CISC '99

악성코드의 기법 분석 및 동향(I)

황규범*, 김광조*, 안철수**

*한국정보통신대학원대학교, **안철수컴퓨터바이러스연구소

Analysis Malicious Code Schemes and Current Status

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

*Information and Communications Univ.
**Dr. Ahn's Anti-Virus Laboratories, Inc.

요 약

본 논문에서는 개인용 컴퓨터 상에서의 컴퓨터 바이러스(이하 바이러스) 및 웜 그리고 트로이목마와 같은 악성코드의 정의와 개념에 대해 기술하고 십수년간 국내에 발견된 컴퓨터 바이러스 및 악성코드들의 주요 기법 및 특징을 분석하며 1999년 10월까지의 바이러스 발견 동향 및 향후 전망에 대하여 기술하고 향후 바이러스 및 악성코드 대응 방법에 관한 연구 방향을 제시하고 논문을 맺는다.

I. 서론

지난 1999년 4월 26일 우리나라를 비롯한 아시아 국가에서 *CIH* 바이러스로 인하여 상당한 피해가 발생하였다. 이런 피해는 바이러스에 대한 예보 및 대응 방법에 문제가 있었던 것이 아니라 많은 사용자의 무관심에서 비롯된 것이라고 할 수 있다.

매년 국내에서 발표되는 자료들을 보면 바이러스를 포함한 악성코드에 의한 피해 정도가 단순히 제작자의 개발자의 장난이나 호기심에 의한 수준을 넘어서 실질적으로 업무에 지장을 주거나 자료를 손상시키는등 직접적인 피해를 주는 양상을 보이고 있다.

본 논문은 바이러스와 인터넷 웜 그리고 트로이목마에 대하여 정의하고 국내에서 발견된 바이러스를 중심으로 인터넷 웜과 트로이 목마를 포함하여 전반적인 기법의 흐름과 동향에 대해서 분석하고 주요 악성코드에 대한 분석 결과 및 대책을 제시한다.

(그림 1)은 우리나라에 *뇌(Brain)*바이러스가 처음 발견된 1988년부터 1999년 1/4 분기까지 국내에 발견된 바이러스 및 트로이목마, 그리고 웜들의 출처별, 종류별로 그 수를 파악한 것이다.[9]

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) 1999년 1/4분기까지 바이러스 발견 동향

본 논문의 구성은 제 2장에서 컴퓨터 바이러스 및 악성코드의 정의 및 구성 요소에 대하여 기술하고 제 3장에서는 1988년부터 1999년 9월까지 국내에 발견된 바이러스들를 포함하는 악성코드의 기술 특징을 분석하고, 제 4장에서는 최근 발견되는 악성코드의 유형과 유입 경로를 기술하며 제 5장에서는 악성코드에 대한 예방 대책에 대하여 기술하고 제 6장의 결론으로 논문을 맺는다.

II. 악성코드의 정의 및 구분

1. 악성코드의 정의

악성코드는 일반적으로 제작자가 의도적으로 사용자에게 피해를 주고자 만든 모든 악의의 목적을 가진 프로그램 및 매크로, 스크립트등 실행 가능한 형태의 모든 유형 포함하여 정의할 수 있다. 따라서 제작자의 의도와 관계없이 실수에 의해서 발생하는 버그는 원칙적으로 악성코드에 포함하지 않는다. 다만 버그로 인하여 사용자에게 실질적으로 피해를 주는 경우 악성코드에 포함하는 경우도 있다.

악성코드의 이름은 바이러스 명명원칙에 준하여 명명하고 있으며 본고에서는 필요에 따라서는 바이러스, 인터넷 웜 그리고 트로이목마등으로 구분하며 표기시에 이탤릭체와 밑줄을 표시하여 구분한다.

2. 악성코드의 구성

악성코드는 주요 3가지 유형인 바이러스, 웜 그리고 트로이목마로 구성하고 있으며 버그가 있는 프로그램도 일부 포함한다.

2.1 바이러스

바이러스의 경우 자기 복제 능력을 가지며 감염 대상 코드의 실행 구조를 변경하거나 내부 구조를 변경하여 대상 코드의 수행 전후에 바이러스가 실행될 수 있도록 변경하는 코드들의 집합을 가진다. 바이러스의 경우 부작용을 가질 수 있는데 이러한 부작용은 메시지 출력, C-MOS 메모리 데이터 삭제로부터 하드디스크 정보 파

괴, 플래시메모리 정보 파괴등으로 피해 규모가 커지고 있다.[2]

뇌(Brain), *절반(One_half)*, *알트엑스(Alt-X)*, *시스터보(SysTurbo)*, *에볼라(Ebola)*, *라루(XM/Laroux)*등 다수가 있으며 *CIH*도 이에 포함된다.

2.2 웜

웜 프로그램은 과거 70년대 대형 컴퓨터 등에서 다른곳에 복사하지는 않고 기억장소에서 자기 복제를 하는 프로그램을 말했다. 그러나 근래에는 실행 코드 자체로 번식하는 유형을 말하며 주로 PC상에서 실행되는 것을 의미한다. 따라서 본고는 PC상에서 정의되는 웜만을 제한적으로 다룬다.

웜과 바이러스의 큰 차이점은 감염 대상을 가지고 있는가에 따라 구분된다. 즉 바이러스는 어떤 감염 대상을 가지고 있지만 웜은 감염 대상을 가지지 않는다. [1]

국내에 발견된 웜은 *I-Worm/Happy99*, *I-Worm/ExploreZIP*, *I-Worm/PrettyPark* 등이다.

2.3 트로이목마

트로이목마는 악의적 목적으로 제작되며 바이러스와 달리 자기 복제 능력이 없으며 악의의 기능을 가지는 코드를 유틸리티 프로그램에 내장하여 배포하거나 그 자체를 유틸리티 프로그램으로 위장하여 배포하게되며 특정한 환경이나 조건 혹은 배포자의 의도에 따른 사용자의 정보 유출이나 자료 파괴와 같은 피해를 준다.

최근에는 상대방 컴퓨터의 정보를 유출하기위한 목적으로 사용되며 *Win-Trojan/Back_Orifice*, *Win-Trojan/SubSeven*등, *Win-Trojan/Ecokys*가 대표적이다.

3. 분류법

악성코드의 경우 바이러스를 제외하면 그 수가 적어 별다른 분류를 하지 않고 있다. 따라서 분류 개념은 바이러스의 분류법을 확장하여 웜과 트로이목마를 포함한다. 본고에서는 개별 분류를 하고 이들을 혼합한 방법을 제안하며 그에 따른 (그림 1)의 분류표의 내용을 재작성 하였다.

3.1 바이러스의 분류

바이러스의 분류는 일반적으로 감염 부위별 분류를 하고 있다. 감염 부위이란 바이러스 코드가 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.[3]

• 부트 바이러스 (Boot virus)

컴퓨터가 처음 가동되면 디스크의 가장 처음 부분인 부트섹터에 있는 프로그램을 실행시킨다. 이곳에 자리잡는 컴퓨터 바이러스를 부트 바이러스라고 한다.

• 파일 바이러스

파일 바이러스란 실행 가능한 프로그램에 감염되는 바이러스를 말한다. 이때 감염되는 대상은 실행파일이 대부분이며 (그림 1)에서와 같이 바이러스의 80% 정도가 파일 바이러스에 속한다.

• 부트/파일 바이러스

부트/파일 바이러스는 부트섹터와 파일에 모두 감염되는 바이러스로 대부분 크기가 크고 피해 정도가 큰 것이 특징이다.

• 매크로 바이러스

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 감염된다.

3.2. 트로이목마의 분류

트로이목마의 분류는 크게 운영체제 또는 실행 환경에 따라 분류하고 있다. 현재는 도스 트로이목마와 윈도우 트로이목마로 구분하고 있다.

• 도스(DOS) 트로이목마

도스에서 수행하는 트로이목마로 유틸리티로 위장하여 특정일자나 특정 조건에 사용자의 컴퓨터 속도를 저하시키거나 파일을 삭제하는 행위를 한다.

• 윈도우 트로이목마

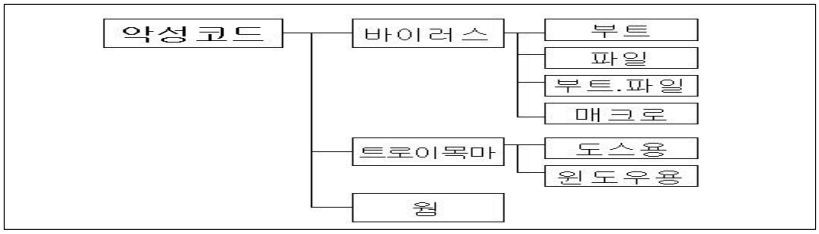
MS윈도우에서 실행되는 프로그램을 말하며 1998년부터 그 수가 증가하였으며 인터넷의 이용 증가에 따라서 주로 상대방의 정보를 불법적으로 취득하는등의 악의적 해킹을 주 목적으로 하는 것이 특징이다.

3.3. 웜의 분류

웜의 경우 얼마전까지 PC상에서는 중요하게 인식하지 않았으나 1999년 들어와 전자우편을 통하여 다른 사람에게 전달되는 형태의 웜이 다수 출현함으로써 일반인들에게 널리 인식되게 되었다. 웜의 경우 아직까지 그 수가 적어 특별한 분류법은 없다.

3.4. 악성코드의 분류법

악성코드의 분류는 악성코드를 구성하는 주요 3요소인 바이러스, 웜 그리고 트로이목마의 분류 방법을 모두 혼합하여 다음 (그림 2)와 같이 분류할 수 있다. 이와 같이 분류할 경우 기존의 바이러스 분류법을 그대로 활용할 수 있고 트로이목마와 웜의 경우 그 수가 적어 이후 더 좋은 방법이 제안되어 새로운 방법으로 재분류하더라도 어렵지않다. 따라서 본고에서는 각 주요 요소를 혼합한 분류 방법을 제안한다.



(그림 3) 악성코드 분류도

제한된 분류도에 의하여 바이러스의 경우 자료가 공개된 1988년부터 1999년 1/4분기의 자료를 사용하고, 트로이목마와 웜의 경우 1988년부터 1999년 10월까지 보도된 자료를 바탕으로 통계표 [표 1]을 작성하였다. 특히 발표되는 자료들은 모두 바이러스를 중심으로 하고 있어 1997년 이전의 경우 트로이목마와 웜의 경우 자료가 불확실하거나 없는 경우가 많아 확인된 자료만을 사용하였다.[4]

[표 1] 악성코드 분류법에 의한 분류(1988년에서 1999년 10월)

*는 1999년 1/4분기까지의 통계로 보도된 결과임

종류 \ 연도		1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	계
바이러스	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
	부트/파일			2	1	2	1	3	5	29	5	7	0*	54
	매크로									1	16	36	20*	73
트로이목마	도스				1			1	1	2		3		8
	윈도우											1	38	39
웜													3	3

Ⅲ. 기술특징

본 장에서는 뇌가 발견된 1988년부터 1999년 10월까지 바이러스를 포함하는 악성코드 제작에 사용된 방법을 백신 입장에서의 기법 변화를 단계별로 작성하였다. 단계 구분은 국내 발견된 바이러스를 중심으로 하며 최초 발견 시점을 기준으로 한다. 특히 1998년 이전에는 트로이목마나 웜을 제외하고 분석되었다.[10]

중요한 특징은 소스가 공개되는 악성코드의 경우 그 변종의 수가 많고 피해 규모

모도 다른 바이러스에 비하여 크다. 소스 공개로 많은 변형을 가진 것은 *시스터보(SysTurbo)*가 대표적이며 *Cri-Cri*, *Level_III* 그리고 *백오리피스(Back_Orifice)*가 대표적이다.

- 1단계(1988-1989) : 부트 바이러스 출현

  국내에서 최초로 뇌가 발견되었으며 대체적으로 간단한 부트 바이러스가 주종을 이루고 있으며 불법복제를 통해 확산되었다. 대표적으로 *뇌* 및 *벌꿀(Honey)*, *LBC*, *LBC.II*, *돌.B(Stoned.B)*가 있다.

- 2단계(1989) : 파일 바이러스 출현

  프로그램의 기능에 영향을 주지않고 감염시키는 기생형 바이러스들이 나타나게 되었다. *예루살렘(Jerusalem)*, *일요일(Sunday)*이 대표적이다.

- 3단계(1990) : 부트 및 파일 바이러스의 다량 출현

  바이러스 수가 전년대비 4배정도 많이 발견되었다. 이 시기의 처음 국내에서 제작된 파일 바이러스가 나타났으며 메모리에 상주하여 실행하는 프로그램을 감염시키는 형태가 일반적이다. 대표적으로 *폭포(Cascade)*, *11월30일(November_30th)*, *한국변형 일요일(Sunday.Kr)*, *양파(Damanaegi)*, *항공경찰(Aircop)*등이 있다.

- 4단계(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 감염시킬수 있으므로 확산이 빠르다. 대표적으로 *침입자(Invader)*, *자유(Liberty)*가 있다.

- 5단계(1991) : 새로운 형태의 연결형 바이러스 출현

  1991년 11월 확산속도가 매우 바른 *DIR_II*가 발견되었다. *DIR_II*는 FAT(File Allocation Table)의 연결 구조를 변경하는 새로운 방법의 연결형 바이러스이며 원래 연결 정보를 암호화해서 보관함으로 인하여 복구에 어려움이 있었다.

- 6단계(1992) : 외국 바이러스의 국내 변형 시작

  국내 제작자에 의하여 다수의 외국산 바이러스의 변형이 나타났고 메시지를 수정에서 새로운 형태의 바이러스를 만들어내는등 광범위하게 변형 작업이 이루어졌다. 대표적으로 *한국변형 예루살렘(Jerusalem.Kr)*, *한국변형 어둠의 복수자(Dark_Avenger.Kr)*, *한국변형 영시간(Zerotime.Kr)*, *한국변형 항공경찰(Aircop.Kr)* 및 *서울(Seoul)*, *Y4*등이 있다.

▪ 7단계(1993) : 간단한 다형성 암호화 바이러스의 출현

바이러스들은 자신의 존재를 숨기기위해 복수의 암호키를 사용하거나 암호화 방법이 감염시마다 변하는 기법을 사용하여 복구를 위한 분석을 어렵게 하였다. 대표적으로 *몰타아메바(Maltese_Amoeba)*가 있다.

▪ 8단계(1994) : 국산 암호화 바이러스의 전성기

1994년들어 국산 암호화 바이러스가 폭발적으로 증가하였다. 한 사람이 여러개의 바이러스가 변형 제작하여 국산 바이러스들도 그룹형태를 가지게 되었던 시기이다. 그리고 이시기에 국내 암호화 바이러스의 모태가 되는 *시스터보*가 발견되었다. 대표적으로 *방랑자(Wanderer)*, *넥스트(Next)*, *푸른하늘(Blue_Sky)*, *HWB*등이 있으며 이들 바이러스는 한해에 2종류 이상의 변형이 나타났다.

▪ 9단계(1995) : 다형성 바이러스의 본격화

암호화 방법을 구현하는 코드들을 변화시켜 특징을 찾기 어렵도록 하여 백신의 검색을 피할 수 있도록 하는 방법이 사용되기 시작한 시기로, 백신은 바이러스와 동일한 암호 해제 루틴을 갖추게 되어 분석 및 백신 개발이 지연되고 그로 인하여 다수의 피해자가 발생하게 되었다. 대표적으로 *경련(Tremor)*, *나타스(Natas)*, *절반(One_half)*, *코니II(Connie_II)* 그리고 *커피숍II(Coffeeshop_II)*가 있으며 1995년 상반기에 집중적으로 발견되었다.

▪ 10단계(1995) : 바이러스 제작 툴킷에 의한 바이러스 출현

1995년 하반기에 국내에 바이러스를 문답식으로 작성하는 바이러스 제작 툴킷이 입수되어 일부 바이러스 제작자들에 의해 바이러스가 다량 제작되기 시작하였다. *NRLG*, *PS-MPC*, *IVP*등이 대표적이다.

▪ 11단계(1995) : 광범위하게 피해를 준 연결형 바이러스 출현

1995년 10월에 연결형 바이러스인 *바이웨이(Byway)*가 발견되어, 광범위하게 확산됨으로써 그 피해가 컸다. *DIR_II*는 도스 v3.3까지만 작동했으나 *바이웨이*는 그 당시 사용중인 모든 도스에서 작동할 수 있어 더 피해가 컸다.

▪ 12단계(1996): 메모리 은폐형 바이러스 출현

바이러스 몸체를 암호화하여 은폐시킴으로써 메모리 내에서 바이러스를 쉽게 찾아내지 못하도록 하는 기법을 사용한 *먹깨비(Mange-tout)* 가 발견되었다.

▪ 13단계(1996) : 새로운 개념의 바이러스 출현

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 되었다.

▪ 14단계(1996) : 윈도우 바이러스 출현

1996년 6월경 *촉수(Win16/Tentacle)*와 *촉수.II(Win16/Tentacle.II)*가 발견되어 한글 윈도95 운영체제가 바이러스에 안전하지 않음이 확인되었고 앞으로 많은 윈도우 바이러스가 출현할 것을 예고하였다.

▪ 15단계(1997) : 다형성 바이러스의 기술적인 발전

1997년 3월에, 외국산 다형성 바이러스인 *Level_III*를 내부적으로 일부 변형한 *FCL*이 국내에서 발견되었다. *FCL*바이러스는 상당한 수준의 프로그래밍 능력을 가지고 있어 분석 및 백신의 개발이 까다로왔다.

▪ 16단계(1997-1998) : 본격적인 윈도95, 윈도NT 바이러스 출현

1997년 11월 한글 윈도95에서 상주하는 *아편걱정(Win95/Anxiety_Poppy)* 이, 12월에는 *아편걱정.II(Win95/Anxiety_Poppy.II)* 가 발견되었고 제작되어 그 피해가 확산되었으며 새로운 운영체제 위에서 작동하는 바이러스의 제작 기법들이 소개되었으며 분석 및 백신 개발은 도스와 전혀 다른 형태의 접근이 필요하게 되었다.

▪ 17단계(1998) : *백오리피스*의 출현

1998년 하반기 *백오리피스* 프로그램이 소개되었다. 다른 PC를 원격지에서 네트워크를 이용하여 조작할 수 있는 기법이 사용되었는데 이러한 특징은 *백오리피스* 서버를 다른 사람에게 배포할 수 있다면 그 사람의 정보를 얼마든지 빼낼 수 있음을 의미하였다. 따라서 이 당시 *백오리피스* 서버를 다른 프로그램에 숨겨 배포하는 방법이 소개되었다.

▪ 18단계(1998) : 다형성 매크로바이러스

1998년 하반기에 발생한 *엑스트라스(XM/Extras)*와 *컴페트(XM/Compat)*의 경우 기존의 매크로 바이러스와 달리 다형성 바이러스의 특징을 가지게 되어 분석 및 치료 기술 개발을 어렵게 하는 의도를 가지게 되었다.

▪ 19단계(1998) : 은폐형 매크로바이러스

다형성 바이러스와 더불에 1998년 12월 은폐형 바이러스의 *클래스(X97M/Class)*가 발견되었다. 은폐형 바이러스의 경우 워드나 액셀에서 매크로 코드를 볼 수 있는 기능을 무력화하는 것으로 바이러스 감염 여부 확인을 어렵게 한다.

▪ 20단계(1999) : 새로운 방식의 바이러스 출현 가능성 예고

1999년 초에 들어서 매크로 바이러스는 정보 유출 기능을 가지게 되었다. *멜리사(W97M/Malissa)*, *파파(X97M/Papa)* 소식이 언론에 공개되어 기업의 중요

자료 유출 가능성에 대한 경각심을 새롭게 가지는 계기가 되었다.

- 21단계(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 플래시 메모리 정보와 하드디스크 정보를 파괴하여 1999년 4월 국내에 천문학적인 피해를 입혀 바이러스의 위험성을 인식할 수 있는 계기가 되었다.

- 22단계(1999) : 자료 유출 가능성 시도 및 인터넷 웜의 확산

1999년의 가장 큰 특징은 인터넷을 이용한 자료 유출의 가능성을 보여주는 바이러스들의 출현과 특정다수에게 광범위한 피해를 입힐 수 있는 악성 프로그램들의 다수 출현이다. 이 당시 신년축하 메시지 형태로 여러 사람에게 확산된 *I-Worm/Happy99*를 비롯하여 *I-Worm/ExploreZIP*, *I-Worm/PrettyPark*등이 인터넷을 통하여 확산 유포되었다.

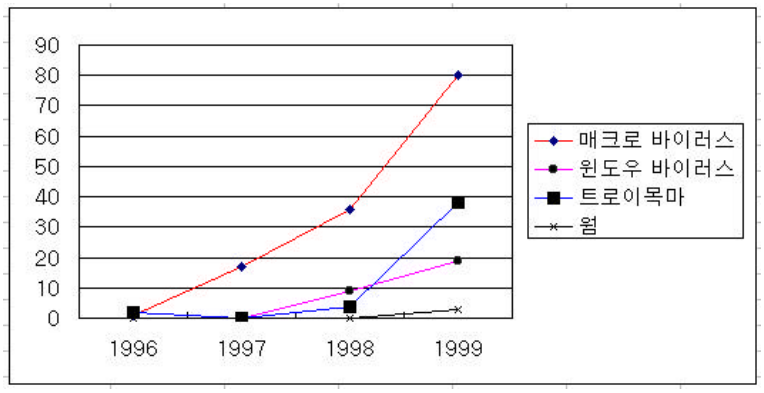
앞으로 바이러스뿐만 아니라 여러 종류의 악성 프로그램들이 다수 나타날 것으로 예상된다.[6]

Ⅳ. 최근 발생하는 악성코드의 주요 유형 및 경로

1. 유형

최근 발생하는 악성코드의 주요 유형은 주로 매크로 및 스크립트 바이러스와 윈도우 바이러스, 트로이목마 그리고 전자메일을 통한 웜등으로 다양한 유형이 나타나고 있다. 그리고 자바(Java) 환경 등에서 작동하는 바이러스들도 소개되고 있다.[8]

(그림 7)은 최근 3년간 악성코드의 증가세를 나타내고 있다.



(그림 4) 주요 악성코드의 발견 추이

(주) 1999년의 경우 1월부터 10월까지 통계

1) 매크로 바이러스

전세계적으로 매크로 바이러스의 수가 폭발적으로 증가하고 있으며 그에 따른 피해 규모가 매우 커지고 있다. 이런 이유는 우선 워드나 엑셀등 MS오피스 제품을 쓰는 사람이 상당히 많다는 점과 전세계적으로 공유하는 프로그램인만큼 인터넷을 통한 정보 교환 과정에서 다른 사람에게 전달 받거나 또 다른 사람에게 전달할 수 있는 가능성이 높고 인트라넷 환경에서 한 대의 PC에서 감염이 된다면 전체 PC로의 감염 확산히 매우 빠르다. [7]

매크로 바이러스의 경우 *엑스트라스(X97M/Extras)* 처럼 다형성 기법을 가진 바이러스 및 *클래스(W97M/Class)*와 같이 다형성 기법과 은폐형 기법을 같이 사용한 바이러스가 출현하고 있으며, 1999년 3월에 미국에서 문제시 되었던 *멜리사(W97M/Melissa)*와 같이 MS아웃룩의 메일 시스템을 통해 다른 사람에게 감염된 문서를 보내도록 하여 정보 유출의 가능성을 가지는 바이러스들이 다수 출현하고 있으며 MS오피스2000과 같은 새로운 환경에서 기존의 바이러스가 변형된 형태로 출현할 것으로 보인다. 앞으로 다형성 기법 및 은폐기법과 같은 고도의 기법이 사용하는 바이러스들이 다수 등장할 것으로 예측된다.

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

2) 윈도우 악성코드

최근 윈도우 악성코드는 *CIH*와 같은 바이러스 뿐만 아니라 트로이목마와 웜이 다수 발견되고 있으며 그 피해도 큰 것으로 보고되고 있다.

바이러스는 1996년에 *보자(Win95/Boza)*가 처음 소개된 이래로 *촉수*, *촉수.II*와 윈도95 메모리에 상주하는 *아편걱정* 그리고 다형성 기법을 가진 *HPS*순으로 복잡한 기법으로 발전하고 있으며 1998년 10월 국내 최초 윈도우 바이러스인 *전갈.1275(Win95/Scorpion.1275)*가 발견되었다.[5]

트로이목마의 경우 전반적으로 정보 유출의 가능성을 보여주고 있다. 1998년에 국내에 소개된 백오리피스와 1999년 7월 윈도95/98 및 윈도NT에서 사용할 수 있는 *백오리피스2000(Win-Trojan/BO 2000)*이 널리 확산되면서 정보 유출 및 악의적 목적의 해킹 도구가 된다는 점을 우려하고 있다. 또한 또 소스가 공개되어 더 복잡한 형태로 배포될 수 있는 가능성을 가지며 두달 사이에 20여종이 넘는 변종이 나타났음을 볼 때 앞으로 백오리피스가 숨겨진 다수의 유틸리티가 악의의 목적으로 배포될 가능성이 높다.

최근 1999년 10월 국내 모 대형 PC통신사의 메일 시스템을 통해 “영상으로 쓰는 편지”란 이름으로 전달된 *에코키스(Win-Trojan/Ecokys)*는 사용자가 입력하는 모

든 키보드 정보를 기록하여 사용자가 PC뱅킹이나 기타 아이디와 암호 정보를 취득할 수 있는 가능성을 보였다.

1999년의 *CIH* 사태 이후의 최근에는 인터넷을 통한 웜이 다수 출현하여 많은 피해를 주고 있다. 이런 웜들은 전반적으로 인터넷을 기능을 이용하기 위한 윈도우 시스템의 소켓라이브러리를 수정하여 전자우편에 자동 첨부되는 형태로 다른 사람에게 전달되는 *I-Worm/Happy99*과 사용자가 받은 메일에 자동으로 답장을 하여 다른 사람에게 전달되며 광범위하게 MS오피스 문서와 프로그램 소스등을 손상시키는 *I-Worm/ExploreZIP*을 비롯하여 1999년 9월 전자메일 주소와 암호등의 개인정보를 유출시키는 *I-Worm/PrettyPark*이 인터넷을 통하여 급속히 확산되면서 큰 문제가 되고 있다.[9]

1999년 1월부터 10월까지 국내에서 *Win95/K32*, *Win32/Kenstone.1895*, *Win95/CIH.1035*, *Win32/Nico*, *Win95/CIH.1019*, *Win95/Sexy*, *Win95/Fono*, *Win32/Weird*등 윈도우 바이러스 8종과 *백오리피스*를 비롯한 트로이목마가 30여종, 그리고 웜이 3종이 발견되었다.

최근 많이 발생하고 있는 전자메일을 통한 웜은 사용자 몰래 발송되는 편지에 웜 프로그램을 첨부하는 형태와 제작자가 고의로 다른 사람에게 유용한 유틸리티로 속여서 보내는 형태가 주로 일어난다. 1999년에 들어 PC상에서 다른 컴퓨터로 번식하는 웜이 다수 발생하여 피해가 점점 커지고 있다.

2. 확산 경로

악성코드의 유입 경로는 대부분 PC통신망을 통해 이루어졌다. 그러나 최근 들어 인터넷 사용이 보편화됨에 따라 인터넷을 통한 악성코드의 전달도 이루어지고 있다. 본 절에서는 주요 3가지 경로를 기술한다. 첫 번째 경로는 사용자가 필요로 하는 유틸리티 프로그램을 외부로부터 입수하여 사용하는 과정에서 유틸리티 프로그램이 악성코드를 포함하고 있거나 그 자체가 악성코드인 경우를 들 수 있고, 두 번째 경로는 자료 교환 및 공유에 있어 상대방의 부주의로 인해 악성코드를 포함하는 자료가 전달되어 그 정보를 이용함으로 인해 피해를 보는 경우, 마지막은 최근 자주 발생하는 것으로 전자 메일을 통하여 상대방을 속여 바이러스나 웜을 전송하는 방법이다.

1) 유틸리티로 가장한 악성코드

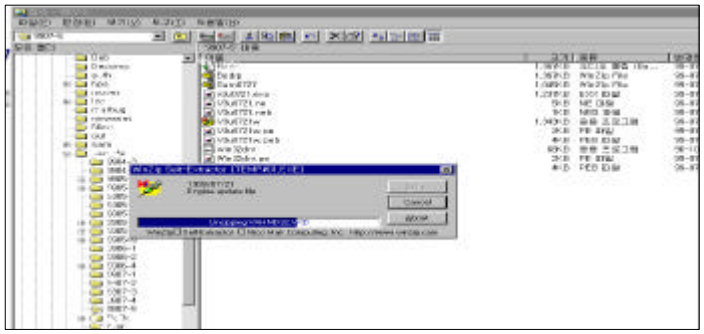
최근 발생하는 바이러스와 트로이목마의 경우 유용한 유틸리티로 가장한 경우가 많다. 이런 경우 제작자가 바이러스나 트로이목마를 유포하기위한 목적 혹은 정보를 유출하기 위한 목적을 가진 경우가 많다.

우선 바이러스의 경우 1998년 V3+의 최신버전으로 가장한 *알트엑스* 및 유명한 셰어웨어 프로그램인 MDIR을 정품 프로그램으로 만들어주는 크랙 프로그램을 통

하여 유포된 *전갈*, 그리고 이야기 7.3 크랙 프로그램을 통하여 유포된 *남벌.1480*이 대표적이며 이들은 많은 사람이 이용하는 유틸리티로 가장한 경우로 피해가 큰 것이 특징이며 최근 국내에 천문학적인 피해를 입힌 *CIH*도 많은 사람들이 사용하는 유틸리티에 감염되어 PC통신망에 올려짐으로 많은 사람에게 확산되게 되었다.

최근에는 *백오리피스*와 같은 해킹 도구가 몰래 숨겨져 있거나 윈도우의 기본 유틸리티에 해킹 도구를 숨겨 새로운 판이라고 소개한 예도 있다. 우리나라의 경우 전반적으로 인터넷을 통한 악성코드의 유포보다는 대형 PC통신망 통한 유포 및 확산이 빠르다.

(그림 8)은 *백오리피스*가 포함된 해적판 V3업데이트 파일로 모단체에서 발견되었다. 이런 프로그램은 *백오리피스* 드롭퍼 제작기를 통해 만들어진다.



(그림 5) 백오리피스가 포함된 해적판
V3업데이트 파일

2) 정보교환을 통한 매크로 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.

3) 전자메일을 통한 웜과 트로이목마의 확산

최근들어 악성코드에 의한 피해가 급증하고 있다. 바이러스에 의한 피해 뿐만 아니라 웜과 트로이목마에 의한 피해가 보고되고 있다. 이러한 웜과 트로이목마는 모두 전자메일을 통하여 확산되고 있다. 특히 인터넷을 통한 웜의 확산은 신뢰있는 송신자로 가장하여 악성코드를 포함하는 메일을 송신하고 수신자는 별다른 의심없이 첨부된 악성코드를 실행함으로써 피해가 발생한다. 1999년 3종의 웜이 인터넷을 통해서 유포되었고 또 피해자가 속출하였다. 이들 인터넷을 통한 웜들은 윈도우 소켓라이브러리를 수정하거나 레지스트리의 등록 정보를 수정하여 웜이 먼저 실행하도록 하는 방법이 주로 사용되고 있으며 사용자가 메일을 보낼 때 첨부시킴으로써 상대방의 의심을 받지않고 널리 확산될 수 있었던 특징을 가졌다.

Ⅴ. 대책

바이러스의 피해를 줄이는 가장 좋은 방법은 예방이다. 현재 가장 좋은 예방 방법은 외부로부터의 문서나 프로그램의 유입을 차단하는 것이다. 대부분의 바이러스는 조직 내부자에 의해 유입되는 것이 아니라 외부에 있는 사람의 의도에 의하여 유입되게 된다. 따라서 이러한 유입을 근원적으로 차단하게 되면 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 좋다.

다수의 백신 연구가들은 예방을 위한 새로운 기술들을 연구하고 이를 실현하기 위해 노력하고 있으나 아직까지 혁신적인 방법이 나타나지 않고 있어 컴퓨터 사용자 스스로 주의하는 것이 중요하며 신뢰성 있는 곳의 자료를 이용해야 한다. 만일 세어웨어 제품을 사용하고자 한다면 제작사의 인터넷 홈페이지가 가서 직접 받는 것이 좋으며 기능이 불분명한 프로그램은 사용하지 않는 것이 좋다. 또한 전자메일에 첨부되는 문서나 실행 프로그램의 경우 양자가 합의에 의하여 보낸 것이 아니라면 매우 조심해야 한다. 특히 프로그램의 경우 그 자체가 파일을 손상시키거나 하드디스크의 정보를 파괴하는 기능을 가진 경우 많은 피해를 입을 수 있음을 명심하는 것이 좋다.

Ⅵ. 결론

본 논문에서는 바이러스, 트로이목마, 웜을 포함하는 악성코드의 개념과 분류 방법에 대하여 제안하였다. 또한 과거 십수년간 국내에 발견된 바이러스를 중심으로한 악성코드들의 기술 동향을 분석하였으며 최근의 동향 및 대처 방법에 대하여 제시하였다.

악성코드의 기법이 점점 발전함으로 인하여 그 피해도 점점 커지고 있다. 악성코드 기법은 제작자들이 주장하는 시스템의 취약점등을 연구하는 목적으로 떠나서 이제는 많은 사람들이 피해를 입히는 방법으로 사용되고 있다. 그 대표적인 예로 근아시아 지역에 많은 피해를 준 *CIH*와 미국에서 문제되었던 *멜리사*, 그리고 최근 소개된 *백오리피스*등이다.

특히 악성코드의 소스 공개는 그 만큼 더 큰 피해를 발생시키는데, 국내의 경우 *시스터보*의 소스 공개 이후, 이를 기반으로 제작된 다수의 복잡한 바이러스가 나타나 많은 확산을 통하여 여러 사람에게 피해를 주었던 사례가 있으며 최근 *백오리피스* 변종의 다수 출현도 앞으로 큰 피해 발생이 우려된다.

따라서 악성코드의 소스 공개나 기법 소개는 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 부축이고 있다. 따라서 이러한 인식을 없애기 위한 모두의 노력이 필요하다.

앞으로의 연구 과제는 국내 발견된 바이러스들에 대한 다양한 분류 방법과 효율적인 분석 방법 그리고 계통도 및 위험도 분석을 위한 기준에 대한 정리를 제안한다.

참고문헌

[1] R. Burger, Computer Viruses a high-tech disease, Abacus, 1988.

[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] 차민석, *"이미 시작된 윈도우 바이러스와의 전쟁-어제와 오늘"*, 안철수컴퓨터바이러스뉴스, 안철수연구소, pp. 10-13, Sep. 1998.

[6] 안철수, *"컴퓨터 바이러스와 악성코드의 현황 및 대책"*, SIS'99, pp.399-410, Apr. 1999.

[7] "99년 1/4분기 동향", 안철수컴퓨터바이러스뉴스, 안철수연구소, June. 1999.

[8] "윈도우98/95용 바이러스, 엑셀매크로바이러스 맹위", 안철수컴퓨터바이러스뉴스, 안철수연구소, pp.15-17, Jan. 1999.

[9] Disse 10월호, KBS 영상사업단, pp.158 - 160, 1999.

[10] 황규범, 김광조, 안철수, *"컴퓨터 바이러스의 기법 분석 및 동향(I)"* Proceeding of KIISC Conf. 충청지부, 1999.