악성코드와 소프트웨어 보안

악성코드란?

- 악성코드의 종류와 특징

악성코드의 종류와 특징

- 바이러스
  - 숙주 프로그램 실행 시 같이 실행
  - “자기 복제” 코드
- 웜
  - 독자적 실행
  - 스스로 전파
  - CPU 자원 낭비
- 트로이 목마
  - 내부 기생 코드
  - 자기 복제 능력 x
  - 백도어(Back-Door) 가능
  - 무한 리부팅 가능
- 애드웨어
  - 다른 프로그램 실행 시 광고를 강제로 띄움
  - 트로이 목마 기능 탑제 가능

바이러스

- 부트 바이러스
- 파일 바이러스
- 부트/파일 바이러스
- 매크로 바이러스

부트 바이러스

- 운영체제 실행 전 실행
- 플로피 디스크 시절 자주 사용 됨
  - 브레인, 몽키, 미켈란젤로
- 하드 디스크 보급화 이후 드물게 발견됨

파일 바이러스

- 실행 파일에 바이러스 복제
- 실행 파일 감염 바이러스
- 자주 사용되던 바이러스
  - 예루살렘, 일요일, 전갈, 까마귀, FCL, Win95/CIH, 스턱스넷 등

부트/파일 바이러스

- 부트 + 파일 바이러스가 합쳐진 형태
- 침입자, 안락사, 에볼라 등

매크로 바이러스

- 감염 대상
  - 오피스 문서 파일
- 문서 파일의 매크로 영역에 침입
- 매크로 실행 시 바이러스 실행
  - 저장 불가
- 라룩스(XM/Laroux)

웜

- 독자적인 실행
- 스스로 전파
- 자기 복사 기능
- 확산 속도 빠름

웜

- 모리스 웜
- 러브레터 웜 / 님다 웜
- 슬래머 웜
- 블래스터 웜

모리스 웜

- 웜의 기본적인 원형
- 버퍼 오버플로의 보안 취약점을 이용
- 여러 번 감염 시 컴퓨터 사용 x

러브레터 웜 / 님다 웜

- 러브레터 웜
  - 메일을 통한 전파 / 첨부 파일 있음
    - .jpg, .zip, .txt, .vbs
- 님다 웜
  - 메일을 통한 전파
  - 첨부 파일을 실행하지 않아도 웜 전파
  - 완전 제거 어려움

슬래머 웜

- SQL Sever 서비스 거부 공격
  - 버퍼 오버플로 약점을 이용한 침입
  - 무제한 복제
  - 무작위 IP 주소에 슬래머 웜 패킷 송신
- 과도한 네트워크 트래픽 발생

블래스터 웜

- 운영체제의 보안 취약점을 이용한 공격
- 메모리 과다 사용으로 운영체제 파손
- 2003년 취약점 패치로 영향력 감소