전파특성에 따른 인터넷 웜의 분류 기법 연구

이승규°, 조규형, 이민수, 문종섭, 김동수*, 서정택*, 박응기*

고려대학교 정보보호대학원/정보보호기술 연구센터, 국가보안기술연구소*

{lsk6464°, khcho, leesle, jsmoon}@korea.ac.kr, {iskim, seojt, ekpark}*@etri.re.kr

Internet worm classification depend on spreading specificity

Swengkyu Lee, G. H Cho, M. S Lee, J. S Moon, D. S. Kim*, J. T. Seo* & E. K. Park*

GSIS/CIST, Korea University , NSRI*

요 약

인터넷 및 네트워크가 급격하게 발전함에 따라 많은 피해가 발생하고 있으며, 이러한 피해중 웜은 많은 장비 및 네트워크 상의 위협을 준다. 이러한 위협이 되는 웜을 잘 대처하기 위해서는 웜의 행동자체에 대한 파악을 반드시 해야 하고 이에 선행 연구작업으로써 웜 분류는 반드시 실시되어야 한다. 외국의 웜 분류 연구중 UC Berkeley와 시만텍사의 분류방안을 살펴보고 그러한 분류 방안에 기반한 트래픽 및 웜 행동 패턴을 기준으로 전파특성과 웜의 행동 단계별 기준하에 재정립 및 분류 기법을 제안하겠다. 이러한 웜의 분류는 차후 시뮬레이터 모듈의 구현과 각 모듈의 조합을 통한 구체적인 웜 모델링에 대한 연구의 기초가 된다.

1. 서 론

컴퓨터 및 네트워크 기술이 발전함에 따라 현재는 사회 대부분의 분야에서 네트워크망을 이용하고 있으며 이러한 네트워크 망은 Slammer 나 Sasser등의 웜에 의해 많은 피해를 받고 있다. 또한 기술이 복잡해질수록 필연적으로 문제점이 증가하고, 이러한 문제점들을 이용한 새로운 웜이나 악성코드가 빈번하게 출현하고 있다. 그러므로 새롭게 나타나는 웜으로 인한 피해를 줄이고 능동적으로 대처하기 위해서는 웜의 행동 특성 자체를 파악하고 정확하게 분석하는 작업이 무엇보다 선행되어야 할것이다.

따라서 본 연구에서는 웜 특성을 파악하기 위한 선행연구로써 국내외 연구기관 및 업체에서 제시한 웜 분류 기법을 분석하고 이를 기반으로 시뮬레이션 및 모델링 기법관점에서 전파특성에 따른 웜을 분류하고자 한다 [1].

2. 본 론

웜의 분류와 관련된 체계적인 연구는 활발하게 진행되지 않고 있으며, 최근(2003년)에 웜의 분류 기법에 관련된 논문이 UC Berkeley와 시만텍에서 발표 되었다. 따라서 이러한 연구결과를 분석하고 이를 기반으로 웜 분류를 살펴보자.

2.1 웜의 모듈별 분류 기법(UC Berkeley)

Nazario는 웜의 구성요소를 총 다섯 가지로 구분하였다[2]. 이처럼 웜은 내부의 역할을 기준으로 분류를 할 수 있으며 UC Berkeley에서도 유사하게 구성요소들을 기준으로 각 요소별 분류하였다[3].

[표 1] 웜의 모듈별 분류

요 소	세 부 설 명
Target discovery	웜이 자신을 전파시키기 위해 새로 감염시킬 호스트들 찾는 메커니즘
carrier	감염시킬 호스트에 자기 자신(웜 코드)을 전파 시키는 메커니즘
activation	웜 코드가 타깃 호스트에서 작동이 시작 되는 메커니즘
payloads	웜 자체를 전파시키기 위한 루틴 외에 웜 코드 작성자의 목적을 수행하는 메커니즘
motivation and attackers	해커로써의 자긍심, 금전적인 이익 등과 같은 웜 제작자의 동기

2.2 웜의 감염 경로에 따른 분류 기법(시만텍)

시만텍의 분류는 바이러스 백신업체로써 많은 양의

데이터 축적과 대응결과 분류한 기법으로 연구적 측면에서의 관점으로 수행되지는 않았지만, 웜의 감염경로에 따라 분류하여 웜과 관련된 다양하고 유용한 경향을 도출시키고 있다[4]. 시만텍에서 분류한 방식은 아래와 같다.

● E-mail 웜

E-mail을 통해 전파되는 웜들은 직접 네트워크 접속을 사용하지 않고 첨부파일 클릭 등의 사용자의 일정한 행위에 의존한다. E-mail은 인터넷상에 웜을 전파시키기에 가장 효과적이며 일반적으로 사용되는 방법이다.

● Windows 파일 공유 웜

Windows 파일 공유 웜들은 Microsoft Windows의 파일 공유 서비스를 이용한다.

● 초기형태 웜

1988년 Morris 웜에서 파생된 분류들이다. 이러한 웜들은 TCP/IP 기반의 프로토콜들에 직접 접근하는 방식을 사용하여 운영체제상이나 어플리케이션상의 취약점을 공격한다[5].

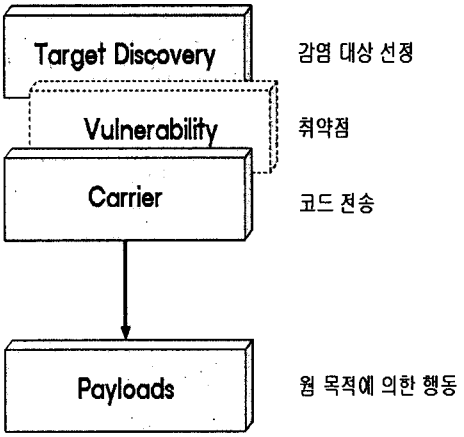
2.3 웜 전파 특성 분석 연구

기존의 연구결과들인 UC Berkeley 와 시만텍의 분류기법들은 시뮬레이터 모듈의 구현과 각 모듈의 조합을 통한 구체적인 웜 모델링에 대한 연구 관점에서 일부 정들이 부적합하다고 판단된다. 따라서 트래픽 및 웜 행동패턴을 기준으로 웜을 새롭게 분류하고자 한다.
본 연구팀은 웜을 크게 4가지로 분류하고 각각의 코드를 다음과 같이 규정하였다.

[표 2] 웜의 대분류

분류 그룹	세 부 설 명	코드
E-mail	E-mail을 통하여 전파	E
windows 파일 공유	Windows의 파일 공유 프로토콜을 이용하여 전파	W
Self propagation	운영체제나 응용 서비스들의 취약점을 이용하여 스스로 전파	S
Multi-method	상단의 세 가지 속성 중 두 가지 이상을 병행하여 전파	M

이와 같은 대분류를 기반으로 1차적인 분류가 가능하다. 또한 웜을 행동 특성에 따라 분류하는 과정에서 고려해야 할 요소로 웜의 행동 단계별 분류 기준들을 순차적으로 정리하면 다음과 같다.



[그림 1] 행동단계별 분류

인터넷 웜의 행동 단계를 및 분류 기준을 바탕으로 웜의 특성을 확인할 수 있도록 코드를 정의하였다.

● Target discovery
- Random scanning: 대상 호스트 선정에 있어서 순수하게 임의의 선택을 통해 찾기(TR)
- Changed random scanning: 순수하게 임의의 호스트를 선정 하지 않고 변형된 방법으로 임의의 호스트를 선정(TC)
- Pregenerated target lists: 대상 호스트에 대한 정보를 웜 제작자가 웜에 사전에 정의(TL)
- External generated target lists: 대상 호스트에 대한 정보를 외부에 저장 하거나, 외부의 서버 정보를 가지는 메타서버를 이용(TE)
- Internal target lists: 감염 된 호스트의 내부의 저장되어 있는 다른 호스트에 대한 정보를 공격 대상으로 선정(TI)
- Passive: 감염된 호스트에 대해서 어떠한 이벤트가 발생 시 그 이벤트를 발생 시킨 호스트를 대상 호스트로 공격(TP)

● Vulnerability
- OS vulnerability: OS의 취약성을 이용(VO)
- SoftWare vulnerability: 응용 프로그램의 취약성

을 이용(VS)
- Mis-management: 관리자의 실수(설정상의 오류)로 인한 취약점을 이용(VM)
- Protocol vulnerability: 프로토콜의 취약점을 이용(VP)

● Carrier
- Self carried: 대상 호스트 선정을 위한 접속 시 웜 코드도 같이 전송(CS)
- Second channel: 대상 호스트 공격 후 다른 서비스를 사용하여 웜 코드를 전송(CC)
- Embedded: 정상적인 통신 채널을 사용하여 전송(CE)

● Payloads
- Non-functional: 전파 기능만 가짐(PN)
- Remote control: 감염된 호스트를 제어(PR)
- Spam-replays: 스팸 메일 서비스 제공(PS)
- Proxies: 다른 호스트들을 속이기 위한 프록시 서비스 용도로 사용(PP)
- DoS attack: 다른 호스트를 DoS 공격(PD)
- Data collection: 여러 가지 데이터 수집(PC)
- Data damage: 감염 된 호스트의 데이터를 훼손(PG)

이러한 방법을 통하여 웜의 일반적인 분류의 기준으로 사용할수 있도록 하였으며, 이를 이용하여 각 특성별 시뮬레이션 코드를 구성한다면 여러 가지 웜에 대한 결과를 쉽게 얻을 수 있을 것이다.

다음 표는 위의 분류 기준에 따라 웜을 분류하는 예제이다. 분류시 코드 이름을 사용하였으며, 코드는 "웜 대분류-target discovery-vulnerability-carried-payload"순서로 표현 하였으며, 이중 E-mail을 통하여 전파되는 웜에 대해서는 위에서 제시한 target discovery, vulnerability, carried등의 기준에 의해서 분류가 불가능함에따라 코드는 "웜 대분류-payload"순서대로 표현하였다. 각 분류기준에 의해 여러개의 방법 사용 시에는 "M-TI(TP)-VM(VS)-CS-RC(PD,PC,PP)"와 같이 "()"를 통하여 표현하였다.

[표 3] 세부 분류 웜 코드표

웜 이름	분류 코드	
netsky	E-PN	
Lovgate	E-PR	
Agobot	W-TI(TP)-VM-CS-PR	
CodeRed	CodeRed v1,v2	S-TR-VS-CS-PD
	CodeRed II	S-TC-VS-CS-PD
Blaster	S-TC-VS-CS-PN	
Slammer	S-TR-VS-CC-PN	
Nimda	M-TI(TR)-VS-CS(CC)-PN	
Spybot	M-TI(TP)-VM(VS)-CS-RC(PD,PC,PP)	
MyTob	M-TI-VS-CS-PR	

3. 결론

이에 본 연구에서는 위의 분류기법들의 특징을 향후 트래픽 및 웜 행동패턴을 기준으로 한 연구와 관점에서 재정의 및 분류하고 분류틀을 제시하였다. 이를 바탕으로 각 대표적인 특징을 한눈에 파악 할 수 있으며 여러 가지 향후 연구시 쉽게 각 특징별 분류가 가능토록 하였다. 추후에는 이러한 분류기법을 토대로 각 분류 항목에 대한 시뮬레이터 모듈의 구현과 각 모듈의 조합을 통한 구체적인 웜 모델링에 대한 연구가 진행되어야 한다.

[참고문헌]

[1] 보안용어사전, 안철수 연구소 "info.ahnlab.com"

[2] Nazario,j., et al.,"The Future of Internet Worms" 2001 Black- hat Briefings,Lasvegas,NV,July 2001

[3] Nicholas Weaver,Vern Paxson,Stuart Staniford, Robert Cunning-ham,"A taxonomy of computer worms",Proceedings of the 2003 ACM workshop on Rapid Malcode,11-18

[4] Darrell M.Kienzle and Matthew C.Elder, "Recent Worms: A Survey and Trends", WORM '03, October 27, 2003, Washington, DC, USA

[5] Cliff Changchun Zou, Weibo Gong, Don Towsly, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense", WORM '03, October 27, 2003, Washington, DC, USA