□특집□

국내 · 외 컴퓨터바이러스 현황과 대책

김 재 성† 이 상 엽†† 임 채 호†††

◈ 목 차 ◈

1. 개 요

대부분의 파일, 부트 바이러스 등 전형적인 컴퓨터바이러스의 감염속도가 더딘 반면에 1988년 11월에 최초로 등장한 인터넷웜의 경우, 인터넷을 통해 사용자 간섭없이 자동으로 웜을 전파시키는 등 최근의 인터넷기반의 컴퓨터바이러스가 도래하면서 감염속도가 급격히 빨라졌으며 미켈란제로 · 멜리사 바이러스, ExploreZip 등의 인터넷웜 등의 최신 바이러스 추세는 수시간 또는 수일내에 인터넷을 통해 전세계에 컴퓨터바이러스를 전파하고 있다.

이에 따라 컴퓨터바이러스 전파속도 보다 신속한 치료법 제공, 신종 또는 알려지지 않은 컴퓨터바이러스 자동탐지, 전염성 및 바이러스 쇄도에 대응하는 처리기술, 자동으로 바이러스 치료를 위한 신속한 처리속도, 급변하는 위협에 신속히 대응할 수 있는 유연성, 백신기술의 안전성 및 신뢰성 보장, 기관의 보안정책에 일치하는 사용자 보호정책 유지기능 등 다양한 바이러스 백신기술이 요구되고 있고 이와 유사한 차세대 백신기술인 컴퓨터바이러스 디지틀 면역시스템 기술은 해외에서는 상용화 단계에 접어 들고있는 실정이다. 본고에서는 99년도에 국내 · 외적으로 출현한 컴퓨터바이러스의 현황과 이에 대한 대응책을 설명하고자 한다.

† 정회원 : 한국정보보호센터 선임연구원
†† 정회원 : 한국정보보호센터 연구원
††† 정회원 : 한국정보보호센터 선임연구원

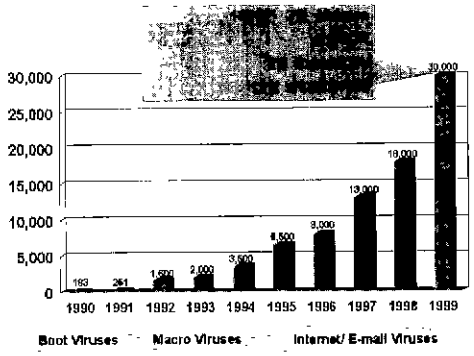
2. 국내 · 외 컴퓨터바이러스 발생현황

2.1 국외 컴퓨터바이러스 발생현황

수년전에만 해도 플로피디스크 등을 통해 일부 PC들에 컴퓨터바이러스에 감염되어 피해를 주는 정도로 소규모적인 컴퓨터바이러스의 전염성을 갖고 있었다. 그러나 인터넷의 급속한 확산을 통해 네트워크상에 접속된 대량의 컴퓨터에 의존하는 정보화 사회가 도래되고 이동코드 형태의 프로그램 개발보급이 확대되면서 E 메일과 인터넷을 통하여 생물학적 바이러스 질병처럼 컴퓨터바이러스 감염에 대한 전염성을 갖추게 되었다. 미국 ICSA(International Computer Security Agency) 분석보고서에 따르면 '97년부터 '99년 2월까지 26개월간 300여개 조직에 806,614대 PC로 부터 263,784개의 컴퓨터바이러스를 발견할 수 있었으며, 조사기간중 한달에 1000대의 PC에서 평균 13개의 컴퓨터바이러스가 발견되었으며, 이는 컴퓨터바이러스의 감염속도가 급격히 증가되었음을 입증하고 있다. 또한 부트바이러스와 매크로바이

러스로부터 최근에는 인터넷웜, 트로이목마 또는 E 메일을 이용한 바이러스들이 기승을 부리고 있는 실정이다.

(그림 1)에서는 국외에서 년간 컴퓨터바이러스 유형별 발생추세를 보여주고 있다.

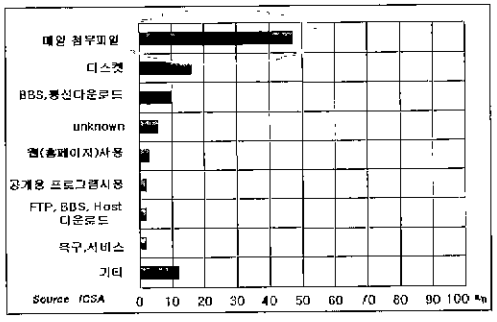


※ 자료 제공 : 트렌드 코리아

(그림 1) 유형별 년간 컴퓨터바이러스 발생추세

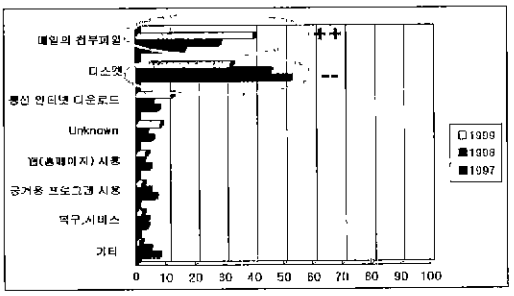
미국 ICSA 분석보고서에 따르면, 299명의 응답자 중 컴퓨터바이러스 샘플이 유포되는 매체로 E 메일을 통한 컴퓨터바이러스 감염이 가장 많은 것으로 나타났다.

바이러스 확산 경로를 살펴보면 (그림 2)와 같이 최근에는 메일 첨부 파일에 의한 감염이 압도적인 원인이 되고 있다. 상대적으로 기존의 부트 바이러스나 파일 바이러스의 감염 원인이었던 디스켓에 의한 감염이 줄어들고 있다.

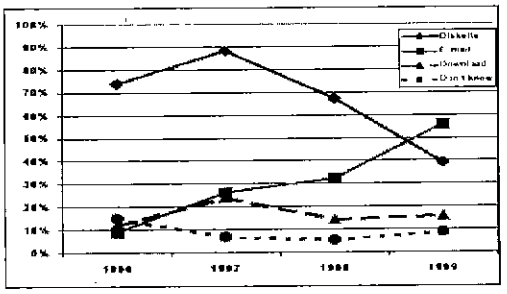


(그림 2) 연도별 컴퓨터바이러스 확산 경로

아래 (그림 3, 4)에서는 연도별 바이러스 감염원인 변화추이를 잘 보여주고 있다. 1997년에 비하여 1999년에는 첨부파일에 의한 감염 증가율이 대단히 높다는 것을 알 수 있다.



(그림 3) 연도별 바이러스 감염원인 변화추이



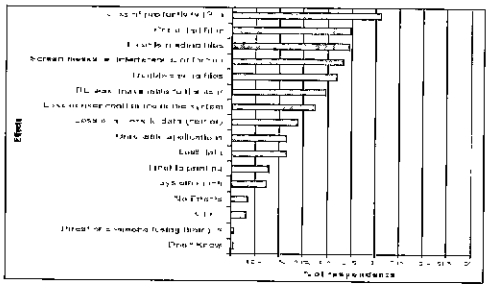
(그림 4) 연도별 감염경로 변경추세

또한 컴퓨터바이러스에 감염되어 복구하는데 소요되는 시간과 노력, 비용측면에서 일반기업의 PC 사용자가 피해를 입은 유형을 살펴보면 다음과 같다.

- o 생산성 저하
- o 파손 및 삭제 등의 파일 변조
- o 파일 판독불능
- o 메시지 화면 출력, 간섭현상, 화면잠금
- o 파일 저장 불능
- o 사용자에게 PC 자원의 가용성 제거
- o 시스템내 사용자의 주요 기밀정보 손실
- o 서버에 있는 데이터 액세스 제한
- o 데이터 손실

- ○ 응용 프로그램의 신뢰성 저하
- ○ 출력상의 제한
- ○ 시스템 붕괴
- ○ PC 동작 불능
- ○ 기타
- ○ 알려지지 않은 PC 오동작
- ○ 업무손실에 따른 사용자에 위화감 조성

(그림 5)에서는 컴퓨터바이러스 감염에 따른 피해유형을 통계치로 보여주고 있다.



(그림 5) 피해유형에 관한 통계치

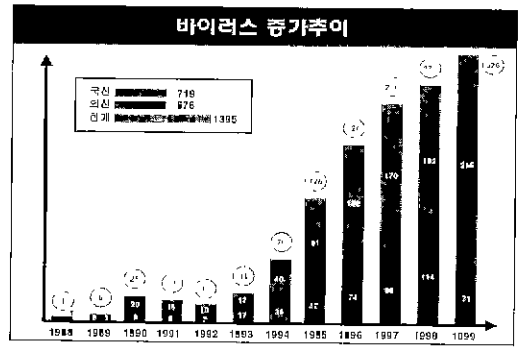
2.2 국내 컴퓨터바이러스 발생현황

99년도 국내에 유입된 컴퓨터바이러스 발생현황을 살펴보면 크게 다음과 같이 세가지로 요약할 수 있다.

- ○ 인터넷웜, 매크로바이러스의 유입 급증
  - E 메일, IRC(Internet Relay Chat) 등의 전송 메커니즘 등을 이용한 네트워크상의 대규모적인 인터넷웜 유포
    ※ ExploreZIp.Worm(6. 11), Toadie(9. 1) 등
  - 윈도우 스크립트인 VBS(Visual Basic Srcipt)를 이용한 신종 컴퓨터바이러스 출현
    ※ VBS.FreeLink(10. 2) 등
  - MS Word, Excel 등의 MS 오피스 대상의 공격형 매크로바이러스 급증
    ※ Melissa(3. 26), JulyKiller(7. 16) 등
- ○ 해킹기법을 이용한 신종 컴퓨터바이러스 등장
  - 해킹기법을 이용한 트로이목마 유포
    ※ BackOrifice2000(7. 13), EcoKys(10. 11) 등
  - PC의 시스템과 개인정보를 유출하는 신종 컴퓨터바이러스 유포
    ※ PrettyPark(9. 9) 등
- ○ Y2K 문제를 가장한 신종 컴퓨터바이러스 국내 유입
  - Y2K 해결 프로그램으로 위장하여 Y2K관련 컴퓨터바이러스 유입
    ※ Y2KCOUNT(9. 29), Fix2001(11. 26), NewApt(12. 20), MyPics('2000. 1. 3) 등

특히 99년 4월 26일 대만산 CIH 바이러스에 감염되어 국내 3%정도 PC의 시스템 파괴 및 데이터 손실로 인하여 20 ~ 30억원 가량의 피해를 입는 컴퓨터바이러스 사고가 발생되었다.

(그림 6)는 99년 국내의 컴퓨터바이러스 발생추세, (그림 7)에서는 99년 국내에 출현한 컴퓨터바이러스의 유형분석, <표 1>에서는 국내 컴퓨터바이러스 발생 통계치를 보여주고 있다.

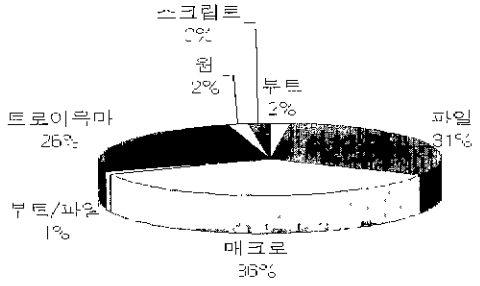


(그림 6) 국내 컴퓨터바이러스 발생추세

'90년대 중반 이후 바이러스는 계속적으로 많은 증가를 나타내고 있으며, 매크로 바이러스와 윈도우 바이러스, 그리고 최근의 웜 등의 바이러스 제작 기술의 향상으로 양적인 증가와 함께 그

위험성도 많이 증가하였다. 그리고 해킹 기술을 응용한 트로이 목마 프로그램도 많은 변종과 함께 발견되어 악성 프로그램의 위협이 이제는 정보 유출과 정보 변조까지 미치고 있어 그 대응이 점점 어려워지고 있다.

한편, '99년도에 국내에서는 메크로 바이러스(36%), 트로이목마(26%), 인터넷웜(2%) 등의 컴퓨터 바이러스가 출현하였다. 이중 Worm.ExploreZip 등의 경우와 같이 국내에 바이러스 감염확산과 함께 네트워크를 통한 대규모적인 PC에 바이러스 피해를 입혀 향후에도 그러한 급속한 전파력을 갖는 웜은 지속적으로 제작 · 유포되어질 것이다.



(그림 7) 국내 출현한 컴퓨터바이러스 유형분석

〈표 1〉 99년 국내 컴퓨터바이러스 발생통계

월 출처	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	합계
국산	7	8	6	6	6	5	4	3	5	13	6	2	71
외산	13	14	12	20	18	18	20	23	40	36	35	6	255
합계	20	22	18	26	24	23	24	26	45	49	41	8	326

※ '99 1~11 : 안철수컴퓨터바이러스연구소, 하우리 자료제공

※ '99. 12 : 한국정보보호센터 Y2K관련 바이러스 해킹 비상대응상황실 자료집계

2.3 국내 · 외 컴퓨터바이러스 피해 사례

2.3.1 Melissa 바이러스 피해 사례

▶ 국외 사례

'99년 3월 주요 오피스 문서를 파괴하는 E-메일을 통한 자체 전파 기능을 갖는 웜인 "Melissa"가 국외의 약 50,000대의 PC 시스템과 100개의 기업체를 감염시킨 사례가 발생하였다.

2.3.2 CIH 바이러스 피해 사례

▶ 국내 사례

'99. 4. 26일 정통부는 국내 PC 보급대수 8백만대중 4%안밖인 30여만대 피해를 입은 것으로 추정하였으며 이와 함께 한국정보보호센터내에 컴퓨터 바이러스 전담팀을 구성해 전문인력을 보강하고 국내외 바이러스 동향 분석과 차세대 백신 프로그램 연구개발을 지원하기로 하였다.

- BIOS손상 및 HDD데이터 손실(4만건), HDD 데이터손실(EPROM BIOS 파괴안됨, 16만건) 등 21억원가량의 피해

※ '99. 5. 10, 정보통신부 집계현황

▶ 국외 사례

중국에서는 4월 26일의 CIH 체르노빌 바이러스에 36만대의 컴퓨터가 감염돼 10억위앤(元) 상당의 경제적 손실이 발생했다고 관영 신화(新華) 통신이 한 조사 결과를 인용 보도했다.

2.3.3 Worm.ExploreZip 피해사례

▶ 국내 사례

'99. 6. 11일 국내에 유입되어 총 79건의 피해사례가 접수되었다.

※ 주요 민간기업 39건, 개인 40건 피해접수됨 ('99. 6. 14 집계현황)

▶ 국외 사례

시카고의 커먼웰스 에디슨사(社) 모기업의 경우 지난 10일 웜이 나타난 이후 e-메일 시스템을 꺼버려 1만여명에 달하는 직원들이 평소와 달리 사무실간 통신을 위해 전화와 팩스 등을 사용할 수 밖에 없는 불편을 겪었다. 또한 GE, 보잉사(社) 등과 같은 일부 다국적 기업들의 전산망에 침투, 수천 대의 개인용 PC에 있는 파일 내용을

삭제했을 뿐 아니라 기업들의 귀중한 컴퓨터 파일까지 파괴되었다.

2.3.4 EcoKys 피해 사례

▶ 국내 사례

'99년 11. 18 EcoKys 트로이 목마 프로그램을 이용해서 남의 통장에서 현금을 인출하는 피해사례가 발생하였다. 범인 황씨는 이 트로이목마를 수정하여 PC 통신 가입자들에게 E-메일에 첨부하여 보낸 뒤 부주의한 사용자가 첨부 파일을 실행하여 감염된 시스템으로부터 이 트로이 목마의 Keylog기능을 이용하여 PC뱅킹 계좌번호 등을 빼내는 방법을 사용하여 한 피해자의 PC뱅킹 계좌에서 140만원을 계좌이체 시킨 후 현금으로 빼냈다 경찰에 꼬리를 잡히는 사건이 발생하였다.

2.3.5 Win32/MyPics 피해 사례

▶ 국내 사례

'99년 12월 6일에 이미 한국정보보호센터 컴퓨터바이러스 전담반에 의해 경보되었던 MyPics 바이러스가 국내에 2000년 1월 3일에 74건이나 출현하여 많은 PC를 파괴하는 사례가 발생되었다. 이 MyPics 바이러스는 감염되면 재부팅 시에 Y2K 오류 메시지를 가상으로 출력하며 시스템을 파괴하는 악성 바이러스로 그 피해가 매우 컸다.

3. 국내 · 외 컴퓨터바이러스 대응현황

3.1 국외 컴퓨터바이러스 대응기관 현황

해외 선진국의 바이러스 대응기술 연구개발은 민간 분야가 주도하여 사람의 면역체계를 모방한 컴퓨터 면역시스템, 신경망 컴퓨터바이러스 탐지기술, 악성 이동코드 등의 연구가 진행중이며, 해외 주요선진국의 컴퓨터바이러스 관련 대응기구를 살펴보면 다음과 같다.

ICSA (International Computer Security Association)
http://www.icsa.net/services/consortia/anti-virus/

※ ICSA는 초기에는 바이러스 침입 보호에 대한 이슈들에 초점을 두었으나 점차 다음과 같은 서비스로 확대제공하고 있음

- ○ 컨소시엄 구성, TruSecure-시스템 인증
- ○ 제품인증(Product Certification)
- ○ 컨소시아 그룹 관리, ICSA 회원 관리
- ○ 위험 프레임워크 및 연속적 인증 모델
- ○ 정보 보급(Dissemination of Knowledge)

CIAC (Computer Incident Advisory Capability)
http://ciac.llnl.gov/ciac/

- ○ 미국 에너지성(Department of Energy, DOE) 산하에 있는 침해사고대응기구로서 관련정보 제공 및 현장기술지원, 동향, 위협 및 취약성 관련 데이터 수집 및 분석, 기술감독 등의 인식 교육 및 훈련

FedCIRC (The Federal Computer Incident Response Capability)
(http://www.fedcirc.gov)

- ○ 국가 기반구조 보안센터 (National Infrastructure Protection Center, NIPC)와 공동연구 추진
- ○ 침해사고 처리, 관련정보 공유, 공통적인 보안문제 해결 방책 등을 연방기관들에 제공

Wildlist Organization International
(http://www.wildlist.org)

- ○ 바이러스 백신 개발업체, ICSA 등으로 구성된 비영리단체로 일반사용자 및 백신제품 개발자에게 바이러스 위협등에 관한 정확하고 적시에 맞는 정보 제공 및 홍보활동 수행 목적으로 설립됨

EICAR (European Institute for Computer Antivirus Research)

(http://www.eicar.org)

○ 유럽 민간바이러스 연구단체로 이사회와 정보보호, 네트웍보안, 바이러스 방지, 침입탐지 관리 4개의 실무작업반(Working Groups)으로 구성되어 있으며, 악성 바이러스 경고 및 피해사고 접수, 백신제품 평가시행, 바이러스 방지정책 수립, 바이러스 관련정보 상호교류, "Checklist for AV scanners"와 같은 특별활동

VTC (Virus Test Center)

(http://agn-www.informatik.uni-hamburg.de/vtc)

○ 독일 함부르크 대학의 컴퓨터 과학부(Computer Science Deparment)소속 바이러스 전문 연구센터

○ 바이러스 경고, 백신성능시험(Amiga Antivirus Test) 연도별 Report 공개, 바이러스 목록 배포, 신종 바이러스 홍보

IPA (Information-technology Promotio Agency)

(http://www.ipa.go.kr)

○ 일본 정보통신진흥협회로서 패키지 소프트웨어 개발 지원 및 정보 프로세싱 산업의 재정 및 보증역할등의 다양한 활동 및 기초 소프트웨어 기술 개발과 최근에는 컴퓨터 바이러스 예보 및 방지 대책을 연구하고 있음

3.2 국내 컴퓨터바이러스 대응현황

국내 PC 이용자들의 바이러스 방지를 위한 백신프로그램 구입의지와 안전조치 인식이 부족하고 비상시 4개의 민간백신업체에 의해 즉각 대응을 위한 정부·공공기관 등 전국적인 연락체계 및 대국민 홍보가 미흡한 실정에서 '99. 4. 26일 CIH 악성 컴퓨터바이러스가 국내에 널리 유포 커다란 피해를 입힘에 따라 '99. 5월 한국정보보호센터 침해사고대응지원팀(CERTCC-KR)내에 컴퓨터바이러스 전담반이 구성되어 다음과 같은 주요 임무를 통해 국가적인 컴퓨터바이러스 대응활동을 추진하고 있다. 또한 새천년 연도전환기('99년 12월 30일 ~ '20년 1월 4일)에 Y2K로 인한 오류와 일반적인 해킹, 컴퓨터바이러스 등에 사안발생시 이에 대한 혼동을 방지하고 Y2K문제와 해킹 및 컴퓨터바이러스 사고에 대해 국내 피해를 최소화하기 위하여 정보통신부 Y2K 정부종합상황실과 연계하여 국내 백신업체(4개), 백업·복구·방역서비스업체(5개), 망사업자(6개) 등의 전문가로 구성된 비상대응반과 한국정보보호센터내에 Y2K관련 바이러스·해킹 비상대응상황실을 중심으로 신속하게 Y2K관련 바이러스 및 해킹사고에 신속한 대응활동을 통해 새천년 전환시기에 국내에서 큰사고가 없었다.

컴퓨터바이러스 전담반은 다음과 같은 활동을 통하여 국내 컴퓨터바이러스 예방을 하고 있다.

○ 국가적인 컴퓨터바이러스 종합대응체계 구축·운영

국내·외 컴퓨터바이러스 관련 대응기관과의 협력체계(virus-hotline@certcc.or.kr) 및 대응체계 구축, 침해사고대응팀협의회(CONCERT)내에 컴퓨터바이러스 전문연구회 구성·운영, 월별·긴급경보 등 컴퓨터바이러스 사전예보제 실시, 국내 컴퓨터바이러스 긴급연락망(virus-alert@certcc.or.kr) 등을 운영하고 있다.

○ 컴퓨터바이러스 종합상황실 운영

국내 컴퓨터바이러스 피해접수를 위한 신고센터(http://www.certcc.or.kr/cvirc, virus-rep@certcc.or.kr) 운영, 종합적인 피해상황 실태 조사분석 및 통계자료 발표, 컴퓨터바이러스 대응정보 DB 구축·운영, 웹기반 바이러스 종합상황실 운영시스템 구축·운영 등을 추진한다.

○ 선도적인 차세대 악성 컴퓨터바이러스 대응 기술 연구개발

신종 컴퓨터바이러스 시험분석, 리눅스 바이러스 및 해킹응용 신종 바이러스 등 차세대 악성 컴퓨터바이러스 대응기술 개발, 국내백신업체와 공동으로 학습형 바이러스 면역시스템 개발 등을 추진하고 있다.

○ 컴퓨터바이러스 방지 관련 법·제도 및 지침서 개발

국내 컴퓨터바이러스 제작자 처벌법안 및 사고피해기관 제재방안 등 컴퓨터바이러스 방지 관련 법·제도 연구, 악성 컴퓨터바이러스 기술권고문 및 예방지침서 개발을 하고 있다.

○ 컴퓨터바이러스 대응 기술교육 및 대국민 홍보활동

센터내 정보보호 기술교육 과정에 컴퓨터바이러스 방지기술 교육과정을 신설하여 전문인력 양성, 컴퓨터바이러스 피해방지를 위한 홍보물 제작 등 대국민 홍보를 강화하고 있다.

4. 대응사례

Y2K관련 컴퓨터바이러스나 해킹문제는 '99년 초반, 한국정보보호센터에서 국내·외 관련정보를 수집하던 중 정보통신부 Y2K상황실에서의 검토 요청을 받고 공식 검토를 시작하였으며, '99년 11월 정보통신부 Y2K상황실·정보보호과, 한국정보보호센터, 백신업체, 망사업자 등이 모여 구체적인 대응방안을 논의하였다. '99월 11월 홈페이지를 개설하고 '99년 12월 15일부터 '20년 1월 4일간에 걸쳐 일반적인 컴퓨터 사용자가 Y2K문제로 위장한 단순 해킹사고 및 컴퓨터바이러스 사고로부터 사전에 예방·조치할 수 있도록 한국정보보호센터내에 Y2K관련 바이러스·해킹 비상대응상

〈표 2〉 Y2K 관련 컴퓨터바이러스·해킹 대응활동 현황

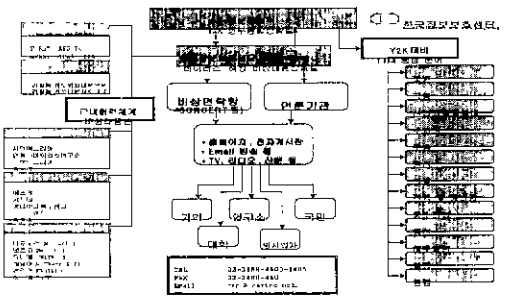
일 자	주 요 내 용	비 고
'99.11 22	홈페이지 개설	http://www.certcc.or.kr/cviic/y2kvirus
11 27	비상대응반, 1차 실무자회의 개최	○ 신고 접수 처리절차 협의 ○ 비상대응반 보도 방안 협의 등
12 3	1차 보도자료배포	"Y2K관련 바이러스·해킹방지 비상체제 돌입"
12 6	대국민 신문광고	전자신문, 동아일보, 조선일보 등
12. 7	관련 설명회 개최, 해킹탐지서비스 게시	상공회의소, 600여명 참석 ※ CD-ROM, 지침서 등 배포
12.9-11	바이러스 모의훈련	418개 기관 대상, 56개 기관 감염 등
12. 15	비상대응상황실 개시	상황관리시스템 운영 http://www.y2kvirus.or.kr
12. 17	비상대응반, 2차 실무자회의 개최	○ 신고접수 양식 등 확정 ○ 2차 모의 훈련 협의
12. 20	2차 보도자료 배포	"Y2K관련 해킹취약점 점검서비스 개시"
12. 28	3차 보도자료 배포	"제2차 Y2K관련 바이러스 모의훈련 실시"
12. 29	4차 보도자료 배포	"CIH변종, 신종바이러스 WIN95/LOVE 발견, 유닉스를 노리는 밀레니엄웜(Millennium Worm) 국내 발견"
'00.01.01	Y2K전환시점 현황보고	해외 바이러스해킹사고 없음, 국내사고무
01. 02	5차 보도자료 배포	"Y2Kaos, XTCP등 신종바이러스 발견"
01. 03	MyPics 경보관련 홍보	"MyPics 국내피해 확산"(4개 방송, 주요신문)
01. 04	6차 보도자료 배포	"비상대응기간 Y2K관련 바이러스·해킹 신고접수 결과 - 큰 피해없이 상황 종료, 하지만 지속적인 대응책 마련 필요"

〈표 3〉 Y2K 관련 컴퓨터바이러스 경보 현황

바이러스 명	감염 특징 및 피해 증상	대응 날짜
W32/MyPics	Y2K 문제 가상 Simulation 바이러스 E-Mail에 PICS4YOU.EXE 파일 첨부 2000년 1월 1일 이후 부팅시 "CMOS Checksum Invalid"라는 메시지 출력, 시스템의 하드 디스크 드라이브 포맷	'99 12.6
W95/Babylonia	Y2K 문제 해결 가장 바이러스 자체 Plugin에 의한 업데이트 기능 IRC로 2KBug-MircFix.exe 파일 전파 데이터의 손상과 부팅 시 메시지 출력	'99. 12.8
Win32/ExploreZip.worm.pak.b	E-Mail을 통한 자체 전파 기능 E-Mail에 FILE_ZIPPUTLEX 파일 첨부 파일 확장자가 DOC, XLS, PPT, ASM, C, CPP 파일의 크기를 0바이트로 만듦	'99. 12.10
W32/NewApt	Y2K 축하 프로그램 가장 바이러스 baby.exe,bboy.exe, boss.exe 등의 파일을 임의적으로 첨부하여 전파 특정 사이트로의 "ping-bomb" 공격이나, 전화 접속 등으로 네트워크 트래픽 증가	'99. 12.20
Win95/Love	겹쳐쓰기, 메모리 상주형 파일 바이러스 윈도우 95/98에서 동작 2000 3. 1이후 매월 1일 음악 연주, 시스템 정지	'99. 12.29
VBS/TUNE	E-Mail을 통한 자체 전파 기능 E-Mail에 TUNE.VBS 파일 첨부	'99. 12 31
Trojan/Y2Kaos	Y2K 문제 가상 Simulation 바이러스 Y2K 관련 신종 바이러스(트로이목마) 2000년 7월 4일 이후에 파일 삭제 2000년 1월 1일 이후에는 시스템 날짜를 2000년 1. 1로 시스템 날짜를 변경	'00 1.1
Trojan/XTCP	신종 바이러스(트로이목마) 원격 시스템 관리, 정보 유출 기능	'00. 1 1
W32/MyPics	Y2K 문제 가상 Simulation 바이러스 E-Mail에 PICS4YOU.EXE 파일 첨부 2000년 1월 1일 이후 부팅시 "CMOS Checksum Invalid"라는 메시지 출력, 시스템의 하드 디스크 드라이브 포맷	'00. 1.3 (재경보)

황실을 구축·운영하고 정보통신부 Y2K 정부종합상황실, 국가정보원, 검·경 수사기관 등의 정부기관과 연계하여 국내 백신업체(4개), 백업·복구·방역서비스업체(5개), 망사업자(6개) 등의 전문가로 구성된 비상대응반과 공동으로 Y2K관련 컴퓨터바이러스 사고에 신속한 대응활동을 통해 새천년 전환시기에 국내에서 큰사고가 없었다.

다음의 (그림 7)에서는 Y2K관련 컴퓨터바이러스·해킹 비상대응체계를 보여주고 있다. 또한 운영기간동안 비상대응반 비상대기요원은 한국정보보호센터 40여명을 포함하여 백신업체, 복구업체 등 총 120여명이었으며, 주요 활동실적은 <표 2, 3>과 같다.



(그림 7) Y2K관련 컴퓨터바이러스·해킹 비상대응체계도

5. 향후계획

최근에 국내외적으로 활동중인 컴퓨터바이러스는 대부분 E 메일을 통하여 전파되는 인터넷웜과 매크로바이러스 및 트로이목마가 주종을 이루고 있다. 이는 지금 현재에 주로 사용되는 윈도우시스템 환경에서의 PC를 대상으로 제작된 경우이나, 올해 초에서부터 해외에서 발생한 컴퓨터바이러스 중에는 향후 리눅스기반의 PC서버를 겨냥하여 제작되는 리눅스 바이러스와 진보된 형태의 해킹기법과 결합된 신종 컴퓨터바이러스가 주종을 이루리라 예측된다.

이에 따라 한국정보보호센터 컴퓨터바이러스 전담반에서는 신종 악성 컴퓨터바이러스 시험분석, 국내 바이러스 대응정보 DB 구축, 바이러스 신고센터 운영확장 등의 웹기반 컴퓨터바이러스 종합상황관리시스템을 개발·운영함으로서 국가적으로 국내 전반에 걸쳐 피해를 줄 수 있는 악성 컴퓨터바이러스에 대한 사전예보제 활동을 강화하고 이와 더불어 실시간 바이러스 예보 및 예방지침을 내용으로 하는 PC 화면보호기(버젼 2.0) 등의 홍보물 제작·보급과 전용 홈페이지 운영 (http://www.certcc.or.kr/cvirc) 등을 통하여 대국민 홍보활동을 지속적으로 펼쳐 나아갈 것입니다.

또한 국책과제로서 컴퓨터바이러스·인터넷웜·트로이목마 등 악성 프로그램 방지지침 개발과 리눅스 바이러스 기법 및 대응기술 연구, 해킹기법 응용 트로이목마 탐지 및 제거기술 연구, 차세대 악성 컴퓨터바이러스 시험분석 연구 등의 컴퓨터바이러스 대응관리시스템 개발과 국내 백신업체·관련학계 전문가와 공동으로 차세대 악성 컴퓨터바이러스 대응을 위한 학습형 면역시스템 연구 등을 수행하여 향후 새천년에 기승을 부릴 컴퓨터바이러스 대응을 위한 기반기술 연구에 박차를 가할 예정입니다.

참고문헌

[1] 한국정보보호센터, "컴퓨터 바이러스 종합방지대책" 1996.

[2] 안철수, "안철수의 바이러스 예방과 치료", 정보시대 1997.

[3] 한국정보보호센터, "불특정 컴퓨터 바이러스 차단 S/W 프로토타입 개발" 1998.

[4] 한국정보보호센터 컴퓨터바이러스 전담반 종합상황실 홈페이지
http://www.certcc.or.kr/cvirc/cvirc-2.htm

[5] 한국정보보호센터, "'99 해킹 및 바이러스 대응 현황" 1999.

[6] 한국정보보호센터, "실무자를 위한 해킹·컴퓨터바이러스 예방 및 방지지침" 1999.

[7] WOI (The WildList Organization International)
http://www.wildlist.org/

[8] 통계 자료 제공 안철수컴퓨터바이러스연구소, 트렌드코리아, Y2K 비상대응반

김 재 성

1986년 인하대학교 전자계산학과 졸업(학사)
1989년 인하대학교 전자계산학과 졸업(이학석사)
1989년 LG 정보통신 중앙연구소 연구원
1990년-95년 한국전자통신연구원 선임연구원
1996년-현재 한국정보보호센터 선임연구원
관심분야 : 해킹 및 바이러스 대응기술, 컴퓨터 및 네트워크 보안, 정보보호 기술표준화, 무선통신 보안

임 채 호

1986년 홍익대학교 전자계산학과 졸업(학사)
1990년 건국대학교 전자계산학과 졸업(이학석사)
1995년 홍익대학교 전자계산학과 박사과정 수료
1985년-1992년 KIST 시스템공학연구소 선임연구원
1992년-1995년 대전실업전문대학 전자계산과 교수
1995년-1996년 KIST 시스템공학연구소 선임연구원
1996년-현재 한국정보보호센터 선임연구원
관심분야 : 인터넷 보안, 분산시스템 보안

이 상 엽

1998년 성균관대학교 제어계측공학과 졸업(학사)
1998년-현재 한국정보보호센터 연구원
관심분야 : 차세대 지능형 통합 보안솔루션 설계, 해킹응용 유닉스 바이러스 및 트로이목마 연구