

2022학년도 1학기

5주차. 악성코드 II
- 간단한 악성코드 제작 -

김지연 교수

jyk@daegu.ac.kr



강의 내용

주차	강의 내용	평가
1	강의 소개 - 강의 목표, 강의 내용, 평가 방법 등	-
2	정보보호 역사, 3대 기본 요소	-
3	암호학의 이해 I (고전암호) 암호학의 이해 II (대칭키 암호, 비대칭키 암호, 해쉬)	과제 5%
4	악성코드 I (바이러스, 웜, 트로이목마, PUP)	-
5	악성코드 II (간단한 악성코드 제작)	과제 5%
6	시스템 보안 I (시스템의 이해, 계정 관리, 세션관리, 접근 제어, 권한 관리, 로그관리, 취약점 관리 등)	과제 5%
7	네트워크 보안 I (스니핑, 스푸핑, 세션 하이재킹 공격) 네트워크 보안 II (서비스 거부공격, 분산서비스 거부공격)	-
8	중간고사	30%
9	네트워크 패킷 모니터링 실습	과제 5%
10	모의 침투 인프라 구축 (칼리리눅스 설치) 모의침투 I (시스템 정보수집 공격)	-
11	모의침투 II (서비스 거부 공격 실습) 모의침투 III (SSH 로그인 공격)	-
12	모의침투 IV (HTTP 로그인 공격) 모의침투 V (악성코드 페이로드 제작을 통한 공격)	-
13	나만의 모의침투 프로젝트 I	-
14	나만의 모의침투 프로젝트 II	-
15	기말고사(나만의 모의침투 프로젝트)	20%

악성코드 감염 증상

대분류	소분류	설명
시스템	시스템 설정 정보 변경	레지스트리 키 값을 변경하여 시스템 정보를 변경한다.
	FAT 파괴	시스템의 파일 시스템을 파괴한다.
	CMOS 변경	CMOS 내용을 변경하여 부팅 시 오류를 발생시킨다.
	CMOS 정보 파괴	CMOS의 일부를 파괴한다.
	기본 메모리 감소	시스템의 기본 메모리를 줄인다.
	시스템 속도 저하	시스템의 속도를 저하시킨다.
	프로그램 자동 실행	레지스트리 값을 변경하여 시스템 부팅 시 특정 프로그램을 자동으로 실행한다.
	프로세스 종료	특정 프로세스를 강제로 종료시킨다.
	시스템 재부팅	시스템을 재부팅시킨다.
네트워크	메일 발송	특정 사용자에게 메일을 발송한다.
	정보 유출	사용자의 정보를 네트워크를 통해 공격자의 컴퓨터로 전송한다.
	네트워크 속도 저하	감염된 컴퓨터가 속한 네트워크가 느려진다.
	메시지 전송	네트워크를 통해 다른 컴퓨터로 메시지를 전달한다.
	특정 포트 오픈	특정 백도어 포트를 연다.

악성코드 감염 증상

대분류	소분류	설명
하드디스크	하드디스크 포맷	하드디스크를 포맷한다.
	부트 섹터 파괴	하드디스크의 특정 부분을 파괴한다.
파일	파일 생성	특정 파일(주로 백도어 파일)을 생성한다.
	파일 삭제	특정 파일이나 디렉터리를 삭제한다.
	파일 감염	특정 파일을 바이러스에 감염시킨다.
	파일 손상	특정 파일에 바이러스가 겹쳐 쓰기 형태로 감염되어 손상된다.
	파일 암호화	파일이 임의로 암호화되어 접근할 수 없다.
특이점	이상 화면 출력	출력 화면에 특정 내용이 나타난다.
	특정 음 발생	컴퓨터에서 특정 음이 발생한다.
	메시지 상자 출력	출력 화면에 특정 메시지 상자가 나타난다.
	증상 없음	특이한 증상이 없다.

I. 시스템 재부팅

Windows 시스템 재부팅

```
#include<stdio.h>

int main()
{
    system("C:\\WINDOWS\\System32\\shutdown.exe /r");

    return 0;
}
```

II. 파일 생성

무한 파일 생성 (예시는 50개 파일 생성)

```
#include <stdio.h>
#include <string.h>

int main()
{
    FILE *file; // 파일 포인터

    char fName[30]; // 최종파일명 21900000_1.txt ~ 21900000_50.txt

    char ID[15] = "21900000_"; // 각자 학번으로 바꾸기

    int cnt = 1; // 몇 번째 파일인지 숫자 카운트 1 ~ 50
    char strCnt[3]; // cnt 값을 문자열로 저장할 변수

    while (cnt <= 50) // 반복횟수 지정
    {
        strcpy(fName, ID);

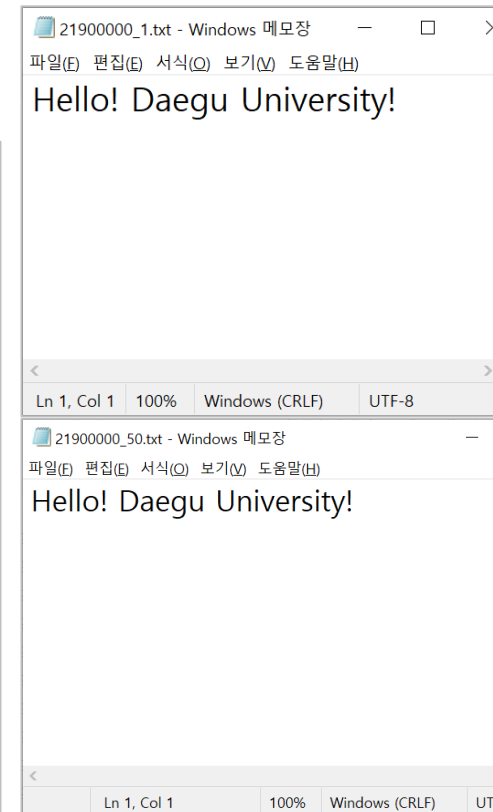
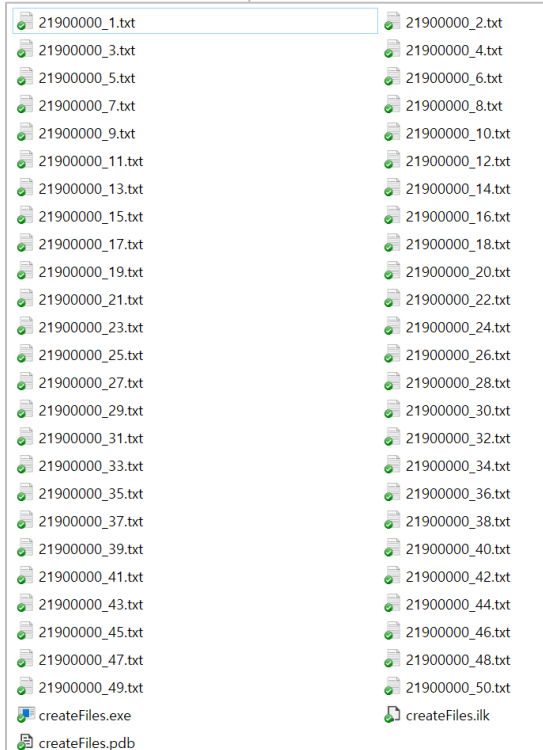
        sprintf(strCnt, "%d", cnt);
        strcat(fName, strCnt);

        strcat(fName, ".txt");

        file = fopen(fName, "w");
        fputs("Hello! Daegu University!", file);

        fclose(file);
        cnt++;
    }

    return 0;
}
```

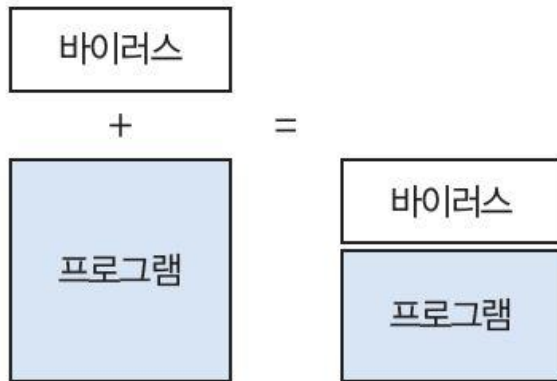


Ⅲ. 악성코드 감염으로 인한 파일손상

1세대 원시형 바이러스

2) 파일 바이러스 (1/2)

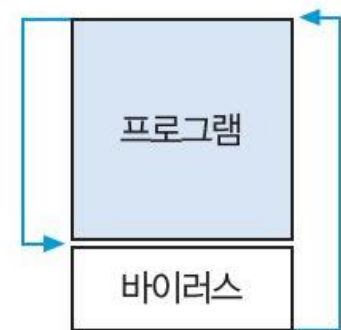
- 파일을 직접 감염시켜 바이러스 코드를 실행
- 감염 위치에 따라 3개의 경우가 존재
 - a) 파일 바이러스는 프로그램을 덮어쓰는 경우
 - b) 프로그램 앞부분에 실행 코드를 붙이는 경우
 - c) 프로그램 뒷부분에 바이러스 코드를 붙이는 경우



(a) 덮어쓰기형



(b) 바이러스가 프로그램
앞에 위치하는 경우



(c) 바이러스가 프로그램
뒤에 위치하는 경우

1세대 원시형 바이러스

2) 파일 바이러스 (2/2)

c) 프로그램 뒷부분에 바이러스 코드를 붙이는 경우

- 백신의 바이러스 스캔으로부터 자신의 존재를 숨기기 위함
- 프로그램 뒷부분에 위치한 바이러스가 실행되는 형태



실행파일 문자열 변경

```
#include<stdio.h>
```

```
int main()
{
    printf("Hello! Daegu University!");

    getchar();
    return 0;
}
```

000064E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000064F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00006500	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00006510	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00006520	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00006530	48 65 6C 6C 6F 21 20 32	31 39 30 30 30 30 30 21	Hello! 21900000!
00006540	21 21 21 21 21 21 21 21	00 00 00 00 00 00 00 00	!!!!!!!.
00006550	10 7C 41 00 20 7D 41 00	78 7E 41 00 9C 7E 41 00	. A. }A.x~A.£~A.
00006560	DC 7E 41 00 10 7F 41 00	01 00 00 00 00 00 00 00	~A..△A.....
00006570	01 00 00 00 01 00 00 00	01 00 00 00 01 00 00 00
00006580	53 74 61 63 6B 20 61 72	6F 75 6E 64 20 74 68 65	Stack around the
00006590	20 76 61 72 69 61 62 6C	65 20 27 00 27 20 77 61	variable '.' wa

선택 D:\Dropbox\Lectures\DUW2022-1\정보보호실습\5주차_간

Hello! Daegu University!

선택 D:\Dropbox\Lectures\DUW2022-1\정보보호실습\5주차_간

Hello! 21900000!!!!!!!!!!

Crack 버전 프로그램

```
#include <stdio.h>

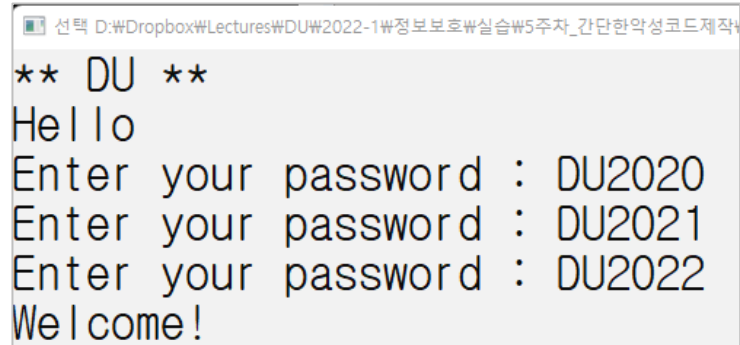
int main()
{
    char password[100];

    puts("** DU **");
    puts("Hello");

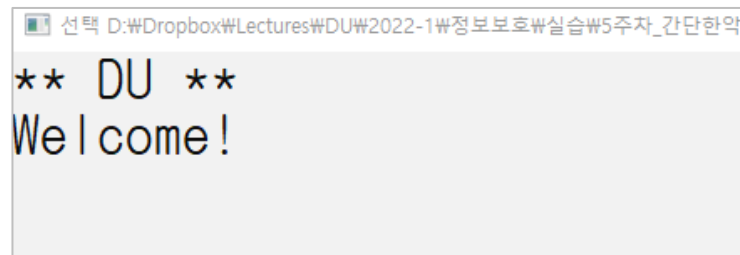
    while (1)
    {
        printf("Enter your password : ");
        scanf("%s", password);

        if (strcmp(password, "DU2022") == 0)
            break;
    }

    puts("Welcome!");
    getchar();
    getchar();
}
```



```
선택 D:\Dropbox\Lectures\DU\2022-1\정정보호실습5주차_간단한악성코드제작
** DU **
Hello
Enter your password : DU2020
Enter your password : DU2021
Enter your password : DU2022
Welcome!
```



```
선택 D:\Dropbox\Lectures\DU\2022-1\정정보호실습5주차_간단한악성코드제작
** DU **
Welcome!
```