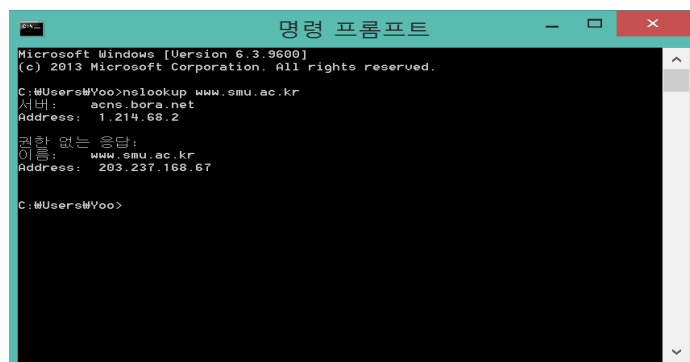


디지털보안학

[5주차. 인터넷보안3]

바이러스 감염 재현

- 가짜 사이트 준비하기
 - 예시로 <http://www.smu.ac.kr> 사용
- 가짜 사이트의 IP 주소 알아내기
 - 명령어 프롬프트에서 nslookup 명령 실행



```
명령 프롬프트
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Yoo>nslookup www.smu.ac.kr
서버:      acns.bora.net
Address:  1.214.68.2

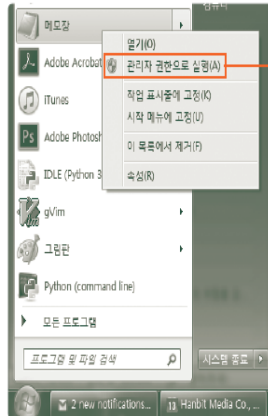
권한 없는 응답:
이름:      www.smu.ac.kr
Address:  203.237.168.67

C:\Users\Yoo>
```

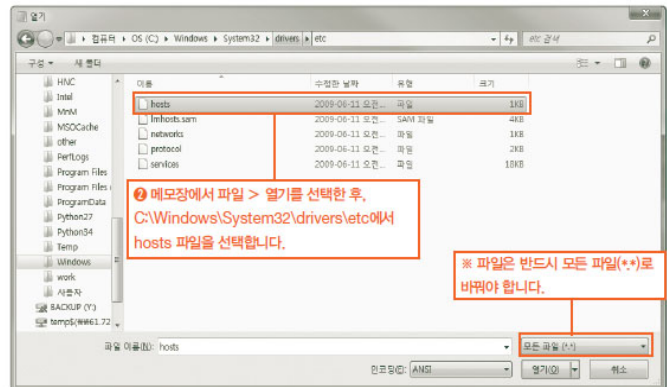
3. 바이러스 감염 재현하기

– hosts 파일 수정하기

- ✓ 앞에서 가정한 진짜 사이트의 호스트명에 가짜 사이트의 IP 주소 할당하는 설정을 추가

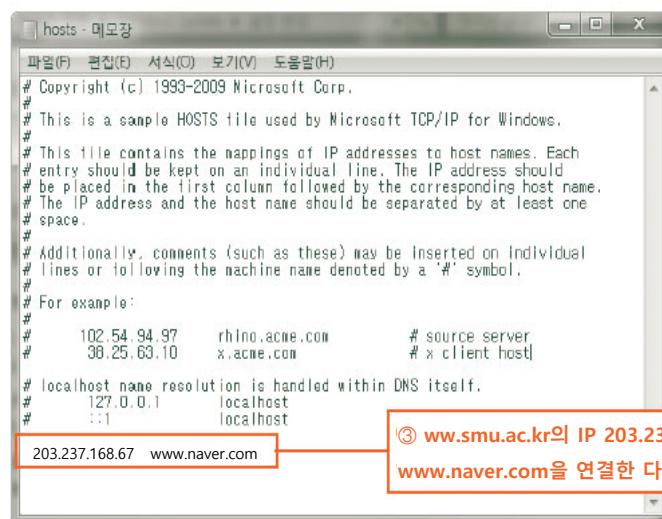


1 시작 버튼에서 메모장을 찾아
오른쪽 클릭을 한 다음에 관리자
권한으로 실행(A)을 눌러 엽니다.



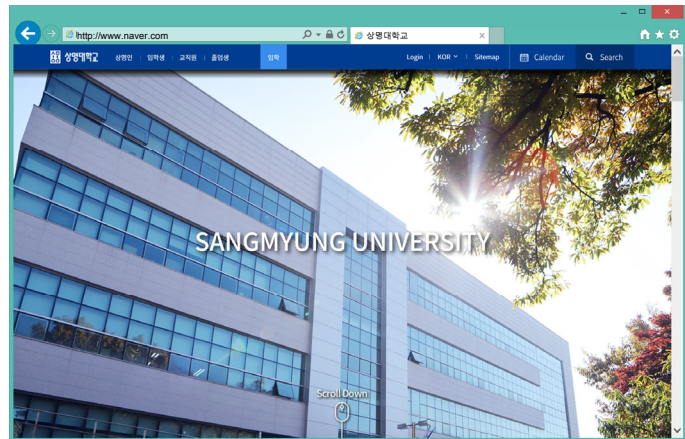
* 파일은 반드시 모든 파일(*)로
바꿔야 합니다.

3. 바이러스 감염 재현하기



3. 바이러스 감염 재현하기

- 웹 브라우저로 열어보기
 - ✓ 진짜 사이트의 URL 입력하면 가짜 사이트 열림
 - ✓ 명령어 프롬프트에서 ping 명령 실행 시에도 같은 결과



- 원래대로 되돌리기
 - ✓ hosts 파일에 추가했던 부분을 삭제

바이러스 감염 재현

- 바이러스란 무엇인가?
 - 바이러스
 - ✓ 컴퓨터에 어떤 형태로든 피해를 입히는 프로그램

바이러스의 정의

제3자의 프로그램이나 데이터베이스에 대해 의도적으로 어떤 피해를 입히도록 작성된 프로그램으로, 다음과 같은 기능을 하나 이상 보유하는 것을 말한다.

자기전염 기능	바이러스 자체의 기능을 이용해 다른 프로그램에 스스로를 복제하거나 혹은 시스템의 기능을 이용해 스스로를 시스템에 복제함으로써 다른 시스템에 전염시키는 기능
잠복기능	바이러스가 발병을 하기 위한 특정 시간, 특정 기간, 처리 횟수 등의 조건을 기억하여, 발병하기 전까지는 증상을 드러내지 않는 기능
발병기능	프로그램, 데이터 등의 파일을 파손하거나 설계자가 의도치 않은 동작을 하게 하는 등의 기능

■ 바이러스의 종류

– 다른 파일에 감염되어 실행되는 타입

- ✓ 매크로나 스크립트를 사용
- ✓ 피해 입히도록 설계된 파일을 배포하여 이용자가 이를 여는 순간 실행되도록 함
- ✓ 랜섬웨어와 같이 PC 내의 파일을 마음대로 암호화한 후, 복구하는 데 금전을 요구하는 경우도 있음

– 독립적으로 실행되는 타입

- ✓ 다른 소프트웨어와 같이 애플리케이션 형태로 배포
- ✓ 악의적인 처리를 배후에서 실행하여 정상적인 소프트웨어로 보이기 쉬움

■ 바이러스의 감염 경로

– 스팸메일

- ✓ 수신자의 뜻을 무시하고 일방적으로 보내지는 메일
- ✓ 여러 경로로 수집한 메일주소나 무작위로 작성된 주소로 일괄적 메일 전송

– 스팸메일 대책

✓ 블랙리스트

- 특정 서버나 메일 주소를 거부
- 정상 사용자의 메일도 스팸으로 자동 등록될 수 있음
- RBL (Real time Blocking List) 정책

✓ 분류

- 메일 서버에서 수상하다고 판단된 메일에 분류 태그 붙여서 이용자에게 보내주기도 함
- 자동 분류 기능 활용하여 손쉽게 구별 가능

✓ OP25B와 발송 도메인 인증 (Outbound Port 25 Blocking)

- 외부의 메일 서버 악용하여 발송하는 것을 방지하기 위해 이용
- 외부의 발송자가 다른 메일 서버를 사용하지 못하도록 인터넷 서비스 제공 사업자가 통신을 차단

■ 웹사이트에서 감염되는 경우

- 파밍 (pharming)

- ✓ 진짜와 똑같이 보이는 사이트 사용
- ✓ 사전에 DNS 설정 바꿔두어, 제대로 된 URL 입력하더라도 가짜 사이트로 유도
- ✓ 가짜 사이트로 유도된 사실을 알아채기 어려움



파밍

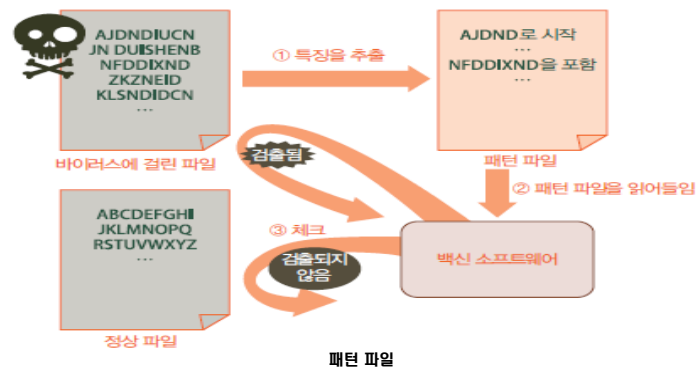
– 드라이브 바이 다운로드

- ✓ 이용자가 버튼 누르지 않더라도 몰래 다운로드 시키는 방식
- ✓ os나 각종 소프트웨어의 취약성 이용

바이러스 감염의 예방과 확대방지

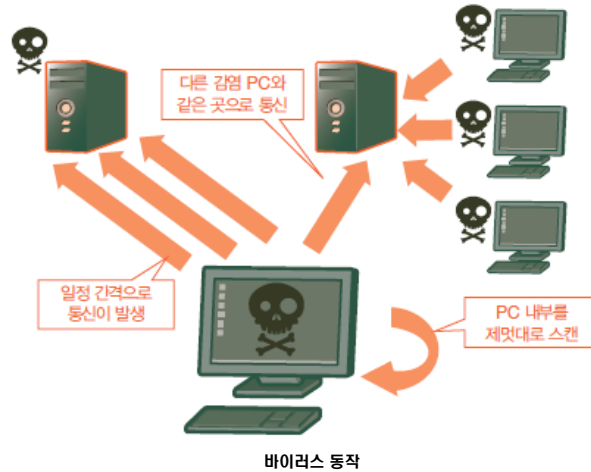
■ 바이러스 감염의 예방과 확대방지

- 백신 소프트웨어의 동작
- 패턴 파일
 - ✓ 최신 바이러스에 관한 특징 등이 적혀있어, 이것에 해당하는 파일 검출 시 경고하거나 삭제
 - ✓ 바이러스 개발에 따라 계속된 업데이트



■ 행동 검출

- 바이러스처럼 행동하는 프로그램을 검출하여 그 실행을 정지



■ 취약점 완화 소프트웨어

- 제로데이 취약점 : 어떤 취약점이 새로이 발견되었으나 거기에 대처할 수정 프로그램이 아직 제공되지 않은 상태
- 만능은 아니나 이용해볼 가치 있음
- 마이크로소프트 EMET (Enhanced Mitigation Experience Toolkit)

■ 허니팟

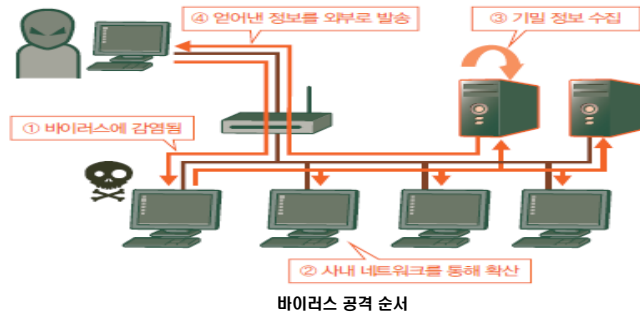
- 미끼로 설치되어 바이러스나 무단침입의 공격이 쉽도록 한 가짜 시스템
- 공격 및 바이러스를 수집하여 패턴 파일 작성에 도움

■ 샌드박스

- 바이러스 여부를 판단하기 위해 준비된 가상환경



■ 입구대책과 출구대책



– 입구대책

- ✓ 바이러스 침입을 막거나 침입하더라도 감염을 방지하는 것
- ✓ 네트워크 분리하여 피해 전파 범위를 한정
- ✓ 관리자 권한을 최소한으로 한정하고 파일이나 폴더의 공유를 제한

– 출구대책

- ✓ 감염된 PC에서 외부로 기밀정보를 보내지 못하도록 하거나, 보내더라도 악영향이 없도록 하는 접근방식
- ✓ 외부로 향하는 발송 데이터 체크, 사내 데이터 암호화, 부정통신 차단 등

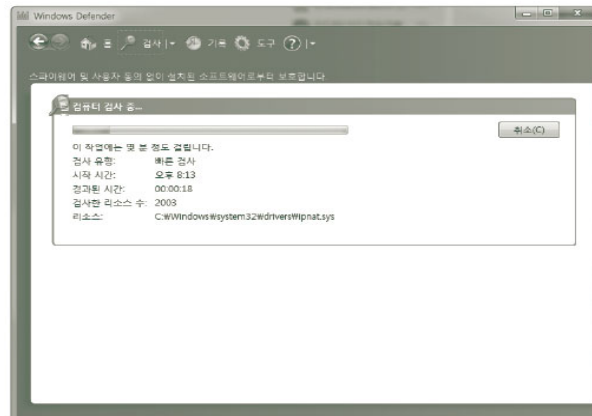
– 정보 유출 시 대응방안

- ✓ 피해 확대 방지
- ✓ 정확한 정보 파악
- ✓ 공표
- ✓ 재발 방지책 실시

스파이웨어 조사

■ Windows Defender 사용

- 윈도우 8부터 기본적으로 설치되어 있음
- 시작 메뉴 검색란에 'Defender' 입력하여 선택해 스캔 실행



■ 스파이웨어란?

- 컴퓨터 이용자 모르게 또는 동의 없이 설치되어 컴퓨터 사용에 불편을 끼치거나 정보를 가로채는 악성 프로그램
- 개인정보를 외부로 보내거나 광고를 표시해 접근 이력 등을 수집
- 무료 게임이나 유틸리티 등에 첨부되어 컴퓨터에 설치됨

■ 스파이웨어의 종류

- 마음대로 개인정보 수집하여 빼돌리는 타입
 - ✓ 컴퓨터의 유저명이나 사이트 방문 기록 등을 인터넷 경유해 자동적으로 발송
- 제멋대로 광고를 표시하는 타입
 - ✓ 무료로 소프트웨어 제공하고 광고 수입을 얻는 등의 형식
 - ✓ 이용자에게 충분한 정보를 제공하지 않거나, 부적절한 광고 표시되거나, 개인정보를 마음대로 빼돌릴 수 있음

■ 스파이웨어 대책

– Windows Defender

- ✓ 스파이웨어 대처용 소프트웨어
- ✓ 실시간 보호 : 스파이웨어 설치되려고 할 때 경고를 표시
- ✓ 스캔 옵션 : 컴퓨터에 설치된 스파이웨어가 있는지 찾아냄