컴퓨터 바이러스와 對處方案

工學博士 姜 永 採

科學評論家

1. 서 론

컴퓨터의 보급이 늘어가고 사용자가 늘어남에 따라서 점차 컴퓨터 바이러스의 被害者도 늘어나고 있어 컴퓨터 사용자들에게 심각한 고민거리로 대두되고 있다. 본고에서는 컴퓨터 바이러스의 종류와 증상 및 예방법에 대하여 알아본다.

컴퓨터 바이러스는 우리가 일반적으로 알고 있는 生物學的 바이러스처럼 實際로 살아 움직이는 生命體가 아니라 컴퓨터의 運營體制나 소프트웨어에 몰래 들어가 시스템 사용자의 프로그램에 自身을 復製하고 컴퓨터 시스템과 파일들을 破壞하는 프로그램을 말하는 것으로서, 그 症狀이 살아 움직이는 바이러스와 흡사하다고 하여 컴퓨터 바이러스라고 부른다.

현재까지 컴퓨터 바이러스는 수백 가지 이상이 발견되었으며, 이들의 共通的인 特徵을 보면 PC 바이러스가 侵入하여 核分裂을 하듯이 수백번 이상의 複寫가 일어나 Bulletin Board나 Network를 통하여 全體 시스템으로 퍼지는 것이다.

계속 복사가 일어나면 수백, 수천개의 PC 시스템들이 순식간에 傳染되어 버리는 것이다.

바이러스 프로그램의 일반적인 증상으로는 첫째, 디스크의 부트(始動) 레코드를 바꾸거나 파괴한다(예 : 브레인, LBC, 핑퐁 바이러스 등).

둘째, 시스템의 부팅 시간이나 액세스 시간이 오래 걸리며, 파일의 크기 증가 및 시스템 다운을 초래한다.

셋째, 디스크의 FAT(File Allocation Table)를 바꾸거나 파괴하며, 디스크의 볼륨 라벨을 바꾼다(예 : ©브레인, Ashar Virus 등).

넷째, 램(RAM) 常住 프로그램의 실행을 중지시키며 키보드의 키가 바이러스 코드에 의해 변형되어 사용자에게 혼란을 준다.

또한 畵面에 갑자기 非定常的인 메시지가 出力되거나 畵面이 변형되는 등을 들 수 있다.

2. 바이러스 종류

바이러스는 종류에 따라 미치는 영향도 다르며, DOS(Disk Operating System ; 디스크 운영체제)에서 作動되는 바이러스만도 종류가 많으나 크게 세 가지로 分類된다.

첫째는 부트 感染 바이러스로, 주로 플로피나 하드 디스크의 부트 섹터(Boot Sector)나 하드 디스크(Hard Disk)의 副섹터에 붙어 있으며 파키스타니 브레인(파키스타인의 두뇌)이라고 하는데 아주 巧妙히 숨어 있어 찾아내기 힘들다.

두번째는 프로그램에 감염되는 것으로는 가장 널리 알려져 있는 것으로 이스라엘에서 開發되었다고 하여 이스라엘 바이러스라고 한다.

이들 바이러스는 速度를 늦추거나 파일 크기를 증가시키면 주로 運用 프로그램인 EXE와 COM 파일에 있다.

세번째는 시스템 감염 바이러스로, Command.COM과 같은 시스템 파일에 존재하는데, 代表的인 것으로는 리하이(Lehigh) 바이러스로서 리하이 대학에서 개발되었다고 하여 이름이 붙여진 것이며, 이것은 하드 디스크(알루미늄이나 플라스틱에 磁性體로 코팅된 円板狀의 記錄媒體)에 있는 모든 데이터를 지워 없애버리는 強力한 바이러스이다.

한편 DOS 바이러스들이 傳染되고 있는 동안은 사용자는 전혀 아무 이상없이 PC를 사용할 수 있으나 火藥庫에 총을 쏘면 폭발하듯이 어떤 要因이 가해지면 症勢가 나타나기 시작한다.

이와 같이 作動시키는 요인은 바이러스가 어떻게 만들어져 있느냐에 따라서 다른데, 예를 들면 특정한 날짜와 시간이 되면 나타나거나 혹은 프로그램을 使用하기 시작하면 나타나는 경우도 있다.

어떤 바이러스는 PC 화면에 눈물을 흘리거나 비가 오는 모습으로 나타나고 혹은 글자들이 뚝뚝 떨어져 내리는 등의 다양한 증세를 보인다.

또한 바이러스에는 사용하고 있는 프로그램이 정확하게 作動하지 못하게 하거나 지워버리는 등 피해를 크게 입히는 경우도 있고, 이와는 반면에 특정한 날짜나 시간에 메시지가 나타나는 흥미있는 바이러스도 있다.

바이러스 그룹 중에는 트로전 호스(Trojan Horse)와 웜(Worm ; 벌레)이라고 하는 바이러스가 있는데, 트로전 호스는 일반 바이러스처럼 스스로 傳染시키지 않고 프로그램 속에 숨어 어느 순간에 하드 디스크를 再次 포매팅하는 등 有用한 役割을 하고 있다.

또한 벌레라고 하는 웜은 아주 작은 프로그램으로서 스스로 계속 복제해 나가다 파일을 파괴하지 않으므로 바이러스와 다르게 구분한다.

다만 繼續的인 增幅으로 컴퓨터의 메모리, 즉 램(RAM)이나 디스크의 자리를 모두 차지하게 되어 컴퓨터의 處理速度가 늦어진다.

2·1 4096 바이러스

4096 바이러스는 1990년 1월에 처음으로 규명되었으며, 사용자들에게 거의 발견되지 않는 Stealth형 바이러스로서 COM, EXE, OVL 파일들을 감염시키게 되면 파일 길이가 4096 바이트로 늘어난다.

이 바이러스는 Century Virus, LDF Virus, 100 Years Virus 등으로 불리우며 실행형 파일(COM, EXE, OVL)에 감염되어 파일에 寄生하며 메모리에 常住하고 感染 파일을 엉키게 만든다.

시스템 메모리에 일단 바이러스가 상주하면 Copy나 XCopy 명령 등의 오픈되는 파일들을 포함하여 모든 오픈되어 있는 實行 파일을 감염시킨다.

바이러스 감염 후 DIR 명령으로 감염된 파일들을 살펴 보아도 길이가 증가한 것이 나타나지 않으며, 디스켓에 있는 파일들을 서서히 엉키게 하여 자료 파일과 실행형 파일 모두를 사용할 수 없도록 한다.

이때는 파일의 엉킴이 서서히 일어나고 사용

자가 바이러스를 認知하지 못하기 때문에 하드웨어의 異常으로 간주하기 쉽다.

파일의 엉킴은 파일들이 섹터를 잃었을 때 사용자가 CHKDSK/F 명령을 사용하여 이를 解決하려 할 때 바이러스가 Fat 부분을 교묘하게 調節하거나 사용 가능한 섹터의 數를 變化시키는 경우에 發生한다.

4096 바이러스가 메모리에 常住하고 있는 동안 어떤 감염된 파일을 Copy할 때 서로 生成될 파일의 이름에 實行形 擴張子를 붙이지 않으면 새로 생성되는 파일은 바이러스에 감염되지 않는다.

따라서 한 시스템상에서 바이러스에 감염된 모든 파일을 正常的으로 復舊하는 한 가지 방법은 메모리에 바이러스가 올라와 있는 동안 바이러스에 감염된 파일들을 정상적인 디스켓에다가 확장자를 붙이지 않고 복사하여 시스템을 끈 다음 다시 바이러스에 감염되지 않는 시스템 디스켓으로 부팅(始動)시키는 것이다.

일단 다시 부팅이 되면(CTRL+ALT+DEL Key를 의미하는 것이 아님) 바이러스가 메모리에서 없어지므로 바이러스에 감염된 파일들을 디스켓에서 모두 찾아서 지우고 복사해 두었던 파일들에 本來의 확장자를 붙인 후 再次 複寫하여 시스템을 사용한다.

이상과 같은 방법으로 바이러스를 시스템에서 除去할 수는 있지만 엉켜 있는 파일들은 여전히 손상을 입은 채 시스템에 남아 있게 된다.

4096 바이러스는 자신의 코드 내부에 부트 섹터(Boot Sector)를 독자적으로 보유하고 있으나 디스켓의 부트 섹터에 겹쳐쓰기(Overwriting)를 하지 않는다.

만일 바이러스 내부의 부트 섹터를 디스켓의 부트 섹터로 옮기고 시스템을 다시 부팅시키면 FRODOLIVES라는 메시지가 나타날 것이다.

4096 바이러스는 SCANV53 이상으로 검색이 가능하며 CLEANV62 이상으로 치료가 가능하다.

예를 들면 CLEAN C:〔4096〕↵

2·2 163 COM 바이러스

一名 TINY 바이러스는 1990년 6월 아이슬랜드의 Fridrik Skulason에 의해서 밝혀졌다. 이 바이러스는 메모리에 상주하지 않으나 Commnad.COM도 感染시키는 일반적인 COM 파일 感染者이다.

처음 163 COM 바이러스에 감염된 파일이 實行되면 이 바이러스는 현재 디렉토리의 첫번째 COM 파일을 감염시키는 부팅이 가능한 시스템 디스크에서는 Command.COM이 감염된다.

이 바이러스는 파일의 본래의 길이가 1K 바이트 이상인 것만 感染시키며, 감염된 파일들은 길이가 163바이트 늘어난다.

디렉토리의 날짜와 시간은 감염 당시의 것으로 바뀌며, 감염된 파일의 끝부분은 항상 16진수 ; '2A 2E 4F 4D 00'로 끝난다.

이 바이러스는 일반적으로 자신을 다른 COM 파일에 複寫만 하며 지금까지 발견된 MS-DOS 바이러스 중 가장 작은 바이러스이다.

2·3 405 바이러스

405 바이러스는 발생지가 오스트리아 또는 독일로서 디렉토리(디스크에 저장된 파일들의 目錄을 담고 있는 領域 또는 파일)내에 있는 COM 파일들만을 감염시키는 겹쳐쓰기 바이러스이다.

만일 감염시킬 COM 파일의 길이가 405 바이트 이하이면 이 바이러스에 감염되고 난 후 405 바이트가 될 것이다.

이 바이러스는 이전에 이미 자신에게 감염된 COM 파일들을 識別하지 못하고 계속 반복 감염시키는 것으로 알려져 있다.

2·4 512 바이러스

一名 512-A, Number of the Beast Virus 및 Stealth Virus라고 하며, 1990년 1월 Vesselin Bontchev에 의해 불가리아에서 처음 糾明되었다.

이 바이러스는 Command.COM을 비롯한 COM 파일들을 감염시키며 최초로 감염된 프로그램이 實行될 때 메모리에 常住한다.

이 바이러스는 메모리에 상주한 후 어떠한 理由에서건 열려(OPEN) 있는 모든 COM 파일을 檢査하여 자신에게 감염되지 않은 파일의 길이가 최소한 512 바이트이면 감염시킨다.

512 바이러스에 감염된 시스템은 使用中 다운될 뿐만 아니라 프로그램이 갑자기 깨져서 예기치 못한 실수(Error)를 겪게 된다.

또한 이 바이러스는 파일을 감염시킬 때 주된 파일만이 아니고 이 파일에 관련된 파일들까지도 連鎖的으로 破壞하며 임의의 1개 파일에 감염되었는지 안되었는지를 구분하는 識別標示를 바이러스 끝부분에 '666'으로 해두기 때문에 "Number of the Beast(금수의 수)"라는 別名을 갖고 있으며, 감염된 파일의 끝부분에 바이러스 코드 512 바이트를 追加하므로 512 바이러스에 감염되었는지의 여부는 쉽게 구별할 수 있다.

이미 알려진 512 바이러스에는 512-B, 512-c, 512-D가 있다.

2·5 1210 바이러스

一名 Prudents라고 하는 이 바이러스는 1989년12월 스페인의 바로셀로나에서 처음 규명되었다.

1210 바이러스는 메모리에 常住하고 있다가 EXE 파일들이 實行될 때마다 감염시킨다.

이 바이러스는 매년 5월 1 일과 5월 4 일 사이에 活動하며, 이 期間中에는 디스크의 Verify 상태를 변화시켜서 디스크에 쓰기(Write)가 절대로 이루어지지 않는다.

바이러스 길이는 1,210 바이트로서 검색방법은 VIRUSCAN V61 이상 버전으로 한다.

2·6 1260 바이러스

一名 Stealth 바이러스라고도 하며 미국의 미네소타州가 발생지이다.

이 바이러스는 메모리에 常住하지 않으나 감염된 COM 파일들에 작용한다고 한다.

1260에 감염된 파일들은 감염 후 길이가 1,260 바이트 증가하며 바이러스는 暗號化되는데, 암호를 푸는 키는 감염된 파일마다 다르다.

1260 바이러스는 본래 VIENNA VIRUS로부터 派生되었지만 수준높게 변형되었으며 파일서버(Server)나 모든 워크 스테이션들을 포함한 근거리통신망(LAN)을 감염시킬 수 있다.

2·7 1392 바이러스

一名 아메바(Amoeba) 바이러스라고 하며 1990년 3 월 인도네시아에서 처음으로 규명되었다.

1392 바이러스는 Command.COM을 포함하여 EXE.COM 파일을 감염시키는 메모리 常住 바이러스이며, 파일 작성날짜를 바이러스에 감염된 당시의 날짜로 바꾼다.

이 바이러스는 어떤 파괴적인 損傷을 일으키는 屬性이 없으며, 다음과 같은 메시지 때문에 아메바라는 別名이 붙여졌다.

"SMA KHETAPUNK-NOUVEL BAND. A.M.O.E.B.A"

2·8 1554 바이러스

一名 TEN BYTES라고도 하며 1990년 2 월에 약 600여명의 VALERT-L 네트워크 全加入者에게 우연히 傳送되었다.

1554 바이러스에 감염된 파일이 實行될 때 바이러스는 메모리에 常住하며 Command.COM을 포함하여 파일의 길이가 1,000 바이트 이상인 COM 파일과 1024 바이트 이상인 EXE 파일을 감염시키며, 감염 후에는 길이가 1,554~1,569 바이트 증가한다.

1554 바이러스는 활동시 파일들의 첫번째 10 바이트를 지우고 끝부분 10 바이트에 잡다한 文字를 집어넣는 方式으로 프로그램과 이에 관련된 자료파일들까지도 사용할 수 없는 상태로 만든다.

검색방법은 VIRUSCAN V58 이상 버전, IBM SCAN.

2·9 1704 바이러스

別名은 없으며 발생지를 알 수 없고 症狀으로는 畵面上에서 文字를 아래로 떨어뜨리고 COM 파일 길이가 증가된다.

바이러스 길이는 1,704 바이트로서 증상이 Cascade 바이러스와 유사하나 活動時 디스크를 포멧한다. 檢索方法으로는 VIRUSCAN, F-PROT, IBM SCAN, PRO-SCAN 등이 있다.

除去方法은 M-1704, CLEANUP, SCAN/D, F-PROT을 이용한다.

2·10 1720 바이러스

一名 PSQR 바이러스라고도 하며, 1990년 3월 스페인 바로셀로나에서 처음 糾明된 예루살렘 바이러스의 變形版이다.

이 바이러스는 예루살렘 바이러스처럼 COM과 EXE 그리고 OVL 파일들을 감염시키지만 Command.COM 파일은 감염시키지 않는다.

감염된 파일이 처음 실행될 때 바이러스는 메모리에 상주하고 이후에 實行되거나 運營되는 파일들을 감염시킨다.

이 바이러스의 파괴적 능력은 현재까지 알려진 바 없다.

검색방법은 VIRUSCAN V61 이상 버전으로 검색이 가능하며, 제거방법은 SCAN/D 혹은 감염된 파일지우기로 치료가 가능하다.

2·11 크리스마스 바이러스

一名 XA1, 1539라고도 하며, 1990년 3월 서독의 Christoff Fischer에 의하여 처음 규명되었다.

이 바이러스는 COM 파일만을 감염시키며 암호화되어 있다. 또한 감염된 프로그램이 처음 實行될 때 감염된 하드 디스크의 파일 배치(File Allocation Table)를 破壞한다.

이 바이러스는 매년 12월24일부터 다음해 1월 1일 사이에 자신에게 감염된 프로그램이 실행되면 畵面 가득히 크리스마스 트리를 표시한다.

검색은 VIRUSCAN V61 이상의 버전으로 검색하며 제거방법은 SCAN/D 또는 감염된 파일 지우기로 치료가 가능하다.

2·12 슬로우 바이러스

SLOW 바이러스는 1990년 5월에 호주에서 발견되었으며 Command.COM을 제외한 COM과 EXE, OVL 파일을 감염시킨 후 메모리에 常住하는 일반적인 실행형 바이러스이다.

처음에 감염된 파일이 시스템에서 실행되면 바이러스는 사용 가능 메모리 중 약 2KB를 차지하며 메모리에 상주한 후 OPEN 또는 OPEN되어 있는 모든 파일을 감염시키고, 감염된 일부의 EXE형 파일을 실행시키면 시스템이 다운되거나 사용자가 再次 부팅을 실시할 수밖에 없는 상황을 만든다.

검색방법은 SCAN V63 이상으로 검색할 수 있고 CLEAN V72 이상으로 치료가 가능하다.

이상에서 열거한 바이러스 이외에도 Dark Avanger, LBC, KOREA, STONE, BRAIN, Jerusalem 및 Vienna 등 380 종류가 되나 紙面 관계상 다음 기회로 미룬다.

3. 앤티 바이러스

인류의 문화생활에 便利함을 위하여 만들어진 컴퓨터의 機能이 일부 몰지각한 사람들에 의하여 紊亂해지고 있어 社會의 큰 문제로 대두되고 있는 것이 현실이다.

다음에는 컴퓨터의 必要惡이라고 하는 바이러스를 완전히 退治할 수 있는 바이러스 백신을 주로 PC Tools 시리즈로 유명한 센트럴 포인트社가 발표한 앤티 바이러스를 중심으로 설명한다.

앤티 바이러스(Anti Virus)의 주요 기능을 보면 첫째, 스캔(走査) 기능으로 프로그램과 하드웨어를 事前에 治療 予防하며 또한 콜린 기능

으로 현재까지 發表된 모든 바이러스를 除去한다.

둘째, 장차 발생할 모든 바이러스의 感染을 사전에 방지하는 특수한 防止法을 考案하며 세째, 바이러스가 메모리에 올라오지 못하도록 事前에 予防함과 동시에 부트 바이러스에 감염되지 않도록 완전히 프로텍션화한다는 것이다.

그러면 컴퓨터를 이용하는 사람들이 지켜야 할 사항은 무엇일까?

첫째, 不法으로 複寫된 소프트웨어는 여러 사람을 거쳐서 보게 되어 감염될 확률이 가장 높으므로 파이럿 카피(不法複寫)는 禁止할 것이며

둘째, 주기적으로 파일들을 반드시 백업(여분)시켜 놓도록 한다.

세째, 바이러스 抗生劑인 앤티 바이러스 프로그램을 사용하여 周期的으로 確認을 해보는 것이다.

끝으로 센트럴 포인트社의 컴퓨터 바이러스 백신에 관한 파일과 機能을 설명하면 다음과 같다.

(1) INSTALL.EXE : 하드에 센트럴 포인트 앤티를 설치하는 파일로 무조건 앤티를 치면 설치가 된다. 그러나 윈도우즈와 병합하여 사용하는 않는 경우에는 C : ＼WINDOW라는 옵션을 지워야 한다.

(2) CPSCOLOR.DAT : VGA(Video Graphic Array)용 메인 프로그램의 실행 데이터 파일. 허큘리스도 프로그램이 자동으로 식별해 풀다운을 지원한다.

(3) CPSHELP.OVL : 메인에서 사용하는 기능 도움말로 메인 툴에서 HELP 기능을 이용해 볼 수 있다.

(4) AVINST.HLP : 인스톨(Install)하는 방법을 설명한 파일

(5) CPAV.ICO : 메인에서 사용하는 아미콘 파일로 트리 등을 말한다.

(6) CPAV.GRP : 메인 프로그램 첨가 파일

(7) BOOTSAFE.EXE : 현재의 파티션(分割) 테이블이나 부트 섹터가 異常이 있는지를 點檢하는 파일로서 이상이 있으면 치료를 해주는 기능도 갖고 있다.

(8) WNTSRAM.EXE : 윈도우(창)에서 사용할 수 있도록 환경을 만들어 주는 파일로 이 파일을 실행한 후 윈도우의 응용 프로그램으로 센트럴 포인트 앤티 바이러스를 사용할 수 있다.

(9) EXCEPT.CPS : 예방을 다한 후 예방기능을 넣지 못한 특정한 파일을 리포트식으로 저장해 놓은 파일

(10) CPAV.HLP : 센트럴 포인트 앤티 바이러스 도움말(설명서)로 DOS의 TYPE 명령으론 볼 수가 없다.

이 HELP를 보려면 메인 프로그램을 실행하여 INDEX 옵션을 이용하여 볼 수 있고 프린트도 할 수 있다.

(11) VSAFE.COM : 바이러스에 의한 감염을 事前에 예방하는 프로그램으로 이 파일을 실행한 후 컴퓨터를 사용하다 바이러스가 발견되면 즉시 경고음과 함께 바이러스가 감염되지 않도록 시스템을 중지시키고 퇴치할 것인가 아니면 시스템을 再次 부팅할 것인가 아니면 현재 實行했던 파일을 다시 실행할 것인가를 메시지한다.

(12) VSAFE.SYS : 기능은 (11)번 기능과 동일하며 이 파일은 부팅될 때 뜨거워지는 RAM 常住 파일이다.

(13) VWATCH.COM : 바이러스 예방 프로그램 파일

(14) VWATCH.SYS : 부팅용 바이러스 예방 프로그램

(15) README.TXT : 센트럴 앤티 바이러스 니리글과 윈도우에서 사용하는 방법을 알려 주는 도움말 파일

(16) VIRLIST.DOC : 메인 프로그램에서 본 백신이 退治할 수 있는 바이러스의 이름과 정보를 볼 수 있는 키를 설명한 파일로 바이러스 리스트를 프린팅할 수도 있다.

(17) CPSMAIF.FNT : 메인 프로그램의 폰트를 지원하는 파일

(18) 이하 생략