# ASEC Annual Report 2003

Ⓡ ASEC Report 2003. 12

안철수연구소의

시큐리티대응센터(AhnLab Security E-response Center)는

악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여

바이러스와 보안 전문가들로 구성되어 있는 조직이다.

이 ASEC Annual Report는 (주)안철수연구소의 ASEC에서

국내 인터넷 보안과 고객에게 보다 다양한 정보를 제공하기 위하여

2003년 한해동안의 바이러스와 시큐리티에 대한

종합된 정보를 요약, 분석한 리포트이다.

AhnLab

AhnLab

# 목 차

# I 2003년 악성코드 피해 동향

작성자 : 정진성 연구원(jsjung@ahnlab.com)

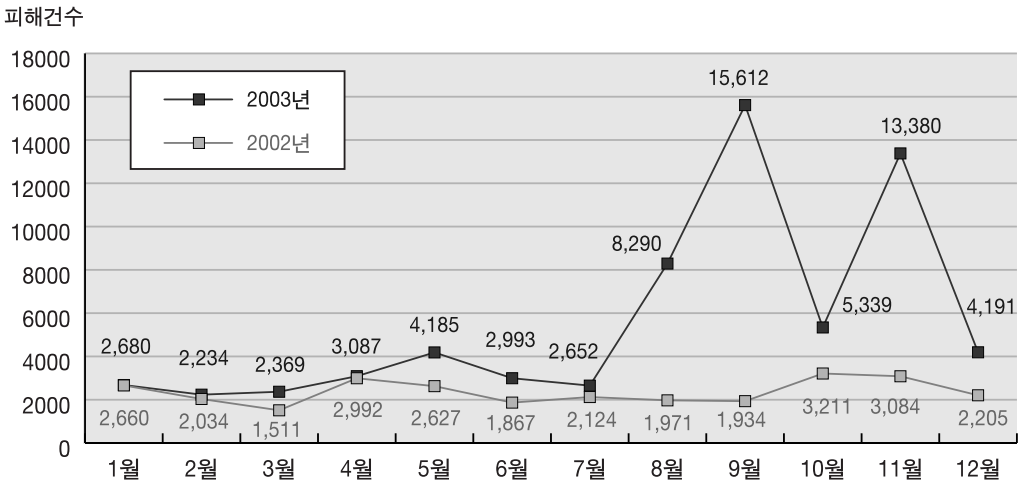
## 1. 2003년 바이러스 피해 통계

2003년은 어느 해 보다도 악성코드에 관한 많은 사회적인 이슈가 있었던 한해이다. 1월에 있었던 인터넷 대란의 주범인 SQL_Overflow 웜(일명 슬래머웜)를 시작으로 8월에 있던 블래스터(Win32/Blaster.worm.6176) 웜, 소빅 F(Win32/Sobig.worm.F) 웜 등이 그 원인이다. 특히 2002년 악성코드 피해발생 수치와 비교하여 올해의 그 수치는 월등히 높다. 그 수치는 [표1]과 같다.

| 구분 | 1월 | 2월 | 3월 | 4월 | 5월 | 6월 | 7월 | 8월 | 9월 | 10월 | 11월 | 12월 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2002년 | 2660 | 2034 | 1511 | 2992 | 2627 | 1867 | 2124 | 1971 | 1934 | 3211 | 3084 | 2205 | 28220 |
| 2003년 | 2680 | 2234 | 2369 | 3087 | 4185 | 2993 | 2652 | 8290 | 15612 | 5339 | 13380 | 4191 | 67012 |

[표1]2002, 2003년 국내 악성코드 피해 신고 통계 수치(2003년은 12월 10일까지 데이터)

[표1]에서와 같이 2003년 총 피해신고 건수는 67,012 건으로 전년대비 142%나 증가한 것을 볼 수 있다. 이를 [그래프1]로 나타내보면 올해는 특정 월에 비약적으로 증가한 것을 볼 수 있다.




[그래프1]2002, 2003년 월 단위 피해건수비교

이렇게 특정 월에 급증한 것은 그만큼 해당 월에 피해가 심했던 악성코드가 많았기 때문이다. 대표적으로 1월에 SQL_Overflow, 5월에 러브게이트 변형(Win32/LovGate.worm.107008), 8월에 블래스터(Win32/Blaster.worm.6176) 웜, 소빅 F(Win32/Sobig.worm.F) 웜, 두마루(Win32/Dumaru.worm.9234) 웜, 미메일(Win32/Mimail.worm) 웜 그리고 구종의 악성코드들도 포함하여 이름만 들어도 익히 알만한 악성코드들이 많은 피해를 주었다.

## 2. 악성코드 피해 Top 20

2002년과 올 한해 피해를 많이 주었던 악성코드는 어떤 것이 있었는지 Top 20을 뽑아보면 [표2], [표3]과 같다.

| 악성코드명 | 건수 |
|---|---|
| Win32/Klez.worm.H | 4,650 |
| Win32/Nimda | 4,400 |
| Win32/FunLove.4099 | 3,637 |
| Win32/Opasoft.worm.28672 | 994 |
| Win95/Spaces.1445 | 850 |
| Win32/Elkern.B | 838 |
| Win32/Nimda.B | 719 |
| Win32/Winevar.worm | 584 |
| Win32/Weird | 509 |
| Win95/CIH | 493 |
| Win32/Yaha.worm.27648 | 471 |
| I-Worm/Wininit | 417 |
| Win32/Nimda.eml.79225 | 402 |
| Win32/Parite.B | 388 |
| Win32/Opasoft.worm.24064 | 370 |
| Win32/Datom.worm.54784 | 330 |
| Win32/Nimda.B.eml.79232 | 328 |
| Win32/Gop.worm.60313 | 288 |
| Win32/Sircam.worm | 285 |
| Win32/Opasoft.worm.28672.B | 260 |

[표2]2002년 악성코드 피해문의건수 Top20

| 악성코드명 | 건수 |
|---|---|
| Win32/Sobig.worm.F | 14,949 |
| Win32/Dumaru.worm.9234 | 14,741 |
| Win32/Blaster.worm.6176 | 4,901 |
| Win32/Yaha.worm.45568.B | 4,732 |
| Win32/LovGate.worm.107008 | 1,571 |
| Win32/Parite | 1,174 |
| Win32/Parite.B | 1,000 |
| Win32/FunLove.4099 | 899 |
| Win32/Welchia.worm.10240 | 819 |
| Win32/Valla.2048 | 803 |
| JS/Fortnight | 728 |
| Win95/Spaces.1445 | 725 |
| Win32/Klez.worm.H | 682 |
| MIRC/Stde9 | 608 |
| Win32/Yaha.worm.27648 | 544 |
| HTML/Redlof | 538 |
| Win32/Nimda | 499 |
| Win32/Opasoft.worm.28672 | 489 |
| Win32/Elkern.B | 443 |
| Win32/Yaha.worm.45568 | 436 |

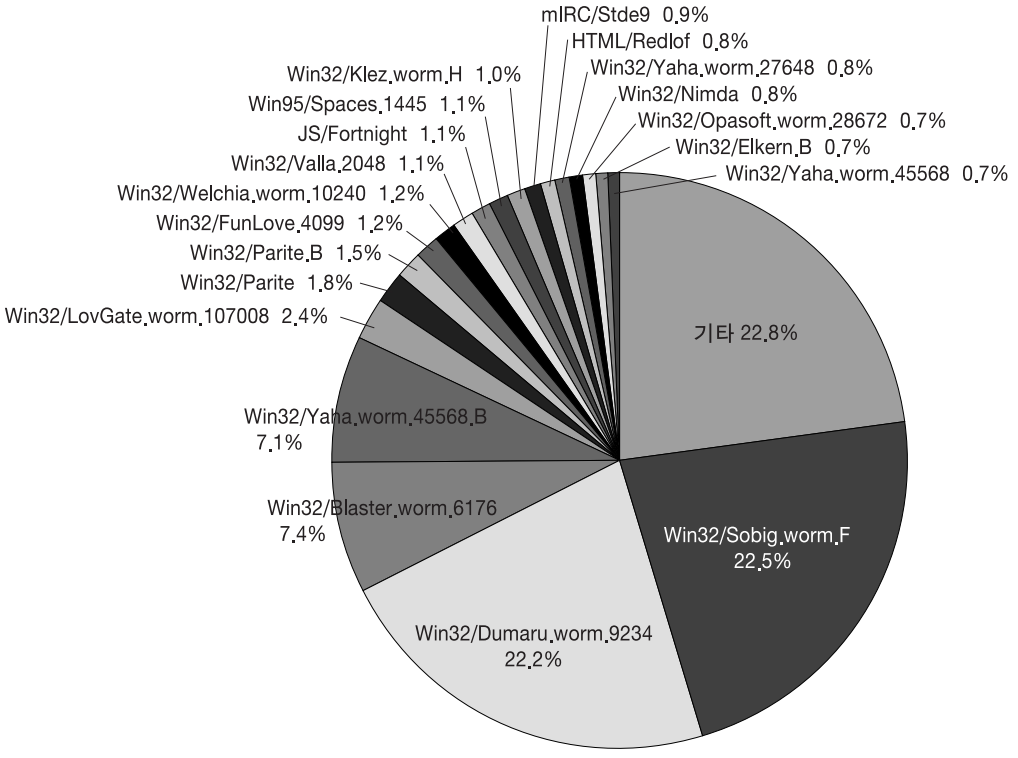
[표3] 2003년 악성코드 피해문의건수 Top 20
* 2003년 자료는 2003년 12월 10일까지의 자료임

[표1]의 전체피해문의 건수 차이도 차이가 나지만 특히 올해는 상위 특정 악성코드들에 집중적으로 많은 피해문의가 접수된 것을 볼 수 있다. 이러한 수치는 안철수연구소가 악성코드에 대한 통계를 시작한 이래 기록적인 수치이다.

[표3] 피해신고 기준으로 선정한 악성코드 Top 5를 순서대로 간략히 정리해보면 다음과 같다.

- Win32/Sobig.worm.F
- Win32/Dumaru.worm.9234
- Win32/Blaster.worm.6176
- Win32/Yaha.worm.45568.B
- Win32/LovGate.worm.107008

1, 2위의 비중이 전체 신고의 44%에 달해 피해의 파급력이 소수의 악성코드에 집중됐으며 이들 모두 2003년에 발견된 것이며, 그중에서도 3개가 8월에 발견된 악성코드이다.
피해신고의 월별 상황을 보면 전체적으로 전년 대비 증가한 것은 공통적이나, 블래스터 웜, 소빅 F 웜, 웰치아 웜 등 전파속도가 빠른 악성코드가 잇달아 등장한 8월부터는 급격히 증가했다. [표3]의 올해의 악성코드 Top 20 자료를 비율로 확인해 보면 [그래프2]와 같다.



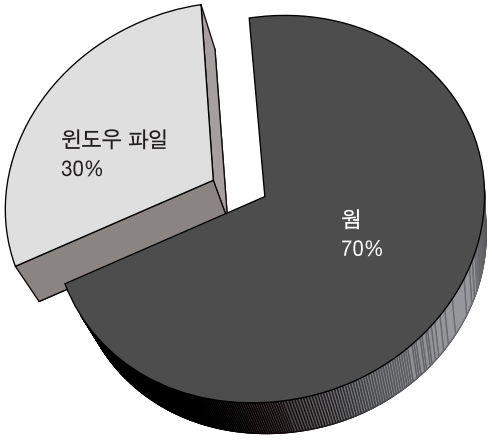

[그래프2] 2003년 악성코드 피해문의건수 Top 20

[그래프2]를 보면 상위에 속해 있는 악성코드들은 모두 웜으로서 메일과 네트워크로 전파되는 방법을 가진 웜들이다. 특히 상위 5개 악성코드중  4개는 웜(Mass Mailer)으로서 기본적으로 메일로 자동 발송될 뿐 아니라 아웃룩 주소록은 물론 다양한 파일에서 주소를 추출해 웜 메일을 발송하기 때문에, 동시에 다수의 사용자에게 웜 메일이 발송되고 발송자를 속이기도 하여 피해의 규모와 오해의 소지도 컸다.

블래스터 웜은 취약점을 이용하여 감염되는 형태로서 올해들어 SQL_Overflow에 이어 두번째로 치명적인 보안 취약점을 이용하였고 그 대상이 윈도우 NT 계열의 개인 사용자들이어서 체감 피해가 다소 컸다.

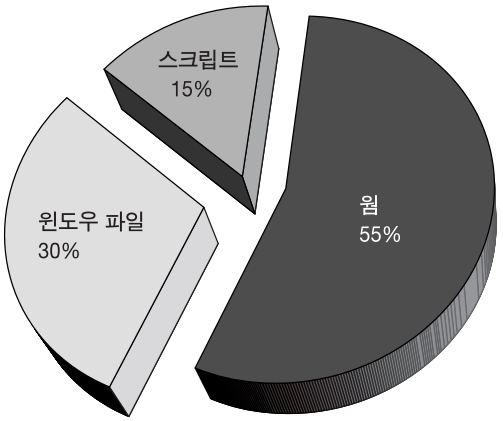
## ■ 2002년, 2003년 악성코드 Top 20 유형별 현황

2002년, 2003년 악성코드 Top 20 의 유형별 분류를 살펴보면 [그래프3],[그래프4]와 같다.




[그래프3] 2002년 Top 20 악성코드 유형별 현황

2002년도는 웜과 윈도우 파일 바이러스 두 유형의 악성코드로 나누어졌다. 순위에 포함된 악성코드들은 모두 Win32 환경에서 동작되었으며 특히 많은 비중을 차지하는 웜의 경우 전통적인 형태의 Mass Mailer 뿐만 아니라 윈도우 9x 환경의 NetBIOS 를 이용하여 공유폴더로 전파되는 웜들이 많았다. 대표적으로 클레즈H(Win32/Klez.worm.H) 웜 와 2001년에 처음보고된 님다(Win32/Nimda), 그리고 윈도우 9x 환경에서 공유폴더로 전파되는 오파소프트(Win32/Opasoft.worm) 웜을 들 수 있다.




[그래프4]2003년 Top 20 악성코드 유형별 현황

2003년도 역시 웜에 의한 피해가 많았으나 스크립트 형태의 악성코드들인 포트나이트(JS/Fortnight)와 레드롤프(HTML/Redlof)의 문의도 많았다. 포트나이트의 경우는 성인 사이트 광고에 이용되면서 피해문의가 급증하였고 레드롤프는 잘 알려진 스크립트 파일 확장자등에 모두 감염되는 증상이 있다. 또한 감염시 탐색기를 이용하여 폴더보기를 구성하는 특정한 파일을 손상시키면서 역시 피해 문의가 많았다.

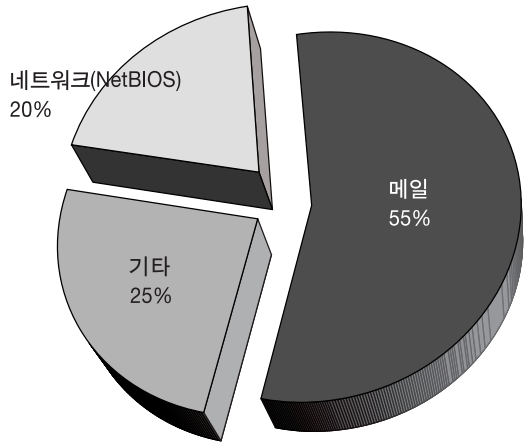
## ■ 2002년, 2003년 악성코드 Top 20 의 전파방법별 현황

2003년에 들어서 웜은 전통적인 메일전파 방법 이외에 취약점을 이용한 전파나, 사용자의 윈도우 관리소홀로 발생할 수 있는 관리목적공유폴더를 이용한 전파방법을 사용하였다. 이는 악성코드들이 기존에 사용자의 실행을 필요로 하는 수동적인 감염형태에서 능동적인 감염형태로 발전하는 양상을 보인 것 이다.

2002년과 2003년도의 악성코드 Top 20 을 비교하여 어떠한 전파방법을 많이 이용하였는지 파악하여 분류한 결과는 [그래프5], [그래프6]과 같다. 그 기준은 해당 악성코드가 하나 이상의 전파방법을 가지고 있다면 가장 많이 사용되고 피해가 많았던 것을 기준으로 하였다.

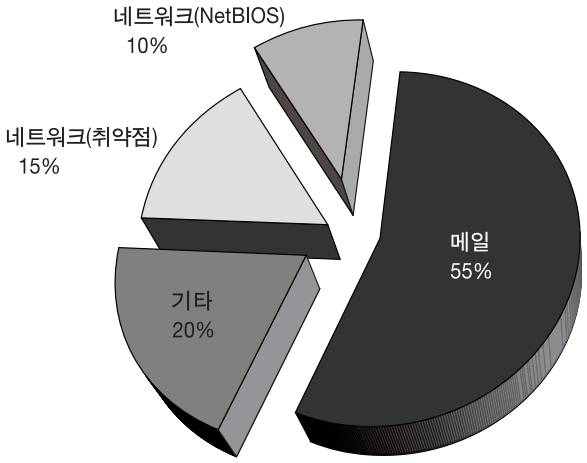
- 메일
- 네트워크(취약점)
- 네트워크(NetBIOS)
- 기타

위 항목중 네트워크를 취약점과 NetBIOS로 분류한 것은 2003년에 들어서부터 취약점 (윈도우 관리목적공유폴더 포함)을 이용하여 전파되는 악성코드들이 많았기 때문이다. 기타로 분류한 것은 대부분 윈도우 파일 바이러스들로서 직접 실행 되어야만 감염활동을 하는 것이고 다른 분류에 비하여 건수가 작아 기타로 분류하였다.




[그래프5]2002년도 악성코드 Top 20 의 전파방법

[그래프5]에서도 알 수 있듯이 2002년도에는 메일을 이용한 전파방법이 월등이 많았으며 큰 위험을 가진 취약점을 이용한 전파방법을 사용하는 악성코드가 순위에 포함되지는 못했다. 또한 기타로 분류된‘ 직접실행 ’되어 감염활동을 하는 윈도우 파일 바이러스 경우는 모두 구종으로, 이중 엘컨B(Win32/Elkren.B), 패리테B(Win32/Parite.B) 등 처럼 네트워크의 읽기/쓰기가 가능한 공유폴더를 대상으로 파일을 감염 시키는 것도 있었다. 또한 약간씩이나마 웜 등에 중복감염 되어져 발견되는 경우가 더러 있었는데 이러한 현상은 2003년도에 더욱 두드러지게 나타났다.



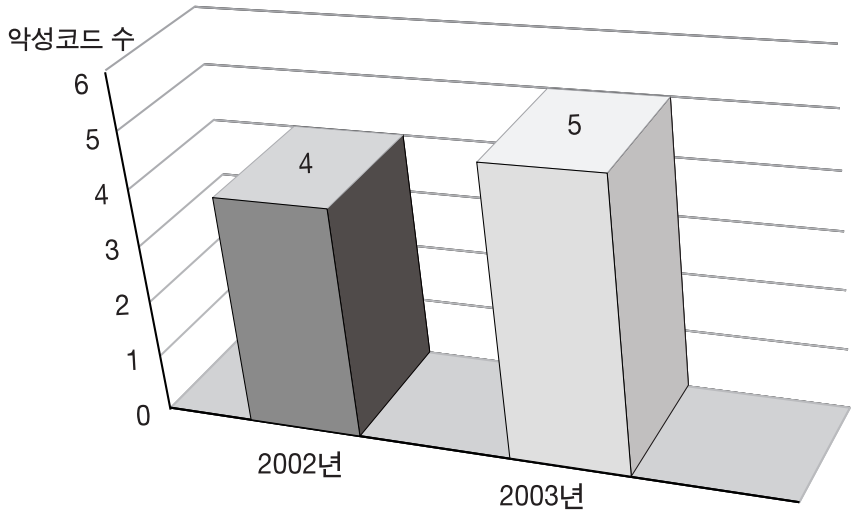

[그래프6]2003년 악성코드 Top 20 전파방법

수적으로는 메일로 전파되는 방법이 더 많았지만 2003년부터 두드러지게 나타나는 것이 바로 취약점과 사용자의 관리소홀의 문제로 전파되는 유형이 증가한 현상이다. 올 8월 RPC DCOM 관련 취약점을 이용한 블래스터 웜을 시작으로 이 취약점을 이용하는 악성코드는 큰

파란을 일으킨 후에도 여전히 많은 악성코드들이 사용하고 있다. 또한 사용자들의 관리소홀로 인하여 관리목적 공유폴더를 이용한 전파방법(null session)도 악성코드 제작자들이 즐겨 사용하는 전파방법이 되었다.

위에서 ' 기타 ' 전파방법으로 분류된 것은 대부분 윈도우 파일 바이러스이다. 비율이 네트워크 전파방법보다 더 많은데 의문을 가질 수 있는데 이유는 바로 위에서 언급한 것 처럼 웜등에 중복감염된 형태로 많이 퍼졌기 때문이다. 월초 문의가 많았던 Dropper/MircPack 시리즈에 Win32/Valla.2048, Win32/Parite 와 B 형 등이 감염된 채로 광범위하게 전파되었다.

악성코드들은 자신을 전파하기 위해서 메일 및 네트워크등를 이용하여 전파된다. 현재는 취약점을 이용하여 네트워크의 특정한 TCP 포트를 이용해 능동적으로 전파 되는 방법을 사용하고 있기도 하다. 따라서 악성코드들은 하나 이상의 전파경로를 가지는 것은 이제 일반적인 것이 되어 버렸다. 2002년과 2003년의 Top 20을 비교하여 하나 이상의 전파방법을 가진 악성코드의 비율이 어떤지, 그 방법은 무엇인지 확인해보자.




[그래프7]2002년, 2003년 다수의 전파경로를 가진 악성코드 수

[그래프7]에서도 볼 수 있듯이 2002년도는 Top 20 의 20% , 2003년도는 25% 가 다수이상의 전파경로를 가진 악성코드들 이였다. 이들은 메일과 공유폴더를 이용하여 자신을 복사해나가는 방법을 이용하였다. 이것은 가장 기본적인 방법들이다. 다수 이상의 전파경로를 가지는 악성코드중 여러가지 경로를 이용하는 것들도 있는데 대부분 다음과 같다.

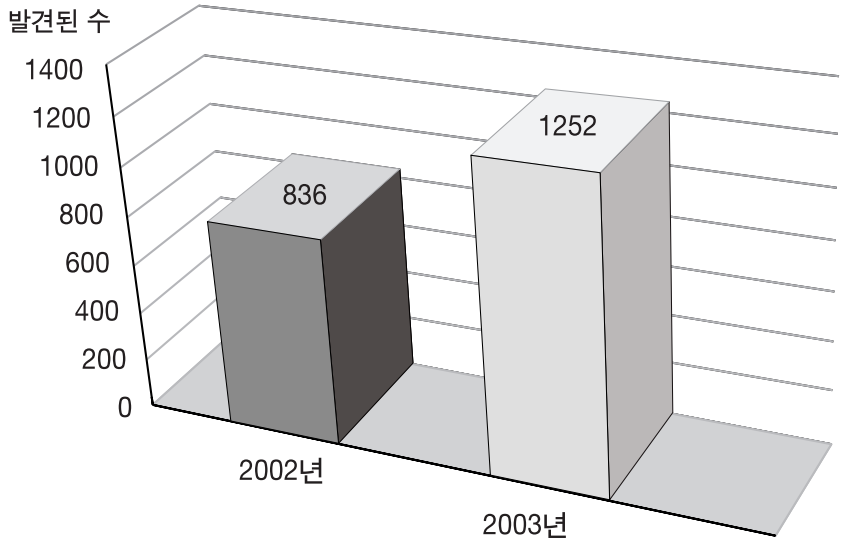
- 메일 (SMTP, MAPI 등의 두개의 프로토콜을 사용)
- 네트워크(공유폴더)
- 네트워크(취약점, 관리목적공유폴더)
- 메신저 (하나 이상의 메신저를 이용, 예를들어 MSN, Yahoo Messanger 등)
- P2P 응용 프로그램 (다양한 종류의 P2P 응용 프로그램을 이용한 전파)

간혹 어떤 악성코드는 자신을 특정한 뉴스그룹에 자동으로 포스팅하는 형태도 있었으나 그리 흔한 방법은 아니였다.

## ■ 2002년, 2003년 피해문의 접수된 악성코드의 종류

2002년도 당시의 악성코드들은 기본적으로 메일과 읽기/쓰기 가능한 공유폴더내에 자신의 복사본을 생성하는 방법으로 하나이상의 전파경로를 사용하였다. 2003년에 들어서는 공유폴더는 물론 관리목적공유폴더를 이용하여 해당 시스템의 관리자 권한을 획득하여 악성코드를 복사 및 실행도 하는 형태로 발전하였다.

그렇다면 이렇게 많은 사용자들에 피해를 주었던 악성코드들이 2002년과 2003년에 몇 종류나 발견되었는지 비교해 보도록 하자. 위에서 언급한 것 처럼 올해는 전년대비 142% 이상 피해문의가 증가하였다라는 걸 감안한다면 올해는 전년보다 많은 종류의 악성코드들에 대한 문의가 있었을 것으로 아래 그래프를 보기전에 미리 짐작해 볼 수 있겠다.




[그래프8] 2002년, 2003년 피해문의 접수된 악성코드 수

[그래프8]에서 알 수 있듯이 2003년은 피해신고된 악성코드의 수가 전년대비 66% 이상 증가하였다. 그 종류는 비단 윈도우 악성코드 뿐만 아니라 도스용 악성코드들에 대한 것도 문의가 다량 접수되었다. 물론 이중에는 상위 Top 20 정도를 제외하고는 그 피해신고 수가 적거나 또는 미미하지만, 그만큼 다양한 악성코드로부터 피해를 입은 사용자가 많다는 것을 의미하는 것이다.

# Ⅱ 2003년 신종 악성코드 발견 동향

작성자 : 정진성 연구원(jsjung@ahnlab.com)

2003년 1월 1일부터 12월 10일까지 발견된 신종 악성코드는 모두 1,133종으로, 2002년 277종에 비하여 무려 4배가 넘게 증가하였는데 [표1], [표2]와 같다.

| 월 | 리눅스 | 파일 | 트로이 | 스크립트 | 웜 | 부트 | 매크로 | 부트/파일 | 합계 |
|---|---|---|---|---|---|---|---|---|---|
| 1월 | 0 | 1 | 2 | 0 | 4 | 0 | 3 | 0 | 10 |
| 2월 | 0 | 0 | 8 | 2 | 2 | 0 | 3 | 0 | 15 |
| 3월 | 0 | 2 | 8 | 0 | 3 | 0 | 2 | 0 | 15 |
| 4월 | 0 | 4 | 6 | 0 | 1 | 0 | 4 | 0 | 15 |
| 5월 | 0 | 1 | 10 | 3 | 1 | 0 | 2 | 0 | 17 |
| 6월 | 0 | 2 | 7 | 4 | 4 | 0 | 0 | 0 | 17 |
| 7월 | 0 | 4 | 13 | 2 | 9 | 0 | 0 | 0 | 28 |
| 8월 | 0 | 0 | 1 | 2 | 1 | 0 | 1 | 0 | 5 |
| 9월 | 0 | 0 | 10 | 0 | 2 | 0 | 3 | 0 | 15 |
| 10월 | 0 | 7 | 24 | 6 | 7 | 0 | 0 | 0 | 40 |
| 11월 | 0 | 15 | 27 | 8 | 10 | 0 | 0 | 0 | 60 |
| 12월 | 0 | 5 | 21 | 5 | 5 | 0 | 0 | 0 | 36 |
| 합 | 0 | 41 | 137 | 32 | 49 | 0 | 18 | 0 | 277 |

[표1]2002년 신종 악성코드 유형별 집계표

| 월 | 리눅스 | 파일 | 트로이 | 드롭퍼 | 스크립트 | 웜 | 부트 | 매크로 | 부트/파일 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1월 | 0 | 7 | 54 | 18 | 3 | 8 | 0 | 0 | 0 | 90 |
| 2월 | 0 | 2 | 80 | 15 | 3 | 13 | 1 | 1 | 0 | 115 |
| 3월 | 2 | 3 | 76 | 24 | 1 | 12 | 0 | 0 | 0 | 118 |
| 4월 | 0 | 1 | 46 | 11 | 3 | 11 | 0 | 0 | 0 | 72 |
| 5월 | 0 | 4 | 44 | 14 | 2 | 14 | 0 | 0 | 0 | 78 |
| 6월 | 0 | 2 | 52 | 6 | 4 | 21 | 0 | 0 | 0 | 85 |
| 7월 | 0 | 3 | 59 | 4 | 1 | 10 | 0 | 0 | 0 | 77 |
| 8월 | 0 | 2 | 93 | 13 | 3 | 20 | 0 | 0 | 0 | 131 |
| 9월 | 0 | 1 | 78 | 7 | 2 | 28 | 0 | 0 | 0 | 116 |
| 10월 | 0 | 0 | 59 | 3 | 0 | 30 | 0 | 0 | 0 | 92 |
| 11월 | 0 | 0 | 50 | 1 | 2 | 58 | 0 | 0 | 0 | 111 |
| 12월 | 0 | 0 | 30 | 3 | 0 | 15 | 0 | 0 | 0 | 48 |
| 합 | 2 | 25 | 721 | 119 | 24 | 240 | 1 | 1 | 0 | 1133 |

[표2]2003년 신종 악성코드 유형별 집계표

이는 연구소가 국내에 접수되는 신종 악성코드발견 통계를 낸 이래 최대치이기도 하다([표 3]참조).

| 연 도 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 2000 | 2001 | 2002 | 2003 | 총 계 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 합 계 | 1 | 6 | 28 | 21 | 17 | 34 | 76 | 128 | 226 | 256 | 276 | 379 | 572 | 435 | 277 | 1133 | 3865 |

[표3]1998년 ~ 2003년 국내 발견 악성코드 통계(2003년 자료는 12월 10일 까지만 포함)

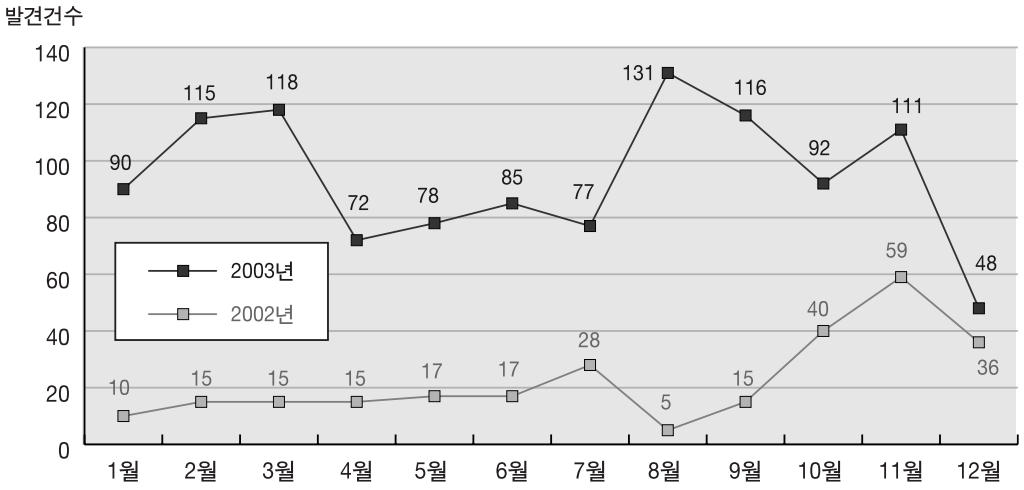
## ■ 올해 신종 악성코드의 동향은

- 해킹과 악성코드의 통합 형태 증가
- 취약점 이용한 자동 감염 기법 등장
- 관리목적 공유폴더를 이용한 감염 기법 증가
- 전통적인 바이러스의 사양세 등으로 그 특징을 요약할 수 있다.

해킹과 악성코드의 통합형태로는 최근 발견되는 대부분의 악성 IRCBot 등이 백도어 기능과 DoS (서비스 거부 공격)기능을 가지고 있었다. 또한 블래스터 웜 역시 DoS를 시도하며 두마루(Win32/Dumaru.worm.9234) 웜과 러브게이트(Win32/LovGate.worm.107008) 웜은 특정 포트가 열려 해킹을 당할 위험을 내포하고 있다. 시스템에 대한 해킹과 DoS 공격은 주로 서버들을 대상으로 이루어져 있던 일이 올해 들어서는 데스트탑용 시스템에서도 이루어져 그 양상이 변화되고 있다는 것을 알 수 있다.

이렇듯 악성코드에 의한 해킹과 DoS 공격은 공격을 받은 시스템에서 끝나는 것이 아니라 공격을 받았던 시스템도 감염되어 다시 다른 시스템을 공격하는 새로운 형태를 보였다. 즉, 피해자가 가해자가 되는 상황으로, 치료를 하지 않고 방치해 두면 자신이 피해를 입는 것은 물론 네트워크에 계속 연결된 경우 다른 시스템들을 공격하여 블특정 다수의 다른 사람까지 피해를 입히는 형태로 발전하였다.

그렇다면 위와 같은 피해를 가장 많이 일으킨 악성코드로는 어떠한 것이 있을까? 그것은 바로 올해 신종 악성코드 유형중 가장 많은 변형이 발견된 IRCBot 트로이목마이다. [표2]에서 알 수 있듯이 트로이목마가 전체 발견건수의 과반수 이상을 차지하고 있다. 과반수를 차지하는 트로이목마 중 전통적인 백도어류를 제외하고는 모두 악성 IRCBot 트로이목마들이다. 또한 가장 많은 유형이 보고된 IRCBot은 트로이목마 뿐만 아니라 웜 형태로도 많은 수가 발견되었다.



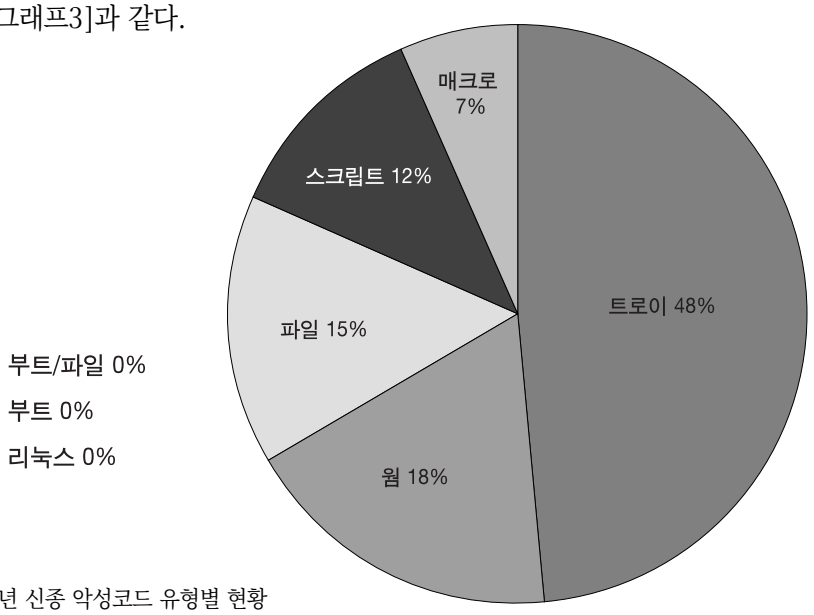

[그래프1]2002, 2003년 월별 신종 악성코드 발견건수

2002년은 워낙 적은 수의 신종 악성코드가 보고되었는데 2002년말부터 악성 IRCBot의 일종인 Win-Trojan/MircPack 등이 기승을 부리기 시작하여 그 건수가 증가하고 있는 것을 볼 수 있다.

2003년은 위에서도 언급한 것처럼 전체 피해문의와 신종 악성코드 발견건수 모두 연구소 집계 이래 최고로 많은 악성코드가 보고되었다. 가장 많은 신종 악성코드가 보고된 8월은 많은 피해를 주었던 소빅F 웜과 블래스터 웜이 발견된 달이기도 하다.

## ■ 전통적인 바이러스의 사양추세

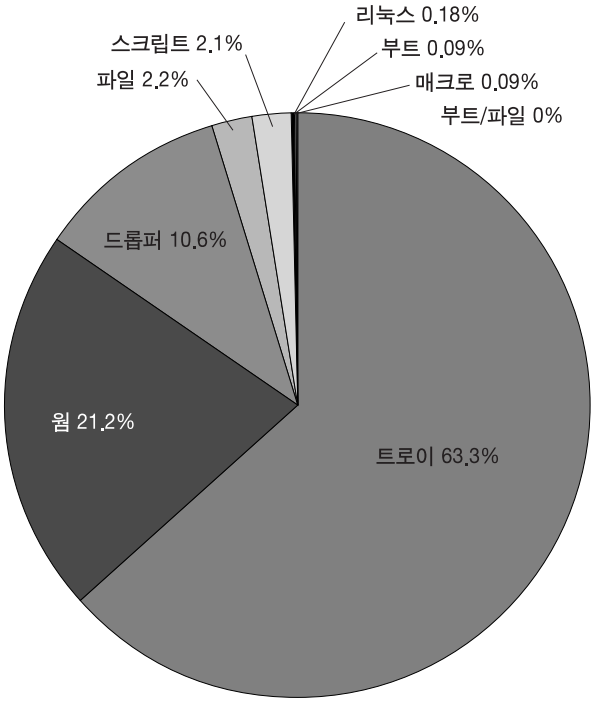
2002년과 2003년의 신종 악성코드의 유형별 현황은
[그래프2], [그래프3]과 같다.




[그래프2]2002년 신종 악성코드 유형별 현황

트로이목마가 전체 신종 악성코드의 반을 차지하고 있다. 하지만 대부분 트로이목마들은 전통적인 백도어류가 일반적이였다. 웜 역시 전통적인 Mass Mailer 일색이였다.

전통적인 바이러스의 감소추세는 2001년 말부터 2002년을 기점으로 서서히 진행되었다. 새로운 형태의 스크립트, 매크로, 윈도우 파일 바이러스 등의 발견건수는 거의 미비한데 이러한 감소추세는 2003년에 더욱 두드러진다.  [그래프3]의 2003년 현황을 보면 트로이목마는 전체 신종 악성코드에서 64%, 웜은 21%를 차지하고 있다. 하지만 전통적인 악성코드들인 윈도우 파일 바이러스, 스크립트, 매크로 바이러스는 거의 자취를 감추었다고 할 정도로 극히 미비한 숫자만이 보고되었다.



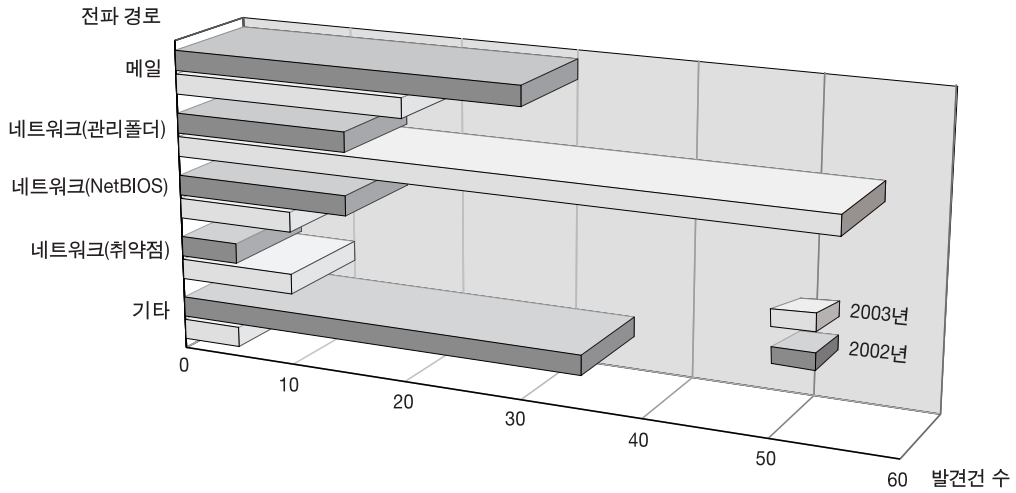

[그래프3]2003년 신종 악성코드 유형별 현황

이러한 경향을 분석해보면 윈도우 파일 바이러스 경우는 무엇보다도 윈도우 기반기술(시스템)을 잘 알고 있어야 하지만 이에 반해 웜이나 트로이목마는 무엇보다는 복잡한 윈도우 기반기술을 이해하지 않아도 손쉽게 제작이 가능한 것이  큰 이유가 되겠다. 매크로와 스크립트 바이러스는 소스가 그대로 노출되어 변형의 제작이 용이하지만 대부분의 안티 바이러스 제품군들은 이러한 변형들을 쉽게 진단할 수 있다. 따라서 이 두 악성코드들은 제작자들 사이에서 흥미가 점점 멀어지게 된 것으로 추정된다.

## ■ 신종 악성코드들의 전파방법의 변화

올해의 신종악성코드는 전년대비 무려 4배가 넘게 증가했다. 그렇다면 2003년도의 신종 악성코드들은 전년대비 어떤 전파방법을 주로 이용했는지 정리를 해보면 [그래프4]와 같다.

* 아래 그래프는 ' 발견건수를 100 '이라고 했을 때의 수치이다.




[그래프4]2002년, 2003년 신종 악성코드 전파경로 현황

전년대비 큰 폭으로 증가한 가장 큰 이유는 바로 악성코드의 전파방법의 변화이다. 정리하면 다음과 같다.

- 취약점을 이용한 자동 감염기법 등장
- 관리목적공유폴더를 이용한 감염기법 증가

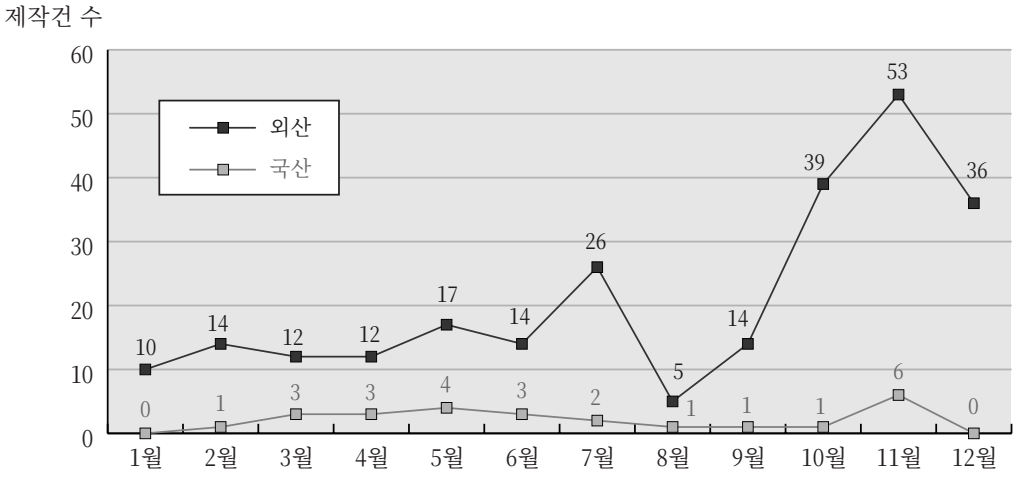
취약점을 이용한 자동 감염 기법은 악성코드가 수동적인 감염방법에서 능동적인 감염형태로 발전했다는 것이다. 예전에는 사용자가 메일에 첨부된 파일을 실행하거나 공유폴더에 복사된 파일을 실행해야 감염이 되었는데 이러한 행위를 하지 않아도 인터넷에 연결만 되어 있으면 보안 취약점을 통해 악성코드에 감염 될 수 있다. 그 대표적인 경우가 SQL_Overflow와 블래스터 웜이다.

두번째로는 관리목적 공유폴더를 이용한 감염 기법 증가이다.  윈도우 NT 계열 이상의 시스템에 기본적으로 설정된 관리목적공유폴더는 원격지에서도 관리자가 시스템에 접근하기 위한 것이었다. 그러나 사용자의 관리지식 부족으로 인하여 대부분의 사용자들이 암호 없이 윈도우에 로그인하거나 유추하기 쉬운 암호를 사용한다는 것이다. 악성코드 제작자들은 이를 이용하여 악성코드에 이를 접목해 많은 웜들이 이런 방법을 이용하여 전파되었고 계속 증가하는 추세이다. 대표적으로 Win32/AgoBot.worm, Win32/SdBot.worm 등이 있다.

또한 이러한 전파방법으로 인하여 새로운 형태의 피해현상이 많이 보고 되고 있는데 바로 ' 네트워크 트래픽 폭증 ' 이다. 일반적으로 위와 같은 웜들은 시스템 폴더나 윈도우 폴더등에 정상파일과 비슷한 파일로 위장되어져 있는 경우가 많아서 발견하기가 어렵다. 그러나 위와 같은 웜들이 자신을 전파하기 위해 네트워크를 스캔하는 과정에서 특정포트들에 대한 엄청난 트래픽을 유발하게 되는데 해당 포트로는 TCP/135, TCP/445 등이 있다.

## ■ 신종 국산/외산 제작 악성코드 비교현황

올 한해 발견된 국산/외산 제작 악성코드의 비율은 역시 외산제작 악성코드가 월등히 많다. 국산제작 악성코드의 경우 전년대비 1.5배 정도가 증가하였다([그래프5], [그래프6] 참조).

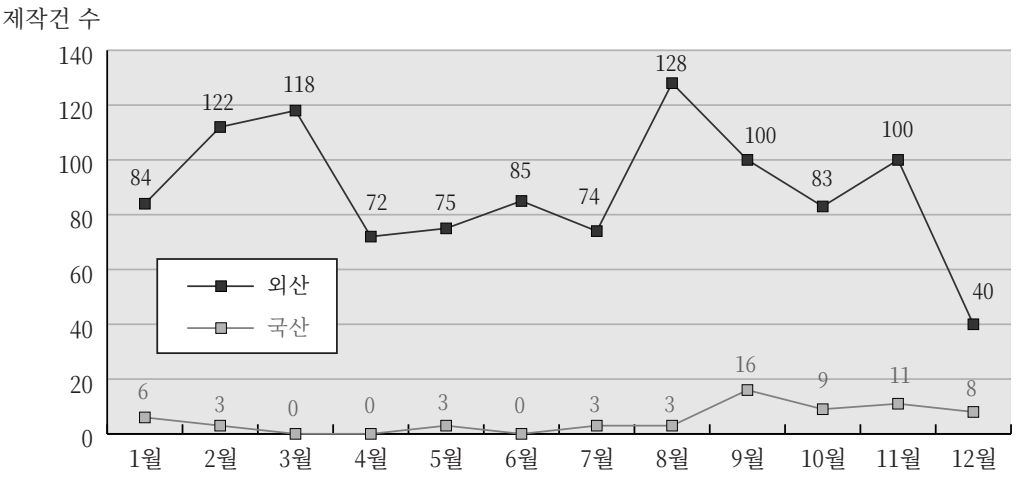



[그래프5]2002년 신종 악성코드 국산/외산 현황

2002년의 국산 악성코드들은 웜 또는 트로이목마 형태로 특정 게임의 CD-Key 를 불법적으로 획득하거나 시스템 파일을 삭제 또는 감염시키는 웜, 사용자 정보를 추출하는 백도어 형태가 그 수는 적지만 제작되어져 피해가 있었다.

2003년도에 발견된 외산 악성코드 유형은 대부분 IRCBot 기반의 백도어들이 많았으며 유사한 형태의 웜도 많았다. 변형이 많았던 악성 IRCBot 은 소스가 공개되고 모듈 형식으로 쉽게 기능을 추가하거나 뺄 수 있고 자세한 컴파일 방법이 소개되어 인터넷 등에서 유포되고 있었다. 대부분의 증상은 비슷하나 대표적으로 특정한 IRC 서버에 접속되어져 명령을 받으면 시스템 정보를 유출 당하거나 다른 시스템에 대한 SYN Flooding 공격과 같은 DoS 공격도 가능하다. 또한 전파시에나 DoS 공격시 상당한 네트워크 트래픽을 유발한다.

국산 악성코드의 유형으로는 대부분 성인 웹사이트 광고메일을 보내는 스팸 메일러였으며, 또한 이 스팸 메일러를 설치하기 위하여 MSN 메신저를 이용하는 웜이 제작되어지기도 하였다. 이와 같은 스팸메일러는 하반기부터 증가하기 시작하였다.




[그래프6]2003년 신종 악성코드 국산/외산 현황

어떤 스팸 메일러는 국내 유명 채팅 사이트의 게시판에 클라이언트와 서버 파일을 올려두고 현재 정확한 경로는 알려지지 않았지만 광고메일을 통하여 Active X 설치를 유도하여 해당 파일이 내려받아지도록 하여, 변형된 파일을 계속 게시판등에 업로드하면서 릴리즈되고 있다.

위와 같이 2003년도 제작되어졌던 국산 악성코드들은 과거 어린학생들이 호기심으로 제작해보거나 악성코드 제작단체가 만들어 유포한 것이 아닌 스팸 메일을 발송하기 위하여 제작되어진 사례가 더 많았다. 이와 유사한 사례로는 Mass Mailer 웜에 감염된 시스템이 스팸메일에 대한 릴레이 서버가 되어 더욱 더 많은 스팸메일을 보내고 있다는 외국기관의 발표도 있었다. 국내는 직접 웜에 의한 사례를 아니지만 앞으로는 이러한 형태의 악성코드의 출현도 예상되고 있다.

# Ⅲ 2003년 취약점 발견 동향

작성자 : 조경원 연구원(dubhe@ahnlab.com)

최근 윈도우의 보안 취약점에 대한 많은 뉴스와 관련 침해사고가 발생하며 이에 대한 관심이 매우 높아지고 있다. 2000년 이전까지 윈도우는 일반 개인 사용자들이 주로 사용하는 클라이언트용 OS였으며 바이러스, 웜, 트로이목마 등의 악성코드들에 의해서 침해를 당하는 것이 대부분이였다. 윈도우는 MS-DOS기반으로 시작하여 윈도우 3.x, 윈도우 9x, 윈도우 NT 계열(NT, 2000, XP)로 발전하였다. 윈도우 9x까지는 일반 사용자가 주로 사용하는 클라이언트 OS였으며, NT계열부터 서버기능을 가진 윈도우 NT와 윈도우 2000 Server계열, 클라이언트 사용자용인 윈도우 2000 Professional로 나누어지게 되었다. 이때부터 일반 클라이언트용 윈도우에서도 서버기능이 추가되기 시작하였다.

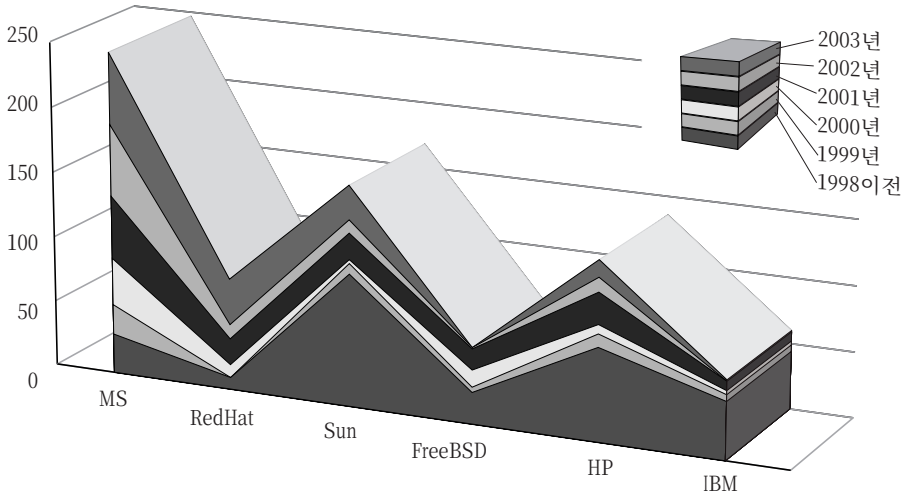
클라이언트 OS와 서버 OS의 구분이 생기게 된 기준은 네트워킹의 지원이다. 네트워킹을 통해 정보(혹은 자원)를 제공하는 서버와 이를 사용하는 클라이언트의 개념이 생기게 되었으며 네트워킹의 지원으로 일반 클라이언트는 서버 및 다른 클라이언트와 접속이 가능하게 되었다. 보안 취약점에 대한 인식 및 연구는 네트워킹의 발달 및 보급과 함께 발전하게 된다.

네트워킹이 보급되기 이전의 보안 취약점은 클라이언트 사용자에게서는 큰 의미가 없었다. 자신이 사용하는 PC 내부에서만 동작이 가능하므로 바이러스, 트로이목마 등의 시스템 파괴 목적의 악성코드 등이 보안 위협이 되었으며 시스템 자체의 취약점 등은 단순한 시스템 파괴 등의 효과 이외에는 다른 활동은 거의 존재하지 않았다. 또한 클라이언트 OS는 네트워킹 지원이 매우 적으며 기본적으로 열려진 포트와 서비스가 적으므로 취약점이 발생 가능한 토대가 적었다. 인터넷 사용의 발달로 일반 PC가 네트워킹이 가능해지며 많은 서비스를 지원하게 되면서 보안 취약점이 늘어나게 되었으며 바이러스, 웜 역시 네트워크를 사용하며 다른 클라이언트를 감염하기 위해서 실제적인 보안 취약점을 사용하게 되었다.

아래의 [표1]과 [그래프1]은 CIAC(http://www.ciac.org/)에 등록된 취약점 리스트로 각 Vendor에 대한 취약점 개수를 나타낸다.

| | MS | RedHat | Sun | FreeBSD | HP | IBM |
|---|---|---|---|---|---|---|
| 1998이전 | 30 | 9 | 101 | 24 | 71 | 44 |
| 1999 | 23 | 0 | 8 | 4 | 10 | 5 |
| 2000 | 36 | 10 | 3 | 13 | 7 | 3 |
| 2001 | 48 | 20 | 20 | 16 | 24 | 7 |
| 2002 | 55 | 11 | 10 | 1 | 11 | 0 |
| 2003 | 55 | 35 | 26 | 0 | 13 | 1 |
| 합계 | 247 | 85 | 168 | 58 | 136 | 60 |

[표1]CIAC 에 등록된 년도별 OS별 취약점 리스트



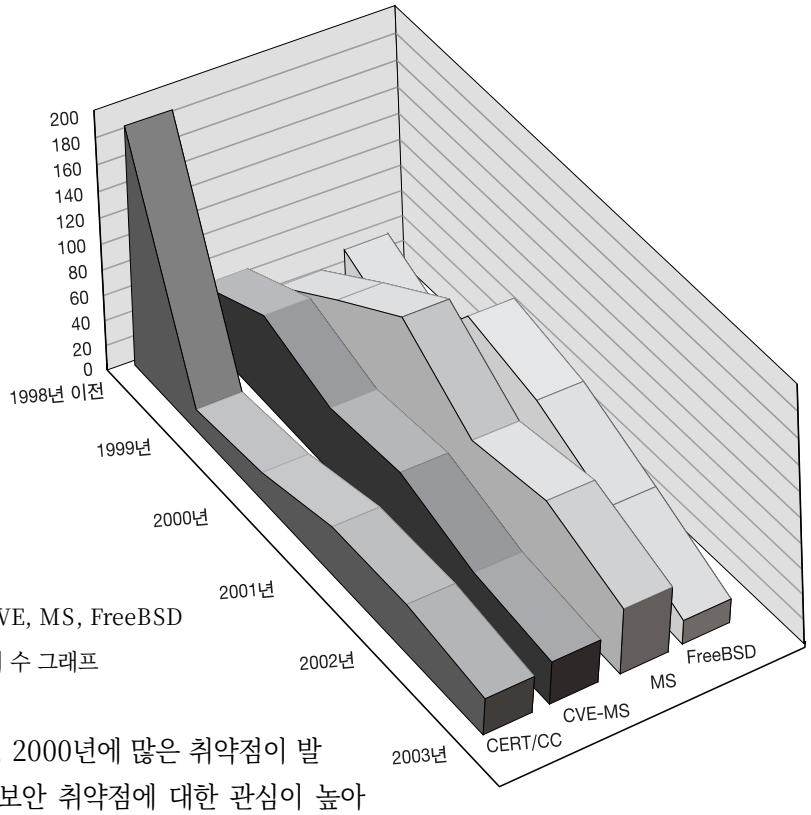

[그래프1]CIAC에 등록된 년도별 OS별 취약점 리스트 그래프

[표1]과 [그래프1]을 보면 MS의 경우 다른 OS에 비하여 매년 매우 많은 취약점이 발견되는 것을 확인할 수 있다.
Sun, HP, IBM등 오래 전부터 개발되고 사용된 시스템의 경우 1998년 이전의 취약점이 매우 많은 반면 이후 각 연도별 발생 건수는 MS에 비해 현저히 적다. MS의 윈도우 계열 OS 사용빈도는 98년 이전에도 매우 높았음에도 불구하고 이런 결과를 나타내는 것은 클라이언트용으로 윈도우 계열 OS가 주로 사용되었기 때문에 보안취약점이 발생할 구조가 적었으며, 또한 보안 취약점에 대한 연구가 다른 Unix계열 OS비해 현저히 적었기 때문이다. 98년 이후 보안 취약점 발견 횟수는 OS 사용 빈도와 거의 비슷한 결과를 보여주고 있다.

[표2] 와 [그래프2]는 CERT/CC, CVE, MS 및 FreeBSD에서 발표한 Advisory의 수로써 CVE는 윈도우 OS에 대한 취약점만을 계산하였다. 기타 다른 Linux, SunOS등의 OS는 Advisory가 아닌 Patch형태로 매우 광범위하게 제공되어 제외하였다.

| | CERT/CC | CVE-MS | MS | FreeBSD |
|---|---|---|---|---|
| 1998년 이전 | 184 | 43 | 20 | 31 |
| 1999 | 17 | 70 | 61 | 6 |
| 2000 | 22 | 51 | 100 | 82 |
| 2001 | 37 | 57 | 60 | 71 |
| 2002 | 37 | 39 | 72 | 46 |
| 2003 | 28 | 33 | 51 | 19 |
| 합계 | 325 | 293 | 364 | 255 |

[표2]CERT/CC, CVE, MS, FreeBSD에서 발표한 Advisory의 수

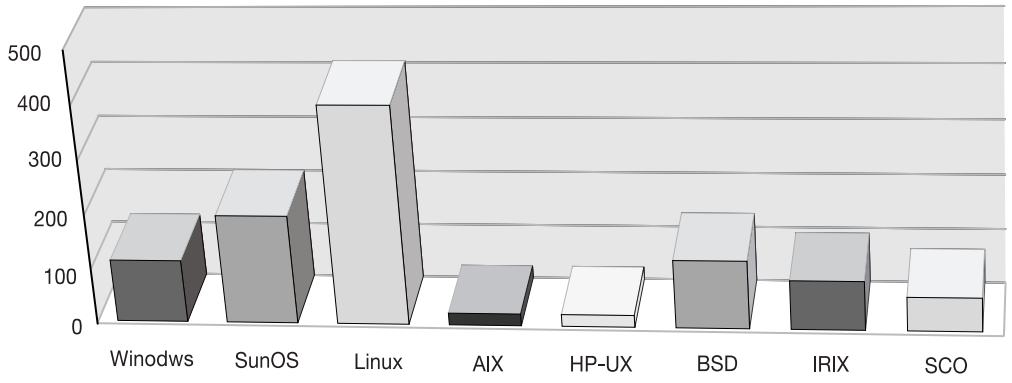



[그래프2]CERT/CC, CVE, MS, FreeBSD 에서 발표한 Advisory의 수 그래프

대체적으로 1999년, 2000년에 많은 취약점이 발견되었으며 이때가 보안 취약점에 대한 관심이 높아지기 시작한 연도이다. MS의 경우 윈도우 2000이 출시되고 서버기능이 강화되면서 취약점이 늘기 시작한 것을 보여준다. 취약점에 대한 연구가 활발해지면 발견되는 신종 취약점이 늘어나지만 취약점의 갯수는 한계가 있으므로 새로운 OS 버전이 나오기 전까지는 감소 추세를 보여준다. CERT/CC의 Advisory는 88년부터 시작하기 때문에 누적된 Advisory수가 매우 많다.

## ■ OS별 공격코드

[그래프3]은 99년 8월 까지의 Exploit 코드를 전문적으로 수집하는 한 사이트에 등록된 실제 Exploit 코드의 개수다.

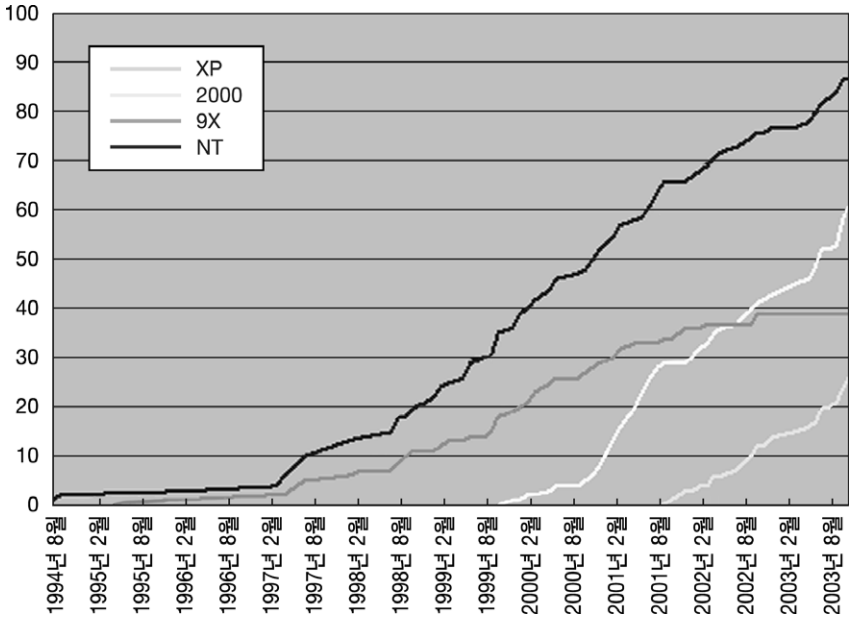



[그래프3]1999년 8월까지의 실제 Exploit 코드 개수

윈도우계열의 취약점은 대부분 NT시스템의 공격 코드 및 9x계열의 시스템 DoS 공격코드이며  나머지 Unix계열의 경우에는 해커들이 테스트가 쉽게 가능한 x86 및 Sparc 아키텍쳐에서 동작하는 Linux, SunOS, BSD, SCO가 대부분을 차지함을 알 수 있다. IRIX의 경우에는 특정 해커그룹에서 연구를 활발이 하여 공격코드가 많이 알려졌으며 HP-UX, AIX는 일반적인 해커들이 사용할 기회가 힘든 대형 기종이기 때문에 상대적으로 공격 코드가 적다. 2000년 이후에는 윈도우 계열에 대한 공격코드가 매우 증가 하였으며 통계를 추출하기 어려울 정도로 많은 변종 및 악용되는 바이러스, 웜이 증가하였다.

## ■ 윈도우 버전별 취약점 증가추세

[그래프4]는 OS버전별 취약점 갯수를 나타내며 데이터는 CIAC의 정보를 사용하였다. OS 자체의 취약점만을 계산하였다.




[그래프4]윈도우 OS버전별 취약점 개수 그래프

윈도우 NT, 2000, XP와 같은 윈도우 NT계열 시스템이 윈도우 9x계열 시스템보다 그래프의 기울기가 월등히 높으며 이는 윈도우 NT, 2000의 Server OS가 취약점이 많다는 것을 보여주고 있다. 특히 윈도우 2000의 경우에는 이전에 나온 윈도우 9x보다 훨신 취약점이 많음을 알 수 있다. 이것은 서버 OS의 특성상 디폴트로 열려진 Port와 서비스가 많기 때문에 취약점이 발생할 확률이 높기 때문이다. 윈도우 XP와 2000은 비슷한 구조를 갖고 있으나 XP가 나왔을 당시 윈도우 2000에서 발생한 보안취약점을 제거하고 출시되었기 때문에 상대적으로 취약점 수가 적게 나왔지만 다른 윈도우 98의 경우에는 OSR 2, 윈도우 2000의 경우 서비스팩 등을 거의 사용하고 있으므로 실제 잔존하는 취약점 수는 크게 차이가 없을것으로 보여진다.

## ■ 2003년 윈도우 취약점 동향

2003년에는 윈도우 OS에 대하여 심각한 취약점이 발견되었으며 실제 취약점이 웜 등에 사용되어 큰 피해를 낳게 되었다. 대표적인 것이 전세계적으로 확산된 블래스터(Blaster), 웰치아(Welchia) 웜이 그 예이다. 블래스터, 웰치아 및 기타 변종 웜들은 MS03-026의 RPC DCOM 취약점을 사용하여 패치되지 않은 시스템을 공격하며 시스템 및 네트워크 장애를 주었다. 이전의 MS 취약점을 사용하는 웜의 경우 대부분 님다(Nimda), 코드레드(CodeRed) 등의 IIS웹 서버, SQL서버의 취약점을 사용한 SQL_Overflow(일명 Slammer) 웜 등 서버용 OS를 상대로 한 것이 대부분이였지만 2003년에는 대상이 일반 PC에 대해서 취약점을 사용한 악성코드가 늘게 되었다는 점이 큰 변화이다.

2003년 이전에 Client OS에 대한 취약점은 대부분 IE, Outlook 등의 어플리케이션 레벨의 취약점이거나 Null Session, 공유폴더 취약점, DoS(Denied of Service) 공격 등이 대부분이였으며 직접적으로 시스템 내부에 접근이 가능한 취약점은 거의 존재하지 않았다. 그러나 2003년 들어와 윈도우에서 Buffer Overflow 공격 실현에 대하여 많은 발전이 있었으며 윈도우 내부의 취약점에 대한 연구 역시 매우 크게 발전하였다.

보안 취약점의 동향으로는 보안 취약점의 발표 시기와 벤더간의 협조에 큰 변화가 있었다. 2003년 이전에는 해커 및 연구단체에서 발견한 보안 취약점의 대부분은 bugtraq이나 보안 사이트에 직접 취약점에 대한 내용과 실제 공격 방법(Proof of Concept), 공격코드(Exploit Code)가 발표되는 것이 대부분이였다. 하지만 이번 RPC DCOM 취약점, Workstation 서비스 취약점, Exchange Server 취약점 등은 EEye, Xfocus등 취약점을 발견한 그룹과 MS가 함께 보안 패치 발표 및 취약점을 발표하여 패치가 나오기 전 존재하는 보안 위협을 최소화 하는데 큰 효과를 거두었다. 이는 보안취약점 발견 시 벤더와의 공동 작업을 하였다는 점에서 매우 좋은 결과라고 생각된다.

앞으로 보안 공격 기술은 점점 발전하여 다른 많은 취약점이 발견될 가능성이 항상 존재하지만 MS는 2003년 중반 새로운 OS 개발 및 프로젝트에는 보안을 크게 고려하여 만든다는 발표를 하였다. 보안 강화 기술을 통하여 취약점이 발견되어도 실제 공격 가능 여부는 크게 줄

어 들 수 있지만 공격 기술 역시 발전을 하므로 미래의 보안 동향에 대해서는 정확한 판단을 내리기는 어렵다.
보안 수단의 강화와 함께 공격 기술 역시 항상 발전하므로 안전한 시스템은 없다. 최대한의 보안은 지속적인 관심과 관리이다.

# IV 2003년 악성코드 사건사고

## 1. 한국의 악성코드 사건사고

작성자 : 차민석 연구원(jackycha@ahnlab.com)

2003년 한해는 1월부터 SQL_Overflow 웜[1]으로 이른바 ' 1.25 인터넷 대란 '이 발생해 국가 인터넷이 마비되는 사건이 발생했다. 여름에는 미메일 웜[2], 블래스터 웜[3], 웰치아 웜[4], 두마루 웜[5], 소빅.F 웜[6] 등이 널리 확산되어 많은 시스템을 감염시켰다. 특정 사이트 광고를 목적으로 제작된 신msn 웜[7], 스미백 웜[8]과 같은 한국산 웜도 발견되었다. 이들은 동일인 혹은 동일 회사에서 광고 수입을 목적으로 제작한 것으로 추정된다. 이외 자신을 백신이나 사용자로부터 숨기는 은폐기법을 사용하는 Win-Trojan/RtKit.128000[9], Win-Trojan/HackDef.50688[10] 등의 트로이목마도 등장하기 시작했다.

11월에는 광고 목적으로 제작된 애드웨어 파일인 hotdog.exe(Win-Trojan/Hotra.49152)[11]가 오동작을 일으켜 많은 사용자들이 컴퓨터 사용에 불편을 느꼈다. 이 사건을 계기로 애드웨어에 대한 사람들의 부정적인 이미지가 강해졌다. 하지만, ' 애드웨어를 악성코드로 분류해 백신에서 해결해야 하는가 '라는 문제는 백신 업계가 계속 고민하고 있다. 악성코드는 은폐기법, 취약점 이용, 실행 압축 등의 기법으로 더욱 교묘해지고 개인 정보를 위협하는 다양한 형태가 등장하고 있지만 사람들의 보안의식은 제자리에 머물러 있어 그 피해는 줄지 않았다.

이 장에서는 이러한 보안 사고들을 중점으로 2003년 한국에서 많은 관심을 끌었던 사고를 정리하여 2003년 한국의 시큐리티 동향을 정리해 보았다.

---

1) SQL_Overflow 웜 : 일명 슬래머 웜, http://info.ahnlab.com/smart2u/virus_detail_1098.html
2) 미메일 웜 : Win32/Mimail.worm, http://info.ahnlab.com/smart2u/virus_detail_1197.html
3) 블래스터 웜 : Win32/Blaster.worm.6176, http://info.ahnlab.com/smart2u/virus_detail_1202.html
4) 웰치아 웜 : Win32/Welchia.worm.10240, http://info.ahnlab.com/smart2u/virus_detail_1206.html
5) 두마루 웜 : Win32/Dumaru.worm.9234, http://info.ahnlab.com/smart2u/virus_detail_1207.html
6) 소빅 F 웜 : Win32/Sobig.worm.F, http://info.ahnlab.com/smart2u/virus_detail_1208.html
7) 신msn 웜 : Win32/Sinmsn.worm.20480, http://info.ahnlab.com/smart2u/virus_detail_1193.html
8) 스미백 웜 : Win32/Smibag.worm.163840, http://info.ahnlab.com/smart2u/virus_detail_1223.html
9) Win-Trojan/RtKt.128000 : http://info.ahnlab.com/smart2u/virus_detail_1222.html
10) Win-Trojan/HackDef.50688 : http://info.ahnlab.com/smart2u/virus_detail_1227.html
11) Win-Trojan/Hotra.49152, http://info.ahnlab.com/smart2u/virus_detail_1240.html

(1) SQL_Overflow웜에 의한 인터넷 대란

1월 25일 토요일 오전 스팸 메일을 발송하는 Win-Trojan/SystEntry.32768.B[12]가 윈도우 98에서 오동작을 일으켜 윈도우 부팅이 되지 않는 문제가 발생했다. 또한 같은 날 오후 1시부터 인터넷 장애가 간헐적으로 나타났고 곧 국내 인터넷이 마비되었다. 원인은 SQL 서버의 취약점을 이용해 전파되는 SQL_Overflow 웜으로 밝혀졌고 한국의 인터넷이 몇 시간 동안 마비되는 이른바 ' 1.25 인터넷 대란 '이 발생했다. 당시에 인터넷 마비의 원인과 책임에 대해서 많은 논란이 있었다.

(2) JS/Fortnight의 꾸준한 확산

JS/Fortnight[13] 바이러스는 짧은 시간에 널리 퍼지지 않았지만 일년 동안 꾸준히 발견되었다. 이 바이러스는 많은 변형을 가지고 있으며 최근 악성코드의 제작자 중에 하나인 인터넷 광고업자들에 의해 제작되었다. 취약점이 존재하는 아웃룩 익스프레스에서 바이러스에 감염된 메일을 읽으면 자동으로 감염된다. 이후 아웃룩 익스프레스로 메일 보낼 때 서명에 특정 사이트 주소를 넣어 상대방이 메일을 읽을 때 해당 사이트에 몰래 접속하게 한다. 해당 사이트도 취약점이 존재하는 웹 브라우저에서 읽을 때 자동 감염된다. JS/Fortnight 바이러스 시리즈가 사용하는 취약점은 몇 가지 있으며 새로운 취약점이 나타나면 해당 취약점을 이용해 자동 감염을 시도한다.

(3) 러브게이트 웜 변형의 확산

러브게이트 변형(Win32/LovGate.worm.107008)[14]이 3월부터 널리 퍼졌다. 중국에서 제작된 것으로 추정되며 여러 변형이 있다. 이중 몇몇 변형은 윈도우 실행 파일(확장자가 EXE)을 감염시키는 바이러스 형태도 존재한다. 치료를 어렵게 하기 위해 이미 실행 중인 시스템 파일에 웜 코드를 끼워 넣는 방법(Code Injection)을 사용한다. 코드 삽입 기법을 사용한 악성코드는 시스템을 재부팅 해야 치료(삭제)가 가능하며 여러 악성코드에서 일반적으로 사용되고 있는 기법 중 하나가 되었다.

(4) Dropper/MircPack 류의 꾸준한 등장

Dropper/MircPack[15]류의 웜도 꾸준히 등장했다. 이들 중 상당수의 변형은 감염 시스템에 FTP 데몬을 설치해 외부에서 파일을 업로드/다운로드 할 수 있게 한다. 하드 디스크 전체를 외부에서 접근할 수 있게 해 개인 정보를 유출하는 경우도 있지만 와레즈(Warez) 사이트로 이용하기도 한다. 따라서, 자기도 모르게 Win-Trojan/ServU.212126[16] 등과 같은 트로이 목마에 감염된 경우 자신의 컴퓨터가 와레즈 서버로 운영되며 여러 사람이 접속할 경우 컴퓨터 속도가 현저히 느려질 수 있다.

---

12) Win-Trojan/SystEntry.32768.B : http://info.ahnlab.com/smart2u/virus_detail_1096.html
13) JS/Fortnight : http://info.ahnlab.com/smart2u/virus_detail_1182.html
14) Win32/LovGate.worm.107008 : http://info.ahnlab.com/smart2u/virus_detail_1135.html
15) Dropper/MircPack.755236 : http://info.ahnlab.com/smart2u/virus_detail_1095.html

(5) 은폐기법을 사용한 트로이목마의 등장

5월 말에는 Dropper/Delf.74240[17]이 발견되었다. 이는 은폐기법(Stealth Technique)을 사용한 트로이목마로, 트로이목마 파일을 탐색기나 일반 윈도우 프로그램으로는 찾을 수 없게 한다. 은폐기법을 이용한 트로이목마는 이외에도 Win-Trojan/RtKit.128000, Win-Trojan/HackDef.50688 등이 있으며 새로운 기법에 대해 계속 연구되고 있으므로 백신이나 사용자가 찾기 어려운 은폐형 악성코드는 계속 등장할 것으로 예상된다.

(6) 광고기능을 포함한 악성코드 등장

여름에 여러 가지 악성코드가 널리 퍼져 사람들을 괴롭혔다. 우선 Win32/Sinmsn.worm.20480은 이후 Win32/Smibag.worm, Win-Trojan/Hotra 등으로 이어지는 광고 기능을 포함한 악성코드가 등장했다. 사용되는 파일 등이 동일 혹은 유사해 동일인 혹은 동일 업체에서 개발하고 있는 것으로 추정된다. 기존의 악성코드 제작자들이 재미나 장난 삼아 악성코드를 제작하고 퍼드리지만 이런 악성코드는 돈이 목적이다.

(7) 블래스터, 웰치아 웜 피해로 인한 업무마비 속출

8월은 2003년 최악의 해로 기록 될 수 있다. 우선 1일부터 Win32/Mimail.worm 이 발견되었다. 이후 RPC DCOM 취약점을 이용한 블래스터 웜, 웰치아 웜이 발견되었다. 이전에도 코드레드 웜(Code_Red), SQL_Overflow 웜 등 취약점을 이용한 웜이 존재했지만 이전 웜은 서버급에서 활동해 감염 비율이 적은 편이었지만 RPC DCOM 취약점은 윈도우 2000과 윈도우 XP 계열에 적용되므로 감염 수는 엄청났다. 특히 웰치아 웜은 정부, 은행, 항공사 등의 시스템들도 감염시켜 업무를 마비시키기도 했다. 웰치아 웜에 감염되어 업무가 마비된 사례는 다음과 같다.

* 관련 기사
- http://www.zdnet.co.kr/ecommerce/biztrend/article.jsp?id=64386&forum=1
- http://news.naver.com/news_read.php?oldid=2003121100008631081
- http://news.naver.com/news_read.php?oldid=20030924000046599902

(8) 메일을 통해 확산되는 소빅F, 두마루 웜 피해 급증

8월 중순 발견된 소빅.F 웜[18]과 두마루 웜[19]은 전형적인 메일을 통해 전파되는 웜이지만 왕성한 전파능력으로 엄청난 메일이 발생했다. 이들 웜은 메일 발신인을 임의로 선택하는데 몇몇 스팸 메일 방지 프로그램과 백신 프로그램에서 웜 감염 결과를 웜을 실제로 보낸 계정이 2003년 9월 10일 이후 활동을 하지 않지만 날짜가 잘못 설정된 시스템도 존재해 9월 10일

16) Win-Trojan/ServU.212126 : http://info.ahnlab.com/smart2u/virus_detail_1151.html
17) Dropper/Delf.74240 : http://info.ahnlab.com/smart2u/virus_detail_1179.html
18) Win32/Sobig.worm.F : http://info.ahnlab.com/smart2u/virus_detail_1208.html
19) Win32/Dumaru.worm.9234 : http://info.ahnlab.com/smart2u/virus_detail_1207.html

이후에도 감염 보고가 계속 되고 있다. 2001년에 발생한 9.11 테러 2주년에 신종 악성코드가 등장할 거라는 우려도 있었지만 하나의 해프닝으로 끝났다. 악성코드는 매일 발생하고 있는 일상적인 문제가 된지 오래이다.

(9) 애드웨어의 피해 증가

11월 초 컴퓨터 속도가 현저히 떨어진다는 문의가 들어오고 문제의 파일로 hotdog.exe 파일이 접수되었다. 확인 결과 해당 파일은 웜, 바이러스, 트로이목마가 아닌 광고를 출력해주는 애드웨어(Adware)로 밝혀졌다. 애드웨어는 제한 없이 무료로 사용되는 프리웨어(Freeware), 일정한 금액으로 제품을 사야 하는 셰어웨어(Shareware) 같이 광고를 보면 사용할 수 있는 프로그램을 뜻하지만 광고를 보여주는 프로그램도 해당된다. 애드웨어는 흔히 사용자 정보를 빼가는 스파이웨어(Spyware)와 혼돈되어 사용되지만 애드웨어는 보통 사용자 동의 하에 설치되며 직접 사용자 정보를 빼가는 행동은 하지 않아 대부분의 백신에서 악성코드로 분류하지 않아 진단하지 않는다. 하지만, 고객들이 원하지 않는 프로그램이며 컴퓨터 사용에 불편도 많고 진단에 추가해달라는 요청도 꾸준해 계속 고민하고 있는 문제이다. 특히 애드웨어가 광고를 받아오고 광고를 보여주면서 발생하는 네트워크 트래픽 양도 만만치 않고 hotdog.exe처럼 프로그램 자체의 버그로 인해 시스템 장애를 발생시켰을 때의 문제도 존재한다. 현재 많은 백신 업체에서 애드웨어 등을 악성코드가 아닌 유해가능 프로그램으로 분류해 사용자가 이들 프로그램에 대한 진단 및 치료(삭제)를 선택적으로 하고 있다.

단, 애드웨어도 다음 내용이 확인되면 트로이목마로 분류되어 V3 제품 군에서 진단/치료(삭제)한다.

- 사용자 정보 유출
- 사용자 동의 없이 설치
- 사용자 동의 없이 프로그램 업데이트 등의 위험 행동

애드웨어의 설치 경로는 보통 웹 서핑, 스팸 메일 등을 통해 발생하며 사용자들이 정확한 설치 경로를 기억하지 못해 설치 경로 확인에 어려움이 있다.

메일, 공유 폴더 등으로 전파되는 과거의 웜에 취약점을 이용해 인터넷에 접속되어 있는 것만으로 감염되는 웜의 등장은 보안에 무관심하거나 잘 모르는 많은 사람들을 괴롭혔다. 게다가 인터넷 서핑 중에 설치를 요구하는 액티브 X 컨트롤을 무심코 설치해 홈페이지가 고정되고 광고에 출력되는 애드웨어로 고생하는 일까지 발생해 사람들을 괴롭히고 있다. 인터넷의 발전은 사람을 편하게 해준 반면, 개인 정보 침해나 악성코드 감염 등의 위협은 나날이 높아지고 사람들의 보안 의식은 제자리에 머물러 있어 보안위협에 대한 노출은 더욱 많아졌다.

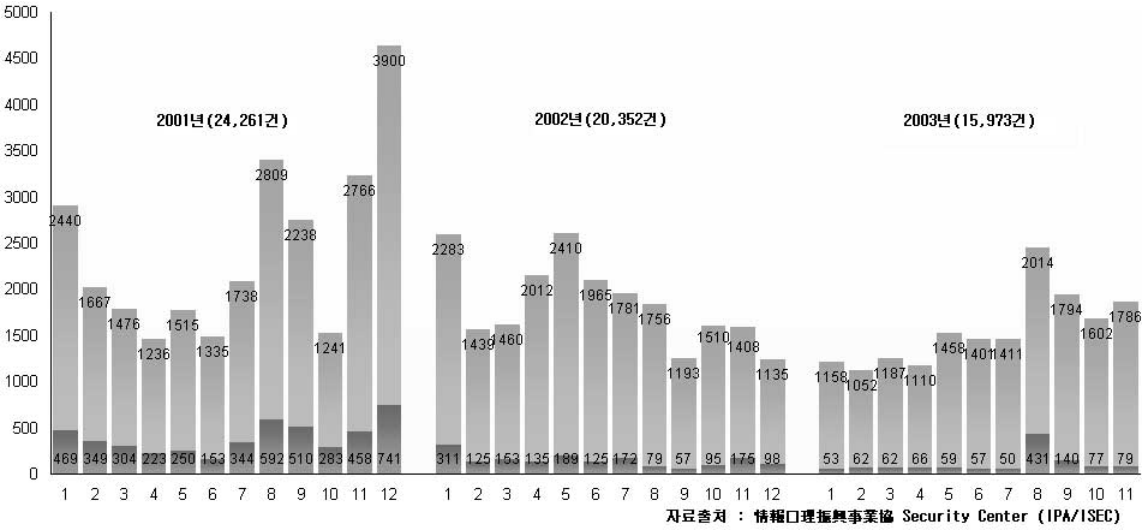
## 2. 일본의 악성코드 사건사고

작성자 : 김소헌 연구원(sopara@ahnlab.com)

인터넷의 발달로 인해 삶의 형태가 급격하게 변화해가면서 그에 대한 부작용 또한 급증하고 있다. 날이 갈수록 심각해지는 바이러스나 스팸 메일의 폐해에 대해서는 심각하다는 말이 무색할 정도이고 새롭게 발생한 악성코드는 국가 기간망을 마비시킬 정도로 위력을 발휘했다. 이러한 현상은 일본의 경우도 크게 다르지 않다. 이 문서에서는 올 한 해 동안 일본에서 발생한 사건들 중 사회적 이슈가 되었던 중요 사건들에 대한 자료를 통해 일본의 보안동향을 파악해 보도록 한다.

(1) 보안 취약점을 이용한 웜에 의한 피해

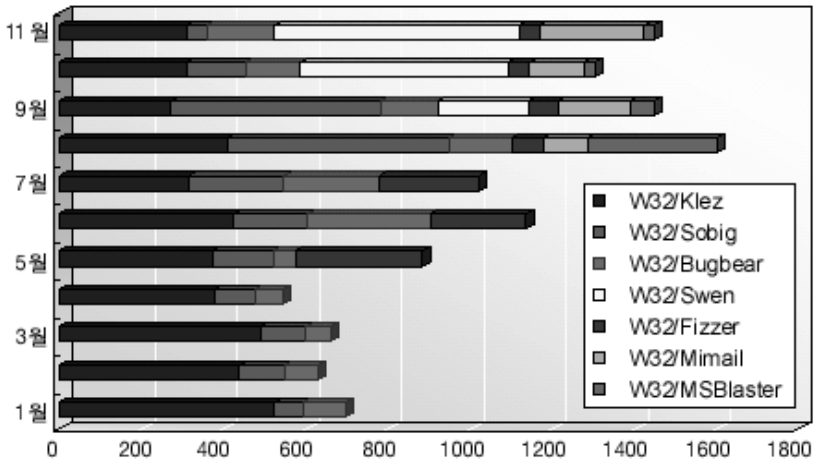
2003년 한 해 동안 일본에서 이슈가 되었던 보안 사고들의 대표적인 것들 중의 하나는 윈도우 취약점을 이용한 SQL_Overflow와 블래스터 웜, 웰치아 웜에 의한 피해일 것이다.
아래의 도표는 일본 IPA/ISEC에서 발생한 바이러스의 연도별 추이에 관한 자료이다. 그래프 상단의 수치는 실제 감염이 아닌 단순 신고 건수를 나타내고 하단의 수치는 이들 중 실제로 감염에 의한 피해를 당한 경우의 수치이다.
2003년의 도표에서 특이할 만한 점은 블래스터 웜 등 RPC 취약점을 이용한 웜의 활동 시작 시기인 8월의 신고 건수 대비 실제 감염 피해 정도가 다른 시기에 비해 월등하게 높다는 것이다. 백신 프로그램의 보급이 일반화되어 실제 감염 빈도가 매우 낮은 2002년 이후의 데이터와 비교해 볼 때 새로운 형태의 웜에 의한 피해의 심각성을 알 수 있을 것이다.




(2) 2003년 일본에서 여전히 유행한 Klez 웜

2003년 한해 동안 일본에서 가장 널리 퍼진 악성코드는 마이크로소프트(Microsoft)사의 Outlook 취약점을 이용하여 전파되는 클레즈 웜(Win32/Klez.worm)이다.
소빅 웜도 지속적으로 확산되었고 특히 소빅.F는 2003년 8월과 9월에 걸쳐 많은 양의 신고 횟수를 기록하였으나 10월 이후로 점점 줄어드는 추세를 보여준다.

도표에는 나타나지 않았으나 오파소프트(Opasoft) 웜이나 님다(Nimda)와 같은 오래된 악성코드들도 여전히 사라지지 않고 남아있는 등 대체적인 감염 추세는 한국 상황과 비슷하다.




(3) 웹 사이트의 고객 정보 유출 사건

컴퓨터 소프트웨어 저작권협회의 홈페이지에 저장된 상담자들 1,184명의 정보가 유출되는 사건이 발생하였다. CGI 프로그램상의 실수로 인해 일반 유저들에게 보여지지 않아야 할 정보가 유출된 이 사건은 일반 사용자가 쉽게 찾아낼 수 있는 형태의 오류는 아니었지만 개인정보의 보호에 민감해야 할 협회에서 사용자의 정보가 노출되었다는 점에서 유감이 아닐 수 없다.

東武철도의 회원 정보가 유출되어 정보가 유출된 회원들에게 가짜 청구서가 발송되는 사건이 발생했다. 東武철도는 열차운행 정보 등을 메일로 전해주는 서비스를 운영하고 있으나 이 서비스를 이용하는 고객의 정보가 유출되어 사용자가 사용하지 않은 서비스에 대해서 비용을 청구하는 수법에 이용되었다. 실제로 돈을 지불한 사람은 없었기 때문에 이로 인한 피해가 발생하지는 않았다고 해도 공신력을 가지고 있는 단체에서 개인의 정보가 쉽게 타인에게 노출되었다는 점에서 심각한 문제가 아닐 수 없다.

(4) 인터넷과 휴대전화 보급이 보편화됨으로 인해 나타난 신종 사기 수법

사용자가 이용하지 않은 서비스에 대한 비용 청구를 하는 방식의 사기 수법이 유행하여 사회문제화 되었다. 올해 들어서 편지나 엽서는 물론 이메일을 통해서 소비자에게 부당한 요금을 청구하는 사례에 대한 소비자센터의 상담 건수가 급격히 증가했고 비용 청구의 대상은 주로 포르노 사이트의 이용대금이었다. 5월에는 이러한 사기 수법을 이용하여 331명으로부터 786만엔의 부당이익을 획득한 혐의로 2명의 회사원이 체포되기도 했다.

일본의 국민생활센터는 작년부터 [사용하지 않은 서비스에 대한 청구]에 대한 피해 방지를 위한 사이트를 운영하고 있는데 이 사이트에는 월 10만회 이상의 사용자 방문 횟수를 기록할 정도로 이러한 유형의 사기 수법에 의한 피해가 빈번하게 발생하고 있다.

(5) Japannet 은행의 시스템 장애로 인한 서비스 중단

5월 8일 Japannet은행에 시스템 장애가 발생하여 22시간 동안 서비스가 중단되는 사태가

발생하였다. Japannet은행은 사건 발생 전인 5월 4일 사용자 증가에 대처하기 위해 하드웨어와 데이터베이스 용량을 증가시키고 버그를 가지고 있는 것으로 확인된 소프트웨어를 업그레이드 하는 작업을 실시하였으나 이 과정에서 문제가 발생하였고 그 결과 5월 8일 서비스가 중단되는 사태가 발생하였다.
같은 달 20일에는 Unix서버의 CPU에 장애가 발생하여 또다시 서비스가 중단되는 사태가 발생하였다. 문제가 발생한 서버는 14개의 CPU를 탑재하고 있으나 그 중 1개의 CPU에 문제가 발생하였고 17분 후 복구되었다. Japannet은행 관계자는 17분이라는 시간은 장애 대처 후 Unix 서버 등이 부팅되는 시간일 뿐이라고 하지만 24시간 운영되는 은행 시스템에서 17분이라는 시간 동안 서비스가 중단된다는 것은 있을 수 없는 일이다.

(6) 공유 프로그램을 이용한 파일 공유로 인한 저작권 문제

인터넷으로 개인들의 파일을 공유할 수 있는 소프트웨어인 Winny를 이용하여 게임 프로그램을 무단으로 복제하게 해준 두 명의 사용자가 京都경찰에 의해 저작권법 위반 혐의로 체포되었다. 체포된 두 명의 남자는 각각 자신의 하드 디스크에 저장된 겜보이용 게임 소프트웨어와 뷰티플 마인드 등의 미국 영화를 불특정 다수에게 배포한 것으로 알려졌다.
일본의 소프트웨어 저작권 협회에 의하면 파일 공유 소프트웨어의 사용자는 수년 전부터 급증하는 추세로 올 초에는 98만 명 정도가 이를 사용하고 있다고 한다.

(7) 사회 문제가 되고 있는 스팸

인터넷의 발달은 보다 빠르고 효율적인 정보 전달이 가능하게 해주었지만 이로 인한 병폐 또한 심각하게 대두되고 있고 스팸으로 인한 피해도 그 중의 하나이다. 스팸은 초기에는 이메일을 통해 광고를 전송하는 경우가 대부분이었으나 현재는 발송 대상이 점점 넓어지고 있는 추세이다.
일본의 경우 이메일은 물론 휴대전화로까지 무차별적으로 전파되는 스팸메일로 인해 문제화되고 있다.

| 범죄 분류 | 2000년 | 2001년 | 2002년 | 2002상반기 | 2003상반기 |
|---|---|---|---|---|---|
| 사기 · 악질 상법 관계 | 1396 | 1963 | 3193 | 1331 | 8776 |
| 위법 · 유해정보 관계 | 2896 | 3282 | 2261 | 1176 | 2605 |
| Internet · Auction관계 | 1301 | 2099 | 3978 | 1495 | 2309 |
| 명예회손 · 비방중상관계 | 1884 | 2267 | 2566 | 1229 | 1349 |
| 미확인 메일 관계 | 1352 | 2647 | 2130 | 1180 | 1246 |
| 불법 접근 · Virus 관계 | 505 | 1335 | 1246 | 693 | 506 |
| 기 타 | 1801 | 3684 | 3955 | 1988 | 2306 |

[표1]하이테크 범죄에 대한 연도별 상담처리 건수(일본 경찰청 자료)

위 [표1]은 일본 경찰청에서 발표한 하이테크 범죄에 대한 연도별 상담처리 건수에 대한 통계자료이다. 전년도에 비해 유해정보와 미확인 메일과 관련된 상담 건수가 현저하게 늘어난 것을 알 수 있고 이를 통해 일본의 유해정보 전파 상태를 짐작해 볼 수 있다.

## 3. 중국의 악성코드 사건사고

작성자 : 장영준 연구원(zhang95@ahnlab.com)

2003년은 시큐리티 분야에서는 예년과 달리 유달리 많은 악성코드와 해킹 사고들이 발생한 해로 평가될 한해이다.

보안 사고들은 이제 단순히 지역적인 사고라는 인식을 벗어나게 되었으며 그 영향은 네트워크를 통해 전세계로 순식간에 퍼져나가게 되었다. 아시아의 떠오르는 강대국이라는 중국에서 발생한 보안 사고들을 종합해 볼 때 이러한 부분에서 예외가 될 수 없을 것이다.

2003년 중국 시큐리티 분야에서 발생한 사건, 사고들은 점점 양적으로 증가하고 있으며 질적으로도 정교한 기술들이 등장하고 있다. 그리고 해당 사고들의 가해자와 피해자 역시 점점 다양한 계층으로 변화하고 있다. 이러한 보안 사고들을 중점으로 2003년 중국에서 많은 관심을 끌었던 9건의 사고를 선정하여 2003년 중국 시큐리티 동향을 정리 해보았다.

(1) Win32/Blaster.worm.6176 확산으로 인한 시스템 마비

8월에 발생한 Win32/Blaster.worm.6176는 중국뿐만 아니라 전 세계적으로 많은 피해를 입혔으며 그 피해로 인해 2003년 중국 최악의 시큐리티 사고로 선정되었다.

Win32/Blaster.worm.6176는 국외에서 발생하자마자 순식간에 네트워크를 타고 중국 전역으로 확산되었으며 마이크로소프트사의 윈도우 2000 계열의 RPC 취약점을 이용하였다. 특히, 감염 증상 중 하나인 윈도우 재부팅으로 인해 시스템의 정상적인 사용 자체를 불가능하게 하였다.

(2) SQL_Overflow 확산으로 인한 중국 네트워크 마비

1월 25일 발생한 SQL_Overflow는 마이크로소프트사의 MS-SQL Database 서버의 ‘ Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution ’ 취약점을 이용하였으며 이로 인해 80% 이상의 중국인들이 정상적인 인터넷 사용이 불가능 하였다. 이 사고는 태국, 일본, 한국, 말레이시아, 필리핀과 인도네시아 등 아시아 국가 대부분의 네트워크에 엄청난 영향을 미쳤으며 전세계적인 피해액은 12억 달러로 추산되고 있다.

(3) 중국 네트워크협회 홈페이지 공격

8월 8일, 중국 네트워크협회에서는 협회의 홈페이지를 통해 중국 내에서 스펨메일 발송에 사용중인 서버들의 IP를 정리하여 ‘ 스펨메일 서버 명단 (1기) ’을 발표하였다. 이 명단이 홈페이지를 통해 발표된 직후, 협회의 홈페이지 주소인 isc.org.cn으로 8월 21일부터 27일 일주일 동안 지속적인 네트워크 공격을 받았다.

(4) 백도(百度) 검색사이트 공격

5월에 발생한 웹 검색사이트인 백도(百度)에 대한 해킹 공격은 중국 네트워크 산업사에 있어서 가장 큰 규모의 공격이었다. 이번 백도(百度)에 대한 네트워크 공격은 백도(百度) 검색엔진에 다양한 검색어를 동시 다발적으로 입력하여 해당 검색엔진의 과부하를 발생시켰다. 그 중에서 가장 많이 검색된 단어는 38863번이나 입력 된 것으로 분석되었다.

(5) 복건성 천수시 교통경찰국 시스템 해킹

1월, 천수시 교통경찰국 전산시스템이 해킹 당하는 사고가 발생하였다. 전산시스템에 침입한 해커는 운전면허 관련 데이터베이스에 접근해 데이터들을 삭제하고 통계관련 프로그램도 삭제 하였다. 복건성 당국에서는 해커의 침입으로 인해 교통경찰국 전산시스템의 정상 운영이 어려운 것으로 보고하였다. 이 사건 발생한 직후, 교통경찰국에서는 전산시스템에 대한 대대적인 보안점검을 실시하고 해당 시스템의 개발회사인 가중화(家中和)사의 협조로 해당 데이터들을 복구할 수가 있었다.

(6) 공상(工商)은행 사칭 고객계정 비밀번호 해킹 시도

한 해커가 공상은행을 사칭하여 ' 온라인 뱅킹 시스템 업그레이드 '라는 제목으로 온라인 뱅킹에 등록되어 있는 고객들에게 메일을 발송하였다. 해당 메일에는 온라인 뱅킹 시스템이 변경되어 고객의 아이디, 은행 계좌번호, 비밀번호가 필요하니 회신을 해달라는 내용이었다. 이에 공상은행 측에서는 긴급히 전 온라인 뱅킹 고객들에게 은행 측에서는 이러한 요청을 한 적이 없으며 고객관련 정보는 외부로 노출하지 않는다는 메일을 발송하였다고 한다.

(7) 20여 기관 및 단체 온라인 계좌 해킹으로 한화 640만원 절도

7월, 한 해커가 해킹 툴을 이용해 온라인 계좌를 해킹한 혐의로 구속되었다. 이 해커는 2달 동안 국가기관, 호텔, 일반 기업 등 20여 기관과 단체들이 온라인 뱅킹 시에 사용하는 계정과 암호를 해킹해 한화 640만원을 절도하였다.

(8) 온라인 게임 ' 미르의 전설 3 ' 해커들의 공격으로 서비스 중단

7월, 온라인 게임 ' 미르의 전설 3 '를 서비스하는 서버들이 3일 동안 해커들의 공격을 받았다. 이 조직적이고 대규모 공격으로 인해 해당 서버들은 정상적으로 서비스를 하지 못하게 되었으며 온라인 게임을 이용하고자 하는 사용자들 역시 정상적인 접속을 하지 못하게 되었다.

(9) 인터넷 바둑 시합에 해커가 선수로 위장 참가

6월 한중 바둑 신인왕전이 중국의 신랑왕 웹 페이지와 한국의 Cyber 웹 페이지에서 진행이 되었다. 주최측은 시합에 쓰일 서버의 사용자 계정에 암호를 설정하지 않은 채로 시합을 준비한 것이 발단이 되어 사고가 발생하였다. 이 문제로 인해 해커가 해당 서버를 해킹한 후 중국 측 선수인 ' 공궐 '의 계정으로 시합에 참가하였으나 주최측은 시합이 10여분이 지나서야 이를 파악하고 재시합을 진행하게 되었다.

## 4. 세계의 악성코드 사건사고

작성자 : 차민석 연구원(jackycha@ahnlab.com)

2003년 전 세계에 발생한 악성코드 상위권은 순위가 조금 다를 뿐 국가 별로 비슷한 양상을 보이고 있다. 이는 인터넷의 발달로 전 세계 컴퓨터가 같은 맞물려 있기 때문 일 것이다. 대부분의 국가에서 소빅.F 웜, 웰치아 웜, 블래스터 웜, 두마루 웜 등이 상위권에 올랐다. 하지만, 국가별로 중-하위권 감염 순위와 피해 양상은 조금씩 다름을 알 수 있다. 특히 지역에서 제작되어 퍼지는 악성코드 비율이 높은 한국과 중국은 세계적으로 널리 퍼진 악성코드 외 해당 국가에서 제작된 악성코드 감염율도 높았다. 메신저로 전파되는 웜도 국가별로 조금씩 달랐는데 MSN 메신저 사용이 보편화된 한국에서는 MSN 메신저를 이용해 전파되는 웜의 수가 많았지만 중국은 자체적으로 개발되어 널리 사용되고 있는 QQ 메신저 등의 메신저로 전파되는 웜이나 스팸 메시지 보내는 트로이목마 등이 많았다. 국내 제작 악성코드 수가 상대적으로 적은 일본은 자국에서 많이 사용되는 P2P(Peer-to-Peer) 프로그램인 Winny를 통해 전파되는 Win32/Antinny.worm.651264[20] 외 지역 악성코드는 크게 눈에 띄지 않았다. 그 외 짧은 시간에 널리 퍼졌다가 금방 사라지는 지역 웜도 상당수 존재해 지속적인 감염 율과 피해 측면에서는 몇 개월에서 몇 년째 꾸준히 괴롭히고 있는 악성코드를 무시 하지 못할 것으로 보인다. 결과적으로 전 세계의 악성코드 동향은 비슷하지만 지역 차이가 약간은 존재함을 알 수 있다.

20) Win32/Antinny.worm.651264 : http://info.ahnlab.com/smart2u/virus_detail_1212.html

# V 2003년 테크니컬 컬럼

## 1. 취약점과 악성코드

작성자 : 차민석 연구원(jackycha@ahnlab.com)

### ■ 취약점이란

취약점(Vulnerability)은 취약성으로도 해석되며 텀즈(http://www.terms.co.kr)에 따르면 다음과 같이 정의된다.

> " 취약성이란 운영체계나 시스템 소프트웨어 또는 응용소프트웨어 컴포넌트가 지니고 있는 보안상의 문제점이나 허점을 말한다. 이러한 취약성을 가지고 있는 시스템이나 네트웍은 외부의 침입에 대해 큰 손상을 입을 잠재 위험이 있다. 보안 전문 회사들은 이를 위해 소프트웨어 버전 별로 취약성 데이터베이스를 유지하기도 한다. "

외부 침입을 쉽게 할 수 있는 약점이라고 이해하면 된다. 일반적으로 취약점은 해킹에서 관리자 권한을 얻기 위해 사용되었지만 최근 바이러스나 웜 같은 악성코드에서도 전파를 손쉽게 하기 위하여 취약점을 이용하고 있다.

### ■ 취약점의 위험성

일반적인 바이러스나 웜의 감염 경로는 메일에 첨부된 파일 실행, 프로그램 다운로드 후 실행 등 대부분 사용자가 실행 파일을 실행할 때 감염되는 경우가 대부분이다. 하지만, 취약점은 사용자가 감염되기 위해 특별한 행동을 하지 않아도 메일 확인이나 취약점이 있는 프로그램을 사용하는 것만으로도 감염된다. 즉, 사용하는 윈도우나 리눅스 같은 운영체계 구성 파일 중 취약점이 존재하고 인터넷으로 외부와 연결되어 있다면 컴퓨터를 켜고 인터넷에 연결되어 있는 것만으로도 웜이나 바이러스 같은 악성코드에 감염될 수 있는 것이다. 2003년 8월 발생한 블래스터 웜이 대표적이다.

### ■ 취약점을 이용한 악성코드의 역사

취약점을 이용해 전파되는 악성코드는 웜이 절대적으로 많다. 바이러스의 경우 개인용 컴퓨터에서 시작되었고 MS-DOS 환경에서는 디스켓 등이 주요 감염 수단이므로 해당 시스템의 많은 파일을 감염시켜 외부로 파일이 전파되도록 노력했고 사용자가 곧 관리자이므로 별도의 관리자 계정을 얻기 위한 노력이 필요 없었다. 하지만, 유닉스나 리눅스는 관리자와 사용자가 구별되고 사용자 권한에서 웜이나 바이러스를 실행해도 사용자 권한 외 파일 감염에는

한계가 있어 이들 시스템을 감염시키기 위해 관리자 권한이 필요하고 이에 취약점이 이용되었다.

취약점을 이용한 웜의 역사는 바이러스 역사만큼 오래되었다. 성공적으로 널리 퍼지고 유명한 웜 중 1988년 발생한 모리스 웜은 당시 시스템의 취약점을 이용해 전파되었다. 불과 몇 년 전만해도 취약점을 이용해 전파되는 웜은 일반적으로 유닉스 혹은 리눅스 환경에서 활동했다. Linux/Ramen[1]은 레드햇 리눅스 6.2나 7.0의 취약점을 이용하며 Linux/Slapper.worm[2]은 리눅스 플랫폼의 아파치 웹 서버의 OpenSSL 취약점을 이용해서 확산되었다.

1996년 이후 윈도우가 널리 사용되고 인터넷 붐과 함께 개인용 컴퓨터의 인터넷 연결도 점차 증가했다. 서서히 윈도우에서도 취약점을 이용한 악성코드가 발견되었지만 이들은 대부분 특정 애플리케이션의 취약점을 이용한 것으로, 접근 방법도 스크립트 등으로 어느 정도 제한적이고 사용자가 메일을 확인하거나 웹 사이트 방문 등의 행동이 필요했었다.

하지만, 2001년 여름 코드레드 웜(Code_Red)이 널리 퍼졌고 코드레드 웜은 파일 형태로 존재하지 않고 기억장소에만 존재해 백신으로 진단/치료하는데  한계를 드러냈다.  2003년 1월 25일 SQL 서버의 취약점을 이용한 SQL_Overflow(일명 슬래머웜, SQL웜)이 전 세계로 퍼지면서 많은 피해가 발생했고 우리나라에서는 인터넷이 불통되는 초유의 사태를 맞이하게 되었다. 코드레드 웜이나 SQL_Overflow 웜이 서버급 시스템을 감염시켰다면 2003년 8월 12일 발생한 블래스터 웜은 윈도우 2000/XP의 RPC DCOM 취약점을 이용해 개인용과 서버 윈도우를 모두 감염시켜 개인용 시스템도 인터넷에 접속만 되어 있으면 악성코드에 감염되는 새로운 시대가 열렸다.

## ■ 취약점을 가진 프로그램

버그가 없는 프로그램이 없듯이 취약점은 많은 프로그램에서 발견되고 있다. 윈도우나 리눅스에 기본적으로 포함된 프로그램 뿐 아니라 일반적으로 사용되지 않는 프로그램에서도 취약점이 발견되며 심지어 보안 제품에서도 취약점이 발견되고 있다.

윈도우 계열에서 발견된 주요 프로그램의 취약점과 이를 악용한 악성코드에 대해 알아보자. 그리고, 보통 이런 치명적인 취약점들은 윈도우 버전이 올라가면서 자동으로 해결되므로 오래된 취약점은 최신 버전의 윈도우에는 적용되지 않는다.

---

1) Linux/Ramen : http://info.ahnlab.com/smart2u/virus_detail_784.html
2) Linux/Slapper.worm : http://info.ahnlab.com/smart2u/virus_detail_1030.html

(1) 아웃룩/아웃룩 익스프레스

1999년 11월 이전까지는 메일을 읽는 것만으로는 바이러스에 감염되지 않는다는 정설이었다. 하지만, 이런 상식을 깨고 패치 적용이 안된 아웃룩 익스프레스로 메일을 읽어보는 것만으로도  감염되는 VBS/BubbleBoy[3]가 발견되었다. 이후 발생한 JS/Kak[4]도 같은 취약점을 이용하는데 이는 HTML 형식의 메일을 읽을 때 내부에 포함된 위험한 행동을 시도하는 스크립트의 행동을 제어하지 못하기 때문에 발생한다. 즉, 로컬 파일 접근, 시스템 자원 접근 등은 제한된 스크립트 행동이지만 이 행동을 아웃룩 익스프레스에서 제한하지 못하고 사용자 동의 없이 자동으로 실행되는 것이다.
이후에도 아웃룩과 아웃룩 익스프레스는 여러 취약점이 발견되었다. 주로 이들 메일 프로그램으로 미리보기를 할 경우 사용자 동의 없어 내부에 포함된 스크립트가 자동 실행되거나 첨부파일이 자동으로 실행되는 문제가 발생했다.

이에 마이크로소프트사는 아웃룩이나 아웃룩 익스프레스에서 메일을 볼 때 확장자에 따라 첨부파일을 아예 열어보지 못하거나 액티브 X 컨트롤러의 사용을 제한하는 방법을 사용하게 되었다. 하지만, 윈도우와 포함된 아웃룩 익스프레스는 인터넷 익스플로러와 여러 기능을 같이 사용하므로 인터넷 익스플로러의 취약점이 존재해도 영향을 받을 수 있다.

(2) 인터넷 익스플로러

이 글을 작성하는 시점에도 인터넷 익스플로러의 보안취약점을 해결한 업데이트(MS03-040)가 공개될 만큼 인터넷 익스플로러의 보안취약점도 계속 발견되고 있다. 아웃룩/아웃룩 익스프레스와 유사하게 HTML 문서를 읽을 때 포함된 스크립트가 사용자 동의 없이 자동으로 실행되는 형태가 가장 많다.

이외에 취약점은 아니지만 사용자의 부주의도 크다. 예를 들어 인터넷 웹 사이트 방문 도중 [그림1]과 같은‘ 보안경고창 ’을 자주 접하게 될 것이다.

이 경우 제 3자가 인증서를 인증했는지 확인할 필요가 있다. 하지만, 인증서가 있다고 해서 설치되는 프로그램의 행동이 완전히 안전하다는 보장은 없다. 따라서 해당 사이트가 신뢰성이 높은 경우가 아니라면 이 프로그램을 설치하지 않는 것이 좋다.

3) VBS/BubbleBoy : http://info.ahnlab.com/smart2u/virus_detail_22.html
4) JS/Kak : http://info.ahnlab.com/smart2u/virus_detail_655.html


[그림1] 보안경고창, 발급자와 인증기관에 대한 확인 필요

인터넷 익스플로러의 취약점 중에는 사용자 동의 없이 시스템에 파일을 설치하거나 레지스트리 등에 접근하는 문제가 가장 많다. MS 가상 머신의 보안상 취약점(Microsoft VM ActiveX Component)이 가장 유명하며JS/Fortnight[5] 등이 이런 취약점을 이용해 자동 실행되고 아웃룩 익스프레스와 같은 메일 프로그램의 서명에 묻어 전파된다.

(3) IIS 서버

아웃룩/아웃룩 익스프레스와 인터넷 익스플로러는 보통 개인사용자에 해당하는 보안 취약점이다. 하지만, IIS 서버의 경우 웹 운영에 사용되는 웹 서버로 주로 회사에서 사용된다. 현재 많은 기업이나 단체가 IIS 서버로 웹 서비스를 운영하고 있으며 IIS 서버에 취약점이 존재해 공격 받을 경우 홈페이지 내용 변경, 서버에 보관된 자료 손상 등의 문제가 발생한다.

IIS 서버 취약점 중 가장 잘 알려진 취약점은 MS01-033[6]과 MS01-044[7] 등으로 코드레드 웜과 님다 바이러스에서 사용되었다.

홈페이지 내용 변경은 일반적인 해킹에서도 자주 사용되며 자신들의 생각을 표현하는 방법으로 사용되기도 한다. Solaris/Sadmind.worm이 취약점이 있는 IIS 서버의 홈페이지 내용을 변경하는데, 변경된 홈페이지를 HTML/Sadmind[8]로 부르며 특정 국가를 비난하는 내용을 담고 있다.

5) JS/Fortnight : http://info.ahnlab.com/smart2u/virus_detail_1182.html
6) MS01-033 : http://www.microsoft.com/korea/technet/security/bulletin/MS01-033.asp
7) MS01-044 : http://www.microsoft.com/korea/technet/security/bulletin/MS01-044.asp
8) HTML/Sadmind : http://info.ahnlab.com/ smart2u/virus_detail_822.html


[그림2] HTML/Sadmind에 감염된 화면

(4) SQL 서버

SQL 서버는 데이터베이스 서버로 몇 가지 취약점이 웜에 악용되고 있다. 주로 비밀번호 없이 사용되는 시스템과 SQL_Overflow(SQL슬래머) 웜에서 사용된 SQL 서버 2000 확인 서비스 내의 버퍼 오버런이 코드 실행을 허용하는 문제(MS02-039)[9]이다.

비밀번호가 없는 시스템은 보통 사용자들이 비밀번호를 넣기 귀찮아 엔터 키를 비밀번호로 지정해서 발생하는 문제점이며, SQL 서버 2000 확인 서비스 내의 버퍼 오버런이 코드 실행을 허용하는 문제는 SQL 서버 2000의 구조적인 문제점이다. 버퍼 오버런이 코드 실행을 허용하는 문제는 2002년 여름에 취약점 패치가 나왔지만 패치를 적용하지 않는 시스템이 많아 2003년 1월 25일 SQL 오버플로우 웜으로 이른바 ' 1.25 인터넷 대란 ' 이 발생했다.

(5) 플래쉬 플레이어

매크로미디어(Macromedia)사의 플래쉬 플레이어(Flash Player)는 플래쉬 무비로 잘 알려진 프로그램으로 인터넷에서 동영상 등에 사용되고 있다. SWF 파일은 플래시 파일로 사용되는데 이 파일에 포함된 스크립트가 시스템에 접근 할 수 있는 문제가 발견되었다. 2002년 1월 8일 완벽하지 않지만 플래시 파일을 감염시키는 SWF/LFM.926[10] 바이러스가 발견되었다. 다행히 웹 브라우저를 통해 볼 때는 감염되지 않고 플래쉬 제작 프로그램이나 전용 재생기 등으로 감염된 파일을 열어봤을 때만 감염된다. 매크로미디어사는 취약점을 해결한 새로운 버전을 제공했다. (http://www.macromedia.com/support/flash/ts/documents/swf_clear.htm)

9) MS02-039 : http://www.microsoft.com/korea/technet/security/bulletin/MS02-039.asp
10) SWF/LFM.926 : http://info.ahnlab.com/smart2u/virus_detail_909.html

(6) RPC DCOM

윈도우 NT 계열(2000/XP 포함)의 개인용, 서버용 윈도우에 취약점이 발견되었다. RPC DCOM 취약점(MS03-026)으로 부르며 안철수연구소에서도 7월 17일부터 보안 패치를 권고했었고 7월 말 취약점 공격 코드 등장 후 취약점 공격 프로그램을 분석하여 웜의 등장을 예고했었다.

하지만, 여전히 많은 사용자들이 윈도우 업데이트 적용을 모르거나 무시했고 8월 초부터 RPC DCOM 취약점을 이용한 웜들이 조금씩 등장하고 있었다. 감염된 컴퓨터 수가 적고 사용자들이 별다른 증상을 느끼지 못했을 뿐이다.

2003년 8월 12일 새벽(한국 시간 기준) 발견된 블래스터 웜(Win32/Blaster.worm.6176)이 급속히 퍼지면서 많은 피해를 줬다. 블래스터 웜은 이전에 공개된 RPC DCOM 취약점 공격 프로그램의 소스를 수정해 웜으로 만들었으며 윈도우 XP에 감염을 시도할 때 종종 시스템을 재부팅 시키는 버그가 있어 피해가 컸다. 만약 윈도우 XP를 재부팅 시키는 버그가 없었다면 사용자는 본인의 시스템이 감염되었는지 인식하지 못한 채  지냈을 지도 모른다.

2003년 8월 18일 웰치아 웜(Win32/Welchia.worm.10240)도 RPC DCOM 취약점을 이용하며 근접해 있는 시스템을 감염 시키므로 동일 네트웍 망에 순식간에 퍼진다. 특히 웰치아 웜은 캐나다의 모 항공사의 시스템을 다운시켜 비행기 이착륙에 문제가 발생했으며 국내의 모 은행에서도 피해를 입혀 은행 업무 중단의 사태가 발생했다.

## ■ 취약점 해결법

취약점 해결 방법은 크게 세가지다.

첫째, 해당 프로그램/서비스 사용 중지
둘째, 취약점 방어 프로그램 사용
셋째, 취약점 패치 적용

첫째 방법인 해당 프로그램/서비스 사용 중지는 정상적인 일을 할 수 없으므로 업무 중단 등의 문제가 발생할 수 있다. 둘째 방법인 해당 취약점 방어 프로그램을 이용하면 해당 취약점을 이용한 공격을 막을 수 있지만 프로그램에 따라 특정 공격 형태만 막는 경우도 있다. 예를 들어 취약점 방어 프로그램이 특정 웜의 공격 형태만 예방 가능하지만 같은 취약점을 공격하는 다른 웜의 공격 방식은 예방할 수 없는 경우도 발생한다. 셋째 방법인 취약점 패치 적용은 해당 취약점 자체를 없애므로 가장 좋은 방법이지만 취약점 패치 적용 후 시스템 오동작 등의 문제가 발생할 수 있다. 특히 서버의 경우 패치나 서비스 팩 설치에 신중할 수 밖에 없다.

## ■ 변화

과거 바이러스의 감염 경로는 플로피 디스크였고 PC 통신의 발전으로 공개 자료실을 통해 바이러스가 퍼지는 경우가 많았다. 이후 인터넷 사용이 폭발적으로 증가하면서 뉴스그룹, 자료실, 메일 등으로 전파 속도는 계속 빨라졌다. 컴퓨터들이 네트웍으로 묶이면서 바이러스나 웜이 하나의 시스템에 감염되면 연쇄적으로 주위 컴퓨터들이 감염되었다. 하지만, 이 경우도 사용자들이 메일을 열어보거나 특정 웹 사이트 방문이나 공유 폴더 등의 사용과 같이 사용자의 액션이 있을 경우에 감염되었지만, 이제 인터넷에 컴퓨터가 접속만 되어 있으면 감염되는 시대가 도래했다. 취약점을 이용한 공격은 일반적으로 해킹 분야였지만 최근 바이러스와 해킹의 경계가 모호해지면서 바이러스 연구가들도 새로운 취약점이 나올 때마다 바이러스나 웜에서 악용 가능한지 분석하는 일이 잦아졌다. 사용자들도 바이러스나 웜에 감염되는 것을 예방하기 위해서 최신 백신 사용 뿐 아니라 보안 패치 적용까지 해야 한다.

현재 PDA나 휴대폰 같은 모바일 뿐 아니라 일반 가전 제품도 인터넷 연결이 시도되고 있다. 미래에는 인터넷에 연결된 기기들에 취약점이 존재해 인터넷을 통해 전파되는 바이러스나 웜 같은 악성코드가 등장할 가능성도 높다.

개발 회사는 취약점을 최대한 줄인 제품을 개발해야 할 것이고 보안전문가 들이 새로운 취약점을 계속 발견하고 발표하면 언론 등에서 이 내용을 사용자들에게 잘 알리고 사용자들도 최신 패치를 적용한 제품을 사용해야 할 것이다. 하지만, 이 모든 일이 순조롭게 이뤄지는 건 어려우며 앞으로도 취약점을 이용하여 제작되는  악성코드의 등장은 증가할 것이다.

## ■ 참고자료

- 안철수연구소 바이러스 정보
  (http://info.ahnlab.com/securityinfo/virus_search.jsp)
- 텀즈(http://www.terms.co.kr)

## 2. 애드웨어란

작성자 : 차민석 연구원(jackycha@ahnlab.com)

컴퓨터 사용 중 갑자기 광고 팝 업 창이 뜨거나 인터넷 익스플로러 실행 시 홈페이지가 성인 사이트나 자신이 선택하지 않은 웹 사이트로 고정되고 홈페이지를 변경해도 다시 변경되는 문의가 많이 들어오고 있다.
웜이나 바이러스 등과 같은 악성코드가 홈페이지를 변경하는 경우도 있지만 흔히 스파이웨어(Spyware)로 알려진 애드웨어(Adware)로 발생하는 문제이다.
애드웨어는 제한 없이 무료로 사용되는 프리웨어(Freeware), 일정한 금액으로 제품을 사야 하는 셰어웨어(Shareware) 같이 광고를 보면 사용할 수 있는 프로그램을 뜻하지만 광고를 보여주는 프로그램이라는 의미로도 사용된다.

여기서 애드웨어는 지속적으로 광고를 내보내는 프로그램으로 정의하고 현재 파악된 애드웨어는 일반적으로 다음과 같은 증상을 보인다.

1) 인터넷 사용 중 어떤 사이트에 방문하거나 메일을 확인하는 도중 성인관련 스팸메일을 읽고 난 이후부터 성인 광고 창이나 특정 광고 팝 업 창이 뜸.
2) 홈페이지 시작페이지가 변경됨. 시작페이지를 변경해도 다시 바뀜.
3) 컴퓨터 사용 중 성인 팝 업 창이 뜸.
4) 작업표시줄에 광고 창이 자동으로 떠 있음.
5) 인터넷 연결 시 다른 인터넷 익스플로러 창이 항상 같이 열림.

현재 애드웨어의 문제점으로는 광고의 지속성이다. 즉, 사용자가 홈페이지 변경을 해도 어느 순간 자신이 원하지 않는 특정 사이트로 변경되는 것이 일반적인 사람들의 고민이고 특히 성인 사이트일 경우 무척 곤란해진다.

### ■ 스파이웨어란? 애드웨어란?

많은 사람들이 스파이웨어와 애드웨어가 같은 것으로 오해하고 있다. 흔히 스파이웨어로 알려진 애드웨어는 사용자 정보를 유출하는 프로그램으로 알려져 있다. 하지만, 대부분의 애드웨어는 사용자 정보를 유출하지 않고 광고만을 보여준다. 스파이웨어라는 용어가 사용되면서 잘못 알려진 상식 중에 하나이다. 현재 스파이웨어로 분류하는 기준이 명확하지 않다. 실제 보안 업체마다 스파이웨어[1]에 대한 정의는 조금씩 다르다.
여기서 스파이웨어를 개인 정보를 사용자 몰래 유출시키는 프로그램이라고 정의할 때 애드웨어는 사용자 정보를 직접적으로 유출하지 않으며, 애드웨어는 보통 광고 서버에 접속해 광고를 가져오고 사용자에게 보여주거나 홈페이지를 특정 사이트로 고정하는 일을 할 뿐이다.

애드웨어는 전문 소프트웨어 업체에서 제작되며 광고주에게 돈을 받고 프로그램을 제작하고 있다. 실제 애드웨어를 제작하는 회사의 홈페이지를 참고하면 광고주에게 월 16만 5천원을 받으며 노출당 0.5원, 키워드 입력 시 팝 업 광고 노출은 키워드 당 월 9,900원 정도로 책정되어 있었다.

간혹 애드웨어가 스파이웨어로 오해 받는 경우가 있는데 가장 대표적인 경우가 Aureate/Radiate[2]이다. Aureate/Radiate사의 애드웨어는 여러 프로그램에 내장되어 광고를 보여주는 기능을 한다. 하지만, 이 기능에 사용자 정보를 빼간다는 주장이 있었다. 이후 이 내용은 사실과 아님이 밝혀 졌고 백신 회사에서는 이들 프로그램을 악성코드로 분류하지 않는다고 발표했다. 하지만, 일부 스파이웨어 진단 프로그램은 여전히 해당 프로그램을 개인정보의 유출 가능성 때문에 스파이웨어로 분류해 진단하고 있다. 이외 Dlder 프로그램[3]처럼 스파이웨어로 오해 받는 애드웨어도 존재한다.

또한 애드웨어 제작 회사의 홈페이지[4]에는 개인 정보는 빼가지 않는다고 명시되어 있다.

## ■ 백신업체 정책

백신 업체는 현재까지 애드웨어를 바이러스, 웜, 트로이목마와 같은 악성코드로 분류할지에 대해 여전히 논의 중이다. 몇몇 백신 프로그램에서 사용자가 선택할 경우 애드웨어 등을 진단하는 정책을 채택하고 있지만 특정 업체에서만 시행하고 있다.

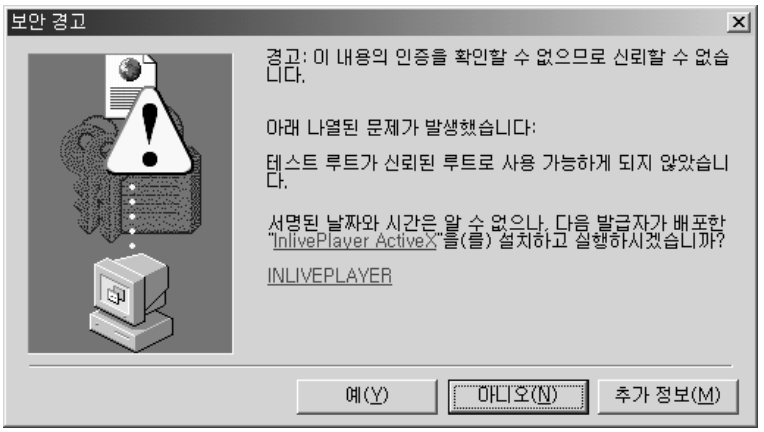
애드웨어는 크게 두 가지 측면에서 트로이목마로 분류하기 어렵다.

첫째, 사용자 동의를 얻어 설치되는 프로그램을 임의로 진단할 수 있는가?

논란의 여지가 있지만 보통 애드웨어는 보통 사용자의 동의를 얻어 설치된다. 하지만, 일반적으로 ' 보안 경고 ' 만으로는 설치되는 프로그램이 광고를 출력하는 애드웨어인지 알 수 없다. 혹은 광고 목적으로 사용된다고 약관에 명시되지만 긴 약관을 제대로 읽어 보는 사용자도 거의 없을 뿐 아니라 일부 사이트는 프로그램을 설치하지 않으면 정상적인 사이트 이용을 어렵게 해 보안 경고 시 ' 예 ' 를 눌러 프로그램을 설치한다.
하지만, [그림1]과 같이 신뢰할 수 없는 경우도 존재한다.

---

1) 스파이웨어 정의 : http://messenger.freechal.com/FcVaccine/FcVacFastType.asp
2) http://grc.com/oo/aureate.htm,
http://www.kaspersky.com/news.html?id=16
http://vmyths.com/hoax.cfm?id=36&page=3
http://www.europe.f-secure.com/v-descs/aureate.shtml
3) http://www.europe.f-secure.com/v-descs/dlder.shtml
http://www.europe.f-secure.com/v-descs/dlder.shtml
4) http://www.flashtrack.net/policy.html




[그림1] 보안경고창이 활성화된 화면

둘째, 홈페이지를 바꾸고 광고를 출력하는 것이 악의적인 일로 볼 수 있는가?

웜이나 바이러스는 자기 복제 행동 때문에 백신에서 진단/치료(삭제)를 하지만 자기 복제 기능이 없는 프로그램의 경우 어떤 프로그램을 트로이목마로 분류한지 의견이 분분하다. 특히 취약점 분석 프로그램 같이 사용하는 사람에 따라 취약점을 찾는 목적으로도 해킹을 위한 목적으로도 사용될 수 있다. 애드웨어의 경우 광고를 보여주고 홈페이지를 특정 사이트로 고정시키는 행동을 악의적으로 볼지는 의견이 다양하다.

물론 이들 애드웨어가 사용자 동의 없이 설치되거나 개인 정보를 빼가는 행위가 증명되면 이들은 트로이목마로 분류되어 백신에서 진단/치료(삭제)된다.
이런 두 가지 문제로 현재까지 애드웨어는 백신에서 기본으로 진단하지 않으며 일부 백신에서 선택적으로 진단하며 사용자가 수동 삭제하거나 전용 진단 프로그램을 사용해야 한다. 스파이웨어 전용 진단 프로그램에 대해서는 스파이웨어 진단 프로그램의 유의점을 참고하기 바란다.

## ■ 증상별 분류

애드웨어가 설치되었을 때 나타나는 증상은 몇 가지 있으며 이중에 특정 사이트(특히 성인 사이트)로 홈페이지를 고정하는 문제가 가장 사람들이 곤란해 하고 있다.

(1) 광고 창이 닫히지 않음

가장 초기에 등장한 광고 방식 중 하나가 특정 사이트를 닫으면 계속해서 광고 창이 뜨는 것이다. 보통 스크립트를 사용했고 창을 계속 닫거나 익스플로러를 종료하면 종료된다. 이런 악성 스크립트 중 일부를 HTML/NoClose[5]로 진단한다.

5) http://info.ahnlab.com/smart2u/virus_detail_987.html

(2) 특정 홈페이지 고정

가장 많은 광고 방법 중 하나로 인터넷 익스플로러의 홈페이지를 특정 사이트로 고정한다. 사용자가 다시 원래 홈페이지로 고정해도 사용자 컴퓨터에 설치된 애드웨어가 다시 지정된 홈페이지로 변경하므로 애드웨어 자체를 찾아 지워 줘야 한다. 특정 홈페이지 고정의 경우 성인 사이트 등이 많아 사람들이 곤란해 하는 경우가 많다.

(3) 일정 시간 간격으로 광고 창 띄움

일정 시간 단위로 광고 서버에서 정보를 받아 설치자 컴퓨터에 광고 창을 띄운다. 애드웨어 종류에 따라 사용자가 컴퓨터 사용을 하지 않는 시간에 띄우기도 하지만 대부분 정상 작업 중에 광고 창을 띄워 컴퓨터 작업을 방해 할 수 있다

(4) 특정 주소를 입력하면 광고주가 원하는 팝 업

인터넷 익스플로러의 내용을 가로채 특정 주소를 입력하면 특정 사이트로 접속하는 것이다.

(5) 특정 한글주소를 입력하면 광고주가 원하는 광고 띄움

최근 웹 브라우저에서 한글 주소 입력이 가능한데 특정 한글 주소를 입력하면 특정 사이트로 유도 할 수 있다. 고객에게 온 문의 중 하나가“ 꽃 ”을 입력하면 경쟁사 홈페이지로 뜬다는 내용도 있었다.

## ■ 설치 형태별 분류

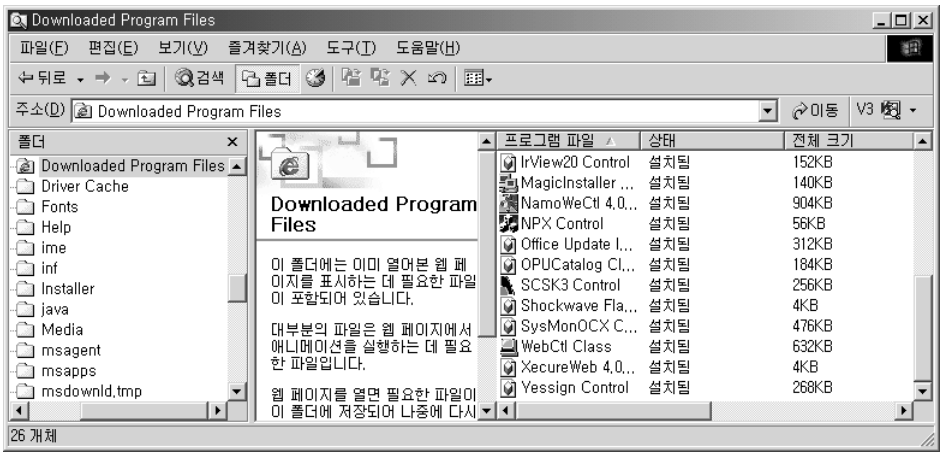
(1) 스크립트

초기의 애드웨어는 VB 스크립트나 HTA 확장자를 가진 프로그램을 HTML 등에 추가해 특정 홈페이지 광고가 뜨게 했다. 혹은 창이 닫힐 때 시작하는 스크립트 등을 넣어 사용자가 창을 닫을 때 지속 적으로 광고가 뜨게 한다. 보통 성인 사이트나 와레즈 사이트에서 많이 볼 수 있다. 하지만, 이런 스크립트는 웹 브라우저를 종료하면 실행되지 않는 등 광고의 지속성에서 미흡하다.

(2) 실행 파일

Active X 컨트롤을 이용해 사용자의 컴퓨터에 광고 프로그램을 몰래 설치한다. 여러 경로로 애드웨어를 배포할 수 있지만 보통 스팸 메일이나 특정 웹 사이트를 통해 프로그램을 설치하도록 유도한다. 일반적인 사용자는 해당 사이트를 이용하게 위해 필요한 프로그램으로 인식해 설치하는 경우가 많다.

보통 이들 프로그램은 윈도우 폴더(일반적으로 C:\Windows 나 C:\WINNT)의 Downloaded Program Files 폴더에 설치된다.([그림2] 참조)




[그림 2]윈도우 폴더의 Downloaded Program Files 폴더에 설치된 화면

(3) DLL 파일

ActiveX 컨트롤을 통해 설치되는 애드웨어는 사용자가 쉽게 삭제할 수 있어 컴퓨터를 조금만 할 줄 알면 쉽게 제거가 가능하다. 이에 애드웨어 제작자들은 다른 EXE 파일을 이용하는 DLL 파일을 이용하기 시작했다. DLL 파일을 EXE 파일에 연동시키면 해당 EXE 파일을 종료하기 전에는 DLL 파일을 삭제할 수 없다. 따라서, 시스템 사용에 꼭 필요한 시스템 파일에 DLL 파일을 연동해 파일 삭제를 어렵게 하는 방법을 사용한다. 이 때 제거를 위해서 사용자는 실행 중인 실행 프로세스를 모두 종료시켜 DLL 파일을 삭제하거나 DLL 파일의 확장자를 변경해 재부팅 후 해당 DLL 과 관련 ActiveX 컨트롤을 삭제해야 한다.

## ■ 애드웨어 설치 경로

애드웨어는 여러 경로를 통해 사용자의 컴퓨터에 설치된다. 보통 스팸 메일, 웹 사이트 방문 시 설치, 웹 사이트 방문 시 취약점을 이용해 자동 설치, 자기 복제가 가능한 웜, 바이러스 형태의 애드웨어가 존재한다. 백신에서 기본적으로 진단/삭제하는 애드웨어는 취약점을 이용해 설치되는 형태와 웜, 바이러스이다.

(1) 스팸 메일

애드웨어 제작자들은 스팸 메일 속에 애드웨어의 설치 주소를 삽입해 사람들에게 발송한다. 사용자가 스팸 메일을 읽을 때 프로그램을 설치하려고 사용자에게 경고 창이 뜨지만 많은 사용자들이“ 예 ”를 눌러 프로그램을 설치 한다.

(2) 웹 사이트 방문

특정 웹 사이트에 방문 했을 때 필요한 기능을 제공하기 위해 프로그램을 설치하는 경우가 있다.

이런 팝 업 광고 서비스는 정보통신법 36제 50조의 5항[6]의 법규를 준수하고 있다고 한다. 하지만, 프로그램 설치 시 보통 해당 사이트나 제작 프로그램의 제작사의 신뢰를 요구하지 정확히 해당 프로그램이 어떤 일을 하는지 알려주는 경우는 드물어 사용자는 해당 사이트의 서비스를 받기 위해 프로그램을 설치하는 경우가 많아 애드웨어 인지 모르고 설치하는 경우가 많다.

(3) 취약점 이용

취약점을 이용해 사용자에게 최소한의 동의 없이 애드웨어가 설치되는 경우도 있다. 이 경우 백신에서는 트로이목마로 간주해 백신에서 진단/치료(삭제)를 한다. 단, 단순히 애드웨어가 설치되었을 경우 사용자 동의를 구하는지 혹은 취약점을 이용해 자동 설치되었는지 확인할 방법이 어렵다.

(4) 자기 복제 애드웨어

자기 복제 능력이 있는 애드웨어는 엄밀히 말해 일반적인 바이러스나 웜에 포함되므로 백신 프로그램에서 진단/치료(삭제)가 기본적으로 추가된다. 아웃룩 익스프레스로 퍼지는 JS/Fortnight 바이러스가 대표적이다.

## ■ 스파이웨어 진단 프로그램 사용시 주의점

흔히 알려진 스파이웨어 진단 프로그램 중 일부는 지나치게 넓은 범위의 프로그램을 진단하고 있다. 예를 들어 쿠키, 애드웨어 등은 기본적으로 진단하며 일부 프로그램은 프로그램 분석에 사용하는 디스어셈블러, 프로그램 오류를 수정할 때 사용하는 디버거 프로그램, 실행 파일 크기를 줄여주는 실행 압축 프로그램 등 직접적으로 사용자 정보를 유출하지 않는 프로그램도 악의적인 프로그램으로 간주해 진단하고 있다.

오진 가능성도 존재해 백신 구성 파일을 트로이목마로 오진해 파일을 삭제해 버리는 경우도 있다. 따라서, 스파이웨어 검색 프로그램으로 자신의 시스템을 진단할 때는 반드시 해당 파일을 백업하고 함부로 삭제하지 않는 것이 좋다.

## ■ 예방법

애드웨어를 예방하는 방법으로는 크게 윈도우 업데이트, 스팸 메일 삭제, 유명 사이트 위주 방문, 주기적으로 불필요한 프로그램 삭제 등이 있다.

6) " 타인의 컴퓨터에 영리 성 광고 프로그램 설치 시 본인 동의를 얻도록 의무 함 "

(1) 수시로 윈도우 업데이트를 한다.

취약점을 이용해 설치되는 애드웨어를 막기 위해서는 윈도우 업데이트를 주기적으로 해줘야 한다.

(2) 스팸 메일을 읽지 않고 삭제한다.

스팸 메일 중 일부는 애드웨어를 설치하는 기능을 포함하고 있다. 스팸 메일을 읽었을 때 수상한 프로그램을 설치하려 한다면 설치 하지 않음을 선택해 프로그램을 설치하지 않는다.

(3) 유명 사이트 위주로 방문 한다.

일반적으로 유명 사이트는 고객들의 불편을 고려해 강제로 홈페이지를 변경하거나 애드웨어 기능을 강하게 넣지는 않는다. 따라서, 신뢰성이 높은 유명 사이트 위주로 웹 서핑을 하며 성인 사이트나 와레즈 사이트는 가급적 방문하지 않는다.

(4) 액티브 X 컨트롤 설치 시 주의해 설치한다.

인터넷 웹사이트를 방문하다 보면 액티브 X 컨트롤을 설치해야 하는 경우가 있다. 이 경우 어떤 일을 하는지 미리 알아보고 꼭 필요할 때만 설치하도록 하자. 특히 성인 사이트, 와레즈 사이트에서 설치하려는 액티브 X 컨트롤은 설치 하지 않는 것이 좋다.

(5) 주기적으로 Downloaded Program Files 폴더를 확인한다

Downloaded Program Files 폴더에 설치된 프로그램을 수시로 확인해 잘 모르는 프로그램을 삭제한다. 해당 사이트 방문 시 다시 설치를 물어보므로 불필요한 프로그램을 삭제하면 된다.

## ■ 맺으며

과거 바이러스나 트로이목마가 개인용 컴퓨터의 가장 큰 문제였다. 현재 과거부터 문제된 바이러스, 웜, 트로이목마로 대표되는 악성코드뿐 아니라 사용자를 불편하게 하는 애드웨어나 사용자 개인 정보를 유출 할 수 있는 각종 프로그램이 등장하고 있다. 현재 백신 업계에서는 백신 프로그램이 어디까지 악성코드로 간주해 이들 프로그램을 진단/치료(삭제)해야 할지 논의가 활발하다. 하지만, 그전에 사용자들도 안전한 컴퓨터 사용을 생활화해야 할 것이다.