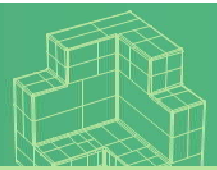
6 악성 코드

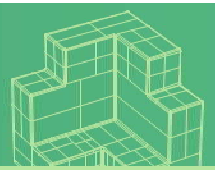
정보 보안 개론 6장

이 장에서 다룰 내용



1. 악성 코드의 종류와 그 특성을 알아본다.
2. 바이러스의 동작 원리를 이해한다.
3. 웜의 동작 원리를 이해한다.
4. 기타 악성 코드의 종류를 알아본다.

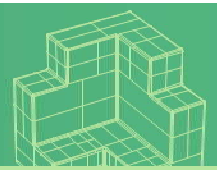
Section 01 악성 코드의 역사와 분류



❖ 악성 코드의 정의

제작자가 의도적으로 사용자에게 피해를 주고자 만든 모든 악의적 목적을 가진 프로그램 및 매크로, 스크립트 등 컴퓨터상에서 작동하는 모든 실행 가능한 형태

악성 코드의 역사



❖ 1972년

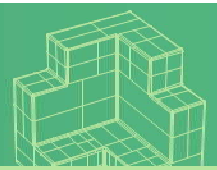
- **컴퓨터 바이러스의 개념이 처음 등장.**
- **소설가인 데이비드 제럴드의 공상과학소설** 『When Harlie was One』 (Nelson Doubleday, 1972)**에는 '다른 컴퓨터에 계속 자신을 복제, 감염된 컴퓨터의 운영체제에 영향을 미쳐 점차 시스템을 마비시키는 장치를 한 과학자가 제작해 배포한다'는 내용이 소개.**

❖ 1984년

- **컴퓨터 바이러스라는 용어는** 1984**년에 프레드 코헨**(Fred Cohen)**에 의하여 다음과 같이 개념이 정립됨.**

We define a computer 'virus' as a program can 'infect' other programs by modifying them to include a possibly evolved copy of itself.

악성 코드의 역사



❖ 1986년

- 일반적으로 1986년에 발견된 브레인 바이러스(Brain Virus)를 최초의 바이러스로 칭함. 이 바이러스는 파키스탄에서 프로그래머로 일하던 알비 형제가 자신들의 소프트웨어가 불법 복제되는 것을 참다못해 바이러스를 만들어서 뿌렸다고 함.

❖ 1987년

- 예루살렘 대학에서 13일의 금요일 바이러스가 발견됨. 유명한 바이러스로 예루살렘 바이러스라고도 불리는데, 13일의 금요일에 시스템내의 파일을 삭제하게 되어 있는 바이러스다. 이탈리아에서 제작한 것으로 알려지고 있음.

❖ 1989년

- 모리스 웜이 발생하여, 미국의 네트워크를 마비시킨 사건이 일어남.
- 최초의 웜으로 알려지고 있음.

❖ 1991년

- 1991년 11월에는 그간의 바이러스와 전혀 다른 특징을 가진 바이러스가 출현. 당시 발견된 DIR II는 MS 도스의 FAT 파일시스템의 연결 구조를 이용하며, 바이러스 감염시 프로그램의 크기를 증가시키지 않고 기생할 수 있다는 특징을 가짐.

악성 코드의 역사

❖ 1997년

- 매크로 바이러스가 출현.
- 매크로(Macro)란 엑셀이나 워드에서 특정한 기능을 자동화시켜놓은 일종의 프로그램인데, 이 바이러스는 시스템 프로그램과 같은 고난이도의 기술만이 웜/바이러스 제작에 이용될 수 있다는 인식을 바꾸어 놓음.

❖ 1999년

- 월 컴퓨터 하드 디스크의 바이오스(BIOS)를 손상시키고 각종 파일을 삭제하는 CIH 바이러스로 인해 많은 컴퓨터가 피해를 입음.

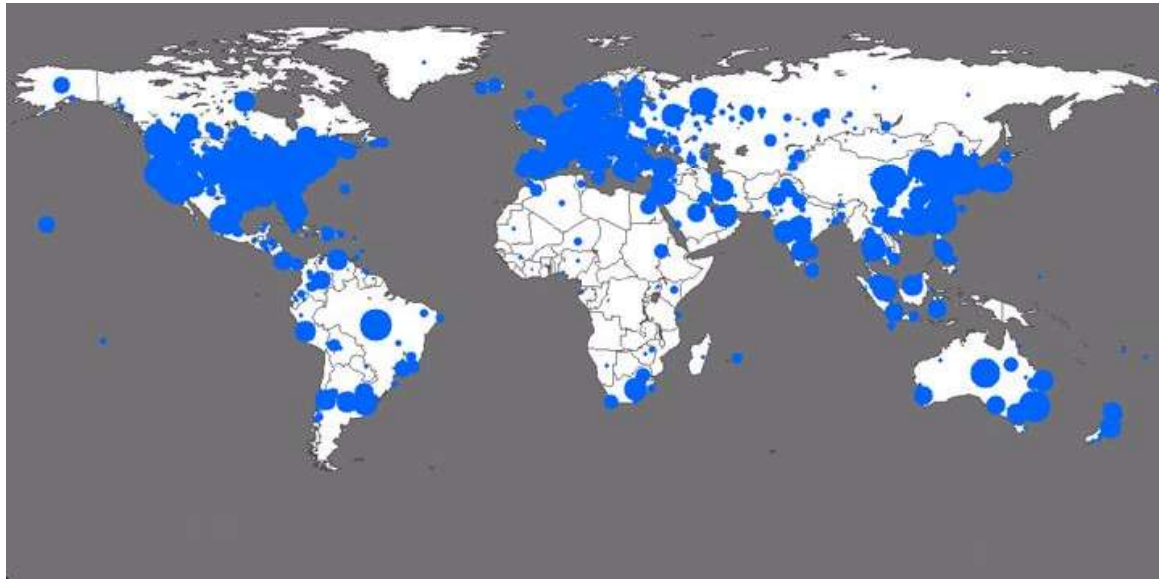
❖ 2001년

- 코드 레드 웜에 의해 8시간 만에 25만대 이상의 컴퓨터가 감염됨. 이 웜은 윈도우 2000과 윈도우 NT 서버를 경유지로 이용해 미국 백악관을 공격하였는데, 국내도 최소 3만대 이상의 시스템이 피해를 입은 것으로 추정됨.

악성 코드의 역사

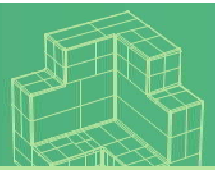
❖ 2003년

- 2003년 1월 25일 인터넷 대란을 일으킨 SQL_Overflow 웜이 등장.
- CAIDA에 따르면, 기준으로 2003년 1월 25일 05시 29분에 슬래머가 퍼지기 시작하여, 06시를 기준으로 전 세계의 74,855대 시스템이 그림과 같이 감염됨.



- 8월에는 1~2분 간격으로 컴퓨터를 강제 재부팅시킴으로써 국내외적으로 큰 피해를 준 블래스터 웜(Blaster Worm)을 시작으로, 웰치아 웜(Welchia Worm), 엄청난 양의 스팸 메일을 집중 발송해 전 세계를 깜짝 놀라게 한 소빅.F 웜(Sobig.F Worm) 등이 발생

악성 코드의 역사



❖ 2004년

- 마이둠 웜(Mydoom Worm)이 1월 26일에 처음 등장해 역대 최고의 전파 속도로 세계적으로 100만대 이상의 PC를 감염. 이외에도 넷스카이, 베이글, 새서 웜 등의 변종이 지속적으로 등장.
- 6월에는 자기 복제가 가능하고 네트워크를 통해 전파되는, 최초의 웜 형태를 지닌 휴대폰 악성 코드인 카비르 웜이 등장

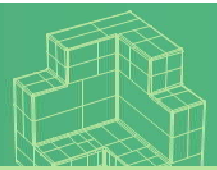
❖ 2005년

- 웜의 다양한 변종이 지속적으로 등장해 컴퓨터 사용자를 괴롭힘.
- 3월에는 블루투스 외에 멀티미디어 메시징 서비스(MMS)를 이용해, 감염된 휴대폰에 저장된 전화번호를 통해 악성 코드를 퍼뜨리는 휴대폰 악성 코드인 컴워리어가 등장하여 전파 방법상에서의 지역적 한계를 넘음.

❖ 현재

- 최근에 알려진 바이러스의 종류도 15만 개 이상.
- IT 시장 조사 기관인 IDC는 2004 년에 37억 달러 규모였던 안티 바이러스 시장이 2009년에는 73억 달러에 이를 것으로 전망.

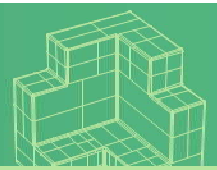
악성 코드의 분류



❖ 정의에 따른 악성 코드의 분류

이름(코드)	설명
바이러스(Virus)	• 사용자 컴퓨터(네트워크로 공유된 컴퓨터 포함)내에서 사용자 몰래 프로그램이나 실행 가능한 부분을 변형해 자신 또는 자신의 변형을 복사하는 프로그램이다. • 가장 큰 특성은 복제와 감염이다. 다른 네트워크의 컴퓨터로 스스로 전파되지는 않는다.
웜(Worm)	• 인터넷 또는 네트워크를 통해서 컴퓨터에서 컴퓨터로 전파되는 악성 프로그램이다. • 윈도우의 취약점 또는 응용 프로그램의 취약점을 이용하거나 이메일이나 공유 폴더를 통해 전파되며, 최근에는 공유 프로그램(P2P)을 이용하여 전파되기도 한다. • 바이러스와 달리 스스로 전파되는 특성이 있다.
트로이 목마 (Trojan Horse)	• 바이러스나 웜처럼 컴퓨터에 직접적인 피해를 주지는 않지만, 악의적인 공격자가 컴퓨터에 침투하여 사용자의 컴퓨터를 조종할 수 있는 프로그램이다. • 고의적으로 만들어졌다는 점에서 프로그래머의 실수인 버그와는 다르다. 또 자기 자신을 • 다른 파일에 복사하지 않는다는 점에서 컴퓨터 바이러스와 구별된다.
혹스(Hoax)	• 인터넷 메신저나 이메일 또는 게시판, 문자 메시지 등에 거짓 정보나 괴담 등을 실어 사용자를 속이는 가짜 컴퓨터 바이러스다. • 우리나라에서는 1997년부터 나타나기 시작해 해마다 등장하고 있는데, 특히 만우절을 전후한 3월 말에서 4월 초에 많이 나타난다. • 한 예로, 2004년 3월에 나타난 혹스에는 '누군가 munrol@hotmail.com이라는 사람의 추가를 요구하면 추가하지 말고 취소하십시오. 바이러스입니다. 지금 MSN 창에 있는 사람들에게도 이 메시지를 빨리 돌려주십시오" 라는 내용이 담겨 있었다. 확인 결과 가짜 바이러스인 혹스로 판명되었다.
악성 자바 코드	• 웹 사이트에서 동적인 기능을 구현하기 위해서 자바 스크립트나 자바 애플릿을 많이 사용하는데, 이런 자바 스크립트나 자바 애플릿을 이용하여 악의적인 기능을 하는 코드를 말한다.
악성 ActiveX	• ActiveX는 마이크로소프트에서 만든 객체지향 프로그래밍을 위한 도구 모음이다. ActiveX 컨트롤은 이 ActiveX를 이용하여 객체지향 프로그래밍을 하기 위한 컴포넌트인데, 이를 이용하여 악의적인 기능을 수행하게 하는 코드를 악성 ActiveX 코드라 한다.

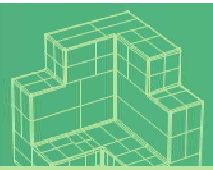
악성 코드의 분류



❖ 악성 프로그램으로 인해 발생할 수 있는 증상

대분류	소분류	설명
시스템 관련	시스템 정보 변경	변경 레지스터리 키값을 변경하여 시스템의 정보를 변경한다.
	FAT 파괴	시스템의 파일시스템을 파괴한다.
	CMOS 변경	CMOS 내용을 변경하여 부팅때 에러를 발생시킨다.
	CMOS 정보 파괴	CMOS의 일부를 파괴한다.
	기본 메모리 감소	시스템의 기본 메모리를 줄인다.
	시스템 속도 저하	시스템의 속도를 저하시킨다.
	프로그램 자동 실행	레지스터리값을 변경해 시스템을 부팅할 때 특정 프로그램을 자동으로 실행시킨다.
	프로세스 종료	특정 프로세스를 강제로 종료시킨다.
	시스템 재부팅	시스템을 재부팅시킨다
네트워크 관련	메일 발송	특정 사용자에게 메일을 발송한다.
	정보 유출	사용자의 정보를 네트워크를 통해서 공격자 컴퓨터로 전송한다.
	네트워크 속도 저하	감염된 컴퓨터가 속한 네트워크가 느려진다.
	메시지 전송	메시지를 네트워크를 통해 다른 컴퓨터로 전달한다.
	특정 포트 오픈	특정 백도어 포트를 연다.
하드 디스크 관련	하드 디스크 포맷	하드 디스크를 포맷한다.
	부트 섹터 파괴	하드 디스크의 특정 부분을 파괴한다.
파일 관련	파일 생성	특정 파일을 생성한다. 주로 백도어 파일을 생성한다.
	파일 삭제	특정 파일이나 디렉토리를 삭제한다.
	파일 감염	바이러스가 특정 파일을 감염시킨다.
	파일 손상	바이러스가 특정 파일에 겹쳐 쓰기 형태로 감염되면 파일이 손상된다.
특이 증상	특정 화면 출력	화면에 특정 내용이 나타난다.
	특정음 발생	컴퓨터에서 특정음이 난다.
	메시지 상자 출력	화면에 특정 메시지 상자가 나타난다.
	증상 없음	특이한 증상이 없다.

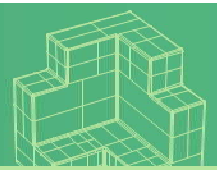
Section 02 바이러스



❖ 바이러스

- 악성 코드 중 가장 기본적인 형태며, 최초의 악성 코드가 만들진 1980년대 이후에서 2000년대 초반까지 악성 코드의 주류를 차지함.

1세대 : 원시형 바이러스



❖ 원시형 바이러스

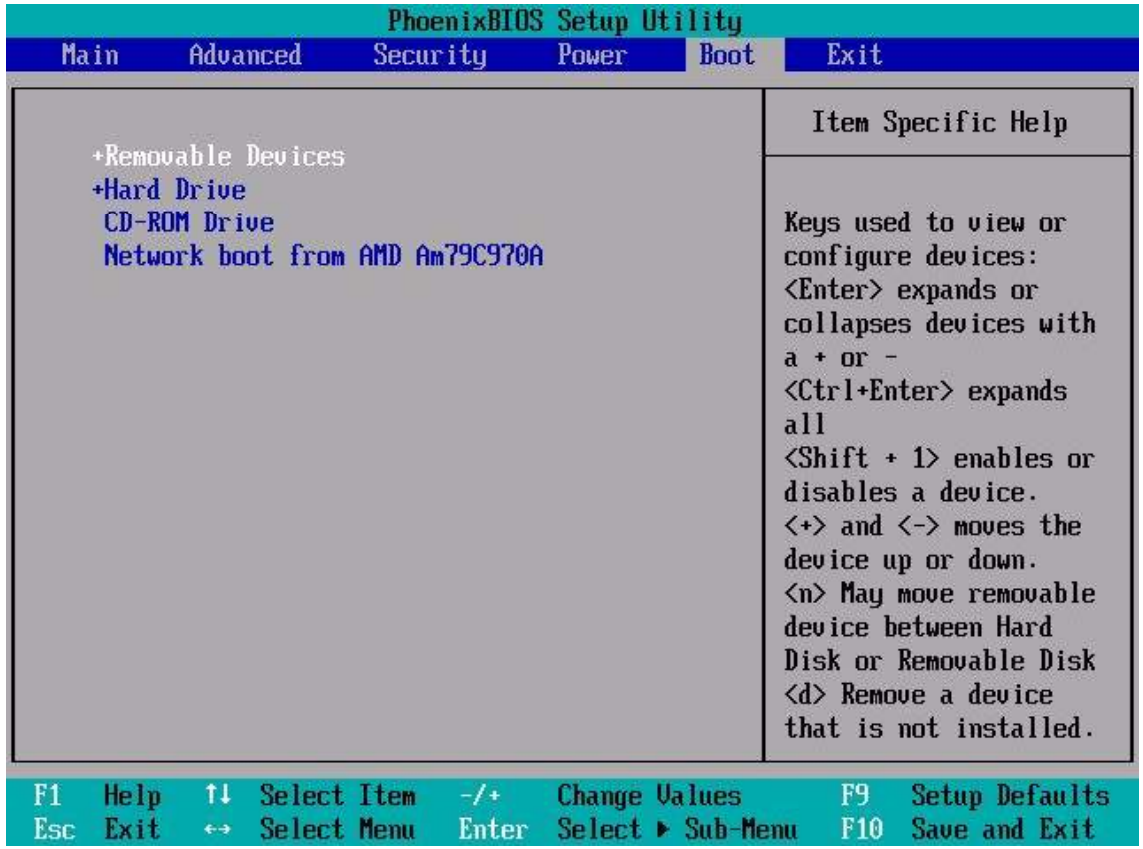
- 컴퓨터 바이러스가 등장하기 시작할 때쯤 퍼지던 가장 원시적인 형태의 바이러스로, 단순히 자기 복제 기능과 데이터 파괴 기능만을 가지고 있음.

❖ 부트 바이러스

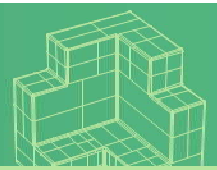
- 플로피 디스크나 하드 디스크의 부트 섹터에 감염되는 바이러스로, 부팅할 때 자동으로 동작.
- 1 단계 : POST
  - POST는 하드웨어 자체가 시스템에 문제가 없는지 기본 사항을 스스로 체크하는 과정.
  - BIOS에 의해서 실행되는데, POST 도중 하드웨어에서 문제가 발견되면 사용자에게 여러 방법으로 그 문제를 알림.

1세대 : 원시형 바이러스

- **2단계** : POST
  - CMOS에서는 기본 장치에 대한 설정과 부팅 순서를 설정할 수 있음.
  - BIOS는CMOS에서 이런 기본 설정 사항을 읽어 시스템에 적용.



1세대 : 원시형 바이러스

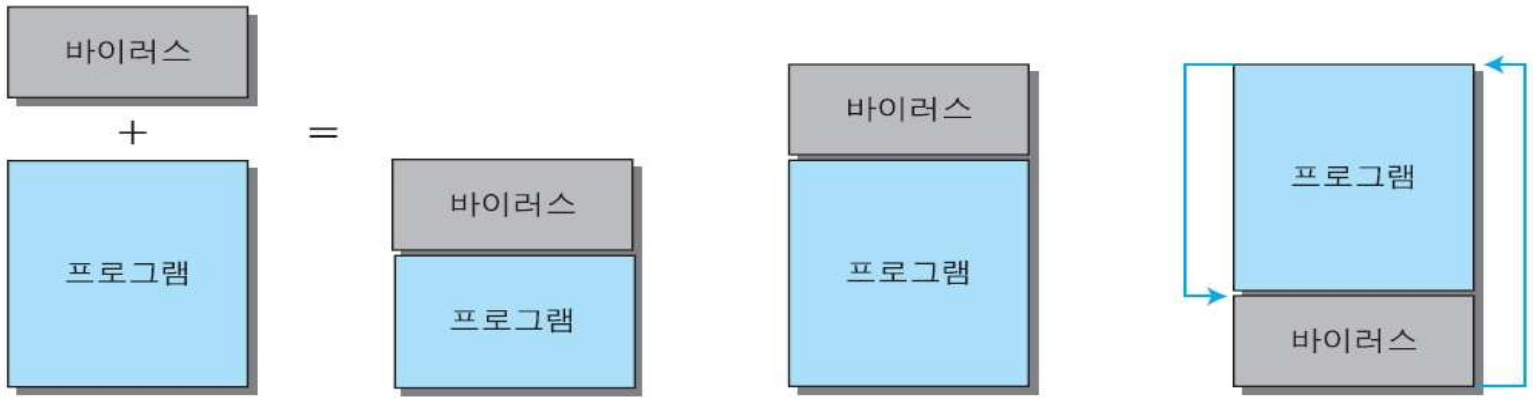


- 3단계 : 마스터 부트 레코드(MBR)
  - CMOS 정보를 읽어 부팅 매체를 확인한 뒤에는 부팅 매체의 MBR(Master Boot Record) 정보를 읽음.
  - MBR은 운영체제가 어디에, 어떻게 위치해 있는지를 식별하여 컴퓨터의 주 기억장치에 적재될 수 있도록 하기 위한 정보로, 하드 디스크나 디스켓의 첫 번째 섹터에 저장되어 있음.
  - MBR은 메모리에 적재될 운영체제가 저장된 파티션의 부트 섹터 레코드를 읽을 수 있는 프로그램을, 부트 섹터 레코드는 운영체제의 나머지 부분을 메모리에 적재시키는 프로그램을 담고 있음.
  - 부트 바이러스는 이 단계에서 동작.
  - 부트 바이러스에 감염된 플로피 디스크로 운영체제를 구동시키면 바이러스가MBR과 함께 PC 메모리에 저장되고 부팅 후에 사용되는 모든 프로그램에 자신을 감염시킴.
  - 부트 바이러스는 브레인, 몽키, 미켈란젤로 바이러스가 있음.

1세대 : 원시형 바이러스

❖ 파일 바이러스

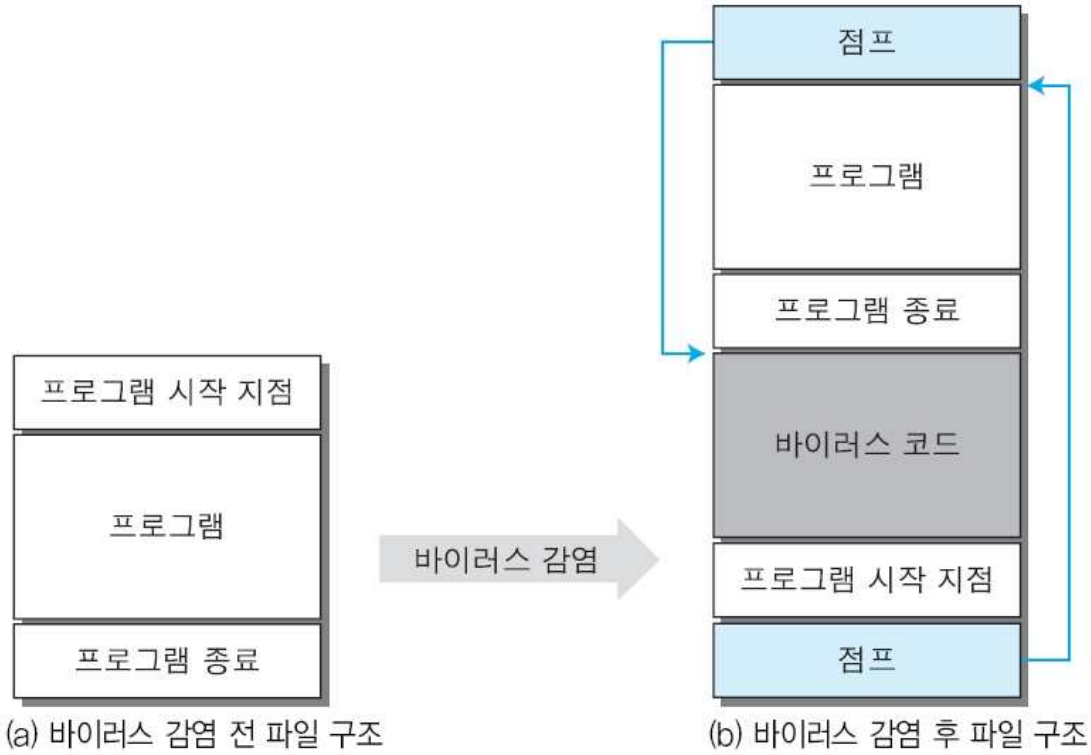
- 파일 바이러스는 파일을 직접 감염시키는 바이러스로서 부트 바이러스와는 달리 하드 디스크가 PC에서 일반화되면서 그 대안으로 나온 형태임.
- 일반적으로 COM이나 EXE와 같은 실행 파일과 오버레이 파일, 디바이스 드라이버 등에 감염되며, 전체 바이러스의 80% 이상을 차지함.
- 바이러스에 감염된 실행 파일이 실행될 때 바이러스 코드를 실행.
- (a) 프로그램을 덮어쓰는 경우, (b) 프로그램 앞부분에 실행 코드를 붙이는 경우, (c) 프로그램의 뒷부분에 바이러스 코드를 붙이는 경우가 있음.



[그림 6-4] 파일 바이러스의 감염 위치

1세대 : 원시형 바이러스

- 바이러스가 프로그램의 뒷부분에 위치한 경우 바이러스의 실행 루틴



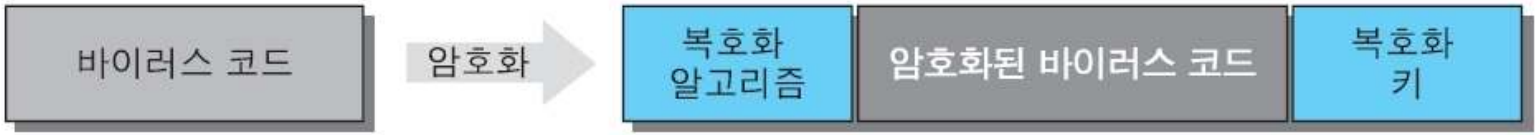
[그림 6-5] 바이러스가 프로그램 뒤에 있는 경우 실행 루틴

- 예루살렘 바이러스가 최초의 파일 바이러스로 알려져 있으며, 이외에도 썬데이, 스콜피온, 크로우, FCL 등이 있음. CIH 바이러스도 이에 해당됨.

2세대 : 암호형 바이러스

❖ 암호형 바이러스

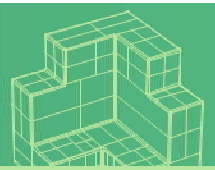
- 바이러스 제작자들은 백신의 진단을 우회하기 위해 자체적으로 코드를 암호화하는 방법을 사용하여 백신 프로그램이 진단하기 힘들게 만들기 시작함.



[그림 6-6] 암호화된 바이러스 코드

- 바이러스가 동작할 때 메모리에 올라오는 과정에서 암호화가 풀리기 때문에 백신 제작자들은 이를 이용하여 암호화하는 방법을 거꾸로 분석하여 감염 파일과 바이러스를 치료함.
- 슬로우, 캐스케이드, 원더러, 버글러 등의 바이러스가 있음.

3세대 : 은폐형 바이러스



❖ 은폐형 바이러스

- 확산되기 전에 바이러스가 활동하기 시작하면 다른 시스템으로 전파되기 힘들기 때문에 일정 기간 동안 잠복기를 가지도록 바이러스를 작성함.

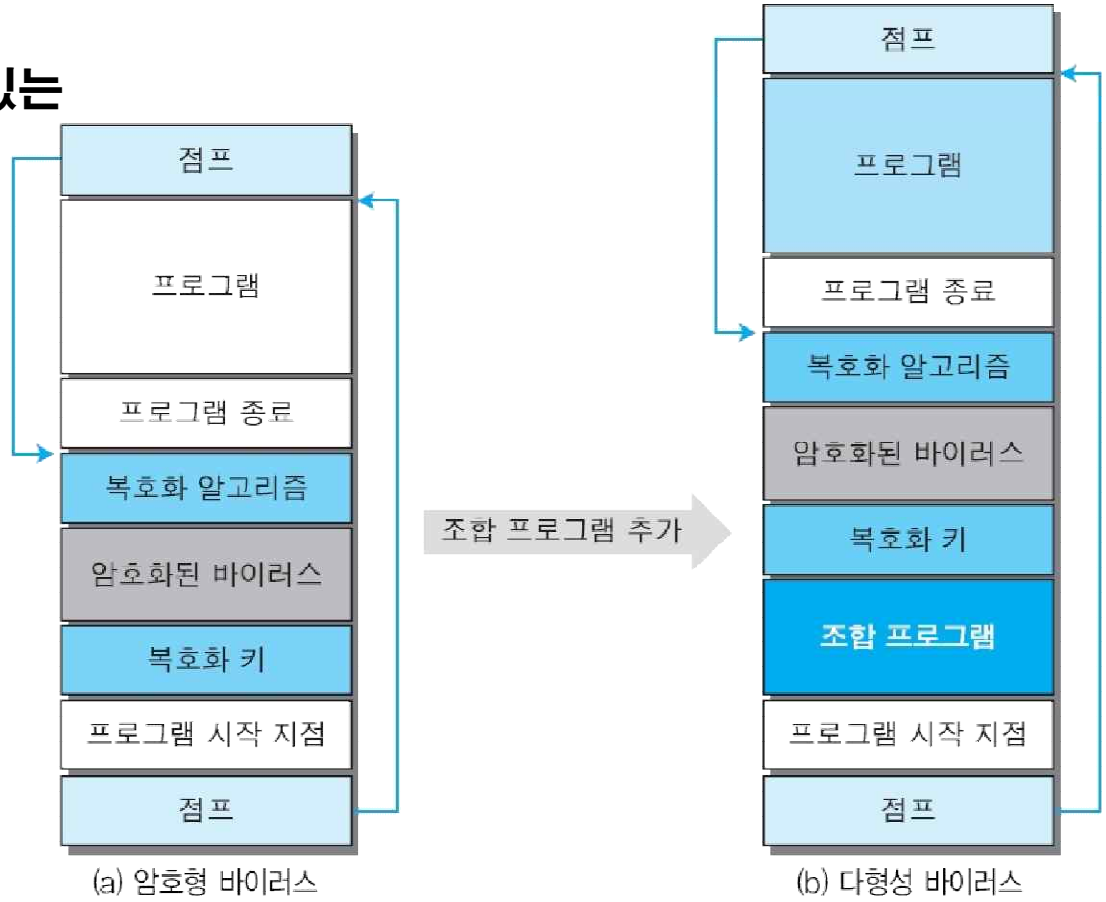
- 이와 같은 이유로 나온 은폐형 바이러스는 직관적인 방법(백신 프로그램 또는 일반적인 정보 확인 등)으로 바이러스 감염 여부를 진단하지 못하게 됨.

- 브레인, 조시, 512, 4096 바이러스 등이 있음

4세대 : 다형성 바이러스

❖ 다형성 바이러스

- 백신 프로그램이 특정 식별자를 이용하여 바이러스를 진단하는 기능을 우회하기 위해 만들어진 바이러스.
- 코드 조합을 다양하게 할 수 있는 조합 프로그램을 암호형 바이러스에 덧붙여 감염되어, 실행될 때마다 바이러스 코드 자체를 변경시켜 식별자로 구분하기 어렵게 함.

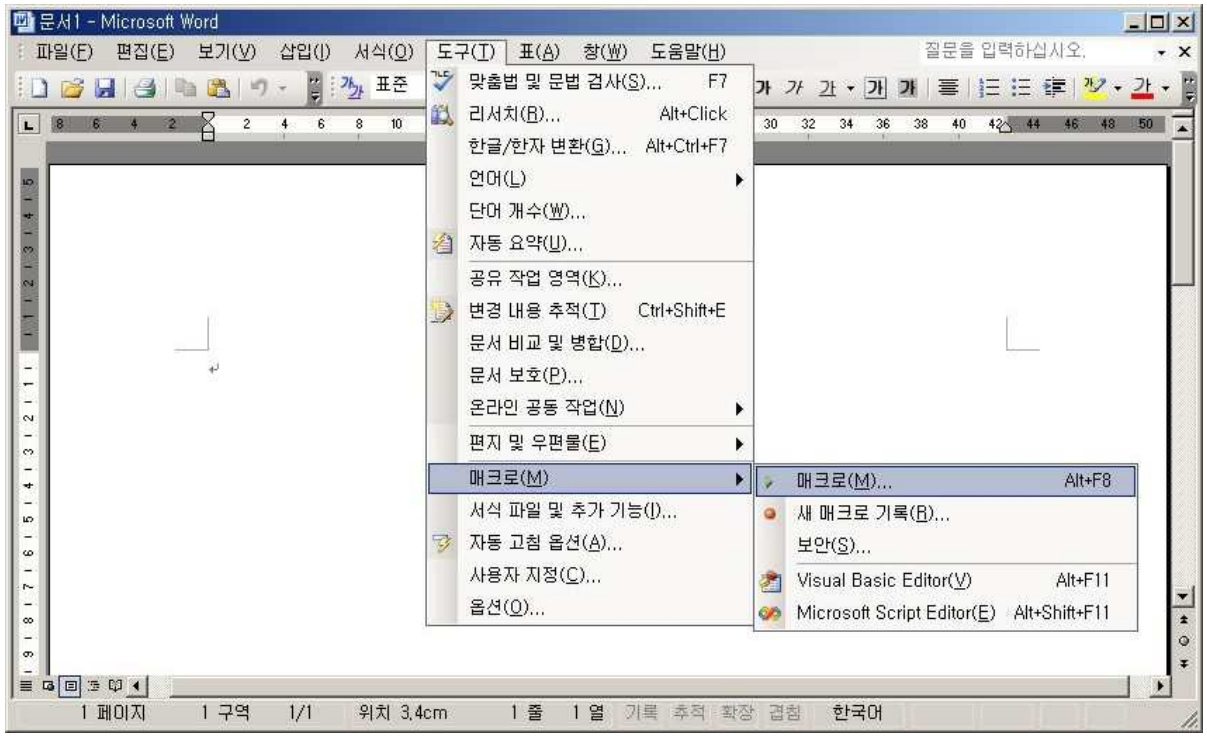


[그림 6-7] 다형성 바이러스

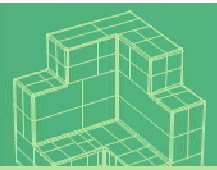
5세대 : 매크로 바이러스

❖ 매크로 바이러스

- 기존의 바이러스는 실행할 수 있는 파일(COM이나 EXE)에 감염된 반면, 매크로 바이러스는 엑셀 또는 워드와 같은 문서 파일의 매크로 기능을 이용하기 때문에 워드나 엑셀 파일을 열 때 감염됨.
- 워드 컨셉트, 와쭈, 엑셀-라룩스, 멜리사 바이러스 등이 있음.



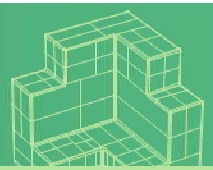
5세대 : 매크로 바이러스



❖ 매크로 바이러스의 증상

- 문서가 정상적으로 열리지 않거나 암호가 설정되어 있음.
- 문서 내용에 깨진 글자나 이상한 문구가 포함어 있음.
- 도구 메뉴 중 매크로 메뉴가 실행할 수 없게 잠겨 있음.
- 엑셀이나 워드 작업 중VB(Visual Basic) 편집기의 디버그 모드가 실행됨.

차세대 바이러스

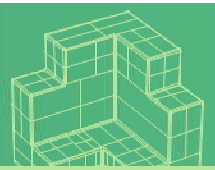


❖ 차세대 바이러스

- 매크로 바이러스에서 나타난 스크립트 형태의 바이러스가 더욱 활성화되고 있으며, 네트워크와 메일을 이용하여 전파되는 방식이 대부분.

- 바이러스는 단순히 데이터를 파괴하고 다른 파일을 감염시키는 형태에서 벗어나 사용자 정보를 빼내가거나 시스템을 장악하기 위한 백도어 기능을 가진 웜의 형태로 진화하고 있음.

Section 03 웜



❖ 웜의 등장

- 1999년 다른 사람의 이메일 주소를 수집하고 스스로 전달되는 형태의 인터넷 웜이 출현하면서 일반인에게 웜이라는 용어가 알려지기 시작.

❖ 웜

- 이메일에 첨부 파일 형태로 첨부되어 확산되거나, 운영체제나 프로그램의 보안 취약점을 이용하여 스스로 침투하는 것이 일반적이나, 현재는 mIRC 채팅 프로그램, P2P 파일 공유 프로그램, 이메일 관련 스크립트 기능, 네트워크 공유 기능 등의 허점을 이용하여 확산하고 증식하는 경우도 있어 피해와 부작용의 범위/크기가 계속 커지고 있음.

MASS Mailer형 웜

❖ 소개

- 최근 발생한 웜 중 약 40%가 MASS Mailer 형에 해당.
- 제목이 없거나 특정 제목으로 전송되는 메일을 읽었을 때 감염. 치료하지 않으면 시스템에 계속 기생하면서 시스템 내부에서 메일 주소를 수집해 계속 메일을 보냄.

❖ 증상

- 메일로 전파되며, 감염된 시스템이 많으면 SMTP 서버(TCP 25번 포트)의 네트워크 트래픽이 증가함.
- 베이글은 웜 파일을 실행할 때 'Can't find a viewer associated with the file'과 같은 가짜 오류 메시지를 출력.
- 넷스카이는 윈도우 시스템 디렉토리 밑에 CSRSS.exe를 만듬.
- 변형된 종류에 따라 시스템에 임의의 파일을 생성.
- 확인되지 않은 메일을 열어볼 때 확산.

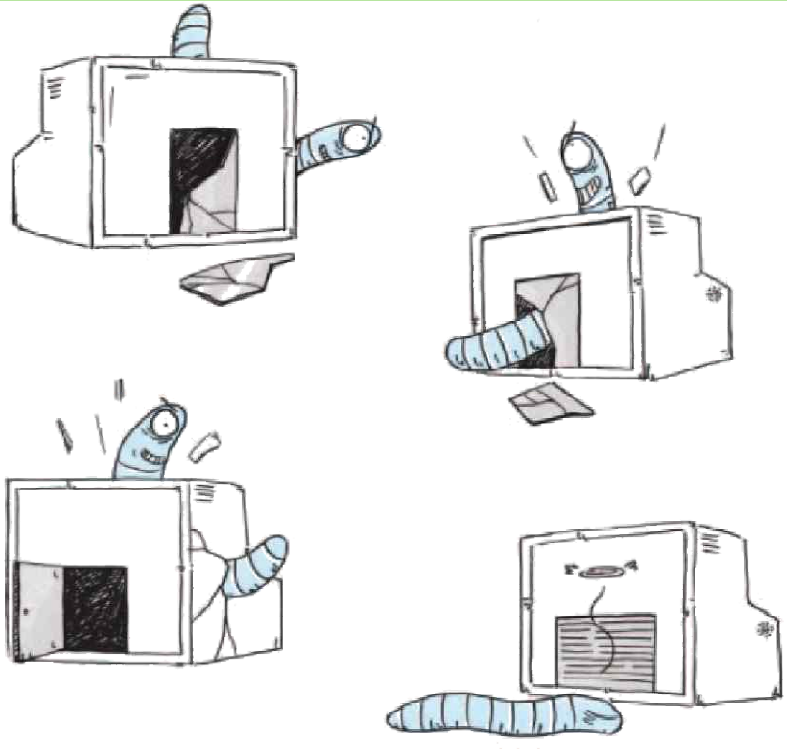
❖ 종류

- 베이글(Bagle), 넷스카이(Netsky), 두마루(Dumaru), 소빅(Sobig) 등

시스템 공격형 웜

❖ 소개

- 운영체제 고유의 취약점을 이용해 내부 정보를 파괴하거나, 컴퓨터를 사용할 수 없는 상태로 만들거나, 외부의 공격자가 시스템 내부에 접속할 수 있도록 백도어를 설치.



[그림 6-9] 취약한 시스템에 대한 웜의 공격

❖ 증상

- 전파할 때 과다한 TCP/135,445 트래픽이 발생.
- winnt, winnt/system32 폴더에 SVCHOST.EXE 등의 파일을 설치.
- 공격 성공 후UDP/5599 등의 특정 포트를 열어 외부 시스템과 통신.
- 시스템 파일 삭제, 정보 유출(게임CD 시리얼 키 등)이 가능.

❖ 종류

- 아고봇(Agobot), 블래스터(Blaster.worm), 웰치아(Welchia) 등

네트워크 공격형

❖ 소개

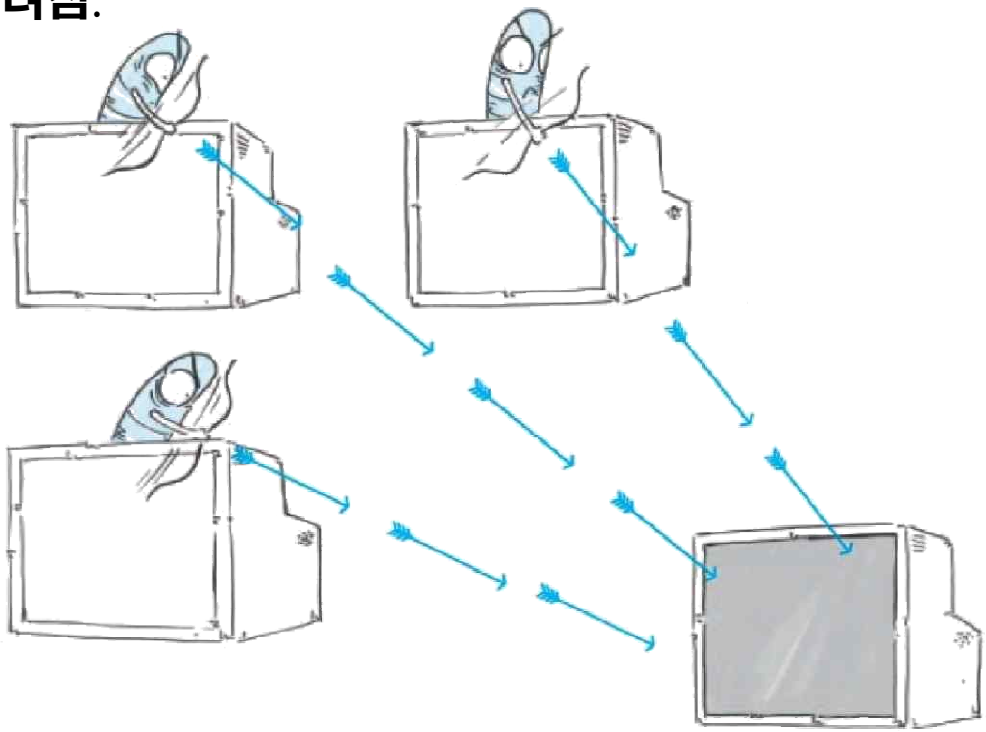
- Syn Flooding, Smurf와 같은 DoS 공격을 수행

❖ 증상

- 네트워크가 마비되거나, 급속도로 느려짐.
- 네트워크 장비가 비정상적으로 동작.

❖ 종류

- 져봇(Zerbo), 클레즈(Klez) 등



[그림 6-10] 웜에 의해 감염된 시스템에서의 네트워크 공격

Section 04 기타 악성 코드- 백도어와 트로이 목마

❖ 트로이 목마

- 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 프로그램

❖ 백도어

- 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로.
- Administrative hook이나 트랩 도어(Trap Door)라고도 부름.

인터넷 악성 코드

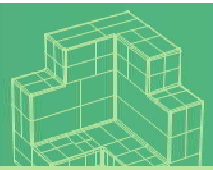
❖ 증상

- 인터넷 익스플로러의 시작 페이지가 계속 다른 곳으로 변경됨.
- 인터넷 속도가 느려지거나 끊김.
- 시스템의 비정상적인 작동으로 운영체제가 사용 불능의 상태가 됨.
- 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 프로그램

❖ 악성 코드를 예방법

- 익스플로러의 [도구]-[보안]-[사용자 지정수준] 메뉴를 클릭→ [보안 설정] 창에서 각 사항을 '확인' 으로 설정
  - 해당 프로그램이 인터넷에서 자동으로 설치되는 것을 막고 사용자가 확인할 수 있음.

스파이웨어

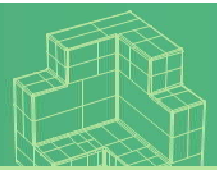


❖ 스파이 웨어

- 자신이 설치된 시스템의 정보를 원격지의 특정한 서버에 주기적으로 보내는 프로그램.

- 사용자가 주로 방문하는 사이트, 검색어 등 취향을 파악하기 위한 것도 있었으나, 패스워드 등과 같은 특정 정보를 원격지에 보냄.

요약



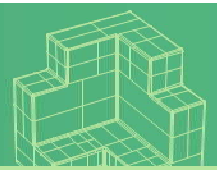
❖ 악성 코드(Malicious Code)

- 수많은 프로그램 코드 중에서 사용자에게 피해를 입히거나 악의적인 동작을 하는 코드를 말한다.

❖ 악성 코드(프로그램)의 종류

- 바이러스
  - 사용자 컴퓨터(네트워크로 공유된 컴퓨터 포함)내에서 사용자 몰래 프로그램이나 실행 가능한 부분을 변형해 자신 또는 자신의 변형을 복사하는 프로그램이다.
  - 가장 큰 특성은 복제와 감염이다.
  - 다른 네트워크의 컴퓨터로 스스로 전파되지는 않는다.
- 웜
  - 인터넷 또는 네트워크를 통해서 컴퓨터에서 컴퓨터로 전파되는 프로그램이다.
  - 다른 컴퓨터의 취약점을 이용하여 스스로 전파되거나 메일로 전파된다.
- 백도어와 트로이 목마
  - 바이러스나 웜처럼 컴퓨터에 직접적인 피해는 입히지 않으나 다른 악의적인 공격자가 컴퓨터에 침투해 컴퓨터를 조작하도록 하는 프로그램이다.
  - 고의적으로 만들어졌다는 점에서 프로그래머의 실수인 버그와는 다르며, 자기 자신을 다른 파일에 복사하지 않는다는 점에서 컴퓨터 바이러스와 구별된다.

요약



❖ 악성 프로그램으로 인해 발생할 수 있는 증상

- 시스템 관련 : 시스템 설정 정보 변경, 파일시스템 파괴, CMOS 정보 파괴, 특정 프로그램 자동 실행, 시스템 종료 등
- 네트워크 관련 : 대량 메일 발송, 네트워크 속도 저하 등
- 하드 디스크 및 파일 관련 : 백도어 및 웜을 위한 백업 파일 생성, 파일 삭제 등
- 특이 증상 : 특정음 발생, 이상 화면 출력, 메시지 상자 출력 등

❖ 바이러스의 종류

- 1세대 원시형 바이러스
  - 부트 바이러스 : MBR과 함께 PC 메모리에 저장되고, 부팅 후에 사용되는 모든 프로그램에 감염시킨다.
  - 파일 바이러스 : 바이러스에 감염된 실행 파일이 실행될 때 바이러스 코드를 실행한다. 바이러스는 프로그램을 덮어쓰는 경우, 프로그램 앞부분에 실행 코드를 붙이는 경우, 프로그램의 뒷부분에 바이러스 코드를 붙이는 경우가 있다.
- 2세대 암호형 바이러스 : 바이러스 코드를 암호화한다.
- 3세대 은폐형 바이러스 : 바이러스가 활동할 때까지 일정 기간 동안 잠복기를 가지도록 제작되었다.

Thank You !

정보 보안 개론 6장 끝