주요기사

컴퓨터 바이러스의 특징과 예방 대책

컴퓨터 바이러스는 사용자 몰래 자신을 다른 곳에 복제, 부작용을 일으키는 프로그램으로 1985년 파키스탄과 이스라엘에서 처음 발견되었다.

컴퓨터 바이러스는 부트 영역에 감염되는 부트 바이러스와 파일에 감염되는 파일 바이러스, 그리고 부트와 파일에 모두 감염되는 부트/파일 바이러스 그리고 최근 발견된 매크로 바이러스가 있다.

신종 바이러스 발견 추세는 종류별로는 매크로 바이러스와 트로이목마가 주종을 이룬다.

안 철 수

안철수컴퓨터바이러스연구소 대표이사

컴퓨터를 사용하거나 컴퓨터에 조금만 관심이 있는 사람이라면 예루살렘 바이러스(13일의 금요일에 실행되는 파일을 삭제하는 바이러스)니 미켈란젤로 바이러스(이탈리아 화가 미켈란젤로의 생일인 3월 6일에 C 드라이브의 데이터를 삭제하는 바이러스)니 하는 말을 한 번쯤 들어보았을 것이다. 그만큼 컴퓨터 바이러스는 컴퓨터 사용자 대다수를 괴롭히고 있는 악성 프로그램이다.

바이러스 정의

컴퓨터 바이러스는 일종의 프로그램으로 다른 프로그램들과 달리 사용자 몰래 자신을 다른 곳에 복사하는 명령어를 가지고 있다. 바이러스라는 이름이 붙은 이유는 생물학적인 바이러스가 자신을 복제하는 유전인자를 가지고 있는 것처럼 컴퓨터 바이러스도 자신을 복사하는 명령어들을 가지고 있기 때문이다. 또한 복사하는 데 그치지 않고 부작용을 일으키는 것도 생물학적인 바이러스와 공통적인 면이다. 감기 바이러스가 기침, 두통 등의 증상을 일으키는 것처럼 컴퓨터 바이러스도 부작용을 일으킨다. 컴퓨터의 실행 속도가 떨어지거나 메모리의 크기가 줄어드는가 하면 프로그램이 실행되지 않거나 아예 다운되는 일도 생긴다. 간혹 예쁜 그림이 화면을 채워 화면 보호기처럼 착각을 하게 만드는 바이러스도 있는데, 보기에는 좋아도 다른 작업을 할 수 없는 곤경에 처하게 된다.

이처럼 여러 가지 공통점 때문에 예전에는 생물학적인 바이러스와 혼동하여 디스켓을 깨끗한 물로 씻거나 컴퓨터에 가까이 가지 않는 사람도 있었다. 하지만 결정적으로 컴퓨터 바이러스는 사람이 만들어내는 프로그램이라는 점에서 생물학적인 바이러스와 구별된다.

바이러스의 역사

컴퓨터 사용자, 특히 초보자들을 괴롭히는 컴퓨터 바이러스가 처음 발견된 것은 1985년 파키스탄과 이스라엘에서였다. 파키스탄에서는 한 프로그래머 형제가 자신들이 애써 개발한 프로그램들이 불법 복제되어 사용되는 것을 보고 복수하는 심정으로 만들었다고 전해지는 브레인(Brain)이라는 이름의 바이러스가 만들어져 전세계의 수많은 컴퓨터들을 감염시켰다. 또한 이 무렵 이스라엘에서도 파일 바이러스인 예루살렘 바이러스(Jerusalem virus)가 만들어져 전세계적으로 그 위세를 떨쳤다. 이러한 아이디어를 받아들인 해커(hacker)들은 브레인 바이러스와 예루살렘 바이러스를 모방한 수많은 컴퓨터 바이러스들을 만들어냈다. 그리고는 전세계적으로 수많은 변형 바이러스들을 보급(?)하기 시작했다.

최근에는 대만에서 제작된 CIH 바이러스가 맹위를 떨쳤다.

바이러스의 분류

컴퓨터 바이러스는 크게 4가지로 구분할 수 있다. 부트 영역에 감염되는 부트 바이러스와 파일에 감염되는 파일 바이러스, 그리고 부트와 파일에 모두 감염되는 부트/파일 바이러스 그리고 최근 발견된 매크로 바이러스가 있다. 매크로 바이러스는 엑셀, 워드 등에서 사용되는 매크로를 통하여 감염되는 것으로, 전세계적으로 광범위하게 유포되고 있다.

바이러스와는 조금 다른 악성 프로그램 중에 인터넷 웜과 트로이 목마가 있다. 인터넷 웜은 인터넷 메일에 첨부되어 자동 발송되며, 실행시키면 컴퓨터에 문제를 일으킨다. 트로이 목마는 복제되지 않고 그 자체가 시스템에 문제를 일으키는 실행 파일로, 에코키스나 백오리피스 같은 정보 유출 프로그램이 여기에 속한다.

최근 바이러스 동향

신종 바이러스 발견 추세로 보면 종류별로는 매크로 바이러스, 트로이목마가 주종을 이룬다.

▷트로이목마의 폭증

트로이목마는 자기 복제는 하지 않는 실행 파일로, 실행했을 때 컴퓨터에 문제를 일으키는 프로그램을 가리킨다. 개인 정보를 유출시키거나 상대의 PC를 자신의 PC처럼 사용할 수 있게 하는 해킹 툴이 대부분을 차지한다. 소스가 공개되어 수많은 변종이 만들어져 앞으로도 피해가 이어질 전망이다.

핫키훅(Win-Trojan/HotKeysHook)이나 에코키스(Win-Trojan/Ecokys)의 경우 윈도우에서 입력되는 모든 키보드 내용을 파일로 저장하는 한편 그 파일 자체를 특정 FTP(트로이목마 제작자의 사이트로 추정됨)로 전송하는 기능이 있어 비밀번호 등이 외부로 유출될 수 있다. 실제로 대전에서 이를 이용해 남의 통장에서 돈을 인출한 사람이 검거된 바 있다.

또한 백오리피스(Win-Trojan/BO_2000)는 이 프로그램이 설치되어 있는 시스템 간의 원격 제어를 가능하게 해 멀리 떨어진 컴퓨터의 파일을, 컴퓨터 사용자보다 많은 권한을 갖고 조작할 수 있다.

▷인터넷 웜의 등장 및 기승

인터넷 웜은 트로이목마와 마찬가지로 자기

복제는 하지 않고 E-메일에 첨부 파일 형태로 유포되는 악성 프로그램을 말한다.

작년의 경우 2월에 해피99(I-Worm/Happy 99)를 시작으로 6월에 익스플로어집(I-Worm/ExploreZip), 8월에 프리티팍(I-Worm/Pretty Park), 11월에 픽스2001(I-Worm/Fix 2001), 12월에 뉴앱트(I-Worm/NewApt) 등 5종의 웜이 잇달아 등장했다. 전파 속도가 빠른 만큼 피해 속도도 빠르다는 특징이 있다.

▷스크립트 웜 등장

99년 9월과 10월에 스크립트 기능을 이용해 작성된 바이러스가 5종 등장했다. 스크립트 기능은 매크로 기능과 유사한 것으로, 단순 반복 작업을 편하게 처리할 수 있는 기능이다.

스크립트 웜은 코렐드로우, IRC 채팅 프로그램 등 스크립트 기능이 내장되어 있는 프로그램의 파일과 모든 윈도우 프로그램 파일, HTML 파일 등을 감염시켜 파일 정보를 변경 또는 삭제한다.

바이러스의 증상

컴퓨터 바이러스에 감염되면 감염된 바이러스 종류에 따라 여러 가지 증상이 나타난다. 바이러스 때문에 나타나는 증상은 일일이 열거할 수 없을 정도로 다양하지만, 자세히 살펴보면 몇 가지 공통적인 특징을 발견할 수 있다. 따라서 바이러스의 종류를 잘 파악하고 있다면 신종 컴퓨터 바이러스도 조기에 발견, 치료할 수 있을 것이다.

컴퓨터 바이러스는 정상적인 프로그램의 실행 과정을 가로챔으로써 여러 가지 증상과 바이러스 프로그램 자체에서 만든 여러 가지 부작용을 불러 일으킨다. 특히 다음과 같은 증상이 나타나면 컴퓨터 바이러스를 의심해 보아야 한다. 바이러스에 의한 증상은 일일이 열거할 수 없을 정도로 다양하지만, 공통적인 것을 모아서 분류하면 다음의 4가지로 나눌 수 있다.

(1) 속도 저하

컴퓨터 바이러스는 정상적인 프로그램 실행 과정을 가로채서 자기가 먼저 실행된 다음에 원래의 프로그램을 실행시키기 때문에, 그만큼 실행 속도가 저하된다. 부트 바이러스에 감염되었을 경우에는 부팅 시간이 길어지며 디스크를 읽거나 쓰는 속도가 떨어지게 된다. 파일 바이러스에 감염된 경우에도 프로그램을 처음 시작할 때 불러들이는 속도가 현저히 떨어진다. 때로는 도스에서 DIR 명령으로 디렉토리를 보려고 할 때 화면에 나타나는 시간이 오래 걸리기도 한다.

(2) 감염 흔적

컴퓨터 바이러스는 감염되는 과정에서 여러 가지 흔적을 남긴다. 기억 장소에서 실행되어야 하므로 사용 가능한 기억 장소의 크기가 줄어들며, 파일 바이러스의 경우에는 파일의 길이가 커지거나 파일 작성일이 변경되기도 한다.

(3) 파괴 증상

프로그램이나 디스크의 특정 영역에 대한 파괴 증상을 나타내기도 한다. 감염 후 프로그램이 갑자기 실행되지 않거나 시스템이 다운되는 등 이상한 동작을 보일 경우가 있다. 또한 의도적으로 프로그램을 지워버리거나 하드디스크의 논리적 구조를 파괴하여 인식되지 않게 만드는 경우도 있다. 디스크의 부트 레코드 내용 및 FAT(File Allocation Table) 내용을 변경

하거나 파괴하며 디스크의 디렉토리 내용도 변경하거나 파괴한다. 디스크의 볼륨 라벨을 변경하며 디스크에 불량 섹터를 만들기도 한다.

(4) 바이러스별 특이 증상

컴퓨터 바이러스 제작자가 컴퓨터 바이러스에 의도적으로 포함시킨 특징적인 증상 또는 부작용이 나타날 수 있다. 이상 증상으로는 컴퓨터 바이러스의 종류에 따라 화면에 엉뚱한 메시지를 출력하는 등의 단순한 것부터 깃발, 벌레 등의 그래픽을 출력하는 것, 나아가 하드디스크 전체 자료를 지워버리는 직접적인 파괴 행위에 이르기까지 매우 다양하다. 다시 말하면 컴퓨터 바이러스도 일종의 프로그램이기 때문에 프로그램에서 가능한 정도의 특이한 증상들을 나타내는 것이다.

예를 들어서 탁구(Pingpong) 바이러스의 경우에는 화면에 까만 점 하나가 탁구공처럼 돌아다니는 것이 주요 증상이며, 크리스마스 인사 바이러스는 'Merry Christmas and Happy New Year!'이라는 메시지와 함께 '고요한 밤 거룩한 밤'이라는 캐롤송을 들려준다.

바이러스 예방법

(1) 우선 정품 소프트웨어를 구입해 사용하는 것이 중요하다.

불법 복사한 소프트웨어는 많은 사람의 손을 거치기 때문에 자연히 바이러스에 쉽게 노출되며, 바이러스가 감염되었을 경우 책임 소재도 가릴 수 없으므로 반드시 정품 소프트웨어를 사용해야 한다. 불법 복사가 성행하는 오락 및 게임 프로그램의 상당수가 컴퓨터 바이러스에 감염되어 유통된다고 한다.

(2) 한두 대의 컴퓨터를 여러 사람이 공동으로 사용할 때는 다른 사람이 사용하고 난 뒤에 반드시 전원을 끈 다음 자신의 부팅 디스켓으로 부팅시킨 후 사용한다.

이 방법은 아직도 하드디스크가 없이 사용하는 PC에 해당되며, 하드디스크가 있는 경우에는 하드디스크로 부팅하면 된다. 이렇게 하지 않으면 어떤 경로든지 컴퓨터에 침투해 메모리에 상주한 바이러스가 이후에 사용하는 모든 사용자의 디스켓을 감염시키기 때문이다.

이때 아무 디스켓으로나 부팅하지 말고 자신의 부팅 전용 디스켓 한 장을 만들어 쓰기방지 탭을 붙여 놓는 것이 중요하다. '깨끗한 부팅 디스켓 만들기'는 뒤에 설명하겠다. 아울러 수시로 시스템을 최신 버전의 백신으로 검사해 바이러스 침투를 예방하는 것도 매우 중요하다.

(3) PC 통신이나 인터넷을 통하여 프로그램을 받을 때는 신뢰할 수 있는 유명 통신망이나 동호회, 포럼 자료실 또는 인터넷 홈페이지에서 받도록 한다.

이런 곳은 자료실 담당자가 불법 복사물인지, 바이러스에 감염된 파일인지 등을 확인한 뒤 등록하기 때문에 바이러스에 노출될 확률이 적다.

사설 BBS의 경우가 위험한데, 잘 알려지지 않은 곳에서는 가급적 자료 받기를 삼가는 것이 좋다. 또 한번 내려 받은 프로그램은 최신 버전의 백신 프로그램으로 바이러스 감염 여부를 확인한 후에 사용하는 것이 안전하다.

(4) 인터넷, 네트워크 등 전산 환경의 발달에 따라 컴퓨터 바이러스가 침투할 수 있는 경로는 매우 다양해졌다.

따라서 위에 소극적인 방법 외에 각 전산환경에 맞는 백신 프로그램을 설치하는 적극적인 대책이 필요하다. 설치보다 중요한 것은 항상 최신 버전으로 업데이트하는 것이다. 신종 바이러스가 한 달에 20종 이상씩 발견되고 있기 때문에 신종 바이러스에 대한 퇴치 기능을 수시 업데이트해야 하는 것이다.

기업 환경에서의 LAN(Local Area Network)을 통한 바이러스 감염은 피해 정도 및 규모로 보아 매우 위험하다. LAN으로 연결된 컴퓨터들은 많은 프로그램을 공유함은 물론 방대한 자료 교환이 고속으로 이루어지기 때문에, 한 곳에 침투한 컴퓨터 바이러스가 순식간에 많은 컴퓨터를 감염시켜 버린다. 시스템 파괴를 비롯해 업무를 마비시켜 재산상의 큰 피해를 가져오는 것이다.

따라서 클라이언트 PC는 물론 서버 전용의 백신 프로그램을 이용하여 유입되는 바이러스를 원천적으로 막아주고, 각 PC마다 독립적인 안티바이러스 기능을 수행하여야 안전하게 업무를 볼 수 있다.

백신 프로그램은 바이러스를 진단 치료할 뿐 아니라 예방까지 가능한 프로그램이다. 그러나 바이러스가 만들어진 다음 그것을 분석한 후에 퇴치 기능을 추가하기 때문에 바이러스가 발견된 후에나 그 바이러스에 대해 완벽한 대책을 세울 수 있다.

따라서 업데이트 주기가 빠른 백신을 사용하는 것이 사용자에게는 이익이다. 안철수연구소의 V3 제품군은 매주 1회 정기 업데이트될 뿐 아니라 대규모 피해가 우려되는 바이러스가 출현했을 때 비상 업데이트된다.

백신 프로그램은 구입보다 지속적인 유지보수가 중요하며, 유사시의 큰 피해에 대비하기 위해 투자한다는 차원에서 보험과 같다.

2000년대의 바이러스 동향

스크립트 웜 다수 등장, 리눅스 바이러스 증가, 해킹 툴 및 백도어 트로이목마 기승, 복합성 바이러스 증가 등으로 예측할 수 있다.

▶스크립트 웜 다수 등장

아직 치명적으로 파일을 손상시키는 바이러스는 제작되지 않았지만 앞으로 파괴력이 보강된 바이러스가 등장할 가능성이 다분하다. 또한 매크로 바이러스처럼 변종 제작과 자체 변형이 쉬워 양산될 가능성이 높다는 점에서 매크로 바이러스만큼 영향력이 커질 것으로 추측된다.

▶리눅스 바이러스 증가

리눅스 운영체계 사용자가 증가함에 따라 리눅스 바이러스가 서서히 등장하고 있다. 1998년 처음 발견된 이래 현재까지 세계적으로 5종 정도가 제작된 것으로 보고되었다. 국내에 유입된 것은 없다. 리눅스 운영체계는 코드가 오픈되어 있어 바이러스를 제작하기도 매우 쉽기 때문에 양산이 우려된다.

▶해킹 툴 및 백도어 트로이목마 기승

백오리피스를 비롯한 해킹 툴 프로그램이 더욱 기승을 부릴 전망이다.

또한 사용자 몰래 개인 정보를 특정 컴퓨터로 빼돌리는 백도어 프로그램들도 더욱 많이 등장할 것으로 보인다.

▶복합성 바이러스 증가

웜과 트로이목마가 결합된 형태, 윈도우 실행 파일과 일반 응용 프로그램을 동시에 감염시키는 바이러스 등 다양한 유형이 등장할 것이다.