한국통신정보보호학회
충정지부 학술대회 99

컴퓨터 바이러스의 기법 분석(I)

황규범*, 김광조*, 안철수**

Analysis Computer Virus Schemes

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

요 약

본 논문에서는 악성 프로그램 중 피해가 큰 컴퓨터 바이러스에 대하여 정의를 하고 십수년간 국내에 발견된 바이러스들의 주요 기법을 분석하고 최근의 바이러스 발견 동향에 대하여 기술하고 대책을 제시하며 바이러스에서 사용하는 기법들은 결과적으로 많은 사람에게 피해를 입히는데 사용되고 있어 그 자체가 무가치함을 결론으로 논문을 맺는다.

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 방해하는 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 중심으로 주요 기법을 분석하고 유형 및 감염 경로에 대하여 기술하고 그에 대한 대책을 제시한다.

(그림 1)은 우리 나라에 뇌(Brain)바이러스가 처음 발견된 1988년부터 1998년 말까지 국내에 발견된 바이러스들을 출처별, 종류별로 그 수를 파악한 것으로 1996년 이후 상당히 큰 증가세를 보이고 있다.[1]

본 논문의 구성은 제2장에서 컴퓨터 바이러스의 정의와 부위별 분류법에 대하여 기술하고 제3장에서는 1988년부터 1999년 초까지 국내에 발견된 바이러스들의 기술 특징을 분석하고, 제 4장에서는 바이러스 예방 대책에 대하여 기술하고 제 5장에서는 결론을 기술한다.

88~98년 종류별 바이러스 동향(단위: 종)

연 도	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	총계
부 팅	1	4	8	5	6	10	13	18	8	15	14	101
파 일		2	10	15	11	23	50	105	180	220	123	661
매크로									1	16	36	53
부트/파일			2	1	1	1	3	5	29	5	7	54
합 계	1	6	20	21	17	34	76	128	226	256	276	1069

그림 2. 1988부터 1998년 컴퓨터 바이러스 발견 동향

Ⅱ. 바이러스의 정의 및 분류

1. 바이러스 정의

컴퓨터 바이러스의 정의는 수식에 의한 일반적인

* 한국정보통신대학원대학교 공학부 암호와 정보보안 연구실 (kityhwang@icu.ac.kr) (kkj@icu.ac.kr)
** 안철수컴퓨터바이러스연구소 (cahn@ahnlab.co.kr)

정의가 용이하지 않으므로 언어적 정의를 따른다. 본 논문은 [2]의한 정의를 기본으로 이해가 용이한 생물학적 정의를 따른다.[3]

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 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 말을 사용했으나 매크로와 스크립트를 이용한 바이러스들이 많이 나타남에 따라 바이러스 코드로 그 의미를 확장시키게 되었다.

컴퓨터 바이러스들은 컴퓨터 상에서 수행되는 것을 말하며 이하 간결하게 바이러스라고 하고, 보다 의미를 명확하게 할 필요가 있는 경우에 한하여 바이러스 프로그램 혹은 바이러스 코드라고 한다.

본 논문에서의 바이러스 이름은 한글과 영문을 병행 표기하고 이탤릭체와 밑줄로써 구분한다. 그리고 바이러스를 예방, 진단 및 치료를 하는 안티바이러스 프로그램(Anti-Virus Program)을 통칭하여 백신이라고 한다.

바이러스들은 자기 복제 능력 외에도 생물학적 바이러스와 같이 부작용을 가지는 경우도 있다. 이런 부작용은 컴퓨터의 처리 속도를 늦게 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.

바이러스에 대한 분류는 여러 방법이 가능하나 본고에서는 감염 부위에 따라 분류를 한다. 감염 부위이란 바이러스 프로그램이 위치하는 영역을 말하는 것으로 크게 4가지로 구분할 수 있다. 부트 영역에 감염되는 부트 바이러스와 파일에 감염되는 파일 바이러스, 그리고 부트 영역과 파일에 모두 감염되는 부트/파일 바이러스 그리고 최근 많이 사용하는 엑셀, 워드 프로그램에서 사용하는 매크로를 통하여 감염되는 매크로 바이러스가 있다.[4]

• 부트 바이러스 (Boot virus)

컴퓨터가 처음 가동되면 디스크의 가장 처음 부분인 부트섹터에 위치하는 프로그램이 가장 먼저 실행되는데, 이곳에 자리잡는 컴퓨터 바이러스를 부트 바이러스라고 한다. 대표적으로 *뇌(Brain)*와 지금까지도 많은 피해를 주고 있는 *원숭이(Monkey)* 및 감염 빈도가 높은 *Anti-CMOS* 등이 있다.

• 파일 바이러스(File virus)

파일 바이러스란 실행 가능한 프로그램에 감염되는 바이러스를 말한다. 이때 감염되는 대상은 실행 파일이 대부분이며 (그림 1)에서와 같이 바이러스의 80% 정도가 파일 바이러스에 속한다. 국내에서는 *예루살렘(Jerusalem)*과 *일요일(Sunday)*를 시작으로, 1997년과 1998년 적지 않은 피해를 주어 잘 알려진 *전갈(Scorpion)*, *까마귀(Crow)* 그리고 *FCL*이 있으며 최근 아시아 지역에 많은 피해를 주었던 *CIH*도 이에 포함된다.

• 부트/파일 바이러스(Multipartite virus)

부트/파일 바이러스는 부트섹터와 파일에 모두 감염되는 바이러스로 대부분 크기가 크고 피해 정도가 큰 것이 특징이다. 우리 나라에서는 1990년 처음 발견된 *침입자(Invader)*를 대표로 외국보다 빠른 대처로 인하여 이름에 혼란이 주었던 *안락사(Euthanasia)*가 있다. 국내 제작 바이러스로는 1998년에 발견된 *에볼라(Ebola)*가 대표적이다.

• 매크로 바이러스 (Macro virus)

최근 발생한 새로운 형태의 파일 바이러스로 감염 대상이 실행 파일이 아니라 마이크로소프트사의 엑셀과 워드 프로그램에서 사용하는 문서 파일이라는 점과 응용 프로그램에서 사용하는 매크로 사용을 통해 감염되는 형태로 매크로를 사용하는 문서를 읽을 때 감염된다는 점이 이전 바이러스들과는 다르다. 대표적인 예로 감염 비율이 매우 높았던 *라루(XM/Laroux)*를 들 수 있다.

Ⅲ. 기법 분석

본 장에서는 뇌가 발견된 1988년부터 1999년 4월까지 바이러스 제작에 사용된 방법이나 백신 입장에서의 기법 변화를 단계별로 작성하였다. 단계 구분은 백신에서 처리한 시기를 기준으로 할 수도 있고 특정 바이러스가 실제로 보고된 시점을 기준으로 할 수도 있다. 또한 연구하는 사람에 따라서 다른 기준을 가질 수 있다. 본 고에서는 국내 발견

된 바이러스를 기준으로 하며 발견 시점을 기준으로 하였다. 따라서 활성화된 시점과 다를 수 있다.

우리 나라에서는 매년 상당수의 바이러스가 발견되고 있다. 특징적인 것으로는 국내에서 제작된 바이러스가 외국에서 제작된 바이러스 수보다 2배정도 많다. 특히 1998년의 경우, 한 해 동안 많은 피해를 주었던 바이러스들은 대체로 *시스터보*의 공개 소스 코드를 변형한 것들이었다. 이로 인해 바이러스 소스의 공개는 더 많은 바이러스를 만들게 되어 순기능보다 역기능이 더 크다는 것을 보여준다.

▪ 1단계(1988-1989) : 부트 바이러스 출현

국내에서 최초로 발견된 바이러스는 뇌이며 이 시기에 발견된 바이러스들은 대체적으로 간단한 부트 바이러스가 주종을 이루고 있다. 이 시기에는 바이러스에 대한 별다른 지식이 없었고 불법 복사가 만연해 있어서 바이러스의 확산이 빠르고 광범위했다. 대표적으로 *뇌* 및 *LBC*, *LBC.II*, *돌.B(Stoned.B)*가 있다.

▪ 2단계(1989) : 파일 바이러스 출현

바이러스 감염 대상이 프로그램 파일로 프로그램의 실행시 바이러스가 먼저 실행되고 원본 프로그램이 수행되는 형태의 기생형 바이러스들이 나타나게 되었다. 이 시기에 발견된 바이러스들은 크기는 컸으나 간단한 유형의 바이러스로 *예루살렘(Jerusalem)*, *일요일(Sunday)*이 대표적이다.

▪ 3단계(1990) : 부트/파일 바이러스의 출현

1990년 11월 경에 국내에서 처음 부트와 파일을 동시에 감염시키는 바이러스가 발견되었다. 부트/파일 바이러스의 경우 메모리에 상주하여 실행하는 프로그램이나 사용하는 플로피디스크와 하드디스크를 감염시키는데 부트와 파일 영역을 모두 감염시킬 수 있으므로 확산이 빠르다. 대표적으로 *침입자(Invader)*가 있다.

▪ 4단계(1991) : 새로운 형태의 연결형 바이러스 출현

1991년 11월 그간 바이러스와 전혀 다른 특징을 가진 바이러스가 출현하였다. 이 당시 발견된 *DIR_II*는 MS-DOS의 파일시스템의 FAT(File Allocation Table)의 연결구조를 이용하며 바이러스 감염시 프로그램의 크기를 증가시키지 않고 기생할 수 있는 특징을 가진다. 이 바이러스의 경우 FAT 연결구조만 수정하게 되므로 감염 속도가 빠르고 아주 광범위하게 감염된다. 바이러스에 의해 원래 FAT정보가 암호화되어 있으므로 치료시 한 디렉토리에 있는 모든 파일을 한번에 치료해야 하므로 치료시 주의가 필요한 바이러스이다.

▪ 5단계(1992) : 외국 바이러스의 국내 변형 시작

이시기에 들어서 외국에서 들어온 바이러스에 대하여 부트 및 파일까지 국내 제작자들에 의해 변형되기 시작하였다. 대체적으로 메시지를 변형하는 정도이지만 많은 부분을 변형하여 새로운 국산 바이러스를 만들어내는등 광범위하게 변형 작업이 이루어졌다. 대표적으로 *한국변형 예루살렘(Jerusalem.Kr)*, *한국변형 어둠의 복수자(Dark_Avenger.Kr)*등이 있다.

▪ 6단계(1993) : 간단한 다형성 암호화 바이러스의 출현

지금까지 바이러스들은 단순한 형태로 고정적인 암호화 방법을 가지고 있었다. 하지만 이 시기에 출현한 바이러스들은 복수의 암호키를 사용하거나 암호화 방법이 감염시마다 변하는 형태의 바이러스들이 출현하여 분석을 어렵게 하였다. 대표적으로 *몰타아메바(Maltese_Amoeba)*가 있다.

▪ 7단계(1994) : 국산 암호화 바이러스의 전성기

1994년들어 국산 바이러스가 폭발적으로 증가하였다. 동년 하반기에 들어서 암호화 바이러스가 다수 출현하였고 한 사람이 여러 개의 바이러스가 변형 제작하여 국산 바이러스들도 그룹형태를 가지게 되었던 시기이다. 그리고 이시기에 국내 암호화 바이러스의 모태가 되는 *시스터보* 바이러스가 발견되었다. 대표적으로 *방랑자(Wanderer)*, *넥스트(Next)*, *HWB*등이 있으며 이들 바이러스는 한 해에 2종류 이상의 변형이 나타났다.

▪ 8단계(1995) : 다형성 바이러스의 본격화

백신이 바이러스 코드의 특징을 찾아 검색한다는 것이 널리 알려지면서 바이러스 제작자들은 암호화 방법을 구현하는 코드들을 변화시켜 특징을 찾기 어렵도록 하여 백신의 검색을 피할 수 있도록 하는 방법이 사용되기 시작한 시기로, 바이러스를 진단, 치료하기 위한 분석 및 기술 개발에 많은 시간이 소요되기 시작한 시기이다. 이 당시 백신은 바이러스와 동일한 암호 해제 루틴을 갖추게 되어 백신 개발이 지연되고 백신 자체의 크기도 커지게 되었다. 대표적으로 *경련(Tremor)*, *나타스(Natas)*, *절반(One_half)*등 있으며 1995년 상반기에 집중적으로 발견되었다.

▪ 9단계(1995) : 광범위하게 피해를 준 연결형 바이러스 출현

1995년 11월에 처음 발견되어 널리 퍼졌던 *DIR_II* 바이러스는 DOS 3.3이하 판에서만 작동하였다. 1995년경에는 대부분 DOS 4.0이상의 판을 사용하고 있었으므로 별다른 문제가 없었으나 1995년 10월에 *바이웨이(Byway)*가 발견되어, 광범위하게 확산됨으로써 그 피해가 컸다. 바이웨이는 *DIR_II*와 마찬가지로 DOS의 파일시스템의 FAT(File Allocation Table)의 연결구조를 이용하며 바이러스 감염시 프로그램의 크기를 증가시키지 않고 기생할 수 있는 특징을 가진다. 이 바이러스의 경우 FAT 연결구조만 수정하게 되므로 감염 속도가 빠르고 아주 광범위하게 감염된다.

▪ 10단계(1996): 메모리 은폐형 바이러스 출현

이전까지의 바이러스들은 쉽게 분석이 가능했으며 메모리 상주시 메모리 내에서 쉽게 찾아낼 수 있어 백신에 의해 간단히 치료가 가능하였다. 그러나 이 시기에는 바이러스 몸체를 암호화하여 은폐시킴으로써 메모리 내에서 바이러스를 쉽게 찾아내지 못하도록 하여 바이러스 분석 및 백신제작을 지연시키는 결과를 가져온 *먹깨비(Mange-tout)*는 분석을 어렵게 하여 치료법 개발이 많이 지연되었다.

▪ 11단계(1996) : 새로운 개념의 바이러스 출현

사용자의 편의를 위하여 문서 편집기와 워크쉬트와 같은 프로그램에서 작성하는 문서에는 작업을 용이하게 하기 위한 매크로를 이용하여 수행하는 경우가 많다. 1996년 6월 국내에 처음 *컨셉트(WM.Concept)*가 발견되어 바이러스가 운영체제 위에서 작동하는 프로그램으로 규정하였던 과거와 달리 매크로나 스크립트 환경에서도 작동할 수 있으므로 감염 대상을 보다 광범위하게 설정하게 되었으며 매크로 바이러스는 주로 기업 환경에서 광범위하게 확산되어 그 피해가 컸다.

▪ 12단계(1996) : 윈도용 바이러스 출현

1996년 우리 나라에도 윈도95가 소개되어 많은 사람들이 사용하기 시작하였다. 윈도95의 경우 바이러스에 안전할 것이라고 인식하고 있던 때 외국에서 *보자(Win95/Boza)*가 발견되어 떠들석하였다. 다행히 한글 윈도95에서는 실행되지 않아 문제가 없었지만 1996년 6월경 *촉수(Win16/Tentacle)*와 *촉수.II(Win16/Tentacle.II)*가 발견되어 한글 윈도95 운영체제가 바이러스에 안전하지 않음이 확인되었고 앞으로 많은 윈도용 바이러스가 출현할 것을 예고하였다.

▪ 13단계(1997) : 다형성 바이러스의 진보

1997년 3월에, 외국산 다형성 바이러스인 *Level_III*를 내부적으로 일부 변형한 *FCL*이 국내에서 발견되었다. 기존 바이러스들은 제한된 범위내에서 변화하는 최소한의 규칙을 가지고 있었지만 *FCL*바이러스는 이러한 규칙을 가지지 않고 상당한 수준의 프로그래밍 능력을 가지고 있어 백신의 개발이 상당히 지연되었었다. 이 바이러스의 경우 *Level_III*를 진단할 수 있는 외국산 백신으로 진단이 불가능하였고, 개인에서 대규모 학원에 이르기까지 광범위하게 확산되었으며, i486컴퓨터에서는 프로그램 파괴 증상을 가지게 되어 많은 피해가 보고되었다.

▪ 14단계(1997-1998) : 본격적인 윈도95, 윈도NT 바이러스 출현

1996년에 발견된 *보자(Win95/Boza)*바이러스의 경우 윈도우 바이러스로 볼 만한 특징점이 없었고 한글 윈도95에서는 실행되지 않는다는 점에서 별다른 문제가 없었다. 그러나 1997년 11월 한글 윈도95에서 상주하는 *아편걱정(Win95/Anxiety_Poppy)* 가 12월에는 *아편걱정.II(Win95/Anxiety_Poppy.II)* 발견되었고 제작되어 그 피해가 확산되었으며 새로운 운영체제 위에서 작동하는 바이러스의 제작 기법들이 소개되었으며 분석 및 백신 개발은 도스와 전혀 다른 형태의 접근이 필요하게 되었다. 윈도95용 바이러스는 , *마르부르크(Win95/Marburg)* 가 있으며 국산은 1998년 10월에 *전갈.1275(Win95/Scorpion.1275)*가 처음 발견되었다.

▪ 15단계(1998) : 다형성 매크로바이러스

1996년 처음 발견된 매크로 바이러스는 1998년 그 수가 35종을 넘어섰다. 매크로 바이러스의 경우 기업 사무환경에서 감염 및 확산되고 있어 피해가 큰 것이 특징이며 1998년 하반기에 발생한 *엑스트라스(XM/Extras)*와 *클래스(WM97/Class)*의 경우 기존의 매크로 바이러스와 달리 다형성 바이러스의 특징을 가지게 되어 분석 및 치료 기술 개발을 어렵게 하는 의도를 가지게 되었다.

▪ 16단계(1999) : 새로운 방식의 바이러스 출현 가능성 예고

1999년 초에 들어서 매크로 바이러스는 정보 유출 기능을 가지게 되었다. 국내에서는 별다른 피해가 없었지만 미국 전역에 확산되어 사회 문제시 되었던 *멜리사(W97M/Malissa)* 바이러스와 MS아웃룩 프로그램의 주소록에 있는 60명에게 자동으로 메일을 보내게 하는 기능을 가진 *파파(X97M.Papa)* 소식이 언론에 공개되어 기업의 중요 자료 유출 가능성에 대한 경각심을 새롭게 가지는 계기가 되었다.〔5〕

▪ 17단계(1999) : 시스템 불능 상태로 만든 바이러스에 의한 대규모 피해

윈도95 바이러스가 1997년 이후 꾸준한 증가세를 보이고 있다. 1998년 6월 *CIH*가 출현하면서 바이러스의 부작용에서 하드웨어 시스템의 파괴 불가라는 통념을 깨고 바이오스 영역을 파괴하고 하드디스크의 정보를 파괴하는 증상을 가지고 있어 시스템을 직접적으로 불능상태로 만들 수 있는 기법이 적용되었다. 이는 1997년 이후 주변장치들의 빠른 발전으로 인해 바이오스의 교체가 빈번해 짐에 따라 소프트웨어적인 개선이 가능하도록 하는 플래시메모리가 채용됨으로써 생긴 취약점을 이용한 것으로, 플래시메모리를 이용하는 컴퓨터 시스템 혹은 주변장치를 정지시킬 수 있다. 이러한 취약점을 이용한 *CIH*는 1999년 4월 국내에 천문학적인 피해를 입혀 바이러스의 위험성을 인식할 수 있는 계기가 되었다.

Ⅲ. 최근 바이러스의 주요 유형과 감염 경로

1. 유형

최근 발견되는 바이러스들은 주로 윈도우 바이러스와 매크로 바이러스로 그 수의 증가뿐만 아니라 피해 규모도 점점 커지고 있다. 〔표 1〕은 1998년 한해동안 접수된 피해 사례를 통계된 것으로 윈도우 바이러스와 매크로 바이러스의 피해가 상대적으로 크다는 것을 보여주고 있다.〔6〕

표 1. 1998년 최다 피해 신고 바이러스 순위

순위	이름	점유율	신고건수	비고
1	엑셀매크로	22.6%	4,854	매크로바이러스
2	CIH	12.7%	2,728	윈도95바이러스
3	원숭이	5.6%	1,203	부트바이러스
4	안티-CMOS	4.1%	881	부트바이러스
5	절반	2.3%	494	부/파바이러스

1) 윈도우 바이러스

최초의 윈도우 바이러스는 *WinVir*로 1992년에 외국에서 처음 발견된 것으로 보고되고 있다. 국내에 처음 알려진 윈도우 바이러스는 1996년에 *보자(Win95/Boza)*로 아주 간단한 바이러스이며 한글 윈도95에서는 실행이 되지 않았다. 하지만 그 해 6월 윈도 3.1용 바이러스인 촉수(Win16/Tentacle)가 국내에 발견되었으며 이후 1997년 12월 메모리에 상주하는 *아편걱정(Win95/Anxiety_Poppy)*이 발견되었고, 1998년 11월 다형성 기법을 가진 *HPS*가 발견되었다.

1998년 6월에 처음 발견되어 1999년 4월 아시아 지역에서 상당한 피해를 주었던 *CIH*는 국내 대형 PC통신망에 올려진 자료에 의하여 국내에 처음 유입되었으며 최근에도 PC통신망 자료실의 일부 자료가 *CIH*를 가지고 있는 것으로 확인되고 있으며 최근 출판된 서적의 부록 CD에서도 발견되어 전량 교체해 주는 등의 사례가 나타나고 있다.

국내에서는 1996년 11월에 맹위를 떨쳤던 *전갈(Scorpion)* 시리즈를 만들어낸 Teak Soft라는 국내 그룹에 의하여 1998년 10월 국내에서 제작된 *전갈.1275(Win95/Scorpion.1275)*가 처음 발견되어 국내에서도 윈도우 바이러스의 제작이 시작되었음이 확인하였다.〔7〕

1999년의 경우 전반적으로 인터넷을 기반으로 하여 전자우편을 통한 자료 유출 가능성을 보여주는 프로그램인 *I-Worm/Happy99*와 실제 사용자의 문서 자료들을 광범위하게 손실시키는 *I-Worm/ExplorerZIP*을 비롯하여 최근에 소개된 *백오리피스(Win-Troyjan/Back_Orifice)*등으로 인하여 정보 보호의 중요성이 강조되고 있다.

인터넷 웜의 경우 인터넷을 넓은 의미의 운영체제로 보아 바이러스의 개념을 사용하기도 한다.

2) 매크로 바이러스

기업 환경에서 많이 사용하는 MS워드나 엑셀등 MS오피스 제품군의 매크로를 이용한 바이러스가 전세계적으로 다량 작성되어 유포되고 있다. 매크로 바이러스의 확산은 감염된 문서의 교환을 통하여 이루어지며 최근에는 *클래스(WM97/Class)*와 *엑스트라(XM/Extras)*와 같은 다형성 바이러스들도 나타나고 있다. 바이러스 유형에서 다형성

바이러스가 가장 복잡한 점을 감안할 때 매크로 바이러스의 발전 정도가 매우 빠르다는 것을 짐작해 볼 수 있다.

특히 1998년 2월경, 국내에서 변형 제작된 한국변형 *라루(XM/Laroux.Kr)*가 발견되어 매크로 바이러스 영역에서도 국내 바이러스 제작자들이 활동하고 있다는 것이 확인되었다. 현재 한국변형 라루는 약 10여종이 있다.

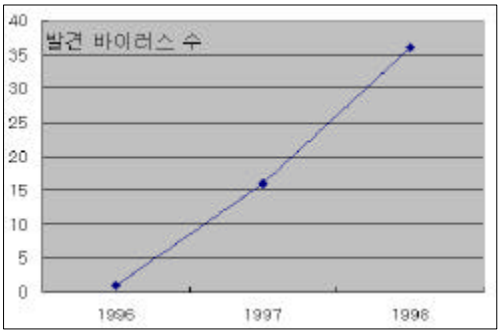

그림 3. 국내 매크로 바이러스 발견 증가세

2. 감염 경로

바이러스의 유입 경로는 다양하고 매우 복잡한 구조를 가진다. 본 절에서는 여러 경로중 대표적인 2가지 경로만 기술한다. 첫 번째 경로는 사용자가 필요로 하는 유틸리티 프로그램을 외부로부터 입수하여 사용하는 과정에서 유틸리티 프로그램이 바이러스 감염 파일 혹은 그 자체가 바이러스인 경우를 들 수 있고, 두 번째 경로는 자료 교환 및 공유에 있어 상대방의 부주의로 인해 감염된 상태로 전달되어 그 정보를 이용함으로 인해 감염되는 경우이다. 수년 전에는 거의 모든 바이러스 감염은 소프트웨어 복제에 의해서 주로 이루어졌지만 최근의 경로들은 PC통신망과 인터넷을 통한 바이러스 감염이 대부분이다.

1) 유틸리티로 가장한 바이러스 확산

최근 발생하는 바이러스들은 유용한 유틸리티로 가장한 경우가 많다. 이런 경우 제작자가 바이러스 확산을 목적으로 하는 매개체로 많은 사람들이 사용을 원하고자하는 프로그램을 통해 바이러스를 전파시킨다.

이런 종류의 바이러스로 우선 윈도우 바이러스인 *CIH*를 들 수 있다 *CIH*는 'MoviePlay V1.46'에 감염되어 유포되었고, 1998년 맹위를 떨쳤던 *알트엑스*는 'V31200.EXE'로 V3+의 최신버전을 가장하여 유포가 되었으며 *전갈*은 유명한 세어웨어 프로그램인 MDIR을 정품 프로그램으로 만들어주는 크랙 프로그램을 통하여 유포되었고 *납벌.1480*은 이야기7.3 크랙 파일이라는 이름으로 유포되었다.[8]

이와 같이 바이러스의 유포 경로를 추적해 보면, 유용한 유틸리티로 가장하여 PC통신망이나 인터넷을 이용하여 바이러스가 확산된 경우가 많다. 특히 우리 나라에서는 인터넷보다는 사설 PC통신망을 통한 확산이 매우 빠르다.

2) 정보교환을 통한 바이러스의 확산

정보교환을 통한 바이러스 이동은 바이러스 감염 프로그램의 실행이 아닌 워드 문서 혹은 엑셀 문서 파일과 같은 데이터 파일의 교환을 통하는 것이다. 이런 경우는 이전까지는 없었던 형태로 정당한 사용자임에도 바이러스가 걸릴 수 있다는 점에서 기존의 바이러스들과는 다른 성격을 가진다.

문서 파일의 경우 상대방을 신뢰한다는 가정에서 필요한 정보를 교환하게 되며 주로 기업이나 관공서와 같은 곳에서 이용하고 있다. 따라서 매크로 바이러스의 경우 주공격 대상이 일반 이용자가 아닌 그룹 이용자가 되고 있으며 문서 파일 작성자가 고의로 바이러스를 확산시키기 위한 목적으로 의도적인 문서 교환에 따른 것보다 외국에서 입수된 문서를 통해 감염되어 확산되는 경우가 많아 외국과 문서 파일 교환이 많은 다국적 기업이나 대학 혹은 대학원과 같은 고등교육기관에서 보내진 문서의 경우 바이러스 감염 빈도가 높다.

Ⅳ. 대책

바이러스의 피해를 줄이는 가장 좋은 방법은 예방이다. 현재 가장 좋은 예방 방법은 외부로부터의 문서나 프로그램의 유입을 차단하는 것이다. 대부분의 바이러스는 조직 내부자에 의해 고의로 유입되는 것이 아니라 외부에 있는 사람의 의도 또는 내부자의 실수에 의하여 유입되게 된다. 따라서 이러한 유입 원인을 근원적으로 차단하게 되면, 즉 외부로의 자료 유입을 차단하면 바이러스로부터 안전할 수 있다. 그러나 정보교환이라는 측면에서 보았을 때 방법 자체가 무리가 따른다. 따라서 보다 현실적인 방법을 찾아보면 무료 백신과 언론의 정보를 효과적으로 이용하는 것이 보다 현실적이다.

지금 현재로서, 가장 효율적인 방법은 여러 백신 제품을 이용하는 것이다. 국내 백신과 외국산 백신을 잘 이용하면 바이러스의 예방 및 치료가 가능하여 바이러스에 의한 피해를 최소화 할 수 있다.

V. 결론

본 논문은 컴퓨터 바이러스를 정의하고 십수년간 국내에 발견된 바이러스들의 기법을 분석하였다. 컴퓨터 바이러스의 기술이 발전하면 그만큼 많은 사람들이 피해를 입게 된다. 그 대표적인 예로 근 아시아 지역에 많은 피해를 준 *CIH*와 미국에서 문제되었던 *멜리사*를 들 수 있다. 국내에서도 *시스터보*의 소스 공개 이후, 이를 기반으로 제작된 다수의 바이러스가 나타나 많은 확산을 통하여 여러 사람에게 피해를 주었던 사례가 있다.

따라서 바이러스에 대한 소스 공개나 기법 공개 등은 컴퓨터 기술 발전에 공헌하기보다는 많은 사람에게 피해를 주는데 사용되고 있으며 언론도 이러한 기법들이 마치 고도의 기술인 것과 같이 보도를 하고 있어 바이러스 제작자들의 영웅 심리를 부추이고 있다. 따라서 이러한 인식을 없애기 위한 노력이 필요할 것이다.

앞으로의 연구 과제는 국내 발견된 바이러스들에 대한 계통도 및 위험도 분석을 위한 기준에 대한 정리 할 것을 제안한다.

참고문헌

〔1〕 "98년 바이러스동향", 안철수컴퓨터바이러스뉴스, 안철수연구소, pp.16-17, Apr. 1999.
〔2〕 Ralf Burger, Computer Viruses and Data Protection, Abacus, 1991.
〔3〕 안철수, 바이러스 분석과 백신 제작, (주)정보시대, 1994.
〔4〕 안철수, 바이러스 예방과 치료, (주)정보시대, 1997.
〔5〕 안철수, "컴퓨터 바이러스와 악성코드의 현황 및 대책", SIS'99, pp.399-410, Apr. 1999.
〔6〕 "윈도우98/95용 바이러스, 엑셀매크로바이러스 맹위", 안철수컴퓨터바이러스뉴스, 안철수연구소, pp.15-17, Jan. 1999.
〔7〕 차민석, "이미 시작된 윈도우 바이러스와의 전쟁-어제와 오늘", 안철수컴퓨터바이러스뉴스, 안철수연구소, pp. 10-13, Sep. 1998.
〔8〕 "98년 상반기 동향", 안철수컴퓨터바이러스뉴스, 안철수연구소, Oct. 1999.