어느덧 성년…
컴퓨터 바이러스의 어제와 오늘

올해는 컴퓨터 바이러스가 최초로 등장한 지 20주년이 되는 해이다. 그다지 반갑지 만은 않은 기념일이지만 갈수록 지능화되고 교묘해지는 악성코드에 대비하기 위해서는 한번쯤 되새겨 보며 그 기원과 역사를 살펴볼 필요가 있을 것이다. 이에 본 고에서는 컴퓨터 바이러스의 기원 및 단계별 발전 과정을 점검해 본다. 최근 사이버 공간에서 발생하는 보안 사고의 범죄성향이 갈수록 짙어지고 있는 만큼 이와 같은 악성코드의 단계별 발전 과정을 살펴보는 것은 앞으로 더욱 거세질 악성코드의 공격에 철저히 대비할 수 있는 첫걸음이라 생각된다. 보안의식 고취를 위한 발걸음을 함께 내디뎌보자.

글 **신선자** 자유기고가

사이버 공간에서 발생하는 보안 사고의 범죄 성향이 갈수록 지능화돼 가고 있다. 보안전문가들에 따르면 최근 사이버 범죄는 금전적 이익을 위한 범죄의 형태로 발전, 특정 회사나 조직을 겨냥해 은밀화, 소규모화되는 추세다. 불과 몇 년 전만 해도 지식에 대한 과시나 사회적 공론화를 위한 집단적 공격 성격이 강했으나 이제 특정 타깃을 대상으로 개인의 금전적 이득을 목적으로 한 범죄로 대체되고 있는 것이다. 보안 사고 발생 건수는 예년에 비해 줄어들었으나 스팸과 컴퓨터 바이러스 등 악성 코드나 기타 보안 침해 공격이 특정 목적을 가진 범죄 형태로 진행되고 있어 인터넷 세상을 위협하고 있다.

바이러스 출현 20주년

특히 지난 1월 세상에 등장한지 20주년을 맞은 컴퓨터 바이러스의 경우 뚜렷한 감소세를 보이고 있지만 봇 공격(PC에 봇 프로그램을 설치한 뒤 이 프로그램을 통해 자신이 원하는 대로 특정 웹 사이트를 공격하는 형태)과 컴퓨터 바이러스, 웜 등의 악성코드를 결합시켜 복합적인 형태로 공격하는 사례가 급증하고 있다. 또한 이들 악성코드는 한층 교묘해지고 지능화되어 강력한 주의가 필요하고, 단순 PC 외에 e메일 · 메신저 · P2P 프로그램 등이 확산돼 언제 어디서 감염될 지 예상하기도 힘들다.

도대체 컴퓨터 바이러스는 언제부터 기원한 것일까.

최초의 컴퓨터 바이러스는 1986년 파키스탄에서 발견된 〈브레인(Brain)〉 바이러스이다. 파키스탄의 프로그래머가 자신이 개발한 프로그램의 복제품이 성행하자 사용자들을 골탕 먹이기 위해 데이터를 파괴하는 악성 바이러스를 처음으로 유포하기 시작했다고 한다. 자신들이 애써 개발한 소프트웨어가 불법 복제로 뿌려지는 것을 본 프로그래머가 바이러스를 제작해 디스켓을 통해 유포시킨 것.

이어 1987년 예루살렘 대학에서는 13일의 금요일에 맞춰 실행되어 13일의 금요일 바이러스라는 별명으로 유명해진 〈예루살렘 바이러스〉가 발견됐다. 우리나라에는 88년 이 같은 바이러스가 유입됐으며 이에 대항한 백신 프로그램이 개발됐다.

그러나 컴퓨터 바이러스 개념이 처음 등장한 것은 1970년대까지 거슬러 올라간다. 소설가 데이비드 제럴드의 공상과학소설 〈할리가 하나였을 때(When Harlie was One)〉에는 '다른 컴퓨터에 계속 자신을 복제, 감염된 컴퓨터의 운영체제에 영향을 끼쳐 점차 시스템을 마비시키는 장치를 한 과학자가 제작해 배포한다' 는 내용이 소개된 바 있다. 또 1970년대 미 국방성의 네트워크 시스템인 알파 네트에 발견된 '크리퍼(Creeper)' 라는 프로그램이 최초의 바이러스라는 주장도 있다.

엄밀히 말하면 바이러스의 첫 등장은 1970년대 초까지 거슬러 올라가지만 이것은 일반 사용자들이 알기 어려웠을 뿐만 아니라 최초의 바이러스라고 부르기에는 그 피해 정도가 미미했다. 따라서 '브레인' 바이러스를 민간에서의 첫 출현 바이러스로 꼽는 게 정설로 여겨지고 있다.

국내의 경우는 '브레인' 바이러스 출현 이후 이와 유사한 부트 바이러스인 LBC 부트 바이러스가 1989년 제작됐고, 대부분 이 LBC 바이러스가 최초의 '국산' 바이러스라고 알려져 있다. 하지만 일부 자료에 따르면 LBC 바이러스 등장 이전인 1989년 초에 이름도 달콤한 '벌꿀(Honey)' 바이러스가 이미 출현했고 이 벌꿀 바이러스가 국내 최초의 국산 바이러스로 기록됐다.

이후 1990년대 초반에는 많은 수의 국산 파일 바이러스가 제작, 발견됐으며 어떤 때에는 외국 바이러스 보다 국내에서 제작된 바이러스가 월등히 그 수가 많을 때도 있었다고 한다.

사이버 테러의 시작은 트로이 목마

그러나 컴퓨터 바이러스가 사이버 테러의 첫 시발점이라고 생각하면 오산이다. 바이러스 등장 이전에도 피해 사례들이 많았다. 일례로 1986년 브레인 바이러스가 등장하기 전 1980년대 초에는 프로그램이나 파일 등을 삭제하는 트로이 목마가 일반 사용자들에게 알려졌으며, 실제 피해도 발생했다고 한다.

만약 독자 여러분이 도스시절부터 백신 프로그램을 사용했던 경험이 있다면 아마도 로즈 그린버그(Ross M. Greenberg)가 제작했던 〈플루샷〉이라는 백신 프로그램을 기억할 것이다.

1984년에는 이 유명한 백신 프로그램으로 위장한 〈플루샷4〉라는 트로이 목마가 게시판 등에 업로드 됐고 이를 많은 사람이 다운 받아 피해를 입은 적이 있다고 하니 현재처럼 다양해지고 교묘해진 악성코드의 기원은 여기서 찾을 수 있을 듯하다.

그렇다면 컴퓨터 바이러스라는 개념을 받아들여서 대량의 컴퓨터 바이러스를 만들기 시작한 나라는 어디일까. 통설에 따르면 미국이다. 미국의 해커들은 브레인 바이러스와 예루살렘 바이러스를 모방한 수많은 컴퓨터 바이러스를 만들었으며, 전세계적으로 수많은 변형 바이러스를 만들어내고 전파했다고 한다.

또한 당시 바이러스로 유명해진 나라로는 불가리아가 꼽힌다. 불가리아는 〈어둠의 복수자〉, 〈Dir-Ⅱ〉 등의 바이러스를 양산해 바이러스 제작소라는 악명을 얻게 됐다. 그리고 최근에는 국경을 불문하고 수많은 국가에서 다양

한 신종 바이러스가 개발 · 제작 · 유포되고 있는 실정이다.

〈표 1〉에서 보는 바와 같이 20여 년의 변천을 거치며 바이러스와 웜, 트로이목마 등의 악성코드는 사이버 세상을 위협하는 무서운 존재로 급부상하고 있다. 더욱이 바이러스를 포함한 악성코드는 그 동안에도 끊임없이 진화하고 있고 현재도 진화를 거듭하고 있다. 초기 도스용 바이러스에서 윈도→네트워크→인터넷용으로 진화하면서 피해 규모도 엄청나게 커졌다. 컴퓨터 시스템을 망가뜨리고 정보를 빼가는 것은 물론 전체 네트워크를 마비시킴으로써 유발하는 금전적인 피해도 서두에서 언급한 것처럼 더욱 막강해지고 있다.

초창기 바이러스들이 플로피디스크를 통해 전파됐던 데 반해 점차 PC통신→인터넷→e메일→네트워크→메신저 등으로 유포경로가 변하면서 그 확산속도와 피해규모는 상상을 초월한다.

그런데 이렇게 바이러스가 급격히 유포될 수 있는 이유는 무엇일까. 이는 바이러스 제작이 비교적 손쉽게 이뤄지고 있기 때문이다. 1990년대 들어 바이러스 제작자들은 친절한 나머지 일반 사용자들도 바이러스를 만들 수 있도록 'Computer virus construction kit'을 제작해 공개하는 등 다양한 해킹 툴들을 쉽게 구할 수 있는 환경이 조성됐다.

이렇게 제작된 툴 킷은 처음에는 도스용 바이러스만을 만들 수 있도록 발전하다가 현재에 이르러서는 매크로 바이러스, VBS 바이러스, 백오리피스와 같은 서버, 클라이언트 개념의 트로이목마 등도 제작할 수 있도록 기능이 다양해졌다.

〈표 1〉 연대별로 본 악성코드의 역사

년도	주요 내용
1980년 초반	트로이목마 유행.
1986	IBM PC용 바이러스 등장. 첫 컴퓨터 바이러스인 브레인 바이러스 발견.
1987	초기 형태 바이러스 등장. 13일의 금요일에 맞춰 등장한 예루살렘 바이러스 발견.
1988	국내 바이러스 등장, 모리스웜, 백신 프로그램 등장.
1989	바이러스 피해 본격 발생, 국산 바이러스 HOOOO 등장.
1990	바이러스 제작소 불가리아.
1991	Dir-II 바이러스 등장.
1992	미켈란젤로 바이러스 신드롬, 윈도용 바이러스 Winvir 등장.
1993	바이러스 제작 기법 발달.
1994	뉴스그룹을 통한 바이러스 확산, 국산 시스터보 바이러스 등장, 매크로(Macro) 바이러스 등장.
1995	매크로(Macro) 바이러스 확산.
1996	윈도95 바이러스 등장, 국산 바이러스 급증.
1997	리눅스 바이러스 등장.
1998	다양한 악성 프로그램 등장. CIH 바이러스 등장
1999	e메일 바이러스 효시인 멜리사 바이러스 등장. e메일로 확산되는 웜 지속 등장, 바이러스에 의한 대규모 피해 발생, Y2K 특수.
2000	감염 규모 신속, 거대화. 러브레터 웜, 나비다드(Navidad) 웜 등이 대표적 웜 바이러스로 등장.
2001	리눅스 등 OS, 각종 애플리케이션의 보안 허점 악용 사례 증가, 님다 웜 및 아웃룩 주소로 자동 발송되어 EXE 파일을 손상시키며 자체 SMTP를 이용해 메일로 발송돼 C드라이브 파일과 폴더를 삭제하는 서캠(Sircam) 웜 등장.
2002	최초의 플래시 감염 바이러스 등장. MSN 메신저를 통해 퍼지는 악성코드 급증. 매크로 바이러스를 만들어주는 제작 사이트 및 P2P 서비스 중 하나인 KaZaA를 통해 퍼지는 벤자민 웜 등장으로 P2P 를 통해 퍼지는 웜 증가 추세 보임. 아웃룩으로 자동 스팸메일을 보내는 형태의 웜 발견 등 공격 매체 다양해짐.
2003	1. 25 대란 발생. 이른바 '웜들의 대공습' SQL_Overflow(일명 슬래머) 웜이 등장, 인터넷 대란을 일으키며 보안의 위협에 적절히 대처해야 할 이유를 알려줌. 이후 8월에는 1, 2분 간격으로 컴퓨터를 강제 재부팅시킴으로써 국내외에서 큰 피해를 발생시켰던 블래스터 웜(Blaster worm)을 시작으로, 웰치아 웜(Welchia worm), 그리고 엄청난 양의 스팸 메일을 집중 발송해 전세계를 깜짝 놀라게 한 바 있는 소빅.F 웜(Sobig.F worm) 등 거의 1주일만에 세계적인 영향력을 가진 웜 3종류가 한꺼번에 공격.
2004	1월 26일 마이둠 웜(Mydoom) 등장. 역대 최고의 전파속도로 세계적으로 100만대 이상의 PC를 감염시킴. 이외에도 넷스카이(Netsky), 베이글(Bagle), 새서(Sasser) 웜 등이 지속적으로 변종을 등장시킴. 한편, 같은 해 6월에는 자기 복제와 네트워크를 통해 전파되는, 최초의 웜 형태의 휴대전화 악성코드인 카비르(Cavir) 웜이 등장, 휴대전화도 악성코드의 위협에 노출되기 시작.
2005	컴워리어(CommWarrior) 휴대전화 악성코드 등장. 3월에는 블루투스 외에 멀티미디어메시징서비스(MMS)를 이용해 감염된 휴대전화에 저장된 전화번호로 악성코드를 퍼뜨리는 바이러스가 등장, 전파 방법상에서의 지역적 한계를 넘어섬.

자료: 안철수연구소

보안의식 강화가 해결책

바이러스 변천이 심해지던 1990년대 중 · 후반쯤 쓰여진 관련 서적에 보면 바이러스의 미래에 대해 기술해 놓은 내용들을 많이 볼 수 있는데, 당시에 언급된 미래에 등장하거나 유행할 바이러스에는 ▲윈도 사용자 증가로 Win32 환경의 바이러스의 증가 ▲전자우편 사용으로 감염되는 바이러스나 웜 ▲네트워크의 발달로 전파되는 바이러스나 웜 ▲리눅스용 바이러스의 출현 등이 언급돼 있다.

이는 실제로 거의 다 적중했다. 보안전문가들이 너무 똑똑해서 전망을 잘했다고 할 수는 없다. 더욱 교묘해지고 지능화된 바이러스의 공격만큼 새로운 바이러스 분석과 치료법 개발 역시 동시에 이뤄지고 있다는 것이니 각별한 주의가 필요하다는 것을 인식해야 할 것이다.

현재도 세계 각지에서 매일 수십 종의 바이러스가 발견되고 있으며 물론 도스시절처럼 다량의 바이러스가 만들어지진 않지만 윈도 파일 바이러스들이나 웜, 트로이목마 등의 악성 프로그램들이 지금 이 시간에도 누군가 의해 제작되고 있을 것이다.

컴퓨터 바이러스는 안전한 사이버 세상을 위협하는 가장 큰 적이자 도처에서 문제를 일으키는 '사이버 지뢰'로서 IT산업 발전을 가로막고 있다. 컴퓨터 없는 삶은 상상할 수 없는 오늘날 컴퓨터 이용자들이 바이러스의 소멸을 소망하고 보안의식을 고취시켜야 하는 이유는 여기에 있다.

문제는 얼마만큼 보안의식을 가지고 이러한 백신 프로그램을 잘 활용해 안전한 컴퓨터 환경을 만드느냐에 있다. 수없이 많은 악성코드가 판을 치고 있지만 안심하고 컴퓨터 게임을 즐기고 인터넷 세상을 둘러보려면 사용자 스스로부터의 보안의식을 공고하게 다지고 챙겨야 깨끗하고 안전한 인터넷 세상을 꿈꿀 수 있다.

단계별로 보는 **컴퓨터 바이러스**의 변천사

1 데이터 파괴 트로이목마(1985년)

바이러스나 웜이 유행하기 전에도 시스템에 존재하는 파일을 삭제하거나 데이터를 손상시키는 트로이목마는 존재했었다. 주로 BBS(Bulletin Board System)를 통해 유용한 공개 소프트웨어로 가장해 일반 사용자의 컴퓨터를 공격했다.

2 부트 바이러스(1986년)

바이러스가 본격적으로 문제가 되기 시작한 1980년대 후반부터 1990년대 초까지 유행한 바이러스는 대부분 제작이 상대적으로 쉬운 부트 바이러스였다. 당시에는 플로피 디스크를 통해 데이터 교환이 이뤄졌고 부트 바이러스는 불법 복제를 통해서도 짧은 시간에 널리 퍼졌다. 브레인 바이러스(Brain virus), 탁구 바이러스(Pingpong virus), 돌 바이러스(Stoned virus), LBC 바이러스(LBC virus), 미켈란젤로 바이러스(Michelangelo virus), 원숭이 바이러스(Monkey virus) 등이 있다.

3 비상주형 파일 바이러스(1987년)

바이러스에 감염된 파일을 실행하면 감염되지 않은 COM 파일이나 EXE 파일을 찾아 감염시키는 비상주형 파일 바이러스가 등장했다. 비상주형 바이러스는 전파 속도가 상대적으로 느리다. 비엔나 바이러스(Vienna virus), 데이터크라임 바이러스(Datacrime virus) 등이 있다.

4 메모리 상주형 파일 바이러스(1987년)

메모리에 상주해 실행되거나 사용되는 실행 파일을 감염시키는 상주형 바이러스가 등장한다. 감염된 파일을 실행 할 때 다른 파일을 감염 시키는 비상주형 바이러스에 비해 상주형 바이러스는 보다 빠른 시간에 시스템에 존재하는 다른 파일을 감염 시킬 수 있다. 예루살렘 바이러스(Jerusalem virus), 르하이 바이러스(Lehigh virus), 어둠의 복수자 바이러스(Dark_Avenger virus) 등이 있다.

5 암호화 바이러스(1987년)

백신 프로그램이 바이러스를 진단 혹은 치료를 어렵게 하기 위해 프로그램의 일부 또는 대부분을 암호화시켜 저장한다. 1987년 독일에서 발견된 폭포 바이러스(Cascade virus)가 최초의 암호화 바이러스이다. 폭포 바이러스(Cascade virus), 영시간 바이러스(Zerotime virus), 시스터보 바이러스(SysTurbo virus) 등이 있다.

6 은폐형 바이러스(1990년)

사용자가 감염 사실을 어렵게 하기 위해 은폐기법(Stealth Technique)이 사용됐다. 바이러스가 기억장소에 상주할 때 부트 바이러스는 정상 부트 레코드를 보고 파일은 증가된 파일 길이를 정상 파일로 보이거나 감염된 파일을 읽을 때 정상 내용을 보여줘 감염 사실을 알기 어렵게 한다. 프로도 바이러스(Frodo virus), 테킬라 바이러스(Tequila virus) 등이 있다. 은폐형 바이러스도 기억 장소를 먼저 검사해 은폐기능을 무력화시키면 쉽게 진단할 수 있다.

7 다형성 바이러스(1992년)

바이러스 제작자들은 진단을 어렵게 하기 위해 암호를 푸는 루틴을 감염할 때마다 달라지는 다형성 기법(Polymorphic Technique)을 개발했다. 암호화 바이러스는 고정적인 암호화 루틴을 가지고 있어 암호해제 코드의 일부로 쉽게 진단할 수 있었다. 최초의 다형성 바이러스는 1990년에 Mark Washburn이 제작한 V2PX 바이러스(V2PX virus)이며 본격적인 다형성 바이러스는 1992년 봄 자신을 어둠의 복수자(Dark Avenger)로 부르는 불가리아인이 제작한 MtE(Mutation Engine)이다. 어둠의 복수자는 자신이 제작한 다형성 엔진을 공개해 다른 바이러스 제작자가 이를 이용해 간단한 바이러스도 다형성 기법을 이용할 수 있도록 했다. 이에 백신 업체는 에뮬레이터를 개발해 코드를 가상으로 실행해 다형성 바이러스를 진단한다. V2PX 바이러스(V2PX virus), 나타스 바이러스(Natas virus), 마버그 바이러스(Win95/Marburg virus), HPS 바이러스(Win95/HPS virus) 등이 있다.

8 갑옷형 바이러스(1994년)

분석을 어렵게 하기 위해 자신을 보호하는 갑옷형 바이러스(Armored virus)가 등장했다. 분석을 어렵게 하기 위해 메모리에서도 자신을 암호화하거나 안티 디버깅 코드를 바이러스에 넣어 분석을 어렵게 한다. 고래 바이러스(Whale virus) 등이 있다.

9 메타모픽 바이러스(1995년)

대부분의 다형성 바이러스가 백신의 에뮬레이터로 진단이 가능하자 바이러스 제작자는 암호화 루틴만 랜덤한 형태가 아닌 바이러스 코드 자체를 만들어내는 메타모픽 바이러스를 제작했다. ACG 바이러스(Amazing Code Generator), Win95/Zmist 바이러스 등이 있다.

10 매크로 바이러스(1996년)

매크로 바이러스는 애플리케이션에 존재하는 매크로를 이용해 자신을 전파하는 바이러스이다. 1994년 MS 오피스의 매크로를 이용해 바이러스를 제작할 수 있음이 XM/DMV 바이러스와 WM/DMV 바이러스로 증명됐고 1995년 여름 WM/Concept 바이러스가 등장해 전세계로 퍼졌다. 매크로 바이러스는 실행 파일이 아닌 문서 파일에 감염되고 실행 파일보다 빈번하게 교환이 이뤄지는 문서의 특성상 보다 빨리 퍼지게 되고 개인사용자보다 문서를 많이 사용하는 기업에서 더 문제가 됐다. 매크로 바이러스는 1996년에서 2000년까지 많은 피해를 입혔으며 초기의 간단한 형태에서 암호화, 은폐형, 다형성도 등장했다. 하지만 MS 오피스의 보안 기능이 강화되면서 일반적인 매크로 바이러스가 활동할 수 없게 되자 2002년 이후 매크로 바이러스는 급격히 감소했다. 개념 바이러스(WM/Concept virus), 캡 바이러스(WM/Cap virus), 클래스 바이러스(W97M/Class, virus), 트리스테이트 바이러스(O97M/Tristate virus) 등이 있다.

11 백도어(1998년)

윈도와 초고속인터넷 사용자가 증가하면서 개인 컴퓨터의 인터넷 사용자도 증가하기 시작했다. 이에 악성코드에도 불법적인 접근 기능을 제공하는 백도어 기능이 포함되고 백도어 역할을 하는 트로이목마가 유행했다. 이때부터 개인 정보 노출이 문제가 됐다. 백오리피스(Win-Trojan/ Back_Orifice), 넷버스(Win-Trojan/Netbus) 등이 있다.

12 메일 전파(1999년)

인터넷의 발전은 악성코드의 새로운 감염 기회를 줬다. 1999년 1월 메일로 전파되는 해피99(I-Worm/Happy99)가 퍼졌으며 3월에는 아웃룩을 통해 메일로 전파되는 멜리사 바이러스(W97M/Melissa virus)가 짧은 시간에 전세계로 퍼져나갔고 FBI까지 동원되어 바이러스 제작자를 검거하게 됐다. 메일의 첨부파일을 통해 전파되는 웜의 등장은 악성코드가 더 이상 국지적으로 활동하지 않고 전세계로 짧은 시간에 퍼질 수 있음을 의미했다. 소버 웜(Win32/Sober.worm), 마이둠 웜(Win32/Mydoom.worm), 넷스카이 웜(Win32/Netsky.worm) 등이 있다.

13 취약점 이용(1999년)

취약점을 이용해 사용자 모르게 감염되는 악성코드가 등장했다. 원래 취약점을 이용한 공격은 대형 컴퓨터에 불법적으로 접속하기 위해 이용됐다. 초기에 취약점을 이용한 악성코드는 취약점이 존재하는 메일 클라이언트로 메일을 읽을 때 웜이 자동으로 실행되도록 제작됐다. 이후 발표되는 다양한 보안 취약점을 이용한 악성코드가 등장하게 되고 사용자들도 패치를 통해 보안 취약점을 해결해야 했다. 버블보이 웜(VBS/Bubbleboy), 칵 웜 (JS/Kak) 등이 있다.

14 스크립트 악성코드(2000년)

윈도에 포함된 VB 스크립트(VB Script)는 베이직과 유사한 형태의 쉬운 문법과 시스템을 접근할 수 있는 강력한 기능을 제공한다. VB 스크립트나 자바 스크립트(Java Script)를 이용한 악성코드 제작이 시작됐다. 2000년 5월 5일 러브레터 바이러스(VBS/Love_Letter virus)가 전 세계를 강타하고 아웃룩을 통해 전파되는 VB 스크립트 웜이 유행했다. 이에 마이크로소프트사는 아웃룩을 통해 실행 파일을 보낼 수 없는 기능을 추가하면서 VB 스크립트 웜은 자취를 감추게 됐다. 러브레터 바이러스(VBS/Love_Letter virus), 프리링크 웜(VBS/Freelink worm), VBSWG 웜(VBS/VBSWG) 등이 있다.

15 해킹과 악성코드의 만남(2001년)

시스템에 존재하는 프로그램의 취약점을 이용해 파일 형태로 존재하지 않고 시스템의 기억장소와 네트워크 패킷으로만 존재하는 웜이 등장했다. 파일로 존재하지 않으므로 파일 검사 기반의 백신에서는 예방과 진단을 할 수 없게 됐다. 네트워크로 전파되는 악성코드에 대한 백신의 한계가 나타났으며 이에 백신 회사는 백신 뿐 아니라 방화벽(Firewall) 등에도 눈을 돌리게 됐다. 주로 버퍼 오버플로우(Buffer Overflow)를 이용해 웜을 실행하며 과거 해킹에서 사용됐던 기법을 웜에서 이용하고 웜이 자동화된 해킹 툴로 발전하며 해킹과 악성코드의 경계가 모호해지게 됐다. 코드 레드 웜(Codered worm), 님다 바이러스(Win32/Nimda virus), SQL 오버플로우 웜(SQL_Overflow worm, 일명 슬래머 웜), 위티 웜(Win32/Witty.worm) 등이 있다.

16 실행 압축 이용(2002년)

대부분의 웜, 트로이목마가 파일의 크기도 줄이고 분석도 지연시키기 위해 실행 압축을 이용했다. 동일한 악성코드도 다른 실행 압축으로 압축할 경우 압축을 풀지 못하는 백신은 진단하지 못하므로 동일한 악성코드를 실행 압축 프로그램만 바꿔 새로운 변형을 만드는 경우도 잦아졌다. 이에 백신 업체는 실행 압축 해제 기능을 백신에 추가하게 된다.

17 루트킷(2003년)

악성코드를 사용자나 백신을 포함한 다른 프로그램에서 숨길 수 있는 루트킷(Rootkit)이 증가했다. 루트킷 기능을 악성코드에 포함하거나 루트킷 기능을 하는 별도의 파일을 실행하는 악성코드가 있다. 핵데프 트로이목마(Win-Trojan/ HackDef), 휴피곤 트로이목마(Win-Trojan/ Hupigon) 등이 있다.

18 네트워크를 통한 전파(2003년)

관리목적 폴더, P2P(Peer-to-Peer) 프로그램, 메신저로 전파되는 웜 등장 이후 취약점을 이용해 시스템이 인터넷에 접속하는 것만으로도 감염되는 웜이 등장했다. 네트워크를 통해 전파되는 웜은 패치를 하지 않으면 근본적으로 예방하기 어려우며 치료되지 못한 몇 대의 시스템으로 회사나 학교의 시스템이 재감염되는 경우가 잦았다. 블래스터 웜(Win32/Blaster.worm), 새서웜(Win32/Sasser.worm) 등이 있다.

19 악성 IRC봇(2004년)

IRC(Internet Relay Chat)을 이용해 악의적인 명령을 내리는 악성 IRC봇이 급증했다. 전세계적으로 한 달에 2,000개에서 3,000개의 새로운 변형이 등장하고 악성 IRC봇 기능은 많은 악성코드에 포함된다. Mirc팻(Dropper/MircPack), Sd봇 웜(Win-Trojan/ SdBot), 아고봇 웜(Win32/AgoBot.worm) 등이 있다.

20 스파이웨어 유행(2004년)

광고를 보여주는 에드웨어(Adware)가 유행했다. 보통 스파이웨어(Spyware)로 알려진 애드웨어는 악성코드와 정상 프로그램의 경계에 있는 프로그램이다. 애드웨어로 불편해하는 사용자가 증가하면서 다양한 안티 스파이웨어 제품이 등장하고 존재하지 않는 스파이웨어나 위험도가 낮은 찌꺼기를 진단해 과금을 요구하는 가짜 안티 스파이웨어 제품도 등장했다. 스파이웨어에 대해 명확한 정의는 현재 없으며 보안 프로그램에서 자신의 프로그램을 스파이웨어로 규정할 경우 법적 소송으로 가는 경우도 있다.

21 금전적 이득(2005년)

악성코드 제작 동기가 실력과시에서 금전적 이득으로 바뀌었다. 악성코드 제작자는 악성코드를 이용해 스팸 업체나 광고 업체에 돈을 받고 스팸 메일을 발송하고 애드웨어를 설치한다. 온라인게임의 계정과 비밀번호를 훔쳐 게임 아이템을 팔아 돈을 버는 사람들도 등장한다. 리니지핵(Win-Trojan/Lineage Hack) 등이 있다.

자료: 안철수연구소