

---

# 10. 악성코드 - I

---

담당교수: 차 영욱

ywcha@andong.ac.kr

# 목차

---

- ❑ 악성코드의 정의 및 증상
- ❑ 컴퓨터 바이러스
  - 파일 바이러스
  - 매크로 바이러스
  - 스크립트 바이러스
- ❑ 웜과 바이러스 웜
- ❑ 트로이목마
- ❑ 스파이웨어
- ❑ 해킹의 정의 및 발달사
- ❑ 스캐닝

# 악성코드(1/2)

---

## □ 정의

- 컴퓨터 및 인터넷의 정상적인 사용을 저해하는 모든 종류의 적대적 소프트웨어
- 일명 악성 소프트웨어(Malicious SW) 또는 멀웨어(Malware)라고 함

## □ 종류

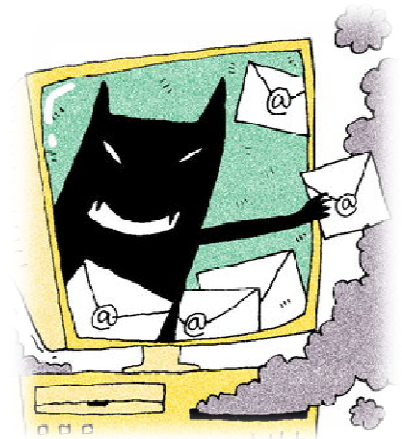
- 컴퓨터 바이러스
- 웜
- 웜 바이러스
- 스파이웨어
- 트로이목마, ...

# 악성코드(2/2)

---

## □ 악성코드의 대표적 증상

- Internet Explorer의 시작페이지가 변경되지 않거나 강제로 변경됨
- 주소 창에 한글 주소 입력 시, 다른 곳으로 접속됨
- 변경하지 않은 Windows 설정이 바뀜
- 접근한 적이 없는 파일이 변경되거나 삭제
- 시스템 속도가 현저히 느려짐
- 문서(워드나 엑셀)가 열리지 않거나 사라짐
- 화면에 이상한 그림이 나타남
- 압축파일 해제 시 에러가 자주 발생



# 컴퓨터 바이러스

□ **생물학:** 스스로 생존하지 못해 숙주 세포 내에 침입해 사는 의존적 생명체

□ **컴퓨터 바이러스**

- 다양한 감염경로(디스켓, 다운로드, 네트워크의 공유폴더, 이메일)로 컴퓨터에 침입하여 실행 가능한 파일이나 문서 파일 내에 복제되어 기생
- 감염된 파일의 실행이나 오픈 시 → 바이러스가 활동하여 컴퓨터에 악의적인 피해를 입히거나 자신을 다른 파일에 복제하여 감염시킴



# 감염 방식에 따른 바이러스

---

- **부트(Boot) 바이러스:** 부트 섹터에 위치하는 바이러스로 컴퓨터의 부팅 시에 활동을 시작
  - 부트 섹터에 쉽게 접근 가능한 운영체제인 MS-DOS나 이를 바탕으로 동작하는 Windows 환경이 주요 공격 대상
  - 뇌(Brain), 원숭이(Monkey), Anti-CMOS
  
- **파일(File) 바이러스:** 확장자로 DLL, COM, EXE를 주로 갖는 실행 가능한 프로그램에 감염되는 바이러스
  - 국내의 80% 정도가 파일 바이러스로 가장 일반적인 유형
  - 예루살렘(Jerusalem:13일의 금요일), Sunday, Win95/CIH. Win95/Morburg
  
- **부트/파일 바이러스:** 부트섹터와 파일을 모두 감염시키는 바이러스
  - 백신 프로그램으로 완전하게 복구할 수 없는 큰 피해를 줌
  - 국내에서 1998년에 발견된 에볼라(Ebola)가 대표적인 바이러스

# 실행파일의 바이러스

□ 실행파일 바이러스인 **예루살렘**에 의한 다른 실행파일의 감염

- ① 파일 바이러스는 실행 파일 내에 자신의 코드를 삽입
- ② 감염된 실행파일을 실행하면 파일 내의 바이러스 코드가 실행되고 바이러스 프로그램이 메모리에 상주
- ③ 이후에 실행되는 모든 실행 파일 내부에 자신의 코드를 복제하여 삽입

```
A:>dir

Volume in drive A has no label
Directory of A:\

JERUSAL COM 1815 1-01-90 9:14p
TEST      COM 1      5-13-90 6:57p
2 File(s) 324096 bytes free

A:>jerusal

A:>test

A:>dir

Volume in drive A has no label
Directory of A:\

JERUSAL COM 1815 1-01-90 9:14p
TEST      COM 1814 5-13-90 6:57p
2 File(s) 322560 bytes free
```

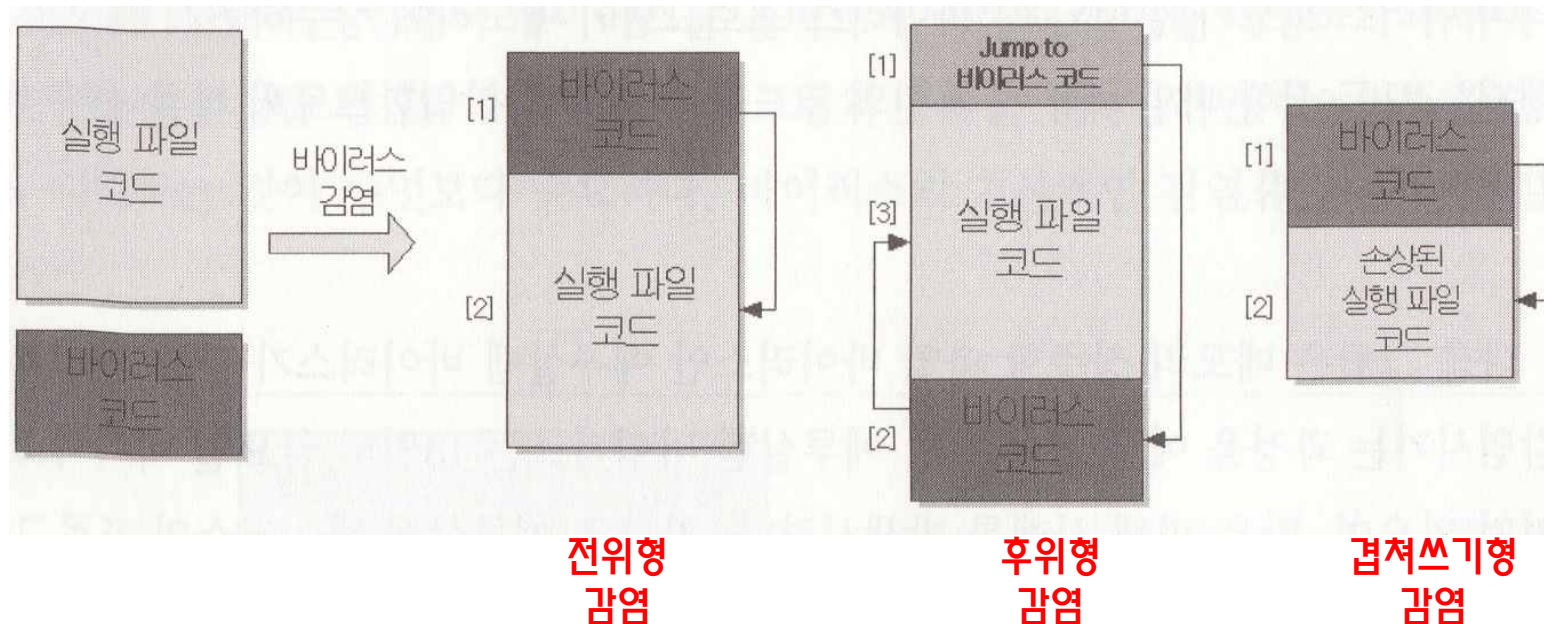
에루살렘 바이러스를 실행하면 바이러스는 메모리에 상주

감염되지 않은 실행 파일을 실행

에루살렘 바이러스에 감염되어 파일 사이즈 증가

# 파일 바이러스의 감염 방식

- 전위형과 후위형 감염: 감염된 파일의 크기가 바이러스 프로그램의 크기만큼 증가하므로 감염 여부를 쉽게 파악할 수 있음
  - 감염된 파일에서 바이러스 코드만을 제거하면 쉽게 복구가 가능
- 겹쳐 쓰기형 감염: 감염된 파일의 크기가 변경되지 않으며, 실행 파일의 일부가 바이러스 코드로 대체되므로 완전한 복구가 어려움





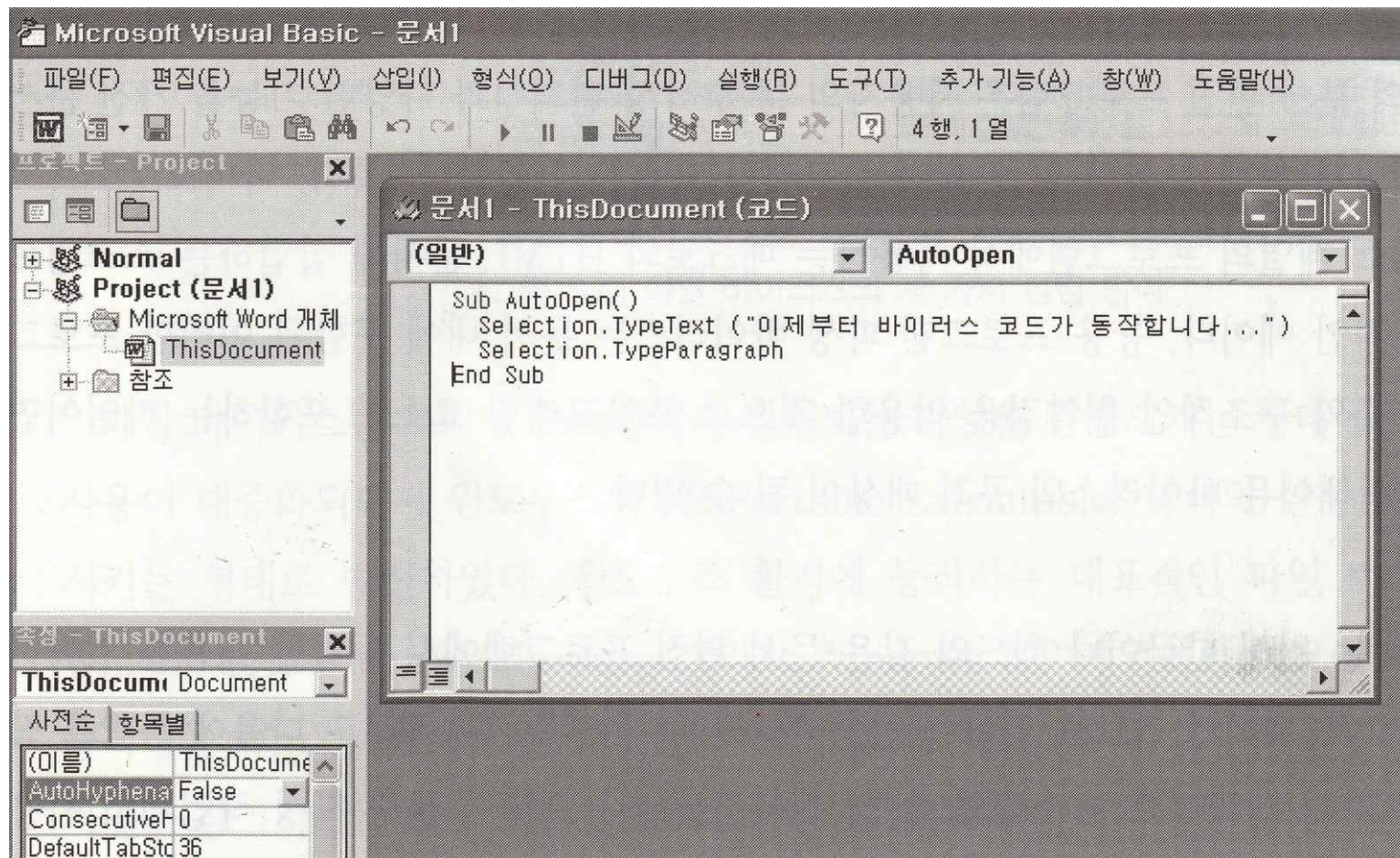
# 매크로(Macro) 바이러스

---

- ❑ 매크로 바이러스는 MS 워드, 엑셀과 같이 매크로 언어를 지원하는 문서파일에 기생
- ❑ 감염된 문서 파일을 여는 순간 바이러스가 동작 → 감염 대상이 실행파일이 아닌 매크로 기능을 사용하는 문서파일
  - 멜리사(W97M/Melisa), 락룩스(XM/Laroux)
- ❑ 멜리사 바이러스: 최초의 매크로 바이러스
  - 오피스 프로그램의 매크로는 오피스 계열의 프로그램에서 사용하는 모든 데이터에 접근 가능하다는 취약점을 이용 → 아웃룩의 주소록에 등록된 50 명의 다른 사용자에게 감염된 문서파일을 첨부하여 전자메일로 송부
  - 메시지 내용: “요청하신 문서입니다. 다른 사람들에게는 보여주지 마십시오.”
  - 첨부된 문서를 여는 순간 컴퓨터는 바이러스에 감염됨
  - 기밀을 요하는 각종 파일이 제멋대로 전송되어 보안에 심각한 문제 발생
  - 과부화로 인한 기업의 전자우편 시스템이 멈추기도 함
  - 인터넷을 타고 순식간에 전세계로 전파되어 ‘인터넷 흑사병’ 이라고 불림

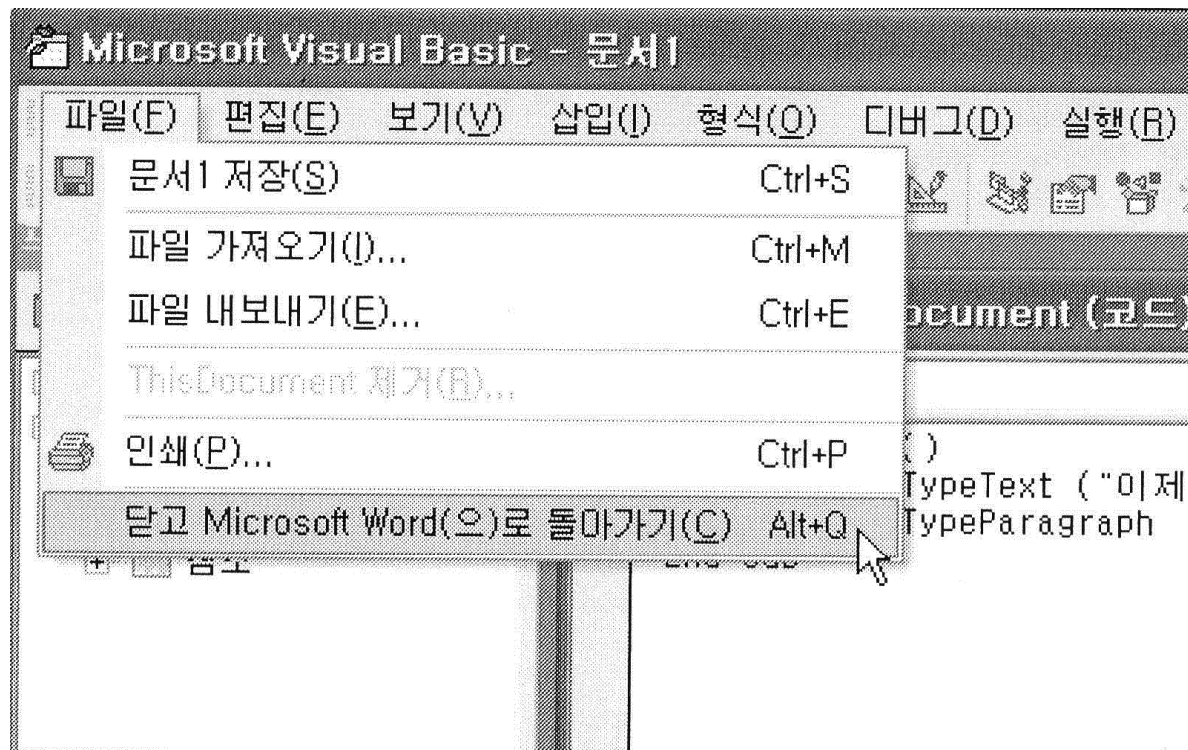
# MS 워드의 매크로 바이러스(1/3)

- ① MS 워드 프로그램을 실행하여 [도구]→[매크로]→[Visual Basic Editor] 메뉴 클릭
- ② VBA(Visual Basic for Application) 언어를 이용하여 매크로 바이러스를 작성



# MS 워드의 매크로 바이러스(2/3)

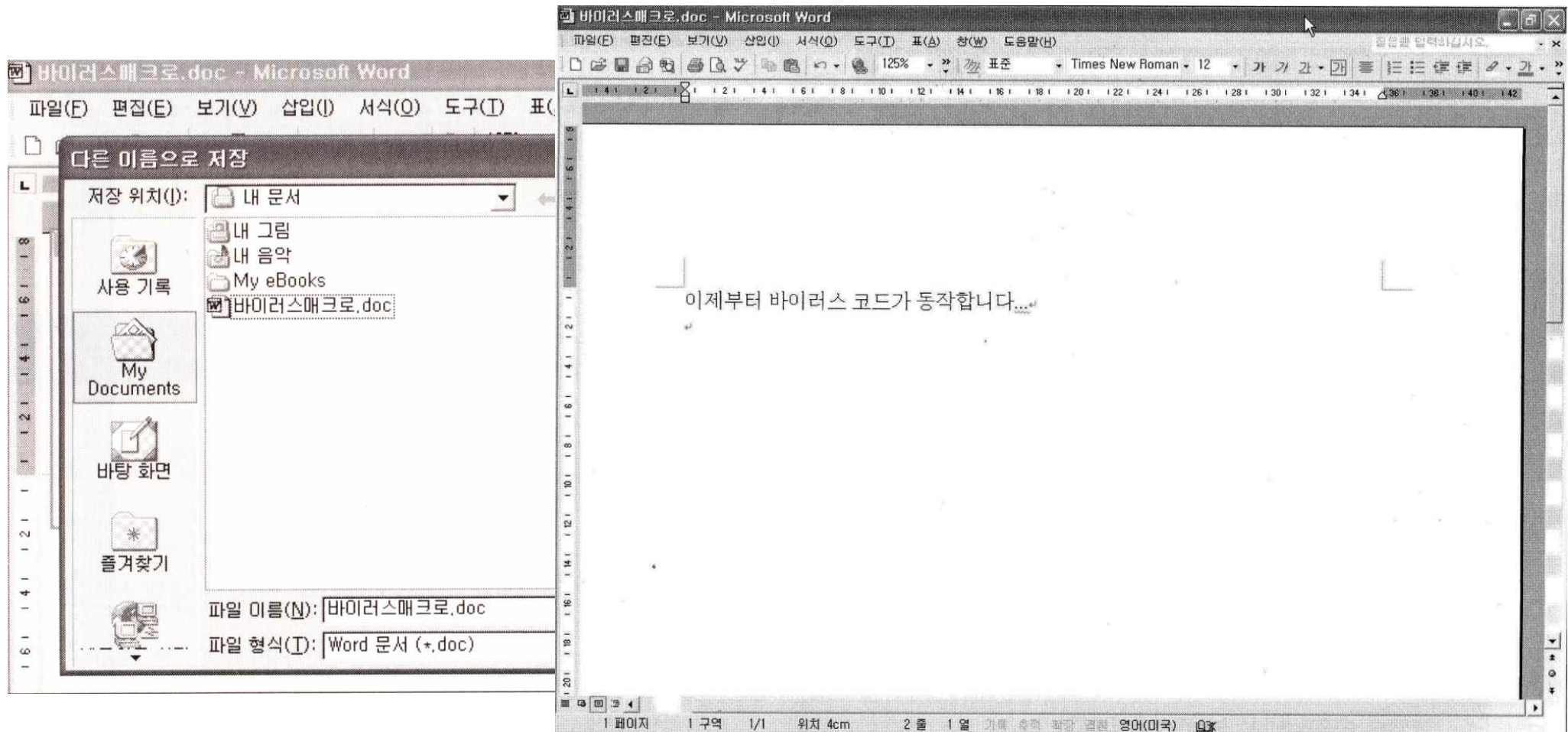
- ③ VBA 편집창에서 [파일]→[... Microsoft Word로 돌아가기]
- ④ MS 워드로 돌아온 다음 [파일]→[다른 이름으로 저장하기]에서 파일을 저장





# MS 워드의 매크로 바이러스(3/3)

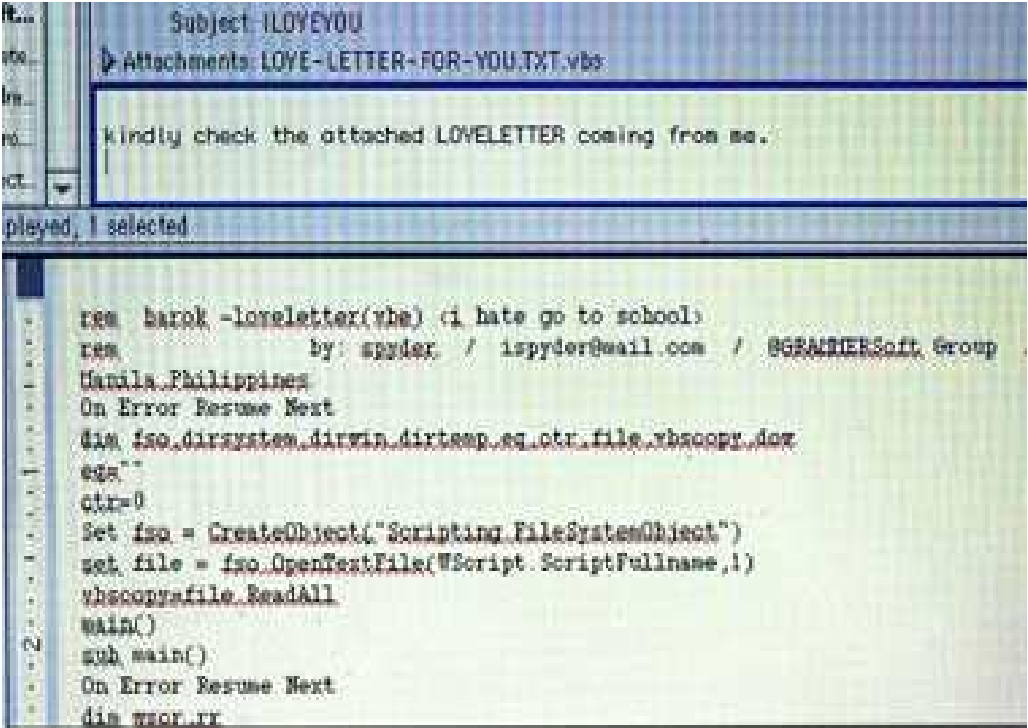
- ⑤ MS 워드를 종료하고 저장된 워드 파일을 더블 클릭하여 열기 → 저장된 매크로가 자동 출력



# 스크립트(Script) 바이러스

- ❑ 바이러스 코드를 스크립트언어(ASP, PHP, Java Script, Visual Basic Script)로 작성
- ❑ 바이러스가 포함되어 있는 문서의 스크립트가 실행되면서 다른 파일을 감염시킴
- ❑ 대표적인 스크립트 바이러스인 러브(Love)는 “I LOVE YOU” 라는 제목의 전자메일을 통하여 유포되며, 첨부된 VBS 파일을 오픈하면 러브 바이러스가 동작

- 하드디스크에 있는 스크립트 파일을 자신의 바이러스 코드로 변경 후에 확장자를 모두 VBS로 변경
- JPG 또는 MP3 파일의 내용을 자신의 바이러스 코드로 변경 후에 확장자를 VBS로 변경 → 인터넷을 통해 그림이나 음악 파일을 쉽게 교환하므로 교환 과정을 통하여 바이러스를 전파하려는 목적
- 레지스트리에 등록하여 감염된 컴퓨터는 부팅과 동시에 러브 바이러스가 동작



```
Subject: I LOVE YOU
Attachments: LOVE-LETTER-FOR-YOU.TXT.vbs

kindly check the attached LOVELETTER coming from me.

played, 1 selected

rem barok -loveletter(vbs) (i hate go to school)
rem
rem by: spyder / ispyder@mail.com / @GAMERSoft Group
 Manila, Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopyr,dos
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullName,1)
vbscopyr=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
```

Love-letter-for-you.txt.vbs

# 바이러스 이름

---

- ❑ 새로운 바이러스가 출현하면 백신 회사는 동작 및 감염 모드 등을 분석하여 CARO(Computer Anti-virus Researcher Organization)의 규약에 의하여 바이러스 이름을 붙이고 백신을 개발
- ❑ 바이러스 이름의 구성 요소(예, Win95/CIH.1024.B)
  - 접두사: 바이러스가 동작하는 운영체제나 프로그래밍 환경 등의 활동 영역을 나타낸다. 윈도우 환경의 경우에는 Win95, W32, JS(Java Script), VBS(Visual Basic Script) 등의 접두사를 사용
  - 특성 명칭: 바이러스에 성을 부여하는 것으로 바이러스 내부의 문자열이나 특징적인 증상을 이용
  - 주요 변수: 바이러스 변종을 구분하는 접미사로 주로 바이러스 프로그램의 길이를 표기
  - 보조 변수: 단일 바이러스의 여러 변종을 구분하는 추가적인 접미사로 알파벳이나 로마자를 사용

# 웜

---

- ❑ 바이러스가 다른 프로그램에 기생하는 것에 반해 웜(Worm)은 독립적으로 존재하는 실행 가능한 프로그램
  - 바이러스와 달리 특정 파일을 감염시키는 것이 아니라 웜 자신을 복제하여 배포
  - 특별한 숙주 프로그램이나 파일에 의존하지 않고 네트워크를 통하여 다른 컴퓨터로 자신을 복제할 수 있음
  - 손상된 시스템의 데이터나 운영체제를 파괴하거나 자신을 무제한으로 복제하고 이를 네트워크에 배포함으로써 시스템과 네트워크를 마비시킴
- ❑ 모리스 웜: 1988년에 생긴 최초의 웜으로 며칠 만에 6천대의 서버가 감염되어 마비
- ❑ 인터넷 웜: e-메일을 읽으면 감염되어 주소록에 있는 사람들에게 웜 자신을 보냄
  - I-Worm/Happy99, I-Worm/ExploreZip, I-Worm/PrettyPark

# 슬래머(Slammer) 웜

---

- ❑ Windows XP 및 NT에서 동작하는 초기의 MS-SQL 서버: 클라이언트가 서버가 지원하는 용량보다 큰 데이터를 전송하는 경우 버퍼의 오버플로우 발생 → 서버 프로그램의 메모리 영역을 침범하면서 서버의 오동작과 제어권을 잃어버리는 경우 발생
- ❑ MS-SQL 서버의 버퍼 오버플로우 취약점을 이용하여 서버 컴퓨터에 침입하고 자신을 무제한 복제하며, 네트워크에 연결된 컴퓨터들의 동일한 취약점을 찾아 공격
  - ① 슬래머 웜은 MS-SQL 서버가 서비스하는 1434 포트로 네트워크의 컴퓨터들에 접속 → MS-SQL서버가 구동하고 있지 않으면 침입할 수 없음
  - ② 서버에 접속 되면 서버가 지원하는 버퍼의 용량보다 큰 데이터(다량의 슬래머 웜 코드)를 한꺼번에 전송 → 서버가 오동작하면서 제어권을 잃음
  - ③ 제어권을 가지게 된 슬래머 웜은 서버가 동작하는 동안 무작위로 생성한 IP 주소로 슬래머 웜 자신을 복제하여 네트워크로 전송
  - ④ 복제되어 전송된 슬래머 웜은 이 과정을 반복하면서 MS-SQL 서버를 찾아 감염시키면서 네트워크의 부하를 증가시킴



# 슬래머 웜에 의한 인터넷 대란

## □ 2003년 1월 25일의 슬래머 웜에 의한 인터넷 대란

- 1차적으로 서버 컴퓨터와 인터넷의 마비가 발생하고 2차적으로 인터넷에 기반한 모든 서비스 중지
- **해결책:** 전국의 모든 MS-SQL 서버 사용자들이 자신의 서버에서 해당 포트를 차단하고 MS가 제공하는 패치 파일을 설치

### [인터넷] SQL슬래머 웜 10분만에 확산

한국일보 | 기사입력 2003-02-04 19:02 | 최종수정 2003-02-04 19:04

#### \*인터넷공격 새모델 될수독\*

지난달 25일 한국의 인터넷 망을 마비시킨 '윈도 SQL 슬래머' 웜은 단10분만에 전세계로 퍼진 역사상 가장 빠른 웜 바이러스이며, 웜 역사의 중요한 전환점이 될 것으로 분석됐다.

3일 BBC 방송에 따르면 인터넷 데이터 분석 협력협회(CAIDA)는 슬래머웜을 분석한 보고서를 통해 이같이 밝히고 "슬래머 웜은 향후 인터넷 공격의 모델이 될 수도

# 슬래머 웜의 감염 속도

---

## □ 가정

- 슬래머 웜(376 바이트의 크기)에 의하여 감염된 MS-SQL 서버는 초당 4MB의 공격 패킷을 전송
- 인터넷에 연결된 100 대의 컴퓨터 중에 1대가 MS-SQL 서버

## □ 감염된 MS-SQL서버는 초당 1,394개의 복제된 슬래머 웜을 전송

- $4,194,304 \text{ 바이트} \div 376 \text{ 바이트} = 1,394$

## □ 감염 속도

- 1초가 경과하면 초당 14대( $1,394 \div 100$ )의 MS-SQL 서버가 감염
- 2초 후에는 196대
- 3초 후에는 2,744대
- ...
- 10초 후에는 약 3억대의 서버가 감염

# 웜의 유형

## □ 시스템 공격형 웜

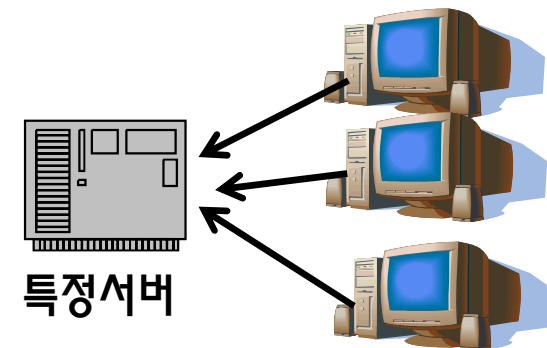
- 운영체제 고유의 취약점을 이용해 내부 정보를 파괴하거나, 컴퓨터를 사용할 수 없는 상태로 만들거나, 외부의 공격자가 시스템 내부에 접속할 수 있도록 백도어를 설치

## □ 대량의 메일 발송형 웜

- 제목이 없거나 특정 제목으로 전송되는 메일을 읽었을 때 감염
- 치료하지 않으면 시스템에 계속 기생하면서 시스템 내부에서 메일 주소를 수집해 계속 메일 전송

## □ 네트워크 공격형 웜

- 웜에 의해 감염된 시스템이 특정시간에 특정서버로 일제히 접속을 시도 하여 DDOS 공격 수행



웜에 의해 감염된 시스템에서의  
네트워크 공격

# 웜 바이러스

---

- 최근의 컴퓨터 운영체제는 악성 소프트웨어의 침입 방어를 위해 프로그램의 실행 권한을 철저히 제한한다. 즉, 네트워크를 통해 침투한 프로그램이 사용자의 실행 명령 없이 실행되는 것을 제한한다.
  - 웜이 특정 컴퓨터에 침입하더라도 실행 권한에 제한이 있을 경우 동작할 수 없다.
  - 이러한 보안 정책을 뚫고 침투하기 위해 악성 소프트웨어 개발자는 **웜과 바이러스의 특성을 가진 웜 바이러스**를 개발
  
- 웜 바이러스의 특징
  - 공격 대상 컴퓨터에 대한 침투까지는 웜의 방식, 침투가 완료된 이후에는 바이러스 방식으로 감염시킴
  - 최근 활동하는 바이러스는 대부분 웜 바이러스 방식

# 바이러스와 웜의 비교

|      | 바이러스   | 웜  |
|------|--|--|
| 감염대상 | 있음(파일을 감염시켜 기생)  | 없음(독립적으로 존재하며 스스로 확산)  |
| 실행방법 | 사용자가 감염된 파일을 동작시켜야 바이러스 실행됨                                  | 네트워크를 통해 번식이 가능한 컴퓨터를 탐색해서 자신을 복제해서 침투                                   |
| 피해   | 정상적인 컴퓨터 작동 및 프로그램 수행을 방해                                    | 네트워크를 손상시키고 대역폭을 잠식시킴  |
| 치료방법 | 파일을 치료 후 복구  | 웜 파일 자체를 삭제  |
| 예    | test.exe 라는 감염된 파일을 실행하면 바이러스가 실행되어 정상적인 다른 파일을 감염 시켜 못쓰게 만듦 | test.exe 라는 웜 파일의 실행 시 다른 파일을 손상시키진 않지만, 1.exe에서 100.exe 라는 파일이 계속적으로 생성 |

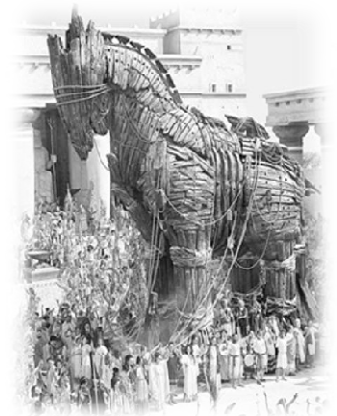
## □ 웜과 바이러스가 분명히 구분 되어야 하는 이유

- 컴퓨터 바이러스를 웜으로 오인하고 삭제 한다면 윈도우에 중요한 파일이 삭제되는 잘못된 치료가 될 수 있음

# 트로이목마

---

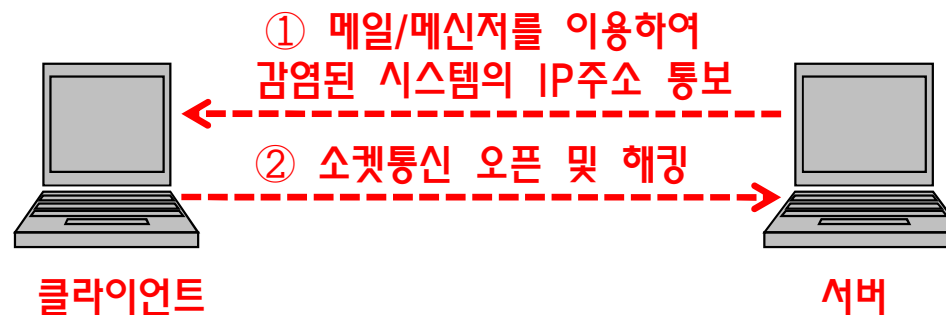
- ❑ 지속적인 정보유출 및 제어권 획득이 목적이므로 컴퓨터 사용자가 트로이목마(Trojan horse)의 침투 및 활동을 인식하지 못하도록 설계되어 있음.
- ❑ 트로이목마는 바이러스와 같이 자기 복제 기능이 없으며 웜과 같이 증식 능력도 없음
  - 자신을 복사하지 않아 파일을 감염시키지 않으므로 해당 파일만 삭제하면 치료 가능
- ❑ 감염경로
  - 유용한 프로그램(백신 프로그램, 게임 프로그램)으로 가장하여 다운로드를 권장 → 다운로드 받은 프로그램 내에 트로이목마 프로그램이 숨겨져 있음
  - 다운로드 받은 프로그램을 실행하면 트로이목마 프로그램도 같이 실행
  - 한번 실행된 트로이목마는 컴퓨터 부팅 시에 자동으로 동작하도록 레지스트리를 변경



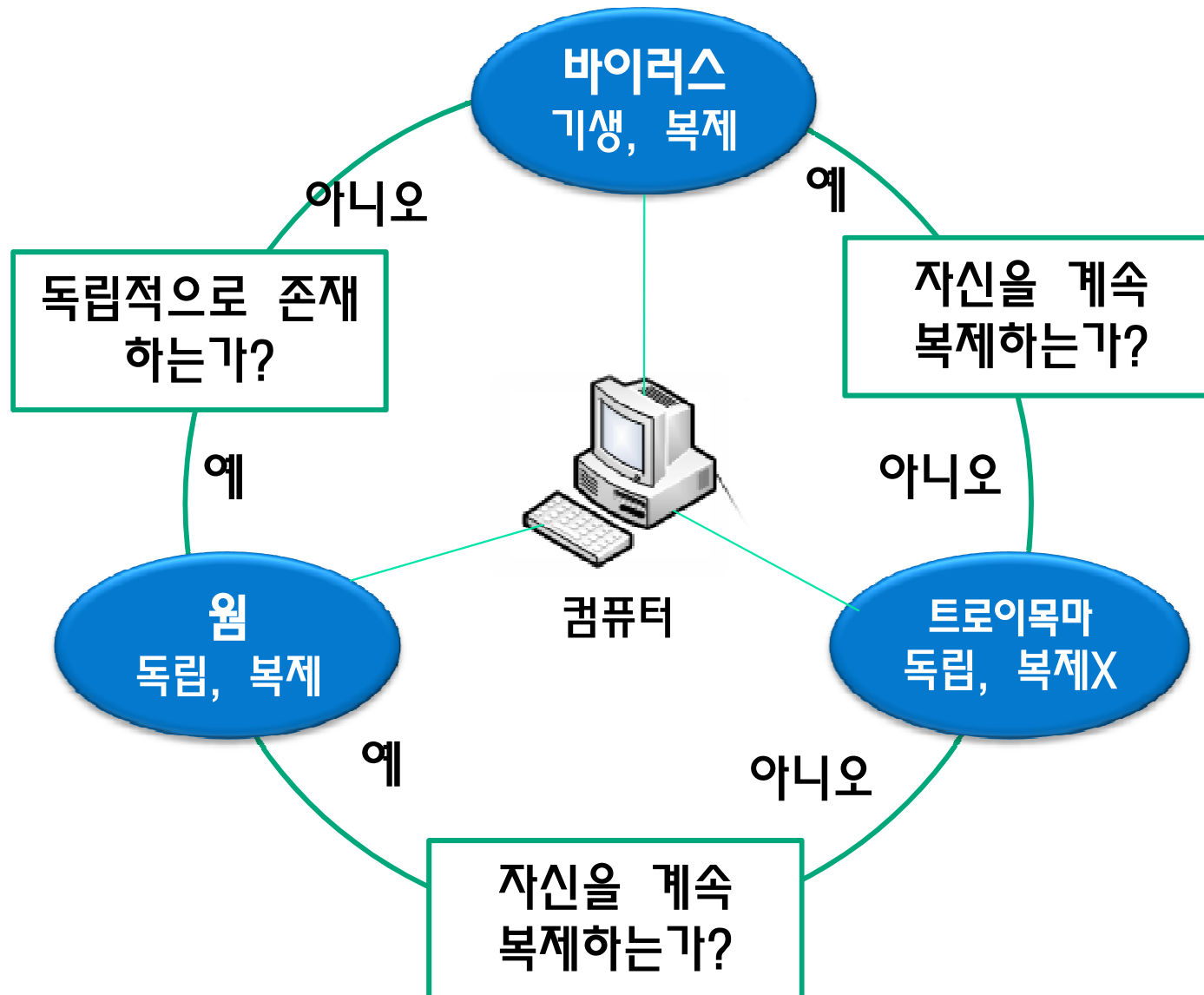
# 트로이목마의 클라이언트 및 서버 프로그램

## □ 트로이목마의 클라이언트 및 서버 프로그램

- 클라이언트 프로그램: 원격에서 공격대상 시스템을 조정하는 프로그램
- 서버 프로그램: 공격대상 시스템에 위치(윈도우가 사용하는 디렉토리에 주로 위치)
- 파일명은 **explorer.exe**와 같이 시스템이 사용하는 파일처럼 위장
- 서버 파일이 설치된 후 외부의 클라이언트가 접속할 특정 포트를 오픈
- 레지스트리나 system.ini, autoexec.bat 등을 수행하여 감염된 시스템이 리부팅하는 경우에 트로이목마의 서버 프로그램도 재실행되도록 설정



# 바이러스와 웜 및 트로이목마의 비교





# 스파이웨어

---

## ❑ 첩자(spy)와 소프트웨어의 합성어

- 과도하게 사용자의 정보를 수집하거나 사용자의 동의 없이 컴퓨터에 몰래 들어와 개인 정보를 빼가는 트로이 목마 형태의 침입으로 변질
- 세어웨어, 프리웨어 등과 함께 다운로드 파일에 포함되어 따라오는 경우가 대부분

## ❑ 스파이웨어의 종류

- **Adware(애드 웨어):** 정보의 수집보다는 광고에 주력하는 프로그램이지만 그 정도가 지나쳐 사용자에게 불편을 초래
  - 사이트 접속 유도: 사이트 바로 가기를 생성, 즐겨 찾기에 사이트 추가
  - 팝업 창 : 웹 브라우저 사용 중에 주기적으로 광고 팝업 창을 출력
  - 시작 페이지 고정: 사용자의 동의 없이 특정 사이트를 시작페이지로 추가
- **Trackware(트랙 웨어):** 사용자의 방문사이트, 검색어 등을 수집하여 제작자에게 전송하는 프로그램으로 개인 정보를 유출 시킴
- **Dialer(다이알러):** 특정 인터넷 사이트에 자동 로그인 또는 지속적으로 로그인을 유지하도록 함으로써 과도한 사용료를 부과하도록 유도하는 프로그램

# 해킹의 정의

## □ 과거와 현재의 해킹(Hacking)

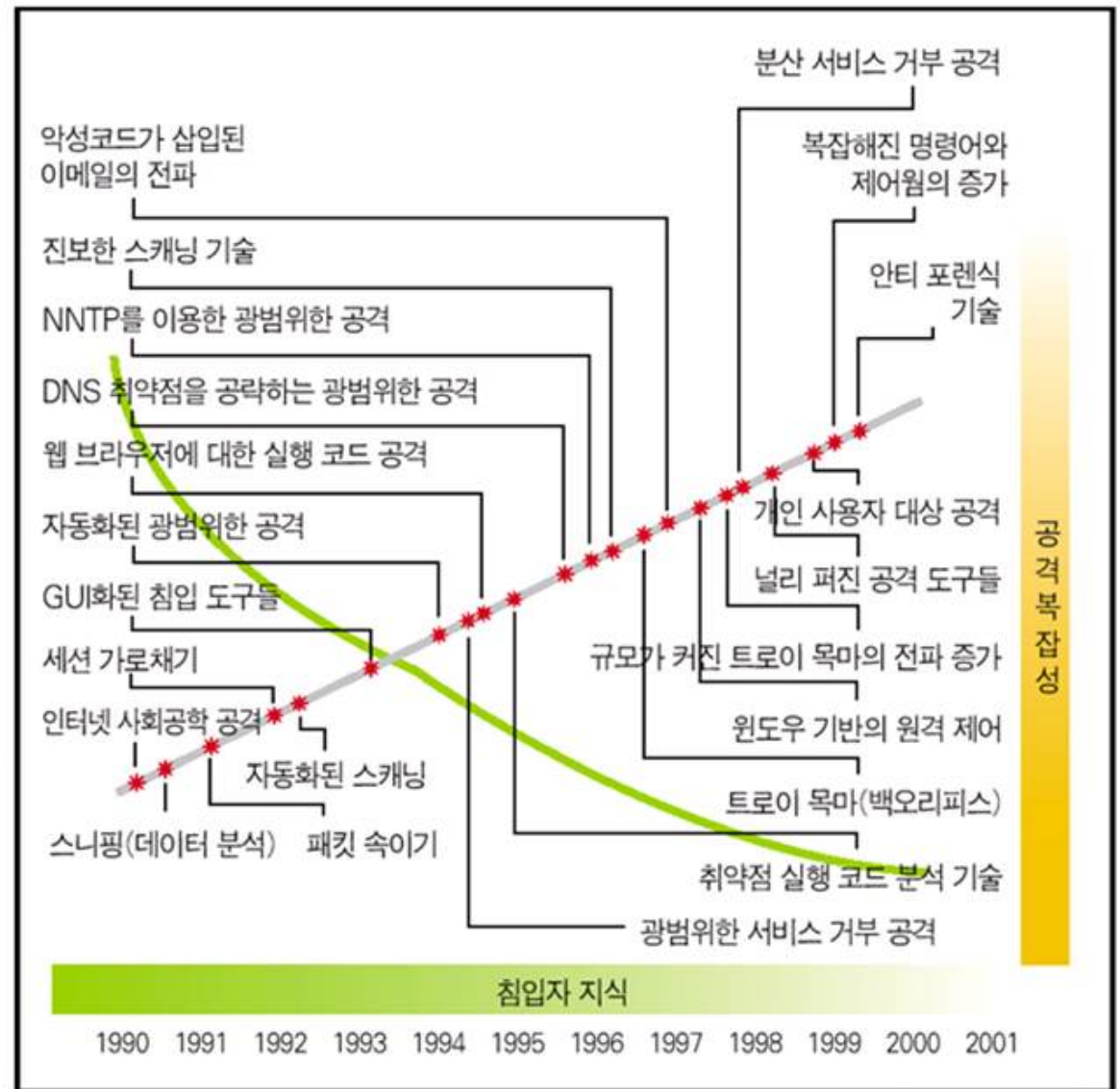
- 과거의 해킹: 컴퓨터에 대해 많은 지식을 가지고 컴퓨터의 사용을 즐기는 행위
- 현재의 해킹: 컴퓨터 네트워크의 보안 취약점을 찾아내어 그 문제를 해결하고 이를 악의적으로 이용하는 것을 방지하는 행위

## □ 크래킹(Cracking): 일반적으로 알려진 컴퓨터를 이용한 범죄

- 컴퓨터 시스템에 다른 사람이 만들어 놓은 지식을 훔쳐 이를 이용하거나,
- 해당 시스템이 어떻게 동작하는지 알기 위해 침투하는 일련의 범죄 행위

# 해킹 기술과 공격도구의 발전사

- ❑ 해커의 자기과시에서 정치적, 경제적 이익 추구
- ❑ 해킹 기술과 공격도구 경향
  - 공격 도구의 사용 편의성 및 공격 능력 증대
  - 침입자에게 요구되는 지식 감소



출처 | 카네기 멜론 대학

# 해커의 종류

- ❑ 레이머(Lamer): 해커가 되고 싶지만 경험도 없고 컴퓨터 관련 지식도 많지 않은 해커
- ❑ 스크립트 키디(Script Kiddies): 네트워크와 운영체제에 대한 약간의 기술적인 지식이 있는 해커
- ❑ 디벨롭트 키디(Developed Kiddies): 대부분의 해킹 기법에 대해 알고 있으며, 취약점을 발견할 때까지 여러 번 시도해 시스템에 침투할 수 있을 정도의 실력을 가진 해커
- ❑ 세미 엘리트( Semi elite): 컴퓨터 운영체제와 네트워크에 대한 포괄적인 지식과 특정 취약점을 이용하여 공격할 수 있는 해킹 코드를 만들 수 있는 수준의 해커
- ❑ 엘리트(Elite): 해킹 하고자 하는 시스템의 새로운 취약점을 찾아 해킹 할 수 있고 흔적도 남기지 않을 정도로 실력이 있는 해커

# 해킹 전의 정보 획득 - 스캐닝

## □ 정보 획득

- 게시판 관리자의 이메일을 통해 관리자의 아이디 취득과 같이 해킹하고자 하는 대상의 기초적인 정보를 습득하는 행위

## □ 스캐닝

- 정보 획득을 위한 기술적인 방법으로 해킹하고자 하는 대상 시스템의 존재 및 작동 여부, 제공하는 서비스 등을 확인하기 위한 방법
- Ping 스캐닝, TCP 스캐닝, UDP 스캐닝, 스텔스 스캐닝, ...

| 포트번호    | 용용 계층   |
|---------|---------|
| 7       | Echo    |
| 13      | Daytime |
| 20, 21  | FTP     |
| 23      | Telnet  |
| 25      | SMTP    |
| 53      | DNS     |
| 67, 78  | BOOTP   |
| 80      | HTTP    |
| 111     | RPC     |
| 161,162 | SNMP    |

# Ping 스캐닝

- ❑ ICMP 프로토콜을 사용하는 Ping 유틸리티를 이용하여 공격 대상 시스템의 활성화 여부를 확인하는 스캐닝
  - 32바이트: ICMP 패킷 길이
  - 시간: ICMP 요청 및 응답 패킷의 왕복지연
  - TTL(Time To Live): 패킷의 최대 수명을 나타내며, 라우터를 지날 때마다 1씩 감소
  - 응답이 오면 상대 시스템이 활성화 되어 있음을 나타낸다. 그러나, 요즘 시스템의 대부분은 ping의 응답 기능을 막고 있다.



```
C:\Windows\system32\cmd.exe

C:\W>ping 220.69.240.197

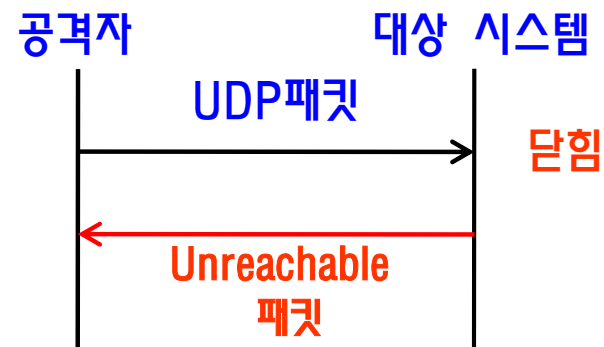
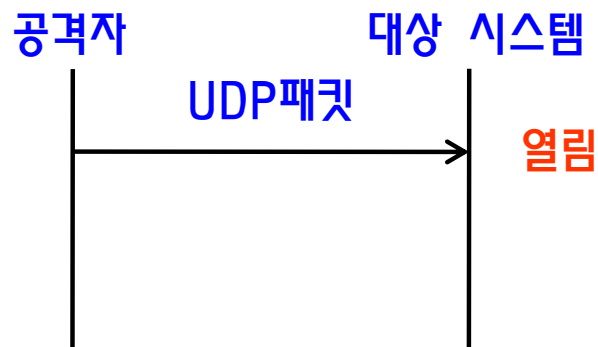
Ping 220.69.240.197 32바이트 데이터 사용:
220.69.240.197의 응답: 바이트=32 시간<1ms TTL=128
220.69.240.197의 응답: 바이트=32 시간<1ms TTL=128
220.69.240.197의 응답: 바이트=32 시간<1ms TTL=128
220.69.240.197의 응답: 바이트=32 시간<1ms TTL=128

220.69.240.197에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
    왕복 시간<밀리초>:
        최소 = 0ms, 최대 = 0ms, 평균 = 0ms

C:\W>
```

# UDP 스캐닝

- UDP를 이용하는 응용계층의 포트번호를 스캔 → 포트가 열려 있다면 해당 시스템의 응용계층이나 프로그램이 활성화 되어 있다고 인식
  - 열린 경우: 응답 없음
  - 닫힌 경우: ICMP의 도달불능(Unreachable) 패킷 리턴



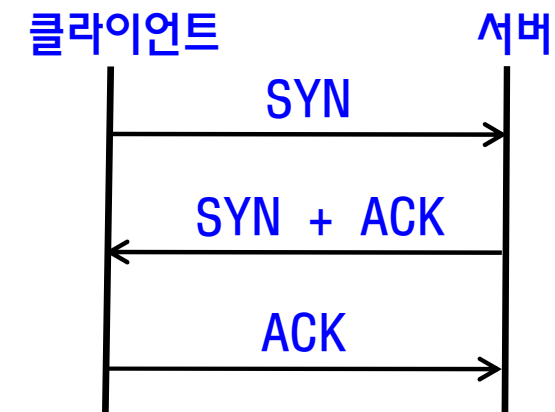
# TCP의 메시지 포맷 및 3중 핸드셰이킹

## □ 제어필드의 플래그

- SYN: Synchronize sequence numbers
- ACK: Acknowledgement
- FIN: Terminate the connection
- RST: Reset the connection
- URG: Urgent pointer
- PSH: Push the data



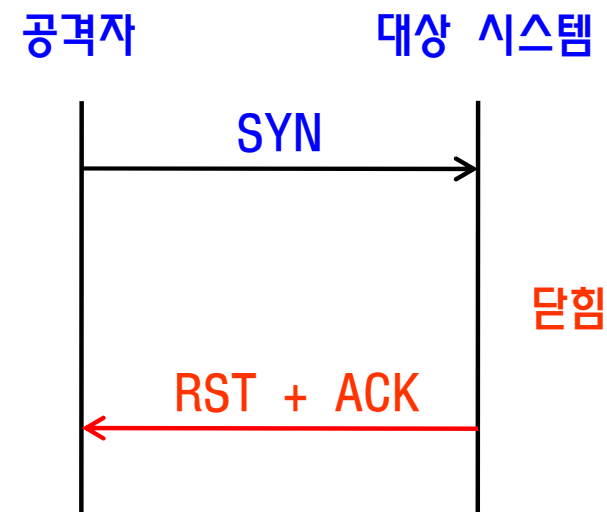
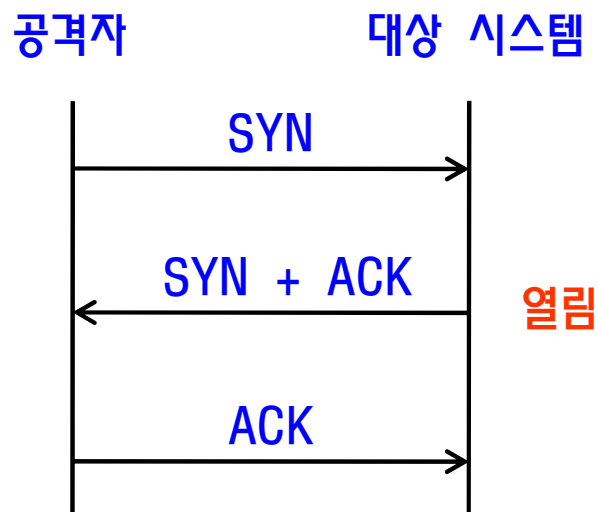
## □ 3중 핸드셰이킹(three way handshaking)을 이용한 연결설정





# TCP Open 스캐닝

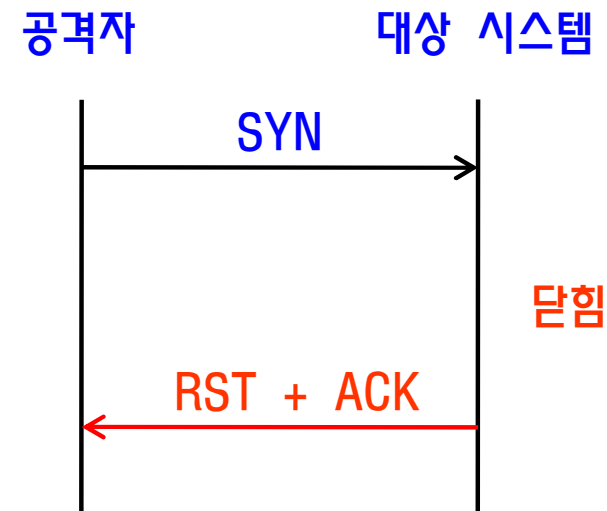
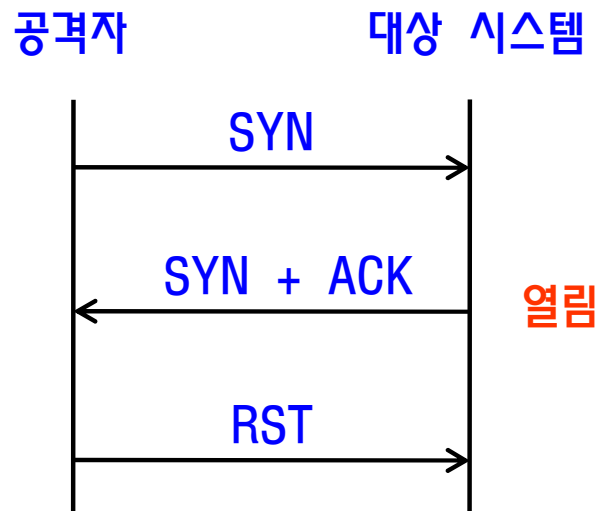
- 3중 핸드셰이킹을 이용하여 TCP의 포트번호를 이용하는 응용계층과의 **완전한 연결을 생성**함으로써 대상 시스템의 활성화 여부를 측정하는 방법
  - **열린 경우**: SYN+ACK가 돌아오고 공격자는 ACK를 전송
  - **닫힌 경우**: RST+ACK 패킷을 받고 종료
  - **단점**: 연결을 생성하기 때문에 대상 컴퓨터의 로그에 방문 기록이 존재



# TCP Half Open 스캐닝

□ TCP Open 스캐닝과 유사하지만 **ACK를 이용하여 연결을 완성하지 않는 방법**

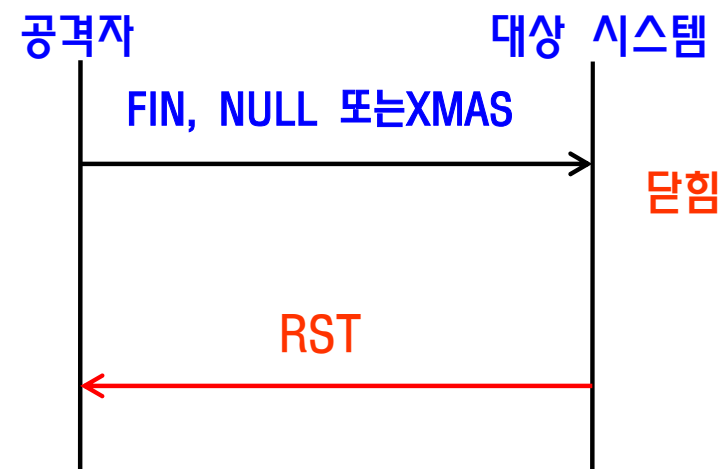
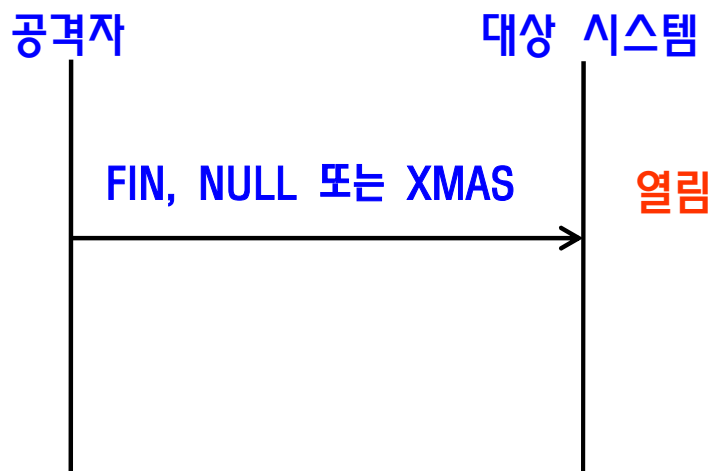
- 연결이 완료되지 않으므로 대상 컴퓨터의 로그에 접속 기록이 남지 않음
- 열린 경우: 연결을 생성하지 않기 위해 RST 패킷을 보내 연결을 해제
- 닫힌 경우: RST+ACK 패킷을 받고 종료



# 스텔스 스캐닝

## □ 공격 대상 시스템에 자신의 흔적을 남기지 않는 스캐닝 방법의 총칭

- 공격자는 대상 시스템의 활성화 여부를 알기 위해 플래그 값이 **FIN, NULL 또는 XMAS** 인 패킷을 전송
  - NULL: 플래그 값을 설정하지 않고 보낸 패킷
  - XMAS: ACK, FIN, RST, SYN, URG 플래그를 모두 설정하여 보낸 패킷
- 열린 경우: 응답이 없음
- 닫힌 경우: RST 패킷의 반송
- TCP Half Open 스캐닝도 스텔스 스캐닝의 일종



# 요점정리(1/2)

- ❑ **악성코드:** 컴퓨터 및 인터넷의 정상적인 사용을 저해하는 모든 종류의 적대적 S/W
  - 컴퓨터 바이러스, 웜, 웜 바이러스, 스파이웨어, 트로이목마, ...
  
- ❑ 바이러스가 다른 프로그램에 기생하는 것에 반해 **웜(Worm)**은 독립적으로 존재하는 실행 가능한 프로그램
  - 바이러스와 달리 특정 파일을 감염시키는 것이 아니라 웜 자신을 복제하여 배포
  
- ❑ **웜 바이러스:** 공격 대상 컴퓨터에 대한 침투까지는 웜의 방식, 침투가 완료된 이후에는 바이러스 방식으로 감염시킴
  - 최근 활동하는 바이러스는 대부분 웜 바이러스 방식
  
- ❑ **트로이목마:** 지속적인 정보유출 및 제어권 획득이 목적이므로 컴퓨터 사용자가 **트로이목마(Trojan horse)**의 침투 및 활동을 인식하지 못하도록 설계되어 있음.
  - 트로이목마는 바이러스와 같이 자기 복제 기능이 없으며 웜과 같이 증식 능력도 없음

## 요점정리(2/2)

- **스파이웨어**: 첩자(spy)와 소프트웨어의 합성어
  - 애드 웨어, 트랙 웨어, 다이알러
  
- **해킹**: 컴퓨터 네트워크의 보완 취약점을 찾아내어 그 문제를 해결하고 이를 악의적으로 이용하는 것을 방지하는 행위
  - **크래킹(Cracking)**: 일반적으로 알려진 컴퓨터를 이용한 범죄
  
- **스캐닝**: 정보 획득을 위한 기술적인 방법으로 해킹하고자 하는 대상 시스템의 존재 및 작동 여부, 제공하는 서비스 등을 확인하기 위한 방법
  - **Ping 스캐닝, TCP 스캐닝, UDP 스캐닝, 스텔스 스캐닝, ...**