사이버 정보전 웜·바이러스 공격 기술 연구

김환국* · 서동일* · 이상호**

*한국전자통신연구원 네트워크보안구조연구팀, **충북대학교 컴퓨터공학과

A Study on the Worm·Virus Attack Technique of Cyber Warfare

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

*ETRI Network Security Architecture Team, **Computer Science Dept. Chung-buk University

E-mail : *{rinyfeel,bluesea}@etri.re.kr, **shlee@cbucc.chungbuk.ac.kr

요 약

정보기술의 급격한 발전으로 사이버공간의 주요 특징인 익명성, 비대면성, 시공초월성 등과 함께 사용자 부주의, 소프트웨어 버그 및 각종 취약점 등으로 인하여 사이버테러로부터 정보 시스템을 보호하는 것은 점점 더 어려워지고 있다. 또한 최근 사이버테러 기술의 악의적, 군사적 활용도가 높아지면서 그 위험성이 매우 높으며 앞으로도 계속 증가할 것으로 예측되고 있다. 따라서 사이버 공간안에서 벌어지는 정보전 공격 기술의 연구는 사회적으로나 국가 안보적 차원에서 그 필요성이 매우 높다. 특히, 웜/바이러스 공격 기술은 사이버 공간에서 빈번하게 발생하고 있으며, 짧은 기간 동안 전 세계의 네트워크에 심각한 피해를 주고 있다. 따라서, 본 논문에서는 정보전의 주요 공격기술인 웜/바이러스 기술에 대해 고찰하고자 한다.

ABSTRACT

With the rapid progress of information technique, it is getting more difficult to protect information systems from cyber terrorism, because of bugs and vulnerabilities of software and the properties of cyberspace such as anonymity. Furthermore cyber terror techniques are highly developed and complicated and their use for a malicious intent and a military purpose are increasing recently. Therefore a study of warfare attack technology on the cyber space is necessary for establishing trusted society and further national security.

Specially, worms/viruses are becoming a more common occurrence on the cyber space . Also, The worm caused a great deal of damage to the large number of networks around the world in a very short period of time. Therefore, we will describe worms/viruses in the warfare attack technique in this paper.

키워드

Warfare, Worms, Viruses, 사이버 정보전, 보안

Ⅰ. 서 론

현재 국가경제와 정보보안은 정보기술과 정보기반 구조에 거의 대부분을 의존하고 있는 실정이다. 정보 기반 구조, 즉 인터넷은 초기 개발 당시 기밀을 필요로 하지 않은 정보를 공유하기 위해 설계되었으나, 오늘날 수백만의 컴퓨터 네트워크가 서로 연결되면서, 이는 국가에서 가장 중요한 기반 구조가 되었다. 이로 인해 악의적인 목적을 가진 인터넷 이용자는 국가 주요 정보기반구조를 공격하는 사례가 빈번히 발생할 가능성이 커지고 있다. 또한, 현대전에서는 다음 표1에서 나타나듯이, 정보전의 공격 기술과 무기들은 군이 보유한 정보전 공격기술과 전략적 군사 무기들로 비 살상용이며, 1차 적인 공격 목표가 적의 주요 정보 시스템이라는 것이 기존 무기들과 차별되는 가장 큰 특징으로 들 수 있다.

이러한 사이버 공간 안에서 벌어지는 정보전 공격 기술의 연구는 사회적으로나 국가 안보적 차원에서 그 필요성이 매우 높다. 특히, 웜/바이러스 공격 기술은 사이버 공간에서 빈번하게 발생하고 있으며, 짧은 기간 동안 전 세계의 네트워크에 심각한 피해를 주고 있다. 따라서, 본 논문에서는 정보전의 주요 공격기술인 웜/바이러스 기술에 대해 고찰하기 위해, 2장에서는 바이러스에 의한 공격에 대해 살펴보고, 3장에서는 웜에 의한 공격에 대해

기술하여 마지막으로 웜/바이러스 대응 기법에 대해 고찰한다.

표 1 정보전에 사용되는 공격 기술 유형

정보전 공격 기술	공격방법	목적
해킹	시스템이나 네트워크의 취약성을 이용한 해킹공격 시도	시스템 운용 장애 및 정보 유출
바이러스, 웜	악성코드를 이용, 버퍼 오버플로우를 발생시켜 공격자가 원하는 실행 코드로 포인터 이동.	시스템 운용 장애 및 정보 유출
트로이 목마	정상적으로 보이는 프로그램의 내부에 숨어서 시스템이나 네트워크에 해를 끼치는 프로그램	시스템 운용 장애 및 정보 유출
논리 폭탄	독립적인 프로그램의 형태 또는 시스템 개발자나 프로그래머에 의해 의도적으로 삽입된 코드의 형태	시스템 운용 장애
전자우편 폭탄/스팸 메일	전자우편을 대량으로 발송, 컴퓨터나 네트워크를 마비시키는 공격	시스템운용 장애
치핑	하드웨어에 의도적으로 특정 조건을 만족하면 동작하는 기능이나 회로를 삽입	시스템운용 장애
나노 머신	적의 정보 센터 등에 살포되어 컴퓨터 하드웨어를 파괴하는 작은 크기의 로봇	시스템운용 장애
미생물	컴퓨터 기판만을 부식시켜 피해를 유발하는 특이한 종류의 미생물 공격방법	시스템운용 장애
재밍	정보통신망을 통해 전달되는 패킷들의 유통을 전자적으로 방해하거나 내용을 변경하는 무기	시스템운용 장애
HREF gun	라디오 주파수대의 고출력 전파를 발생시켜 전자 장비들을 마비	시스템운용 장애
EMP	전자기파를 발생시킴으로써 이 전자파에 노출된 컴퓨터나 통신 시스템의 모든 전자 회로들을 파괴	시스템운용 장애
AMCW	스스로 네트워크를 따라 목표를 찾아 돌아다니며 바이러스 기술 등을 이용하여 적의 컴퓨터나 네트워크 시스템을 파괴하거나 정보를 조작하는 무기	시스템운용 장애

II. 바이러스에 의한 공격 기술

2003년 1.25 인터넷 침해사고를 기점으로 하여 악성코드의 일종인 인터넷 웜 해킹기술에 대한 관심이 부쩍 증대된 상태이다. 악성코드란 주로 다른 사람에게 피해를 주기 위한 목적으로 제작된 모든 컴퓨터 프로그램을 의미하며, 여기에는 전통적인 컴퓨터 바이러스, 트로이 목마, 웜 등이 해당 된다. 컴퓨터 바이러스란 감염 대상 프로그램 혹은 일반 파일에 자신의 코드 및 변형코드를 감염시키며, 이로 인하여 컴퓨터 자원을 소모시키거나 데이터를 변형시키는 역할을 한다. 국내의 경우, 1988년경 처음으로 발견된 Brain virus가 있으며, 최근까지도 많은 피해를 주고 있는 CIH Virus, 미켈란젤로 바이러스 등이 있다.

바이러스를 분류 하는 기법은 감염부위에 따라 부트, 파일, 부트/파일, 매크로 바이러스로 분류 할 수있으며, 운영체제에 따라, 도스 바이러스, 윈도우 바이러스, 애플리케이션 파생 바이러스, 유닉스,/ 리눅스/ 맥/OS/2 바이러스, 자바 바이러스로도 구분된다. 본 장에서는 바이러스의 형태 및 기법 분류에 따른 바이러스 들을 Simple Viruses, Encrypted Viruses, Polymorphic Viruses 로 나누어 살펴보도록 하겠다[1].

1. Simple Viruses

단순바이러스는 오직 자신을 복제하는 기능만을 가진다. 사용자가 감염된 프로그램을 실행하면, 바이러스는 해당 시스템의 제어를 획득하고 자신의 복사본을 다른 프로그램 파일에 Attach 시킨다. 이러한 바이러스는 스캐닝을 통해 쉽게 탐지가 가능하다.

2. 32bit Encrypted Viruses

기본적으로 바이러스 코드의 기능을 암호화시키는 것으로, 바이러스 Body를 암호화하여 바이러스 스캐너에 탐지되지 않도록 Virus signature 를 숨기는 바이러스이다. 이 바이러스는 뒤따르는 암호화된 바이러스 body 를 Decryrpt 하기 위해 고정된 Decryption Routine(Decryptor) 가 있다.

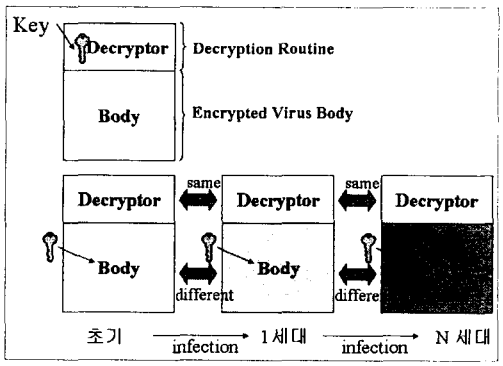

그림 4. 암호화 바이러스 구조 및 감염 생성 흐름

그림 1은 암호화 바이러스의 구조와 바이러스가 감염되면서 새로운 바이러스를 생성하는 흐름도이며, 암호화 바이러스는 같은 Decryption routine(Decryptor)을 사용하여 전파된다. Decryption routine 의key 값은 감염 될 때마다 변하게 된다. 결과적으로 감염이 진행될 때 마다 바이러스의 body는 변하게 된다.

암호화 바이러스는 virus decryption routine, 암호화된 virus body 로 구성된다. 사용자가 감염된 프로그램을 실행하면 virus decryption routine 은

컴퓨터의 제어를 얻고, 암호화된 virus body 를 해독한다. 그리고 decryption routine 은 컴퓨터의 제어를 해독된 바이러스에게 넘긴다. 암호화 바이러스는 프로그램과 파일을 단순 바이러스 처럼 감염시키고, 새로운 프로그램을 감염시킬 때마다 바이러스는 복호화된 virus body와 decryption routine의 사본을 만들어 이 사본을 암호화한다. 그리고 대상 파일에 attach 시킨다. Virus body 를 암호화하기 위해, 암호화된 바이러스는 key 를 사용한다. 이 키가 변할 때마다 virus body 가 변하게 되고, virus는 감염될 때마다 다르게 보여진다. 이것이 signature 기반 Anti-Virus 도구가 virus signature 를 탐지 하기 어렵게 만드는 이유이다. 반면에 decryption routine 은 일정하게 유지된다.

3. 32bit Polymorphic Viruses

Polymorphic 바이러스는 암호화 바이러스와 유사하다. Polymorphic 바이러스는 암호화 바이러스의decryption routine, virus body 에 새로운 프로그램을 감염시킬 때마다 바뀌는 임의의 decryption routine 을 생성하는 mutation engine 이 추가된다.

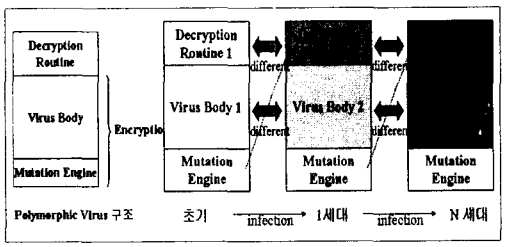

그림 5. Polymorphic 바이러스 구조

Polymorphic 바이러스 경우, mutation engine 과 virus body가 암호화된다. 사용자가 polymorphic 바이러스에 감염된 프로그램을 실행 시킬 때, decryption routine 은 컴퓨터의 제어를 얻고, mutation engine 과 virus body 를 복호화 시킨다. 그리고 decryption routine은 감염된 새로운 프로그램에 상주한 바이러스에게 컴퓨터의 제어를 넘긴다. 이때 바이러스는 RAM에 virus body 와 mutation engine의 copy를 만든다. 그리고 바이러스는 새로운 decryption routine을 생성하는 mutation engine을 실행하고, 바이러스는 새로운 virus body 와 mutation engine의 copy를 암호화한다. 마지막으로 virus 는 이 새로운 decryption routine을 새롭게 encrypted 된 바이러스와 mutation engine에 추가시킨다. 결과적으로 virus body 뿐만 아니라 virus decryption engine 도 변하게 된다. 이것은 고정된 signature와 고정된 decryption engine이 아니기에 탐지를 어렵게 한다.

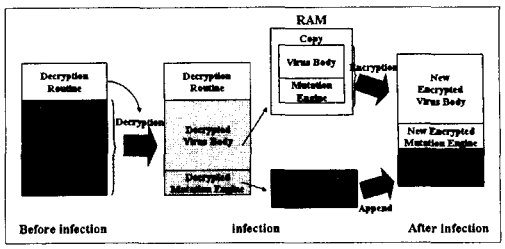

그림 6. 감염 구조

III. 웜에 의한 공격 기술

웜(Worm)이란 기억장소에 코드 형태로 존재하거나 혹은 실행 파일로 존재하며 작동 시 파일이나 코드 자체가 네트워크를 통하여 다른 시스템으로 감염되는 악성 코드이다. 대표적으로는 1999년경 윈도우기반의 아웃룩 소프트웨어의 주소록을 통하여 급격히 확산되어 많은 피해를 입혔던 멜리사 웜이 있으며, 최근의 러브 바이러스, Nimda 바이러스, Code Red바이러스, 그리고 1.25 인터넷 침해사고의 원인으로 밝혀졌던 MS SQL 슬래머 웜 등이 여기에 해당된다. 이외에도 다른 사람에게 거짓된 악성 정보를 유포하여 사용자에게 심리적인 위협이나 불안감을 조장하는 혹스(Hoax), 프로그램이 실행되면서 물리적인 피해는 없으나 사용자를 놀라게 하거나 심리적인 위협, 불안감을 심어주는 조크 프로그램 등이 악성코드라 할 수 있을 것이다.

인터넷 웜은 1998년에 ADM Internet worm (ADMw0rm)이, 1999년에는 ADMw0rm 과 유사한 Millennium Internet Worm이 공개되었으며, 국내 침해사고에서도 발견된 적이 있다. 이러한 인터넷 웜은 자동으로 임의의 공격 목표를 정하고 공격이 성공하고 나면 그 지점부터 또 다른 공격을 시작하므로 위의 취약점을 가진 많은 사이트가 공격을 당할 수 있다. trin00, TFN 등 DDOS 공격도구 또한 위와 비슷한 종류의 인터넷 웜을 통하여 서버에 설치될 수 있는데, 실제로 몇 몇 침해사고에서 인터넷 웜과 비슷한 기능의 스크립트들이 발견되었다. 또한 유닉스 및 윈도우 기반의 공격 프로그램들이 다양한 플랫폼별로 포팅되어 공개되는 경우가 증가하고 있어, 공격도구의 자동화 또는 패키지화는 가속화 될 것이다. 이미 이러한 자동화된 공격 시스템에 대한 연구가 상당부분 진행 중인 상태이다. 자동화된 공격도구는 pareral한 형태의 공격패턴을 제공하는데, 이는 공격자에게 공격범위 및 속도를 향상시켜주며, 결국 조만간 공격자에게 인터넷을 전복시킬만한 시스템 및 네트워크 자원을 제공할 수도 있다. 그리고 이러한 공격에 에이전트 형태의 공격도구를 사용하게 되면 공격자는 실제의 공격라인으로부터 떨어져 있게 되고, 역추적은 사실상 불가능하게 된다.

다음 표2 는 2003~2004년 유행하고 있는 신종 웜을 중심으로 웜의 종류와 증상 그리고 감염경로

에 대해서 조사하였다.

표 2 최근 웜의 종류와 증상

종류	감염	증상	해결방법	대상
Adware.Hotbar	웹상의 유틸 다운로드로 발생	익스플로러 실행시 계속적인 핫바 실행	두 프로세스 hbinst, HbSrv 를 강제 종료 레지스트리값 정리	윈도우 계열
Adware.Lookinet	웹상의 유틸 다운로드로 발생	시작메뉴 및 빠른 가기 메뉴에 자동 아이콘 생성 시작페이지 고정	Uninstall	윈도우 계열
Worm.Slammer (Worm.SQL .Slammer)	MS-SQL Server의 알려진 취약점을 통해 확산	시스템 및 네트워크 속도 저하 서비스 거부 공격	SQL관련 보안 패치	SQL Server
Worm.Dumaru (I-Worm.Win32. Dumaru.9234)	첨부파일을 통해 확산	프로세스의 CPU 사용을 증가 네트워크 트래픽 대량증가	백신으로 치료 가능	윈도우 계열
Worm.Welchia(Worm.Win32.W elchia.10240)	Windows DCOM RPC 취약점을 통해 감염	네트워크 트래픽 증가	RPC 보안 패치를 설치	윈도우 NT계열
Worm.Blaster(Worm.Win32.Bl aster.6176)	Windows DCOM RPC를 이용확산	계속적인 시스템 재시작, 네트워크 트래픽 증가	RPC 보안 패치를 설치	윈도우 NT계열
Worm.Agobot (Worm.Win32. Agobot.272387)	웜 은 Windows의 보안 취약점을 이용하여 전파	네트워크 트래픽 증가	실행된 바이러스의 서비스 설정을 변경	윈도우 NT계열
Worm.Beagle (I-Worm.Win32. Beagle.15872)	이메일을 통해 전파	프로세스의 CPU 사용률 폭주 네트워크 트레픽 대량증가	백신으로 치료 가능	윈도우 계열
Worm.Mydoom (I-Worm.Win32. Mydoom.22528)	이메일을 통해 전파	프로세스의 CPU 사용률 폭주 네트워크 트래픽 대량증가	백신으로 치료 가능	윈도우 계열

IV. 결 론

최근 컴퓨터 바이러스의 특징은 유입경로의 다양화, 네트워크 및 해킹 기술의 결합, 피해의 대형화, 빠른 확산속도, 보안 취약점 이용 증가, 백도어 및 트로이 목마 형 바이러스 증가 등으로 특징 지울 수 있다. 이렇게 날로 발전하는 바이러스의 위협에 효과적으로 대처하기 위한 안티 바이러스 제품들은 대개 감염이 되면 바이러스가 바이러스를 탐지하는 Detection 단계, 감염된 프로그램에 대한 바이러스를 식별하는 Identificatin 단계, 감염된 프로그램으로부터 감염 이전의 시스템 초기상태로 되돌리는 Removal 단계를 거쳐 바이러스 예방을 취한다. 다음은 안티바이러스 기술을 분류한 것이다[3].

표 3. 안티 바이러스 기술

세대별 분류	내용
Signature-based Scanning	기 분석된 바이러스의 패턴이나 "masks"를 기반으로 바이러스를 검사하는 기술
Heuristic Scanner	바이러스 또는 악성 코드와 관련이 있는 것으로 알려진 기능이나 행위에 대한 분석을 바탕으로 알려지지 않은 바이러스도 발견해 낼 수 잇는 기술이나 통계를 바탕으로 바이러스 감염 가능성에 대해 판단흐므로 잘못된 판단을 내릴 가능성이 존재함.
Vaccination Technology	응용 프로그램을 수정하여 자가 진단할 수 있는 코드를 삽입하는 기술로 프로그램 순서 등이 바뀌었을 때 감염가능성을 파악하는 기술
Snapshot Technology	크리티컬한 정보에 대한 로그를 주기적으로 덤프하여 바이러스 또는 악성코드의 존재 여부를 검사하는 기술
Sandbox Technology	바이러스가 의심스러운 코드를 샌드박스에서 실행하면서 코드의 영향을 모니터링 하여 바이러스 여부를 검사하는 기술
Behavior Blockers	메모리에 프로그램을 상주시켜 MBR에 대한 쓰기, TSR 프로그램으로 등록 등을 검사하여 잠재된 바이러스의 위험 등을 경고하는 기술

본 논문에서는 정보전의 주요 공격기술인 웜/바이러스 기술에 대해 고찰하기 위해, 2장에서는 Simple Viruses, Encryption Virus, Polymorphic Virus 에 대해 살펴보았으며, 3장에서는 웜 공격의 정의와 최근 웜의 특징에 대해 기술하였으며 마지막으로 안티 웜/바이러스 기술에 대해 살펴보았다.

참고문헌

[1] Carey Nachenberg. "Understaing and Managing Polymorphic Viruses." The Symantec Enterprise Papers.

[2] Peter Szor, Peter Ferrie, "Hunting for Metamorphic",Virus Bulletin Conference, 2001

[3] 권석철,"안티 바이러스 국제기술 동향", 제9회 정보보안기술 표준화 워크샵,2003