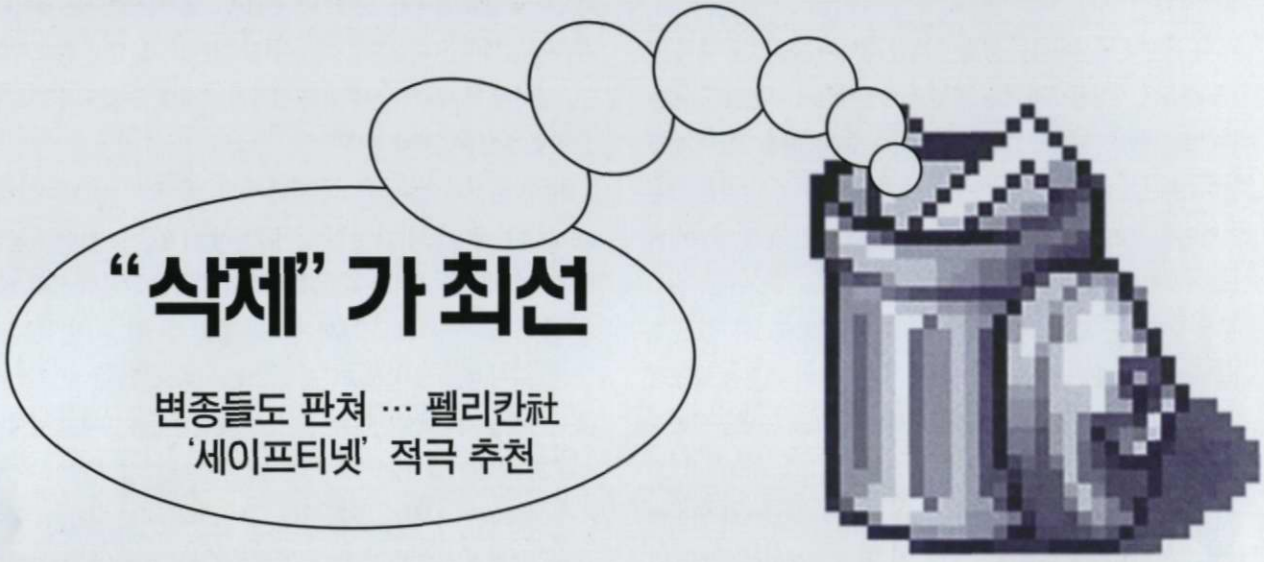
러브바이러스와 그 변종의 피해와 치료



"삭제" 가 최선

변종들도 판쳐 … 펠리칸社 '세이프티넷' 적극 추천

하루 아침에 웬 날벼락인가? 바로 바이러스에 당했을 때 하는 말이다. 그것도 사랑스러운 벌레(Love Worm)에 물렸을 때...

5월 4일 아침에 편지함을 열어보았더니 제목이 'ILOVEYOU' 혹은 'FW: Joke'이고 그 첨부파일의 확장자가 VBS나 JPG, 혹은 TXT인 메일이 있었지만 첨부파일을 클릭할 시간이 없어서 그냥 둔 행운의 사용자가 분명히 있었을 것이다. 하지만 아직도 그 메일이 편지함에 남아있다면 가차없이 휴지통으로 보내길 바란다.

이와 반대로 무슨 메일이지? 친구 편지인가? 같은 호기심 때문에 첨부파일을 무심결에 클릭한 사용자도 있을 터이니, 이제 그 사용자는 한 마리의 인터넷 웜(worm)을 자신의 컴퓨터에 풀어놓게 된 것이다.

일명 (뉴)러브 바이러스라 불리는 이 신종 인터넷 웜은 첨부파일이 열리는 순간 활동을 개시해 마이크로소프트 아웃룩이나 아웃룩 익스프레스의 주소록에 있는 사람들에게 바이러스를 보낸다 - mIRC 채트 클라이언트도 예외는 아니다. 또한 이놈은 멜리사와 같은 웜이나 다른 컴퓨터 바이러스와 달리 사용자의 하드 디스크의 중요한 파일 확장자를 vbs로 바꾸고 크기를 0 byte로 만들어 놓는다.

러브 바이러스/웜의 피해는 다음 4가지로 요약된다:

1. 엄청난 양의 메일로 인해 서버가 다운되거나 마비된다.

2. 다른 메일 서버는 더 이상의 피해와 웜의 전송을 막기위해 오프라인 상태를 취한다.

3. 사용자의 파일은 이름이 바뀌어지고 파일이 갖고 있던 원래 내용은 웜으로 대체된다. 중요한 사용자 파일이 없어지지만, 이름이 바뀐 파일은 특정한 확장자(VBS)를 갖고 있으며, 이 확장자를 갖고 있는 감염된 파일을 삭제해야 한다.

4. 시스템 가동시 웜이 활동하도록 만드는 스크립트 라인과 코드가 추가되기 때문에 일부 시스템 파일이 바뀌게 된다.

CIH가 막강한 위력을 떨치고 있는 가운데 등장한 러브 바이러스. 이 바이러스 때문에 발생한 사건과 해결 방법 등을 이제 살펴보자. 한가지 참고할 사항은 이 바이러스의 무대는 윈도우라는 점이다.

따라서 유닉스나 맥과 같은 기타 OS 사용자들은 이 기사를 읽을 필요가 없으며, 반면 윈도우를 사용하면서 아웃룩을 쓰거나 쓰지 않는 사용자들(메일을 통한 바이러스 확산이 적용되지 않음)은 이 기사를 참조하기 바란다. 아울러 WSA(Windows Scripting Host)를 사용하지 않는 사용자들은 피해를 예방할 수 있다.

공포의 '러브 레터'

러브 바이러스의 첫 번째 공격과 그 피해에 대한 첫 번째 보고는 5월 4일 목요일 아침에 발생하였으며, 오전 중에 경고가 발동되었다. 하지만 당시 유럽과 미국의 메일 서버의 처리 속도는 매우 늦었으며, 결국 문제가 있다는 사실이 개인 사용자들을 위시하여 미국방성, 뉴질랜드 의회, 영국 국회 의사당을 포함한 전 세계 정부기관과 기업들을 통해 보고되기에 이른다.

멜리사와 같이 지금까지 발견된 일반적인 e-메일 바이러스나 웜은 아웃룩이나 아웃룩 익스프레스의 주소록에 담긴 주소를 통해 메일을 다시 보낼 수 있는 한계치가 50명이었다. 하지만 러브 바이러스는 자기 자신을 복제하여 아웃룩이나 익스프레스의 전체 주소록에 담긴 모든 주소로 메일을 보낼 수 있다. 이는 감염된 사용자당 100명이 될 수도 있다.

또한 이 러브 바이러스는 아웃룩이나 익스프레스 뿐만 아니라 유명한 윈도우용 IRC 프로그램인 mIRC를 이용하여 메일을 보낼 수도 있다.

러브 바이러스의 악독한 피해는 사용자 파일을 파괴(덮어쓴다거나 완전히 파괴)한다는 점이다. 또한 시스템 파일을 덮어쓰고, 익스플로러를 통해 특정 사이트에 접속함으로써 재감염 활동을 위해 코드를 다운로드한다. 그 다음에는 사용자의 패스워드를 훔치는 트로이 목마로 활동함으로써 메일을 통해 목적지가 필리핀인 IP 주소로 사용자 패스워드를 전송한다.

이 모든 과정은 사용자가 전혀 모르는 상태에서 은밀히 이루어진다. 러브 라이러스/웜은 표면상으로는 아무런 해가 없을 것 같은 제목(예를 들면 loveletter-for-you.txt.vbs와 같이)을 지닌 첨부파일을 가지고 사용자에게 접근한다.

여기서 알아둘 것은 일반 e-메일 창에서 볼 때는 제목 부분에서 vbs는 숨겨지기 때문에 일반 텍스트 파일인 것으로 착각할 수 있다는 점이다. 오리지날 러브 바이러스가 담긴 메일의 제목은 보통 ILOVEYOU이지만, 이미 성행 중인 변종들은 새로운 이름을 갖고 있다.

이를테면 "VeryFunny," "Susitikim," "Mother's Day Order Confirmation"등이 있는데, 그 중에서도 특히 세 번째 것은 오리지날 웜과 동일한 피해를 낳지만 invoice.vbs라는 다른 VBS 파일 이름을 갖는다. 5월 둘째 주가 시작된 첫 날인 8일에는 인터넷 상에서 발견된 러브 바이러스 중 반 이상이 이러한 변종들이었다.

변종들도 많아

시만텍 안티바이러스 리서치 센터는 현재 다음과 같은 러브 바이러스(VBS.LoveLetter.A) 변종들을 잡아냈다:

VBS.LoveLetter.A (LoveLetter) VBS.LoveLetter.B (Lithuanian) VBS.LoveLetter.C (VeryFunny) VBS.LoveLetter.D (BugFix) VBS.LoveLetter.E (MothersDay) VBS.LoveLetter.F (VirusWarning) VBS.LoveLetter.G (Virus ALERT!!!) VBS.LoveLetter.H (No Comments) VBS.LoveLetter.I (Important! Read carefully!!)

5월 5일자, PDT 기준 오후1시30분(GMT 기준 9:30)에 안티바이러스 정보를 갱신한 시만텍의 고객이라면 위의 열거된 모든 변종들을 예방할 수 있다. 위의 변종 중 VBS.LoveLetter.G(Virus ALERT!!!)는 마치 시만텍 기술 지원팀이 보낸 메시지인 양 Virus ALERT!!!이란 제목을 당당하니 내걸고 있는데, 이 변종은 확장자가 bat, com인 파일을 몽땅 지워버리는 악독한 놈이다. 주의할 것은 Virus ALERT!!!이란 제목의 메일은 시만텍이 보낸 것이 아니므로 즉시 삭제하기 바란다.

5월 5일자로 유즈넷 comp.security.announce 뉴스그룹(www.cert.org/)에 올라온 CERT 어드바이저리(해킹가능한 여

러 버그나 루틴들에 대한 해결책과 문제점을 다분히 갖고 있는 OS들에 대한 주석을 단 보고서) CA-2000-04에 수록된 내용 중 일부분을 눈여겨 보자. 당신은 여러가지 방법에 의해 러브 레터 웜에 감염될 수 있는데, 여기에는 전자 메일, 윈도우 파일 공유, IRC, 유즈넷 뉴스, 웹 페이지가 있다.

하지만 유즈넷 뉴스 기사가 바이러스를 전송한다는 점에 대해서는 아직 불확실하다. 이 외에도 HTML 기반의 e-메일 클라이언트를 통한 배포도 가능하지만, 유도라와 같이 HTML로 포맷된 메시지를 실행하는 스크립트를 거부하는 프로그램에서는 불가능하다.

한편 러브 바이러스와 그 변종들은 시스템 가동시 활동할 목적으로 윈도우 레지스트리에 레지스트리 키를 추가하며, 윈도우 시스템 파일도 수정한다. 모든 레지스트리 키 목록과 내용을 보고싶은 독자는 시만텍의 노턴 안티바이러스 웹 페이지를 방문하기 바란다.

러브 바이러스의 활동은 보통 파일을 덮어쓰는 것으로부터 시작하는데, 아래에 열거된 확장자에 해당되는 파일들은 새로운 확장자인 VBS를 가진 파일로 바뀌게 된다. 따라서 susan.jpg는 이제 더 이상 수잔의 사진이 아니라 웜이 되어버린 것이며, 그 웜의 파일 이름은 susan.jpg.vbs이다. 종종 감염된 jpg 파일이 제대로 이미지를 보여주기도 하지만, 웜 코드에 의해 감염된 JPG 파일은 이미지를 보여줄 때 깨지거나 이상하게 나오는 경우가 많다.

다음과 같은 확장자가 감염된다.

.JPG, .JPEG, .MP3, .MP2, .VBS, .VBE, .HTA, .SCT, .WSH, .JS, .JSE, .CSS.

그 후 웜은 자기 자신을 포함하는 확장자가 HTM인 파일(LOVE-LETTER-FOR-YOU.HTM)을 생성하여 메일 클라이언트를 통해 전송한다. 공격 대상은 앞서 언급했듯이 아웃룩의 주소록에 담긴 모든 주소이다.

비밀번호 해킹까지

한가지 알아둘 점은 주소록이 익스플로러와 윈도우 인터넷 메일 클라이언트를 통해 공유할 수 있으며, 이는 시작 메뉴나 파일 탐색기, 또는 엑셀이나 워드와 같은 프로그램에 의해 액세스가 가능하다는 사실이다. 웜은 이 같은 주소록의 주소를 이용하여 오리지날 메시지와 확장자가 .txt.vbs인 첨부파일을 함께 보낸다. 어쩌면 이렇게 보내어진 파일은 제목만 보고 스팸메일을 가장한 메일이 아닌가 생각할 수도 있다. 자, 이제 웜의 활약은 모두 끝난 것인가?

천만에, 아직 할 일이 남았다. 러브 바이러스는 익스플로러를 이용하여 WIN-BUGSFIX.EXE가 있는 사이트(지금까지 알려진 것은 4개 정도)로 접속을 시도하여 그 프로그램을 다운받는다. 그후 이것을 실행하여 패스워드를 훔치는 트로이 목마를 설치한다.

이 트로이 목마는 사용자 레지스트리에 저장된 패스워드(프로그램 이용을 위한 패스워드)와 익스플로러에 쿠키로 저장된 패스워드(웹사이트 이용을 위한 패스워드)를 메일을 통해 필리핀(정확히 말해서 Supernet)으로 보낸다. 러브 웜이 최초 활동한 24시간 동안 가장 많은 방문을 기록한 곳이 대부분 대기업과 공공 기관 사이트이므로, 관련 사용자는 자신의 패스워드를 바꿀 필요성이 있다. 마지막으로 트로이 목마는 레지스트리에 설치되어 자동으로 시스템을 재가동 시킨다. 사용자는 우선 감염된 파일을 즉시 삭제하여 바이러스의 확산을 막아야 한다. 만약 감염된 파일 중 단 하나라도 하드에 남을 경우, 그 파일을 처음 열었을 때 웜은 다시 처음부터 활동을 개시할 것이고, 그 후 사용자가 시스템을 켤 때마다 움직일 것이다. 대다수 백신 프로그램은 사용자의 하드에 존재하는 감염파일만을 감지해 낼 수 있다. 즉 이러한 프로그램은 물이 엎질러진 다음에야 그것을 처리한다는 뜻이다.

예방책은 별로 없어

백신을 완전히 신뢰할 수 없기 때문에 당신이 할 수 있는 예방책은 다음과 같다:

1 WSH(Windows Scripting Host)가 설치되어 있다면 그것을 삭제하라(제어판의 프로그램 추가삭제에서 삭제할 수 있음). 삭제하는 이유는 웜이 VBS로 작성되었으며, 결국 실행을 위해서는 WSH를 필요로 하기 때문이다. 사용자는 이와 같이 WSH를 사용하지 않음으로써 러브 웜과 그 변종들을 예방할 수 있다.

윈도우 95에서 WSH를 disable시키는 방법은 윈도우 폴더에 들어있는 2개의 파일 이름을 바꾸면 된다.

windows/system/wscript.exe
windows/system/command/cscript.exe

이를테면 나중에 잊어먹지 않게끔 "cscript.bak"으로 바꾸는 것이 좋겠다.

한가지 주의할 점은 WSH가 있어야만 제 기능을 다하는 프로그램이 존재한다는 것이다. 물론 오피스 97/2000의 경우도 매크로와 템플릿을 위해 VBS를 사용하지만, 프로그램 자체내에 풍부한 스크립트를 가지고 있기 때문에 굳이 위험을 감수하면서 WSH를 사용할 필요는 없을 것이다. 하지만 알다시피 워드나 엑셀은 자신들을 괴롭히는 매크로 바이러스의 위험성을 항시 내포하고 있다.

2 익스플로러의 액티브 스크립트 기능을 끄기 바란다. 이 조치로 인해 사용자가 바라는 일부 기능이 작동되지 않을 수 있다. 또한 익스플로러가 제공하는 여러가지 보안 수준을 확인하고 높음(high)으로 올리기 바란다.

3 IRC 클라이언트에서는 Auto-DCC Reception을 끄기 바란다. IRC 프로그램의 사용자들은 DCC를 통해 자신들에게 제공되는 파일에 대한 자동 리셉션 기능을 끔으로써 안전해질 수 있다.

다시 한번 강조하건대 가급적이면 ICQ나 기타 채팅 전문 프로그램의 자동 파일 리셉션 기능을 사용하지 않기 바란다. 최근 패스워드를 훔치는 트로이 목마의 유포가 ICQ를 통해 이루어졌다. 그리고 확고한 예방 차원에서 채팅 프로그램의 보안과 리셉션 설정을 확인하기 바란다.

만약 susan.jpg.exe(주의할 점은 jpg와 exe사이에 무려 100칸의 공백이 존재한다는 사실이다)란 이름의 파일을 ICQ를 통해 받았다면, 보기에는 jpg이지만 실상은 실행 프로그램을 받은 것이다. 알다시피 윈도우는 최대 255문자로 이루어진 파일 이름을 지원하는데, 이 웜은 무려 100칸의 공백이 존재하니 아무리 큰 해상도라 하더라도 알아볼 수가 없다.

이 세가지 정보 외에도 다른 여러가지 정보들이 이용 가능하다. 현재CERT는 SendMail, PostFix, Procmail과 관련한 예방책을 소개하고 있으며, 바이러스, 웜, 스푸핑(spoofing), 악성 웹 스크립트, 메일폭탄에 관한 기술적 팁도 제공한다(www.cert.org/tech_tips/for details).

또한 몇몇 기업과 사용자들은 러브 바이러스에 의한 피해를 일부 고칠 수 있는 스크립트와 조언을 제공한다. The Pope(www.thepope.org/index.pl?node_id=140)를 참조하기 바란다.

이들은 웜이 어질러 놓은 코드 라인을 제거하기 위한 레지스터리 편집 팁과 더불어 감염된 파일, 시스템 파일에 추가된 명령 라인이 어떤 것인지를 자세히 제공하고 있으며, 감염된 파일(vbs를 포함하여)을 삭제하는 것이 가장 좋은 방법이라는 점도 잊지않고 알려준다.

최신 백신으로 갱신해야

Dr.솔 로 몬 (www.drsolomons.com)과 Network Associates(NAI와 맥아피의 홈페이지: www.nai.com & www.mcafeeb2b.com/asp_set/anti_virus/alerts/intro.asp)는 바이러스 정보와 갱신 서비스를 제공한다.

한 가지 이상한 점은 5월 4일부로 NAI와 Dr Solomon은 합병되었는데도 불구하고 둘은 여전히 약간 다른 정보를 제공한다는 점이다.

기타 참조할 사이트는 www.f-secure.com/v-descs/love.htm, www.symantecstore.com, www.digitalriver.com/symantec 등이 있다.

마이크로소프트도 러브 바이러스에 대한 정보 페이지를 게시하였는데, 이들의 업데이트 버전은 보다 강력한 메시지를 담은 경고창과 더불어 수신함의 메일창에서 직접 첨부파일을 실행하는 것을

막아주는 기능을 제공한다. 현재 오피스 2000이 아웃룩의 업데이트 버전을 담고 있다.

하지만 이 같은 보강된 기능에도 불구하고 이러한 종류의 웜과 바이러스를 완벽히 예방할 수는 없다. 중요한 예방책은 다음과 같은 말로 요약된다. "이방인이 준 사탕을 건네 받지 말라." 즉, 요청하지 않은 첨부파일, 제목이 낯설은 첨부파일은 열어보지 않고 삭제하는 것이 상책이다.

달리 말하자면 첨부파일의 출처나 진짜 내용을 확인하지 않고 아무런 생각없이 파일이나 이미지를 열지 말라는 이야기다. 한가지 웃지 못할 사실은 웜 바이러스에 감염된 컴퓨터를 갖고 있는 당신의 친구가 자신이 감염된 사실도 모른채 바이러스를 당신에게 보낼 수도 있다는 것이다.

당신이 받은 메일의 출처를 확실히 알고 있는가? 예상하지 않은 첨부파일을 수신했을 경우, 그것이 친구가 보냈을 것 같은 예쁜 카드라 할지언정 정확한 출처를 모른다면 절대 열어보지 말라. 그리고 필요한 조치는 오직 삭제 내지는 백신 검사이다.

잘 아는 친구로부터 러브 바이러스를 받았을 경우, 그것을 열어본 당사자는 또 다시 그 바이러스를 자신의 친구들에게 몽땅 보내게 되고, 마찬가지로 그 친구도 같은 행동을 반복함으로서 삽시간 안에 자신이 아

는 모든 지인들이 감염되는 결과를 낳게 된다.

이러한 바이러스의 여파로 물밀듯이 몰려오는 메일 트래픽을 감당할 수 없으므로 메일 서버들은 오프라인 상태로 갈 수밖에 없다. 대표적인 예로서 런던 국회 의사당에 위치한 메일 서버의 트래픽 처리 속도가 굉장히 느려지고 급기야는 마비 상태에 이르자 네트워크 담당자가 메일 서버를 오프라인 상태로 전환시킨 사건이 있었다.

출처 불분명한 메일은 '수신거부'

여기에서는 앞서 전술했던 예방책 이외의 유용한 팁들을 모아보았다.

❶ 만약 컨버젼 플러스와 같은 파일 컨버전 프로그램을 가지고 있다면 모든 첨부파일의 진짜 이름을 밝혀낼 수 있다. 이를테면 아웃룩에서 보여지는 이름이 susan.jpg일 경우, 파일 컨버전 프로그램을 이용하면 susan.jpg.vbs라는 이름으로 보일 것이다. 이는 매우 훌륭한 예방책 중 하나이며 실행을 위해서는 단지 윈도우 파일 탐색기에서 마우스의 오른쪽 클릭을 이용하면 된다.

이 같은 기능을 제공하는 프로그램은 주위에 찾아보면 많다. 하지만 당신이 가지고 있는 컨버전 프로그램이 처음부터 확장자를 보여주지는 않는다. 이 프로그램은 파일 자체에 내장된 실제 코드 헤더를 조사한 다음에 정확한 내용을 밝혀낼 수 있게 된다.

❷ 적어도 한 달에 한 번씩은 백신 프로그램을 업데이트하라. 대부분의 백신 업체에서는 1주일 간격으로 업데이트 서비스를 제공하기 때문에, 업데이트 정보가 새로이 올라오는 즉시 다운받아서 설치하기 바란다. 노턴과 같은 업체는 업데이트 소식을 메일을 통해 직접 고객에게 통지하며, 또한 안티바이러스 프로그램이 제공하는 리마인더(reminder)를 통해서도 업데이트가 필요함을 사용자에게 알려준다.

이 외에도 대부분의 백신 업체들은 무료로 이용할 수 있는 메일링 리스트를 지원하므로, 꼭 가입하기 바란다. 이러한 메일링 리스트는 신종 바이러스, 웜, 트로이 목마가 발견되었을 경우, 그 정보와 업데이트 소식을 즉시 알려주기 때문에 일반적인 매체인 라디오나 TV보다 훨씬 더 빠른 반응성을 보여주고 있다.

❸ 잠재적인 위험성을 안고 있는 메일과 브라우저의 기능들을 끄기 바란다. 아웃룩, 아웃룩 익스프레스, 익스플로러 메일, 넷스케이프 메일를 사용하고 있을 경우, 당신이 HTML

로 작성된 메일 메시지를 열어볼 때마다 이 프로그램들은 잠재적인 위험을 안고 있는 이미지와 스크립트를 보여줄 가능성이 있다.

유도라의 경우 그러한 기능을 끌 수 있는 옵션과 함께 첨부파일의 이름이 JPG일 경우 안전을 위해 자동으로 보여주는 것이 아니라 따로 남겨두는 기능을 제공한다. 패스워드를 훔치는 트로이 목마의 경우 이미지를 가장하여 유포되는 경우가 비일비재하다. 이외에도 유도라는 잠재적 위험성을 안고 있는 스크립트를 손쉽게 효과적으로 예방할 수 있는 기능을 제공하며, 무엇보다 무료로 이용할 수 있기 때문에 적극 추천하는 바이다(eudora-survey.qualcomm.com/live/download).

유도라의 데이비드 로스, 허미 제임스, 제프 버클리는 메일 중에서 HTML로 짜여진 내용을 포함하고 있는 메시지에 숨어있는 웜과 바이러스를 막기위한 팁을 소개하고 있다:

'이미지'로 가장해 전달

유도라를 사용하고 있다면 HTML로 작성된 메시지를 보여주는 기능(Microsoft's viewer)을 끄기 바란다. 유도라 설정(Tools/Options/Viewing Mail)으로 들어가서 use Microsoft's viewer 를 끄면 된다. 텍스트 포맷팅과 같은 간단한 HTML은 이용이 가능하지만, 잠재적인 위험성을 내포하고 있는 HTML의 경우(이것은 Microsoft's viewer로 볼 수 있음)에는 이용이 불가능하다.

유도라의 'Allow Executables in HTML content'를 끄기 바란다. 이 기능(Tools/Options/Viewing Mail)은 디폴트로 꺼져있지만, 돌다리도 두드려보는 심정으로 다시 한번 확인해보기 바란다. HTML에 내장된 잠재적 위험성을 내포하고 있는 모든 스크립트는 모두 무시될 것이다. 여기에는 VBS, 자바, 자바스크립트 등이 포함된다.

만약 당신이 익스플로러 메일이나 넷스케이프의 그것을 사용한다면 Grr!과 같은 프로그램을 이용할 필요성이 있다. 그 이유는 익스플로러와 넷스케이프는 너무도 충직하게 화려한 HTML을 내장된 스크립트와 함께 몽땅 보여주기 때문이다. 두 프로그램의 충실한 실행성을 막을 수 있는 방법은 없다.

4 당신의 시스템과 시스템 파일을 감시할 수 있는 유익한 프로그램을 사용하라. 이런 의미에서 Grr!을 적극 추천하는 바이다. 이 프로그램은 레지스터리, INI 파일을 포함한 시스템 파일(당신이 미처 생각치도 못한 파일들이 수두룩함)을 모두 감시한다. 만약 특정 시스템 파일이 이상하다고 판단될 경우, Grr!은 그 파일이 하드에 쓰여지는 것을 막을 수가 있다(www.greyware.com).

한편 펠리칸 시큐리티는 기업 서버용 보안 제품인 펠리칸 세이프티넷을 이달중 출시할 예정이다.이 제품은 가장 뛰어난 샌드박스(sandbox) 보안 제품이 될 것으로 예상된다. 또한 보안에 관한 훌륭한 화이트 페이퍼가 이들의 사이트(www.pelicansecurity.com/pages/PelicanWP.pdf)에서 이용 가능하다.

결론적으로 HTML 기반의 메일과 첨부파일은 취약성을 지니고 있다. 만일 누군가가 러브 바이러스와 같은 VBS 스크립트를 작성하여 HTML에 포함시킨 다음 그것을 메일로 유포시키면 어떻게 될까? 기술적인 견지에서 이러한 일은 바이러스가 mIRC와 웹 페이지를 사용하여 IRC 채널로 자신을 복제 전송함으로써 가능하며, 벌써 여기저기서 행해지고 있는 방법이다.

우리는 메일을 통해 확산되는 HTML 웜/바이러스의 새로운 변종들이 설치치 않을 가능성보다 그 반대의 가능성이 훨씬 높은 무서운(?) 시대에 살고 있다. 자기 자신을 보호할 사람은 자기 자신밖에 없다. 메일에서 이루어지는 불필요한 HTML 표시에 대해서는 되도록 거부하라. 괜찮겠지 하다가는 당신의 파일과 패스워드와, 최악의 경우 하드까지 통째로 잃어버리는 파국을 맞게 될지도 모르니까...

개인 사용자라면 Grr을 사용하라! 기업 사용자인가? 그렇다면 펠리칸의 세이프티넷을 사용하라. 그 외에도 당신의 시스템 파일을 지켜줄 수 있는 새로운 'sandboxing' 제품이 있다면 주저하지 말고 사용하라. 중요한 것은 예방이다. 엎질러진 물을 모두 담기에는 지금의 기술력으로는 역부족이다. 끝으로 몸조심이 아닌 바이러스 조심을 하기 바란다.