.

본 논문에서는 감염된 호스트와 공격 대상 호스트 사이에 발생되는 웜의 시간적인 행동패턴에 초점을 맞추어, 각 호스트 상에서 웜의 행동 패턴을 4단계로 정의하고, 각 단계별 통신 메시지를 중심으로 정형화된 표현 방안을 제안한다.

논문의 서술 순서는 다음과 같다. 2장에서는 인터넷 웜의 분류 방법을 서술하고, 3장에서는 웜의 시간적인 행동 및 공격 패턴의 분류 방법을 제안한다. 4장에서는 3장에 정의된 시간적인 행동 패턴에 따른 표현방법을 도출하고, 마지막으로 5장에서 결론 및 향후 연구방향을 기술한다.

II. 관련 연구

인터넷 웜은 네트워크를 통해 스스로 전파되는 특성에 의해 전파 시 일정한 패턴을 가지고 행동한다. 웜의 일정한 패턴에 대한 연구는 웜의 전파 방식에 의한 분류 기법과 웜의 세부 행동 패턴에 대한 분류 기법으로 연구가 진행 되고 있다. [1,3,5]

웜의 전파방식에 의한 분류기법은 시만텍을 중심으로 연구되었는데, Darrell Mkienzle 등에 의해 기존의 바이러스에 관한 축적된 자료를 토대로 웜의 전파특성에 따라 크게 전통적인 웜, 윈도우 파일 공유 웜, 이메일 웜등 총 3가지로 표 1과 같이 분류하였다. [1]

표 1. Darrell M.Kienzle등의 웜 분류

이름	분류 기준
이메일 웜	이메일을 통하여 전파되는 웜
윈도우 파일 공유 웜	윈도우 파일공유를 통하여 전파되는 웜
전통적인 웜	외부의 영향 없이 스스로 전파되는 웜

표 1과 같이 웜의 전파과정에서 사용하는 방식에 의한 분류로, 각 웜들이 전파되는 행동패턴에 대해 구분이 가능하다.

Nazario등은 웜의 행동패턴을 세부적인 기준에 의해 분류하였다. [3] 즉, 하나의 웜이 자신을 전파하기 위하여 대상 호스트를 찾는 모듈, 실제 목표시스템을 공격하는 모듈, 같은 종류의 웜에 감염된 호스트 사이의 통신 모듈, 공격의 결과 감염된 호스트들의 2차적인 행동모듈, 웜을 효율적으로 전파하기 위해 웜 노드들에게 다양한 정보를 제공해 주는 모듈 등으로 분류하였다.

Nazario등의 분류방법과 유사하게 Nicholas weaver등은 웜의 행동 패턴을 기준으로 표2와 같이 5가지의 구성 요소로 분류하고, 각 요소에 따라 발생 가능한 세부종류를 정의하였다. [5]

표 2. Nicholas weaver등이 제안한 웜 분류 [5]

구성 요소	세부 종류
Target discovery	Scanning ,Pre-generated target lists, Externally generated target lists, Internal target lists, Passive
Carrier	self-carried, Second-channel, Embeded
Activation	Human activation, Human activity-based activation, Scheduled process activation, Self-activation
Payloads	None/non-functional, Internal remote control, Spam-relays, HTML-proxies, Internet dos, Data collection, Data damage, Worm maintenance
Motivation and attackers	Experimental Curiosity, Pride and Power, Commercial Advantage, Extortion and Criminal Gain, Random Protest, Political Protest, Terrorism, Cyber Warfare

기존의 웜 분류에 대한 연구 사례들은 웜의 행동패턴에 대한 정형화 가능성을 보여준다.

III. 웜 행동의 순서에 따른 정형 표현기법 제안

본 논문에서는 인터넷 웜의 정형화 된 행동패턴을 정의하기 위하여 인터넷 웜의 전파 과정에서 발생하는 통신 메시지(통신 데이터)의 흐름을 기준으로 웜의 시간에 따른 행동 패턴을 정의한다.

웜 감염 호스트와 공격 대상 호스트 사이의 행동패턴과 통신 메시지를 단계별로 정의하였으며, 정의된 메시지를 기준으로 웜의 종류에 따른 공격의 패턴 타입의 분류 방식을 제안한다.

1. 웜의 시간에 따른 행동 패턴

웜이 전파될 때 일반적인 행동 패턴은 감염 호스

트와 공격 대상 호스트에 따라 다른 패턴을 나타낸다. 먼저 감염 호스트에서 행동 패턴은 대상 호스트 선정을 위한 스캔 메시지를 전송 단계, 시스템 장악을 위한 공격 코드 메시지 전송 단계, 웜 코드 전송 단계, 감염된 웜의 특성에 따른 행동진행 단계를 가진다.

공격 대상 호스트는 감염 호스트로부터 전송 받은 스캔 메시지에 응답하는 단계, 시스템을 장악 당하는 단계, 코드를 전송 받는 단계, 감염된 웜의 특성에 따른 행동진행 단계를 가진다.

본 논문에서는 웜의 정형화된 시간에 따른 행동 패턴을 정의하기 위하여 웜의 전파과정에서 통신 메시지의 특성들을 대상으로 단순화하여 그림 1과 같이 4가지 종류의 단계의 행동패턴을 정의한다.

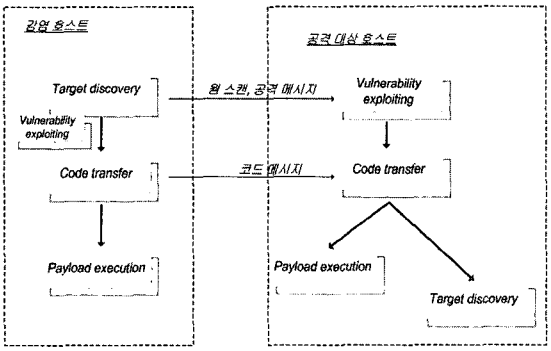


그림 1. 웜의 시간에 따른 행동패턴

행동패턴의 4단계는 그림 1과 같이 Target discovery, Vulnerability exploiting, Code transfer, Payload execution 단계로 정의 하였으며, 각 단계는 각 호스트의 상태(감염, 공격대상)에 따라 다른 행동패턴을 가진다.

감염 호스트는 웜이 활동하는 상태이기 때문에 Vulnerability exploiting 단계가 발생하지 않고, 대상 호스트 선정 및 공격을 위한 Target discovery 단계와 코드 전송을 위한 Code transfer단계, 웜의 특성에 따른 행동패턴을 진행하는 Payload execution 단계로 구성된다.

공격 대상 호스트의 경우 웜의 스캔 메시지와 공격 메시지에 반응하는 Vulnerability exploiting 단계부터 진행되어, Code transfer 단계 후 Payload execution 단계와 Target discovery 단계로 구성된다.

그림 1의 4단계의 행동 패턴들은 표현 대상이 되는 웜의 특성에 따라 표 3과 같은 세부적인 패턴으로 표현 할 수 있으며, 본 논문에서는 웜의 특성들을 기준으로 표 3과 같이 각 행동 패턴의 단계에 따라 발생 가능한 세부패턴을 정의한다.

표 3. 웜의 행동패턴 단계별 세부패턴

행동 패턴 단계	세부 패턴	설 명
Target discovery	랜덤 스캐닝	대상 호스트 선정 시 임의의 값을 추출
	변형된 랜덤 스캐닝	랜덤 스캐닝에 효율성 공유 알고리즘 적용
	최초 전파 전 생성대상 리스트	웜 코드에 대상 호스트 하드 코딩
	외부 생성대상 리스트	외부의 메타서버를 활하여 대상 호스트 선정
	내부 대상 리스트	감염 호스트 내부의 주소정보 활용
	수동적인 방식	감염 대상 호스트가 감염 호스트에 접속하도록 유도
Vulnerability exploiting	OS의 취약성	OS 취약점 이용
	소프트웨어의 취약성	응용프로그램 취약점 이용
	관리 실수	관리자 실수 이용
	프로토콜 취약성	프로토콜 자체 취약점 이용
Code transfer	자가 전송	스캔 및 공격과 동시에 코드전송
	세컨드 채널	스캔 및 공격과 다른 통신 채널 이용
	임베디드	안전한 통신 채널로 알려진 라인 이용
Payload execution	기능 없음	기능 없음
	호스트 제어	감염 호스트 제어
	스팸 발송	스팸 메일 서비스 제공
	프록시	프록시 용도로 사용
	DoS 공격	DoS공격용 좀비로 사용
	데이터 수집	데이터 수집 기능
	데이터 훼손	데이터 삭제 및 수정기능

2. 웜 공격패턴에 따른 유형 분류

웜 전파 과정에서 감염 호스트와 감염 대상 호스트 사이에는 일정한 패턴의 통신 메시지가 발생 하는데, 본 절에서는 이러한 통신 메시지를 이용하여 웜의 종류 별 공격패턴을 분류해보고자 한다.

웜의 전파과정에서 발생 가능한 통신 메시지들은 '대

상 호스트를 찾기 위한 스캔 메시지', '대상 호스트를 공격하기 위한 공격 코드 메시지', '자기 복제 코드 전송을 위한 메시지', 마지막으로 '웜 제작자의 의도에 따른 다양한 행동에 의해 생성되는 메시지'들이 존재한다.

실제 웜의 전파를 위한 행동 패턴에서는 각 메시지들이 동시에 발생하는 하는 경우와 각각 순차적으로 발생하는 경우가 나타난다. 각 통신 메시지의 발생형태(동시 발생, 개별 발생)를 이용하여 공격 패턴의 분류 기준을 정의하였다. 단, 웜 제작자의 의도에 따른 다양한 행동에 의해 발생하는 통신 메시지는 각각 매우 다양한 형태를 가지기 때문에 공격패턴의 분류 기준에서 제외한다.

먼저 통신 메시지는 Scan(스캔 메시지), Attack(공격 코드 메시지), Code(자기 복제 코드 메시지)로 정의하고, 각 통신 메시지의 발생 형태를 기준으로 표 4와 같이 공격 유형을 총 4가지 타입으로 정의한다.

표 4. 웜의 공격패턴 분류

타 입	공격 유형	웜	설 명
Type 1	{Scan},{Attack},{Code}	Sasser	각 코드 따로 전송
Type 2	{Scan+Attack},{Code}	Blaster	스캔과 공격 코드는 함께, 웜 코드는 따로 전송
Type 3	{Scan+Attack+Code}	Slammer	모든 코드 함께전송
Type 4	{Scan},{Attack+Code}	-	스캔코드, 공격과 웜 코드 전송은 함께

그림 2는 표 4에 정의된 타입을 기준으로 이미 감염된 호스트와 감염 대상이 되는 호스트 사이의 통신 메시지의 흐름을 이해하기 쉽게 표현한다.

그림 2-a는 스캔 메시지가 감염 대상 호스트에 전송이 되면, 취약점을 가지고 있는 감염 대상 호스트에서 스캔 메시지에 대한 반응을 하고, 다시 감염 호스트는 공격 메시지를 전송하며, 공격 메시지를 받은 감염 대상 호스트는 다른 통신 포트를 사용하여 웜 감염 호스트로부터 웜 코드를 전송 받아 감염 대상 호스트의 감염 행동을 위한 통신이 종료하는 과정을 보여준다. 그림 2-a와 같이 Type 1의 공격 유형은 Scan, Attack, Code 메시지들이 각각 전달되는 방식을 사용하는 웜이다. 그림 2는 Type1외에도 Type 2,3,4도 Scan, Attack, Code 메시지의 전달방법에 의해 분류되는 것을 표현한다.

웜의 공격 패턴에 따른 분류방법은 웜의 일반적인 행동패턴을 나타내는 기준으로 활용이 가능하며, 본 논문에서는 이를 정형화 된 웜의 분석 데이터의 표현에 적용하는 방안에 대해서 제안한다.

3. 정형화 된 표현 기법 제안

본 절에서는 앞서 제안한 웜의 시간에 따른 행동 패턴과 공격의 패턴타입에 따른 유형 분류를 기반으로 인터넷 웜의 정형화된 표현방식에 대해 제안해보고자 한다. 시간에 따른 행동 패턴과 공격 패턴의 효율적인

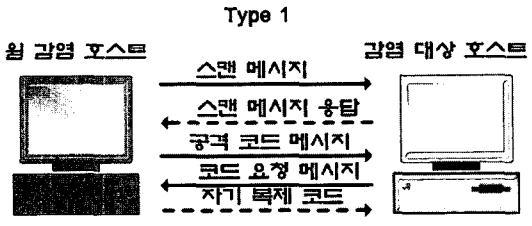


그림 2-a. Type 1 공격에 따른 메시지 패턴 유형

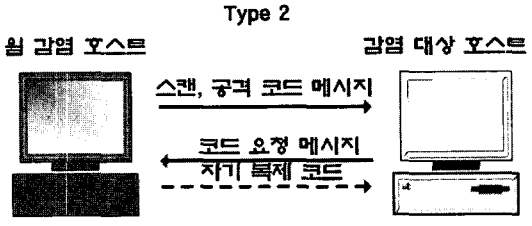


그림 2-b. Type 2 공격에 따른 메시지 패턴 유형

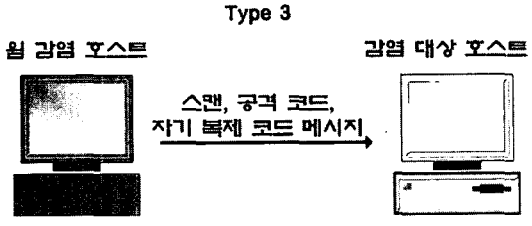


그림 2-c. Type 3 공격에 따른 메시지 패턴 유형

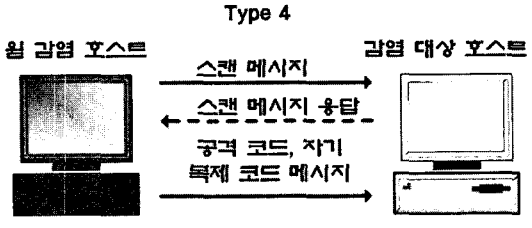


그림 2-d. Type 4 공격에 따른 메시지 패턴 유형

표현을 위하여 클라이언트/서버 모델을 적용하여 표현하였다. 즉, 이미 감염되어 다른 호스트를 감염 시키고 있는 호스트를 클라이언트의 역할로, 취약점을 가지고 있으면서 감염의 대상이 되는 호스트를 서버의 역할로 하여 분석할 웜의 시간에 따른 행동패턴과 공격패턴을 표현하는 방안에 대해 제안한다.

정형화 된 표현을 위하여 먼저, 통신 메시지의 영향을 주는 요소인 서비스 포트를 웜의 시간에 따른 행동패턴에 따라 표 5와 같이 정리하는 방법을 정의한다.

표 5. 전파 특성 표현법

웜 특성	설 명
공격 패턴타입	웜 공격패턴에 따른 유형 분류
취약한 서비스포트	Target discovery단계의 취약한 서비스 및 포트확인
공격 코드 전송	Vulnerability exploiting단계의 서비스 포트 확인
웜 코드 전송 포트	Code transfer단계의 서비스 포트 및 코드 이름 확인

표 5의 첫 번째 필드인 공격 패턴 타입은 표 4에서 제시한 유형정의에 의해 감염 호스트와 대상 호스트 간의 통신 메시지의 흐름에 대한 패턴이며, 그 외의 필드들에서 각 행위 순서별 사용 서비스 포트에 대한 정보들을 명시한다. 본 논문에서는 웜의 시간에 따른 행동 패턴을 정형화하여 표현하기 위해서 표 6과 같이 정형화 된 표현 방식에 대해 정의하고, 그림 3과 같이 절차적인 표현 형태를 정의한다.

표 6의 각 절차적인 표현 규칙은 그림 3의 각 숫자를 의미한다. 그림 3은 감염된 호스트와 대상 호스트 사이의 관계를 중심으로 표현하며, 각 호스트는 총 4가지의 시간적인 행동 패턴간의 관계와, 통신 메시지의 흐름을 중심으로 표현한다.

그림 3과 같이 절차 표현도의 시작은 감염 된 호스트의 Target discovery 단계에서 스캔 메시지를 전송하는 행동 패턴으로 시작되며, 표 3에서 제시하였던 시간에 따른 행동패턴의 따른 세부 분류표를 기준으로 스캔기법을 선택하여 표현한다. 그림 3의 ⑦과 같이 각 메시지에서 사용되는 서비스 포트 및 프로토콜 정보 또한 절차 표현도 내에 기술함으로써 인터넷 웜의 통신 메시지와의 관련성을 명확하게 표현 가능하도록 제안한다. 마지막으로 Payload execution 단계의 설명을 위해서 스캔 기법 표현방식과 같이 표 3에서 제시하였던 세부 분류에서 선택하여 기술 하도록 제안한다.

본 논문에서 제안한 절차적인 표현방법에 의한 분석 데이터는 실제 웜의 통신 메커니즘의 세부적인 내

표 6. 절차 표현도 규칙

시간에 따른 행동패턴의 절차표현도 규칙
1. 각 호스트는 총 4가지의 시간에 따른 4가지 행동 패턴을 갖는다. 2. 절차 표현도상 하나의 감염된 호스트와 하나의 대상 호스트로 표현한다. 3. 감염 호스트에서 대상 호스트로의 각 메시지는 오른쪽 방향의 화살표로 표현한다. 4. 대상 호스트에서 감염 호스트로의 각 메시지는 왼쪽 방향의 화살표로 표현한다. 5. 각 행위 순서 별 전달 가능 메시지를 갖는다. : 실제 발생 가능한 메시지 세부 형식을 표 3에서 선택하여 제시한다. Target discovery : 스캔 메시지, 공격 코드 메시지 Code transfer : 자기 복제 코드 메시지 Payload execution : 각 기능 메시지 6. 각 통신 메시지별 구분은 그림 2와 같이 화살표의 선 모양을 기준으로 한다. 7. 각 행위 순서별 관련 서비스 포트를 갖는다. 8. 스캔 메시지, 각 기능 메시지의 방식은 표 3의 분류표의 내용을 토대로 기술한다.

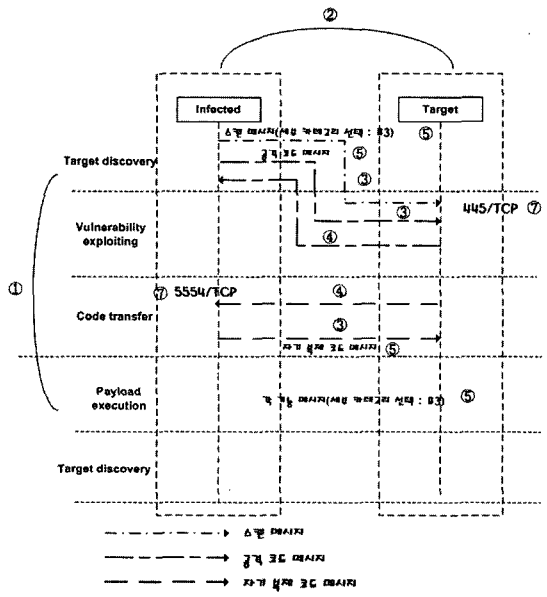


그림 3. 절차 표현도 정의

용을 파악 할 수 있는 점과 인터넷 웜이 동작 할 때의 동적인 속성 또한 표현 할 수 있는 장점을 가진다.

Ⅳ. 제안기법의 실험 및 검증

1. 검증을 위한 웜 분석 데이터 수집

본 논문에서 제안한 웜의 시간적인 행동패턴에 따른 정형화된 표현기법 사용하여, 웜의 행동 양식을 표현하기 위하여, 실제 웜의 행동 패턴에 대한 데이터를 수집한다. 이때, 사용한 환경은 그림 4와 같이 IBM에서 사용하였던 동적인 분석 기법을 확장한 가상 망을 사용한다.[6]

웜의 외부로의 전파 경로를 차단하기 위하여 분리된 가상 네트워크를 그림 4와 같이 2개를 구성하고, 웜의 전파에 필요한 환경을 만들기 위해 초기 감염된 호스트 역할을 하는 A와 감염 대상이 되는 호스트 B, 웜에 영향을 받지 않는 호스트 C를 가상 네트워크에 연결하여, 웜의 전파가 발생 할 때 각 호스트들에서 다양한 툴을 활용하여 웜의 행동 패턴을 분석 한다.

각 분석 데이터들을 수집하기 위하여 네트워크 레벨에서는 Ethereal 및 tcpdump를 시스템 레벨에서는 sysinternals에서 제공하는 FileMon, RegMon, TCP View, Pstools등의 분석툴을 사용한다.[10]

2.정형화 된 표현 기법 검증

정형화된 표현기법의 검증을 위해 W32.Sasser.B웜, W32.Blaster웜, W32.Slammer웜들을 대상으로 제안한 방법에 의해 분석 데이터를 표현 하였고, 시만텍의 securityresponse에서 제공하는 데이터와 비교하였다.

시만텍에서 제공하는 웜의 분석 데이터는 크게 위협평가, 기술적인 세부사항, 권장사항, 제거 지침 등 총 4가지형태의 웜 분석 데이터를 웜의 특성을 고려하지 않은 단순히 서술하는 표현 형태로 제공하고 있다.[9]

2.1 W32.Sasser.B웜에 대한 분석 데이터

2.1.1 정형화 된 표현기법

W32.Sasser.B웜은 lsass 취약점을 이용하여 전파되는 웜으로 2004년 5월에 처음 발견되었다.[11]

표 7. W32.Sasser.B 전파특성

웜 특성	실제 값
공격 패턴타입	Type 1
취약한 서비스포트	445/TCP(LSASS 취약점)
공격 코드 전송	445/TCP
웜 코드 전송 포트	5554/TCP(xxxx_up.exe)

표 7은 각 행위 순서에 따른 포트 변화의 특성을 보여 주고 있으며, 그림 5는 정형화 된 표현 기법에 따라 시간적인 행동 패턴을 절차적인 표현에 의해 클라이언트/서버 모델의 형태로 나타내고 있다.

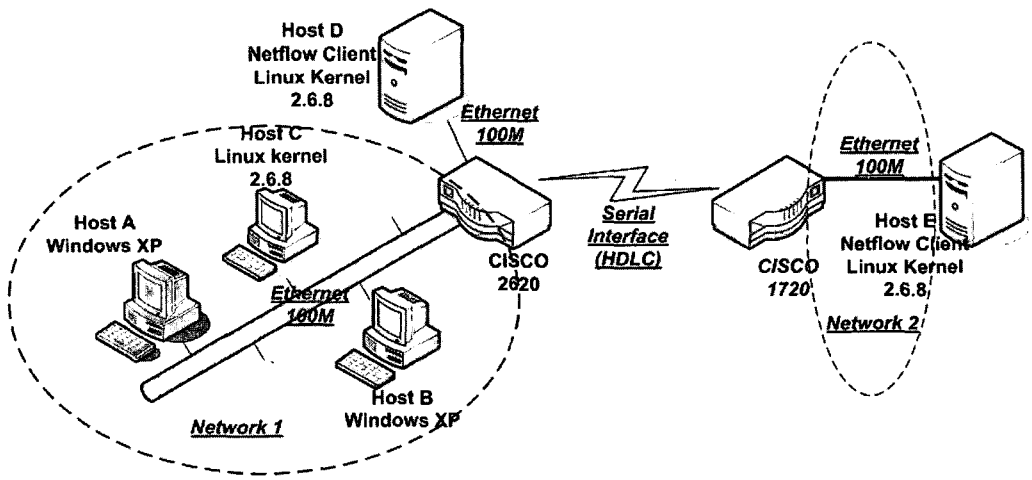


그림 4. 웜 분석을 위한 구축 환경

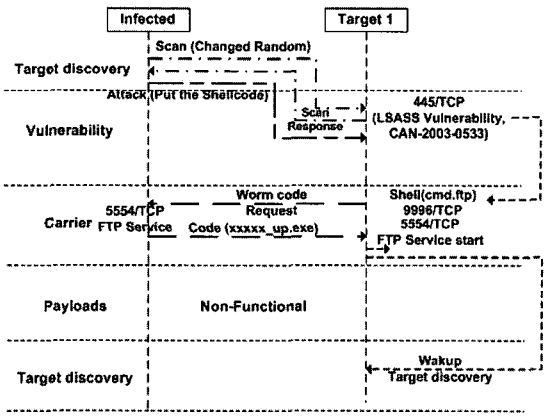


그림 5 W32.Sasser.B웜 절차 표현도

W32.Sasse.B웜은 공격유형은 그림 2-a와 같은 양식을 갖는 Type 1으로 Scan, Attack, Code 전송이 각각 발생한다. 먼저 Scan의 경우, 본 연구에서 제안한 웜 세부 분류 기준 중 변형된 랜덤 스캔기법을 사용하며, 스캔에 성공하면 공격 코드인 쉘 코드를 전송하고, 이 쉘 코드는 공격 성공 후 다시 초기 감염 호스트에 웜 코드 전송을 요청하고, 웜 코드를 다운로드 받아 저장한다.

W32.Sasser.B웜은 웜 자신의 웜을 전파 하는 것 외에는 다른 행동 패턴을 가지지 않는 것을 그림 5에서 표현하고 있다.

각 메시지별 특징은 표 8와 같이 표현한다. 표 8의 Scan 메시지의 알고리즘은 IP 주소의 각 옥텟별 생성 값들(x.x.x.x)의 생성 비율을 변경하여 네트워크로 전파되는 효율을 높이는 알고리즘을 사용한다. 표 8의 "a.a.a.x"에서 a는 감염 된 호스트 아이피의 각 옥텟 값을 의미한다.

표 8. W32.Sasser.B 통신 메시지 별 세부사항

통신 메시지	내용	
	유형	설명
취약한 서비스포트	변형된 랜덤	변형된 랜덤 사용하여 IP생성 x.x.x.x : 51.6% a.a.x.x : 25.0% a.x.x.x : 23.4%
공격 코드 전송	TCP 445포트를 사용하는 lsass 취약점을 이용 공격과 동시에 쉘 코드를 동작 시킴	
자기복제 코드 메시지	TCP 5554 포트를 사용하여 웜 코드 복제함 감염된 호스트로부터 ftp 프로토콜 이용	
각 기능 메시지	기능 없음	

2.1.2 시만텍 사의 분석 데이터[11]

시만텍의 분석 데이터는 2절의 시작에서 언급한바와 같이 추상적으로는 4가지 카테고리를 제공하고 있지만, 실제 웜 행동 양태는, 표 9와 같은 방식으로 설명이 되어있다[9]. 즉, 시만텍에서 제공하고 있는 분석 데이터는 표 9와 같이 인터넷 웜이 대상 호스트에 감염되는 시점에서부터 웜의 실행 코드를 분석하여 순차적으로 나열한 형태를 가지고 있다.

표 9. W32.Sasser.B 분석 자료(기술적 세부 사항)[9]

기술적 세부 사항
1. 'JumpallsNlsTillt'라고 불리는 뮤텍스(mutex)의 생성을 시도하고 실패하면 그냥 시스템을 빠져나옵니다. 이 뮤텍스는 시스템에서 한번 만 실행하도록 합니다. 2. 뮤텍스(mutex) "Jobaka3"를 생성을 시도하지만 활용 목적이 불분명합니다. 3. 자신을 %Windows 폴더%에 Avserve2.exe으로 복제 4. ....중략... 8. 웜이 Windows LSASS 취약점을 악용한 이후, Lsass.exe 프로세스가 종료될 것입니다. 또한 Windows에서 1분안에 시스템이 종료될 것이라는 메시지가 나타납니다.

2.2 W32.Blaster웜에 대한 분석 데이터

2.2.1 정형화 된 표현기법

W32.Blaster웜은 DCOM RPC 취약점을 이용하여 전파되는 웜으로 2003년 8월 11일에 처음 발견되었다.[12]

표 10. W32.Blaster 전파특성

웜 특성	실제 값
공격 패턴타입	Type 2
취약한 서비스포트	135/TCP(DCOM RPC 취약점)
공격 코드 전송	135/TCP
웜 코드 전송 포트	69/UDP(msblast.exe)

표 10은 W32.Blaster의 각 행동의 순서에 따른 포트 변화의 특성을 보여 주고 있으며, 이러한 데이터와 각 행동 순서에 기반 하여, 감염 된 호스트와 취약점을 가진 대상 호스트 사이의 관계는 다음과 같이 절차 표현도로 표현 할 수 있다.

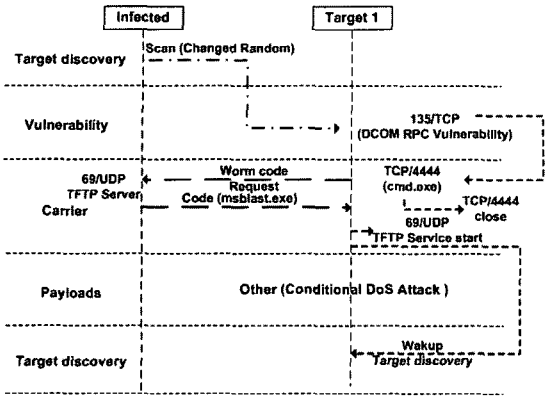


그림 6 W32.Blaster웜 절차 표현도

W32.Blaster웜은 공격유형은 Type 2유형으로, Scan과 Attack 메시지가 동시에 전송되고, 그 후 Code가 전송되는 순서를 따른다. 웜이 전파 될 때, 먼저 Target discovery 단계에서 본 연구에서 제시한 세부 분류 기준 중 변형된 랜덤 스캔기법을 사용하여 스캔을 하며 이때 스캔 동작 과정에서는 스캔 메시지와 함께 공격 메시지가 전송되어 스캔과 동시에 웜의 공격 시도가 발생한다.

따라서 W32.Sasser.B웜의 절차 표현도인 그림 5와는 다른 형태를 보인다. 스캔과 동시에 공격이 성공하면, 공격 코드에서 내부적으로 초기 감염 호스트에 tftp 프로토콜을 사용하여 웜 코드를 요청하고, 다운로드 받아 대상 호스트에 저장한다.

그림6은 W32.Blaster웜이 자기전파 외에 특정 사이트(Windowsupdate.com)에 대해 DoS 공격이 가능한 기능을 가지고 있음을 표현한다.

각 메시지별 특징은 표 11과 같이 표현한다.

표 11. W32.Blaster 통신 메시지 별 세부사항

통신 메시지	내용	
	유형	설명
취약한 서비스포트	변형된 랜덤	감염 호스트의 주소가 대상 호스트 선정에 영향을 미침
공격 코드 전송	TCP 135포트를 사용하는 DCOM RPC취약점 사용 스캔 패킷 동시에 공격 패킷을 전달	
자기복제 코드 메시지	UDP 69번인 tftp 서비스를 이용	
각 기능 메시지	날짜조건 기준에 의한 DoS공격 수행	

2.2.2 시만텍 사의 분석 데이터[12]

시만텍의 분석 데이터 중 기술적인 세부 사항의 내용은 표 11과 같다.

표 12. W32Blaster 분석 자료(기술적 세부 사항)

기술적 세부 사항
1. "Billy"라는 뮤텍스(mutex)를 만듭니다. 뮤텍스가 존재한다면 웜도 존재할 것입니다. 2. 다음 레지스트리에 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 아래의 값을 추가합니다. "windows auto update"="msblast.exe" 3. TCP 포트 135로 DCOM RPC 취약점을 이용해서 아래와 같은 작업을 수행할 데이타를 전송합니다. 숨김 파일로 cmd.exe 원격 셸을 만들어서 TCP 포트 4444를 감시합니다. ...중략... 5. 화면에 나타나지 않지만 다음과 같은 메시지를 포함하고 있습니다. I just want to say LOVE YOU SAN!! billy gates why do you make this possible ? Stop making money and fix your software!!

시만텍에서 제공하고 있는 분석 데이터는 표 12와 같이 인터넷 웜이 대상 호스트에 감염 되는 시점에서부터 웜의 실행코드를 분석하여 순차적으로 나열한 형태를 가지고 있으며, 바이너리 분석을 통해 동적인 분석 환경 하에서는 발견할 수 없는 데이터도 포함을 하고 있다.

2.3 W32.Slammer웜에 대한 분석 데이터

2.3.1 정형화 된 표현기법

W32.Slammer웜은 MS SQL의 취약점을 이용하여 전파 되는 웜으로 2003년 1월 24일에 처음 발견되었다.[2,13]

표 13. W32.Sasser.B 전파특성

웜 특성	실제 값
공격 패턴타입	Type 3
취약한 서비스포트	1434/UDP(MS SQL 취약점)
공격 코드 전송	1343/UDP
웜 코드 전송 포트	1343/UDP

표 13은 각 행위 순서에 따른 포트 변화의 특성을

보여 주고 있으며, 이러한 데이터와 각 행위 순서에 기반 하여 감염 된 호스트와 취약점을 가진 대상 호스트 사이의 관계를 Slammer웜은 다음과 같이 절차 표현도로 표현 할 수 있다.

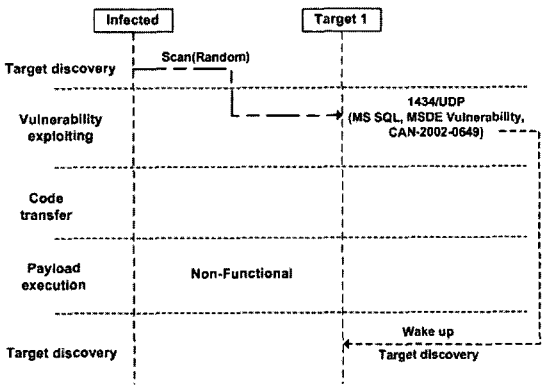


그림 7. W32.Slammer웜 절차 표현도

W32.Slammer웜은 Type 3로 스캔, 공격 코드, 자기 복제 코드 메시지 전송이 동시에 발생 하는 공격 유형을 가진다. Slammer웜은 앞서 표현한 웜들과는 달리 스캔 시 세부 분류 기준 중 랜덤 스캔기법을 사용하고, UDP 프로토콜을 사용한다는 것을 그림 7을 통해 표현 하였다.

W32.Slammer웜은 자기 전파 외에 다른 어떠한 행동 패턴도 갖지 않는 다는 것을 확인 할 수 있다.

각 메시지별 특징은 표 14와 같이 표현한다.

표 14. W32.Slammer 통신 메시지 별 세부사항

통신 메시지	내용	
	유형	설명
취약한 서비스포트	랜덤	대상 호스트를 랜덤하게 선정
공격 코드 전송	TCP 445포트를 MS SQL 2000 서버의 SQL Resolution 취약점을 사용 UDP 1434포트를 사용하여 공격 코드가 전달 스캔 패킷 동시에 공격 코드 패킷이 전달	
자기복제 코드 메시지	스캔 패킷과 동시에 자기 복제 코드 전송	
각 기능 메시지	기능 없음	

2.3.2 시만텍 사의 분석 데이터[13]

시만텍의 분석 데이터 중 기술적인 세부사항의 내용은 표15와 같다.

표 15. W32.Slammer 분석 자료(기술적 세부 사항)

기술적 세부 사항
W32.SQLExp.Worm이 시스템 성능을 저하시키면 다음과 같은 현상이 일어납니다. 1. 악성 패킷을 전송하는 무작위 IP주소 생성하기 위해 Windows API 기능인 "GetTickCount"를 이용합니다. 2. 반복적으로 자신을 임시 포트에서 1434 UDP 포트의 모든 IP 주소로 전송합니다. 3. W32.Slammer.Worm은 계속해서 다른 IP 주소로 패킷을 전송하며, 이로써 서비스 거부 공격 (Denial of Service) 이 발생합니다.

시만텍에서 제공하고 있는 분석 데이터는 표 15와 같이 인터넷 웜이 대상 호스트에 감염 되는 시점에서부터 웜의 실행코드를 분석하여 순차적으로 나열한 형태를 가지고 있으며, 바이너리 분석을 통해 동적인 분석 환경하에서는 발견할 수 없는 데이터도 포함을 하고 있다.

2.4 장/단점 비교 분석

인터넷 웜의 정형화에 대한 연구는 공개되어 있는 데이터의 한해서 진행 된 바가 없다. 따라서 이를 비교 및 검증하기 위해서 본 논문에서는 기존의 바이러스 분석 보고서 형태를 웜에 그대로 적용하여 사용하는 안티 바이러스 회사의 분석 보고서를 비교 대상으로 선정하였다.

안티 바이러스 회사 중 대표적인 시만텍의 분석 보고서와 표 16과 같이 비교한다.

시만텍에서 제공하는 웜 분석 보고서와 본 논문에서 제안하는 시간적인 행동 패턴에 따른 표현기법은 웜의 행동에 대한 분석 데이터라는 점은 유사하지만, 표현 형식, 제공 데이터, 분석 접근 방법 등에서 많은 차이점을 보인다.

표 16. 분석 데이터 표현기법 비교

	제안된 기법	시만텍
표현 형식	행위 순서별 상관관계를 동적으로 제시	웜 실행순서에 따라 나열 형으로 제시
표현 데이터	감연 호스트와 공격대상 호스트 사이의 통신 메시지 및 정보 중심의 데이터 표현	웜 코드에 들어 있는 명령어 셋의 해석을 통한 세부 데이터 표현
주요 분석 접근 방법	동적인 분석 기법 (가상 망 환경 분석 기법)	정적인 분석기법 (리버스 엔지니어링)
가독성	간결하고 명확함	세부적인 행동 확인
차이점 파악	웜의 행동 패턴 구분가능	웜 간의 차이점 구분 어려움

표 16에서와 같이 정형화된 표현 방식의 장점은 시만텍에서 제공하는 분석 데이터 표현 방식과 비교하여, 간결하고 명확하게 웜의 전파 진행 과정을 동적으로 표현 할 수 있는 장점을 가진다. 백신의 시그니처를 위한 웜 분석 데이터 외에 웜 탐지 및 대응, 전파 특성 분석 등의 다른 분야에서는 사용되지 않는 데이터를 표현 형식에서 제외시킴으로써 표현 데이터의 효율성을 높였다.[4,8]

마지막으로 웜의 공격 패턴에 따른 유형을 정의하여 표현 방식에 적용함으로써, 정형화된 표현 기법을 이용한 분석 데이터는 분석된 웜들의 특성에 따른 분류가 쉬어지며, 웜들의 영향을 쉽고 빠르게 예측이 가능하다.

V. 결론 및 향후 연구

본 논문에서 우리는 시간에 따른 웜의 행동패턴을 정형화하여, 이를 웜의 분석데이터의 표현방식에 적용 시키는 방안에 대해 제안하였다. 특히 웜의 행동패턴을 단계별로 분류함으로써 웜의 능동적인 행동패턴에 대한 표현이 가능하도록 정의하였다. 본 논문에서 제안한 방법은 웜의 시간에 따른 행동패턴에서 나타나는 서비스 포트, 웜 공격 호스트와 대상 호스트 간의 메시지 전송 등 인터넷 웜의 동적인 특성에 초점을 맞춘다. 따라서 각 웜의 행동패턴에 대한 세부적인 행동들에 관한 표현방식은 고려되지 않았으므로 향후 웜의 각 행동 순서에서의 세부 패턴의 표현방식에 대한 연구가 필요하다.

참 고 문 헌

[1] Kienzle DM, Elder MC, "Recent Worms: A Survey and Trends", in Proceeding of the 2003 ACM workshop on Rapid Malcode, Oct 2003. pp 1-10

[2] Moore D, Paxson V, Savage S, Shannon C, Staniford S and Weaver N,"Inside the slammer worm", IEEE Security and Privacy, August 2003, pp 33-39

[3] Nazario J, Anderson J, Wash R and Connelly C, "The Future of Internet Worms" 2001 Blackhat Briefings, LasVegas, NV, July 2001. pp 4-7

[4] Wangner A, Dübendorfer T, Plattner B, Hiestand R, "Experiences with worm propagation simulations" ,Proceedings of the 2003 ACM workshop on Rapid malcode Oct 2003, pp 34-4

[5] Weaver N, Paxson V, Staniford S and Cunningham R, "A taxonomy of computer worms", in Proceeding of the 2003 ACM workshop on Rapid Malcode, Oct 2003. pp 11-18

[6] Whalley I, Arnold B, Chess D, Morar J, Segal A, Swimmer M, "An Environment for Controlled Worm Replication and Analysis", Virus Bulletin Conference, 2000, pp 77-100.

[7] Szor P, "The Art of Computer virus Research and defense ",Addison-Wesley, 2005

[8] snort,"Snort", http://www.snort.org Visited 2005

[9] symantec,,"Symantec Security Response", http://securityresponse.symantec.com, Visited 2005

[10] Sysinternal, "Sysinternal Utils", http://www.sys internals.com

[11] symantec,,"Symantec Security Response", http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.b.worm.html, Visited 2005

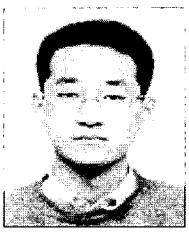
[12] symantec,,"Symantec Security Response", http:// securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html, Visited 2005

[13] symantec,,"Symantec Security Response", http:// securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html, Visited 2005

〈著者紹介〉

이 민 수 (Min-Soo Lee) 학생회원
2003년 2월: 국립 목포대학교 컴퓨터공학 졸업
2004년 8월~현재 ;고려대
정보보호대학원 석사과정
<관심분야> 네트워크보안, 패턴인식

손 태 식 (Tae-Shik Shon) 정회원
2005년 8월: 고려대 공학박사
2004년~2005년: Research Scholar, Univ. of Minnesota
2005년8월 ~현재: 삼성전자 통신연구소
〈관심분야〉 Abnormal Detection, 802.11/15/16 Security, Sensor network Security



조 상 현 (Sang-hyun Cho) 정회원
1997년 2월: 고려대학교 컴퓨터학과 졸업
1999년 2월: KAIST 전산학과 졸업(석사)
2005년 2월: KAIST 전산학과 졸업(박사)
2005년 3월~현재: 고려대학교 정보보호대학원 연구교수
〈관심분야〉 정보보호, 네트워크 보안, 침입탐지

문 종 섭 (Jong-Sub Moon) 정회원
1981년~1985년 :금성 통신 연구소 연구원
1991년 : Illinois Institute of technology 졸업(전산학 박사)
1993년 ~ 현재 :고려대 전자 및 정보공학부 교수
〈관심분야〉 생체인식, 침입탐지, 운영체제

김 동 수 (Dong-Soo Kim)
1998년 2월: 성균관대학교 정보공학과 졸업
2000년 2월: 성균관대학교 전기전자및컴퓨터공학부 공학석사 졸업
2004년 8월: 성균관대학교 정보통신공학부 공학박사 졸업
2004년 11월~현재: ETRI 부설 국가보안기술연구소 연구원
〈관심분야〉 네트워크 보안관리, 접근제어/보안모델

서 정 택 (Jung-Taek Seo) 정회원
1999년 2월: 국립충주대학교 컴퓨터공학과 졸업
2001년 2월: 아주대학교 컴퓨터공학과 공학석사 졸업
2006년 2월: 고려대학교 정보보호대학원 공학박사 졸업
2000년 11월~현재: ETRI 부설 국가보안기술연구소 선임연구원
〈관심분야〉 시스템 및 네트워크 보안, 정보보호 컨설팅, 유비쿼터스 보안

손 기 욱 (Ki-Wook Sohn) 정회원
1990년 2월: 성균관대학교 정보공학과 졸업
1992년 2월: 성균관대학교 정보공학과 공학석사
1992년 1월~1999년 12월: 한국전자통신연구원(ETRI) 선임연구원
2002년 8월 성균관대학교 전기전자컴퓨터공학부 공학박사
2000년 1월~현재: ETRI 부설 국가보안기술연구소 선임연구원
〈관심분야〉 키분배 프로토콜, 보안관제