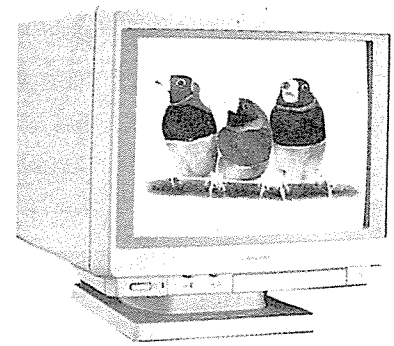
컴퓨터 바이러스
(Computer Virus)



金 道 鎭
〈나래이동통신 상무이사/본지 편집위원〉

"야! 이 컴퓨터 바이러스에 걸렸네… 너 이 디스켓 바이러스 검사한거야?" "내일은 3월6일로 미켈란젤로 탄생일입니다.그러므로 미켈란젤로 바이러스에 감염될 수 있으므로, 각 컴퓨터 사용자들은 즉시 날짜를 하루 더 연기하여…"우리는 주위에서 이런 이야기를 많이 듣는다. 컴퓨터에 익숙한 사람도 이런 알쏭달쏭한 이야기를 잘 이해하지 못하고 넘어가는 수가 있다. 도대체 바이러스가 뭐야? 또 컴맹(컴퓨터문맹)에 걸린 어느 분은 이 디스켓이 바이러스 걸린 것이라고 하니까 감염될까봐 만지지도 못하고 소독약으로 닦아내는 등 웃지 못할 이야기도 있다. 그러면 바이러스란 과연 무엇인가?

바이러스 개념 및 특징

간단히 이야기해서 바이러스는 일종의 프로그램이다. 여러분들이 많이 쓰는 워드프로세서나 스프레드시트처럼 아니, 더 쉽게 게임프로그램처럼 한개의 프로그램이다. 그러나 이 바이러스 프로그램은 몇 가지 특징을 가진 프로그램인 것이다. 무슨 특징이냐 하면…

첫째, 이 프로그램은 보이지 않는다. 즉 도스상태에서 파일상태로 보이지 않고 다른 프로그램 속에 숨어 있는다. 이것을 소위 트로이의 목마 속성이라고 한다. 둘째, 이렇게 다른 프로그램 속에 숨어서 좋은 일을 하는 것이 아니라, 그 프로그램을 혼란시키거나 파괴하는 나쁜 일을 수행한다는 것이다. 우리는 이런 특징을 가진 프로그램을 소위 컴퓨터 바이러스라 말하는 것이다. 누가 바이러스라 명명했는지 참 뛰어난 명칭이다. 정말 인간에게 있어서 바이러스라는 존재와 너무 흡사하다. 나타나지 않고 사람 몸속에 숨어서 병을 일으키고(심하면 죽기도 하지 않은가?) 사람을 괴롭히는 그런 존재, 컴퓨터에 있어서도 똑같은 효과를 가져온다.

이와 같이 컴퓨터가 바이러스에 걸리면 그 안의 프로그램이 다 파괴되고, 심하면 컴퓨터 자체를 전부 파괴하는 수가 있다. 많은 밤을 새워 작성한 일과 수백만원 들여 구입한(아직 월부금도 다 붓지 못하고 있는) 컴퓨터가 모두 무용지물이 되어 버린다니…그러니 우리에게 컴퓨터 바이러스란 두려운 존재인 것이다. 그러면 바이러스는 도대체 어떻게 생겨났을까? 여기에는 대체로 몇 가지 설이 있으나, 아직 완전히 확인되지는 않고 있다. 보통 아래와 같은 원인들이 혼합되어 발생한 것이 아닐까 추정할 뿐이다.

첫째, 가장 널리 알려진 발생설은 프로그램(소프트웨어) 지적소유권 보호 차원에서 일어났다는 것이다. 자… 당신이 한 5년을 밥도 못 먹고, 잠도 못 자고, 어두운 방안에서 오직 컴퓨터만을 벗으로 삼아 컴퓨터가 모든 계산을 대신해주는 획기적인 프로그램을 짜기 시작했다. 그리고… 드디어 5년만에 눈물겹게 그 프로그램을 완성하여 두손에 5년간의 피와 땀과 눈물이 담긴 두장의 결정체를 들고 있다. 그 두장 안에 당신이 만든 프로그램이 모두 들어 있는 것이다.이제 당신은 부자가 된 것이다. 이 프로그램 하나에 백만원씩만 받아도, 사람들이 줄을 서서 기다릴 것이며, 그 프로그램의 효용성에 놀랄 것이다. 점점 유명해질 것이고 모든 명예와 돈과 희망이 당신에게 물결치며 다가오는 것을 느낄 수 있을 것이다. 아아 당신은 드디어 성공을 한 것이다.

드디어 디스켓을 팔기 시작했다. 그러나, 당신은 결정적으로 실수를 한 것이다. 그 프로그램의 효용성은 천만금을 주고도 못 살 획기적인 것이지만, 컴퓨터에는 복사(COPY) 기능이 있다는 것을 잠시 잊었던 것이다. 당신이 온갖 노력을 다하여 만든 그 프로그램은 COPY라는 컴퓨터 명령어로 간단히 복사해서 사용할 수 있는 것이다. 사람들의 양심은 별로 아름답지 못하였다. 한 인간의 영혼이 깃든 그 프로그램을 아무런 대가도 없이 간단히 복사해서 쓰다니. 당신은 복수를 결심하게 된다. 그래서 이 프로그램을 무단으로 복사해 가는 사람은 조금 사용하다 보면 무조건 하드디스크가 다 망가지게 프로그램을 만들어 그 프로그램안에 숨겨놓고 자신만이 그 푸는 비밀을 알고 있었다. 그러나 사람들은 그것도 모르고 여전히 야! 이 프로그램 좋다. 좋다… 또 복사… 그래서 바이러스가 등장하여 온 천지에 난무하게 된 것이다.

둘째, 이렇게 이상한 프로그램이 난무하는 것을 본 사람들 중에 꼭 못된 사람이 있다. 남이 안되는 것을 좋아하는 사람들… 그래서 고의로 그런 프로그램을 만들어 세상에 배포해 놓고 혼자서 기뻐하는 사람들이 등장하게 된 것이다. 이런 사람을 흔히 컴퓨터 해커라고 한다. 그래서 또 한번 바이러스는 다양한 얼굴로 세상에 춤을 추게 된다.

셋째, 순전히 컴퓨터 오류로 발생했다는 설이다. 이것은 인간이 완전하지 못하므로 프로그램을 짤 때, 우연발생적으로 생겨나 세상에 퍼지기 시작했다는 것이다.

그러나 이 세가지 설 중에서 보통 첫번째 설이 가장 유력하다. 왜냐하면 컴퓨터 바이러스는 컴퓨터 전문 프로그래머가 아니면 짜기 힘든 고도의 기술이기 때문이다.

바이러스의 종류

이제는 세상에 나돌아다니는 대표적인 바이러스에는 어떤 종류가 있는지 한번 알아보기로 하자.

1) 브레인 바이러스(Brain Virus) : 이 바이러스에 걸리면, 디스크 목록을 보려고 dir을 치면 목록이 나오지 않고 CBrain 이라는 것이 나온다.

2) LBC 바이러스 : 이 바이러스는 그 첫글자를 따서 이병철 바이러스라고 하는데 말 그대로 부자 바이러스다. 즉 싼 플로피디스크는 손상이 없고 비싼 하드디스크만 파괴하는 바이러스이다. 이 바이러스는 순수 토종인 듯하다. 그래서 KOREA 바이러스라고도 한다.

3) 예루살렘 바이러스 : 이스라엘 바이러스라고도 한다. 평소에는 아무 이상이 없다. 그러나 악마가 날뛰는 13일의 금요일만 되면 온갖 활개를 치며 디스크를 몽땅 파괴해버린다. 이런 종류의 바이러스를 날짜 바이러스라고도 하는데 유사한 것으로 미켈란젤로 바이러스가 있다.

4) 미켈란젤로 바이러스 : 마찬가지다. 미켈란젤로를 광적으로 좋아하는 어느 해커가 만들었는지 미켈란젤로의 생일인 3월6일만 되면 그 날을 기념하기 위해 프로그램을 무자비하게 파괴한다. 날짜 바이러스는 DATE라는 도스 명령어로 간단히 해결할 수 있다. 즉 다음날이 3월6일이면 3월7일로 입력해놓고 그 다음다음날 다시 복귀시키면 얼씬도 못한다.

5) 느림보 바이러스 : 이 바이러스에 걸리면 AT486도 XT 속도가 된다. 아무 소용이 없다. 무지무지하게 속도가 느려진다. Slow 바이러스, 거북이 바이러스라고도 한다.

6) D2 (디투)바이러스 : 이것은 가장 악성 바이러스다. 도대체 부팅이 안된다. 이 바이러스의 원명은 dir2 바이러스다. 부팅이 안되니 난감하다. 그래서 꼭 시스템 디스켓이 있어야 한다. 그래야 하드디스크로 들어가 치료할 수 있다.

이밖에도 바이러스 종류는 수없이 많다. 컴퓨터를 한참 사용하고 있는데 느닷없이 CHRISTMAS GREETING이라는 인사가 뜨는 크리스마스 바이러스, 일요일만 되면 "오늘은 일요일… 당신은 쉬지 않고 무엇을 하고 있습니까" 라는 문구가 뜨는 일요일 바이러스, 생각지도 않은 음악이 나오는 음악 바이러스, 시도 때도 없이 쿠키(COOKIE)를 달라고 하는 쿠키 바이러스(이 바이러스는 쿠키를 달라고 하여 쿠키를 주지 않으면 : COOKIE라는 글자를 치지 않으면 전혀 프로그램이 작동이 안된다) 등 여러 종류의 바이러스가 있다.

바이러스의 감염경로

그러면 바이러스는 어떻게 컴퓨터에 감염되는 것일까. 최초에 어느 컴퓨터(하드디스크)에 바이러스가 있었다고 하자. 이 바이러스는 앞에서 밝혔듯이 프로그램에 숨어서 보이지 않는다. 그러니 겉으로 보아서는 확인할 수 없다. 그런데 당신의 친구가 게임을 하나 복사해 달라고 디스켓 한장을 들고

왔다. 그것은 별로 어려운 일이 아니다. 당신은 당신의 컴퓨터 드라이브에 그 디스켓을 넣고 당신이 애용하는 게임 몇개를 복사해주었다. 당신의 친구는 그 게임이 든 디스켓을 자신의 컴퓨터 하드디스크에 복사를 한다. 그리고 열심히 게임을 한다. 이거 아주 재미있군...이렇게 바이러스는 전파된다. 또한 바이러스는 처음에는 한 프로그램에만 숨어 있다가 하드디스크로 옮겨지면 그 디스크 전체에 감염된다. 그러니 이제는 감염된 그 디스크에 아무 프로그램이나 복사를 해도 바이러스 감염이 〔확실히〕 되는 것이다.

또한 LAN으로 연결된 전송선을 타고도 유유히 전파된다. 바이러스는 아주 생명력이 강해 아무리 멀리 떨어진 컴퓨터 사이라도 조그마한 전송선만 있다면 쉽게 감염된다.

바이러스 백신

자 이런 바이러스가 난무하는 세상에서 우리는 어떻게 그들을 대비하고 처치할까. 우리나라의 안철수씨가 이런 바이러스를 일격에 죽이는 통쾌한 바이러스 백신(VACCINE) 프로그램을 개발하였다. 바로 그 유명한 V3 프로그램이다.

이 프로그램은 첫째, 바이러스를 잡아서 (V1), 확인한 후 (V2), 잡아죽이는(V3) 확실한 절차를 거쳐서 당신의 컴퓨터에서 완전히 바이러스를 죽이는(없애는) 프로그램이다.

◈ 백신의 원리 - 바이러스란 앞에서 밝혔듯이 다른 프로그램속에 숨어 있는 한개의 악성 프로그램이다. 이것을 그 프로그램을 구성하고 있는 파일 하나하나 검색하면서 그 파일이 정상적으로 이루어지고 작동되는지를 검사한다. 만일 그렇지 못하다면 그 파일은 바이러스에 감염된 것이다. 이렇게 바이러스를 찾아낸다. 또한 그 파일을 찾아내었다면 그 악성 프로그램을 정상적으로 돌리는(푸는) 작업을 해준다. 심하게 꼬여 있는 끈의 매듭을 찾아서 풀어주는 작업을 하는 것이다. 그러니까 백신 프그램은 악성 프로그램을 찾아서 풀어주는 프로그램이라 할 수 있다.

◈ 백신의 작동방법 - 보통 백신은 V3 파일로 이루어져 있다. 이것을 실행시키기만 하면 디스크 안의 모든 파일을 검사하여 치유해준다. 간단하다. 또한 백신 V3 프로그램중에는 V3-RES라는 프로그램이 있는데, 이것은 컴퓨터 램안에 상주하면서 바이러스를 체크, 사살하는 프로그램이다. 이것을 설치해놓으면 항시 체크할 수 있어서 좋기는 한데 기억용량을 잡아먹는다는 단점이 있다. 보통 AUTOEXEC.BAT 파일에 작성해 놓으면 편하다. 그러나 이 프로그램도 단점은 있다. 아주 악성 바이러스인 경우에는 파일을 지우는 수밖에 없다는 것이다. 만일 프로그램 사용법을 잘 모르겠거든 V3.DOC 파일을 읽어보라. 그 안에 당신이 원하는 모든 정보가 다 들어있을테니까.

이 프로그램으로 치유가 안될 때는 미국의 NORTON이 발명한 NDD(Norton Disk Doctor)를 사용하는 수밖에 없다. 이 프로그램은 디스크 전체의 용량이나 메모리, 정보 등을 종합적으로 체크해주며 치유해준다.

바이러스 예방방법

가장 좋은 것은 수시로 바이러스 체크를 하는 것이다. 특히 다른 곳에서 가져온 디스켓을 드라이브에 넣고 작동시킬 때는 작동하기 전에 필히 바이러스 체크를 해야한다.

또 다른 사람이 당신의 컴퓨터를 쓰다 감염되는 수도 있을테니 자신의 컴퓨터는 될수록 자신이 사용하는 것이 좋다. 패스워드를 걸어놓고 사용하고, 부득이한 경우 바이러스 검사를 꼭 부탁하자. 그리고 피치못해 바이러스에 감염되었을 때를 대비하여 수시로 중요한 데이터는 플로피 디스켓에 백업(Backup)을 받아두는 작업을 해 두어야 한다.

바이러스 감염시는 간단히 두단계 작업만 해주면 된다.

1) V3로 체크를 한 후,

2) NDD로 한번 시행해주면 디스크 내부를 체크해가며 전체적으로 거의 완전히 치유해준다. 그러나 NDD는 잘못 사용하면 하드디스크 전체가 감염되거나 파괴될 수 있으니 꼭 V3를 체크한 후 사용하는 것이 좋다.

또한 부팅이 안될 때를 대비하여 플로피 디스켓 한장을 깨끗이 시스템 포맷하여 쓰기방지 테이프를 붙여놓자.

자 이상으로 바이러스에 대해 대충 알아보았다. 그러나 바이러스는 아마 컴퓨터가 있는 한 영원할 것이다. 아무리 좋은 프로그램을 만들어도 말이다. 우리가 이 바이러스를 완전히 퇴치하는 방법은 아름다운 마음을 가지고 순수하고 사랑스러운 마음으로 서로를 대하고, 컴퓨터를 이해하는 방법이 가장 중요한 일일 것이다. ST