컴퓨터 바이러스의 유형과 예방대책

1990

경제기획원 조사통계국
전산담당관실

머 리 말

고도정보사회에 접어들면서 컴퓨터의 보급은 실로 놀라울 정도로 확산되고 있읍니다. 이 엄청난 확산과 동시에 한편으로는 전문해커들에 의해 만들어진 컴퓨터 바이러스가 전세계적으로 기승을 부리는 시점에서 이에 대한 대책마련이 절실히 요구되는 실정입니다.

따라서 본 책자에서는 컴퓨터의 보급확산과 더불어 위협적 존재로 부각되고 있는 컴퓨터 바이러스의 유형 및 이에 대한 예방대책과 백신 프로그램을 소개하고자 자료를 모아 편집하였읍니다.

여러분들의 많은 참고가 되시길 바랍니다.

1990년 5월

電算擔當官 李 慶 義

☎ 735 - 5371 (交 310) 金 慶 蘭
720 - 3074

목 차

1. 개요

최근 들어 매스컴을 통하여 컴퓨터 바이러스(Computer Virus)라는 말이 컴퓨터를 다루는 사람들 뿐만 아니라 일반인들에게도 많이 알려지게 되었다. 하지만 컴퓨터 바이러스에 대하여 잘못된 생각을 가지고 있는 사람들이 의외로 많은 것같다. 컴퓨터 바이러스를 잘못 이해하고 있는 사람들은 크게 두 부류로 나누어 생각 할 수 있다. 한부류의 사람들은 컴퓨터를 사용하는 사람들이 감염되는 질환의 일종으로 생각하고, 또 다른 부류의 사람들은 이것이 컴퓨터의 내부에 사는 미생물로서, 전원을 끄더라도 계속 존재하는 것이라고 생각한다. 이렇게 오해가 생긴 것에 대해서는 여러가지 원인이 있을 수 있겠지만 가장 큰 이유중의 하나는 바이러스라는 명칭에서 비롯된 것 같다.

컴퓨터 바이러스란 컴퓨터를 다루는 사람들에게 감염되는 질환이 아니라 컴퓨터를 동작시키는 하나의 프로그램이다. 우리가 사용하는 대부분의 프로그램들이 사용자들이 원하는 바람직한 기능을 가진 것에 비하여 , 컴퓨터 바이러스 프로그램들은 바람직하지 않은 기능을 가지고 있는 것이다. 예를 들면, 컴퓨터의 속도를 떨어뜨리거나, 데이타를 파괴하고, 디스크를 초기화시키는 등의 원하지 않는 기능을 수행한다. 바이러스라는 이름은 컴퓨터 바이러스가 실제의 생물학적인 바이러스처럼 발견하기 어렵고, 자기자신을 복제하고, 전염성이 있고,특정 대상만 공격하고, 예방이 가능하다는 점에서 불여진 명칭이다. 그래서 컴퓨터 바이러스를 예방, 치료하는 프로그램도 Doctor, Vaccine(예방주사), Syringe(주사기) 등의 의학 용어를 많이 사용한다.

수년전부터 전문가들이 컴퓨터 바이러스 프로그램의 출현 가능성과 그것의 가공할 위험성을 경고하고 이에 대한 대응책 수립을 주장하였으나 대부분 이와 같은 예측을 안이하게 생각하였고 극소수 사람에게만 관심의 대상이 되어 왔다. 미국의 CVIA(컴퓨터 바이러스 산업협회)에서 조사한 통계에 의하면 최근까지 발견, 확인된 바이러스는 총 67종이나 된다고 한다. 또한 88년 7월에는 바이러스에 감염되는 컴퓨터 수가 월 약 6,000대 정도였으나, 89년에는 월 약 30,000대로 증가했고, 90년대는 더욱 증가하는 추세를 보일 것이라 밝혔다.

이와 같이 바이러스가 전세계적으로 확산되고 과거의 예측이 현실로 나타남에 따라 이제 바이러스 문제점은 극소수 관심가들의 영역을 벗어나 일반 사용자 및 기업 경영층까지 중대한 관심사가 되고 있다. 바이러스의 제조기술도 소수의 전문가에 국한되어 있던 것이 이제 널리 확산되어 있고, 프로그램이 짧기 때문에 약간의 시간과 능력만으로도 쉽게 만들 수 있다.
또한, 신종 바이러스는 자기 자신을 암호화해서 프로그램 내에 숨는 등 종래의 바이러스에 없는 고도의 기술을 활용하고 있으므로 점점 더 대책이 어렵게 되고 있다.

이러한 바이러스 제조자에 대해서는 여러가지 이야기가 있지만, 추측으로는 컴퓨터에 광적인 열정과 자기 성취감에 사로잡힌 컴퓨터 해커(hacker)들과, 작업 중 실수로 바이러스 프로그램을 이식한 아마츄어 프로그램 개발자, 마지막으로 자기가 개발한 소프트웨어를 일반 사용자가 불법으로 복사하여 사용하지 못하도록 비밀리에 유포 시키는 소프트웨어 개발회사일 것이라고 추정하고 있다.

2. 역사

1950년대 말 : Logic bomb - 어떤 논리에 의해서 미리 설정한 조건(경과시간, 프로그램 실행횟수, 날짜 등)이 만족될 때 주어진 명령이 실행됨

1960년대 : Bomb - hacker들이 타인의 프로그램을 자신의 의도대로 수정

1970년대 말 : 일정기간의 잠복기를 가지고 전염성을 가짐
1980년대 초

1983년대 초 : Fredrick Cohen 박사가 'Computer Virus : Theory and Experiment' 라는 논문에서 컴퓨터 바이러스라는 명칭 처음 사용

1988년대 초 : 국내에서 컴퓨터 바이러스 소개 - Brain virus ((C) brain)

1988년대 중 : 'TIME'지에 컴퓨터 바이러스 소개 (9월 26일자)

3.컴퓨터 바이러스의 정의 및 분류

컴퓨터 바이러스의 정의 및 분류는 아직도 확실히 정립되어 있지 않으나, 대부분 정의는" 컴퓨터를 동작시키는 기본 소프트웨어에 몰래 들어가 시스템 자원이나 사용자의 프로그램및 화일을 파괴 또는 운영에 제한을 가하며 같은 기종의 컴퓨터나 망을 통하여 자료를 복사하거나 공유할 경우 그 컴퓨터의 디스크나 디스켓을 감염 시키는 프로그램이다. "라고 말하고 있다.

바이러스 대책은 속수무책이지만 감염된 바이러스 종류를 식별하는 백신프로그램이 등장하고 미국 기업에서는 바이러스 감염방지를 위해 컴퓨터 이용절차를 작성하는등 종합적인 바이러스 대책을 실시하기 시작했다.한편 국내에서는 88년 봄 Brain이라는 컴퓨터 바이러스가 발견되어 사회 전체에 큰 충격을 주게 되자, 안이한 태도를 보이던 기업들이 적극적으로 이문제점에 대해서 관심을 갖게되었다.

현재 국내에서 유행되고 있는 컴퓨터 바이러스는 얼마전 한동안 유행했던 Brain 바이러스외에 요즈음 한창 유행하고 있는 변종 Brain 바이러스, Jerusalem 바이러스-13일의 금요일 바이러스, Lbc 바이러스, Stoned 바이러스, Sunday바이러스, 1701 바이러스(1704 Cascade), Pingpong 바이러스등이 있다.

이와 같은 컴퓨터 바이러스의 확산은 정보산업 발전에 막대한 영향을 끼치게 될 것으로 보이며, 이것을 방지할 목적으로 디스켓을 이용한 소프트웨어의 교환이나 정보통신망을 이용한 정보교환등 사용자들간의 자유로운 정보의 흐름을 통제하는 것, 또한 모든 정보산업의 비용증가를 유발시켜 정보산업 발전에 커다란 장애 요인으로 등장하게 될 것이다.

4. 컴퓨터 바이러스 의 변화 추세

초기의 바이러스는 소수에 의해 악의가 없이 개발되어 왔으나 현재는 바이러스 프로그램이 짧고 약간의 능력과 시간이 있으면 쉽게 개발할 수 있고 기존의 바이러스 종류를 변형시킬 수 있으므로 다수의 사람에 의해 유포되고 있으며, 공격 대상 또한 특정 업체 및 시스템을 목표로 하고 있다. 바이러스 변화를 단계별로 분류하여 살펴보면 아래 그림과 같다.

단 계	제 1 단 계	제 2 단 계	제 3 단 계
시 기	1987년 ⇒	88년후반 ⇒	90년대
형 태	단 순	복 잡	특정대상 공격
특 징	- 수법이 단순 - 단순히 재미로 바이러스를 만듬	- 피해를 주는 방법 침입 수법이 가공 - 악의를 가진자가 바이러스를 개발	- 어느 특정의 Application 언어를 목표로 공격 - 바이러스 작성자는 특정의 기업에 악의를 가진 사람
해 당 바이러스	- 대부분 바이러스 (Brain, 예루살렘 등)	- 1701 바이러스 - FU Manchu 바이러스	- dBASE 바이러스
대 책	- 백신으로 진단 가능	- 백신으로 진단 가능	- 백신으로 진단 가능

5. 국내외 바이러스 피해 현황

5.1. 국내 바이러스 피해 실태

가. 현재 운용중인 국내 전자게시판(BBS)을 보면 이용자들의 대부분이 한두번이상 바이러스에 감염되어 하드디스크의 중간 데이타를 잃어 버린 경험이 있는 것으로 나타남.

나. 청계천 세운상가의 경우는 바이러스에 감염된 줄도 모르고 Diskette을 배포하여 PC 구입자에게 난처한 경우가 있었다고 함.

다. 국내에서 주로 발견되는 바이러스는 Lbc바이러스, 이스라엘 바이러스, 신종 Brain 바이러스, Sunday 바이러스, Stoned 바이러스, 1701 바이러스 등이 있음.

5.2. 해외 바이러스 피해 실태

한달에 30,000대의 PC가 바이러스에 감염되었다. 신종 바이러스만이 아니고 종래부터 존재하고 있는 바이러스도 계속해서 피해를 발생시키고 있다는 사례가 보고되고 있다. 특히 87년에 발견된 이스라엘 바이러스는 아직도 감염 사례가 많다. 매우 최근의 예로서 실리콘 밸리에 있는 브마이즈 엘렉트로닉스라는 VAR(부가 가치 재판매)업자가 사내의 컴퓨터 시스템이 이 이스라엘형으로 감염되어 고객에게 바이러스가 감염된 시스템을 배포한 사건이 일어났다.

신.구 바이러스에 의한 사건은 감염된 기계댓수만 보아도 88년에 비교해 5배로 상승하고 있으며, 바이러스에 감염된 기계댓수는 CVIA가 미국내에서 조사한바에 따르면 작년 7월은 월 6,000대이고, 현재는 월 30,000대에 이르고 있다.

6.바이러스 유형 및 특성

6.1 Ross Greenberg 분류(유명한 백신 프로그램인 Flu-Shot+의 저작자)

가. 벌레(Worm) 프로그램

1) 컴퓨터내의 다른 시스템에는 직접적인 영향을 미치지 않음
2) 단순히 기억장소내에서 자기자신을 계속 복사시키는 프로그램
3) 다른 시스템에 직접적인 영향을 미치지 않는다는 점에서 '트로이 목마 프로그램'과 다름
4) 다른 프로그램내에 포함되지 않는다는 점에서 '컴퓨터 바이러스'와 다름

나. 트로이 목마(Trojan Horse) 프로그램

1) 고의적으로 사용자가 모르는 다른 기능을 프로그램 내에 포함 시킴
2) 증식하지 않는다는 점에서 '벌레프로그램'과는 다름
3) 다른 프로그램내에 포함되지 않는다는 점에서 '컴퓨터 바이러스'와 다름
4) 고의적으로 포함되었다는 점에서 프로그램의 버그와 다름

다. 컴퓨터 바이러스 (Computer Virus)

1) 트로이 목마 프로그램의 특별한 형태
2) 운영체제나 다른 프로그램의 내부에 자기자신을 포함(감염)시키는 프로그램을 말함
3) 시스템에 직접적인 영향을 미친다는 점에서 '벌레프로그램'과 다름.
4) 이 프로그램이 공격하는 형태
   - FAT(File Allocation Table) 공격
   - 0 섹터 즉,부트 섹터 공격
   - 가장 심각한 형태로 하드디스크를 초기화

6.2 컴퓨터 바이러스 프로그램 분류

89년 여름까지 발견된 컴퓨터 바이러스 56종(CVIA의 조사에 의함)을 분류 기준에 따라 원본 바이러스와 변형 바이러스를 열거하고 각각의 특성을 정리하였다.

Virus	Original Virus명	파생한 Virus 명	특 징
boot sector /partition record virus	Alameda Virus (별명:이이르. 메리트, 북경, seoul)	Alameda-B (새크라멘트Virus) Alameda-C Sfvirus golden gate virus (500 virus) golden gate-B golden gate-C (마자트란바이러스) golden gate-D	-boot sector 감염 -original은 시스템에 피해를 주지 않음 -Alameda-C는 100회 감염하면 floppy를 초기화시킴 -golden gate는 C drive를 초기화 시킨다 -발견장소 : 캘리포니아주 Merit대학 -발견시기 : 87 년
	Brain virus (파키스탄brain, 베이지트 brain)	brain-B(brain-HD, harddisk brain 휴스턴 brain) brain-C clone virus 슈 virus (UIUC virus) 슈 virus-B clone-B 죠크 virus 타스 슈virus	-floppy의 boot sector에 감염 -길이는 최대 3K byte -원래의 boot sector를 별도 장소에 옮긴다. -boot sector의 검사를 위해 백신이 들어가면 감염된 sector가 아닌 원래의 sector를 검사하도록 하므로 감염을 검출하기 어렵다 -발견장소 : 키스탄레이호 -발견시기 : 86년 1월
	Italian virus (bouncing ball 베라 크루즈)	Italian-B	-floppy의 boot sector감염 -화면에서 돌면서 움직이는 점(dot)이 발생 -재 boot로 멈출 수 있음 -발견장소 : 불명 -발견시기 : 88년 3월
	New Zealland (스텐드바이러스)	뉴질런드 B 뉴질런드 C	-floppy boot sector에 감염 -boot의 8회째마다 '당신의 컴퓨터는 취해있다' 라는 message가 나온다 -발견장소 :뉴질런드 베린트 -발견시기 : 88년 초
	search (덴츠크, 베네즈 에러)	search-HD search B sys virus sys B sys C	-boot sector에 감염 -FAT에 Write되어 read(write) Error 발생 -sys Virus는 display Code를 바꿔 써넣어서 sys program을 실행 불가능하게 함 -발견장소 및 시기 : 불명

command.com virus	Lehigh	Lehigh2	-command.com 화일에 감염 -매우 넓게 감염되어 있는 바이러스 -4번째 감염이면 disk boot sector, root directory, user 화일 일부를 파괴함 -발견장소 : 하와이 대학 -발견시기 : 87년 말
object file virus (memory에 단기체재)	DOS-62 (유네스코 바이러스)	62-B	-.com 화일에 감염 -감염된 화일 실행중 Random하게 시스템을 재 boot함 -발견장소 : 모스크바 -발견시기 : 88년 7월 말
	13일의 금요일 (comvirus, 512virus)	13일의 금요일-B 13일의 금요일-C	-memory에 상주하지 않고, 화일에 감염 -13일의 금요일이 되는 날 프로그램이 실행되면 Host 내의 프로그램을 모두 소거시킨다 -발견장소 : 남아프리카 -발견시기 : 87년
	Austria virus (648 virus)	Austria-B	-com에 감염하여 화일 크기를 648byte분 증가 시킨다. -오스트리아-B에서는 때때로 화일이 실행 불가능하게 된다 -발견장소 : 런던 -발견시기 : 88년 가을
	405 virus		-.com화일에 감염 -화일을 파괴하고 45 Byte의 바이러스로 바뀌게 됨 -발견장소및 시기 : 불명
object file virus (memory상주)	Jerusalem virus (이스라엘 13일의 금요일-위에 기술한 것과는 별도임, pro)	Jerusalem-B Jerusalem-C (뉴예루살렘) black hall (러시아 바이러스) Jerusalem-D Jerusalem-E century virus (오레곤 바이러스) century-B	-메모리에 상주하여 .com과 .exe를 감염시킴 -13일의 금요일이 되면 그날에 실행된 프로그램 모두를 소거함 -예루살렘-D는 90년 이후에 활동 개시 -Century는 2000년 1월 1일에 활동을 시작 한다. -발견장소 : 예루살렘 헤브류대학 -발견시기 : 87년 가을

	4월 1일	4월 1일-B	-.com 화일에 감염 -감염된 화일을 실행하면 '4월 1일. 하하하 너는 바이러스를 갖고있다' 라는 메세지를 표시한다. -발견장소, 시기 : 불명
	Cascade virus (1701, 폴링 디아즈, Autumn Lives)	Cascade-B 1704(black jack) 1704-B 1704-C 1704-D	-.com 화일에 감염 -1701 byte분 증가시 원래는 utility인 체하여 기계에 들어가 화면에 표시한 문자를 낙하 시키는 '트로이 목마' -암호화 수법을 이용하는 등 종래의 바이러스에 비교하여 고도의 기술을 사용 -발견장소 : 불명 -발견시기 : 87년 말
	dBASE virus		-com,exe 감염.Ashton tate의 'dBASE' 화일을 목표로 한다. -감염한지 90일만에 virus는 Root directory와 FAT의 Data를 처리함 -발견장소, 시기 : 불명
	Gropax virus (music virus)		-.com 화일에 감염 -단지 속성, 화일의 크기 (61980 byte 이상)에 의해 감염되지 않는 화일도 있음 -활동 개시하면 3종류의 멜로디를 반복하여 7분간 연주 -발견장소, 시기 : 불명

6.3. 컴퓨터 바이러스 프로그램 목록

IBM PC 및 호환기종에 감염되는 바이러스의 특징을 가장최근에 발견된 순서로 열거하면 다음과 같다.

VIRUS CHARACTERISTICS LIST 2.7V57 (Copyright 1989, McAfee Associates)

Fixed Disk Partition Table 감염
Fixed Disk Boot Sector 감염
Floppy Diskette Boot 감염
Overlay Files 감염
EXE Files 감염
COM Files 감염
COMMAND.COM 감염
RAM 상주
자신을 암호화

바이러스명	복 구	V V V V V V V V V V	사이즈증가	파 괴
Joker	CleanUp	. x x x		O,P
Icelandic-3	CleanUp	. x . . x	853	O,P
Virus-101	CleanUp	x x x x x x x . .	2560	P
1260	CleanUp	x . . x	1260	P
Perfume	CleanUp	. . . x	765	P
Taiwan	CleanUp	. . . x	708	P
Chaos	MDISK	. x . . . . x x .	N/A	B,O,D,F
Virus-90	CleanUp	. x . x	857	P
Oropax	CleanUp	. x . x	2773	P,O
4096	CleanUp	. x x x x x . . .	4096	D,O,P,L
Devil's Dance	CleanUp	. x . x	941	D,O,P,L
Amstrad	CleanUp	. . . x	847	P
Payday	CleanUp	. x . x x x . . .	1808	P
Datacrime II-B	CleanUp	x . x x x	1917	P,F
Sylvia/Holland	CleanUp	. x . x	1332	P
Do-Nothing	CleanUp	. . . x	608	P
Sunday	CleanUp	. x . x x x . . .	1636	O,P
Lisbon	CleanUp	. . . x	648	P
Typo/Fumble	CleanUp	. x . x	867	O,P
dBASE	CleanUp	. x . x	1864	D,O,P
Ghost Boot Versio	MDISK	. x . . . . x x .	N/A	B,O
Ghost COM Version	CleanUp	. . . x	2351	B,P
New Jerusalem	CleanUp	. x . x x x . . .	1808	O,P
Alabama	CleanUp	. x . . x	1560	O,P,L
Yankee Doodle	CleanUp	. x . x x	2885	O,P
2930	CleanUp	. x . x x	2930	P
Ashar	CleanUp	. x . . . . x . .	N/A	B
AIDS	CleanUp	. . . x	Overwrites	
Disk Killer	CleanUp	. x . . . . x x .	N/A	O,P,D,F
1536/Zero Bug	CleanUp	. x . x	1536	O,P
MIX1	CleanUp	. x . . x	1618	O,P
Dark Avenger	CleanUp	. x x x x x . . .	1800	O,P,L
3551/Syslock	CleanUp	x . . x x	3551	P,D
VACSINA	CleanUp	. x . x x x . . .	1206	O,P

바 이 러 스 명	복 구	↓ V	↓ V	↓ V	↓ V	↓ V	↓ V	↓ V	↓ V	↓ V	사이즈증가	파 괴
Ohio	MDISK	.	x	.	.	.	.	x	.	.	N/A	B
Typo(Boot Virus)	MDISK	.	x	.	.	.	.	x	x	.	N/A	O,B
Swap/Israeli Boot	MDISK	.	x	.	.	.	.	x	.	.	N/A	B
1514/Datacrime II	CleanUp	x	.	.	x	x	.	.	.	.	1514	P,F
Icelandic II	CleanUp	.	x	.	.	x	.	.	.	.	661	O,P
Pentagon	MDISK	.	.	.	.	.	.	x	.	.	N/A	B
3066/Traceback	M-3066	.	x	.	x	x	.	.	.	.	3066	P
1168/Datacrime-B	CleanUp	x	.	.	x	.	.	.	.	.	1168	P,F
Icelandic	CleanUp	.	x	.	.	x	.	.	.	.	642	O,P
Saratoga	CleanUp	.	x	.	.	x	.	.	.	.	632	O,P
405	CleanUp	.	.	.	x	.	.	.	.	.	Overwrites	
1704 Format	CleanUp	x	x	.	x	.	.	.	.	.	1704	O,P,F
Fu Manchu	CleanUp	.	x	.	x	x	x	.	.	.	2086	O,P
1280/Datacrime	CleanUp	x	.	.	x	.	.	.	.	.	1280	P,F
1701/Cascade	CleanUp	x	x	.	x	.	.	.	.	.	1701	O,P
1704/CASCADE-B	CleanUp	x	x	.	x	.	.	.	.	.	1704	O,P
Stoned/Marijuana	CleanUp	.	x	.	.	.	.	x	.	x	N/A	O,B,L
1074/CASCADE	CleanUp	x	x	.	x	.	.	.	.	.	1704	O,P
Ping Pong-B	CleanUp	.	x	.	.	.	.	x	x	.	N/A	O,B
Den Zuk	MDISK	.	x	.	.	.	.	x	.	.	N/A	O,B
Ping Pong	CleanUp	.	x	.	.	.	.	x	.	.	N/A	O,B
Vienna-B	CleanUp	.	.	.	x	.	.	.	.	.	648	P
Lehigh	CleanUp	.	x	x	.	.	.	.	.	.	Overwrites	P,F
Vienna/648	M-VIENNA	.	.	.	x	.	.	.	.	.	648	P
Jerusalem-B	CleanUp	.	x	.	x	x	x	.	.	.	1808	O,P
Yale/Alameda	CleanUp	.	x	.	.	.	.	x	.	.	N/A	B
Friday 13th COM	CleanUp	.	.	.	x	.	.	.	.	.	512	P
Jerusalem	CleanUp	.	x	.	x	x	x	.	.	.	1808	O,P
SURIV03	CleanUp	.	x	.	x	x	x	.	.	.		O,P
SURIV02	CleanUp	.	x	.	.	x	.	.	.	.	1488	O,P
SURIV01	CleanUp	.	x	.	x	.	.	.	.	.	897	O,P
Pakistani Brain	CleanUp	.	x	.	.	.	.	x	.	.	N/A	B
Lbc	V2PLUS	.	x	.	.	.	.	x	.	.	N/A	B,O,L

☞ 범례

1. 파괴필드 : B - Corrupts or overwrites Boot Sector
   O - Affects system run-time operation
   P - Corrupts program or overlay files
   D - Corrupts data files
   F - Formats or erases all/part of disk
   L - Directly or indirectly corrupts file linkage

2. 사이즈 증가 : The length, in bytes, by which an infected program or overlay file will increase

3. 특징 : x - Yes
   . - No

4. 복구 : SCAN/D - VIRUSCAN with /D option
   SCAN/D/A - VIRUSCAN with /D and /A options
   MDISK/P - MDISK with "P" option
   All others - the name of disinfecting program

6.4. 네트워크 바이러스

가. 크리스마스 메시지 바이러스(X-mas Message Virus)

벌레 프로그램의 일종으로 시스템 메모리 내에 자신을 복제하여 메모리를 전부 채우고 그 시스템 네트워크에 관련되어 있는 모든 터미날들에 퍼트려서 터미날 사용자들이 전자 사서함을 보려하면 크리스마스 축하 메시지와 트리가 출력된다. '87년말 서독에서 발생하여 IBM의 국제 통신 네트워크에 연결된 약 350,000대의 터미날이 감염되었다. 이 바이러스는 데이타에 손상을 주지는 않았지만 네트워크의 운용 속도를 크게 떨어뜨려 그 위력이 네트워크에까지 미칠 수 있다는 것을 보여 주었다.

나. 버클리 유닉스 바이러스(Berkeley Unix Virus)

'88년 11월 미 국방성의 네트워크들인 ARPANET, MILINET, NSF 등에 침입하여 핵무기 연구기관, MIT, 코넬대학, NASA, 하바드대학, 스텐포드 대학으로 확산되어 여기에 연결되어 있는 전 컴퓨터의 10%를 감염시켰다.

UNIX의 버클리 버전에만 감염되며 전자 사서함을 통하여 다른 시스템을 감염시킨다. 이 바이러스의 특징은 기존의 MS-DOS 바이러스가 사용자의 'DIR'이나 'TYPE'등의 명령을 줄때에만 다른 화일이나 디스크를 향해 동작시키는데 비해 바이러스 스스로 상대방의 암호를 알아내면서 시스템을 감염시킨다.

7. 바이러스별 분석

7.1. Lbc 바이러스

VIRUS 명	Lbc Virus
파생된 VIRUS 명	파생된 바이러스가 많음
출 처	미 상
전염기종	IBM PC및 호환기종
전염종류	부트 섹터 감염자
비 고	- 현재 미국이나 일본등 해외에서는 발견되었다는 보고 없음 - 최근국내에 가장 널리퍼진 악성바이러스로 피해가 더욱 확산중 - 변종이 상당히 많음 - '퍼스널 컴퓨터' 89년 10월 호에 상세한 소스 분석

7.1.1. 특 징

가. 0섹터의 내용이 11섹터(트랙:0, 면:1, 섹타:3)에 복사되어 있음.

나. Lbc 바이러스자신이 0섹터(트랙:0, 면:0, 섹타:1)에 들어 있음.

다. 디스크 Map을 조사해 보면 'bad cluster'가 나타나지 않음.

라. 메모리 크기를 2K 감소

7.1.2. 감염경로

가. 감염된 디스크로 부팅하면 바이러스 프로그램이 메모리에 상주

나. 상주후 INT 13h을 수행시 감염시킴

7.1.3. 감염증상

가. C: 드라이브로 부팅이 안됨

나. FDD에는 영향을 미치지 않으나 단지 이상한 소리가 좀 나거나 갑자기 읽기가 안되는 경우가 발생할 수 있음

7.1.4. 감염여부 검진

가. Debug 이용

```
A>또는 C>에서 debug <CR>
-l100 0 0 1 <CR>
-d  <CR>                                    ....4.Eh3.....
-d  <CR>
-d  <CR>                                    ..   vires pr
                                            ogram message
                                            Njh to LBC
```

이렇게 해보면 우측 텍스트부근에 위와 같이 ...Eh.... 문자가 나타나면 감염된 것임.

(원래는 MS-DOS로 나타나거나 Pctools등 포멧한 디스켓이 나타남)

나. Utility이용 (PCTOOLS,NORTON,MACE)

View Edit기능으로 들어가 Boot Sector에서 Debug에서와 같은 메세지가 나타나면 바이러스에 감염된 것임.

7.1.5. 복구방법

가. 감염된 디스켓 복구방법

(1) 감염되지 않는 디스켓을 A:드라이브에 넣고 boot하거나 C:드라이브에서 boot한다.

(2) B:드라이브에 새로운 디스켓을 넣고 초기화한 다음 A:드라이브에 감염된 디스켓을 넣고 화일단위로 복사를 하면 복구 됨

(주의) 'DISKCOPY'프로그램은 절대 사용치 말것

(3) 복사한 다음에는 바로 프로텍트를 붙일것.

나. 하드 디스크 복구방법

(1) Master Boot sector 복구

- Disk Utility를 이용하여 같은 DOS Version, Hard Disk의 Master Boot Sector를 복사
- 'fdisk'로 파티션을 다시함(감염전과 똑 같이)

(2) Boot Sector 복구

- Disk Utility를 이용하여 같은 DOS Version의 Boot Sector를 복사
  - o. PCTOOLS : Sector 단위 복사
  - o. NORTON : Sector 단위 복사
- NDD(Norton Disk Doctor)의 Make Boot disk 이용

(3) FAT 복구

- Disk Utility(pctools, Norton 등)로 FAT에 바이러스가 복사해 둔 프로그램 부분을 꺼내와 FAT 복사본을 Sector 단위로 그 위치에 복사
  - o. 즉, 논리 Sector 59를 논리 Sector 18에 복사
  - o. 단, FAT 복사본도 같이 오염되어 있으면 오염된 2 Sector에 해당되는 데이타는 복구할 방법이 없음
  - o. 거의 대부분을 회복시킬 수 있으나 일부는 잃어 버릴 수도 있음.

다. 복구 프로그램 이용

V2plus, Killer, Mdisk

7.1.6 예방대책

가. 디스켓의 바이러스 검사후 미감염 디스켓에는 write-protect

나. 외부로부터 온 디스켓은 부트디스켓으로 사용하지 말 것

다. 하드디스크 사용자는 절대 A: 에서 부트하지 말 것

라. 게임 디스켓은 거의 감염된 것으로 생각하고 대처할 것

7.1.7 Lbc 프로그램 분석

가. Source Dump 리스트 설명

이 리스트는 감염된 디스켓의 Boot Sector를 Dump한 것이다.

```
122D:0100  FA EB 05 90 34 12 45 68-33 C0 8E D8 8E D0 BC F0   ....4.Eh3.......
                                    바이러스 감염 스트링 →  --

122D:0110  02 70 00 D0 02 FD 02 00-09 00 02 00 00 00 00 00   .p..............
122D:0120  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 0F   ................
122D:0130  00 00 00 00 01 00 FA 33-C0 8E D0 BC 00 7C 16 07   .......3.....|..
122D:0140  BB 78 00 36 C5 37 1E 56-16 53 BF 2B 7C B9 0B 00   .x.6.7.V.S.+|...
122D:0150  FC AC 26 80 3D 00 74 03-26 8A 05 AA 8A C4 E2 F1   ..&.=.t.&.......
122D:0160  06 1F 89 47 02 C7 07 2B-7C FB 8A 16 FD 7D CD 13   ...G...+|....}..
122D:0170  72 66 A0 10 7C 98 F7 26-16 7C 03 06 1C 7C 03 06   rf..|..&.|...|..
122D:0180  0E 7C A3 3F 7C A3 37 7C-B8 20 00 F7 26 11 7C 8B   .|.?|.7|. ..&.|.
122D:0190  1E 0B 7C 03 C3 48 F7 F3-01 06 37 7C BB 00 05 A1   ..|..H....7|....
122D:01A0  3F 7C E8 94 00 B0 01 E8-A9 00 72 19 8B FB B9 0B   ?|........r.....
122D:01B0  00 BE D5 7D F3 A6 75 0D-8D 7F 20 BE E0 7D B9 0B   ...}..u... ..}..
122D:01C0  00 F3 A6 74 18 BE 76 7D-E8 61 00 32 E4 CD 16 5E   ...t..v}.a.2...^
122D:01D0  1F 8F 04 8F 44 02 CD 19-BE BF 7D EB EB A1 1C 05   ....D.....}.....
122D:01E0  33 D2 F7 36 0B 7C FE C0-A2 3C 7C A1 37 7C A3 3D   3..6.|...<|.7|.=
122D:01F0  7C BB 00 07 A1 37 7C E8-3F 00 A1 18 7C 2A 06 3B   |....7|.?...|*.;
122D:0200  7C 40 50 E8 4D 00 58 72-CF 28 06 3C 7C 76 0C 01   |@P.M.Xr.(.<|v..
122D:0210  06 37 7C F7 26 0B 7C 03-D8 EB D9 8A 2E 15 7C 8A   .7|.&.|.......|.
122D:0220  16 FD 7D 8B 1E 3D 7C EA-00 00 70 00 AC 0A C0 74   ..}..=|...p....t
122D:0230  21 B4 0E B3 FF CD 10 EB-76 69 72 73 65 20 70 72   !.......virse pr
                                    바이러스 감염 스트링 →  --------

122D:0240  6F 67 72 61 6D 20 20 20-6D 65 73 73 67 65 20 4E   ogram   messge N
                                    바이러스 감염 스트링 →  ----------------

122D:0250  6A 68 20 74 6F 20 4C 62-63 20 00 00 00 00 00 00   jh to Lbc ......
                                    바이러스 감염 스트링 →  ---------
```

7.2 Brain 바이러스

VIRUS 명	Brain Virus(파키스탄 Brain)
파생된 VIRUS 명	- (C) Brain - Brain-B - 슈 바이러스 - 베이지트 Brain - Clone Virus
출 처	1986년 6월 파키스탄의 Lahore, 두 형제(배시트와 암자드 알비)가 개발
전염기종	IBM PC 호환 기종
전염종류	부트 섹터 감염자
비 고	- 변종이 상당이 많고 국내에 가장 많이 확산 - '88. 7월호 '마이크로 소프트웨어'지에 상세한 소스 분석

7.2.1 특징

가. original 부트 섹터를 교체

나. original 부트 섹터를 다른 장소로 이동

다. 바이러스의 잔류자를 포함한 7개의 섹터를 추가

라. 바이러스 보호를 위해 모든 변경된 섹터들을 사용불가로 표시(연속된 3 클러스트)

마. 플로피 디스켓의 부팅영역 전염

바. 메모리 크기를 7K 감소

사. 하드 디스크는 감염 시키지 않음

☞ 변형 Brain 바이러스의 경우

가. 디스크상의 절대위치(Absolute sector # 656-661)에 바이러스가 전염

나. 그곳(전염위치)에 화일이 있거나 없거나 상관없이 전염

다. 볼륨라벨을 '(C) Brain'으로 바꾸지 않음

라. FAT(File Allocation Table)에 bad cluster marking을 하지 않음

마. 하드디스크 FAT의 전 Sector를 16 Sector 씩 Shift 시킴
(0 Sector를 16 Sector로, 1 Sector를 17로)

7.2.2 감염경로

가. 감염된 디스켓으로 부팅하면 바이러스 프로그램이 메모리에 상주

나. 상주후 INT 13h을 수행시 감염 시킴

7.2.3 감염증상

가. 'Copyright (C) BRAIN'이라는 라벨이 감염된 디스크에 표시됨

나. 재부팅 과정에서 속도가 느려짐

다. 단순 작업에도 플로피가 과도하게 작동

라. 일부 DOS 버전에서 프로그램 파괴

마. 인터럽트 벡터의 변경

☞ 변형 Brain 바이러스의 경우

가. 하드 디스크로 Booting이 안됨

나. 'DISKCOPY'프로그램이 작동이 안됨(DOS 파라메타 변경)

다. 데이타 디스크의 데이타가 이유없이 깨짐

라. 오락 프로그램의 화면이 깨짐

7.2.4 감염여부 검진

가. Debug 이용

A>또는 C>에서 debug <CR>

```
-1100 0 0 1 <CR>
-d <CR>
122d:0100 FA E9 4A 01 34 12 00 09    . . .        ..J.4..
  .   .                  -- --                  Welcome to the
  .   .                                         Dungeon
  .   .                                         (c) 1986 Brain.&
-d <CR>
```

이렇게 해보면 좌측 맨위 5번째 HEX값이 '34 12'로 나타나면 감염된 것임(원래는 MS-DOS로 나타나거나 PCTOOLS등 포멧한 디스켓이 나타남)

나. Utility 이용(PCTOOLS, NORTON, MACE)

View Edit기능으로 들어가 Boot Sector에서 Debug에서와 같은 메세지가 나타나면 바이러스에 감염된 것임.

☞ 변형 Brain 바이러스의 경우

가. 이러한 특징때문에 어지간한 판찰력을 갖추지 않는 한 변형 Brain을 발견하기는 쉽지가 않음

나. Brain 계통의 바이러스를 발견하는 제일 쉬운 방법은 주기억 장치의 크기가 줄어들었는가를 확인하는 것

- DOS의 CHKDSK,NORTON UTILITY등의 프로그램을 이용
- 주기억 장치의 크기가 DOS에 의해 633K byte로 표시되는 것을 확인

다. 실제로 Brain 계열에서는 7K byte의 주기억 장치를 점유함

7.2.5 복구방법

가. V2plus, MDISK 복구 프로그램 이용

나. DOS의 'SYS' 명령으로 boot sector를 재기록

다. utility로 볼륨 시리얼 라벨을 재생성(7개의 불량 섹터에 죽은 바이러스 그대로 존재)

☞ 변형 Brain 바이러스의 경우

가. 시중에 나와 있는 (c)Brain 원판 제거 프로그램들이 무리없이 작동

나. 변형 (c) Brain에 의해서 파괴된 데이타는 복구되지 않음

- 하드디스크 FAT의 전 sector를 16 sector씩 Shift시킨 변형 Brain일 경우는 Utility를 이용하여 다시 역순으로 16 sector를 0 sector로 , 17 sector를 1로, ... sector 단위로 복사를 하면됨. 그러나 끝부분에 있는 16 sector에 있는 데이타는 복구 불가능

다. write protect를 사용할 수 없는 데이타 디스켓의 경우

- 바이러스가 감염되는 절대 sector#656-#661(Cluster #324-#326)를 File Allocation Table에서 미리 Bad Cluster나 Allocated로 set하면 바이러스가 전염되는 위치에 데이타가 기록되는 것을 방지함으로써 귀중한 데이타의 손실을 사전에 막을 수 있음

7.2.6 예방대책

가. 출처 불명의 플로피 디스켓으로 부트하지 말것

나. 하드 디스크가 있으면 그것으로 부트

다. 모든 부트가능 디스켓에 write-protect

☞ 변형 Brain 바이러스의 경우

가. 오염되지 않은 DOS 디스켓에 write protector만 붙여서 사용하면 감염을 완전히 막을 수 있음

나. 절대 sector 656 뿐만 아니라 다른 위치에 전염되는 바이러스가 앞으로 만들어지거나 아니면 이미 만들어졌을 가능성이 있기 때문에 상당한 주의가 필요

다. 백신 프로그램을 이용하여 수시로 검진한다

7.2.7 Brain 프로그램 분석

가. 변형 Brain의 메모리 덤프(dump) 예

이 리스트는 감염된 디스켓의 Boot Sector를 덤프한 것이다.

```
20CD:0000  FA E9 4A 01 34 12 00 09-20 01 06 20 00 00 00 00   ..J.4... .. ....
                     -- --   ← 바이러스 감염 스트링

20CD:0010  57 65 6C 63 6F 6D 65 20-74 6F 20 74 68 65 20 20   Welcome to the
20CD:0020  44 75 6E 67 65 6F 6E 20-20 20 20 20 20 20 20 20   Dungeon
20CD:0030  28 63 29 20 31 39 38 36-20 42 72 61 69 6E 17 26   (c) 1986 Brain.&
20CD:0040  20 41 6D 6A 61 64 73 20-28 70 76 74 29 20 4C 74    Amjads (pvt) Lt
20CD:0050  64 20 20 20 56 49 52 55-53 5F 53 48 4F 45 20 20   d   VIRUS_SHOE
20CD:0060  52 45 43 4F 52 44 20 20-20 76 39 2E 30 20 20 20   RECORD   v9.0
20CD:0070  44 65 64 69 63 61 74 65-64 20 74 6F 20 74 68 65   Dedicated to the
20CD:0080  20 64 79 6E 61 6D 69 63-20 6D 65 6D 6F 72 69 65    dynamic memorie
20CD:0090  73 20 6F 66 20 6D 69 6C-6C 69 6F 6E 73 20 6F 66   s of millions of
20CD:00A0  20 76 69 72 75 73 20 77-68 6F 20 61 72 65 20 6E    virus who are n
20CD:00B0  6F 20 6C 6F 6E 67 65 72-20 77 69 74 68 20 75 73   o longer with us
20CD:00C0  20 74 6F 64 61 79 20 2D-20 54 68 61 6E 6B 73 20    today - Thanks
20CD:00D0  47 4F 4F 44 4E 45 53 53-21 21 20 20 20 20 20 20   GOODNESS!!
20CD:00E0  20 42 45 57 41 52 45 20-4F 46 20 54 48 45 20 65    BEWARE OF THE e
20CD:00F0  72 2E 2E 56 49 52 55 53-20 20 3A 20 5C 74 68 69   r..VIRUS  : \thi
20CD:0100  73 20 70 72 6F 67 72 61-6D 20 69 73 20 63 61 74   s program is cat
20CD:0110  63 68 69 6E 67 20 20 20-20 20 20 70 72 6F 67 72   ching      progr
20CD:0120  61 6D 20 66 6F 6C 6C 6F-77 73 20 61 66 74 65 72   am follows after
20CD:0130  20 74 68 65 73 65 20 6D-65 73 73 61 67 65 73 2E    these messages.
20CD:0140  C2 88 16 3B 7C 33 D2 F7-36 1A 7C 88 16 2A 7C A3   ...;|3..6.|..*|.
//////////////////////////////////////////////////////////   ////////////////
20CD:0350  EB 25 90 03 00 20 28 63-29 20 31 39 38 36 20 42   .%... (c) 1986 B
20CD:0360  72 61 69 6E 20 26 20 41-6D 6A 61 64 73 20 28 70   rain & Amjads (p
20CD:0370  76 74 29 20 4C 74 64 E8-AD 00 A1 BE 06 3D FD FF   vt) Ltd......=..
```

7.3 Jerusalem 바이러스

VIRUS 명	Jerusalem Virus(Israeli)
파생된 VIRUS 명	- Jerusalem-B Virus - Jerusalem-C Virus - Jerusalem-D Virus - Jerusalem-E Virus - Century Virus - Century-B Virus - 13일의 금요일 바이러스 - black hall - Hebrew Virus - comvirus
출 처	1987. 12 Jerusalem의 Hebrew 대학
전염기종	IBM PC 및 호환 기종
전염종류	일반적인 애플리케이션 감염자
비 고	.EXE 화일을 되풀이 하여 감염시키는 버그가 있어 .EXE 화일 크기를 메모리에 적재 불가능할 때까지 증가시킴. 이 문제는 미상의 해커에 의해 최신 버전에서는 제거

7.3.1 특징

가. .COM 또는 .EXE 프로그램을 감염

나. 감염된 프로그램 크기를 1808 바이트 증가시킴

다. 감염된 프로그램은 변형되어 메모리에 상주

라. 감염된 시스템에서 실행화일을 수행시킬때 그 프로그램에 감염

마. 플로피나 하드 디스크가 감염가능

바. INT 13h, INT 8h번을 가로챔

7.3.2 감염경로

가. 감염된 .EXE 및 .COM 사용시 메모리 상주

나. 이후 수행시키는 화일마다 화일 크기를 증가(1808 byte) 시키면서 감염

7.3.3 감염증상

가. 일반적인 증상

- 시스템의 일반적인 속도 저하
- 사용가능 시스템 메모리 용량이 감소
- .COM 화일들은 한번만 감염(화일 크기 증가 1808 byte)
  : 앞부분에 감염
- .EXE 화일들을 계속해서 감염(화일 크기가 수행시 마다 1808 byte 증가)
  : Header 화일을 변경하고 뒷부분만 감염

나. 13일의 금요일 증상

- 수행시키는 프로그램을 삭제
- 일부 버전은 하드디스크상의 모든 데이터 파괴

7.3.4 감염여부 검진

가. Viruscan 프로그램 이용

- SCAN 화일명

☞ 사용예

```
[C:/] scan a:
SCAN 1.7V50 Copyright 1989 by McAfee Associates.
Scanning for 52 viruses.
Scanning A:/CAT.EXE
Found Jerusalem Virus Version B

Disk A: contains 1 directories and 26 files.
1 file contains a virus.
```

나. Disk Utility 이용

- 화일내 "MsDos" 문자열이 3번 이상 나타나면 감염

다. Debug 이용

7.3.5 복구방법

가. 삭제된 화일 복구

- Disk Utility 이용하여 복구(화일 UNDELETE 기능 이용)

나. 감염된 화일 복구

- 감염된 실행가능 화일은 감염되지 않은 프로그램으로 교체
- Viruscan 프로그램으로 복구(SCAN /D/A)
- V2PLUS 프로그램으로 복구

☞ 사용예

```
[C:/]v2plus a:

VACCINE II puls (Version 1, 2A)

(c) Copyright 1989 by Ahn Cheolsoo

System is Safe.
Insert a disk in drive and press<Enter>

Boot sector is Safe.
Searching files for viruses...
CAT.EXE is infected with Jerusalem-B VIRUS ----> CURED

Test another disk (Y/N) ?
```

7.3.6 예방대책

가. 출처 불명의 소스로부터의 프로그램은 실행시키지 말 것

나. 실행가능 코드를 내포한 디스크는 교환하지 말 것

다. 메모리의 배치와 프로그램 화일 크기를 감시할 것

7.3.7 Jerusalem 프로그램 분석

가. Source Dump 리스트 설명

이 리스트는 감염된 화일을 Dump한 것이다

```
122D:0100  FA EB 05 90 34 4D 73 44-6F 73 8E D8 8E D0 BC F0   ....4MsDos......
                                        바이러스 감염 스트링 → -----

122D:0110  02 70 00 D0 02 FD 02 00-09 00 02 00 00 00 00 00   .p..............
122D:0120  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 0F   ................
122D:0130  00 00 00 00 01 00 FA 33-C0 8E D0 BC 00 7C 16 07   .......3.....|..
//////////////////////////////////////////////////////////   ////////////////
122D:06F0  BB 78 00 36 C5 37 1E 56-16 53 BF 2B 7C B9 0B 00   .x.6.7.V.S.+|...
122D:0700  FC AC 26 80 3D 00 74 03-26 8A 05 AA 8A C4 E2 F1   ..&.=.t.&.......
122D:0710  06 1F 89 47 02 4D 73 44-6F 73 8A 16 FD 7D CD 13   ...G.MsDos...}..
  바이러스 감염 스트링 →  -----

122D:0720  72 66 A0 10 7C 98 F7 26-16 7C 03 06 1C 7C 03 06   rf..|..&.|...|..
122D:0730  0E 7C A3 3F 7C A3 37 7C-B8 20 00 F7 26 11 7C 8B   .|.?|.7|. ..&.|.
122D:0740  1E 0B 7C 03 C3 48 F7 F3-01 06 37 7C BB 00 05 A1   ..|..H....7|....
//////////////////////////////////////////////////////////   ////////////////
122D:07D0  3F 7C E8 94 00 B0 01 E8-A9 00 72 19 8B FB B9 0B   ?|........r.....
122D:07E0  00 BE D5 7D F3 A6 75 0D-8D 7F 20 BE E0 7D B9 0B   ...}..u... ..}..
122D:07F0  00 F3 A6 74 18 BE 76 7D-E8 61 00 32 E4 CD 16 5E   ...t..v}.a.2...^
122D:0800  1F 8F 04 8F 44 02 CD 19-BE BF 7D EB EB A1 1C 05   ....D.....}.....
122D:0810  B4 4C CD 21 4D 73 44 6F-73 3C 7C A1 37 7C A3 3D   .L.!MsDos<|.7|.=
           ---------- -------------- 바이러스 감염 스트링 →  -----
```

7.4 Stoned 바이러스

VIRUS 명	Stoned Virus(Marijuana)
파생된 VIRUS 명	
출 처	
전염기종	IBM PC 및 호환 기종
전염종류	부트섹터 감염자
비 고	최근 국내에서 발견된 악성 바이러스로 피해가 더욱 확산중

7.4.1 특징

가. 디스켓일 경우 : 0 섹터의 내용이 tr:0 he:1 se:3에 복사되어 있음

나. 하드디스크일 경우 : 0 섹터의 내용이 tr:0 he:0 se:7에 복사되어 있음

다. Stoned Virus 자신이 0섹터에 들어 있음

라. 메모리 크기를 2K 감소

7.4.2 감염경로

가. 감염된 디스크로 부팅하면 바이러스 프로그램이 메모리에 상주

나. 상주후 INT 13h을 수행시 감염시킴

7.4.3 감염증상

가. 디스켓일 경우

- 0 섹트의 내용이 ROOT DIR 부분(tr:0 he:1 Se:3)에 복사되어 있어 치명적인 데이타 손실은 없음

나. 하드 디스크일 경우

- 0 섹터의 내용이 FAT 부분(tr:0 he:0 Se:7)에 복사되어 있어 1 섹타분의 데이타 손실
- 손실된 부분의 데이타를 읽을 때 에러 발생

7.4.4 감염여부 검진

가. Debug 이용

```
A> 또는 C> 에서 debug
-l100 0 0 1 <CR>
-d  <CR>                                          ................
-d  <CR>                                          .3.......Your P
-d  <CR>                                          C is now Stoned!
                                                  ....LEGALISE MA
                                                  RIJUANA
```

이렇게 해보면 우측 텍스트부근에 위와 같은 문자가 나타나면 감염된 것임(원래는 MS-DOS로 나타나거나 PCTOOLS등 포맷한 디스켓이 나타남)

나. Utility 이용(PCTOOLS, NORTON, MACE)

View Edit기능으로 들어가 Boot Sector에서 Debug에서와 같은 메세지가 나타나면 바이러스에 감염된 것임

다. 바이러스 스캔 프로그램 이용

7.4.5 복구방법

가. 감염된 디스켓 복구방법

1) 감염되지 않은 디스켓을 A:드라이브에 넣고 부트하거나 C:드라이브에서 부트한다.

2) B:드라이브에 새로운 디스켓을 넣고 초기화 한다음 A:드라이브에 감염된 디스켓을 넣고 화일 복사를 하면 복구됨

(주의) 'DISKCOPY'는 절대 사용치 말 것.(DOS부분까지 복사되기때문)

3) 복사한 다음에는 바로 프로텍트를 붙일것

나. 하드 디스켓 복구방법

1) Master Boot Sector 복구

- Disk Utility를 이용하여 같은 DOS Version,Hard Disk의 Master Boot Sector를 복사
- fdisk로 파티션을 다시함 (감염전과 똑같이)

2) Boot Sector 복구

- Disk Utility를 이용하여 같은 DOS Version의 Boot Sector를 복사
  - o. PCTOOLS : Sector 단위 복사
  - o. NORTON : Sector 단위 복사
- NDD(Norton Disk Doctor)의 Make Boot disk 이용

3) FAT 복구

- Disk Utility(pctools, Norton 등)로 FAT에 바이러스가 복사해 둔 프로그램 부분을 찾아와 FAT 복사분을 Sector단위로 그 위치에 복사
  - o. 즉, 논리 Sector 46을 논리 Sector 5 에 복사
  - o. 단, FAT 복사분도 같이 오염되어 있으면 오염된 2 Sector단위에 해당되는 데이타는 복구할 방법이 없음
  - o. 거의 대부분을 회복 시킬수 있으나 일부는 잃어 버릴 수도 있음

7.4.6 예방대책

가. 디스켓의 바이러스 검사후 미감염 디스켓에는 write-protect

나. 외부로부터 온 디스켓은 부트디스크로 사용하지 말 것

다. 하드디스크 사용자는 절대 A:에서 부트하지 말 것

라. 게임 디스켓은 거의 감염된 것으로 생각하고 대처할 것

7.4.7 Stoned 프로그램 분석

가. Source Dump 리스트 설명

이 리스트는 감염된 디스켓의 Boot Sector를 덤프한 것이다.

```
0100  EA 05 00 C0 07 E9 99 00-00 1A 03 00 C8 E4 00 80   ................
      -- -- -- -- -    ← 바이러스 감염 스트링

0110  50 00 F6 E7 D1 E0 D1 E0-32 FF 03 D8 2E 8E 1E 8D   P.......2.......
0120  6F 81 E1 1F 3F 2E 87 0E-89 6F 2E 80 3E 88 6F 00   o...?....o..>.o.
0130  74 03 E8 62 11 2E 8B 0E-89 6F E8 5A 11 2E C6 06   t..b.....o.Z....
0140  88 6F 01 58 5B 59 1F CF-2E F6 06 64 72 03 74 05   .o.X[Y.....dr.t.
0150  2E FF 2E DF 56 1E 52 51-53 50 33 DB 8E DB 8A 1E   ....V.RQSP3.....
0160  62 04 D0 E3 8B 87 50 04-89 97 50 04 8B D8 2E 8E   b.....P...P.....
0170  1E 8D 6F 2E 80 3E 88 6F-00 74 15 B8 50 00 F6 E7   ..o..>.o.t..P...
0180  D1 E0 D1 E0 32 FF 03 D8-2E 8B 0E 89 6F E8 07 11   ....2.......o...
0190  B8 50 00 F6 E6 D1 E0 D1-E0 32 F6 03 C2 8B D8 2E   .P.......2......
01A0  8B 0E 89 6F E8 F0 10 2E-C6 06 88 6F 01 58 5B 59   ...o.......o.X[Y
01B0  5A 1F CF 2E F6 06 64 72-02 74 0D 2E F6 06 64 72   Z.....dr.t....dr
01C0  01 74 06 2E FF 2E DF 56-CF 1E 52 53 50 33 DB 8E   .t.....V..RSP3..
01D0  DB 32 E4 2A 06 62 04 BB-00 01 F7 E3 2E 01 06 8D   .2.*.b..........
01E0  6F 58 5B 5A 1F 2E C6 06-E3 6E FF 2E FF 2E DF 56   oX[Z.....n.....V
01F0  2E F6 06 64 72 03 74 0B-2E C6 06 E3 6E FF 2E FF   ...dr.t.....n...
0200  2E DF 56 E8 58 10 FC 06-1E 57 56 55 52 51 53 50   ..V.X....WVURQSP
0210  8A D8 2E A1 8D 6F 8E D8-8E C0 8B E9 2B D1 FE C6   .....o.......+...
0220  FE C2 B8 50 00 F6 E5 8B-F8 32 ED 03 F9 57 D1 E0   ...P.....2...W..
0230  D1 E0 03 C1 8B F8 8B CD-02 EB B8 50 00 F6 E5 8B   ...........P....
0240  F0 32 ED 03 F1 56 D1 E0-D1 E0 03 C1 8B F0 8A E7   .2...V..........
0250  80 E4 7F 80 FC 0F B0 00-76 02 B0 FF 0A DB 74 06   ........v.....t.
0260  62 04 D0 E3 8B 87 50 04-89 97 50 04 8B D8 2E 8E   b.....P...P.....
0270  FE C2 B8 50 00 F6 E5 8B-F8 32 ED 03 F9 57 D1 E0   ...P.....2...W..
0280  03 33 DD FE C1 CD 13 EB-C5 07 59 6F 75 72 20 50   .3........Your P
                  바이러스 감염 스트링 →                 ------
0290  43 20 69 73 20 6E 6F 77-20 53 74 6F 6E 65 64 21   C is now Stoned!
                  바이러스 감염 스트링 →                 ---------------
02A0  07 0D 0A 0A 00 4C 45 47-41 4C 49 53 45 20 4D 41   .....LEGALISE MA
                  바이러스 감염 스트링 →                 ---------------
02B0  52 49 4A 55 41 4E 41 21-BA                        RIJUANA!.
                  바이러스 감염 스트링 →                 ---------
```

7.5 Sunday 바이러스

VIRUS 명	Sunday Virus
파생된 VIRUS 명	
출처	워싱턴주 시애틀
전염기종	IBM PC 및 호환 기종
전염종류	일반적인 애플리케이션 감염자
비고	메모리에 적재 불가능할 때까지 증가 시킴

7.5.1 특징

가. .COM, .EXE, .OVL 프로그램을 감염

나. 감염된 프로그램 크기를 163 바이트 증가시킴

다. 감염된 프로그램은 변형되어 메모리에 강주

라. INT 8h, INT 21h Vector 변경

7.5.2 감염경로

가. 감염된 .EXE 및 .COM 화일 수행시 메모리 상주

나. 이후 수행시되는 화일마다 화일크기를 증가(1636 Byte)시키면서 감염

다. INT 8h, INT 21h 이용

7.5.3 감염증상

가. 일반적인 증상

- 시스템의 일반적인 속도 저하
- 사용 가능 시스템 메모리 용량이 감소
- .COM 화일들은 한번만 감염(화일크기 증가 : 1636)
  : 앞부분에 감염
- .EXE 화일들은 한번만 감염(화일크기 증가 : 1636)
  : 뒷부분에 감염

나. 일요일 증상

- 일정 시간마다 주기적으로 메세지 출력

```
"Today is Sunday! Why do you work so hard?...
 All work and no play make you a dull boy!...
 Come on! Let's go out and have some fun!"
```

- 수행시키는 프로그램을 삭제
- 일부 버전은 하드디스크상의 모든 데이터 파괴

7.5.4 감염여부 검진

가. Viruscan 이용

- [c:W]SCAN 화일명 <CR>

나. Disk Utility 이용

- 화일내 "Sunday" 문자열 나타나면 감염

다. Debug 이용

- 화일내 "Sunday" 문자열 나타나면 감염

7.5.5 복구방법

가. 삭제된 화일 복구

- Disk Utility를 이용하여 복구 (화일 'UNDELETE' 기능 이용)

나. 감염된 화일 복구

- 감염된 실행가능 화일은 감염되지 않은 프로그램으로 교체
- Viruscan 프로그램으로 복구(SCAN /D)
- V2plus 프로그램으로 복구

7.5.6 예방대책

가. 출처불명의 소스로부터의 프로그램은 실행시키지 말것

나. 실행가능 코드를 내포한 디스켓은 교환하지 말것

다. 메모리의 배치와 프로그램 화일크기를 감시할 것

7.5.7 Sunday 프로그램 분석

가. Source Dump 리스트 설명

이 리스트는 감염된 화일을 덤프한 것이다.

```
1217:0100  E9 92 00 73 55 C8 F7 E1-EE E7 00 01 0B 0E 00 00   ...sU...........
                      -- -- -- -- --   ← 감염 체크 스트링

1217:0110  00 02 00 AA 00 CD 0B 60-14 5B 02 56 05 9B 0C 90   .........[.V....
1217:0120  7E 00 00 00 00 00 00 00-00 00 00 00 00 00 E8 06   ..............
//////////////////////////////////////////////////////////   ////////////////
1217:0160  06 84 19 C4 00 01 11 22-00 00 00 F5 B4 4C CD 21   .......".....L.!
1217:0170  05 00 20 00 21 00 DB 00-00 02 10 00 10 12 01 00   ....!...........
1217:0180  B9 41 2A 9B 43 4F 4D 4D-41 4E 44 2E 43 4F 4D 01   .A*.COMMAND.COM.
1217:0190  00 00 00 00 00 FC B4 FF-CD 21 80 FC FF 73 15 80   .........!...s..
//////////////////////////////////////////////////////////   ////////////////
1217:0330  02 2E 8A 04 3C 24 74 05-CD 10 46 EB F4 2E C7 06   ....<$t...F.....
1217:0340  1F 00 90 7E 5E 5B 58 2E-FF 0E 1F 00 2E FF 2E 13   ....^[X.........

1217:0350  00 54 6F 64 61 79 20 69-73 20 53 75 6E 44 61 79   .Today is SunDay
1217:0360  21 20 57 68 79 20 64 6F-20 79 6F 75 20 77 6F 72   ! Why do you wor
1217:0370  6B 20 73 6F 20 68 61 72-64 3F 0A 0D 41 6C 6C 20   k so hard?..All
1217:0380  20 77 6F 72 6B 20 61 6E-64 20 6E 6F 20 70 6C 61    work and no pla
1217:0390  79 20 6D 61 6B 65 20 79-6F 75 20 61 20 64 75 6C   y make you a dul
1217:03A0  6C 20 62 6F 79 21 0A 0D-43 6F 6D 65 20 6F 6E 20   l boy!..Come on
1217:03B0  21 20 4C 65 74 27 73 20-67 6F 20 6F 75 74 20 61   ! Let's go out a
1217:03C0  6E 64 20 68 61 76 65 20-73 6F 6D 65 20 66 75 6E   nd have some fun
1217:03D0  21 24 9C 80 FC FF 75 05-B8 00 04 9D CF 80 FC DD   !$....u.........
                                                                    |
                          Sunday 바이러스 메세지   ==============+
```

7.6 1704 바이러스

VIRUS 명	1074 / Cascade 바이러스
파생된 VIRUS 명	- 1071 - Cascade-B - 1704-B - 1704-C - 1704-D
출 처	
전염기종	IBM PC 및 호환 기종
전염종류	일반적인 애플리케이션 감염자
비 고	- 암호화 수법을 이용하는 등 고도의 기술을 사용 - 외국에서는 87년 말에 발견 - 국내에서는 89년 말에 발견

7.6.1 특징

가. 시스템(.COM 화일)에 침입한 후 자기자신을 암호화해 버린다.

- 암호화를 기생하는 화일의 길이에 의해 변화시킴
- 이러한 바이러스는 백신 등에 의한 검출이나 그 내용 분석이 매우 곤란

나. 바이러스의 활동을 난수, 기생하고 있는 H/W 종류,사용 monitor 종류, clock card 유무, calender 등의 재조건을 이용해서 변화시킴

다. IBM 호환기에만 감염

7.6.2 감염경로

가. 감염된 .COM화일 수행시 메모리 상주

나. 이후 수행시키는 .COM화일마다 화일크기를 증가(1701 Byte)시키면서 감염

7.6.3 감염증상

가. .COM화일의 사이즈가 1701 혹은 1704 Byte 증가함

나. 시스템의 속도 저하

다. 어느시기(88년 10-12월) 또는 매년(8월-12월등)이 되면 활동

라. 활동 상황이 되면 화면에 표시된 문자를 떨어뜨린다

마. 문자의 낙하 중에도 시스템은 정상으로 동작함

7.6.4 감염여부 검진

가. Viruscan 프로그램 이용

나. debug나 기타 Disk Utility로 발견하기 어려움

7.6.5 복구방법

가. 감염된 실행가능 화일은 감염되지 않은 프로그램으로 교체

나. CleanUp 프로그램으로 복구

7.6.6 예방대책

가. 출처 불명의 소스로부터의 프로그램은 실행시키지 말것

나. 실행가능 코드를 내포한 디스켓은 교환하지 말 것

다. 메모리의 배치와 프로그램 화일 크기를 감시할 것

7.7 기타

7.7.1 Lehigh

VIRUS 명	Lehigh Virus
파생된 VIRUS 명	- Lehigh 2
출처	1987년-가을, 미국의 베들레헴에 있는 Lehigh 대학
전염기종	IBM PC및 호환기종
전염종류	시스템 감염자
특징	- COMMAND.COM 화일을 감염 - 346 바이트 정도의 크기 - 프로그램의 생성 일자와 시간을 변경 - 4번째 감염후 활성화 - 모든 시스템 데이터를 파괴 - COMMAND.COM 스택영역의 59AFh - 5B09h 사이에서 시작
전염방식	- 감염된 디스크로 COMMAND.COM 수행 - INT 21h을 가로챔 - 11h : find first file - 4Bh : execute program - 사용중인 디스크에 COMMAND.COM이 존재하면 감염시킴
증상	- COMMAND.COM 크기 변경 - 계수기가 4가 되면, INT 26h(absolute disk write)를 이용하여 32섹터를 0으로 채운다. 즉, FAT와 루트디렉토리를 파괴
잠정피해	- 하드디스크상의 모든 데이터 손실
예방책	- 시스템 디스크에 애플리케이션 프로그램 전송 금지 - 다른 컴퓨터에 시스템 디스크 삽입 금지 - COMMAND.COM화일의 일자 및 크기의 변화를 감지
복구방법	- 시스템을 끔 - original write-protect된 시스템 매스터로 재부트 - 하드디스크와 모든 감염된 플로피의 COMMAND.COM삭제 - 원래의 매스터에서 COMMAND.COM복원
비고	- 매우 짧은 활동주기 (4번째 디스크에서 활성화)때문에 데이타 파괴전에 발견할 기회가 불충분

7.7.2 Alameda

VIRUS 명	Alameda Virus
파생된 VIRUS 명	- Merit Virus - Golden Gate Virus - Sfvirus
출 처	1988년 봄, 캘리포니아 오클랜드의 Merritt 대학
전염기종	IBM PC 및 호환 기종
전염종류	부트 감염자(부트 섹터)
특 징	- 원래의 부트 섹터를 바이러스로 교체 - 원래의 부트 섹터를 첫번째 빈 섹터에 저장 - 소프트웨어 재부트 과정을 통해 감염 - 원래의 부트 섹터에 이상이 있음을 알리지 않음 - 플로피 디스켓의 맨 마지막 섹터 파괴
전염방식	- 출처 불명인 원본 디스켓으로 부터의 부팅 - 감염된 시스템에 미감염 부트디스켓 삽입시 감염
증 상	- 부트과정 저속화 - 시스템 붕괴 - 데이타 손실
잠정피해	- 데이타 손실
예 방 책	- write-protect된 플로피로만 부트 - 플로피 하드디스크 시스템을 부팅하지 말 것 - 다른 시스템에 부트 디스크를 삽입하지 말 것
복구방법	- 시스템을 끔 - write-protect된 original 매스터 디스크로 부트 - 디스크의 부트 섹터 교체를 위해 DOS SYS 수행
비 고	- Brain Virus와는 달리 감염후에 원래의 부트 섹터를 protect하지 않음 - 원래의 Instruction은 우연한 사고로 over written 되어질 수 있음, 그때 부트 실패가 발생

7.7.3 dBASE 바이러스

가. 컴퓨터의 메모리에 상주하고 dBASE의 데이타 화일-'.DBF 화일'- 이 기록가능 상태인 경우는 random하게 2 byte를 바꿔 넣는다.

나. 90일 후에 바이러스는 root directory와 FAT를 소멸시킴

7.7.4 FU Manchu 바이러스

가. 제 2단계에 속하는 악질 바이러스

나. 감염되면 'The world will hear from me again!'이라고 표시가 된 후 시스템을 다시 부트 시킴

다. 키보드로 부터 입력중 저명한 정치가의 이름이 포함되어 있는 경우, 입력을 바꿔서 key board buffer에 넣는다는 점

7.7.5 Data Crime 바이러스

가. 고도의 기술을 갖는 바이러스는 아니지만 수법이 악질

나. 매년 10월, 12월에 하드 디스크내의 데이타를 모두 없애 버린다

다. 유럽에서 매우 만연되어 있고 최근 미국에도 상륙되었다는 점

8.바이러스 예방 및 퇴치 프로그램 분석

8.1 Antivirus프로그램의 기능

1. 예방(prevention)
   가. 예방은 처음부터 바이러스가 감염되는 것을 방지한다.
   나. 바이러스가 발을 붙이지 못하게 수행 화일에 수정을 금지 한다.
   다. 사용자가 허락하지 않는한 RAM에 프로그램이 상주하지 못하도록 한다.
   라. 승인된 리스트에 등록되어 있지 않거나 시험된 응용시스템이 아니면 수행하지 못하도록 한다.
2. 검출(detection)
   가. 바이러스 감염후에 사용자에게 경고하며 바이러스 증상을 관찰한다.
   나. 수행화일과 부트 섹터를 체크하며 전에 기록한 기호(Signature)와 비교한다.
3. 확인(identification)
   가. 특정 바이트 형태를 인식하여 바이러스의 종류를 확인한다.
   나. 바이러스 코드의 일부 변경만 있어도 판별하기 힘들기 때문에 효과적인 방법은 아니다.
4. 백신(Vaccination)
   가. 수행화일에 백신을 실제 투입한다.
   나. 백신 프로그램이 수행되면 백신이 투입된 코드가 기호 체크를 수행하고 만일 변경이 있으면 경고 한다.
5. 복구(damage control)
   가.일부 antivirus 프로그램은 예방뿐만 아니라 복구 기능도 제공한다.
   나. FAT의 복사부분이 있으면 피해를 복구할 수 있다.

8.2 백신 프로그램이 사용하는 전략

1. 직접 바이러스를 진단하는 방법
   가. 이미 알려진 바이러스가 있는지 검사
   나. 프로그램내에 이상한 문장이 있는지 검사
   다. 프로그램내에 하위 수준의 디스크 쓰기 루틴등의 코드가 있는지 검사
   라. 승인된 프로그램 리스트를 가지고 여기에 등록되어 있지 않은 프로그램의 실행을 방지
   마. 승인된 램상주 프로그램 리스트를 가지고 여기에 등록되어 있지 않은 프로그램이 상주 하면 통보
2. 바이러스의 증식을 막는 방법
   가. 화일들을 쓰기 방지 상태로 함
   나. 디스크상의 화일들을 검사 (전에 계산해 놓은 checksum과 비교)
   다. 프로그램을 실행시킬때 checksum을 검사
3. 파괴적인 활동을 막는 방법
   가. 도스에 의한 디스크의 사용만을 허용함으로써 하위 수준에서 시스템 영역의 파괴를 방지
   나. 하드디스크 사용 방지
   다. FAT 복사
   라. CMOS 복사

8.3 antivirus 프로그램의 제약사항

1. 백신 프로그램을 너무 믿어서는 안된다. 왜냐하면 프로그램이 모든 바이러스에 대하여 효과가 있다고 확신할 수 없기 때문이다.
2. 대부분의 프로그램이 RAM상주 프로그램으로 시스템의 속도를 저하시키고 사용자에게 여러가지 불편을 줄 수 있다. 예를 들면, 포멧팅도 자유롭지 못할 뿐만 아니라 새로운 프로그램을 작성하면 등록되어 있지 않다고 시스템에 의해 바이러스로 오인받을 가능성도 있다.

8.4 백신 프로그램 소개

8.4.1 목록

구분	프로그램명	개 발 회 사	개발년도	버 전	주 요 특 징
예방및검진	VIRUSCAN	McAfee Ass.	1990. 2	2.7V57	67종 바이러스 검진, 복구
	SCANRES	McAfee Ass.	1989. 12	1.8V51	램상주,검진(54종)
	FLU-SHOT+	S/W Concept	1989	V1.7	예방, 선택된 화일만 보호
	VIRUS GUARD	I. P. Tech.	1988	V1.0	예방, checksum 이용
	TRAPDISK	Audy Hopkin		V1.	예방, INT 13h 이용
	NOVIRUS	Yan Seiner	1988		특정화일 검진
	ANTIVRS		1989. 8		검진, 다양한 가능
	CONDOM	Charlie Ro.	1988		바이러스 예방
	CHK4BOMB				검진, 스트링 추출
	VACCINE		1987		예방, checksum 이용
	VACINE	Art Hill	1988	V1.3	예방, Protection용 PG
	VCHECK	Systemberat		V1.1E	예방 checksum이용
	VIRUSIM	british Com	1989		Cascade,Denzuk,Fu Man-
					바이러스 시뮬레이션
복구	V2PLUS	안철수	1989.12	V1.2	Jerusalem, Lbc, Brain, Stoned, Sunday 복구
	BRAIN		1988		BRAIN 바이러스 복구
	M-JRUSLM	McAfee Ass.	1989. 8		예루살렘 바이러스 복구
	M-VIENNA.	McAfee Ass.	1989. 8		비엔나 바이러스 복구
	M-1704	McAfee Ass.	1989.		1704,1701 바이러스 복구
	M-3066	McAfee Ass.	1989.		3066 바이러스 복구
	NOCRIME	Christina H	1989. 9	V0.1	DATACRIME 1280,1168, DATACRIME II 복구
	COLUMBUS	Dave Bushon	1989.10		콜럼부스 바이러스 복구
	MDISK	McAfee Ass.	1989. 8	V1.0	부트, 분할섹터 복구

8.4.2. Viruscan (CVIA)

가. VIRUSCAN은 바이러스가 갖는 특징을 인식하여 바이러스명을 판정하는 백신 프로그램이다.

나. 먼저 Boot Sector 및 FAT를 검진하고 .exe 및 .com 화일을 검진한다.

다. CVIA가 Public Domain으로 제공하고 있다. 현재까지 CVIA가 발견한 바이러스는 67종류이며 VIRUSCAN은 이 모두를 식별할 수 있다.

라. 각 바이러스가 갖고 있는 특징인 'signature code'를 data로서 갖고 있으므로 이것을 이용하여 바이러스를 판별한다.

마. 약점은 사전 대책이 아니고 사후적이라는 것이다.

8.4.3 Flu-Shot+ (S/W 개념 설계)

가. 감염방지, 검출용 S/W

나. 종래의 백신 S/W flow-shot에 비해 조작성을 향상시켜 기업에서 이용할 수 있도록 기능을 추가

다. Shareware(사용해 좋으면 요금을 지불하는 S/W)인 백신 S/W

라. 현재 가장 널리 알려진 S/W

8.4.4. Certus (Foundation Ware)

가. 감염방지, 검출, 복구용 S/W

나. 10종류의 프로그램, 7종류의 utility로 됨

다. 실행가능한 OS, 사용자가 선택한 화일에 관하여 화일 크기 CRC등을 check하고 이상이 있으면 경고를 한다.

라. 바이러스대책만이 아니고 사용자가 하드디스크 내용을 없애라는 명령을 한때에도 경고를 하는등 시스템 관리에 이용가능하다.

마. Password설정 및 보안 단계를 9단계로 정할 수 있다.

- 특히 보안에 관계하는 부 프로그램에 패스워드를 설정할 수 있도록 해서 일반 사용자가 뭔가 변경을 하기가 어렵게 했다.
- 이런 의미에서는 시스템 관리자 지향적 S/W라고도 할 수 있다.

8.4.5 Vaccinate PLUS(Computer integrity)

가. 감염방지, 검출용 S/W

나. 10종류의 프로그램 으로 구성됨

다. 바이러스로부터 보호하고 싶은 화일에 self checking code (1 KByte 검사용 프로그램)를 부가하여 바이러스 감염을 발견 할 수 있다.

라. 화일 길이, CRC 등을 'hash code'라 부르는 독자의 수법으로 check한다.

마. .COM 및 .EXE 화일 이외 예를 들어 FAT등의 검사에는 Boot Track용 백신 'BOOT CAMP'를 이용한다.

바. 화일 자신에 백신을 투여하므로 N/W에서 유효

바이러스가 침입한 경우 바이러스는 프로그램 실행전에 자기자신 활동을 시작하여 아무일도 없었던것처럼 프로그램 실행위치로 되돌려 논다.그렇지만 미리 백신을 주사해 놓은 경우에는 바이러스가 프로그램의 실행위치에 되돌렸다 해도 갑자기 프로그램 실행전에 우선 백신을 실행한다. 백신은 화일의 길이나 프로그램 변경이 있었는지 여부를 조사하므로 바이러스의 활동 개시전에 검출 가능하게 된다.

N/W 이용 환경하에서는 일반의 백신을 이용하는 경우 단말기 한대 한대에 모두 백신을 이용해야만 하지만 Vaccine PLUS에서는 화일 그자체에 감염 검출 기능이 부가되어 있으므로 한번 백신을 주사하여 화일 server에 시켜 놓으면 단말기측에서는 화면에 경고문이 나오는지 여부만을 판찰하면 된다.

8.4.6 Virus Guard(I.P. Technology)

가. 감염검출용 S/W

나. 미리 등록한 화일의 크기, Checksum등을 boot시에 조사한다.

다. 조작성이 좋다.

라. 프로그램의 건강진단이 가능하다는 것으로 판매하고 있다.

9. 바이러스 대책

컴퓨터 바이러스에 대한 완벽한 대책 방안은 불가능하다고 본다. 왜냐하면 바이러스가 1종이 등장하면 조만간 수많은 변종 바이러스가 등장하고 그 기법도 다양해지기 때문이다. 그래서 컴퓨터 바이러스에 대한 대책은 예방이 최선이라고 생각되며, 현 시점에서 체계화된 대책을 세워 추진하는 것이 바람직 하다고 생각된다.

가. 경영관리적 절차 수립

1. 국내.외 바이러스에 관한 정보를 신속히 수집 및 분석
2. 발견된 신종 바이러스에 대한 홍보 및 교육
3. 바이러스에 대한 경영 관리와 기술적인 대응 대책을 수립
4. 감염 예방과 침투된 바이러스의 확산 방지 및 피해 복구를 수행
5. 컴퓨터 바이러스에 관한 조사 교육 등을 실시하고 있는 주요 단체와 의견 교환
   - Computer Virus Industrial Association(CVIA) : 88.5, 컴퓨터 관련기업 230개 회사
   - S/W Publisher Association Security Special Interest Group(S.I.G) : 88.10, S/W Vendor 50개 회사
   - S/W Development Council Antivirus Task Force : 88.11, Machintosh 지향 S/W 개발 House 8개 회사
6. 기기의 관리
   - PC 나 LAN으로 사용하고 있는 기기의 관리
   - 중요한 시스템은 LAN과 격리
   - 개발 시스템과 운영 시스템의 격리

나. 기술적 절차 수립

1. 수시 또는 정기적으로 Backup 받는다.
   - 사용자는 바이러스보다는 하드디스크의 파괴로부터 더 많은 고통을 받고 있지만 이와 같은 두가지 경우를 대비해서라도 Backup을 자주 할 필요가 있다.
   - 바이러스가 감염되고 데이타가 파괴 되었다고 판단되면 Backup을 이용하여 복구한다.
2. 바이러스 감염 확인 백신 S/W(Viruscan Virus Guard등)를 이용하여 철저하게 바이러스 감염여부를 검진하고 퇴치한다.
   - 프로그램 Up/Down loading시
   - 불법 복사 프로그램을 부득이 사용시
   - BBS로부터 다운 로드된 소프트웨어 사용시
   - 프로그램 디스켓을 빌려주고 받을시
   - 개발된 프로그램을 배포할 시
3. 감염 예방용 프로그램을 활용하여 바이러스의 침투를 처음부터 방지함
   - Flu-Shot, TrapDisk, Certus, Vaccinate PLUS 등 antivirus 프로그램 사용
4. 하드디스크일 경우 절대로 플로피 디스크로 부팅하지 않는다.
   - FDD에서는 하나의 부트 디스크만 사용한다.
5. 저장할 데이타가 없는 플로피 디스켓은 write-protect tab을 붙인다
6. 타인이 시스템을 사용하지 못하게하고 이것이 안되면 자기의 프로그램 디스크에서 작업하지 못하게 한다.
7. .COM과 .EXE 화일을 read only로 만든다.
8. COMMAND.COM 화일을 루트 디렉토리로부터 제거한다.
   - CONFIG.SYS 화일에서 작업한다.

10. 결론

바이러스의 확산과 피해는 갈수록 심각할 것으로 보인다. 해외에서는 NASA와 국방망 및 BBS에 바이러스가 침투하는등 극성을 부리고 있지만, 아직 네트워크가 발달하지 않은 우리나라에서는 네트워크를 통한 감염보다는 시스템의 불법 복사로 인하여 극성을 부리고 있는 실정이다. 하지만 앞으로 우려되는 점은 정보 통신망을 통한 바이러스 감염이다.이런경우 사용자들간의 자유로운 정보흐름을 통제할 수 밖에 없는데 이는 정보산업의 비용을 증가 시키고 아울러 정보산업의 발전에 커다란 장애 요인이 될 수 있다.

고도화하는 바이러스에 대해서 일찍부터 일부의 S/W기술자는 관심을 갖고 이에 대한 S/W를 개발하고 있으며, 그 결과 백신 프로그램이 등장하게 되었다. 사용자는 이것을 사용하여 바이러스의 침투를 예방하고 감염여부를 확인할뿐만 아니라 복구를 할 수도 있다. 그러나 이 제품의 대부분은 한 종류의 바이러스에는 유효 하지만 다른 종류의 바이러스에는 별 효과가 없고, 또한 사용자는 이것의 사용으로 인해 불편을 가져온다.

백신 프로그램을 사용한 바이러스의 예방 및 복구도 중요 하지만 바이러스에 대한 홍보를 통해 관심을 가지게 하고 경영관리적 및 기술적 대책을 수립하여 대책 자체는 간단하지만 철저하게 지키는 일이 더욱더 중요하다고 하겠다.

참 고 문 헌

1. 한국정보과학회 『정보과학회지』, 5권 3호 , 87. 9
2. 김문익 , 『컴퓨터범죄론』, 법영사
3. 『컴퓨터 범죄와 암호화 대책』,
   정보와 사회 시리즈 - 15 , 89.12
4. (주) 정보시대 『마이크로 소프트웨어』, 88. 7
5. (주) 정보시대 『마이크로 소프트웨어』, 89. 9
6. (주) 정보시대 『마이크로 소프트웨어』, 90. 1
7. (주) 정보시대 『마이크로 소프트웨어』, 90. 2
8. (주) 정보시대 『마이크로 소프트웨어』, 90. 3
9. (주) 정보시대 『정보시대』, 90. 4