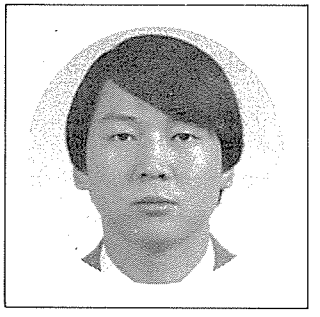
컴퓨터바이러스의 종류와 피해현황

감염의 大型·多樣化추세 뚜렷



안 철 수
〈檀國大醫大교수〉

컴퓨터 바이러스

컴퓨터 바이러스(Computer Virus)라는 말이 신문이나 TV 등의 각종 매스컴을 통하여 널리 알려지면서 여러가지 잘못된 개념들이 일반인들과 컴퓨터 사용자들 사이에서 통용되는 것 같다. 이렇게 된데는 여러가지 원인이 있을 수 있겠지만 가장 큰 이유중의 하나는 '바이러스'라는 명칭에서 비롯되는 것 같다.

컴퓨터 바이러스란 컴퓨터를 다루는 사용자나 컴퓨터 자체에 감염되는 바이러스가 아니라, 컴퓨터에서 수행되는 프로그램(Program)이다. 하지만 이 프로그램은 다른 프로그램들과 달리 자기 자신을 다른 곳에 복사시키는 명령어들을 가지고 있다. 바이러스라는 이름이 붙은 이유는 실제의 바이러스가 자기 자신을 복제하는 유전인자를 가지고 있는 것처럼 컴퓨터 바이러스도 자기 자신을 복사하는 명령어들을 가지고 있기 때문이다.

컴퓨터 바이러스는 아주 최근에 문제가 되기 시작한 분야이기 때문에, 컴퓨터 보안 전문가들 사이에서 조차 컴퓨터 바이러스에 대한 정확한 정의가 내려지지 않은 상태이다. 어떤 사람들은 컴퓨터에 해로운 일을 하는 프로그램을 모두 총칭해서 컴퓨터 바이러스라는 용어를 사용하기도 하며, 어떤 사람들은 컴퓨터 바이러스를 트로이 목마 프로그램의 한 부분으로 보기도 한다. 이 문제를 해결하기 위하여 1988년 말에 국제적인 컴퓨터 보안 전문가들이 모임을 가졌으나, 컴퓨터 바이러스에 대한 정의를 내리지 못했다.

필자는 컴퓨터 바이러스란 '컴퓨터의 프로그램이나 실행가능한 부분을 변형하여, 여기에 자기 자신 또는 자기 자신의 변형을 복사하는 명령어들의 조합'이라고 정의하고자 한다. 여기서 실행가능한 부분의 예로는 오버레이(Overlay), 장치구동기(Device Driver), 부트 레코드(Boot Record), 운영체제(Operating System) 등을 들 수 있다. 또한 여기서 자기 자신의 변형이란 용어를 사용한 이유는 컴퓨터 바이러스에 따라서 자기 자신을 그대로 다른 곳에 복사하는 것이 아니라 자기 자신을 일부 변형시켜서 다른 곳에 복사하는 컴퓨터 바이러스도 있기 때문이다.

컴퓨터 바이러스는 실제의 바이러스와 비슷하게 부작용(Side Effect)을 가지고 있는 경우가 많다. 즉, 감기 바이러스가 인체내에서 증식만 하는

것이 아니라 감기를 일으키듯이, 컴퓨터 바이러스도 자기 자신을 복사하는 명령어들의 조합만을 가지고 있지않고 하드 디스크를 지우는 등의 다른 일을 수행하는 명령어들을 포함하는 경우가 많다. 컴퓨터 바이러스가 사람들에게 경계의 대상이 되는 이유는 사용자 몰래 자기 자신을 복사하는 데 있는 것이 아니라 그 부작용 때문이다. 하지만 자기 자신을 복사하는 것 이외의 부작용은 일으키지 않는 컴퓨터 바이러스도 있기 때문에 이것은 정의에 포함시키지 않았다.

컴퓨터 바이러스는 여러가지 나쁜 영향을 미치는 악성 프로그램이지만, 이러한 악성 프로그램이 모두 컴퓨터 바이러스는 아니다. 개인용 컴퓨터에서 문제가 되는 악성 프로그램은 크게 컴퓨터 바이러스와 트로이목마 프로그램(Trojan Horse)의 두가지로 나눌 수 있다. 대형 컴퓨터에서는 이것들 이외에 벌레 프로그램(Worm)이라는 것이 존재하고 있지만, 개인용 컴퓨터에서는 아직 문제가 되지 않기 때문에 제외하는 것이 바람직하다고 생각된다.

컴퓨터 바이러스와 구별해야 할 것으로 '트로이목마 프로그램'(Trojan Horse Program)이 있다. 트로이목마 프로그램에 대한 정의도 아직 확실히 정립되어 있지 않으나, 필자는 '컴퓨터의 프로그램 내에 사용자 몰래 고의적으로 포함된, 자기 자신을 복사하지 않는 명령어들의 조합'이라고 정의를 내리고자 한다. 트로이목마 프로그램은 고의적으로 포함되었다는 점에서 프로그래머의 실수로 포함된 프로그램의 버그(Bug)와는 틀리다. 또한 트로이목마 프로그램은 자기가 포함되어 있는 프로그램 내에서만 존재하고 다른 곳으로 자기 자신을 복사하지 않는다는 점에서 컴퓨터 바이러스와 틀리다. 따라서 어떤 프로그램을 실행시켰을 때 하드 디스크의 화일들을 지우지만 다른 프로그램에 복사되지 않으면, 이것은 컴퓨터 바이러스가 아니라 트로이목마 프로그램이다.

트리이목마 프로그램의 공통적인 특징은 사람들의 호기심을 자극하는 내용이거나 또는 기존의 유명 프로그램에 대한 새로운 소식이나 샘플 프로그램(Sample Program)의 가면을 쓰고 있는 점이다. 그중 유명한 것이 RCKVIDEO.EXE이다. 이 프로그램을 실행시키면 유명한 가수인 마돈나가 노래부르는 모습을 보여준 뒤에 디스크의 모든 화일을 지우고 "You are stupid to download a video about rock stars "(너는 가수에 대한 화일을 가져올 정도로 멍청하다)와 같은 내용을 담은 화일만을 남겨둔다. 또 다른 것으로 SEX-SHOW.EXE가 있다. 이것 또한 음란한 장면들을 보여주면서 모든 화일들을 지우는 것이다. 따라서 미국에서는 새로운 프로그램을 시험해 보기 전에 다음과 같은 교훈을 상기하라고 한다. "When something is too good to be true, it usually is "(어떤 것이 사실이라고 믿기에는 너무 좋아보인다면, 그것은 사실이 아닐 경우가 많다.)

컴퓨터 바이러스의 분류

컴퓨터 바이러스에 대한 분류도 아직 논란의 대상이 되고 있다. 일부의 사람들은 컴퓨터 바이러스가 가지고 있는 부작용의 성질에 따라 컴퓨터 바이러스를 양성 바이러스와 악성 바이러스로 나누기도 한다. 여기서 양성 바이러스란 컴퓨터에 수록된 자료들을 파괴하지 않는 바이러스를 말하고, 악성 바이러스란 컴퓨터에 있는 자료들을 파괴하는 바이러스를 말한다. 이러한 분류에 따르면 하드 디스크의 프로그램이나 데이타를 지워버리는 바이러스는 악성 바이러스에 속한다.

하지만 필자는 양성 바이러스란 용어는 잘못된 것이라고 생각하며, 필자가 그렇게 생각하는 데는 다음과 같은 네가지 이유가 있다. 첫째, 컴퓨터 바이러스란 양성이나 악성에 관계없이 사용자가 원하지 않는 쓸모 없는 프로그램이다. 둘째, 컴퓨터 바이러스가 실행되는 동안에는 컴퓨터의 속도가 떨어지고 사용가능한 기억장소 및 디스크의 공간을 줄여서 귀중한 자원을 함부로 낭비하는 결과를 초래하게 된다. 셋째, 양성 바이러스라고 불리는 것들은 컴퓨터에서 어떤 부분을 사용하지 않는다는 가정하에 그 부분을 이용하여 만들어진 것이기 때문에, 만약 컴퓨터에서 그 부분을 사용하게 되면 컴퓨터 바이러스에 의해서 자

료가 파괴될 수 있다. 넷째, 양성 바이러스라는 용어는 컴퓨터 바이러스를 만드는 이들에게 양성 바이러스를 만드는 것은 죄가 되지 않는다는 그릇된 인상을 심어줄 수 있다. 따라서 컴퓨터 바이러스는 모두 악성이며, 컴퓨터 바이러스를 양성 바이러스와 악성 바이러스로 나누는 것은 잘못된 것이라고 생각한다.

컴퓨터 바이러스를 나누는 데 가장 일반적인 분류법은 컴퓨터 바이러스가 감염되는 컴퓨터의 종류에 따른 분류일 것이다〈그림-(가)〉. 컴퓨터 바이러스는 그 컴퓨터가 가지고 있는 특정한 기능들을 이용하기 때문에 여러 기종에 감염되는 컴퓨터 바이러스란 존재하지 않기 때문이다. 이 분류에 따르면 컴퓨터 바이러스는 크게 대형 컴퓨터에 감염되는 컴퓨터 바이러스와 개인용 컴퓨터에 감염되는 컴퓨터 바이러스로 나눌 수 있다. 그리고 개인용 컴퓨터에 감염되는 컴퓨터 바이러스도 그 기종에 따라서 애플(Apple) Ⅱ 바이러스, IBM-PC 바이러스, 매킨토시(Macintosh) 바이러스, 아미가(Amiga) 바이러스, 아타리(Atari) 바이러스 등으로 나눌 수 있다. 국내에서는 IMB-PC가 개인용 컴퓨터의 대부분을 차지하고 있기 때문에, 가장 문제가 되는 것도 IBM-PC 바이러스이다.

그림-1 컴퓨터 바이러스의 분류

(가) 컴퓨터 종류에 따른 분류

- 대형 컴퓨터 바이러스
- 개인용 컴퓨터 바이러스
  - 애플 Ⅱ 바이러스
  - IMB-PC 바이러스
  - 매킨토시 바이러스
  - 아미가 바이러스
  - 아타리 바이러스
  - 기 타

(나) 부작용에 따른 분류

- 즉시 부작용을 나타내는 바이러스
- 나중에 부작용을 나타내는 바이러스
  - 시한 폭탄
  - 논리 폭탄

(다) 피해 복구에 따른 분류

- 피해 복구가 가능한 바이러스
- 피해 복구가 가능하지 않은 바이러스

(라) 암호화에 따른 분류

- 암호화 기법을 사용하는 바이러스
- 암호화 기법을 사용하지 않는 바이러스

IBM-PC 바이러스는 바이러스가 감염되는 부위에 따라 부트 바이러스(Boot Virus), 화일 바이러스(File Virus)와 부트/화일 바이러스의 세가지로 나눌 수 있다(그림-2).

컴퓨터를 처음 켰을 때 디스크의 가장 처음 부분(부트 섹터, Boot Sector)에 위치하는 프로그램(부트 레코드, Boot Record)이 제일 먼저 실행되는 데, 여기에 자리잡는 컴퓨터 바이러스를 부트 바이러스라고 한다. 부트 바이러스도 감염되는 디스크의 종류에 따라서 플로피 디스크에만 감염되는 것과 하드 디스크에도 감염되는 것으로 나눌 수 있다. 또한 하드 디스크에 감염되는 것들도 하드 디스크의 주 부트레코드(Master Boot Record)에 감염되는 것과 도스 부트레코드(DOS Boot Rocord) 에 감염되는 것으로 나눌 수 있다.

1990년 5월 1일까지 국내에서 발견된 부트 바이러스는 브레인 바이러스(Brain Virus), LBC 바이러스, LBC-Ⅱ 바이러스, 스톤 바이러스(Stoned Virus), 핑퐁 바이러스(Ping Pong Virus)와 디스크 살해 바이러스(Disk Killer Viurs)의 6종이다. 이들 중에서 브레인 바이러스와 LBC-Ⅱ 바이러스는 플로피 디스크에만 감염되는 바이러스이며, LBC 바이러스와 스톤 바이러스는 플로피 디스크 및 하드 디스크의 주 부트레코드에, 핑퐁 바이러스와 디스크 살해 바이러스는 플로피 디스크 및 하드 디스크의 도스 부트레코드에 감염되는 바이

러스이다.

화일 바이러스란 일반적인 프로그램에 복사되는 컴퓨터 바이러스를 말한다. 이때 감염되는 프로그램들은 COM 화일, EXE 화일 등의 실행화일(Executable File)이나 오버레이 화일(Overlay File) 등이며, 실행할 수 없는 데이타 화일(Data File)에는 감염되지 않는다.

1990년 5월 1일까지 국내에서 발견된 화일 바이러스는 예루살렘 바이러스(Jerusalem Virus), 일요일 바이러스(Sunday Virus), 1701 바이러스와 1704 바이러스의 4종이다.

화일 바이러스는 화일에 감염되기 위하여 여러 가지 다양한 전략을 사용하기 때문에, 어떤 한가지 방법으로 분류할 수 없다. 가장 일반적인 분류 방법은 감염되는 프로그램의 종류에 따른 것이다. 즉, 감염되는 프로그램에 따라서 특정화일 감염 바이러스, COM 화일 감염바이러스, EXE 화일 감염 바이러스, COM 및 EXE 화일 감염 바이러스의 4가지로 분류할 수 있다. 또한 COM 화일 감염 바이러스도 COMMAND.COM에 감염되는 것과 감염되지 않는 것이 있다.

대표적인 특정화일 감염 바이러스에는 러하이 바이러스(Lehigh Virus)가 있다. 러하이 바이러스는 COMMAND.COM에만 감염되는 화일 바이러스이며, 국내에서는 아직 발견되지 않았다. 국내에서 발견된 COM화일 감염 바이러스로는 1701 바이러스와 1704 바이러스가 있으며, COM 화일 및 EXE 화일 감염 바이러스에는 예루살렘 바이러스와 일요일 바이러스가 있다. 이들 중에서 예루살렘 바이러스와 일요일 바이러스는 COMMAND. COM에 감염되지 않지만, 1701 바이러스와 1704 바이러스는 COMMAND. COM에 감염되는 바이러스이다.

또 다른 분류 방법은 화일 바이러스가 프로그램내의 어디에 위치하느냐에 따르는 것이다. 만약 기존의 프로그램을 파괴하지 않고 프로그램의 앞이나 뒤에 바이러스 프로그램이 붙게 되면, 이것을 기생형 바이러스(Parasitic Virus)라고 부른다.

따라서 기생형 바이러스는 필연적으로 프로그램의 크기를 증가시키게 된다. 만약에 기존의 프로그램이 있는 곳에 바이러스 프로그램이 위치하게 되면, 이것을 겹쳐쓰기형 바이러스(Overwriting Virus)라고 한다.

겹쳐쓰기형 바이러스에 감염된 화일은 기존의

그림-2 IBM-PC 바이러스의 분류

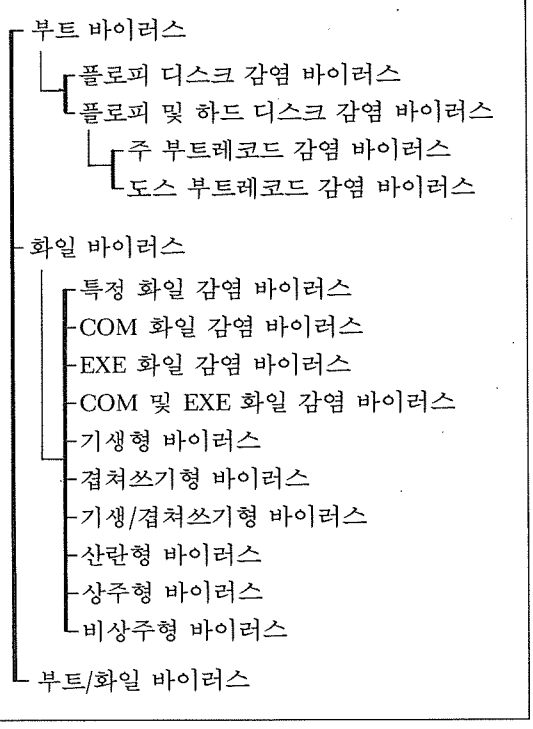
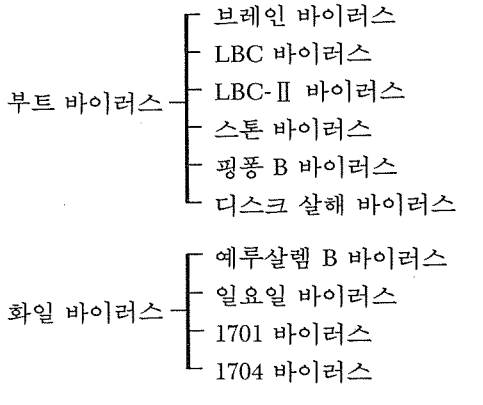


그림-3 한국에서 발견된 컴퓨터 바이러스 (1990년 5월 1일 현재)



프로그램이 파괴되어 정상적으로 수행되지 못할 경우가 많지만, 바이러스가 프로그램에서 사용하지 않는 영역을 찾아서 들어갈 경우에는 기존의 프로그램의 수행에는 전혀 영향을 미치지 않게 된다. 또한 기존의 프로그램의 크기가 바이러스 프로그램보다 클 경우에는 감염된 프로그램의 크기가 커지지 않으므로 사용자가 눈치채기 어렵다. 보통은 기생형 바이러스로 동작하면서 가끔 겹쳐쓰기를 시행하는 바이러스는 기생/겹쳐쓰기형 바이러스라고 하며, 국내에서는 아직 발견되지 않은 비엔나 바이러스(Vienna Virus)가 여기에 속한다.

그 이외에 최근에 발견된 AIDS Ⅱ 바이러스의 경우에는 EXE 화일에 직접 감염되지 않고 같은 이름의 COM 화일을 만들어서 여기에 바이러스를 넣어두는 경우도 있다. 같은 이름의 COM 화일과 EXE 화일이 동시에 같은 디렉토리내에 존재할 때 화일이름을 입력시키면 COM 화일을 우선적으로 실행되기 때문에, 화일에 바이러스가 직접 감염된 경우와 같은 효과를 나타내게 된다.

이러한 바이러스를 산란형 바이러스(Spawning Virus)라고 한다. 이것은 화일의 변형여부를 검사하여 컴퓨터 바이러스의 감염여부를 알아내는 프로그램으로는 진단할 수 없는 바이러스이다. 지금까지 국내에서 발견된 화일 바이러스들은 모두 기생형 바이러스이다.

참고로 기생형 바이러스의 경우에는 감염되었을 때 증가하는 프로그램의 크기가 그 바이러스의 이름이 되는 경우가 많다. 예를 들어서 1704 바이러스는 프로그램의 크기를 1704 바이트 증가시키기 때문에 붙여진 이름이다. 어떤 사람들은 이렇게 증가된 화일의 크기로 이름을 짓는 것이 많은 사람들의 혼동을 막는다는 의미에서 바람직한 방법이라고 주장하기도 한다.

하지만 예루살렘 바이러스의 경우와 같이 증가된 화일의 크기가 COM 화일과 EXE 화일이 틀린 경우도 있고(COM 화일의 경우에는 1813 바이트, EXE 화일의 경우에는 1808 바이트) 1701 바이러스와 1704 바이러스의 경우와 같이 바이러스를 조금 바꿔서 크기가 달라지는 경우도 있기 때문에 모든 경우에 이러한 방법을 사용할 수는 없는 실정이다.

그외에도 화일 바이러스가 수행된 후에 기억장소에 계속 머물러 있는가에 따른 분류 방법도 있다. 만약 화일 바이러스가 '사이드킥(Side Kick)'과 같은 램상주 프로그램들처럼 기억장소에서 계속 머물러 있다면 이것을 상주형 바이러스(Resident Virus)라고 하며, 보통의 프로그램들과 같이 한번 실행된 후에 기억장소에서 없어지면 이것을 비상주형 바이러스(Nonresident Virus)라고 한다. 상주형 바이러스의 경우에는 바이러스에 감염된 프로그램이 한번 실행되면 다음에 실행되는 프로그램들이 계속 감염될 수 있지만, 비상주형 바이러스의 경우에는 바이러스에 감염된 프로그램이 실행될때만 바이러스가 동작하여 다른 프로그램에 감염된다. 지금까지 국내에서 발견된 화일 바이러스들은 모두 상주형 바이러스이다.

부트/화일 바이러스는 부트 섹터와 화일 모두에 감염되는 바이러스이다. 이것은 전세계적으로도 두종류밖에는 발견되지 않았고, 국내에서는 아직 보고가 없다.

지금까지 설명한 바와 같이 컴퓨터 바이러스를 감염되는 컴퓨터 기종에 따라 분류할 수도 있지만, 부작용을 일으키는 조건에 따라 컴퓨터 바이러스를 분류하기도 한다〈그림－1(나)〉. 즉, 실행되는 즉시 부작용을 나타내는 바이러스와 어떤 조건이 되어야만 작용을 나타는 바이러스로 나눌 수 있다. 일반적인 컴퓨터 바이러스들은 한동안 부작용을 나타내지 않음으로써 바이러스가 널리 퍼질 수 있도록 한다. 즉시 부작용을 나타내는 대표적인 바이러스에는 LBC 바이러스가 있다.

LBC 바이러스는 실행 즉시 하드 디스크의 주 부트레코드를 파괴한다. 또한 즉시 부작용을 나타내지 않는 바이러스들도 컴퓨터 바이러스 내부에서 부작용을 나타낼 시기를 판단하는 기준에 따라 시한 폭탄(Time Bomb)과 논리 폭탄(Logic Bomb)으로 나누기도 한다. 시한 폭탄은 일정한 날짜가 되면 파괴를 시작하는 것으로, 13일의 금요일에 화일을 삭제하는 예루살렘 바이러스가 여기에 속한다. 논리 폭탄은 프로그램 내에서 계산을 하다가 어떤 일정한 값에 도달하거나 또는 프

표-2 화일 바이러스들의 비교

부트 바이러스	플로피 디스크	하드 디스크	감염시기	기억장소 감소	불량 클러스터	기타 증상
브레인 바이러스	5.25인치 360KB에만 감염	×	디스크 읽기	7K 바이트	3개	볼륨라벨을 바꿈
LBC 바이러스	○	주 부트레코드	디스크 읽기	2K 바이트	×	하드디스크 파괴
LBC-Ⅱ 바이러스	5.25인치 360KB에만 감염	×	디스크 읽기	3K 바이트	1개	메시지 출력
스톤 바이러스	○	주 부트레코드	디스크 읽기, 쓰기	2K 바이트	×	메시지 출력
핑퐁B 바이러스	○	도스 부트레코드	디스크 읽기	2K 바이트	1개	까만점이 돌아다님
디스크 살해 바이러스	○	도스 부트레코드	디스크 읽기	8K 바이트	3개	하드디스크 파괴

로그램을 일정 횟수 사용했을 때 파괴를 시작하는 것으로, 러하이 바이러스가 여기에 속한다.

그 이외에도 컴퓨터 바이러스에 의한 피해가 복구 가능한 지에 따른 분류법도 있고〈그림-1(다)〉, 암호화 기법을 사용하여 진단이나 분석이 되지 않도록 되어 있는 지에 따른 분류법도 있다〈그림-1(라)〉. 지금까지 국내에서 발견된 바이러스들중에서는 화일 바이러스들이 일부의 EXE 화일을 파괴하는 것으로 알려져 있다. 또한 암호화기법을 사용하는 바이러스로는 1701 바이러스와 1704 바이러스가 알려져 있다.

국내에서 1990년 5월1일까지 발견된 IBM-PC 바이러스는 10종이며, 계속 그 숫자가 증가하고 있는 추세이다. 국내에서 발견된 부트 바이러스는 브레인 바이러스, LBC 바이러스, LBC-Ⅱ 바이러스, 스톤 바이러스, 핑퐁 B 바이러스, 디스크 살해 바이러스의 6종이며, 화일 바이러스로는 예루살렘 B 바이러스, 일요일 바이러스, 1701 바이러스, 1704 바이러스의 4종이 보고되어 있다〈그림-3〉. 이중에서 LBC 바이러스와 LBC-Ⅱ 바이러스는 국내에서 제작된 것으로 추정되고 있다.

그 이외에도 국내에서 제작된 변형 브레인 바이러스, 변형 LBC 바이러스, 변형 예루살렘 B 바이러스들이 있지만 이들은 기존의 바이러스 코드

표-1 부트 바이러스들의 비교

화일 바이러스	종류	COM 화일	EXE 화일	화일작성일 및 속성	암호화	기타 증상
예루살렘 B 바이러스	상주형	1813바이트 증가 COMMAND.COM 제외	1808~1823 바이트 증가	변하지 않음	×	화면 스크롤, 속도저하 EXE화일파괴, 화일지움
일요일 바이러스	상주형	1636바이트 증가 COMMAND.COM 제외	1636~1651 바이트 증가	변하지 않음	×	×
1701 바이러스	상주형	1701바이트 증가	×	변하지 않음	○	글자가 떨어져 쌓임
1704 바이러스	상주형	1704바이트 증가	×	변하지 않음	○	글자가 떨어져 쌓임 IBM-PC에는 감염안됨

*예루살렘 B 바이러스가 EXE 화일에 감염될 때는 여러번 감염될 수 있다.

를 일부만 바꾼 것이기 때문에 이들을 다른 종류로 본다는 것은 무리가 있다. 일부 매스컴이나 자칭(?) 바이러스 전문가들 중에서는 이들을 모두 모아서 국내에서 발견된 바이러스가 수십종에 이른다고 하기도 하지만, 이것은 많은 사람들을 자극하는 효과밖에는 없기 때문에 바람직하지 않다고 생각한다.

국내에서 발견된 컴퓨터 바이러스들의 특징을 〈표-1〉과 〈표-2〉에 요약했다.

국내에서의 피해 현황

필자가 국내에서 컴퓨터 바이러스에 의한 피해 현황을 조사하기 위해 1990년 4월에 컴퓨터 사용자 765명을 대상으로 시행한 설문조사의 결과는 다음과 같다.

컴퓨터바이러스를 경험한 시기는 1988년 이전이 5.0%, 1988년 1~4월이 7.9%, 1989년 5~8월이 11.3%, 1989년 9~12월이 22.1%, 1990년 1월 이후가 20.7%로서, 1989년 9월 이후부터 급격하게 증가하는 경향을 보였다.
이 5.0%, 88년 1~4월이 7.9%, 89년 5~8월이 11.3%, 89년 9~12월이 22.1%, 90년 1월 이후가 20.7%로서, 89년 9월 이후부터 급격하게 증가하는 경향을 보였다.

컴퓨터 바이러스를 경험한 횟수는 0회가 10%, 1~3회가 43.2%, 4~7회가 16.6%, 8~10회가 7.8%, 10회 이상이 18.5%로서, 1~3회가 가장 많았으며 10회 이상 계속 감염되는 사람도 많은 비율을 차지하였다.

컴퓨터 바이러스의 감염 경로로는 아는 사람에게 복사를 하고 나서가 57.4%, 원본 디스크에서 4.7%, 통신에서 2.7%, 모르겠다가 13.3%를 차지했다. 처음에 예상했던 대로 컴퓨터 바이러스는 불법복사로 인해서 많이 감염되었으며, 통신으로 받은 화일때문에 감염되는 경우는 예상외로 극히 적었다. 아마도 컴퓨터 통신을 하는 사람들은 다른 사람들에 비하여 컴퓨터 바이러스에 대한 정보가 빠르고 조심을 하기 때문인 것으로 분석된다.

컴퓨터 바이러스를 경험한 사람들을 대상으로 감염된 바이러스의 종류를 조사해본 결과 여러 종류의 바이러스에 중복 감염된 사람들이 많았다. 또한 이들중 절반 이상인 53.2%가 브레인 바이러스(Brain Virus)를 경험하였고, 38.7%가 예루살렘 바이러스(Jerusalem Virus), 31.9%가 LBC 바이러스를 경험한 것으로 나타났다.

따라서 이 세가지 바이러스가 국내에서 감염되는 컴퓨터 바이러스의 거의 대부분을 차지한다는 사실을 알 수 있었다. 한가지 특이한 점은 최근에 발견된 LBC-Ⅱ 바이러스에 감염된 비율이 16.0%로 생각보다 높게 나타났고, 일요일 바이러스(Sunday Virus)에 감염된 비율이 6.3%로 낮게 나타났다는 것이다. LBC-Ⅱ 바이러스의 이름을 들어서 알고 있는 사람이 42.7%로 5위, 일요일 바이러스를 알고 있는 사람이 47.3%로 4위를 차지한 것에 비하면 이 결과는 의외라고 할 수 있다. 그외에 스톤 바이러스(Stoned Virus)가 5.5%, 핑퐁 바이러스(Ping Pong Virus)가 2.9%, 디스크 살해 바이러스(Disk Killer Virus)가 2.9%, 1701 바이러스가 1.6%, 1704 바이러스가 1.6%를 각각 차지했다. 1701 바이러스와 1704 바이러스도 조사전에 생각했던 것보다는 경험한 사람이 많지 않았다.

컴퓨터 바이러스로 인해 금전상의 손실을 본 사람은 응답자 중에서 15.2% 정도였다. 컴퓨터 바이러스에 의한 직접적인 피해는 화일 파괴(55.6%), 하드 디스크 파괴(40.8%), 디스켓 파괴(38.2%)의 순이었다.

하지만 피해를 입은 사람들의 피해 금액은 만원 이하가 응답자의 36.0%, 만원에서 10만원까지가 27%, 10만원에서 50만원까지가 15%, 50만원에서 100만원까지가 4%였고, 100만원 이상이 15%나 되었다. 응답자 중에서는 2000만원까지 피해 금액을 적은 사람도 있었다.

이것은 아마도 LBC 바이러스때문에 하드 디스크의 귀중한 자료가 파괴되었는데, 이것을 복구시키지 못해서 생긴 것으로 추정된다. 따라서 컴퓨터 바이러스때문에 직접적인 재산상의 피해를 받는 사람들의 숫자가 많지 않다고 하더라도, 많은 손실을 가져올 가능성이 있다는 점이 입증된 셈이다.