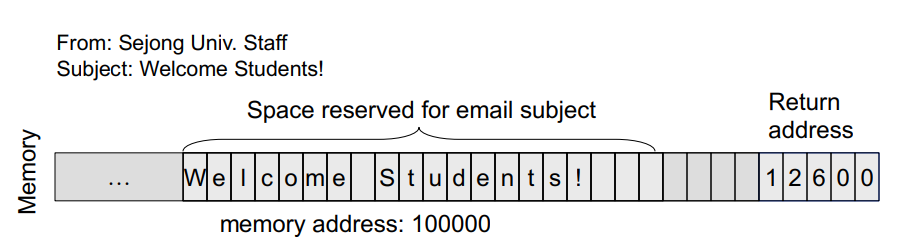
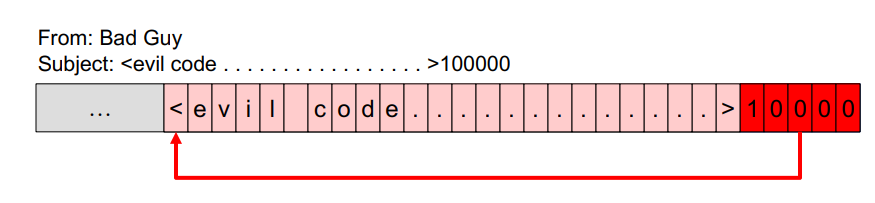
1. MALWARE
   1. 정의
      1. 피해자의 데이터 애플리케이션 또는 운영체제의 기밀성, 무결성. 가용성을 훼손하거나 피해자를 괴롭히거나 방해하려는 목적으로 시스템에 일반적으로 은밀하게 삽입되는 프로그램
2. 뭘웨어 분류
   1. 크게 두 가지로 분류
      1. 전파하는 방법에 따른 분류
      2. 대상에 도달하면 수행하는 작업에 따른 분류
   2. 그 외의 경우
      1. 호스트 프로그램(숙주)이 필요한 뭘웨어 – 바이러스
      2. 독립적이며 자체적인 프로그램이 있는 뭘웨어 – 웜, 트로이 목마, 봇
      3. 복제되지 않는 악성 프로그램(스팸, 스팸 전자 메일)
      4. 복제하는 악성 프로그램(바이러스. 웜)
3. 뭘웨어 종류
   1. 전파 메커니즘
      1. 나중에 다른 시스템으로 확산되는 바이러스에 의한 기존의 컨텐츠의 감염
      2. 웜 또는 Drive-By-Downloads 방식(사용자가 특정 웹사이트에 접속하였을 때 사용자도 모르게 뭘웨어가 다운되는 방식)에 의한 뭘웨어 복제 허용
      3. 트로이 목마를 설치하거나 피싱 공격을 막기위한 보안 메커니즘을 우회하기위해 사용자를 설득하는 사회 공학적 방법
   2. 뭘웨어 대상 시스템 도달 시 수행하는 작업
      1. 시스템 또는 데이터 파일 손상
      2. 좀비PC로 만들기
      3. 시스템/키로그 정보 훔치기
      4. 존재를 시스템에서 숨기기
4. 컴퓨터 바이러스
   1. 컴퓨터 바이러스
      1. 자가 복제
      2. 빠르게 확산
      3. 악의적인 작업이 있을 수도 없을 수도 있다.
   2. 바이러스 감염 증상
      1. 평소보다 컴퓨터 실행 속도가 느림
      2. 컴퓨터 부팅이 더 이상 안됨
      3. 화면이 깜박거릴 수도
      4. PC에서 주기적으로 신호음이 울림
      5. 이유없이 시스템이 충동됨
      6. 파일, 폴더가 사라지는 경우도 있음
      7. DoS
   3. 다른 프로그램 또는 데이터 파일을 감염시켜 확산 -> 자체 복제 프로그램
   4. 감염된 파일을 열도록 사용자를 속여야 함
   5. 바이러스 단계
      1. 휴식기
         1. 바이러스가 유휴 상태
         2. 어떤 사건에 의해 활성화될 것
         3. 모든 바이러스가 이 단계를 갖는 것은 x
      2. 유발 단계
         1. 바이러스가 원래 의도했던 기능을 수행하기 위해 활성화됨
         2. 다양한 시스템 이벤트로 인해 발생할 수 있음
      3. 실행단계
         1. 기능 수행
         2. 무해하거나 유해할 수 있음
      4. 전파 단계
         1. 바이러스가 자신의 복사본을 다른 프로그램이나 디스크의 특정 시스템 영역에 배치
         2. 전파 버전과 동일하지 않을 수 있음
         3. 감염된 각 프로그램에는 이제 자체적으로 전파 단계로 진입하는 바이러스 복제본이 포함
   6. 바이러스 분류
      1. 대상 별 분류
         1. 부트 섹터 감염자
            1. 부팅 디스크 감염 -> 바이러스 포함된 디스크에서 시스템 부팅하면 확산
         2. 파일 감염자
            1. 운영체제나 쉘이 실행가능하다고 간주하는 파일 감염
         3. 매크로 바이러스
            1. 응용 프로그램에서 해석하는? 매크로 로 파일 감염
         4. 다중 바이러스
            1. 다양한 방법으로 파일 감염
      2. 은닉 전략 분류
         1. 암호화된 바이러스
            1. 바이러스의 일부분이 임의 암호화 키를 생성하고 나머지 바이러스를 암호화
         2. 스텔스 바이러스
            1. 안티바이러스 소프트웨어에 의해 탐지되지 않도록 명시적으로 설계된 바이러스 형태
         3. 다형성 바이러스
            1. 감염될 때마다 변이되는 바이러스
         4. 변성 바이러스
            1. 매번 반복할 때마다 완전히 변이하고 다시 쓰며 행동과 외관을 바꿀 수 있는 바이러스
   7. 바이러스 전파 방법
      1. 네트워크 연결 찾기, 네트워크 상의 다른 호스트에 복사
         1. 프로그래밍 기술 大
      2. 호스트 주소록에 있는 모든 사용자에게 메일 보내기
         1. 프로그래밍 기술 小
   8. 전자 메일 전파
      1. 일반적
         1. Microsoft Outlook으로 작업하기 쉽습니다.
         2. 5줄의 코드로 인해 Outlook이 전자 메일을 은밀하게 보낼 수 있습니다.
      2. 다른 바이러스들은 자신의 이메일 엔진을 이용해 퍼짐
   9. 네트워크 전파
      1. 빈도 小 BUT 효과적
   10. 웹사이트 전송
       1. 사용자의 실수에 의존
   11. 바이러스 전파 매게체는 더욱 흔해지고 있음
   12. 바이러스를 방지 방법
       1. 바이러스 스캐너 사용
       2. 의심스러운 파일 열지 X
       3. 보안 경고를 믿지X
5. 컴퓨터 웜
   1. OS의 보안 취약점(예 : 소프트웨어의 버그)을 이용해(exploit) 사람의 개입(intervention) 없이 자체적으로 확산, 이 특성을 제외하고는 바이러스와 같은 자체 복제(self-replicating) 프로그램
   2. 더 많은 시스템 감염시키기 위해 감염시킬 컴퓨터를 찾음
   3. 감염된 시스템 -> 다른 시스템을 공격하기 위한 컨트롤 타워와 같은 역할을 수행하게 됨
   4. 공유 미디어(USB, CD 등)를 통해 확산
   5. Email 웜 : 첨부 파일 및 메신저 파일 전송에 매크로 또는 스크립 코드로 확산하는 웜
   6. 일반적인 형태의 payload가 존재
6. 웜 복제
   1. 전자메일 사용
      1. 자신의 복제본을 다른 시스템에 전자메일로 보냄
      2. 자기 자신을 첨부파일로 전송
   2. 파일 공유
      1. 이동식 저장 장치에서 자체적으로 복사본을 생성, 파일을 바이러스에 감염시킴
   3. 원격 실행 기능
      1. 다른 시스템에서 자기 복제본을 실행함
   4. 원격 파일 엑세스 or 전송
      1. 원격 파일 엑세스 or 전송 서비스를 이용 -> 한 시스템에서 다른 시스템으로 자신 복사
   5. 원격 로그인 기능
      1. 원격 시스템에 로그인 -> 커멘더 실행 -> 다른 시스템으로 복제
7. 모바일 웜
   1. 스마트폰을 대상으로
   2. 블루투스, MMS 이용
   3. 휴대폰 비활성화, 데이터 삭제 등의 피해 발생
   4. 블루투스 통해 다른 전화기에 자기 복제, 자기 연락처의 모든 사람들에게 MMS 파일 전송
8. 해커들이 웜, 바이러스를 사용하는 이유(그냥 웜 바이러스를 이용해서 해킹하는 이유…)
   1. 봇
      1. 바이러스/웜 -> 목표 컴퓨터에 봇 프로그램 설치
      2. 봇 -> 목표를 좀비로 만듦 -> 공격자가 원격으로 조종 가능
      3. 봇 프로그램 -> 백그라운드에서 silently하게 실행, 해커의 지시를 기다림
9. 왜 봇을 만드는 것이 문제인가
   1. DDOS
   2. 스팸 보내기 위해
10. 트로이 목마
    1. 온화한(benign) 프로그램인 것처럼 보이나, 아님
    2. 겉으로 정상적인 프로그램은 밑의 payload를 할 수 있다.
       1. 악성 소프트웨어 설치
       2. 키 로거설치
       3. 백도어를 만듦
    3. 유능한(competent) 프로그래머는 트로이 목마 무언가를 어필하기 위해 만듬
    4. 회사 정책 -> 무단 다운로드 금지시켜야
11. 바이러스 vs 웜 vs 트로이목마 정리
    1. 바이러스
       1. 자신의 복사(propagate)본을 다른 프로그램에 삽입하여 전파하는 악성 프로그램
       2. 한 컴퓨터에서 다른 컴퓨터로 전파되어 이동하면서 감염
    2. 웜
       1. 자가 복제한다는 점에서 바이러스와 유사, 같은 유형의 피해
       2. 바이러스 -> 감염된 파일의 확산이 필요함(사람이 파일을 확산 시켜야함) 웜 -> 단독으로 작동하는 프로그램 -> 사람의 개입없이 전파
    3. 트로이목마
       1. 정상적으로 보이나 억성 소프트웨어
       2. 파일을 감염시켜 확산하지 X, 자체 복제 X
12. 버퍼 오버 플로우
    1. 프로그램 -> 할당된 버퍼를 벗어나더라도 데이터 기록
       1. 버퍼 – 스택, 힙, 글로벌 데이터에 버퍼 있을 수 있다.
    2. 흔한 공격 메커니즘
    3. 원래의 유효한 데이터에 악의적인 데이터 및 코드를 덮어씀 -> 실행
    4. 인접한(adjacent) 메모리 영역에까지 덮어씀
       1. 프로그램 데이터 손상
       2. 악의적으로 관한을 취득할 수 있음
       3. 메모리 엑세스 위반
       4. 공격자가 작성한 코드를 실행시킬 수 있음
    5. 부주의한 프로그래밍 기술, 이미 많이 유포된 버그 등으로 인해 발생
    6. 예
       1. 
       2. 
13. 버퍼오버플로우 방지
    1. 안전한 프로그래밍 언어 사용 (예 : Java)
       1. C언어는?
          1. 많은 보안적 이슈가 존재
    2. 긴 문자열 등으로 블랙 박스 테스트를 해봄
    3. 어떤 소프트웨어를 내부 구조나 작동 원리를 모르는 상태에서 소프트웨어의 동작을 검사하는 방법
    4. 스택을 실행 볼가능(non-executable)으로 설정 -> 코드 실행X
    5. 리턴 주소 암호화, 스택 위치 랜덤화 -> XOR암호화 방식으로
    6. 배열 또는 버퍼 경계 -> 런타임 검사
    7. 다양한 도구 사용
    8. 오버플로우 찾기위해 정적 분석(프로그램 실행없이 소프트웨어 분석)
14. 스파이웨어
    1. 광고 목적으로 웹 서핑 습관 추적, 그에 대한 대가로 기능이나 유틸리티 제공 -> 기만적인(deceptive) 소프트웨어
    2. 악성 소프트웨어인 이유
       1. 짜증남
       2. 네트워크를 집약적(intensive)으로 사용
       3. 사생활(privacy) 침해
       4. 보안상 위험 가능성
    3. 형태
       1. 웹 쿠키
       2. 키로거
    4. 합법적인 사용 예
       1. 아이 컴퓨터 모니터링
       2. 직원 모니터링
    5. 불법적인 예
       1. 배포가 은밀하게(covert) 진행
    6. 스파이웨어 증상 (5 – signs)
       1. 시스템 트레이 아이콘(작업 표시줄 시간 옆에 있는 것들)
       2. 브라우저 추가적인 툴바
       3. 리디렉션된 홈 페이지
       4. 팝업이 많이 뜸
       5. 컴퓨터가 느려짐
15. 뭘웨어 다른 형태
    1. 루트킷
       1. 시스템에 비밀접근 유지를 위해 시스템에 설치된 숨겨진 프로그램
       2. 해킹이 가능한 툴들을 갖추고 있음
          1. 트래픽, 키 로깅
          2. 백도어 생성
          3. 툴이 감지되지 않도록 함
          4. 같은 네트워크 상의 다른 컴퓨터를 공격
16. 악의적인 웹 기반 코드
    1. 웹 기반 모바일 코드
       1. 모든 OS에서 가벼운 코드들
       2. 웹상에서 빠르게 퍼짐
17. 바이러스, 스파이웨어 제거
    1. 안티바이러스 소프트웨어 작동 방식
       1. 버이러스 signature 검색
          1. Signature을 최신 상태로 유지
       2. 실행파일(executable)의 동작을 감시
          1. 주소록 접근 시도
          2. 레지스트리 설정 변경 시도