# ASEC Report 4월

® ASEC Report

2006. 5



안철수연구소의 시큐리티대응센터(AhnLab Security Emergency response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스와 보안 전문가들로 구성되어 있는 조직이다.

이 리포트는 ㈜안철수연구소의 ASEC에서 국내 인터넷 보안과 고객에게 보다 다양한 정보를 제공하기 위하여 바이러스와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

# I. 4월 AhnLab 악성코드 동향

## (1) 악성코드 피해동향

작성자: 이철수 연구원(lcstop@ahnlab.com)

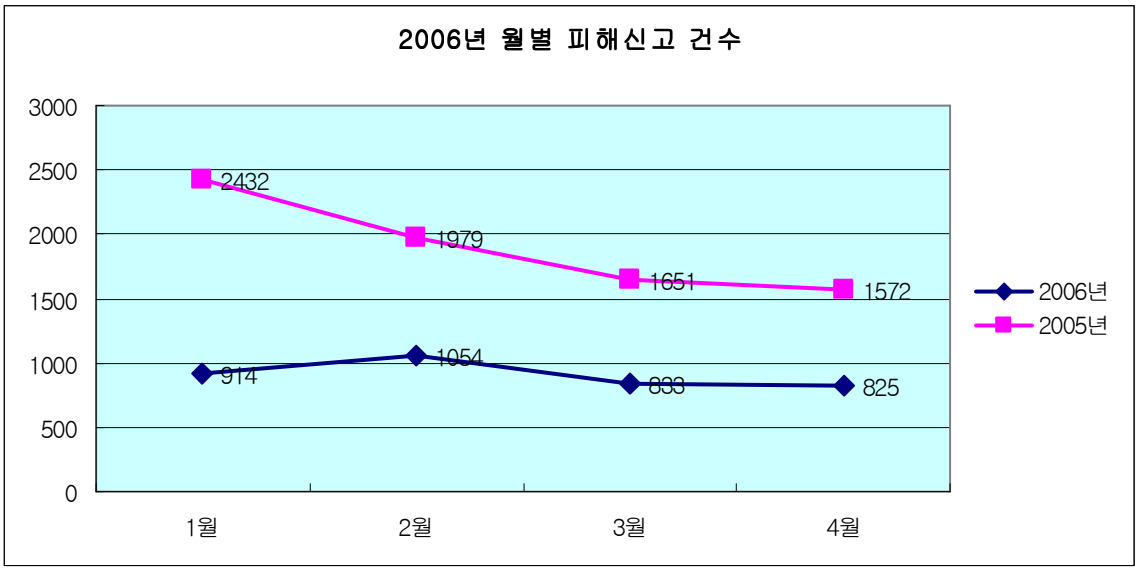
| 순 위 | | 악성코드명 | 건수 | % |
|---|---|---|---|---|
| 1 | - | Win32/Netsky.worm.Gen | 114 | 13.8% |
| 2 | new | Win-Trojan/Downloader.225597 | 35 | 4.2% |
| 3 | ↑3 | Win32/Tenga.3666 | 32 | 3.9% |
| 4 | new | Win32/Mytob.worm.48766.C | 27 | 3.3% |
| 5 | ↓1 | Win32/Bagle.worm.19666 | 19 | 2.3% |
| 6 | new | Win32/Zotob.worm.31744 | 14 | 1.7% |
| 7 | ↓4 | Win-Trojan/Downloader.38925 | 12 | 1.5% |
| 8 | ↑1 | Win32/Mytob.worm.Gen | 12 | 1.5% |
| 9 | new | Win32/Mytob.worm.51062 | 10 | 1.2% |
| 10 | new | Win32/Bagle.worm.21696 | 8 | 1.0% |
| | | 기타 | 542 | 65.7% |
| 합 계 | | | 825 | 100.0% |

[표1] 2006년 4월 악성코드 피해 Top 10

**4월 악성코드 피해 동향**

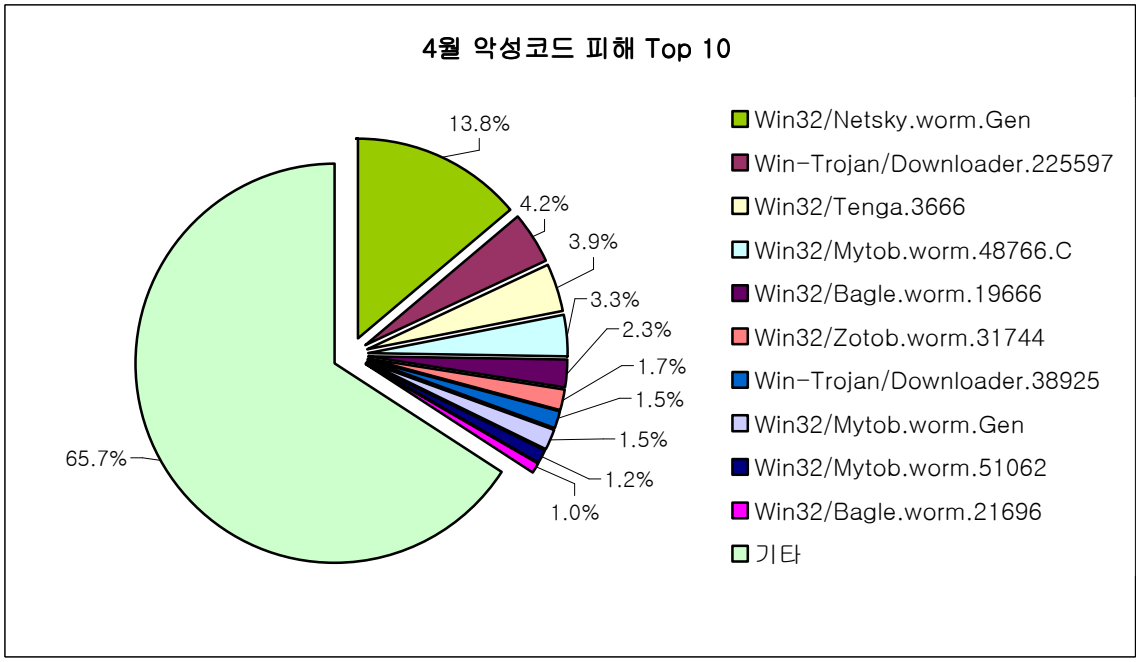
2006년 4월에는 전월에 많았던 제마.183808.B 트로이목마(Win-Trojan/Xema.183808.B), 코게임핵.11264 트로이목마(Win-Trojan/KorGameHack.11264)와 같은 트로이목마 프로그램이 악성코드 피해 Top 10 순위에 들어 있지 않다. 그 대신 날짜를 변경하는 다운로더.225597 트로이목마(Win-Trojan/Downloader.225597)가 Top 10 순위 2위를 차지하고 있으며, 2005년 8월에 발견되었던 조톱 웜(Win32/Zotob.worm.31744)이 다시 순위권에 진입하면서 6위를 차지하였다. 넷스카이 웜(Win32/Netsky.worm.Gen)은 여전히 Top 10의 순위 1위를 유지하고 있으며, 윈도우 실행 파일을 감염시키며 텡가 바이러스(Win32/Tenga.3666)는 전월 순위에서 3단계 상승하였다.

피해건수가 20건 미만인 악성코드의 수가 전체 피해통계의 74.9%에 해당하는 617건이며, 2006년 전체 피해건수는 전년도 동월에 비해 많이 감소하여, 전년 동월 1,572건의 52.5%에 해당하는 825건으로 집계되었다.




[그림1] 2006년 월별 피해신고 건수

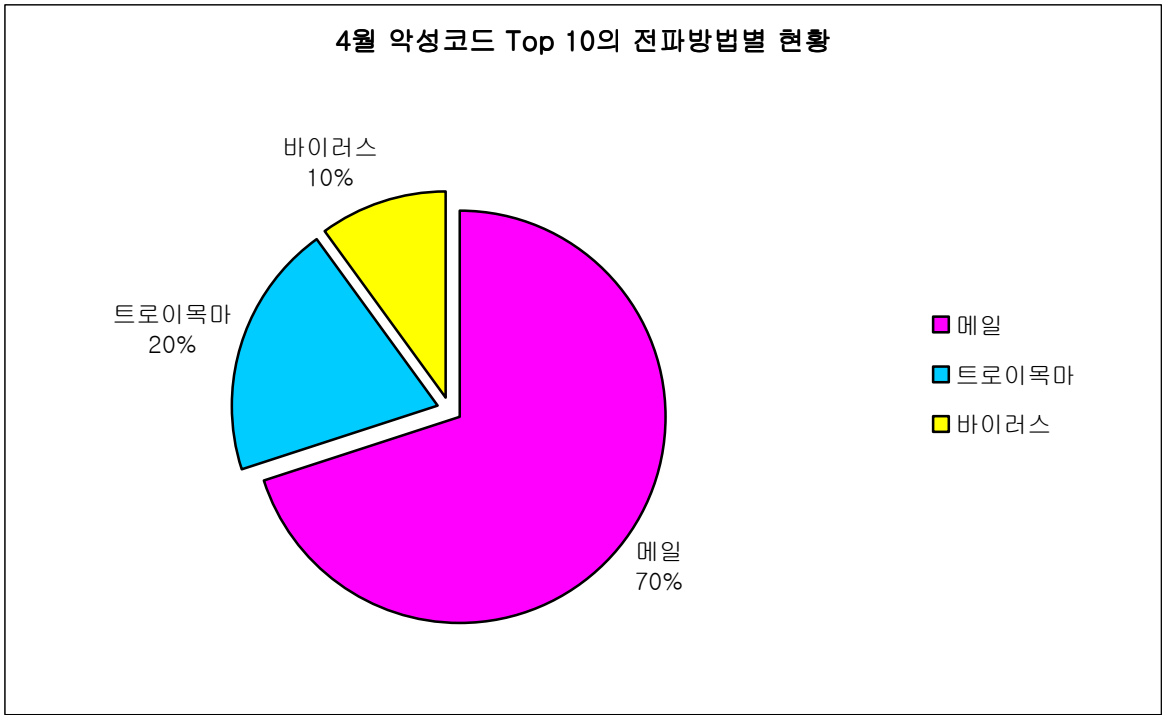
4월의 악성코드 피해 Top 10을 도표로 나타내면 [그림2]과 같다.




[그림2] 2006년 4월 악성코드 피해 Top 10

**4월 악성코드 Top 10 전파방법 별 현황**

[표1]의 Top 10 악성코드들은 주로 어떠한 감염 경로를 가지고 있는지 [그림3]에서 확인할 수 있다.

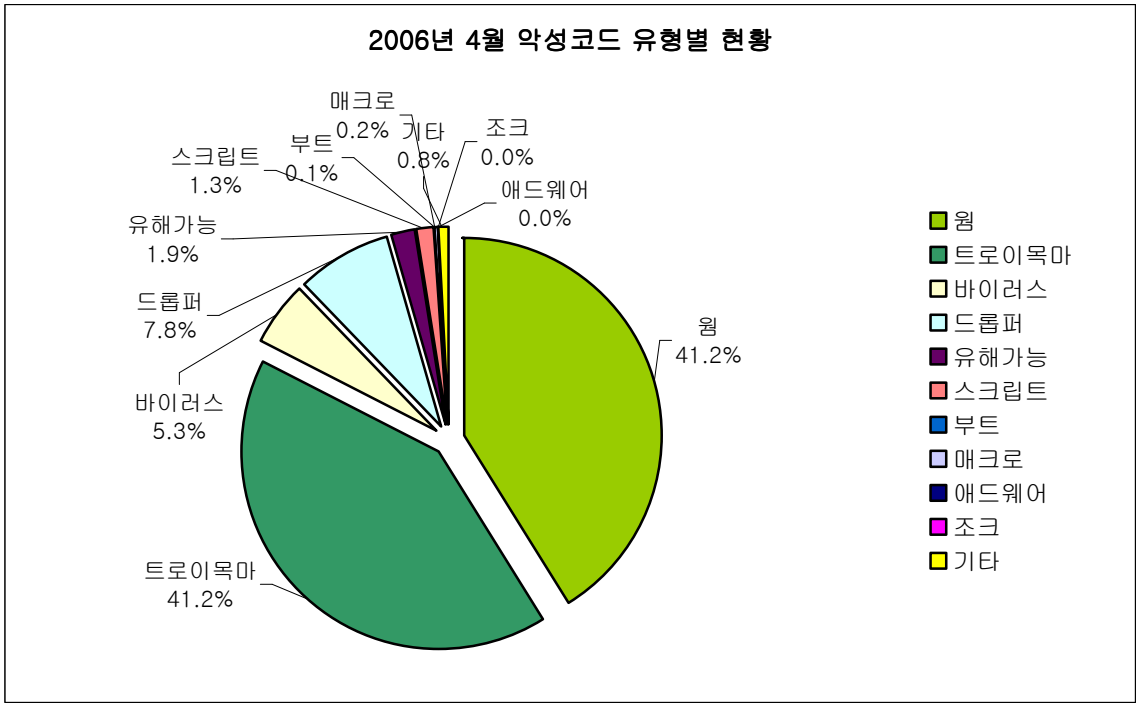



[그림3] 2006년 4월 악성코드 Top 10의 전파방법 별 현황

메일로 전파되는 특징이 있는 매스메일러는 70%, 트로이목마와 바이러스가 각각 20%, 10%를 차지했다. 3월에는 취약점, 네트워크의 특징을 이용하여 전파되는 악성코드가 각각 30%와 10%를 차지했었으나 4월에는 취약점과 네트워크를 이용한 공격은 Top 10 안에 들어 있지 않았다. 매스메일러의 경우 2006년 1월 60%에서 2월에는 50%로 10% 감소하였는데, 3월에는 40%를 차지해 또 다시 10%가 줄어드는 현상을 보였다. 1분기 동안 감소추세를 보이던 매스메일러가 Top 10에서 차지하는 비율이 4월부터 다시 증가하고 있다. 그러나 피해건수를 비교하면 지난달과 거의 비슷한 수치를 보이고 있어 앞으로의 추이를 좀 더 지켜보아야 하겠다.

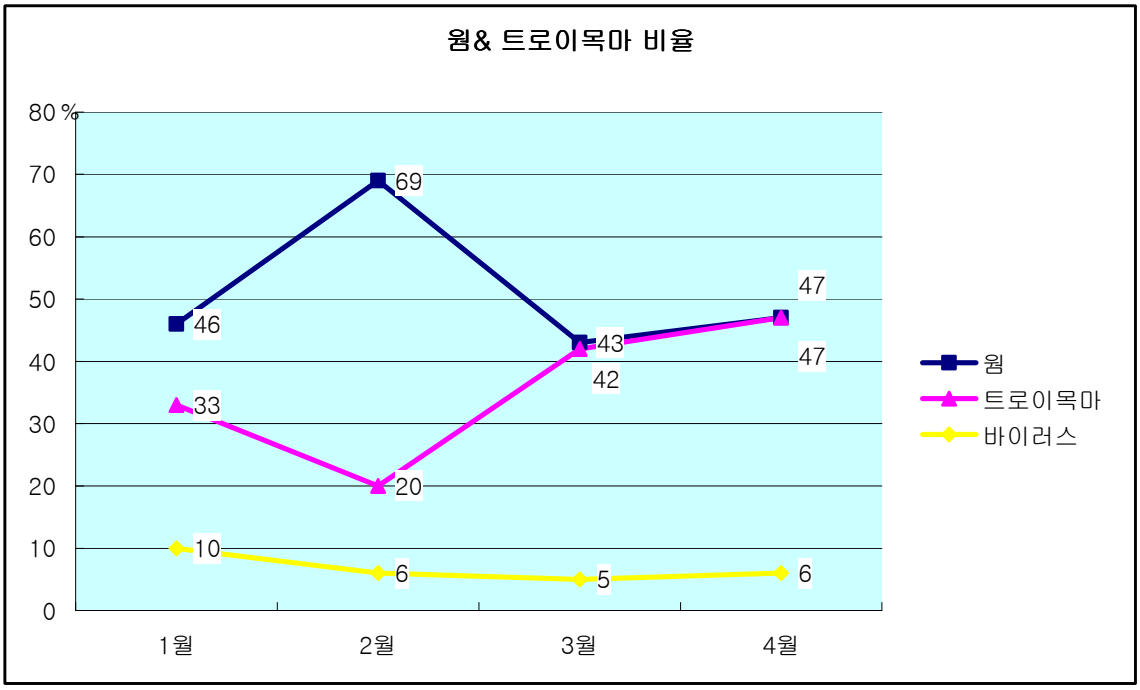
**피해신고 된 악성코드 유형 현황**

2006년 4월에 피해신고 된 악성코드의 유형별 현황은 [그림5]와 같다.




[그림5] 2006년 4월 피해 신고된 악성코드 유형별 현황

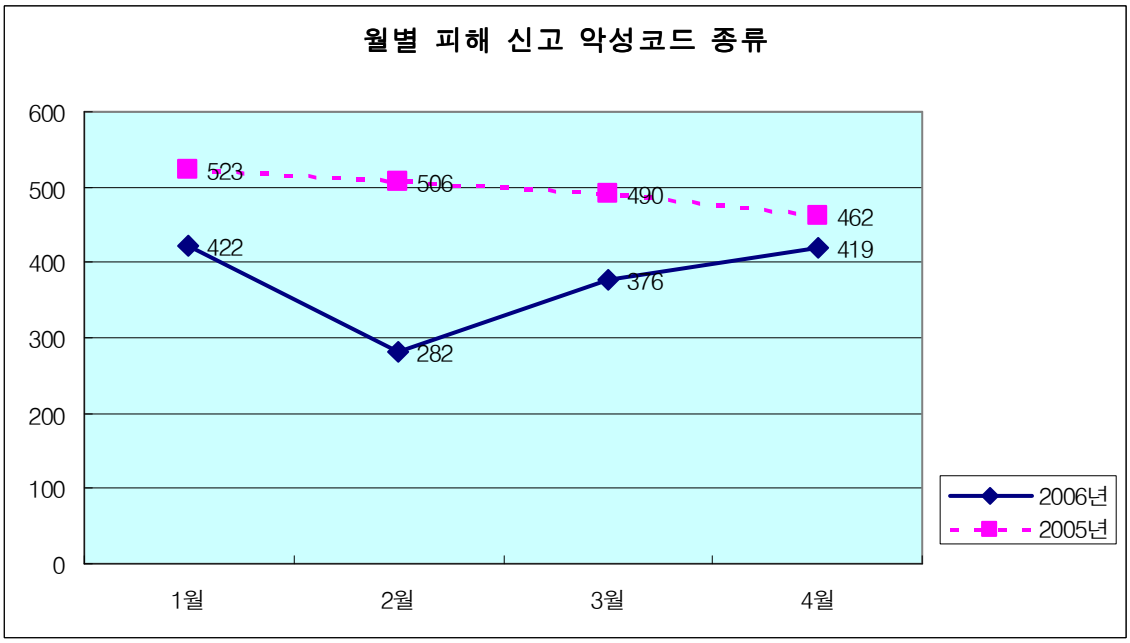
악성코드 유형에서는 웜과 트로이목마가 모두 41.2%씩을 차지하고 있는 가운데 드롭퍼와 바이러스가 각각 7.8%와 5.3%를 차지하였다. 지난해부터 트로이목마에 대한 피해가 증가추세를 보이더니 급기야 4월에는 웜과 트로이목마가 차지하는 비율이 동일하게 나타나며 트로이목마의 지속적인 증가추세를 보였다. 게임의 계정을 탈취하는 트로이목마의 피해는 전월과 비슷하나, 특정 게임의 계정을 탈취하던 이전 형태와 달리 다수의 온라인 게임의 계정을 탈취하는 형태의 트로이목마로 인한 피해는 증가하였다. 바이러스에 의한 피해는 지난달과 비슷한 비율을 보이고 있다.




[그림6] 2006년 월별 웜, 트로이목마 피해신고 비율

**월별 피해신고 된 악성코드 종류 현황**

4월에 피해 신고된 악성코드 개수는 모두 419개로, 이는 전년도 동월에 비해 43건 정도 감소한 수치이다.




[그림7] 2005년, 2006년 월별 피해신고 악성코드 개수

특정 게임사이트의 정보유출을 노리거나, 특정 사이트에 접속한 후 악성코드를 다운로드 하

는 트로이목마로 인한 피해가 4월에도 여전히 많이 발생하였다. 이런 악성코드로부터의 피해를 예방하기 위해서 악성코드의 동향에 항상 주의를 기울이며, 동시에 중요 데이터 백업과 보안 소프트웨어의 주기적인 업데이트가 중요하겠다. 아울러 좀 더 다양해진 개인정보의 유출위협에 대한 경각심을 가지고 주기적인 시스템 보안 패치나 암호변경, 개인방화벽 프로그램 사용 등의 조치를 취하여 좀 더 안전한 시스템 환경을 만들어 사용하는 것 또한 중요하겠다.

### (2) 신종(변형) 악성코드 발견 동향

작성자: 정진성 주임연구원 (jsjung@ahnlab.com)

4월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1], [그림2]와 같다.

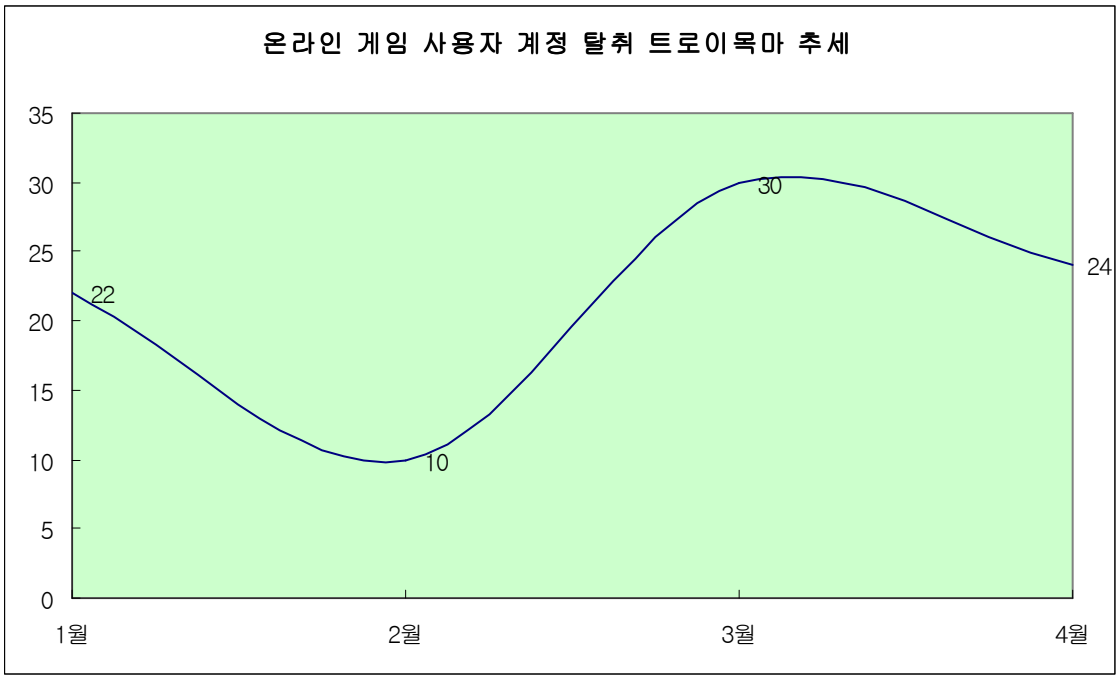
| 웜 | 트로이 | 드롭퍼 | 스크립트 | 파일 | 매크로 | 부트 | 부트/파일 | 유해가능 | 비윈도우 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 42 | 154 | 32 | 0 | 1 | 0 | 0 | 0 | 11 | 0 | 240 |

[표1] 2006년 4월 유형별 신종 (변형) 악성코드 발견현황

악성코드 유형 중 웜이 차지하는 비율이 줄어들고 있다. 이번 달은 42건의 신종 및 변형 웜 중에서 고객으로부터 보고된 수는 20건 밖에 되지 않는다. 나머지 22건은 국내에서 자체 수집된 샘플들이며 마이톱 웜(Win32/Mytob.worm)과 마이둠 웜(Win32/Mydoom.worm)이 대부분을 차지하고 있다. 이중 마이톱 웜 변형은 동일 제작자의 소행으로 보여지는 부분이 확인 되었다. 사용된 실행압축의 종류가 동일하며 압축을 해제한 후 바이너리 사이즈와 해당 바이너리 내 임포트 함수와 분기점들이 유사했다. 마이톱 웜은 소스가 제작자들 사이에서 공개가 되어있어 이를 이용한 변형이 많다.

그 다음으로 변형이 많이 발견된 브론톡 웜(Win32/Brontok.worm)은 고객으로부터 보고 된 것이다. 7개의 변형이 고객으로부터 접수 되었다. 이 웜은 자신을 안전모드에서도 실행되도록 해 두거나 winlogon 프로세스에 인젝션 되도록 해두기도 한다. 또한 레지스트리 편집기나 작업 관리자 실행을 방해하여 사용자가 임의로 자신을 제거하지 못하도록 한다. 이 웜의 변형은 이 글을 작성하는 현재에도 발견되고 있어 앞으로 변형이 계속 보고 될 것으로 예상된다.

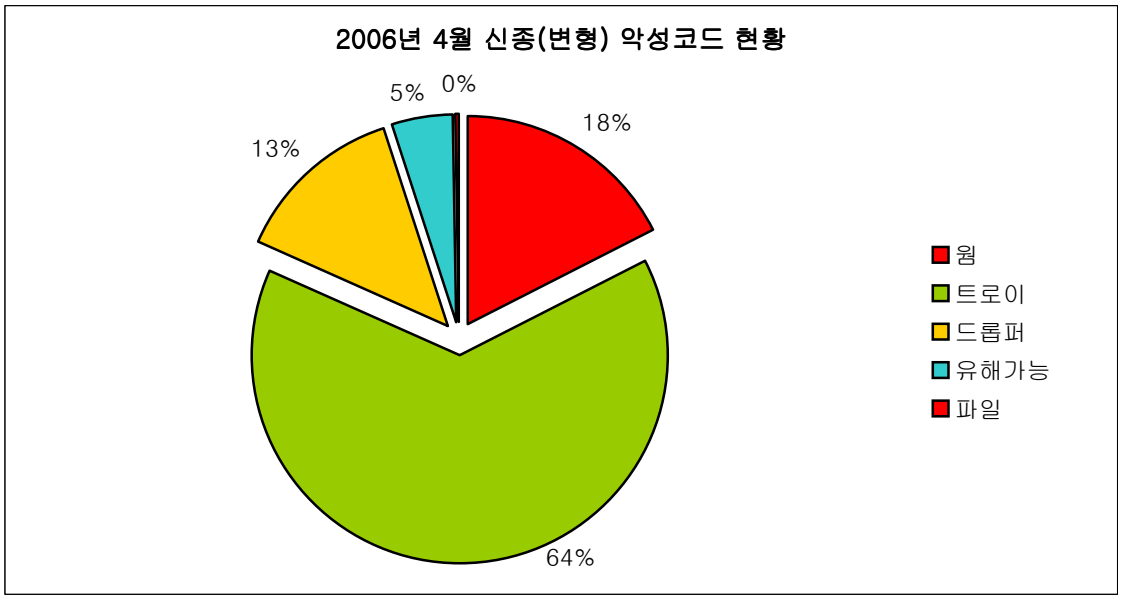
다음은 국내에 많은 피해를 주고 있는 온라인 게임의 사용자 계정을 탈취하는 악성코드의 발견 건수에 대한 그래프다. 본 통계는 드롭퍼(Dropper)라고 불리는 악성코드를 설치하거나 파일을 생성하는 형태는 제외한 수치이다.




[그림1] 온라인 게임 사용자 계정 탈취 트로이목마 현황

최근 온라인 게임 계정 탈취 트로이목마의 양상이 변화 되었다. 새로운 게임을 타겟으로 계정을 훔쳐내는 형태도 나타나지만 이제는 온라인 게임뿐만 아니라 국내 일부 포탈 사이트의 계정도 훔쳐내는 형태 즉, 온라인 게임 계정과 포털 사이트의 계정 등을 모두 탈취 할 수 있는 형태가 늘어나고 있다.

[그림2]은 4월 신종(변형)악성코드의 비율을 나타낸 것이다.




[그림2]2006년 4월 신종(변형) 악성코드 비율

트로이목마의 비율이 점점 많아지면서 덩달아 늘어나는 악성코드 형태가 있다. 바로 드롭퍼이다. 악성코드 파일을 생성하거나 설치하는 드롭퍼는 대부분 온라인 게임 계정 탈취 증상을 갖는 트로이목마의 비율과 비례한다. 유해가능 프로그램 경우 FTP 데몬이 많았으며 이들 증상은 대부분 해킹후 소위 '와레즈' 라고 불리우는 파일 서버로 곧잘 이용된다.

**4월 주요 신종(변형) 악성코드 정리**

이번 달은 악성코드에 의한 피해이슈는 크게 2건이 있었다. 그리고 새로운 악성코드 관련 소식도 있다. 여기서 소개되지 않은 새로운 악성코드로는 MS 퍼블리셔 악성코드와 MathWorks 사의 Matlab 제품의 소스 파일을 감염시키는 형태가 있다. 첫번째 퍼블리셔 악성코드는 비주얼 베이직 어플리케이션 환경을 제공하는 퍼블리셔에서 충분히 예상이 가능한 형태였다. 그리고 수치계산 프로그램으로 유명하고 관련 프로그래밍을 쉽게 도와주는 Matlab 경우는 소스 파일을 감염시키는 바이러스였다. 이 둘 모두 개념증명 형태이기 때문에 일반 사용자가 감염될 확률은 극히 적다.

주요 이슈를 정리해보면 다음과 같다.

**► 크로스플랫폼 바이러스**

외산 안티 바이러스 업체가 경고한 크로스플랫폼 바이러스는 일반에게 보고 되지 않은 형태이다. 윈도우 실행파일(PE)과 리눅스 실행파일(ELF)를 모두 감염시킨다. 이러한 크로스플랫폼 악성코드는 이전에도 존재 했었다. 최근 들어 듀얼 프로세서나 맥과 윈도우 OS의 듀얼 부팅으로 인해 더 일반인들에게 관심을 갖는 게 아닌가 하는 생각이 들기도 한다. V3는 Win32/Biwili , Linux/Biwili로 진단하고 있다.

**► 커널모드 봇 (슈퍼 봇) 소식**

기존의 윈도우 개인 방화벽 제품을 무력화 할 수 있다는 내용의 보도자료가 나가서 더 알려지게 되었다. 이 악성코드는 기존의 윈도우 개인 방화벽 제품들이 TDI(Transport Driver Interface) 및 윈속 레벨에서만 동작하기 때문에 NDIS(Network Driver Interface Specification)의 커널단에서 동작하는 이 악성코드가 대부분의 개인 방화벽 제품을 우회 할 수 있다고 알려졌다. 이는 맞는 말이지만 '슈퍼 봇' 또는 '커널모드 봇'처럼 불리는 것은 옳지 않다. 윈도우 개인 방화벽 제품들은 여러 종류가 있기 때문에 사용자들은 해당 방화벽 제품들이 어느 레이어 까지 지원되는지 확인해보고 해당 제품을 사용하는 것이 바람직하다.

**► 베이글 트로이목마(Win-Trojan/Bagle) 그리고 은폐기법**

4월 한달 동안 다수의 베이글 트로이목마가 보고 되었다. 첫번째 형태는 은폐형으로 커널 서비스 테이블의 정보를 조작하여 자신을 은폐하도록 되어 있다. 이 은폐형 베이글 트로이목마의 주요 증상은 안티 바이러스와 같은 보안 관련 프로그램의 프로세스나 서비스를 강제 종료하여 사용하지 못하도록 하는 형태였다. 두번째로 알려진 베이글 트로이목마는 조금 색다

른 형태로 트로이목마가 감염된 시스템에서 메일 주소를 수집하고 이를 특정 호스트에 포스팅 하도록 되어 있었다. 그리고 난 후 자신은 삭제되므로 감염 되었더라도 사용자들은 모르고 지나칠 수도 있다.

**► 온파인드서치 애드웨어(Win-Adware/OnFindSerach)**

4월 19일, 고객으로부터 시스템 날짜의 시간이 과거로 변경 된다는 다수의 문의를 받았다. 문제의 시스템을 보기 전까지는 이것이 악성코드에 의한 것인지 아니면 응용 프로그램의 버그인지 알 수 없었다. 그러나 해당 증상이 발생하는 고객의 시스템을 직접 확인한 결과, 증상을 유발시키는 프로그램 하나를 찾아내었고, 그 파일의 분석결과 그 증상은 온파인드서치라고 불리우는 애드웨어가 발생한 일이었다. 자세한 사항은 ASEC 이달의 컬럼 코너에서 살펴보자.

**► 인서트아이프레임 트로이목마(Win-Trojan/InsertIframe)**

웹 해킹을 통한 온라인 게임 계정 탈취 트로이목마 설치가 늘어나면서 발견된 형태이다. 이 트로이목마는 웹 사이트에서 사용되는 스크립트 파일에 지속적으로 그리고 자동으로 악성코드가 업로드 된 특정 호스트 주소가 담긴 내용의 iframe을 삽입한다. 이는 관리자가 스크립트 파일을 수정하여도 이 트로이목마가 지속적으로 iframe 내용을 다시 기록하도록 한다. 따라서 트로이목마를 진단하고 치료하지 않으면 삽입된 iframe 내용을 삭제하더라도 지속적으로 다시 삽입되므로 해당 웹사이트가 악성코드 배포의 온상으로 오해 받을 수 있다.

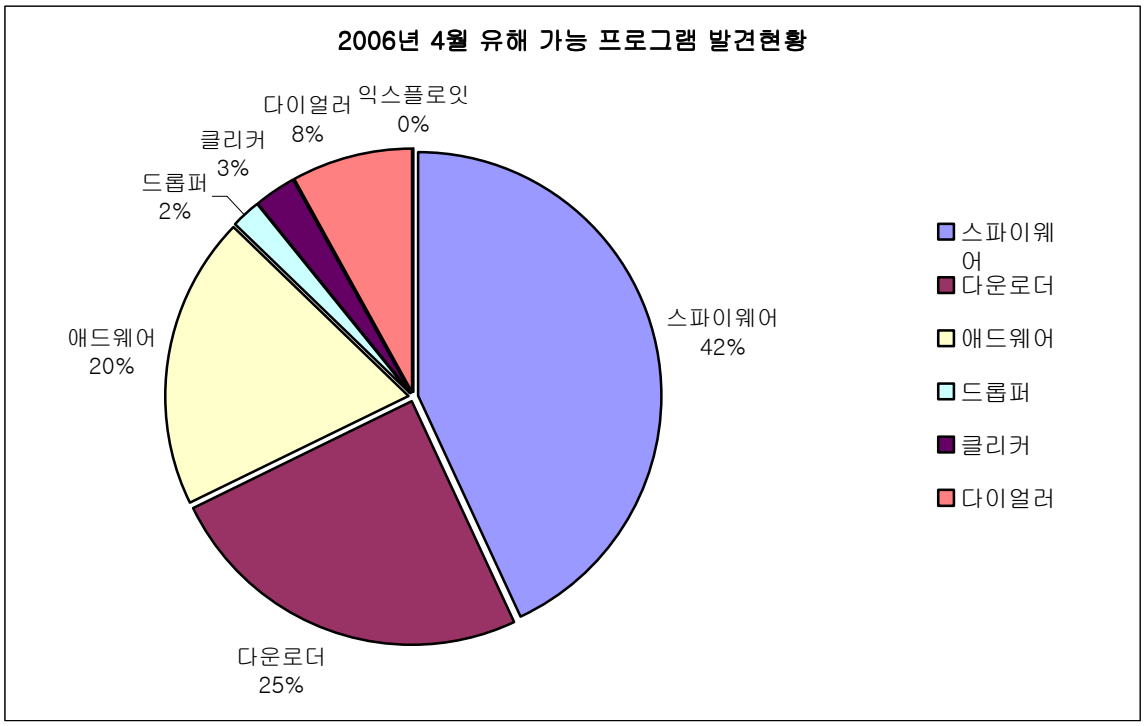
# II. 4월 AhnLab 스파이웨어 동향

작성자: 박시준 연구원(sjpark@ahnlab.com)

4월 한달 동안 접수된 신종(변형) 유해가능 프로그램 건수는 [표1], [그림1]과 같다.

| 스파이웨어 | 다운로더 | 애드웨어 | 드롭퍼 | 클리커 | 다이얼러 | 익스플로잇 | 합계 |
|---|---|---|---|---|---|---|---|
| 466 | 265 | 211 | 21 | 30 | 85 | 1 | 1079 |

[표1] 2006년 4월 유형별 유해가능 프로그램 발견 현황



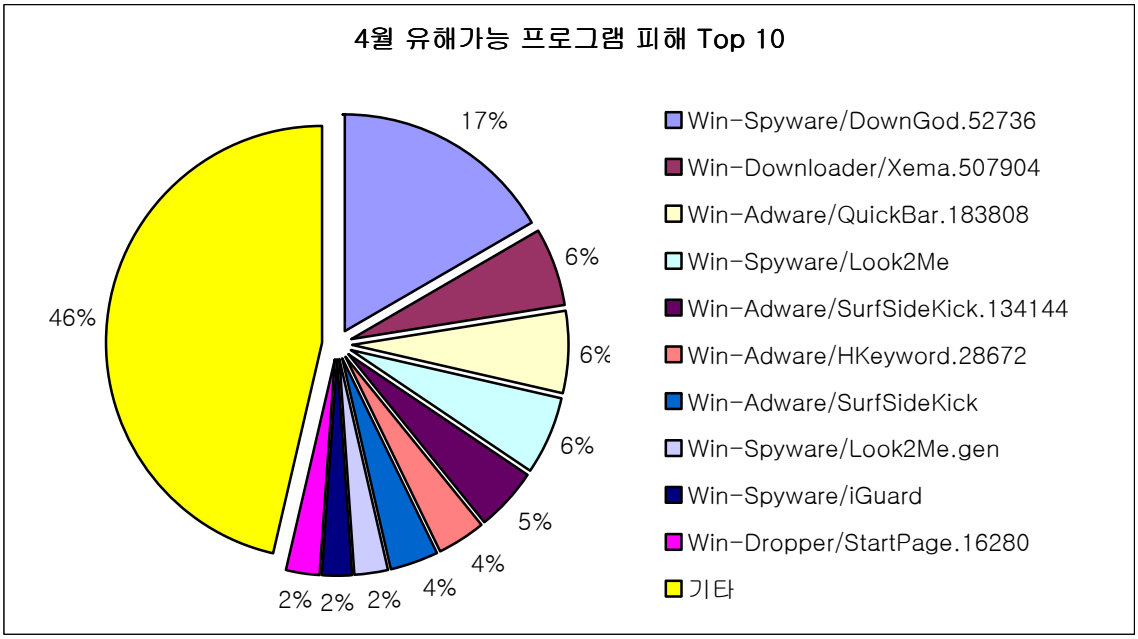

[그림1] 2006년 4월 유해 가능 프로그램 발견 비율

4월에는 스파이웨어를 지속적으로 다운로드하고 설치하는 다운로더(Win-Downloader)의 발견이 증가함에 따라 유해가능 프로그램의 전체적인 발견수치가 크게 증가하였다. 다운로더는 제작이 비교적 쉬우며 사용자 PC에 한번 설치되면 지속적으로 스파이웨어를 설치할 수 있다는 점 때문에 꾸준히 신종 및 변형이 증가하고 있다. 또한 중국에서 제작 및 배포하는 PWS 스파이웨어(Win-Spyware/PWS) 역시 지속적으로 발견 되고 있다. 특이점은 이전엔 하나의 온라인 게임만을 대상으로 계정 정보를 유출 했으나, 최근에는 하나의 PWS 스파이웨어가 온라인 게임 서비스를 제공하는 다수의 포탈 사이트들의 계정 정보를 유출하는 경향을 보이고 있다. 이들은 불특정 웹사이트를 해킹한 후 인터넷 익스플로러의 보안 취약점을 이용해 스파이웨어를 설치하는 코드를 삽입하는 형태로 배포하고 있어 사용자들의 각별한 주의가 필요하다.

4월 피해 신고된 유해가능 프로그램 Top 10을 살펴보면 [표2], [그림2]와 같다.

| 순위 | | 유해가능 프로그램명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | New | Win-Spyware/DownGod.52736 | 14 | 17% |
| 2 | ↑8 | Win-Downloader/Xema.507904[1] | 5 | 6% |
| 3 | ↓2 | Win-Adware/QuickBar.183808 | 5 | 6% |
| 4 | ↓2 | Win-Spyware/Look2Me | 5 | 6% |
| 5 | New | Win-Adware/SurfSideKick.134144 | 4 | 5% |
| 6 | - | Win-Adware/HKeyword.28672 | 3 | 4% |
| 7 | New | Win-Adware/SurfSideKick | 3 | 4% |
| 8 | ↓4 | Win-Spyware/Look2Me.gen | 2 | 2% |
| 9 | New | Win-Spyware/iGuard | 2 | 2% |
| 10 | New | Win-Dropper/StartPage.16280 | 2 | 2% |
| | | 기타 | 39 | 46% |
| 합계 | | | 84 | 100% |

[표2] 2006년 4월 유해가능 프로그램 Top 10




[그림2] 4월 유해가능 프로그램 피해 Top 10

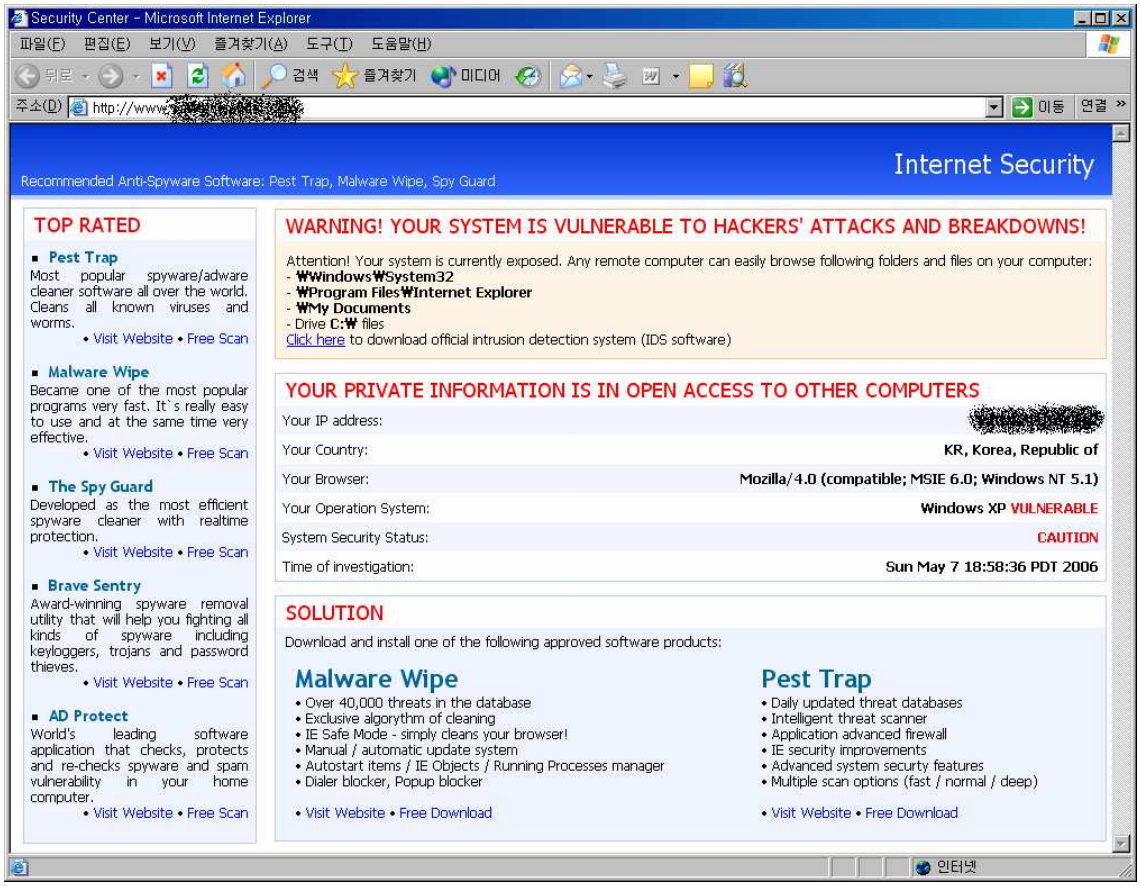
4월 피해 동향을 살펴보면 다운갓.52636(Win-Spyware/DownGod.52736)이 새롭게 피해

[1] Win-Downloader/Xema.507904는 기존 Win-Downloader/Wizscreen.507904의 변경된 진단명이다.

접수 1위를 차지한 것을 볼 수 있다. 이 스파이웨어가 불특정 웹사이트에서 인터넷 익스플로러의 보안 취약점을 이용해 설치되고 있는 것으로 미루어 볼 때, 국내 다수의 웹 서버가 해킹되어 해당 스파이웨어를 설치하는 코드가 삽입되었다는 것을 짐작할 수 있다.

작년부터 꾸준히 피해 사례가 신고되고 있는 룩투미(Win-Spyware/Look2Me)의 경우 다운로더에 의해 사용자 동의 없이 다운로드 및 설치되며, Winlogon에 인젝션(Injection)되어 동작하며 로그인한 사용자 계정의 프로그램 디버깅 권한을 제거하고 윈도우의 로그온 및 로그오프시 자신을 변형시켜 다시 설치하는 기능을 가지고 있다. 또한 안전모드(Safe mode)에서도 정상적으로 작동하므로 사용자가 이를 수동으로 제거하기가 매우 어려워 지속적으로 관련 피해 문의가 접수되고 있는 것으로 보인다.

스타트페이지(Win-Spwyare/StartPage)를 드롭(Drop)하고 설치하는 스타트페이지 드롭퍼(Win-Dropper/StartPage.16280)가 새로 순위에 추가되었다. 설치된 스타트페이지는 인터넷 익스플로러의 시작 페이지를 [그림3]과 같이 사용자의 컴퓨터 시스템이 해커에 의해 공격받고 파손 되었다는 허위 경고 페이지로 리다이렉션(Redirection)시켜 사용자들에게 불안감을 조성시키다. 또한 해당 허위 경고 페이지에서 추천하는 허위 안티 스파이웨어(Win-Adware/Rogue)의 설치를 유도하며, 거짓되거나 과장된 진단 결과를 보여줘 사용자에게 유료 결제를 유도하여 금전적 피해를 입힌다.



[그림3] 스타트페이지에 의해 리다이렉션된 인터넷 익스플로러 시작페이지

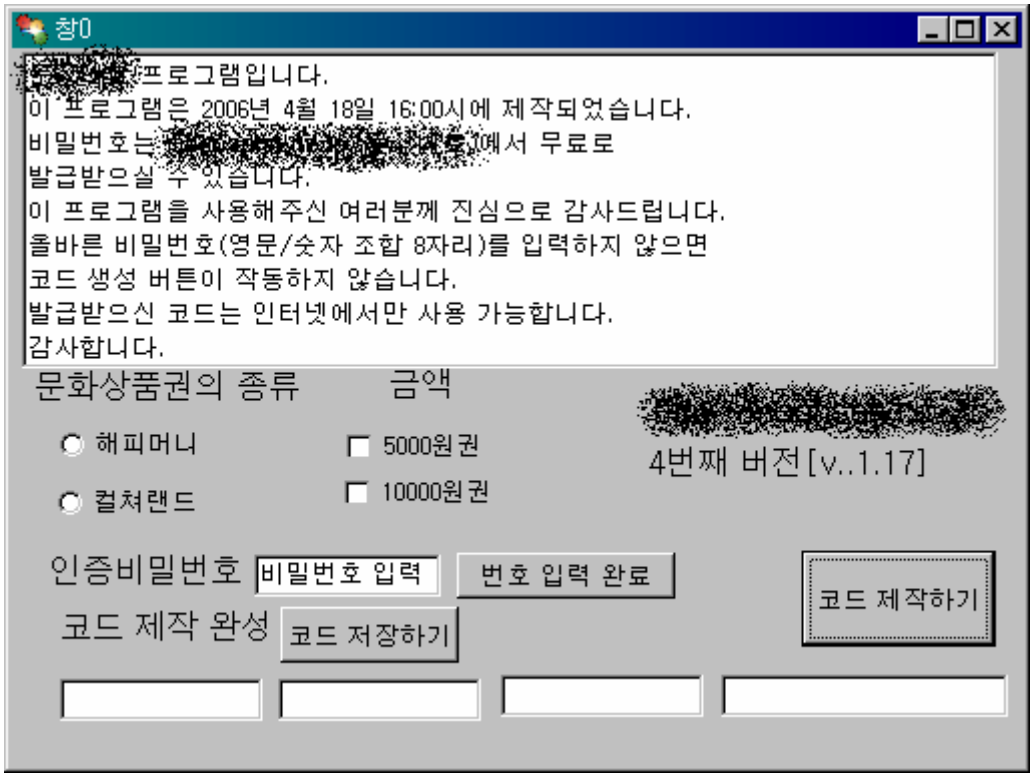
**특정 목적을 위해 사용자를 속이는 프로그램의 증가**

최근 국내에서 웹 사이트를 홍보하거나 금전적 이익을 취득할 목적으로 제작된 프로그램이 꾸준히 발견되고 있다.

도토리(Win-Clicker/Dotori.1147051)의 경우 여러 명에게 해당 프로그램을 배포한 후 실행하면 특정 사이트의 사이버 머니를 충전할 수 있다는 메시지를 출력한다. 하지만 실제로는 제작사의 홈페이지가 팝업될 뿐 어떠한 기능도 가지고 있지 않다. 즉, 일반 사용자를 통해 프로그램을 배포할 홍보 수단으로 실제 불가능한 사이버 머니 충전 프로그램을 미끼로 사용하고 있는 것이다.


[그림4] 도토리(Win-Ckicker/Dotori.1147051)의 실행 화면

문상(Win-Adware/Moonsang.640946, Win-Adware/Moonsang.739404)의 경우 인터넷에서 사용할 수 있는 문화상품권 코드를 생성해 주는 프로그램이라고 홍보하고 있으며, 해당 프로그램을 통해 문화상품권 코드를 생성하려면 비밀번호를 입력해야 한다. 그러나 해당 비밀번호는 가입자를 유치하면 일정량의 적립금을 주는 사이트에 제작자를 추천인으로 등록한 후 메일을 보내면 메일을 통해 알려 준다며 허위 광고를 하고 있다. 뿐만 아니라 실제 해당 프로그램은 메뉴만 제공하고 있으며 그 이외엔 어떠한 기능도 없어, 제작자의 가입자 유치 비용 적립을 위해서 일반 사용자들을 이용한 프로그램이라 할 수 있다.




[그림5] 문상(Win-Adware/Moonsang.739404) 실행 화면

이런 프로그램들은 일반 사용자들이 컴퓨터에 대한 전문적인 지식이 부족하다는 점을 이용한 것으로, 사용자는 비정상적이거나 부정한 방법으로는 어떠한 이득도 취할 수 없다는 점을 인지하고 이런 프로그램에 이용 당하지 않도록 각별한 주의가 필요하다.

# III. 4월 시큐리티 동향

작성자: 김지훈 선임연구원(smallj@ahnlab.com)

이번 달에는 마이크로소프트사(이하 MS)의 정기 보안 패치가 총 5개 발표되었다.

**마이크로소프트사의 4월 주요 취약점 현황[1]**

| 위험등급 | 취약점 | 공격코드 유/무 |
|---|---|---|
| HIGH | Internet Explorer 누적 보안 업데이트 (MS06-013) | 유 |
| HIGH | MDAC(Microsoft Data Access Components) 기능의 취약점으로 인한 원격 코드 실행 문제점 (MS06-014) | 무 |
| HIGH | Windows 탐색기의 취약점으로 인한 원격 코드 실행 문제점 (MS06-015) | 무 |
| HIGH | Outlook Express 누적 보안 업데이트 (MS06-016) | 무 |
| MEDIUM | Microsoft FrontPage Server Extensions의 취약점으로 인한 사이트 간 스크립팅 문제점 (MS06-017) | 무 |

► Microsoft Internet Explorer CreateTextRange() Code Execution (CVE-2006-1359)[2]

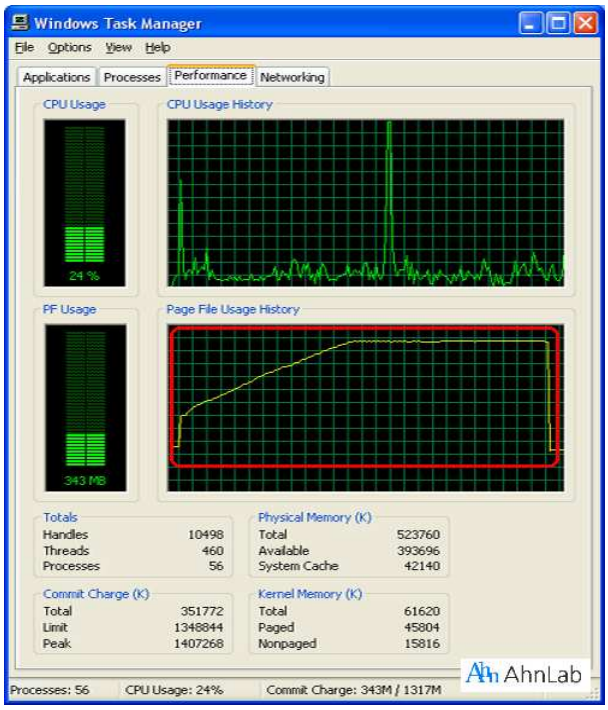
2005년 12월말 발생한 WMF 취약점에 이어, 또 다른 제로데이 공격(0-day Attack) 위협으로 기록되었다. 악의적인 공격자는 WMF 취약점과 마찬가지로 이번 취약점을 이용하여 악성코드, 스파이웨어의 설치 및 배포에 활용하였다. 이 취약점에 대한 발견에서 패치파일 발표까지의 히스토리는 다음과 같다.

[1] 취약점 현황은 ASEC 의 보안전문가들에 의해 공격코드 유/무, 악성코드 활용가능성, 취약점의 위험도 등 다양한 관점에서 판단하여 선별된 것으로, 사용자들의 주의가 필요한 것임을 나타낸다. 공격코드의 존재유무는 이 리포트를 작성하는 시점에서 인터넷 상에서 접할 수 있는 기준으로 작성되었다.

[2] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1359

2006/01/02, 시큐니아에서 발견
2006/01/13, MS 에 통보
2006/02/21, MS 에서 취약점 확인
2006/03/22, 컴퓨터 테러리즘에서 취약점 내용을 메일링리스트에 공개
2006/03/23, 시큐니아에서 권고문 발표
2006/03/28, 트러스가드(TrusGuard) 대응
2006/03/28, eEye와 Detemina 비공식 패치 발표
2006/04/11, MS06-013 보안 패치 발표

"createTextRange()"는 선택한 범위 또는 문서 전체 영역을 하나의 객체로 만들어 이 안에서 다양한 문자열 조작 및 태그의 변형을 가능하게 만드는 TextRange 객체를 생성하는 DHTML(dynamic HTML) 메쏘드이다. 이번 취약점은 "createTextRange()" 메쏘드 상에서 발생하는 프로그램 디자인상의 오류를 이용하고 있다.
실제 공격 코드에서는 "createTextRange()" 메쏘드를 호출하는 과정에서 대량의 데이터(NOP+ Shellcode)로 Heap 메모리 영역을 채우도록 만든다. 이 과정에서 다음과 같이 시스템의 메모리 사용이 급격하게 증가하는 모습을 확인할 수 있다.




[그림1] createTextRange() 취약점에 대한 공격코드 실행 시 메모리가 급증한 화면

인터넷 익스플로러가 앞서 Heap 메모리에 채워진 NOP+ Shellcode 부분을 가리키게 되고 공격자가 삽입해 놓은 임의의 코드를 실행하게 된다.

```
7D5322B1 MOV ECX,DWORD PTR DS:[EDI]
7D5322B3 PUSH EAX
7D5322B4 PUSH mshtml.7D4A1CA8
7D5322B9 PUSH EDI
7D5322BA CALL DWORD PTR DS:[ECX]
```

**► MS 4월 보안 패치의 문제점**

MS 4월 보안 패치 중 MS06-013과 MS06-015의 2가지 보안 패치가 다른 응용 프로그램과 충돌을 일으킬 수 있다고 공지되었다. 특히 MS06-015 윈도우 탐색기 관련 보안 패치의 경우, HP Share-to-web, Sunbelt Kerio 방화벽 등과의 충돌로 인해 보안 패치 파일이 수정 후 재배포되기도 하였다.[1] MS06-013 IE 누적업데이트의 보안 패치 적용 시에는 ActiveX 컨트롤 문제로 인해 구글 툴바, 시벨 사의 소프트웨어, 자바 소프트웨어 등의 이용에 불편함을 초래할 수 있으나, 아직까지 해당 보안 패치들로 인한 고객의 피해 사례가 특별히 보고된 바는 없다.[2]

**다양한 플랫폼의 취약점**

이제 악성코드는 MS의 보안 취약점의 굴레를 벗어나, 다양한 플랫폼과 어플리케이션의 취약점을 서서히 공략해가며 점차 그 활동 범위를 확대해 나가고 있다. 이러한 흐름은 SANS (SysAdmin, Audit, Network, Security) Institute를 통해서도 확인해 볼 수가 있다. SANS는 2006년 1Q의 주요 보안 취약점을 정리하여 발표하였다[3]
4월에 발표된 주요 플랫폼의 취약점 동향을 살펴보자.

**► 오라클, 4월 정기 보안 패치 발표**

오라클(Oracle)에서는 지난 4월 18일 정기 오라클 보안 패치 CPU(Critical Patch Update) Apr2006을 발표하였다.[4] 이번 오라클 CPU의 대상이 된 것은 오라클 데이터베이스의 취약점 14건과 오라클 컬러보레cnldir이션 슈트(Oracle Collaboration Suite)의 취약점 5건, OAS(Oracle Application Server)의 취약점1건, Oracle E-Business Suite and Applications의 취약점 15건, 오라클 엔터프라이즈 매니저(Oracle Enterprise Manager)의 취약점 2건, 피플소프트 엔터프라이즈 포털 애플리케이션(PeopleSoft Enterprise Portal Applications)의

---

[1] Microsoft, MS06-013 IE 누적 보안 업데이트의 문제발생가능성 (http://support.microsoft.com/kb/912812)
[2] Microsoft , MS06-015를 설치한 후 Windows 탐색기 또는 Windows 셸의 문제발생 가능성(http://support.microsoft.com/kb/918165)
[3] SANS, 2006 SANS Top 20 Spring Update - Technical details on specific vulnerabilities (http://www.sans.org/top20/2005/spring_2006_detail.php)
[4] Oracle, Critical Patch Updates and Security Alerts (http://www.oracle.com/technology/deploy/security/alerts.htm)

취약점 1건, 그리고 JD Edwards 소프트웨어의 취약점 1건이다.
작년 11월경, 오라클은 InnoDB의 인수를 기반으로 Oracle 10g XE(Express Edition)라는 무료 데이터베이스를 출시하였고, 이로 인해 사용자의 오라클 활용도가 크게 신장될 것으로 기대하고 있다. 활용도가 커질수록 악의적인 공격자의 보안 위협에 노출되기 쉽기 때문에 보안 패치의 중요성을 상기하고, 보안 취약점 관리에 신중을 기해야 할 것이다.

**► 애플의 Mac OS X 보안 취약점 공개**

애플의 Mac OS X도 더 이상은 안전하지 않음을 증명이라도 하듯 필자가 이 글을 쓰고 있는 이 시점까지 패치 되지 않은 다수의 보안 취약점과 개념증명코드(Proof of Concept)가 공개되었다. 사파리 등의 어플리케이션을 이용하여 BMP, GIF, TIFF 포맷의 악의적인 그림파일을 처리하는 과정에서 발생되는 취약점이 대부분이고, 압축파일 처리 과정에서 발생되는 취약점도 포함되어 있다. 공격자는 이번 취약점을 이용하여 타겟 시스템에 DoS (Denial of Service)공격을 수행할 수 있다.

보안을 100% 유지할 수 있는 솔루션은 어디에도 없다. 이용자의 보안에 대한 정확한 이해와 실천만이 기업 내의 보안 강도를 높일 수 있는 가장 강력한 보호 수단임을 잊지 말고, 스스로의 보안 실천 가이드를 만들어 꾸준히 지켜나가야 할 것이다.

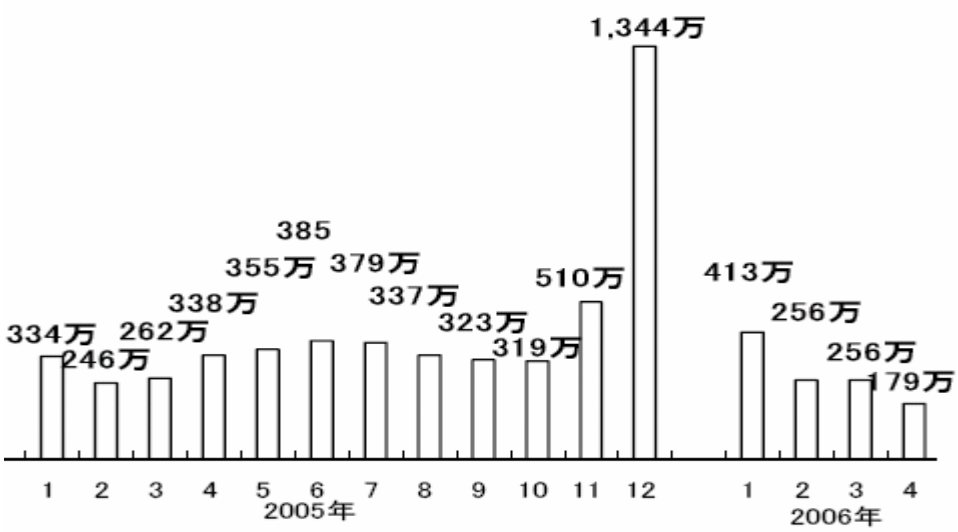
# Ⅳ. 4월 세계 악성코드 동향

2006년 4월 세계 악성코드 동향은 특정 매스메일러들이 순위권에 차지하고 있는 것 외에는 2006년 지난 몇 달에 비해 큰 변화가 없었다. 다만 지역적으로 일본에서는 2006년 들어 악성코드 신고 건수가 줄어들고 애드웨어가 조금씩 증가하고 있다. 중국 역시 악성코드 동향은 큰 변화가 없으나 애드웨어의 순위변화는 심했다.

## (1) 일본의 악성코드 동향

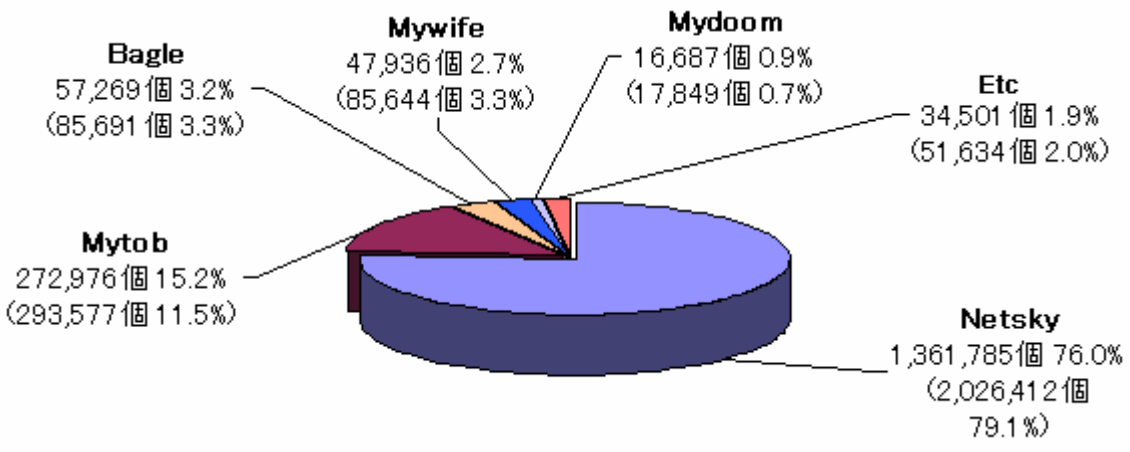
작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

2006년 4월 일본의 악성코드 동향에서 가장 주목할 점은 올해 들어 악성코드 발견 수치가 점점 줄어들고 있다는 것이다. [그림1]에서 2005년과 2006년 초 악성코드 신고 건수에 대한 통계이다. 올 해 들어 감염 피해가 점점 줄어들고 있고 4월 들어서는 그 수치가 현저하게 줄어든 것을 볼 수 있다.




[그림1] 일본의 월별 악성코드 발견 추이

악성코드 신고 건수 또한 전월의 4,270건에서 3,537건으로 현저하게 줄어 들었는데 이러한 현상이 발생한 원인은 매스메일러의 피해 건수가 줄어든 것이 원인으로 생각된다. [그림2]는 악성코드 별 탐지 건수를 표로 나타낸 것이다. 넷스카이 웜이 여전히 매우 많은 양의 메일을 배포하고 있으나 그 총 개수는 현저하게 떨어진 것을 볼 수 있다.




[그림2] 악성코드 유형 별 탐지현황

실제 감염 피해 또한 매우 낮아졌는데 이와 관련한 구체적인 자료는 아래의 [표1]의 데이터를 참고하기 바란다.

**일본 악성코드 동향**

2006년 4월 일본에서 가장 많이 유행한 악성코드는 넷스카이 웜(Win32/Netsky.worm)이다. 넷스카이 웜의 경우 순위에는 변화가 없으나 감염 피해 건수가 전월에 비해서 많이 감소한 것을 볼 수 있다. 이러한 현상은 마이톱 웜(Win32/Mytob.worm)이나 베이글 웜(Win32/Bagle.worm)도 마찬가지이다.

| Window/Dos Virus | 금월피해<br>전월피해 | Macro Virus | 금월피해<br>전월피해 | Script Virus | 금월피해<br>전월피해 |
|---|---|---|---|---|---|
| Win32/Netsky | 826<br>988 | Xm/Laroux | 18<br>11 | VBS/Redlof | 26<br>46 |
| Win32/Mytob | 347<br>531 | W97M/X97M/P97M/Tristate | 8<br>5 | VBS/Lovelette r | 14<br>8 |
| Win32/Mydoom | 258<br>298 | W97M/Bablas | 3 | VBS/Kakworm | 10<br>3 |
| Win32/Mywife | 221<br>288 | XF/Sic | 3<br>7 | Wscript/Fortnight | 4<br>2 |
| Win32/Bagle | 216<br>449 | W97M/Ethan | 1<br>1 | VBS/Soraci | 2<br>1 |
| Win32/Klez | 169<br>195 | W97M/Sting | 1 | | |

[표1] 악성코드 피해 신고 현황(출처: 일본IPA)

**악성코드의 감염 경로 별 통계**

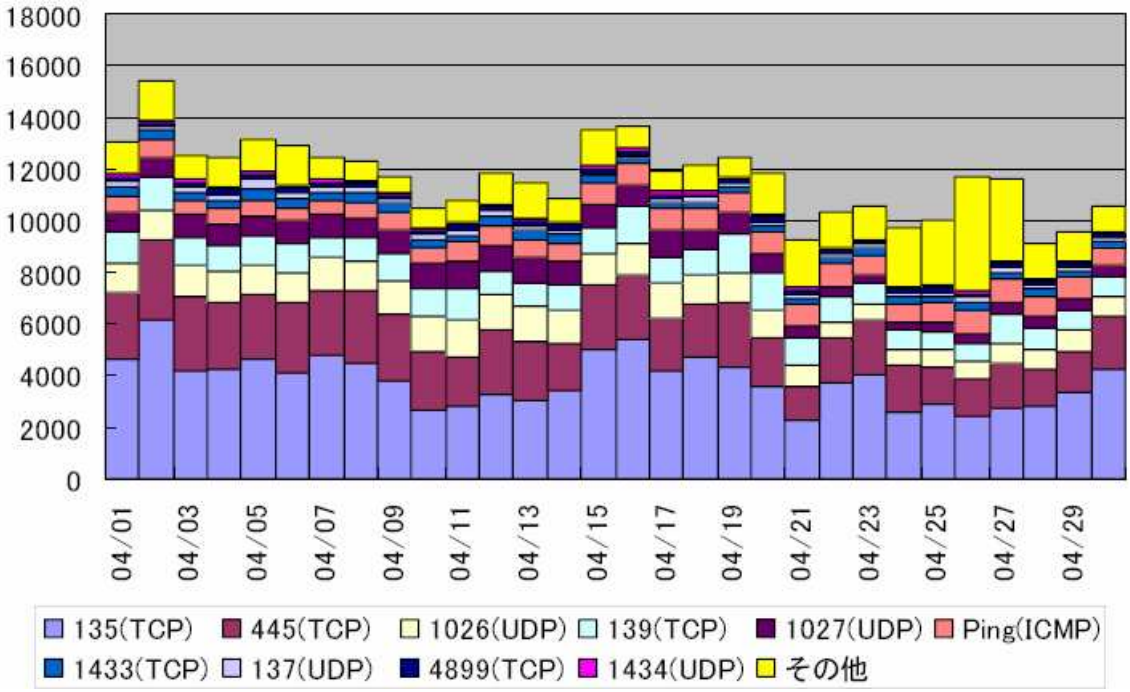
[표2]는 악성코드 감염 경로 별 통계를 나타낸 것으로써 메일을 이용해 확산되는 악성코드가 가장 많은 양을 차지하고 있는 것을 확인할 수 있다. 메일 이외에는 네트워크를 이용한 악성코드가 많이 발견되고 있음을 알 수 있다. 또한 총 합계가 전월에 비해 매우 많이 줄어든 것을 볼 수 있다.

| 감염경로 | 피해 건수 | | | | | |
|---|---|---|---|---|---|---|
| | 2006년 3월 | | 2006년 3월 | | 2005년 4월 | |
| 메일 | 3,433 | 97.1% | 4,140 | 96.9% | 4,381 | 98.7 |
| 외부의 모체 | 1 | 0.0% | 1 | 0.0% | 1 | 0.0% |
| 다운로드 | 1 | 0.0% | 4 | 0.1% | 4 | 0.1% |
| 네트워크 | 98 | 2.8% | 122 | 2.9% | 51 | 1.1% |
| 기타 | 4 | 0.1% | 3 | 0.1% | 3 | 0.1% |
| 합계 | 3,537 | | 4,270 | | 4,846 | |

[표2] 악성코드 감염 경로 통계(출처: 일본IPA)

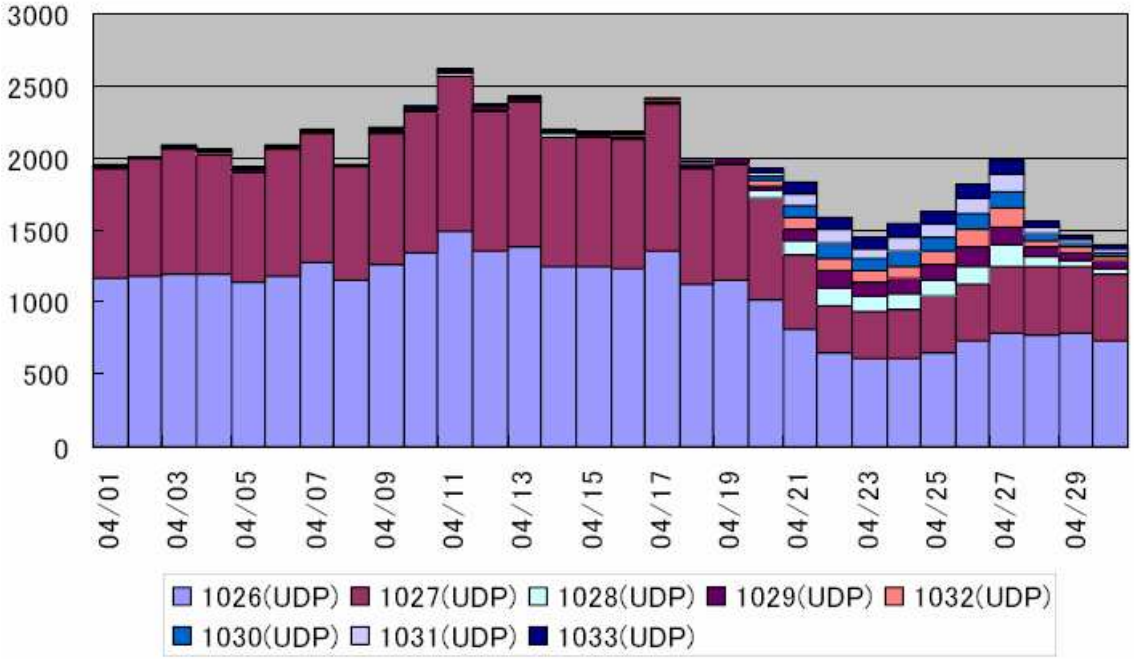
**일본 네트워크 트래픽 현황**

[그림3]은 4월 한 달 동안 일본의 네트워크 트래픽 현황에 대한 통계를 그래프로 나타낸 것이다. TCP135 포트와 TCP445 포트의 트래픽이 매우 많은 것을 볼 수 있는데 이 포트들은 윈도우 OS에서 사용되는 포트들이지만 IRCBot과 같이 OS의 취약점을 이용하여 전파되는 악성코드들에서도 사용되므로 주의가 필요하다.



[그림3] 일본의 네트워크 트래픽 현황(출처: 일본IPA)

TCP 1026 포트와 1027 포트의 트래픽 사용량 또한 매우 많은 것을 볼 수 있다. 해당 포트들은 윈도우의 메신저 서비스에서 이용되는데 최근 중국에서 광고 목적으로 메신저서비스를 이용한 것이 주 원인일 수 있다.




[그림4] 102x-103x 포트의 사용 현황

한국의 경우에도 작년에 메신저 서비스를 이용한 광고가 무작위로 배포된 사례가 종종 발생한 사례가 있다. 이러한 광고를 원천적으로 막기 위해서는 윈도우 메신저 서비스를 종료하여야 한다.

## (2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

2006년 4월 중국 악성코드 동향은 3월 동향과 유사하게 트로이목마 형태가 강세를 보이고 있지만 세부적인 사항들을 살펴보면 사용자의 개인정보 유출을 시도하는 악성코드보다는 스파이웨어, 애드웨어와 유사한 형태의 유해가능 프로그램들이 강세를 보이고 있다. 이러한 흐름은 지난 3월 동향에서 그 변화의 조짐이 서서히 발견되기 시작하여 이번 4월에서는 더욱 뚜렷하게 나타난 것으로 분석된다. 특히나 중국 로컬 백신 업체인 라이징(Rising)과 강민(JiangMin)의 월간 악성코드 동향 중에서도 강민의 동향에서 이러한 변화가 뚜렷하게 나타나고 있다. 특히 유해가능 프로그램들 중에서도 중국 로컬 인스턴트 메신저 프로그램인 QQ 메신저 프로그램과 관련 있는 형태들이 많이 발견된 것을 알 수 있다. 이러한 흐름으로 미루어 2006년은 애드웨어와 스파이웨어 형태의 확산으로 이어질 것으로 추정된다.

**악성코드 TOP 5**

| 순위 | 순위 변화 | Rising |
|---|---|---|
| 1 | - | Trojan.DL.Agent |
| 2 | New | Trojan.DL.QQHelper |
| 3 | ↓1 | Backdoor.Gpigeon |
| 4 | ↓1 | Trojan.DL.Small |
| 5 | - | Dropper.Agent |

[표1] 2006년 4월 라이징(Rising) 악성코드 TOP 5

먼저 2006년 4월 라이징의 악성코드 TOP 5를 살펴보도록 하자. 순위 1위에는 지난 3월과 동일한 순위를 유지하고 있는 Trojan.DL.Agent(V3 진단명 – Win-Trojan/Agent)이 2월에서부터 3개월간 순위 변화 없이 1위를 유지하고 있다. 2위에는 이번 4월에 새롭게 순위에 진입한 Trojan.DL.QQHelper(V3 진단명 – Win-Trojan/QQHelper)가 차지하고 있다. 그리고 3위와 4위에는 지난 3월에 비하여 한 계단씩 순위 하락한 Backdoor.Gpigeon(V3 진단명 – Win-Trojan/GrayBird 또는 Win-Trojan/Hupigon)와 Trojan.DL.Small(V3 진단명 – Win-Trojan/Xema)이 차지하고 있다. 그리고 5위에는 순위 변화 없이 Dropper.Agent(V3 진단명 – Dropper/Agent)이 차지하고 있다.

| 순위 | 순위 변화 | JiangMin |
|---|---|---|
| 1 | New | Adware/Downloader.QQHjit.gen |
| 2 | ↑2 | Adware/Downloader.QQHelper.gen |
| 3 | New | Adware/Downloader.QQHres.gen |

| | | |
|---|---|---|
| 4 | ↓3 | Adware/Downloader.QQHelper.cb |
| 5 | New | Adware/Downloader.QQHjit.a |

[표2] 2006년 4월 강민(JiangMin) 악성코드 TOP 5

강민의 악성코드 TOP 5는 라이징의 악성코드 TOP 5와 비교하여 스파이웨어, 애드웨어 형태의 유해가능 프로그램의 순위 변화가 다양하다. 특히 [표2]에서와 같이 Adware/Downloader.QQHjit와 Adware/Downloader.QQHelper 같이 애드웨어를 다운로드하는 형태가 1위에서 5위까지의 순위를 모두 차지하고 있다. 지난 3월 악성코드 TOP 5와 비교한다면 순위 중 2건만 포함되어 있던 것이 순위 전체로 확대된 것을 잘 알 수가 있으며 변형들도 상당수 발견된 것을 알 수 있다. 특히 라이징의 4월 악성코드 TOP 5에서도 Trojan.DL.QQHelper가 새롭게 2위를 차지하고 있는 점으로 미루어 중국 내에서 금전적인 목적을 위해 제작되는 스파이웨어와 애드웨어 형태의 유해가능 프로그램들이 상당한 수치로 확산되어 있는 것을 잘 알 수 있다. 그리고 강민에서 4월 하순 경에 발표한 보도 자료에 따르면 최근에 발견되고 있는 악성코드 형태 중 60% 이상이 이러한 금전적인 목적을 위해서 제작된 애드웨어와 스파이웨어 형태이다.

**주간 악성코드 TOP 5**

| 순위 | 1주 | 2주 | 3주 | 4주 |
|---|---|---|---|---|
| 1 | Trojan.DL.QQHelper | Trojan.DL.QQHelper | Trojan.DL.Agent | Trojan.DL.Agent |
| 2 | Trojan.DL.Agent | Trojan.DL.Agent | Trojan.DL.QQHelper | Trojan.DL.QQHelper |
| 3 | Backdoor.Gpigeon | Backdoor.Gpigeon | Backdoor.Gpigeon | Backdoor.Gpigeon |
| 4 | Trojan.DL.Small | Trojan.DL.Small | Dropper.Agent | Trojan.DL.Small |
| 5 | Dropper.Agent | Dropper.Agent | Trojan.DL.Small | Dropper.Agent |

[표3] 2006년 4월 라이징(Rising) 주간 악성코드 순위

주간 악성코드 TOP 5를 살펴보면 4주간의 흐름에서는 크게 변화가 없지만 지난 3월과 비교하면 앞서 이야기한 애드웨어, 스파이웨어와 같은 유해가능 프로그램의 변화가 큰 것을 알 수 있다. 특히 지난 3월 1주차에서만 애드웨어인 AdWare.Hbang가 잠깐 순위에 포함되었을 뿐이다. 그러나 이번 4월 동향에서는 지난 3월 동향에서 포함되어 있지 않은 Trojan.DL.QQHelper가 4월 1주차에서부터 1위를 차지하며 마지막 주까지 큰 순위하락 없이 그 흐름을 이어가고 있다. 그 외 주간 악성코드 TOP 5에 포함되어 있는 악성코드 들의 경우에는 전반적인 큰 흐름의 변화 없이 3월과 유사한 흐름을 보여주고 있다.

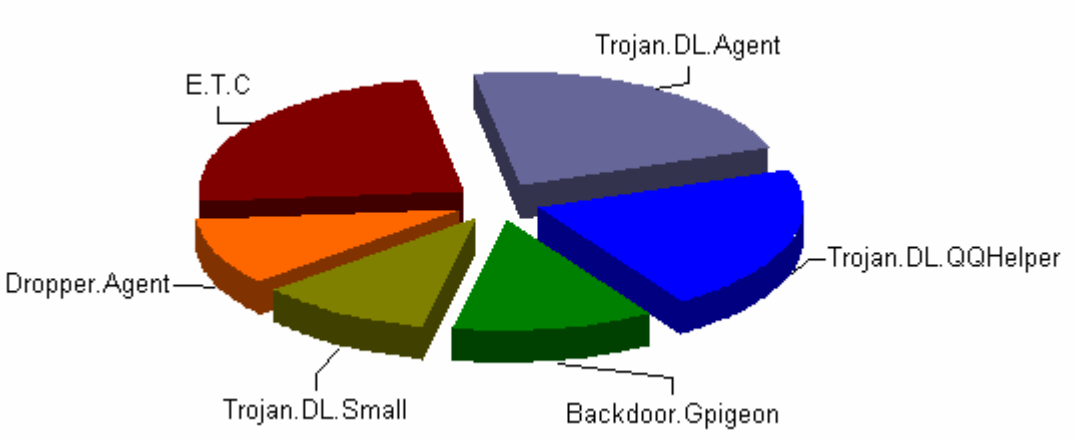
| 순위 | 1주 | 2주 | 3주 | 4주 |
|---|---|---|---|---|
| 1 | Adware/Downloader .QQHjit.gen | Adware/Downloader .QQHjit.gen | Adware/Downloader .QQHjit.gen | Adware/Downloader .QQHjit.gen |

| | | | | |
|---|---|---|---|---|
| 2 | Adware/Downloader .QQHelper.gen | Adware/Downloader .QQHelper.gen | Adware/Downloader .QQHelper.gen | Adware/Downloader .QQHelper.gen |
| 3 | Adware/Downloader .QQHres.gen | Adware/Downloader .QQHres.gen | Adware/Downloader .QQHelper.cb | Adware/Downloader .QQHelper.gb |
| 4 | Adware/Downloader .QQHelper.cb | Adware/Downloader .QQHres.gen | Adware/Downloader .QQHres.gen | Adware/Downloader .QQHelper.cb |
| 5 | Adware/Downloader .QQHjit.a | Adware/Downloader .QQHjit.a | Adware/Downloader .QQHelper.gb | Adware/Downloader .QQHres.gen |

[표4] 2006년 4월 강민(JiangMin) 주간 악성코드 순위

강민의 주간 악성코드 TOP 5는 라이징과 달리 4월 1주차에서부터 4주차까지 모두 유사한 흐름을 보여주고 있다. 이러한 흐름은 3월 4주차 1위에서 4위까지 모두 Adware/Downloader.QQHelper와 Adware/Downloader.QQHres, 그리고 Adware/Downloader.QQHjit 변형들이 차지하면서 5주간 유사한 흐름을 유지해 온 것으로 분석된다.

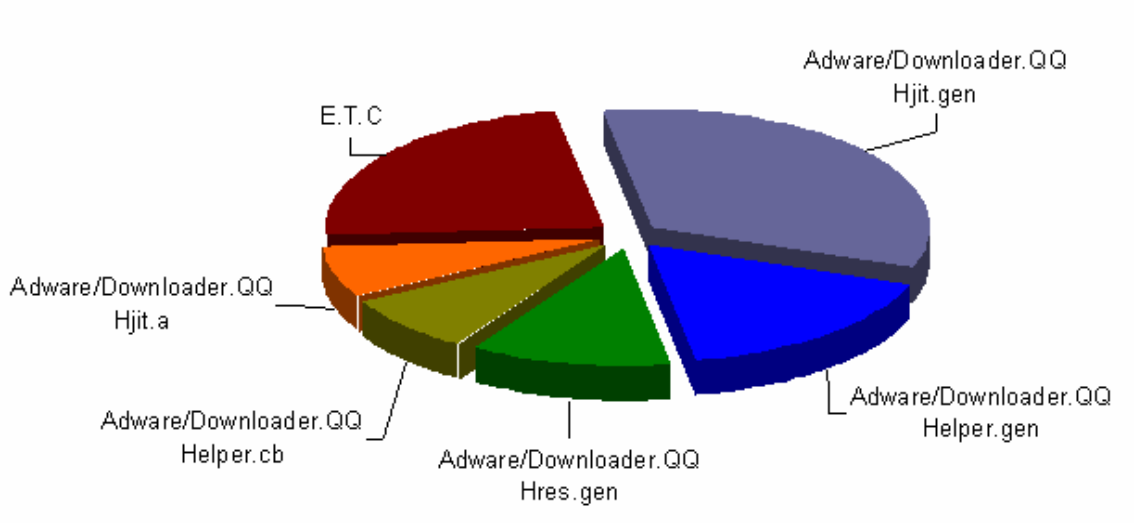
**악성코드 분포**




[그림1] 2006년 4월 라이징(Rising)의 악성코드 분포

악성코드 분포면에서 라이징의 경우 악성코드 TOP 5에서 1위를 차지한 Trojan.DL.Agent만이 21.81%에서 22.27%로 약 1% 정도가 증가하였으며 나머지 악성코드들은 그 수치가 감소하였다. Backdoor.Gpigeon는 17.49%에서 12.45%로 5% 가량, Trojan.DL.Small은 13.24%에서 10.6%로 감소하였으며 순위 변화가 없었던 Dropper.Agent만이 8.8%에서 9.74%로 1% 가량 증가하였다. 그리고 4월에 새로이 악성코드 TOP 5에 진입한 Trojan.DL.QQHelper은 Trojan.DL.Agent과 근사한 21.43% 수치를 차지하고 있다. 악성코드 TOP 5에 포함되지 못한 기타 악성코드의 경우에도 27.69%에서 23.49%로 감소하여 전

반적인 악성코드 분포는 Trojan.DL.QQHelper로 인해 다른 악성코드들의 분포가 감소 추세를 보이고 있다.




[그림2] 2006년 4월 강민(JiangMin)의 악성코드 분포

강민의 악성코드 분포에서는 Adware/Downloader.QQHelper와 Adware/Downloader.QQHres, Adware/Downloader.QQHjit의 커다란 분포 잠식으로 인해 기타 악성코드마저도 40.27%에서 23.35%로 큰 폭으로 감소하였다. QQ 메신저와 관련이 있는 유해가능 프로그램들은 전체 악성코드 분포에서 77% 가량을 차지할 정도로 이번 4월 악성코드에서 큰 변화를 차지하고 있는 것을 잘 알 수 있다.

4월 중국 악성코드 동향은 앞서 이야기한 바와 같이 전체적인 변화의 흐름이 광고를 목적으로 하는 애드웨어와 스파이웨어 형태의 유해가능 프로그램들로 이루어지고 있는 것으로 보여진다. 이러한 형태의 유해가능 프로그램들의 제작목적 자체가 금전적인 이득을 취하기 위한 것이어서, 중국 내에서도 온라인 상에서 발생하는 다양한 형태의 금전적인 손실을 야기하는 보안사고가 발생할 것으로 예측된다.

### (3) 세계의 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

2006년 4월 통계 역시 여전히 매스메일러들이 순위권을 차지하고 있다. 다만, 카스퍼스키 연구소의 통계에 따르면 자피 웜(Win32/Zafi.worm) 변형이 순위권에서 사라졌다.

소포스의 2006년 4월 통계 [1] 에 따르면 1위는 여전히 넷스카이 웜 변형(Win32/Netsky.worm)으로 25개월 이상 피해 순위권을 차지하고 있다. 그 외 나이젬 웜 변형(Win32/Nyxem.worm)이 여전히 3위를 차지하고 있다. 나이젬 웜은 2006년 초에 널리 퍼졌지만 한국 지역에는 보고가 거의 없었다. 새롭게 진입한 웜은 돌레봇(Dolebot)으로 기존 악성 IRC봇의 취약점 전파 기능과 함께 메일로도 전파된다.

카스퍼스키 연구소의 2006년 4월 통계[2]에 따르면 마이톱 웜 변형(Win32/Mytob.worm), 넷스카이 웜 변형(Win32/Netsky.worm), 러브게이트 웜 변형(Win32/LovGate.worm) 등이 순위권을 차지하고 있다. 특이하게 소포스에서는 상위권을 계속 차지하고 있는 자피 웜 변형이 순위권에서 완전히 사라졌다.

카스퍼스키 연구소의 온라인 2006년 4월 검사 결과 통계[3]에 따르면 3월과 통계가 전혀 다르게 1위는 다운로더(Downloader) 변형과 2위는 시스템 정보를 빼가는 LdPinch가 차지했다. 18위의 Exploit.HTML.CodeBaseExec는 웹 서버를 해킹 후 취약점을 포함한 페이지를 몰래 삽입 해 사용자가 웹사이트 방문 시 사용자 모르게 악성코드를 설치하게 하는 역할을 한다. 이 방법은 국내에서 특정 온라인 게임 계정 및 비밀번호 탈취에 이용되고 있으며 외국에서도 이 방법이 이용되고 있음을 알 수 있다.

온라인 검사 결과 순위권에 든 20개의 악성코드 중 10개가 새롭게 등장한 악성코드이고 1위가 3.84%이고 순위권 외의 악성코드가 76.96% 인 것으로 보아, 실제 시스템에 감염되어 있는 악성코드는 다양하게 분포되어 있는 것으로 보인다.

[1] http://www.sophos.com/pressoffice/news/articles/2006/05/toptenapr06.html
[2] http://www.kaspersky.com/news?id=185639268
[3] http://www.kaspersky.com/news?id=185639740

# V. 이달의 ASEC 컬럼 - 날짜변경 트로이목마의 정체

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

### 시스템 날짜 변경 증상

2006년 4월 19일 오전부터 시스템 날짜가 1900년, 1924년, 1953년 등 과거로 바뀌는 증상을 호소한 사용자가 갑자기 증가했다. 동시에 여러 사용자가 증상을 호소하는 것으로 보아 새로운 악성코드일 가능성이 높았으며, 증상을 호소하는 시스템 중 하나를 확인한 결과 수상한 파일을 찾아 내었다. 분석 결과 해당 시스템 의날짜를 변경한 파일은 인터넷에서 시스템에 사용자 몰래 파일을 다운로드 하는 Win-Trojan/Downloader.225597[1] 였다.

### 다운로더가 원인

다운로더(Downloader)는 인터넷을 통해 파일을 다운로드하는 프로그램이다. 다운로더는 최근 프로그램에서 지원하는 자체 업데이트 기능으로 볼 수 있다. 하지만, 악성코드나 스파이웨어로 분류되는 다운로더는 대체로 설치된 제품과 독립적으로 실행되며 사용자에게 동의나 통보 없이 실행 파일을 다운로드 해 시스템에 설치한다. 사용자 모르게 프로그램을 설치하는 것도 문제지만 다운로드 된 파일이니 설치된 프로그램이 대부분 사용자들에게 원하지 않는 광고 기능을 출력하는 애드웨어(Adware)라는 점이 사용자들에게 더 큰 피해를 주고 있다. 상당수 프로그램 개발사들은 자신의 프로그램이 일부 손상되거나 삭제되었을 때 사용자 통보 없이 인터넷에서 다운로드 해 재설치하는 기능을 추가하고 약관에 포함시켜 문제가 없다고 한다. 하지만, 이렇게 사용자가 지워도 다시 살아나는 프로그램에 대해 끝없이 스파이웨어 논쟁이 발생하고 있다.

### 스파이웨어 퍼뜨리기

추가 분석을 통해 이 다운로더가 다른 다운로더인 Win-Trojan/Downloader.28672.Q[2]를 다운로드 하는 것으로 확인되었다. 이 트로이목마는 한국산 애드웨어를 설치하는 것으로 밝혀져, 결국 이 다운로더의 목적은 한국에서 제작된 애드웨어를 사용자 모르게 배포하기 위해서였던 것으로 보인다. 보통 애드웨어 제작 업체와 배포 업체는 분리되어, 제작 업체는 배포 업체들에게 책임을 전가하고 있지만 결국 누워서 침 뱉기가 아닐까 싶다.

### 사건의 교훈

사실 이번 날짜 변경 증상은 다운로더의 버그로 추정된다. 애드웨어(Adware)의 오동작으로 시스템에 문제가 발생한 일은 이번이 처음이 아니다. 이전에도 윈도우 시스템에서 오동작을 일으키는 애드웨어인 Win-Trojan/SystEntry.32768.B[3] 와 Win-Trojan/Hotra[1] 등이 발견되

[1] http://info.ahnlab.com/smart2u/virus_detail_4075.html
[2] http://info.ahnlab.com/smart2u/virus_detail_4086.html
[3] http://info.ahnlab.com/smart2u/virus_detail_1096.html

었다. 이전의 사건은 애드웨어 자체의 버그로 인해 발생했다면 이번 사건은 애드웨어를 사용자 몰래 퍼뜨리기 위해 작성된 프로그램의 문제로 발생했다.

애드웨어를 사용자 몰래 컴퓨터에 설치하기 위해 만들어진 악성코드들은 시스템 속도 저하 등의 심각한 문제를 일으킬 수 있다. 애드웨어 제작사들이 자신들의 프로그램이 스파이웨어로 분류되어 억울하다고 생각하기 전에, 진정으로 고객들을 위한다면 자신들의 프로그램이 사용자에게 불편을 주지 않도록 수정해야 할 것이며 자신들의 프로그램 배포를 위해 고용된 배포 업자들을 통해 어떻게 배포되고 있는지도 확인 해야 하지 않을까 싶다. 앞으로도 돈을 목적으로 급조된 애드웨어와 이를 배포하기 위해 제작된 악성코드의 버그로 시스템에 문제가 발생하는 일은 잦아 질 것으로 보인다.

[1] http://info.ahnlab.com/smart2u/virus_detail_1240.html