KIISC Journal Vol. 9, No 4.

CIH 바이러스 분석 및 대책

황규범*, 김광조*, 안철수**

Analysis and Recovery of CIH virus

Kyu-beom Hwang*, Kwangjo Kim*, Charles Ahn**

요 약

본 논문은 악성 프로그램 중 피해가 큰 컴퓨터 바이러스에 대하여 정의 및 부작용, 그리고 형태 변화에 대하여 고찰 한 후, 최근 아시아 지역에서 많은 피해를 준 CIH바이러스에 대한 특징, 메모리와 파일 치료방법을 기술하고 피해 복구방법으로 윈도95/98 운영체제하에서 FAT32 파일 시스템 구조를 가지는 하드디스크를 복구하는 방법을 제안하고, 실제로 상용의 백신 프로그램을 이용한 복구 사례를 제시한다.

Abstract

In this paper, we introduce the definition and historical overviews of computer virus program, and review their side-effect and ways of infections. We describe the feature of CIH virus which damaged lots of PC systems in Asian countries recently and propose new methods how to rescue against destruction under the operating system of the Microsoft's Windows 95/98. Our experiment results can fix hard disk having FAT32 file system structure and show some popular program cases of having recovered by commercial vaccine program.

Keyword: CIH virus, Anti-Virus, FAT32

Ⅰ. 서론

개인용 컴퓨터의 보급과 발전으로 컴퓨터 이용을 편리하게 해주는 많은 수의 응용 프로그램들이 다양한 분야에 나타났다. 이들 응용 프로그램을 이용하면 원하는 작업을 보다 정확하고 빠르게 수행할 수 있게 되어 업무 수행에 있어 많은 도움을 준다.

그러나 다른 한편으로는 많은 사람들에게 전파되어 컴퓨터 시스템을 파괴하거나 작업을 지연 또는 방해하는등 피해를 주는 프로그램들도 다수 나타났다. 이런 프로그램들은 컴퓨터 이용을 어렵게 하고 정신적 물질적 피해를 준다. 이러한 프로그램을 악성 프로그램이라고 하며 특성에 따라 통상 컴퓨터 바이러스, 웜, 트로이목마로 구별한다. 본 논문에서는 피해가 크고 광범위한 컴퓨터 바이러스를 다룬다.

본 논문에서의 바이러스 이름은 가능하면 한글과 영문을 병행 표기하고 이탤릭체와 밑줄로써 구분한다.

(그림 1)은 우리나라에 *뇌(Brain)*가 처음 발견된 1988년부터 1999년 초까지 국내에 발견된 바이러스들을 출처별, 종류별로 그 수를 파악한 것으로 1996년 이후 상당히 큰 증가세를 보이고 있다.[1]

이와 같이 급속하게 증가하고 있는 국내 바이러

* 한국정보통신대학원대학교 공학부 암호 및 정보보안연구실 (kityhwang@icu.ac.kr, kkj@icu.ac.kr)

** 안철수컴퓨터바이러스연구소 (cahn@ahnlab.co.kr)

연도	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999 1/4분기	총계
국산	-	3	8	5	10	17	40	81	152	170	162	21	669
외산	1	3	20	16	7	17	36	47	74	86	114	39	460
합계	1	6	28	21	17	34	76	128	226	256	276	60	1129

연도	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999 1/4분기	총계
부트	1	4	8	5	5	10	13	18	8	15	14	2	103
파일		2	18	15	11	23	60	105	188	220	219	38	899
매크로	-	-	-	-	-	-	-	-	1	16	36	20	73
부트/파일			2	1	1	1	3	5	29	5	7	-	54
합계	1	6	28	11	17	34	76	128	226	256	276	60	1129

그림 2. 1988-1999년 컴퓨터 바이러스 발견 동향
Fig 1. Number of detected computer viruses, 1988-1999

스 프로그램은 제작 의도가 불순하거나 영웅 심리를 가진 악의의 해커 그룹들에 의하여 유포되어 사회적으로 큰 피해를 입히고 있다.

최근 많은 피해를 주었던 *CIH*는 기존의 바이러스 프로그램과 달리 시스템을 작동 불능 상태로 만드는 능력과 하드디스크 정보를 파괴하는 능력을 동시에 가짐으로써, 개인뿐만 아니라 기업 그리고 관공서에서 사용하는 수 많은 PC를 무력하게 만들어 커다란 경제적인 손실을 입힌 바가 있다.

우리는 이러한 악의의 프로그램으로부터 선의의 사용자의 피해를 최소화하고 건전한 정보화 사회를 구현하기 위하여 *CIH*에 관한 상세한 기술 특성과 대비책에 관한 기술을 제안하고 실험 결과를 제시하고자 한다.

본 논문은 사용자 개개인이 이러한 악성 프로그램으로부터 피해를 정확히 인식하고 네트워크로 연결된 PC를 이용할 때에는 특히 주의를 강조한다. 특히, 윈도우 환경에서 백신 사용의 주의점을 설명하고 *CIH*에 의하여 손상된 하드디스크의 복구 방법을 제안한다. 제안된 하드디스크 복구 방법은 바이러스에 의한 손상뿐만 아니라, 원인 불명의 이유로 인하여 주부트섹터(MBS, Master Boot Sector)와 도스부트섹터(DBS, DOS Boot Sector) 그리고 FAT(File Allocation Table)의 일부가 손상된 경우까지 확대 적용이 가능한 특징을 가지고 있다.

본 논문의 구성은, 제 2장에서 바이러스의 정의와 특징을 기술하고, 제 3장에서는 *CIH*의 특징과 제거 및 파손된 하드디스크 복구방법을 제안하며, 제 4장에서는 결론을 기술한다.

Ⅱ. 바이러스의 정의 및 특징

1. 바이러스 정의

생물학적 바이러스는 자신을 복제하는 유전인자를 가지고 있다. 컴퓨터 바이러스는 이러한 생물학적 바이러스와 그 성질은 같으나 감염 대상이 컴퓨터 프로그램이나 데이터 파일이라는 점이 다르다. 따라서 감염시 원본 프로그램(Original Program) 혹은 데이터 파일에 바이러스 코드를 붙이거나 겹쳐 쓰기를 한다. 다시 말해, 컴퓨터 바이러스는 일종의 명령어들의 집합으로 사용자 몰래 자신을 다른 곳에 복사하는 명령어를 가지고 있어 컴퓨터 바이러스 프로그램 혹은 바이러스 코드라고 한다. 예전에는 바이러스 프로그램이라는 말이 정확했으나 매크로와 스크립트를 이용한 바이러스들이 나타남으로써 바이러스 코드라는 말을 쓰기도 한다.

본 논문에서는 컴퓨터 바이러스들은 컴퓨터 상에서 수행되므로 이하 간결하게 바이러스라고 하며, 보다 의미를 명확하게 할 필요가 있는 경우 바이러스 프로그램 혹은 바이러스 코드라 하고 바이러스를 예방, 진단 및 치료를 하는 프로그램(Anti-Virus Program)을 통칭하여 백신이라고 한다.

2. 부작용

바이러스들은 자기 복제 능력 외에도 생물학적 바이러스와 같이 부작용을 가지는 경우도 있다. 이런 부작용은 컴퓨터의 처리 속도를 느리게 하는 경우도 있고 파일에 손상을 주거나 하드디스크의 정보를 파괴하는 행위를 하기도 한다. 최근에는 시스템 롬 바이오스(System ROM BIOS 이하 바이오스)가 저장되어 있는 플래시메모리(Fresh Memory)의 정보를 파괴하는 기능을 가진 바이러스들이 나타나 시스템의 작동 불능 상태를 만드는 경우도 있다.

3. 형태변화

(그림 2)는 바이러스 감염전 프로그램(이하 원본 프로그램)의 형태와 감염후 바이러스에 의해 달라지는 형태를 보여준다. 바이러스 유형은 크게 원본 프로그램에 손상을 주는 겹쳐쓰기형, 원본 프로그램 앞에 붙어 먼저 실행하는 전위기생형, 프로그램 뒤쪽에 붙어 실행 흐름을 가로채어 바이러스가

먼저 실행하는 후위기생형 그리고 바이러스가 원본 프로그램 중간에 들어가는 이동형 바이러스가 있다.[2]

그림 3. 바이러스 감염 전·후 형태변화
Fig 2. Change of file structure after the infection of a virus.

III *CIH* 바이러스

최근 바이러스에 큰 관심을 가지게 된 계기는 *CIH*에 의해 발생한 전국적인 대규모 피해 때문이다. 정보통신부의 통계에 의하면 손실은 대략 20억원 정도로 추산하고 있어 지금까지 단일 바이러스에 의한 피해 규모로는 가장 크다.

*CIH*는 제작자의 영문 이름인 Chen In Hau(천잉하우, 陳盈豪)의 영문 첫 글자를 따서 명명한 바이러스로 1998년 4월 26일에 대만에서 초기 버전이 제작되었고 아시아 지역에 많은 피해를 주었던 것은 초기 버전을 개량한 *CIH* V1.2로 동년 5월 21일에 완성된 것으로 알려져 있고 국내에서는 동년 6월 12일 처음 발견되었다. 이 바이러스에 감염된 프로그램이 국내 대형 통신망의 공개 자료실에 등록되어 여러 이용자가 이를 사용하는 과정에서 국내에 넓게 확산되었다. 아직도 대형 통신망 자료에 등록된 파일 중에 *CIH*에 감염된 파일이 확인되고 있으나 종합적인 확인이 어려운 문제로 인하여 완전한 근절은 어려울 것으로 보인다.

현재 국내 각 언론들에 의해서 그 피해 규모가 널리 알려져 있으나 백신으로 치료가 불가능하다는 것은 사실과 다르다. 백신에서 파일 치료가 가능하며 메모리 치료 기능을 가진 백신으로 국내 제품으로는 안연구소의 V3Pro98, V3Pro2000, 하우리의 바이로봇(Virobot) 그리고 외국 제품으로는 시멘텍사의 NAV가 있다. 그러나 윈도우 운영체제의 특성상 치료시 몇가지 유의 사항이 있지만 이런 유의사항을 제대로 알지 못하거나 지키지 않아 발생한 피해도 상당수에 이른다.[3][4]

(그림 3)는 *CIH*사태 당시 사설 통신망이나 인터넷으로 쉽게 입수 및 사용이 가능한 셰어웨어 백신인 V3+를 이용하여 *CIH*를 진단한 것이다.

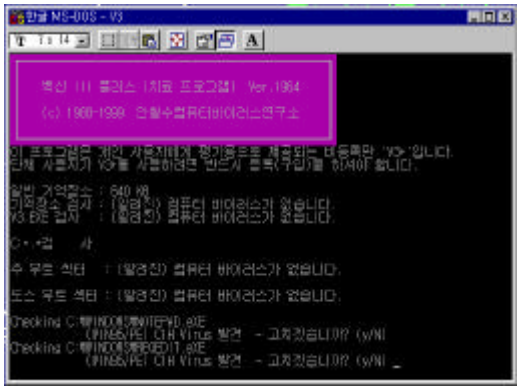

그림 4. 셰어웨어 백신을 이용한 *CIH* 검사
Fig 3. Checking *CIH* using a shareware vaccine.

1. 특징

*CIH*는 기존의 바이러스들과 별다른 차이가 없으며 특별한 기술적 우위 요소도 없다. 그러나 다른 윈도우 바이러스들과 달리 바이오스를 파괴하는 증상과 하드디스크 정보 파괴라는 부작용을 가지고 있어 그 피해 규모가 크다. *CIH*에 대한 치료 방법은 이미 널리 알려져 있고 치료하는 과정상 아무런 문제가 없다. 다만 윈도우 환경에서 실행 중인 감염 프로그램을 치료할 수 없는 문제점이 있어 특별한 치료 방법이 필요하다.

*CIH*의 경우 윈도우 가상드라이버 영역에 상주하게 되므로 복구시 우선 메모리로부터 바이러스 제거가 필수적이다. 따라서 백신들은 우선 메모리에서 *CIH*를 제거한 후, 감염된 파일의 치료를 수행하게 된다. 이때 윈도우상에 항시 실행중인 몇 개 프로그램의 경우 백신으로 바이러스 감염 여부를 알 수 있으나 치료는 불가능하다. 따라서 이를 이러한 파일을 치료하는 방법은 윈도95가 종료시 제공하고 있는 MS-DOS모드를 이용하여 치료를 시도해야 한다. (그림 4)는 윈도95의 시스템 종료에서 MS-DOS모드를 선택하는 것이다.

본 장에서는 *CIH*치료에 대한 방법을 설명하고 백신을 통해서 이루어 질 수 없는 하드디스크의 복구 방법에 대하여 제안한다.

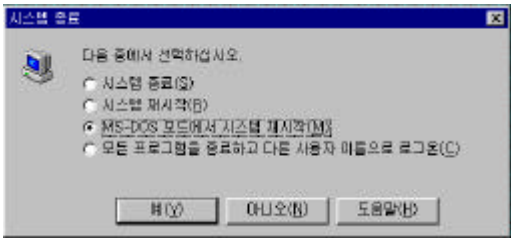

그림 4. 윈도95의 MS-DOS모드
Fig 4. Execution of MS-DOS mode in Windows '95

2. CIH의 치료

CIH의 치료는 크게 윈도우 메모리에서 바이러스 기능을 정지시키는 메모리 치료가 있고 감염된 파일들을 찾아 제거하는 파일 치료가 있다. 만일 바이러스가 작동하여 하드디스크의 파괴와 시스템 바이오스의 파괴가 있었다면 우선 시스템 바이오스는 소프트웨어적인 방법으로 복구할 수 없으므로 컴퓨터 구입처에 사후지원을 의뢰하여 바이오스 칩을 교체하거나 수리하는 방법밖에 없다. 따라서 치료와 관련하여 메모리 치료 방법, 파일 치료 방법 및 손상된 디스크의 복구 방법에 대하여 기술한다.

2.1 메모리 치료

CIH는 (그림 5)와 같이 윈도95의 메모리 공간 중 3GB이후의 가상 장치 드라이버가 위치하는 공간에 상주하게 되며 시스템에서 파일을 접근하기 위한 장치 드라이버인 IFSMGR(Install File System Manager)의 InstallFileSystemApiHook 기능을 수행하여 프로그램이 실행될 때마다 바이러스가 작동하도록 하여 실행하는 프로그램을 감염시킨다. 따라서 CIH를 메모리에서 제거하기 위해서는 프로그램이 실행될 때 바이러스가 실행되지 않도록 하여야 한다. 이 방법은 IFSMGR의 부가 기능들의 시작 주소 값을 갖는 테이블에서 InstallFileSystemApiHook의 시작 주소를 찾아 그 기능이 수행될 때 거치게되는 함수들의 체인 중에 바이러스가 위치하는 전후 체인을 연결함으로써 메모리 치료가 가능하다. 이미 V3Pro98/2000을 비롯한 몇 개의 백신에서 이러한 방법을 이용하여 CIH를 정확하게 치료하고 있으므로 별다른 설명이 필요 없을 것으로 보여진다.[5]

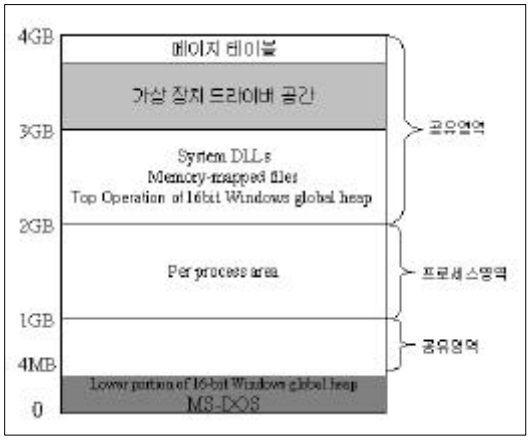

그림 5. 윈도우 메모리 구조
Fig 5. The memory structure of Windows '95
MB=Mega byte(메가바이트), GB=Giga byte(기가바이트)

2.2 파일 치료

CIH는 윈도95에서 실행되는 프로그램에 대해서만 감염을 시킨다. 파일 감염의 확산은 그만큼 바이러스 제거를 어렵게 하고 파일 치료를 하지 않는 경우 메모리 치료 이후에 다시 재감염 될 수 있다. 따라서, 파일 치료시 감염 파일을 모두 치료해야 한다.

윈도우 환경에서 사용자의 명령에 의해 수행 가능한 파일은 확장자가 COM파일과 EXE파일이다. 이중 EXE파일은 세부적으로 4가지 형식으로 각각 PE(Portable Execution)헤더, NE(New Execution)헤더, LE(Linear Execution)헤더 그리고 MZ(Magic)헤더를 가진다. 〈표 1〉는 EXE파일의 4가지 형식에 따른 실행 환경을 구분한 것이다.[6]

표 1. EXE파일의 4가지 형태
Table 1. Four types of executable files.

헤더	실행 환경
MZ	도스 환경 실행 파일
PE	윈도95/98, 윈도NT용 실행파일
NE	윈도 3.1용 실행파일 (윈도95/98/NT에서도 실행 가능)
LE	윈도95/98, 윈도NT용 가상 장치 드라이버(VxD)

CIH는 특별히 PE헤더를 가진 파일(이하 PE 파일구조)에 감염되어 실행되게 된다. 윈도우의 모든 실행 파일은 도스 환경에서 실행 가능한 영역을 가지게 되어 MZ헤더를 가지게 된다. PE의 구조

는 (그림 6)과 같으며 실제 파일에서의 구성은 (그림 7)과 같다.

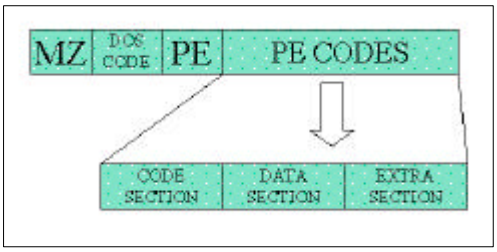

그림 6. PE의 구조
Fig 6. The structure of PE-file

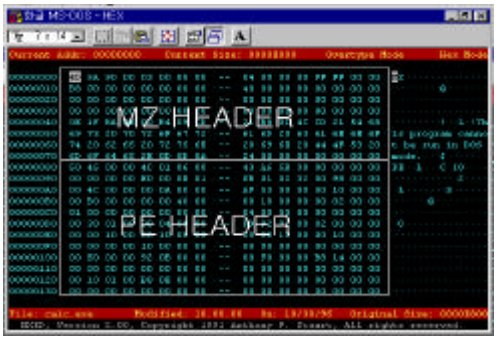

그림 7. PE 프로그램의 형태
Fig 7. The form of a PE program

CIH는 윈도우 환경에서 실행되는 프로그램에 포함되므로 PE헤더 정보를 수정하여 작동하게 된다. PE헤더의 중요한 내용은 (그림 8)과 같으며 PE헤더는 크게 두 부분으로 구성하고 있다. 앞부분은 PE파일 전체에 대한 정보들을 가지고 있고 뒷부분에서는 각 섹션들의 메모리 위치, 크기, 속성 등을 가지고 있는 섹션 엔트리로 구성되어 있다. 바이러스 치료는 PE헤더의 여러 정보 중에 몇 가지 중요한 정보를 복구한다. 치료시 복구하는 중요 정보는 우선 PE파일이 메모리에 설치될 때 기본이 되는 메모리 위치를 가지고 있는 dwImageBase, 프로그램이 실행될 때 처음 진입하게 되는 주소를 가지고 있는 dwEntryPointRVA가 있고, 사용한 섹션 수를 가지고 있는 wNumberofSections등이 있다.

dwImageBase의 경우 실제 사용되는 메모리 위치를 계산할 때 사용하는 것으로 A섹션에 설정된 가상 주소가 $1000_{(16)}$일 때 dwImageBase = $8000_{(16)}$의 정보를 이용해 보면 실제 A섹션이 위치하는 주소는 $8000_{(16)} + 1000_{(16)} = 9000_{(16)}$ 가 된다. 즉 실제 사용주소는 dwImageBase와 기본적으로 설정된 가상 주소를 덧셈하여 결정하게 된다.

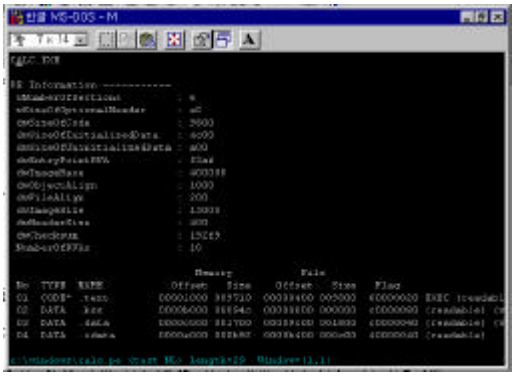

그림 8. PE헤더의 중요 정보
Fig 8. The essential information of PE header

CIH에 감염된 파일은 (그림 9)의 하단과 같이 파일 내부에 바이러스의 일부가 위치하게 된다. 이런 영역은 미사용 영역 혹은 실행에 민감하지 않은 영역이다. CIH는 최소 2개 부분에서 보통 4개 부분으로 나뉘어 PE파일 내에 위치하게 된다. 바이러스가 위치한 영역은 실행에 관계없거나 파손되어도 별 문제가 없는 영역으로 치료시 이런 부분을 모두 찾아서 정보를 모두 $00_{(16)}$으로 채워 주는 작업이 필요하다. 치료 정보는 PE헤더에 근접하는 첫 번째 부분 정보에 포함되어 있다.

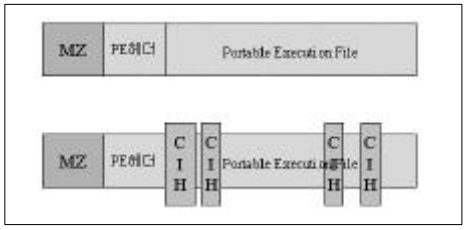

그림 10. CIH 감염 파일의 CIH 분할정보(상단-감염전, 하단-감염후)
Fig 10. Partial CIH informations in CIH infected file (top-before infection, down-infected)

감염 파일 치료는 우선 PE파일의 시작주소 (Entry Point) 정보를 읽어 첫 번째 분할 영역을 파일에서 읽어 온다. 읽어온 정보는 (그림 10)과 같으며 우선 읽어온 CIH의 몸체로부터 필요로 하는 감염전 시작 주소를 읽어온다. 그 뒤 (그림 10)의 영역에서 분할 영역에 대한 정보를 읽어 바

이러스 일부가 위치하는 분할된 영역을 모두

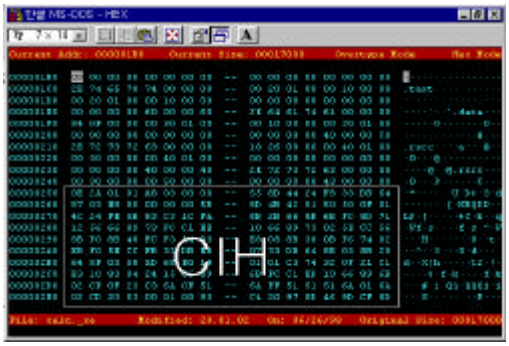

그림 11. *CIH*의 몸체 첫부분
Fig 10. The first partial information of *CIH*

00(16)을 채우며 감염시 변경되었던 섹션엔트리의 정보들을 수정하고 감염전 실행 시작 주소 값을 PE헤더에 저장하면 파일 치료는 모두 끝나게 된다.

파일 치료에 있어서 주의할 점은 윈도우 환경 하에서 실행중인 프로그램 파일의 수정을 금지하므로 반드시 MS-DOS모드를 이용하여 치료를 해야 한다. 그리고 감염 프로그램 치료시 섹션엔트리의 정보를 잘못 수정하는 경우 프로그램 수행에 문제가 생기므로 감염전 파일보다 사용하고자 하는 가상 공간의 크기 값이 작아지면 안된다. 바이러스에 감염되면 일반적으로 이런 정보 값은 증가하게 된다. *CIH*의 경우 필요로 하는 가상 메모리 크기는 증가하나 파일 크기는 변하지 않는다. 〈표 2〉은 윈도우에서 주로 사용되는 프로그램들에 대해 바이러스 감염전, 감염후 그리고 백신을 이용하여 치료한 파일의 필요한 가상 메모리 크기의 변동을 나타내는 것으로 바이러스 감염전보다 감염후 프로그램의 필요한 가상 메모리 크기가 증가하지만 백신을 이용한 치료 파일은 원본과 동일하다.

3. 피해 복구

*CIH*는 4월 26일(*CIH* V1.4의 경우 매월 26일)에 부작용을 나타낸다. 부작용은 하드디스크의 정보를 파괴하는 행위와 시스템 바이오스의 파괴를 들 수 있다. 시스템 바이오스의 파괴는 바이오스를 소프트웨어로 쉽게 교체할 수 있는 기능을 가진 PC가 대상으로, 복구시 해당 플래시 롬을 교체 혹은 수리하여야 하므로 제작사의 사후지원을 받아야 한다. 정보가 손상된 하드디스크에 중요한 데이터를 가지고 있는 경우 전문 복구 업체를 이용하는 것이 시간적으로 유리하나 보안을 요하는 경우나 복구 비용에 부담을 가지는 경우 자체 복구를

표 2. *CIH* 감염 전, 후 및 치료시 메모리 크기 변화
Table 2. The change of memory usage in normal, infected and repaired files
* *CIH*의 경우 겹쳐쓰기형 바이러스로 감염 전후 파일 크기의 변동이 없음
* No changes of the infected file size because *CIH* is a overwrite virus.

파일이름	필요한 가상 메모리			비고
	감염전	감염후	치료후	
CALC	85930	87452	85930	계산기
DLLHOST	5872	10060	5872	
EXCEL	5796854	5797536	5796854	엑셀
EXPLORER	168514	169408	168514	탐색기
HMAPSI	110613	111388	110613	
HNCCFG	35475	36332	35475	
HNCHELP	94328	95024	94328	
HNCMEMO	50662	51440	50662	
HWPDIC	8785	9642	8785	한글 사전
NETSTAT	20306	21926	20306	
NOTEPAD	45216	47232	45216	메모장
POWERPNT	3454956	3455916	3454956	파워포인트
REDIR32	10280	13204	10280	
REGEDIT	88388	84914	88388	
REGWIZ	26271	29730	26271	
SPOOL32	30808	34278	30808	프린터 스풀러
TASKMAN	36384	30128	36384	
WINWORD	5661712	5662666	5661712	워드

시도하되 하드디스크 백업후 복구 작업을 수행하는 것이 좋다. 본 고에서는 복구가 가능한 경우를 정의하고 복구 과정의 예를 보여준다. 작업 대상은 윈도95/98 운영체제하에서 FAT32 파일 시스템 구조를 가지는 하드디스크로 한정한다.

3.1 하드디스크의 복구

하드디스크에는 앞부분에 윈도95의 파일 시스템 정보 영역을 가지고 있으며 주부트섹터, 도스부트섹터, FAT, 루트디렉토리(Root Directory), 데이터 영역으로 (그림 11)과 같이 구성되어 있다.

MBS의 경우 하드디스크 분할 정보인 파티션테이블(Partition Table)를 가지고 있고 DBS의

경우 하드디스크를 윈도95에서 사용할 수 있도록 하는 디스크 인식 정보인 DPB(Disk Parameter Block)를 가지고 있다. FAT에서는 각각의 파일들이 디스크의 어느 영역을 사용하는가에 대한 정보를 가지고 있고 윈도95에서는 직접 사용하는 FAT-1 테이블과 물리적인 파손을 대비한 FAT-2 테이블이 있다. 루트디렉토리는 각 디스크 드라이브의 최상위 디렉토리 정보를 가지고 있다. 여기서 복구가 가능한 경우는 FAT-1과 FAT-2 루트디렉토리가 완전히 파손되지 않은 경우에 해당한다. 만일 FAT-1과 FAT-2가 모두 파손된 경우라면 일반적인 방법에 의한 복구는 사실상 불가능한 경우이다.

복구는 우선 MBS와 DBS 정보를 찾는 단계와 FAT-1정보와 FAT-2정보간의 관계를 찾는 단계로 수행한다.

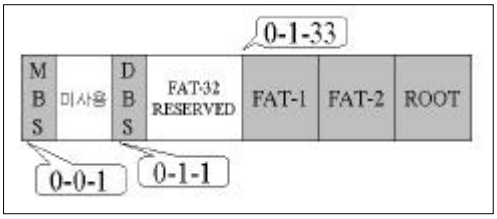

그림 11. 윈도95의 파일 시스템의 정보 영역
Fig 11. Information area of Windows '95 file system.

1) MBS와 DBS의 복구

MBS와 DBS가 파손된 경우 운영체제에서 하드디스크를 인식할 수 없게 되어 사용할 수 없게 된다. 따라서 인식 정보를 재설정 해주어야 하는데, 윈도95의 경우 일반적으로 SUHDLOG.DAT 혹은 SUHDLOG.--- 라는 파일을 만들어 MBS와 DBS에 관한 내용을 보존하고 있다. 이 파일은 *CIH*가 파괴하는 영역밖에 있는 경우가 대부분으로, 하드디스크 섹터 에디터를 이용하여 시작 부분이 '[HMR1:' 인 섹터를 찾으면 필요한 정보를 얻을 수 있다. 'SUHDLOG.DAT 혹은 SUHDLOG.---' 파일의 정보는 (그림 12)와 같으며 실선 안쪽으로 표시된 부분이 MBS의 내용이고 $3EC_{(16)}$이후 영역이 DBS의 내용이다. 두 영역을 각각 원래 영역에 복사를 하면 복구에 필요한 기본 작업을 마치게 된다.

2) FAT의 복구

FAT32시스템의 경우 FAT-1은 일반적으로 0

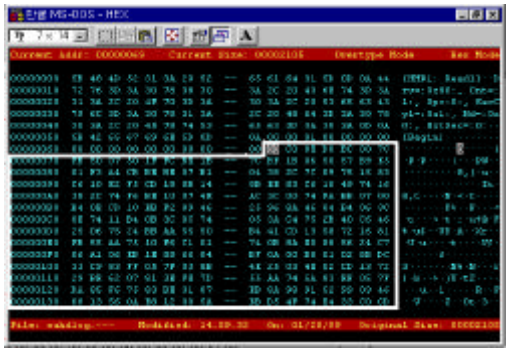

그림 12. SUDHLOG 파일의 내용
Fig 12. The information of SUDHLOG

실린더, 1헤드, 33섹터부터 시작한다. 정상적인 FAT의 형태는 (그림 13)와 같으며 첫부분이 '$F8_{(16)}$ $FF_{(16)}$ $FF_{(16)}$ $0F_{(16)}$' 로 시작한다. 위와 동일한 데이터를 가지는 FAT-2는 섹터 에디터를 통해 찾아야 한다. 만일 FAT-1의 내용이 'F8 FF FF 0F'로 시작하며 (그림 13)에서 실선으로 표시된 4바이트 값중 앞에서부터 1-2바이트 정도의 값이 있는 경우 즉 작은 값을 가지는 경우 정상이라고 할 수 있다. 만일 FAT-2정보가 손상되지 않았고 DBS정보가 있는 경우라면 디스크 복구 유틸리티를 이용하여 쉽게 복구가 가능하다. 이런 경우 복구 유틸리티는 디스크 내에서 DBS영역을 찾아 MBS정보를 새로 구성하게 되며 FAT-1과 FAT-2를 비교하여 다른 부분이 있을때 FAT-2의 정보를 기준으로 복구하고 복구가 잘못되었을 경우를 대비하여 복구 전으로 환원하는 정보를 만들게 된다.

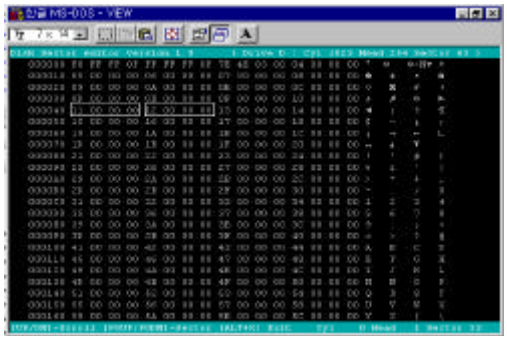

그림 14. 정상적인 FAT의 형태
Fig 13. The normal form of FAT

(그림 14)은 *CIH*에 의하여 파괴된 FAT-1의 모습이다. 정상적인 FAT의 모습과 달리 어떤 규칙성이 전혀 없다. 만일 FAT-1과 FAT-2가 모

두 이런 형태로 손상이 된 경우라면 복구가 사실상 불가능하다.

FAT-2 정보는 3기가바이트 하드디스크의 경우 *CIH*에 의해 손상되는 영역 밖에 있으므로 복구가 쉽다. 이런 경우 앞에서 말한 SUHDLOG 파일 정보만 찾아 MBS와 DBS의 정보를 복구하면 기존의 디스크 복구 유틸리티를 이용하면 쉽게 복구할 수 있다.

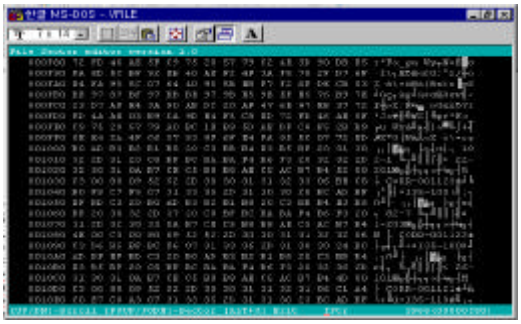

그림 14. *CIH*에 의하여 손상된 FAT
Fig 14. Damaged FAT by *CIH*

3) 복구 프로그램의 작성

만일을 대비하여 운영체제와 함께 복구 프로그램을 가진 복구 디스크를 만들어 놓는 것이 좋다. 이때 복구 디스켓은 통상 1.44MB로 용량이 제한되어 있어 운영체제로는 MS-DOS를 사용하는 것이 좋다. 디스크의 정보는 윈도95 파일 시스템이라도 BIOS가 제공하는 인터럽트 $13_{(16)}$번(이하 INT-13h)을 통하여 쉽게 접근이 가능하므로 복구 프로그램은 INT-13h를 통해 이루어진다. C로 프로그램을 작성하는 경우 _bios_disk() 함수를 이용하면 쉽게 작성이 가능하다.

_bios_disk함수는 (기능, 드라이브명, 실린더, 헤드, 섹터, 읽은데이터 저장주소) 인자를 가진다. 이때 기능은 2번이 디스크 읽기, 3번이 디스크 쓰기가 되며 드라이브명은 물리적 드라이브 번호로써 첫 번째 하드 디스크는 $80_{(16)}$이고 두 번째 하드디스크는 $81_{(16)}$이며 읽고자 하는 실린더, 헤드, 섹터와 읽은 데이터를 저장할 메모리를 지정해 주면 된다.

복구 프로그램에서 하드 디스크 정보가 있어야 한다. 실린더, 헤드, 섹터수를 알아야 한다. 첫 번째 드 디스크의 경우는 인터럽트$41_{(16)}$번의 주소에 정보가 있고 두 번째 하드 디스크는 인터럽트$46_{(16)}$번의 주소에 있다.

본 논문에서 제시한 모든 방법을 이용할 수 있도록 하는 프로그램을 C로 작성하였다. 소스 프로그램은 1100줄이고 실행 프로그램은 약 30KB로 1.44디스크에 운영체제와 필수 유틸리티를 포함하여 활용이 가능하다.

(그림 15)는 운영체제와 복구에 필요한 프로그램들을 저장해 놓은 복구 디스크의 내용이다.

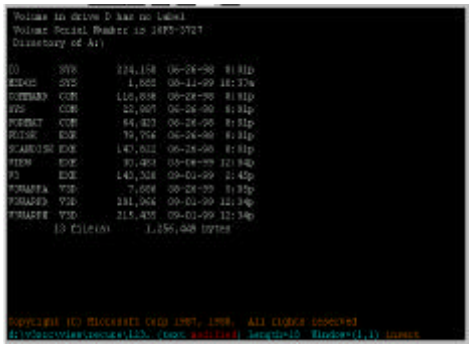

그림 16. 복구 디스크 파일 목록
Fig 15. Lists of files in SOS Disk

4 효과분석

앞 절에서 언급한 메모리, 파일의 치료 방법은 국내 두개 백신 제품과 외국의 일부 백신 제품에서 지원하고 있어 치료에 별다른 문제가 없다. 다만 치료의 관점에 차이가 있는데 이는 V3를 비롯한 잘 알려진 외국산 백신들은 대체적으로 감염 프로그램 내에서 *CIH*이미지를 완전히 없애는 반면, 한 제품의 경우 바이러스 실행 시작점에 원본 프로그램으로 분기하도록 하는 명령어를 심어 원본 프로그램을 실행하도록 하고 있는데 실행상 차이는 없지만 이는 다른 문제점을 유발할 수도 있는 방법이며 다른 백신을 사용했을때 바이러스가 있다고 진단할 수도 있으므로 바이러스 이미지를 완전히 지우는 것이 바람직하다. 최근 중국 공안당국에서는 *CIH* 치료후 이미지를 지우지 않아 중국 백신에 의해 감염 파일로 오진해 프로그램 배포자를 추적하는 한편 국내에 감염 여부 확인을 요청한 사례가 있었다. (그림 16)과 (그림18)은 각각 감염된 윈도95의 CALC.EXE에서 *CIH*의 첫부분과 마지막 부분을 보여주는 그림이고 (그림 17)과 (그림 19)는 해당 영역에서 *CIH*를 제거한 그림이다.

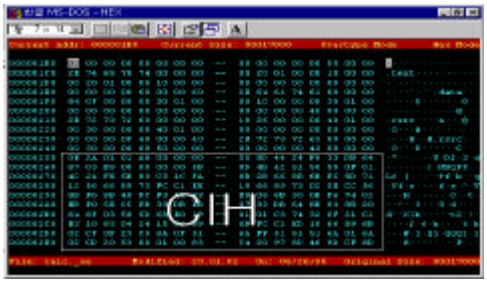

그림 17. CIH감염된 CALC.EXE의 첫부분
Fig 16. The first part of the CIH-infected CALC.EXE

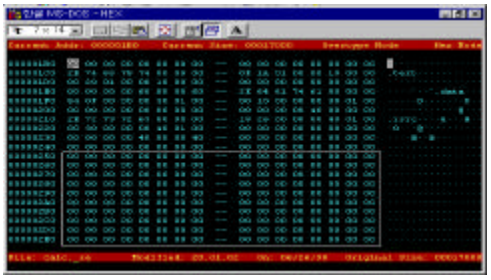

그림 18. CIH를 치료한 CALC.EXE의 첫부분
Fig 17. The first part of CIH-repaired CALC.EXE

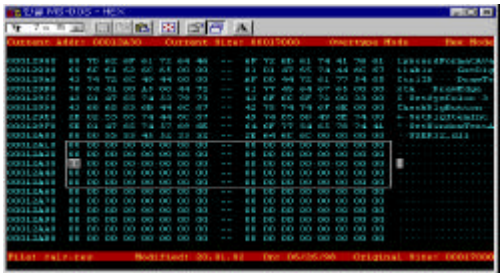

그림 19. CIH를 치료한 CALC.EXE의 뒷부분(CIH의 마지막 부분)
Fig 19. The last part of the CIH-repaired CALC.EXE

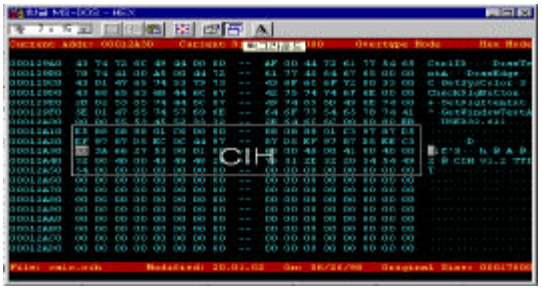

그림 20. CIH에 감염된 프로그램 뒷부분(CIH의 마지막 영역)
Fig 19. The last part of the CIH-infected file

CIH는 앞부분부터 2048섹터만큼 완전히 파괴를 하므로 흔히 사용하는 고용량 하드디스크의 경우 MBS, DBS, FAT-1이 파괴되므로 제안된 복구 방법을 통해 FAT-2를 FAT-1에 복사하고 데이터 영역에서 MBS와 DBS 정보를 찾아 복구하면 완전하게 복구가 가능하다. 그러나 2GB정도의 저용량 하드디스크의 경우 MBS, DBS, FAT-1, FAT-2 영역이 완전히 손상되는 경우가 많아 일부, FAT-1과 FAT-2의 특정 영역만 손상되는 경우 제한적으로 사용할 수 있다. 이런 경우, FAT-2의 내용과 FAT-1의 내용을 적절히 비교하여 복구하게된다. 만일 루트디렉토리가 모두 손상된 경우라면 완전한 복구는 사실상 불가능하다. 루트디렉토리의 일반적인 형태는 (그림 20)과 같으며 파일 이름이나 디렉토리 이름 등을 가지고 있다.

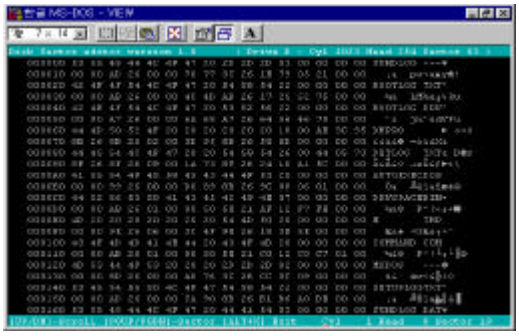

그림 20. 정상적인 루트디렉토리 형태
Fig 20. The normal form of Root directory

5. 대비책

CIH의 경우 백신을 사용하여 충분히 대비할 수 있으며 감염시 치료 방법을 정확하게 알고 있다면 최근 발생한 것과 같은 엄청난 피해는 더 이상 반복되지 않을 것이다. 백신 제작사들은 폭넓은 정보 수집을 통하여 악성 바이러스를 예방, 치료할 수 있는 백신을 제작하고 있다. 바이러스에 따르는 백신 사용상 주의점을 잘 지킨다면 CIH와 같은 악성 바이러스에 대한 피해를 방지할 수 있다. (그림 21)은 상용화 백신 제품인 V3Pro98에서 윈도우 메모리에 감염된 CIH를 진단 치료하는 것이고 (그림 22)는 CIH 감염 파일을 복사하거나 실행했을 때 시스템 감시 프로그램에서 바이러스를 차단한 것이다.

그림 21. 윈도우 메모리내의 *CIH* 진단 및 치료
Fig 21. *CIH* detection and reparing in Windows '95 Memory

그림 22. *CIH* 감염 파일의 복사 및 실행 차단
Fig 22. The cancellation of exeucting *CIH*-infected file

Ⅳ. 결론

지금까지 발견된 바이러스들은 대체로 특정한 운영체제(윈도95/98 혹은 도스)에서 작동하는 것이 일반적이다. 그러나 최근에는 매크로 바이러스에서 볼 수 있듯이 운영체제가 아닌 환경에서도 작동이 가능한 것들이 많이 나타나고 있다.

우리나라에서 발견되었던 바이러스들은 주로 외국산 바이러스의 변형 바이러스이다. 그러나 1997년부터 순수 국내 제작 바이러스가 다수 출현하였으며 1998년 이후 점점 복잡해지고 피해가 커지고 있다. 앞으로 *CIH* 출현을 시작으로 비슷한 증상을 가지는 바이러스들이 다수 나타날 것으로 보인다. 따라서 최근의 *CIH*피해에서 보았듯이 치료가 가능한 백신이 다수 존재했음에도 상당한 피해가 있었던 것은 바이러스에 대한 예방 방법 그리고 제거 방법을 홍보하는 것보다 *CIH* 자체의 특징만을 홍보한 결과로 분석된다.

본 논문에서는 윈도우 환경에서 백신 사용의 주의점을 설명하였고 하드디스크 복구 방법을 제안하였다. 제안된 하드디스크 복구 방법은 바이러스에 의한 손상뿐만 아니라 원인 불명의 이유에 의해서 MBS와 DBS 그리고 FAT의 일부가 손상된 경우까지 확대 적용이 가능하며 기존의 방법에 비하여 저렴하고 과정상 복잡함이 없다.

앞으로의 과제는, 기 제작된 복구 유틸리티의 기능을 향상시켜 모든 과정을 자동으로 수행할 수 있도록 하여 누구나 쉽게 사용할 수 있는 응용 프로그램을 작성하는 것이다.

참고문헌

〔1〕 "98년 바이러스동향", 안철수컴퓨터바이러스뉴스, *안철수연구소*, Apr. 1999, pp.16-17.
〔2〕 안철수, *바이러스 분석과 백신 제작*, *(주)정보시대*, 1994.
〔3〕 안철수, *바이러스 예방과 치료*, *(주)정보시대*, 1997.
〔4〕 안철수, "컴퓨터 바이러스와 악성코드의 현황 및 대책", 정보보호 심포지움, Apr. 1999, pp. 399-410.
〔5〕 Randy Kath, "Managing Virtual Memory in Win32", Microsoft Developer Network Technology Group, 1993.
〔6〕 Matt Pietrek, *Windows Internals*, Addison-Wesley, 1993.

▫ 著者紹介

황규범 (Kyu-beom Hwang) 학생회원

1998년 2월 : 한남대학교 수학과 졸업(학사)
1995년 4월~현재: 안철수컴퓨터바이러스연구소 주임연구원/엔진팀장
1998년 3월~현재: 한국정보통신대학원대학교 석사과정

〈관심분야〉 컴퓨터 안티바이러스, 정보보호와 암호이론 및 응용

김광조 (Kwangjo Kim) 종신회원

1979년 2월: 연세대학교 전자공학과(학사)
1983년 2월: 연세대학교 전자공학부(석사)
1991년 2월: 요꼬하마 국립대 전자정보공학부(공학박사)
1979년12월~1997년12월 : 한국전자통신연구원 부호1실장
1996년 3월 ~ 1997년 8월 : 충남대학교 컴퓨터과학과 겸임 교수
1998년 1월 ~ 현재 : 한국정보통신대학원 공학부 교수, 본학회 학술(국외) 이사, 세계암호학회 회원, Asiacrypt 조정 위원회 위원,

〈관심분야〉 정보보호와 암호 이론 및 응용

안철수 (Charles Ahn) 정회원

1986년 2월: 서울대학교 의학과 졸업(학사)
1991년 2월: 서울대학교 의대 대학원 졸업(석/박사)
1997년 8월: 펜실베니아 대학 공대 및 왓튼스쿨(경영공학석사)
1991년 2월: 서울대학교 의학과(의학박사)
1989년 9월~1991년2월 : 단국대학교 의과대학 의예과 학과장
1991년 2월 ~ 1994년 4월 : 해군 군의관
1995년 2월 ~ 현재 : 안철수컴퓨터바이러스연구소 대표
본학회 산학이사, 서울지검 정보범죄수사센터 자문위원, 아시아바이러스연구협회 부회장, 정보보호산업협회 부회장

〈관심분야〉 컴퓨터 안티바이러스, 정보보호