ASEC Report 12월

® ASEC Report

2008. 1

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 바이러스와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

I. ASEC 월간 통계

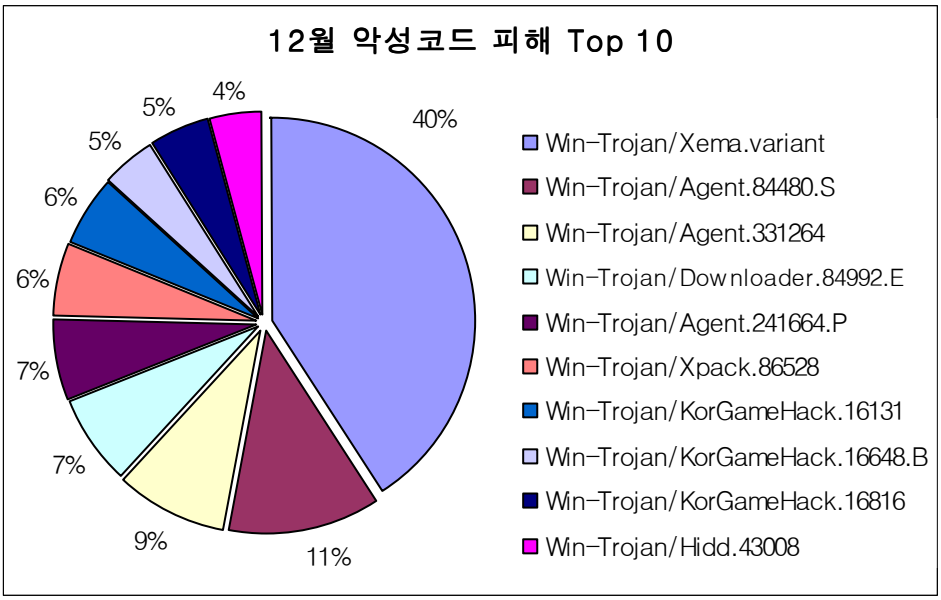
(1) 12월 악성코드 통계

순위		악성코드명	건수	%
1	-	Win-Trojan/Xema.variant	163	41.0%
2	new	Win-Trojan/Agent.84480.S	47	11.8%
3	new	Win-Trojan/Agent.331264	35	8.8%
4	new	Win-Trojan/Downloader.84992.E	29	7.3%
5	new	Win-Trojan/Agent.241664.P	26	6.5%
6	new	Win-Trojan/Xpack.86528	23	5.8%
7	new	Win-Trojan/KorGameHack.16131	22	5.5%
8	new	Win-Trojan/KorGameHack.16648.B	18	4.5%
9	new	Win-Trojan/KorGameHack.16816	18	4.5%
10	new	Win-Trojan/Hidd.43008	17	4.3%
합계			398	100.0%

[표 1-1] 2007년 12월 악성코드 피해 Top 10

[표 1-1]에서 12월 악성코드 피해 Top 10에 랭크 된 상위 10종의 악성코드에 의해서 발생한 피해건수는 398건으로 12월 한달 간 접수된 총 피해건수(5352건)의 7.44%로 12월 한달 전체 악성코드 피해건수에서 차지하는 비중이 크지 않다. 이는 사용자에게 피해를 입히는 악성코드가 다수 발생하고 있는 것을 의미한다고 할 수 있다. 또한, 12월 피해 Top 10에 랭크된 상위 10종에 의해서 발생한 피해건수를 전월(11월)의 Top 10과 비교해 보면 전체적으로 감소하였음을 알 수가 있는데 이는 12월 한달 동안 접수된 전체 악성코드에 대해서 피해건수가 고르게 분산되었기 때문인 것으로 판단된다.

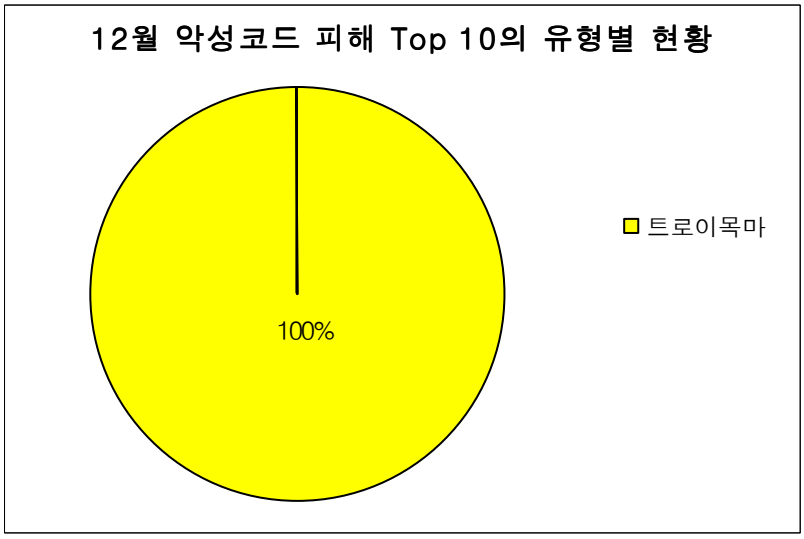
Win-Trojan/Xema.variant의 경우 전월 대비 약 50%의 감염피해 건수가 감소하였으나 전월에 이어 12월 악성코드 피해 Top 10에서도 부동의 1위를 고수하였다. 전월의 경우 Win-Trojan/Xema.variant를 주축으로 온라인 게임 관련 트로이목마 및 드랍퍼가 악성코드 피해 Top 10을 대부분을 차지하였지만 12월의 경우 온라인 게임 관련 트로이목마는 단 3종으로 각각 7, 8, 9위에 랭크 되어 있으며 Win-Trojan/Agent 계열이 각각 2, 3, 5위로 12월 악성코드 피해 Top 10에 새롭게 진입하였다.



[그림 1-1] 2007년 12월 악성코드 피해 Top 10

[그림 1-1]을 보더라도 12월 악성코드 피해 Top 10의 하위권에 랭크 된 온라인 게임 관련 트로이목마 3종이 Top 10에 미치는 영향은 적다는 것을 알 수가 있다. 12월 한달 동안 온라인 게임 관련 트로이목마와 드랍퍼 종류의 악성코드로 인한 피해접수 건수는 2800 여건으로 전체 피해건수의 절반을 넘어선 약 53%를 차지하고 있는데 앞서 언급했던 대로 악성코드 피해건수의 분산화가 원인인 것으로 보인다.

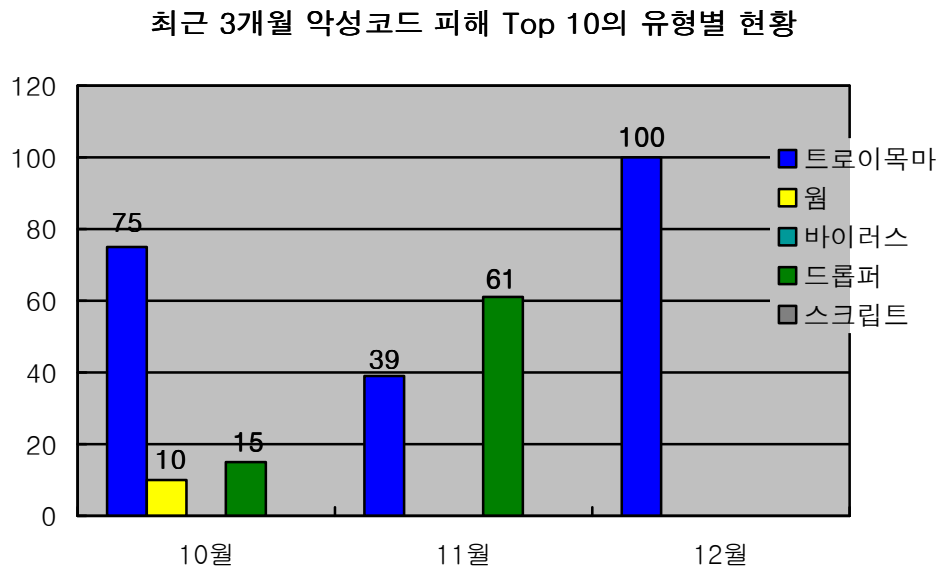
12월 악성코드 피해 Top 10의 유형별 현황



[그림 1-2] 12월 악성코드 피해 Top 10의 유형별 현황

[표 1-1]에 열거된 12월 악성코드 피해 Top 10을 유형별로 분류해 보면 전월과 마찬가지로 금전적인 이득을 노린 트로이목마로 인한 피해가 가장 많이 접수되었음을 [그림 1-2]를 통해서 알 수가 있고 특이한 점은 악성코드 피해건수의 분산화로 인해 12월의 경우 유형별 현황은 트로이목마가 100%를 차지했다는 점이다.

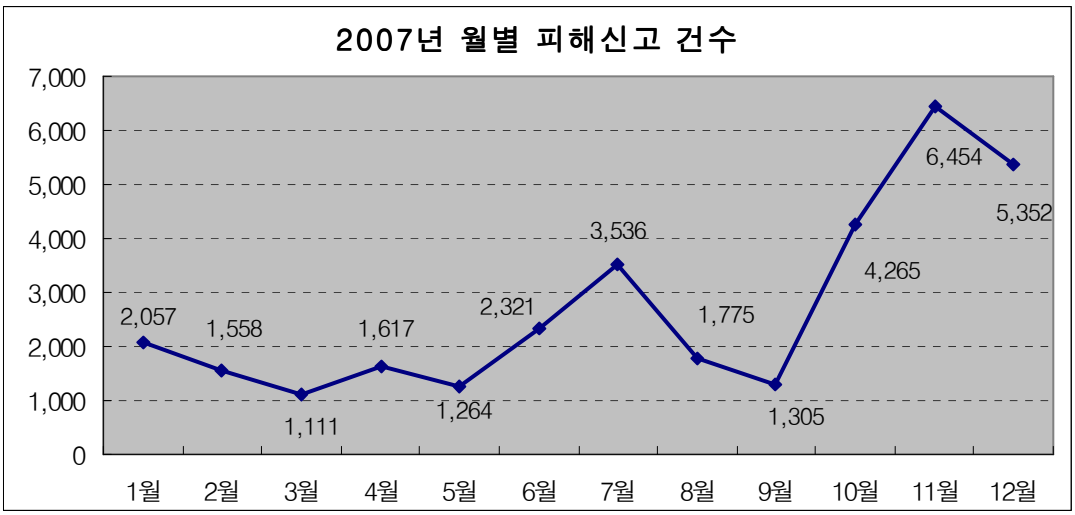
최근 3개월 악성코드 피해 Top 10에 랭크 되었던 악성코드들의 유형별 점유율을 비교해 보면 [그림 1-3]과 같다.



[그림 1-3] 최근 3개월 악성코드 피해 Top 10의 유형별 현황

[그림 1-3]에서 10월의 경우 트로이목마 75%, 웜 10%, 드랍퍼 15%를 점유하면서 전형적인 피해동향 형태임을 알 수가 있다. 그러나 11월에는 트로이 목마가 36%감소, 반면에 드랍퍼가 46% 증가하면서 유형 면에서 나머지 악성코드들은 Top 10 순위권 밖으로 밀려나면서 일부 악성코드 유형에서 나타났던 피해신고 점유율의 편향 현상이 심화되었고 12월에는 트로이목마가 악성코드 피해 Top 10 전체를 점령함으로써 그 현상이 더욱 심화되었다.

2007년 월별 피해신고 건수



[그림 1-4] 2007년 월별 피해신고 건수

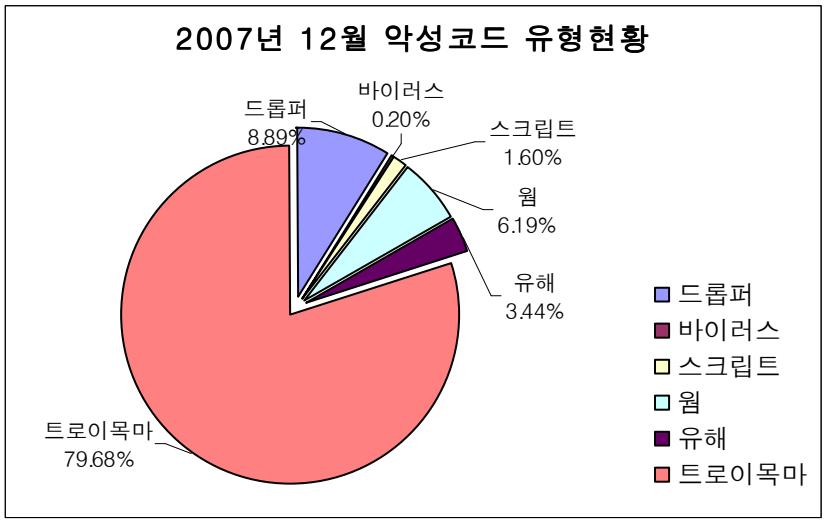
[그림 1-4]를 보면 12월의 총 피해접수 건수는 5,352건으로 전월 대비 17% 감소하였는데 그 원인은 아래 표와 같다.

	11 월	12 월	백분율
트로이목마	4444	4201	↓ (5.47%)
바이러스	29	19	↓ (34.58%)
드랍퍼	1469	493	↓ (66.44%)
유해가능	131	209	↑ (59.54%)
스크립트	151	128	↓ (15.23%)
웜	230	302	↑ (31.30%)
Total	**6454**	**5352**	↓ (17%)

[표 1-2] 최근 2개월간의 악성코드 유형별 피해신고 건수

[표 1-2]를 보면 유해가능과 웜 유형을 제외한 나머지 유형에서 피해신고 건수가 하락했기 때문이다. 그리고 12월의 경우 웜의 피해신고의 상승이 눈에 띄는데 크리스마스 및 새해를 겨냥한 Zhelatin 웜이 집중적으로 발견되었기 때문이다.

피해 신고된 악성코드 유형현황



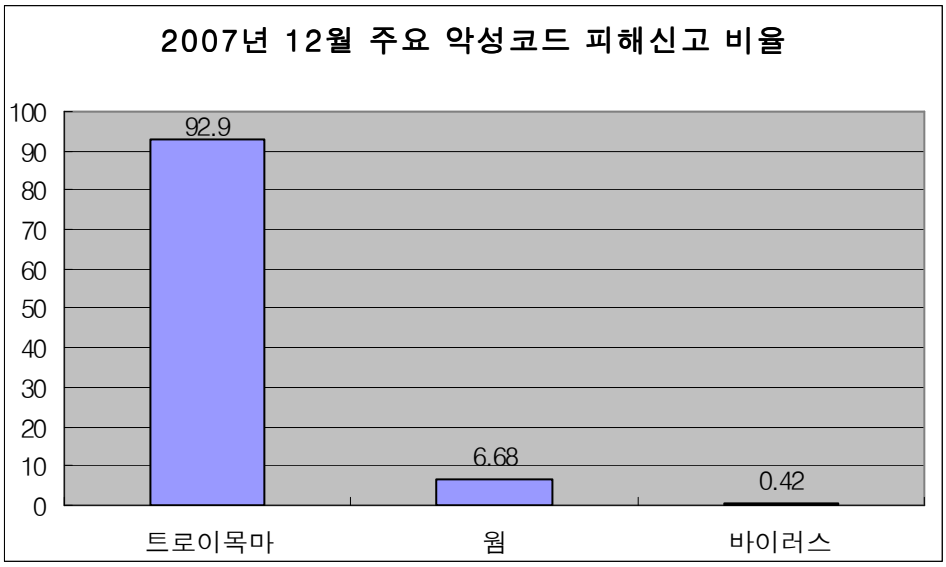
[그림 1-5] 12월 피해 신고된 악성코드의 유형별 현황

[표1-1]과 [그림 1-3]을 통해서 12월 악성코드 피해신고 Top 10의 경우 트로이목마의 점유율이 100%로 편향현상이 심했지만, 전체 악성코드 피해 신고 현황을 보면 [그림 1-5]와 같이 12월에도 전월과 마찬가지로 유사한 형태의 분포를 보이고 있다.

	10 월	11 월	12 월
트로이목마	831(75.55)	1439(79.5)	1596(79.68)
바이러스	2(0.18)	3(0.17)	4(0.20)
드랍퍼	142(12.9)	156(8.62)	178(8.89)
유해가능	28(2.55)	76(4.2)	69(3.44)
스크립트	22(2)	40(2.21)	32(1.60)
웜	75(6.82)	96(5.3)	124(6.19)
Total	1100(100)	1810(100)	2003(100)

[표 1-3] 최근 3개월 악성코드의 유형별 현황

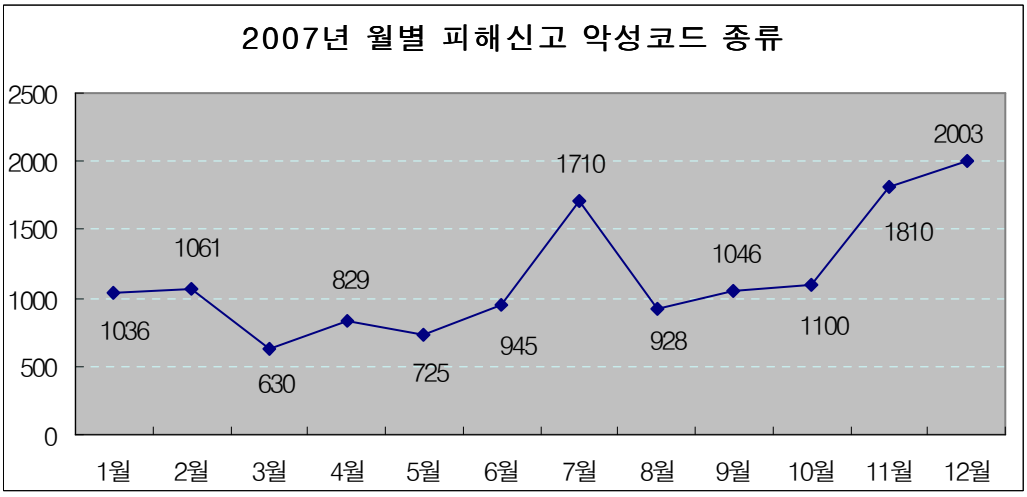
[표 1-3]을 보면 트로이 목마는 유형별 및 점유율에서 꾸준히 상승하고 있으며 드랍퍼의 경우는 해당 월의 유형별 건수는 꾸준히 상승했지만 점유율에서는 소폭의 상승과 하락을 반복하고 있고, 유해가능은 유형별 및 점유율 모두에서 소폭의 상승 및 하락을 반복하고 있다. 이중 주요 악성코드 유형인 트로이목마, 바이러스, 웜에 대한 피해신고 비율을 계산해 보면 [그림 1-6]과 같다.



[그림 1-6] 12월 주요 악성코드 피해신고 비율

[그림 1-6]을 보더라도 12월 악성코드 유형의 피해신고 비율은 전월 대비 큰 폭으로 상승하거나 하락하는 등의 변동은 없었으며 소폭의 상승 및 하락만이 반복될 뿐이다.

월별 피해 신고된 악성코드 종류 현황



[그림 1-7] 2007년 월별 피해신고 악성코드 종류

[그림 1-7]은 바이러스 신고센터로 접수된 2007년 월별 피해 신고된 악성코드의 종류에 대한 현황을 나타내며, 8월 이후로 다시 증가추세를 보이고 있으며, 12월의 경우 [표 1-2]를 통해서 전체 피해건수는 5352건으로 전월 대비 17%로 감소하였음을 알 수 있었으나 그와는 반대로 [그림 1-7]를 통해서 유형별 악성코드 종류는 전월 대비 약 9.64% 상승하였다.

국내 신종(변형) 악성코드 발견 피해 통계

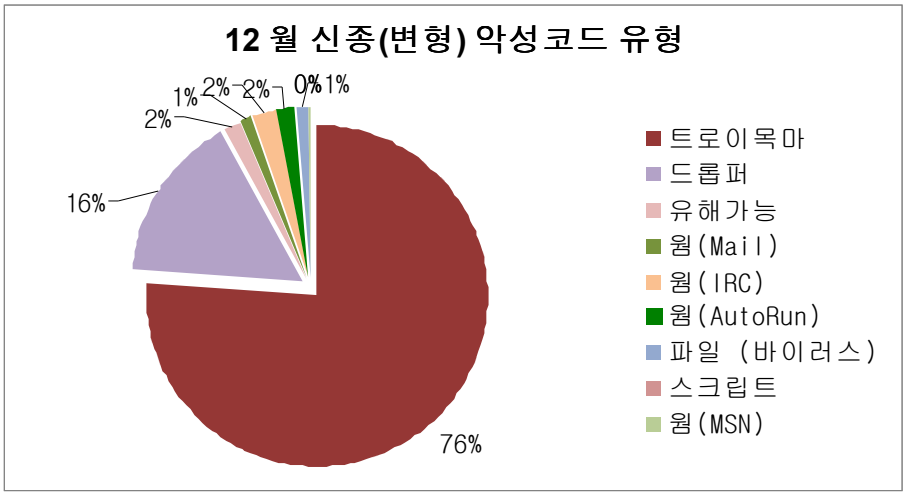
12월 한달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표1-4], [그림1-8]과 같다.

	웜	트로이	드랍퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
10 월	23	269	55	1	2	0	0	0	5	0	355
11 월	24	406	62	1	1	0	0	0	22	1	517
12 월	26	387	80	1	5	0	0	0	9	0	508

[표 1-4] 2007년 최근 3개월간 유형별 신종 (변형) 악성코드 발견현황

이번 달 악성코드는 전체적으로 전월 대비 -2% 감소하였다. 트로이목마 유형은 소폭 감소하였고 드랍퍼 유형은 증가 하였다. 또한 유해가능 프로그램도 전월 대비 감소 하였다. 파일 바이러스는 소폭 증가 하였고 웜 유형은 큰 차이를 보이지 않고 있다.

다음은 이번 달 악성코드 유형을 상세히 분류 하였다.



[그림 1-8] 2007년 12월 신종 및 변형 악성코드 유형

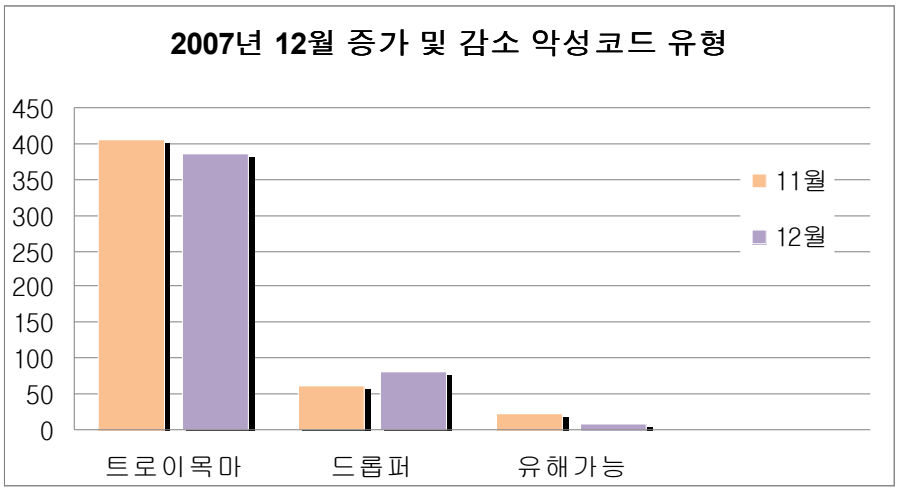
이번 달에도 다양한 유형의 악성코드가 보고 되었는데 Autorun.inf를 만들어 이동식 저장장치에 자신의 복사본과 Autorun.inf 파일을 복사하는 형태가 매달에 발견되고 있다. 악성 IRCBot 웜은 전체 악성코드의 2%로 낮은 비중을 차지고 하고 있으며, 이는 2005년 ~ 06년 전체 악성코드의 반 이상을 차지 했던 때와 비교하면 격감한 것이다. 드랍퍼 유형은 온라인 게임 관련 사용자 계정을 탈취 하는 형태가 전월 대비 29% 증가 하였다. 일반적으로 드랍퍼가 증가하면, 해당 드랍퍼가 드랍하는 트로이목마도 증가 할 것으로 예상할 수 있지만 일반적으로 악성코드 제작자들은 진단 회피 목적으로 드랍퍼만 손을 본다. 즉, 드랍퍼에서 드롭된 파일은 수정하지 않아 기존 엔진에서 진단되는 형태가 많다. 이런 경우를 볼 때 악성코드 제작자들은 단순히 도구만을 이용했거나 악성코드 제작에 지식이 낮은 수준으로 추정 된다

이번 달은 5종의 바이러스가 보고 되었는데 다음과 같다.

- Win32/Diskgen.D
- Win32/Klest.E
- Win32/Mumawow.F
- Win32/Viking.DJ
- Win32/Virut.Gen

위 바이러스들은 모두 올해 발견, 보고 되었던 바이러스에 대한 변형들로 특히 Win32/Virut.Gen 경우는 기존 Win32/Virut 바이러스 원형에 대한 변형이 계속적으로 발견되어 이를 Generic 하게 진단 할 수 있는 방법을 추가 하였고 이에 대한 진단명이다.

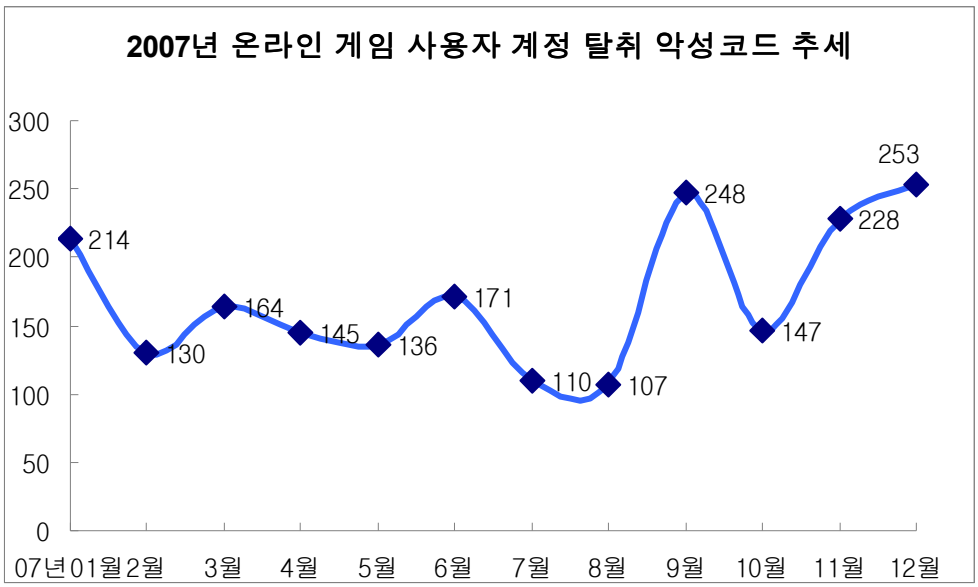
다음은 12 월에 증가 및 감소한 주요 악성코드 유형에 대한 현황이다.



[그림 1-9] 2007년 12월 감소 및 증가 악성코드 유형

위에서도 언급 했듯이 트로이목마는 전월 대비 -5% 감소, 드랍퍼는 29% 증가 하였다. 그러나 온라인 게임의 사용자 계정을 훔쳐내는 악성코드 유형 (트로이목마와 드랍퍼 유형을 합한 수)은 올해 가장 많이 보고 되었다. 이는 해당 유형의 드랍퍼의 증가와 Agent 및 Downloader 유형이 소폭 감소하는 바람에 트로이목마 유형이 상대적으로 전월 대비 소폭 감소 한 것이다.

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



[그림 1-10] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

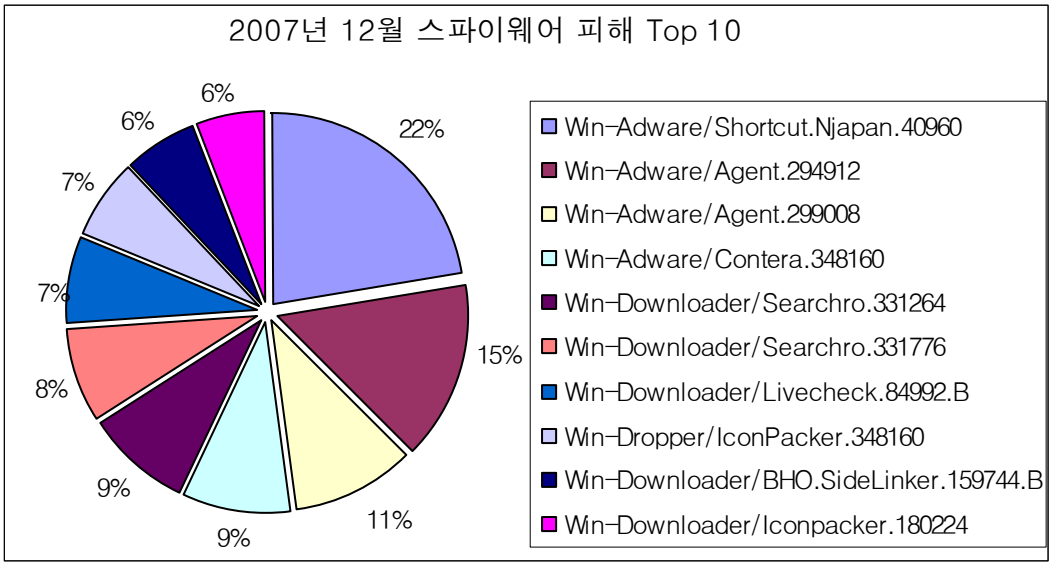
전월 대비 11% 증가한 이 악성코드 유형은 올해 들어 가장 많은 수가 보고 되었다. 특히 온라인 게임 서비스가 우리나라를 비롯 중국, 대만 현지에서도 인기를 끌자 현지 게임을 노리는 형태가 급증 하였다. 특히 중국내 인터넷 사용자와 온라인 게임을 즐기는 사용자가 증가함에 따라서 해당 악성코드의 수도 이에 늘어나는 추세라 하겠다.

(2) 12월 스파이웨어 통계

12월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	↑5	Win-Adware/Shortcut.Njapan.40960	90	22%
2	New	Win-Adware/Agent.294912	59	15%
3	New	Win-Adware/Agent.299008	41	11%
4	↓3	Win-Adware/Contera.348160	37	9%
5	New	Win-Downloader/Searchro.331264	35	9%
6	New	Win-Downloader/Searchro.331776	32	8%
7	New	Win-Downloader/Livecheck.84992.B	29	7%
8	New	Win-Dropper/IconPacker.348160	27	7%
9	New	Win-Downloader/BHO.SideLinker.159744.B	25	6%
10	↓2	Win-Downloader/Iconpacker.180224	23	6%
합계			398	100%

[표 1-5] 2007년 12월 스파이웨어 피해 Top 10



[그림 1-11] 2007년 12월 스파이웨어 피해 Top 10

2007년 12월 전체 스파이웨어 피해신고 건수는 총 1413건으로 지난 11월의 1535건과 비슷한 수치를 기록하였다. 이 중 상위 Top 10 의 스파이웨어 피해신고 건수는 총 398건으로 2007년의 다른 달 보다 그 비중이 높아진 것을 확인할 수 있다. 상위 Top 10 의 대부분은 국내에서 제작된 애드웨어 및 다운로더가 대부분을 차지하고 있으며, 2007년 하반기부터 시작된 국내제작 스파이웨어 피해 증가를 반영하고 있다.

12월 스파이웨어 피해신고 상위 Top 10에는 지난 11월부터 지속적인 피해를 입히고 있는 스파이웨어를 발견할 수 있다. 애드웨어 숏컷 엔재팬(Win-Adware/Shortcut.Njapan.40960)은 사용자 동의 없이 성인 사이트의 바로가기를 바탕화면 및 즐겨찾기 등에 생성하는 애드웨어이다. 다른 여러 스파이웨어의 번들로 설치되기 때문에 피해신고 건수가 많은 것으로 예상되며 지난 11월에도 상위 Top 10의 5위를 기록한 바 있다. 이 외에도 애드웨어 콘테라(Win-Adware/Contera.348160), 애드웨어 아이콘패커(Win-Adawra/Iconpacker.180224) 또한 11월에 이어 지속적인 피해를 입히고 있는 스파이웨어로 다른 스파이웨어의 번들로 설치되는 특징을 가진다.

2007년 12월 유형별 스파이웨어 피해 현황은 [표 1-6]와 같다.

	스파이웨어류	애드웨어	드랍퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
10월	632	131	38	180	7	11	0	0	0	999
11월	480	354	147	525	3	25	1	0	0	1535
12월	325	446	164	461	4	8	4	0	1	1413

[표 1-6] 2007년 12월 유형별 스파이웨어 피해 건수

12월 유형별 스파이웨어 피해 통계를 살펴보면 애드웨어의 피해신고 건수가 스파이웨어류의 피해신고 건수를 상회하고 있는 것을 발견할 수 있으며, 이는 중국에서 제작된 온라인게임 계정 유출 스파이웨어 등의 외국산 스파이웨어 피해 보다 국내에서 제작된 애드웨어와 다운로더의 피해가 상대적으로 많다는 것을 보여준다.

최근의 국내에서 제작된 애드웨어의 배포 방법(다운로더를 이용한 번들 설치)과 피해신고 건수 등의 여러 통계 수치로 미루어 당분간은 국내에서 제작되는 애드웨어 및 다운로더의 피해가 지속될 것으로 생각된다.

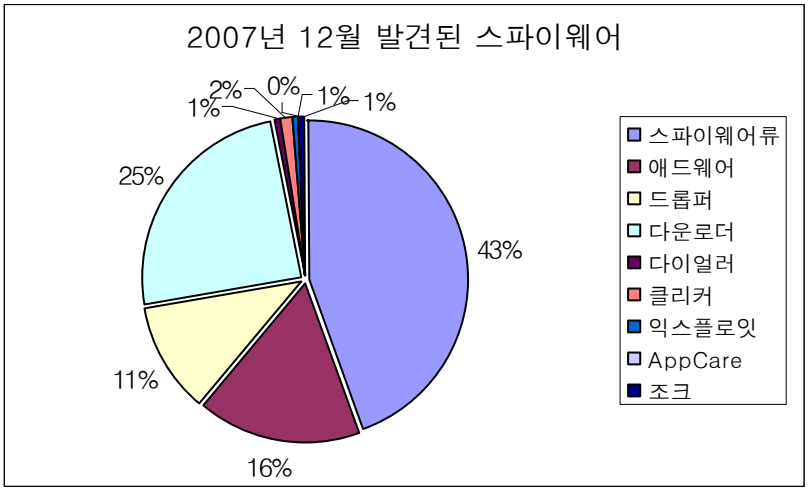
아래 12월 스파이웨어 발견 현황에서 애드웨어와 다운로더의 신종 및 변형 발견 개수는 지난달에 비하여 크게 감소하였으나 오히려 피해신고 건수는 증가하였다. 12월에 새로 발견된 스파이웨어보다 11월 이전부터 피해를 입힌 스파이웨어들이 상대적으로 많은 피해를 입히고 있기 때문이다.

12월 스파이웨어 발견 현황

12월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-7], [그림 1-12]와 같다.

	스파이웨어류	애드웨어	드랍퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
10월	98	42	14	51	5	6	0	0	0	216
11월	99	61	15	112	3	5	0	0	0	295
12월	86	32	22	48	1	3	1	0	1	116

[표 1-7] 2007년 12월 유형별 신종(변형) 스파이웨어 발견 현황

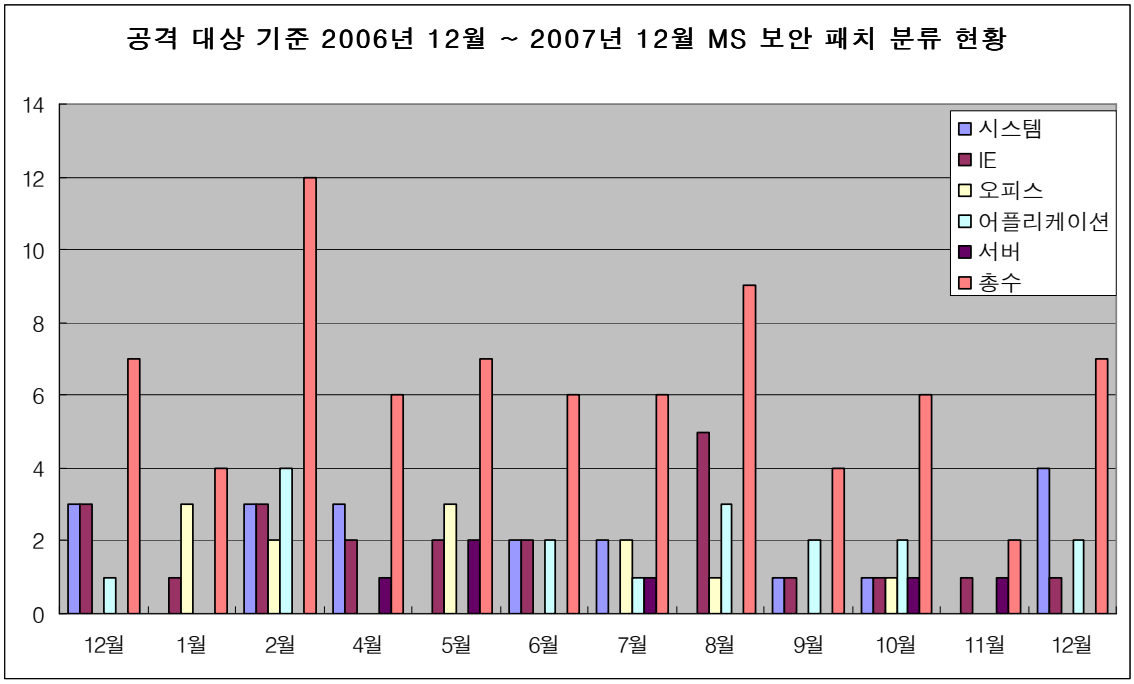


[그림 1-12] 2007년 12월 발견된 스파이웨어 프로그램 비율

[표 1-7]과 [그림 1-12]는 2007년 12월 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 11월 295개의 신종 및 변형 스파이웨어가 발견된 데 비하여 12월에는 116개의 신종 및 변형 스파이웨어가 발견된 데 그쳤다. 주로 온라인게임 계정 유출 스파이웨어로 구성되어 있는 스파이웨어류의 발견 개수는 비슷한 가운데 11월에 많은 비중을 차지하고 있던 애드웨어와 다운로더의 신종 및 변형 발견 개수는 절반 이상 크게 감소한 것을 볼 수 있다.

(3) 12월 시큐리티 통계

2007년 11월에는 이전 달과 비해 마이크로소프트사에서 7개의 보안 업데이트를 발표하고, 발표된 업데이트는 긴급(Critical) 3개, 중요 4개로, 11월의 총 2건에 비해서, 증가하였다. 이 중에서 서버군 제품의 공격에 사용될 수 있는 MS07-065 에 대한 패치가 포함되었으며, 제로데이 공격으로 알려진 Macrovision secdrv.sys 드라이버 파일에 대한 패치인 MS07-067 이 포함된 것이 특징이라고 할 수 있다.

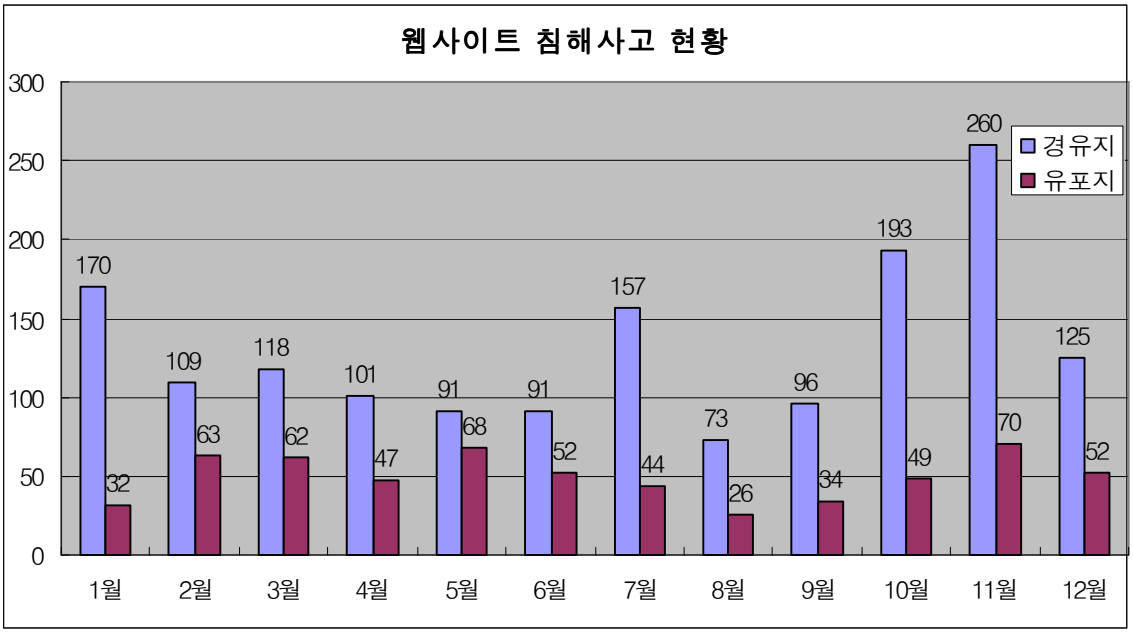


[그림 1-13] 2006년 12월 ~ 2007년 12월 공격대상 기준 MS 보안 패치 현황

[그림 1-13]을 보면, 전반적으로 2007년에 들어와서, 어플리케이션 취약점들(IE, 오피스, 기타 어플리케이션) 취약점들이 증가 추세에 있는데 반해, 서버 관련 취약점들은 줄어든 것을 알 수 있다. 그러나, 12월에 Message Queuing의 취약점으로 인한 원격 코드 실행 문제점 MS07-065 는 특히 윈도우 2000 서버군 제품(2000 서버, Advanced 서버 등)을 원격에서 공격할 수 있기 때문에, 주의가 필요하다.

12월에 발표된 마이크로소프트사의 패치의 특징중 하나인 윈도우 미디어 플레이어 관련 취약점(MS07-068)과 DirectX 취약점 (MS07-064)는 미디어/동영상 관련 파일들에서 길이값을 검사하지 않아서 오버플러우등의 문제가 발생하는 것으로, 조작된 미디어/동영상 파일들에 악성코드가 포함 되어져 메일이나 웹을 통해 공격가능하기 때문에, 신뢰하지 않는 사용자에게서 오는 미디어/동영상 파일들에 대한 주의가 필요하다. 비단 오피스 파일의 공격뿐만 아니라, 기타 어플리케이션들의 취약점 또한 증가 추세임으로, 안전한 시스템 사용을 위해서는 항상 보안 패치가 필요하다.

2007년 12월 웹 침해사고 현황



[그림 1-14] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2007년 12월의 웹 사이트 침해지/배포지 수는 125/52로 2007년 12월과 비교하여 침해지수가 크게 감소하였다. 침해지수의 감소에 대한 원인은 별도 분석이 필요하지만, 비록 침해지수가 감소가 배포지수 감소를 의미하지는 않고 여전히 지난달과 비슷하다. 이는 소수의 공격자의 의해 다수의 웹사이트가 침해되고 있으며. 그리고 계속해서 새로운 사이트가 공격 대상이 되고 있다는 것을 나타낸다.

또한 2007년 12월의 경향중 특이한 점은 MS07-017 취약점을 이용하는 배포 비율이 13%로 2007년 11월 비해 큰 폭으로 감소하였다는 것이다. 공격자의 배포경향이 바뀐 것이 원인일수도 있고 다른 원인이 존재할 수 있다. 보다 정확한 분석은은 2008년 1월 통계 결과를 보아야만 알 수 있을 것이다.

II. ASEC Monthly Trend & Issue

(1) 악성코드 - 연말 연시와 관련된 악성코드

이번 달은 한 해의 마지막 달로써 연말 연시와 관련된 악성코드 소식을 자주 접 할 수 있었다. 그 중 하나는 올해 가장 맹위를 떨쳤던 Win32/Zhelatin.worm 변형이고, 다른 하나는 MSN 메신저로 자신을 전파하는 악성 IRCBot 웜이다. 둘다 크리스마스와 새해 인사를 가장한 내용을 가지고 사용자들의 호기심을 자극하고 있다.

► 연말연시와 관련된 내용을 담은 악성코드들

먼저, Win32/Zhelatin.worm (이하 젤라틴 웜) 은 다양한 메일제목과 본문을 가지고 유포 되고 있다. 연말 연시를 맞아 이 웜의 변형이 어김없이 등장하였고 이와 관련해서 국내,외에서 약간의 이슈가 되었다. 다음과 같은 제목과 내용으로 전파 되었다.

메일 제목 : Seasons Greetings 메일 내용 : his Christmas, we want to show you something you will really enjoy. This might not be fun for the whole family, but I bet you'll like it come one take 2 min and check it out. H??p://merrychristmas(제거됨).com/

[표 2-1] 젤라틴 웜이 첨부된 메일 제목과 본문

메일 본문 하단의 링크를 클릭하면 다음과 같은 그림이 보여지는 웹 사이트로 연결 된다. 그리고 페이지내 어디를 클릭하여도 'stripshow.exe' 란 파일을 다운로드 하도록 유도 한다.

[그림 2-1] 젤라틴 웜이 유도하는 웹 페이지 일부 그림

해당 파일을 실행하면 C:₩WINDOWS₩disnisa.exe에 자신의 복사본을 생성한다. 그리고 특정 UDP 포트를 이용하여 외부의 호스트로 접속 한다. 이곳은 P2P 기반의 봇넷으로 이후 공격자는 파일전송, 메일 발송, DDoS 와 같은 공격을 수행 할 수 있게 된다. 또한 로컬 드라이브에서 [그림 2-2]의 윗쪽에 있는 확장자로부터 메일주소를 수집하거나, [그림 2-2]의 아래쪽에 있는 문자열을 포함하는 특정 메일주소로는 자신이 첨부되지 않도록 한다. 이는 일반적으로 안티 바이러스 업체 쪽에서 악성코드 샘플을 수집하는 메일 주소에 포함되어 있기 때문이다.

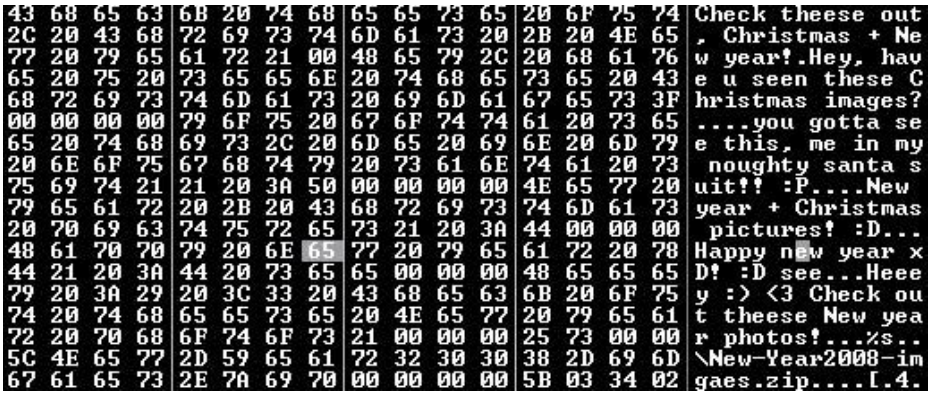
```
00418470  2E 6C 73 74 00 00 00 00 2E 64 61 74 00 00 00 00  .lst.....dat....
00418480  2E 6A 73 70 00 00 00 00 2E 64 68 74 6D 00 00 00  .jsp.....dhtm...
00418490  2E 6D 68 74 00 00 00 00 2E 63 67 69 00 00 00 00  .mht.....cgi....
004184A0  2E 75 69 6E 00 00 00 00 2E 6F 66 74 00 00 00 00  .uin.....oft....
004184B0  2E 78 6C 73 00 00 00 00 2E 73 68 74 00 00 00 00  .xls.....sht....
004184C0  2E 74 62 62 00 00 00 00 2E 61 64 62 00 00 00 00  .tbb.....adb....
004184D0  2E 77 73 68 00 00 00 00 2E 70 6C 00 2E 70 68 70  .wsh.....pl..php
004184E0  00 00 00 00 2E 61 73 70 00 00 00 00 2E 63 66 67  .....asp.....cfg
004184F0  00 00 00 00 2E 6F 64 73 00 00 00 00 2E 6D 6D 66  .....ods.....mmf
00418500  00 00 00 00 2E 6E 63 68 00 00 00 00 2E 65 6D 6C  .....nch.....eml
00418510  00 00 00 00 2E 6D 64 78 00 00 00 00 2E 6D 62 78  .....mdx.....mbx
00418520  00 00 00 00 2E 64 62 78 00 00 00 00 2E 78 6D 6C  .....dbx.....xml
00418530  00 00 00 00 2E 73 74 6D 00 00 00 00 2E 73 68 74  .....stm.....sht
00418540  6D 00 00 00 2E 68 74 6D 00 00 00 00 2E 6D 73 67  m....htm.....msg
00418550  00 00 00 00 2E 74 78 74 00 00 00 00 2E 77 61 62  .....txt.....wab

00418300  70 6F 73 74 6D 61 73 74 65 72 40 00 72 6F 6F 74  postmaster@.root
00418310  40 00 00 00 6C 6F 63 61 6C 00 00 00 6E 6F 72 65  @...local...nore
00418320  70 6C 79 00 40 61 76 70 2E 00 00 00 70 67 70 00  ply.@avp....pgp.
00418330  73 70 61 6D 00 00 00 00 63 61 66 65 65 00 00 00  spam....cafee...
00418340  70 61 6E 64 61 00 00 00 61 62 75 73 65 00 00 00  panda...abuse...
00418350  73 61 6D 70 6C 65 73 00 77 69 6E 72 61 72 00 00  samples.winrar..
00418360  67 6F 6F 67 6C 65 00 00 77 69 6E 7A 69 70 00 00  google..winzip..
00418370  40 6D 65 73 73 61 67 65 6C 61 62 00 66 72 65 65  @messagelab.free
00418380  2D 61 76 00 40 69 61 6E 61 00 00 00 40 66 6F 6F  -av.@iana...@foo
00418390  00 00 00 00 73 6F 70 68 6F 00 00 00 63 65 72 74  ....sopho...cert
004183A0  69 66 69 63 00 00 00 00 6C 69 73 74 73 65 72 76  ific....listserv
004183B0  00 00 00 00 6C 69 6E 75 78 00 00 00 62 73 64 00  ....linux...bsd.
```

[그림 2-2] 젤라틴 웜이 메일 주소를 수집하는 파일 확장자와 수집제외 문자열

두번째로는 Win32/MsnBot.worm.59895 이다. 해당 악성코드는 올해 많은 보고가 있었던 MSN 웜의 일종이다. 이들은 IRC 서버에 접속하여 공격자의 명령에 따라서 메신저를 통하여 자신을 첨부하여 메시지를 보낸다. 실행하면 윈도우 폴더에 msmsgrsu.exe 란 자신의 복사본을 생성한다. 그리고 특정 IRC 서버로 접속하며 명령을 대기 한다.

그리고 다음과 같은 메시지를 메신저 상대방에서 보내고 덧붙여 'New-Year2008-imgaes.zip' 파일을 보내어 실행을 유도 한다.



[그림 2-3] MsnBot 웜이 보내는 메시지와 첨부파일명

연말 연시가 되면 그랬듯이 악성코드 제작자들은 사용자의 호기심을 자극하는 주제를 가지고 악성코드 전파에 곧 잘 사용한다. 올해도 어김없이 사용된 연말 연시와 관련된 내용은 조금만 주의를 기울이면 악성코드가 보낸 것 인지하여 악성코드로 인한 피해를 예방할 수 있다.

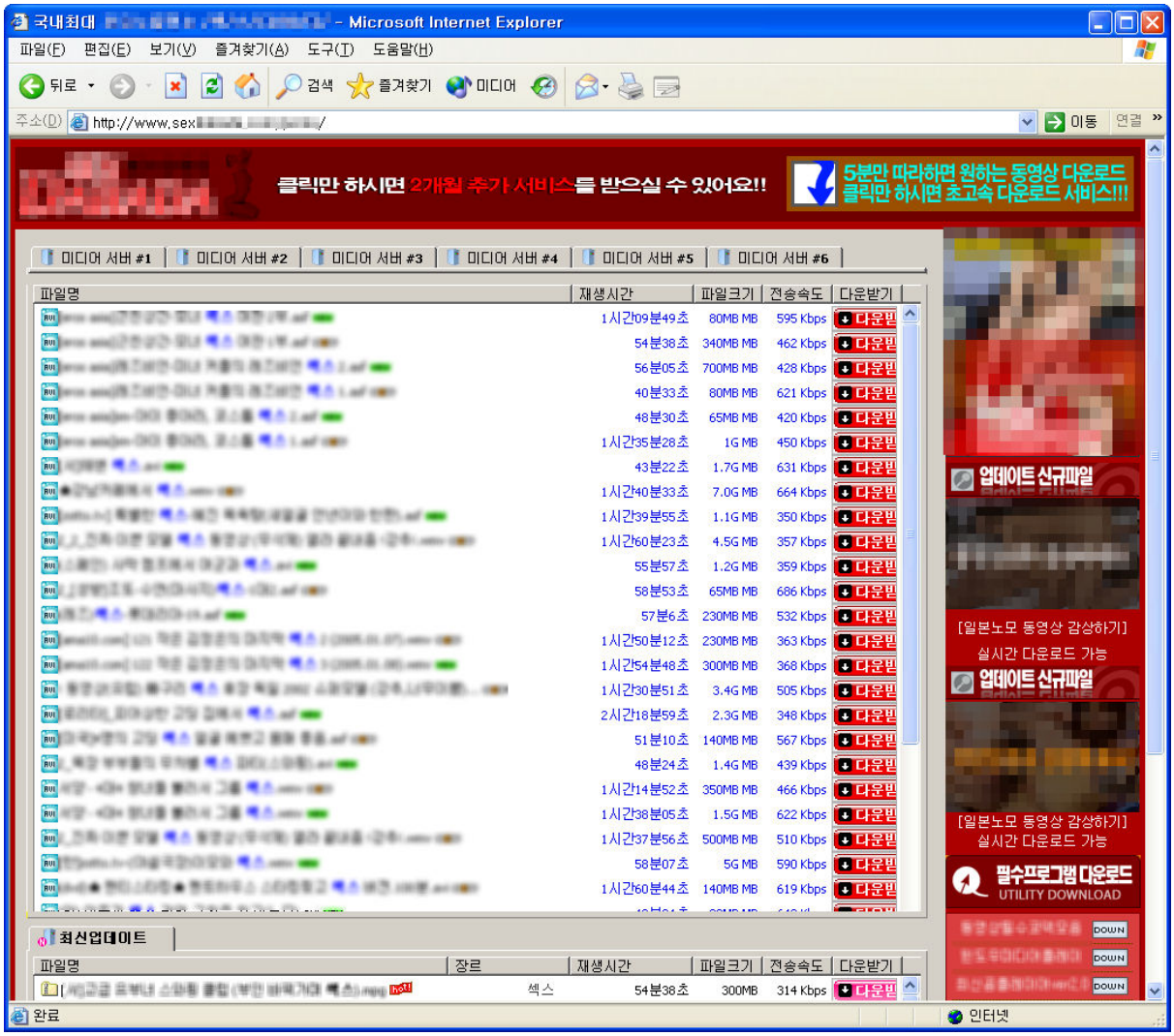
(2) 스파이웨어 – 더욱 교묘해지는 스파이웨어의 배포 및 수익 구조

“무제한동영상”이라는 아이콘이 바탕화면에 보인다면 어떻게 할까? 아마 대부분 사용자들이 제목만 보고는 해당 아이콘을 더블클릭 하고 있는 자신을 발견할 것이다. 하지만 이것은 시작에 불과하다. 이런 과정으로 방문한 사이트에선 무료를 가장해 유료 결제를 유도하여 금전적 피해를 입히는 경우가 종종 발견되고 있기 때문이다.

최근 국내에서 지속적으로 발견되고 있는 다운로더인 Win-Downloader/KorAdware의 경우 보안 취약점을 이용해 사용자의 컴퓨터에 설치되어 공격자가 설치하고자 하는 다른 스파이웨어를 추가로 다운로드 하여 설치하는 사례가 급증하고 있다. 이는 보안 업체 및 관련 기관의 지속적인 홍보로 ActiveX로 스파이웨어가 설치될 수 있음이 널리 알려져 이를 조심하는 사용자들이 증가함에 따른 대안책으로 보인다. 과거엔 스파이웨어 제작사로부터 설치 건당 일정 금액을 받거나 광고 노출로 수익을 얻는 구조가 대부분 이였지만, 최근엔 사용자의 주머니에서 직접 돈을 빼내기 위해 결제를 유도하는 형식이 증가하고 있다. Win-Downloader/KorAdware가 사용자 몰래 다운로드하고 실행하는 Win-Adware/Shortcut.SDabada의 경우 바탕화면, 빠른실행, 프로그램 메뉴, Internet Explorer의 즐겨찾기등에 “무제한동영상”이라는 아이콘을 생성한다.

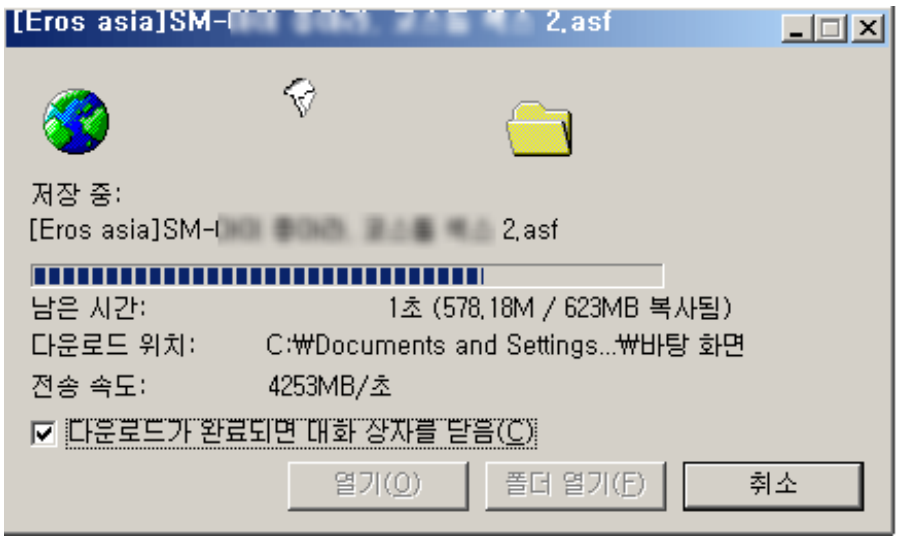
[그림 2-4] 사용자 동의 없이 생성된 인터넷 바로가기 아이콘

이 아이콘을 더블 클릭하면 [그림 2-5]와 같이 호기심을 불러 일으키는 선정적인 제목의 동영상 목록을 보여주며, 클릭을 유도한다.



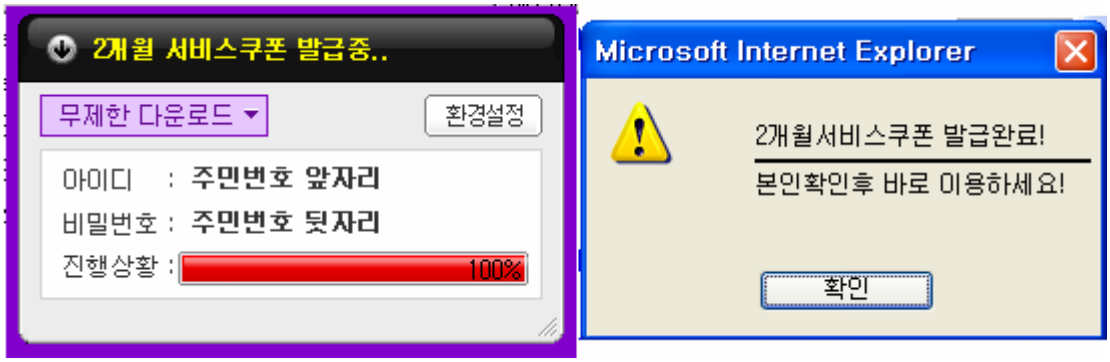
[그림 2-5] 선정적인 제목의 동영상 목록을 가진 사이트로 연결됨

해당 목록을 클릭할 경우 [그림 2-6]과 같이 허위로 다운로드 하는 화면을 보여준다. 이 과정은 파일을 다운로드 하는 것이 아니라 사용자를 속이기 위한 단순한 움직이는 그림 파일이다.



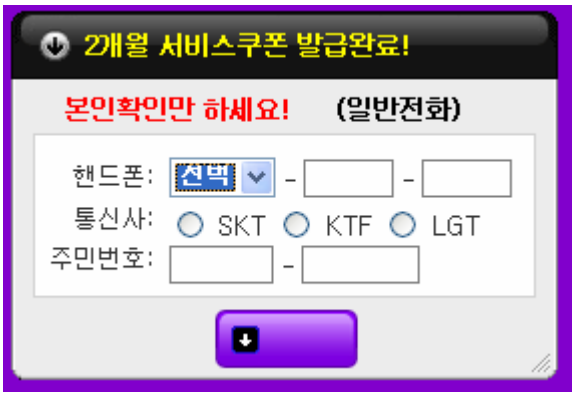
[그림 2-6] 허위 다운로드 과정을 표시한 그림 파일

곧바로, 무료 서비스 쿠폰이 발급되었다는 허위 메시지를 출력한다. 메시지 내용만 보면 2개월 동안 무료로 사용할 수 있는 쿠폰이 발급 되었으며, 본인 확인 과정만 거치면 되는 것처럼 표시하고 있다.



[그림 2-7] 무료 서비스 쿠폰 발급을 사칭한 허위 메시지

[확인] 버튼을 누르면 본인을 확인하는 창이 나타난다. 하지만, 이 창은 본인 확인 기능이 아니라 유료 서비스 소액 결제 화면이다.



[그림 2-8] 본인 확인을 사칭한 허위 메시지

해당 페이지의 HTML(Hyper Text Markup Language)의 소스를 살펴보면 다음과 같이 33000원을 결제하는 페이지임을 쉽게 알 수 있다.

```
<INPUT TYPE="HIDDEN" NAME="Carrier" value="">
<INPUT TYPE="HIDDEN" NAME="ItemAmt" value="33000">
<INPUT TYPE="HIDDEN" NAME="ItemName" value="www.s[illegible]m_MB">
<INPUT TYPE="HIDDEN" NAME="Amount" value="33000">

<INPUT TYPE="HIDDEN" NAME="skin" value="5">
<INPUT TYPE="HIDDEN" NAME="_price_" value="33000">
<INPUT TYPE="HIDDEN" NAME="etc" value="">

<INPUT TYPE="HIDDEN" NAME="skin" value="">
<INPUT TYPE="HIDDEN" NAME="etc" value="">
```

[그림 2-9] 소액 결제 페이지 HTML 소스

스크롤바를 이용하여 해당 사이트의 하단을 살펴보면 다음과 같은 안내 메시지를 확인할 수 있다.

"본 사이트는 온라인정보제공료 (1개월 3,000원 10개월사용 + 무료서비스2개월 VAT별도)가 청구 됩니다. 본 사이트 가입후 정보이용시 온라인정보업 특정상 환불은 안됩니다."

사용자의 동의 없이 설치된 스파이웨어가 사용자를 특정 사이트로 접속을 하게한 뒤, 무료라는 가짜 미끼를 사용하여 33000원의 유료 결제를 유도하는 방식이다. 또한 환불이 불가능하다는 문구를 사용자가 쉽게 확인할 수 없는 영역에 삽입해 놓고 있어 환불 과정에서 사용자와 해당 업체와의 마찰이 예상된다.

따라서 이러한 피해를 예방하기 위해서는 다음 사항은 꼭 확인 해야 한다.

1. **윈도우 업데이트를 주기적으로 실행한다.**
   윈도우 업데이트는 윈도우에서 발견된 각종 보안 취약점을 해결한 것으로 보안의 시작이라 할 수 있다. 미국 시간 기준으로 매월 둘째 주 화요일에 업데이트가 발표되므로 매달 둘째 주 수요일에 윈도우 업데이트를 확인하는 것이 좋다.

2. **대가가 없는 무료는 없으며, 개인 정보를 요구할 경우는 일단 의심 해 보아야 한다.**
   개인 정보의 경우 악의적인 용도로 사용될 소지가 매우 높으며 이렇게 입은 피해를 보상받기 위해선 많은 노력과 시간이 필요하므로, 신뢰할 수 있는 사이트가 아닌 경우엔 가능하면 요청에 응하지 않는 것이 바람직하다.

3. **신뢰할 수 있는 보안 업체에서 제공하는 보안 제품을 사용하며 자동 업데이트를 활성화 시켜 놓아야 한다.**
   최근 보안 위협 채널이 다양화됨에 따라 이런 위협에서 보다 효과적으로 대응하기 위해서는 신뢰할만한 보안 업체에서 제공하는 통합 보안 제품을 사용하는 것이 바람직하다. 또한 여러 이유로 자동 업데이트를 비활성화 시켜 놓는 경우가 많은데 보안 제품의 특성상 이는 바람직하지 않으므로 활성화 시켜 놓는 것이 좋다.

(3) 시큐리티 - Mac OS X 보안 위협 증가

마이크로소프트사는 총 7개의 패치를 2007년 12월 정기보안 업데이트에 포함하여 발표하였다. 이중 위험등급이 긴급(critical)인 패치의 개수는 3개이며 중요(important)인 패치의 개수는 4개이다. 2007년 12월에 발표된 패치의 개수(7개)는 2007년 총 평균(5.7개)과 비교하여 약간 큰 수치로 다른 달과 비교하여 특별히 많은 수의 취약점이 보고되었다고 보기는 힘들다. [표 2-2]은 2007년 12월 발표된 취약점의 목록 및 공격 코드 공개 여부이다.

위험등급	취약점	PoC
긴급	DirectX의 취약점으로 인한 원격 코드 실행 문제점 (07-064)	무
긴급	Windows Media 파일 형식의 취약점으로 인한 원격 코드 실행 문제점 (07-068)	무
긴급	Internet Explorer 누적 업데이트 (07-069)	무
중요	SMBv2의 취약점으로 인한 원격 코드 실행 문제점 (07-063)	무
중요	Message Queuing의 취약점으로 인한 원격 코드 실행 문제점 (07-065)	유
중요	Windows 커널의 취약점으로 인한 권한 상승 문제점 (07-066)	무
중요	Macrovision 드라이버의 취약점으로 인한 로컬 권한 상승 문제점 (07-067)	무

[표 2-2] 2007년 12월 마이크로 소프트 정기 보안 패치

아직까지 공격코드가 공개된 MS07-065 취약점 이외의 취약점에 대한 공격코드는 공개되지는 않았지만 발표된 취약점 모두 코드 실행이 가능하거나 관리자 권한의 획득이 가능한 취약점이기 때문에 반드시 마이크로소프트에서 제공하는 보안 업데이트를 설치하여 운영체제나 관련 제품의 상태를 항상 최신의 것으로 유지하도록 해야 한다.

Mac 환경에서 위협의 증가

2007년 11월 트렌드에서 Mac 환경에서의 보안 위협을 지적한 이후, Mac 환경에서의 위협이 계속 증가하고 있다. 2007년 12월에 공격코드가 공개된 Mac 운영체제의 취약점은 총 4개이다. [표 2-3]은 2007년 한해 발표된 취약점의 위험 등급과 개수를 윈도우 운영체제(XP, Vista)와 Mac 운영체제를 비교한 것이다. (http://blogs.zdnet.com/security/?p=758)

	XP	Vista	XP + Vista		Mac OS X
매우 심각	3	1	4		0
심각	19	12	23		234
위험	2	1	3		2
중요	3	1	4		7
총계	34	20	44		243

월평균	2.83	1.67	3.67		20.25

[표 2-3] 2007년 Windows XP, Vista, Mac OS X 취약점 통계

지금까지는 윈도우 운영체제의 취약점의 개수가 다른 운영체제보다 높다는 것이 일반적인 인식이었다. 하지만 위 표에 따르면 Mac 운영체제의 보고된 취약점의 개수는 243으로 윈도우 운영체제의 44개 보다 5배 가량 높은 것으로 나타났다. 비록 Mac 운영체제의 시장 점유율이 윈도우 운영체제의 점유율보다 낮을 뿐만 아니라 실제 공격 코드의 개수도 윈도우 운영체제의 것이 훨씬 많긴 하지만 Mac 환경에서의 보안 위협이 점차 증가 하고 있다는 것은 Mac 운영체제의 중요도가 점점 높아지고 있다는 것을 나타내는 것이다. 따라서 앞으로도 계속 주의를 기울여야 할 것이다.

Adobe Flash Player 다중 취약점 패치 발표

2007년 12월 총 9개의 Flash Player의 취약점 패치가 발표되었다. UCC등 웹에서 사용 가능한 컨텐츠의 내용이 다양해지면서 플래시 파일의 사용도 폭발적으로 증가하고 있다. 이에 따라 보안 위협의 심각성도 증가하고 있다. 이번에 발표된 다중 취약점 중 4개의 취약점이 사용자의 시스템에서 임의의 코드를 실행하거나 권한 상승이 가능한 취약점으로 Flash 플레이어를 사용하는 사용자는 반드시 패치를 해야 한다. [표 2-4]는 발표된 취약점의 종류 및 설명이다.

취약점 번호	취약점 설명
CVE-2007-4324	플래시 파일이 실행될 때 원격에서 열려진 포트 정보를 알수 있는 취약점
CVE-2007-4768	플래시 파일을 처리할 때 발생하는 원격 코드 실행가능
CVE-2007-5275	DNS Rebinding을 이용한 크로스 사이트 스크립트 취약점
CVE-2007-5476	Mac 운영체제의 오페라 웹브라우저와 관련한 취약점
CVE-2007-6242	JPG 헤더 분석 과정에서 발생하는 힙 오버 플로우 취약점
CVE-2007-6243	웹서버내 보안 정책을 우회하는 권한 상승 취약점
CVE-2007-6244	액션스크립트중 특정 함수의 파라미터 값을 올바르게 처리하지 못해 발생하는 원격 코드 실행 취약점
CVE-2007-6245	HTTP 헤더를 조작하여 발생하는 크로스 사이트 스크립팅 취약점
CVE-2007-6246	메모리 접근 권한을 설정하는 과정에서 발생하는 권한 상승 취약점

[표 2-4] 2007년 12월 발표된 플래시 플레이어 취약점

공격자는 조작된 플래시 파일을 웹서버에 게시하여 사용자들의 접속을 유도하고 플래시 파일을 사용자의 시스템에서 실행하여 임의의 코드를 실행하거나 권한을 획득할 수 있다. 플래시 파일은 우리가 인터넷을 하면서 항상 접하게 되는 것이니 만큼 일반 사용자는 반드시 패치를 설치하여 해당 어플리케이션의 상태를 항상 최신의 것으로 유지하도록 해야 한다.

고도화된 악성 웹페이지 암호화

악성 코드를 배포하기 위해 웹서버에 게시되는 악성 페이지들은 대부분 안티바이러스 프로그램의 진단을 우회하기 위해 암호화 되는 것이 대부분이다. 이를 위하여 사용되었던 암호화 알고리즘은 일부 공격자에 의해서 고안된 단순한 것들이 많았으나 2007년 큰 문제가 되었던 Mpack, ICEPack등 자동화된 웹 익스플로잇 툴킷에 의하여 점점 고도화되고 있는 추세이다. [그림 2-10]은 2007년 12월 실제 해커의 의해 변조되어 게시되었던 악성 웹 페이지의 일부이다.

```
function xxtea_decrypt(Cu26,NcC27)
{
    if(Cu26=="")
    {
        return "";
    }

    var mMFb28=str2long(Cu26,false);
    ....
    return long2str(mMFb28,true);
```

[그림 2-10] 암호화에 사용된 XXETA 알고리즘

웹페이지를 암호화하는데 XXETA 알고리즘이 사용되었을 알수 있다. XXETA 1998년 발표된 암호화 알고리즘으로 XETA 알고리즘을 개량한 것이다. (http://en.wikipedia.org/wiki/XXTEA 참조) 또한 암호화 코드에 사용되는 변수명 등이 일반적인 단어가 아닌 것으로 보아 웹 페이지의 변조에 Mpack등의 웹 익스플로잇 툴킷이 사용되었을 가능성이 매우 높다고 추정할 수 있다. 실제 이 페이지에 사용된 암호화 알고리즘은 XXETA 알고리즘 이외에 총 4개로 암호화가 적용된 순서는 다음과 같다. (http://fullc0de.egloos.com/3484340 참조)

A. HEX 인코딩
B. BASE64 인코딩
C. XXETA 인코딩
D. UTF-16 인코딩

다음 코드 [그림 2-11]은 최종 복호화가 끝난 것으로 취약점이 존재하는 다수의 ActiveX 객체를 공격하여 악성 코드를 배포한다. 여러 개의 Active X 객체를 동시에 공격하는 웹 익스플로잇 툴킷의 특성을 고려하면 역시 이 페이지는 Mpack등과 같은 웹 익스플로잇 툴킷에 의해 제작되었음을 알 수 있다.

```
try {
    var e;
    var ado=(document.createElement("object"));
    ado.setAttribute("classid","clsid:[redacted]");
    var as=ado.createobject("Adodb.Stream","")
}
...
try {
    var f;
    var storm=new ActiveXObject("[redacted]")
}
...

try {
    var g;
    var pps=new ActiveXObject("[redacted]")
}

try {
    var h;
    var obj=new ActiveXObject("[redacted]")
}
```

[그림 2-11] 최종 복호화가 끝난 코드

웹페이지를 이용한 악성 코드의 배포는 불특정 다수를 대상으로 할 수 있다는 장점 때문에 공격자들이 가장 선호하고 있는 공격방법중에 하나 이다. 주로 윈도우 운영체제의 취약점을 공격하였던 과거와는 달리, Mpack등의 웹 익스플로잇 툴킷이 출현하면서 다수의 ActiveX 객체들을 공격하는 것으로 특징이 변화되고 있다. 아울러 AV 제품의 진단을 우회하기 위한 암호화 방법도 갈수로 고도화 되고 있으며, 이에 따른 대책의 필요성도 높아지고 있다. 사용자는 의심스러운 웹페이지는 방문하지 말아야 하며 AV제품의 상태도 항상 최신의 것으로 유지하여 악성 코드로부터 자신의 시스템을 보호하여야 한다.

III. 2007년 동향

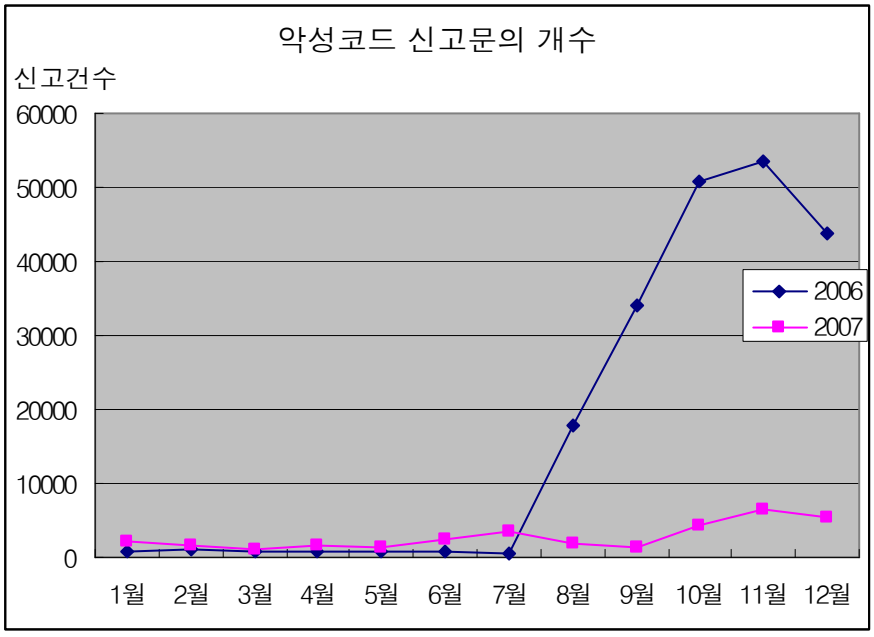
(1) 2007년 악성코드 피해 동향

2007년 악성코드 통계

2006년은 Netsky, Bagle, Mytob같은 전형적인 매스 메일러(Mass Mailer)형 웜들의 지속적인 강세와 Virut 바이러스의 등장 그리고 8월부터 12월까지 폭발적인 Virut 바이러스에 의한 감염 피해신고 등으로 인해 전체 악성코드 피해신고가 많았던 반면, 2007년은 2006년까지 악성코드 피해통계에서 항상 상위권을 점유했던 매스 메일러 (Mass Mailer)형 웜들의 몰락과 Virut 바이러스의 피해신고 감소하였고, 대신 트로이목마 및 스파이웨어 등으로 인한 피해신고가 많았다.

	1 월	2 월	3 월	4 월	5 월	6 월	7 월	8 월	9 월	10 월	11 월	12 월	**합계**
2006	914	1054	833	825	729	808	668	17755	34174	50771	53639	43902	**206072**[1]
2007	2057	1558	1111	1617	1264	2321	3536	1775	1305	4265	6454	5352	**31653**

[표 3-1]2006, 2007년 국내 악성코드 피해신고 건수

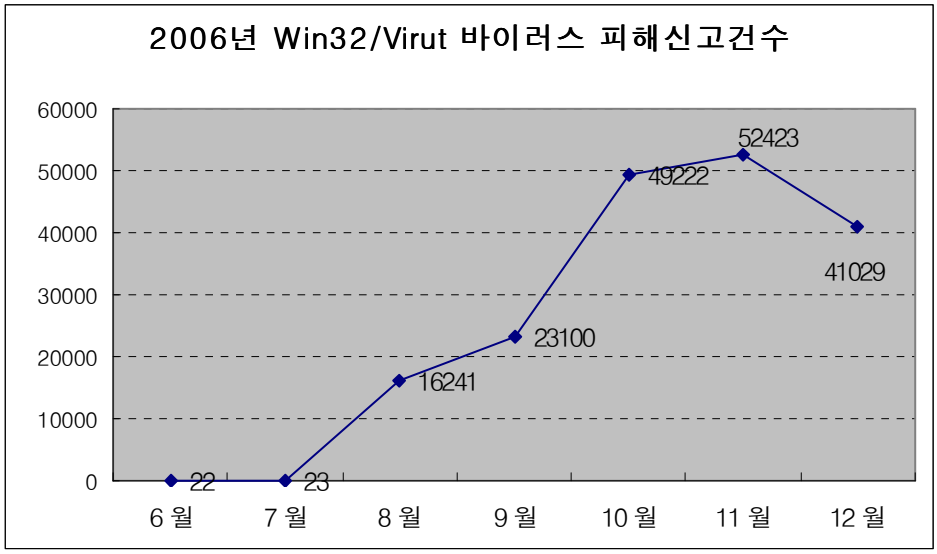


[그림 3-1]2006, 2007년 국내 악성코드 피해신고건수 비교

[그림 3-1]을 통해서 2007년의 악성코드 피해신고건수가 2006년보다 급감했음을 확실히

[1] 2006년의 Win32/Virut 피해신고 건수는 대부분 중복으로 접수되어 실제 피해 신고 건수보다 과다하게 산정된 값이다.

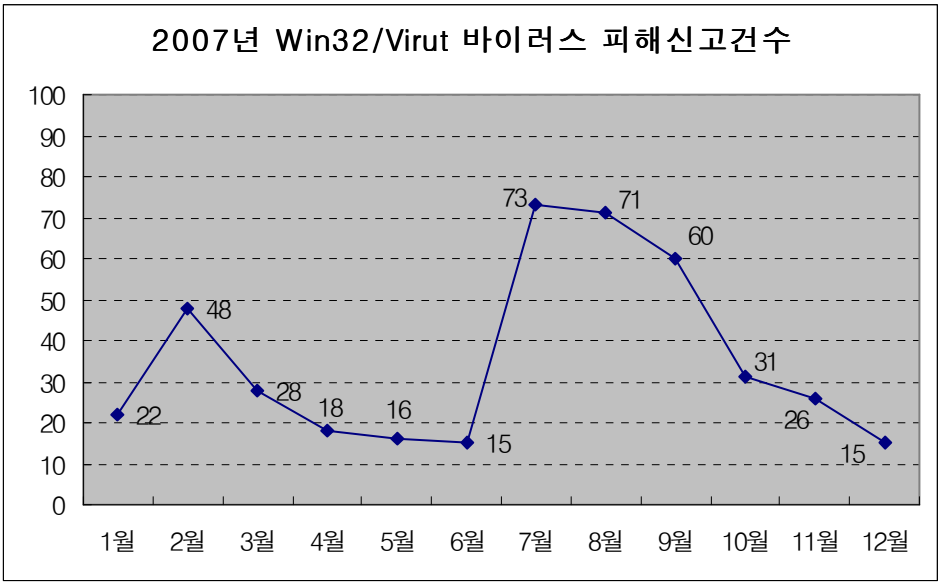
알 수가 있다. 앞에서도 언급했듯이 Virut 바이러스의 피해신고건수가 급감함에 따라 자연히 2007년 악성코드 피해신고 건수도 2006년에 비해 급감하였는데 그 원인을 살펴보기에 앞서 2006년에 Virut 바이러스가 특히 8월부터 12월까지 5개월 동안 피해신고가 급증한 원인을 살펴볼 필요가 있다.



[그림 3-2] 2006년 Win32/Virut 바이러스 피해신고건수

보통 바이러스는 라이프 사이클(Life Cycle, 생성-활동-소멸)주기가 다른 악성코드에 비해 짧다는 특징을 가지고 있다. 그러나 Virut 바이러스의 라이프 사이클은 [그림 3-2]을 통해서 그 주기가 비교적 길다는 것과 6월부터 Virut 감염 피해가 접수되기 시작하면서 8월부터 12월 5개월 동안 감염 피해신고가 급증했음을 알 수 있다. 그 원인은 Virut 바이러스에 감염된 다른 악성코드가 광범위하게 확산되었기 때문인 것으로 풀이된다. 특히 Netsky, Bagle, Mytob같은 매스 메일러(Mass Mailer)형의 웜들이 Virut 바이러스에 감염된 채 메일을 비롯한 P2P, IM, (Instant Messenger)등 다양한 경로로 확산되었던 경우가 많았다.

그러나 2006년까지 월별 악성코드 피해신고에서 항상 Top 10을 굳건히 지키고 있던 매스 메일러(Mass Mailer)형의 웜들의 몰락이 2007년에 더욱 가속화됨에 따라 Virut 바이러스의 피해신고건수도 자연스럽게 감소하였고 백신업체들의 Virut 바이러스 치료기능 강화와 전용 백신 제공 등도 Virut 바이러스의 피해신고가 감소하는데 한 몫한 것으로 보인다.



[그림 3-3] 2007년 Win32/Virut 바이러스 피해신고건수

[그림 3-3]를 보면 2007년에도 Win32/Virut는 소멸되지 않고 2006년만큼은 아니지만 꾸준하게 피해신고가 접수되었음을 알 수가 있다. 이는 2006년과 마찬가지로 트로이목마나 애드웨어 그리고 심지어 안티스파이웨어 제품이 Virut 바이러스에 감염된 채 유포되었기 때문인 것으로 판단된다.

2006년과 2007년 양해 가장 많은 악성코드 피해신고가 되었던 악성코드들의 Top 20를 비교해 봄으로써 2006년까지 월별 악성코드 피해 Top 10에서 전통적으로 강세를 보였던 매스메일러(Mass Mailer)형의 웜들이 2007년 들어서 왜 몰락할 수 밖에 없었는지에 대해서 알아보도록 하겠다.

악성코드 피해 Top 20, 2006 vs. 2007

2006 년		
순위	악성코드 명	건수
1	Win32/Virut	154,114
2	Win32/Virut.B	38,497
3	Win32/Netsky.worm.Gen	670
4	Win32/Bagle.worm.19666	551
5	Win32/Mytob.worm.Gen	537
6	Win32/Bagle.worm.19834	355
7	Win32/Parite	329

2007 년		
순위	악성코드 명	건수
1	Win-Trojan/Xema.variant	1448
2	Win32/Virut	351
3	Win32/IRCBot.worm.variant	341
4	Dropper/QQPass.23599.B	298
5	Dropper/QQPass.23599.D	293
6	Dropper/OnlineGameHack.23087	272
7	Win-Trojan/KorGameHack.17920.BR	272

8	Win32/Bagle.worm.40565	273	8	Win-Trojan/KorGameHack.26624.AI	267
9	Win32/Bagle.worm.94126	177	9	Win-Trojan/KorGameHack.14848.FO	195
10	Win32/Netsky.worm.29568	165	10	Win-Trojan/KorGameHack.6430	149
11	Win32/Bagle.worm.69842	127	11	Win-Trojan/Downloader.38400.I	141
12	Win-Trojan/Xema.variant	68	12	Dropper/OnlineGameHack.15988	130
13	Win32/Bagle.worm.95369	65	13	Win-Trojan/OnlineGameHack.15360.I	120
14	Win32/Tenga.3666	61	14	Win-Trojan/Downloader.169984.D	116
15	Win32/Mytob.worm.48766.C	58	15	Win-Trojan/KorGameHack.19456.BM	113
16	Win32/Maslan.C	55	16	Win-Trojan/KorGameHack.7295	102
17	Dropper/Maslan.60928	52	17	Win-Trojan/KorGameHack.43072	96
18	Win32/Stration.worm.150844	45	18	Dropper/OnlineGameHack.29743	95
19	Win-Trojan/Disnoexecute.21504	39	19	Win-Trojan/KorGameHack.12800.EI	88
20	Win32/Maslan.worm.58880	35	20	Win-Trojan/KorGameHack.15064	88

[표 3-2] 악성코드 피해 Top 20, 2006 vs. 2007

[표 3-2]를 보면 2006년의 경우 Win32/Virut와 그의 변종, Virut.B 그리고 일부 바이러스를 제외한 대부분이 매스 메일러(Mass Mailer)형 웜들임을 알 수가 있는데 그 당시 제작자들간의 자존심 싸움 및 실력과시로 인해 수많은 매스 메일러(Mass Mailer)형의 웜들이 양산됨으로 인해 2006년 악성코드 피해 Top 20의 대부분을 매스 메일러(Mass Mailer)형의 웜들이 장식하게 되었다.

하지만 2007년에는 Virut 바이러스 만이 2007년 Top 20에서 2위로 그 명맥을 유지하고 있을 뿐 대부분이 정보유출 목적과 연관성이 있는 트로이목마 계열의 악성코드로 이는 2006년과 비교했을 때 확연하게 차이를 보이고 있다. 그 원인은 **『IT 인프라가 사회전반에 미치는 영향과 그에 따른 악성코드 제작자의 성향변화』**로 요약할 수 있다. 불과 몇 년 전만 해도 IT인프라가 정치 ▪ 사회▪ 경제활동에 미치는 영향은 그다지 크지 않았으나 지금은 잘 발달된 IT 인프라를 기반으로 정치 ▪ 사회▪ 경제활동이 행해지고 있기 때문에 악성코드 제작자들도 상호간에 자존심 싸움 및 실력과시에서 탈피하여 약 3년 전부터 자연스럽게 금전적 이득을 취하기 위한 목적으로 이동하였으며 2007년에는 그 성향이 더욱 심화 되었다고 볼 수 있다.

[표 3-2]에 보여진 2007년 악성코드 피해 Top 20 악성코드의 총 피해건수는 4,624(Virut 제외)건으로 2007년 한 해 악성코드 피해건수 30,996건에서 차지하는 비중이 2006년에 비하면 그다지 크진 않으나 이를 반대로 생각해보면 정보 유출과 연관성이 있는 트로이목마의 다양한 신종 및 변종이 양산되었다는 증거이다.

	1월	2 월	3 월	4 월	5 월	6 월	7 월	8 월	9 월	10 월	11 월	12 월
웜	109	228	200	259	127	299	994	145	82	75	96	124
트로이목마	771	1057	659	1093	869	1673	2248	618	782	831	1439	1596
바이러스	23	91	45	27	31	34	87	8	4	2	3	4
드랍퍼	130	130	151	146	145	245	180	108	128	142	156	178
유해가능	22	36	29	38	62	27	35	28	17	28	76	69
스크립트	38	16	27	54	30	43	42	21	33	22	40	32

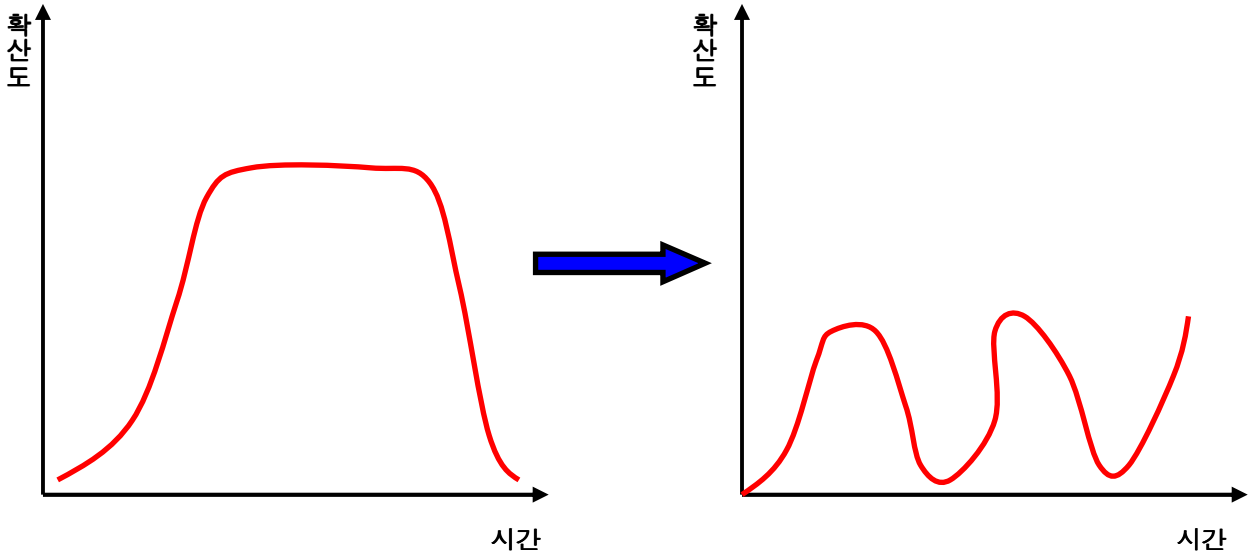
[표 3-3] 2007년 악성코드 유형별 현황

따라서 2006년에 Virut 바이러스의 피해신고를 제외한다면 2007년의 경우 피해신고가 급감한 것이 아니라 위에서 언급한 이유 때문에 오히려 2006년보다 악성코드 피해신고가 급증했다고 봐야 할 것이다.

또한 [표 3-2], [표 3-3]을 통해서 국내와 외국의 악성코드 동향에 대해서 어느 정도 파악해 볼 수 있다. 국내의 경우는2007년 악성코드 피해 Top 20에 나열된 대부분의 악성코드가 특정 온라인 게임 사용자의 계정정보를 빼내 금전적인 이득을 취하기 위한 목적을 가지고 있는 온라인 게임 관련 트로이목마라는 것이다.

온라인 게임 관련 트로이목마가 2007년 한 해 동안 극성을 부렸던 원인은 다른 나라에 비해 비교적 잘 발달된 국내 IT 인프라를 기반으로 다양한 온라인 게임이 양산되었고 이들 게임에서 사용하는 아이템들이 실제로 암암리 고가에 거래되고 있기 때문이고 온라인 게임시장의 규모가 수천억원 대에 이른다는 통계자료도 이를 뒷받침한다. 국내와는 다르게 외국의 경우는 여러 가지 제약조건 때문에 국내처럼 온라인 게임시장이 활성화되지 못 하여 주로 BotNet을 이용한 스팸메일, 피싱, 그리고 트로이목마를 이용한 온라인 뱅킹 정보 절취 등이 주류를 이루고 있어 국내와는 확연한 차이를 보이고 있다. 하지만 국내나 외국이나 악성코드 배포의 목적은 금전적인 이득을 취하기 위함이라는데 공통점이 있다는 것을 여러 사례를 통해서 알 수 있었다.

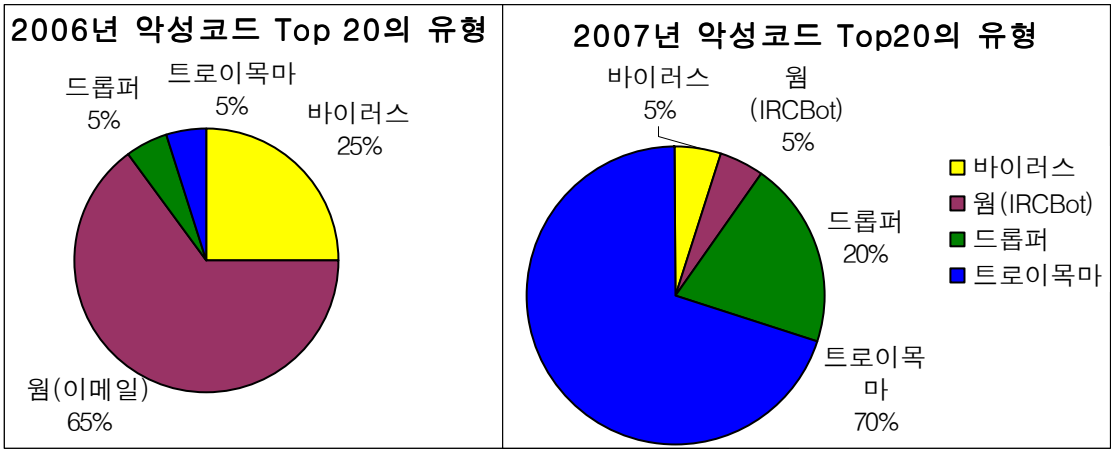
위에서 설명한 것처럼 IT 인프라가 사회전반에 미치는 영향과 그에 따른 악성코드 제작자의 성향변화로 인해 악성코드의 라이프 사이클(Life Cycle, 생성-활동-소멸)도 꾸준히 변해 왔고 이는 오래 전부터 언급되어 온 내용이지만 2007년 악성코드 동향을 결산하는 시점에서 이에 대해서 한번 알아 볼 필요가 있다.



[그림 3-4] 악성코드의 라이프 사이클(Life Cycle) 변화

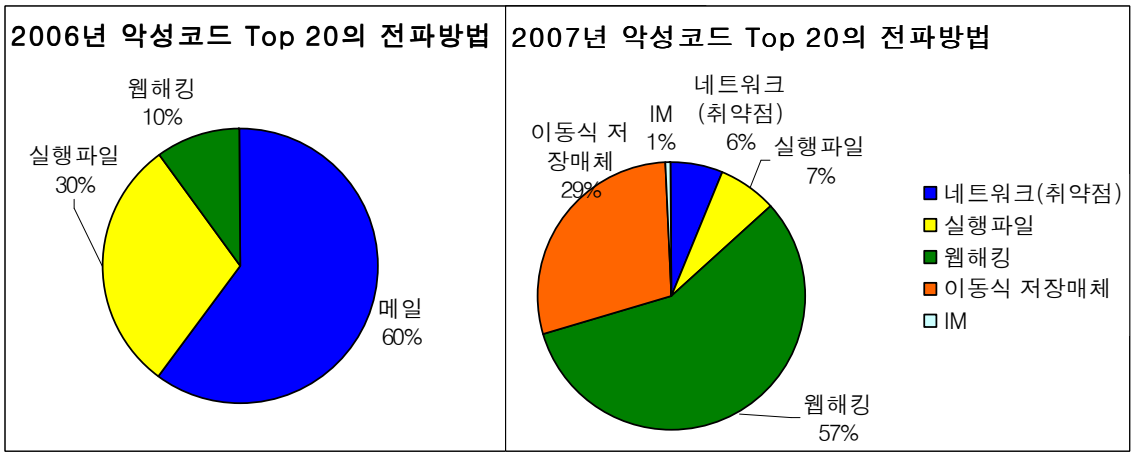
[그림 3-4]에서처럼 악성코드의 라이프 사이클(Life Cycle, 생성-활동-소멸)변화는 크게 보면 이메일, IM, 취약점, P2P 등을 통해서 확산을 시도하는 웜 형태의 악성코드가 등장하면서 한번 변했고, 웹 해킹과 악성코드의 결합 및 유포가 이슈화 되면서 다시 한번 변하게 된다.

[그림 3-4]를 종합해 보면 악성코드의 확산력은 떨어지는 반면에 국지성, 복합성, 물량화 등의 심화로 인해 그래프의 반복 주기가 짧아 졌음을 알 수가 있다. 이는 백신의 기술력(Heuristic, 사전방역, 다양한 실행압축 지원 등) 향상 및 짧아진 치료엔진의 배포주기 그리고 네트워크 장비와 결합하여 확산 전 차단했기 때문이다. 이에 악성코드 제작자들 역시 끊임없이 신종 및 변종 악성코드(코드 변경, 재 컴파일, 다중압축, 은폐기술, 파일감염 등)를 제작함으로써 악성코드 라이프 사이클(Life Cycle, 생성-활동-소멸)의 주기가 짧아 졌다고 볼 수 있다. 그 예로 2007년 악성코드 피해 Top 20의 대부분을 차지하고 있는 온라인 게임 관련 트로이목마를 들 수 있다.



[그림 3-5] 2006년 vs. 2007년 악성코드 Top 20의 유형

[그림 3-5]에 나타난 양 년도의 악성코드 Top 20의 유형을 비교해 보더라도 2006년과 2007년이 확실히 다르다는 것을 알 수가 있다. 우선 2006년 악성코드 Top 20의 유형에서 각각 65%, 25%를 점유했던 웜(이메일)과 바이러스의 경우, 2007년 악성코드 Top 20에서는 웜(이메일)의 존재가 사라지면서 그 자리를 트로이목마류가 대신하였는데, 그 이유는 금전적인 이득을 목적으로 한 악성코드 배포 증가하였기 때문이다. 그리고 바이러스의 점유율은 5%로 급감했으며 반대로 트로이목마와 드랍퍼의 점유율이 각각 70%, 20%로 급증했다.



[그림 3-6] 2006년 vs. 2007년 악성코드 Top 20의 전파방법

[그림 3-6] 역시 [그림 3-5]처럼 Top 20의 전파방법에서 확연한 차이를 보이고 있다. [그림 3-6]에서 2007년 악성코드 Top 20의 전파방법을 보면 웹 해킹을 통한 전파방법이 2006년에 비해서 급증했음을 알 수가 있는데 웹 해킹은 전파방법에서 표현한 단어일 뿐, 엄밀히 말하면 서버와 클라이언트에 존재하는 취약성을 이용하여 악성코드를 유포하는 방식이라 할 수 있다.

대부분 자동화 툴에 의한 SQL Injection, XSS, 게시판 취약점 공격 등을 통해서 웹 서버의 취약한 웹 페이지에 iframe을 삽입하거나 파일을 업로드 하는 경우가 대부분이다. 그리고 해당 서버의 관리자로 하여금 쉽게 대응할 수 없도록 iframe을 조각 내거나 정상 서비스되는 플래시 파일에 iframe을 삽입하는 경우도 있었다.

웹 해킹을 통해서 유포되는 악성코드가 클라이언트에서 실행되기 위해서 사용되는 취약성은 대부분 IE에 존재하는 것들로 흔히 사용되는 취약성들을 나열해 보면 아래와 같다.

MS03-014 / MS05-001 / MS05-026 / MS06-001 / MS06-014 / MS06-040 / MS06-046 / MS06-057/MS07-017

2007년 하반기부터 기존의 웹 해킹과 악성코드 유포방식에 ARP Spoofing을 이용한 방법이 새롭게 추가되었는데 감염된 시스템이 속한 네트워크 대역으로 무작위 ARP 패킷을 발송함으로써 네트워크 장애의 원인이 되기도 하며 최초 악성코드에 감염된 시스템을 Gateway로 바라보게 하여 다른 시스템들이 특정 웹사이트에 접속할 때 정상적인 사이트로의 접속이 아닌 악성코드가 다운로드 되는 사이트로 리다이렉션(redirection) 시키기도 한다. 이렇게 되면 위에서 언급한 취약성이 존재하는 다른 시스템이 직접 악성코드를 유포하는 사이트에 접속하지 않아도 접속하는 것처럼 되어 악성코드를 설치하게 된다. 이러한 현상은 아파트나 기업처럼 동일한 네트워크에 속해 있는 경우에서 피해사례가 자주 발생하였다.

최근에는 언론에 부토 바이러스 등장이라는 기사가 보도된 적이 있는데 이는 Google에 Benazir Bhutto란 검색어를 입력할 경우 검색된 일부 결과물을 클릭할 경우 Internet Explorer에 취약성(MS06-014)이 존재한다면 악성코드가 다운로드 되는 경우이다. 참고로 V3에서는 다운로드 되는 악성코드들을 Win-TrojanDownloader.43008.AC, JS/Iframe, Win-Trojan/Downloader.144384.C로 진단 및 삭제할 수 있다.

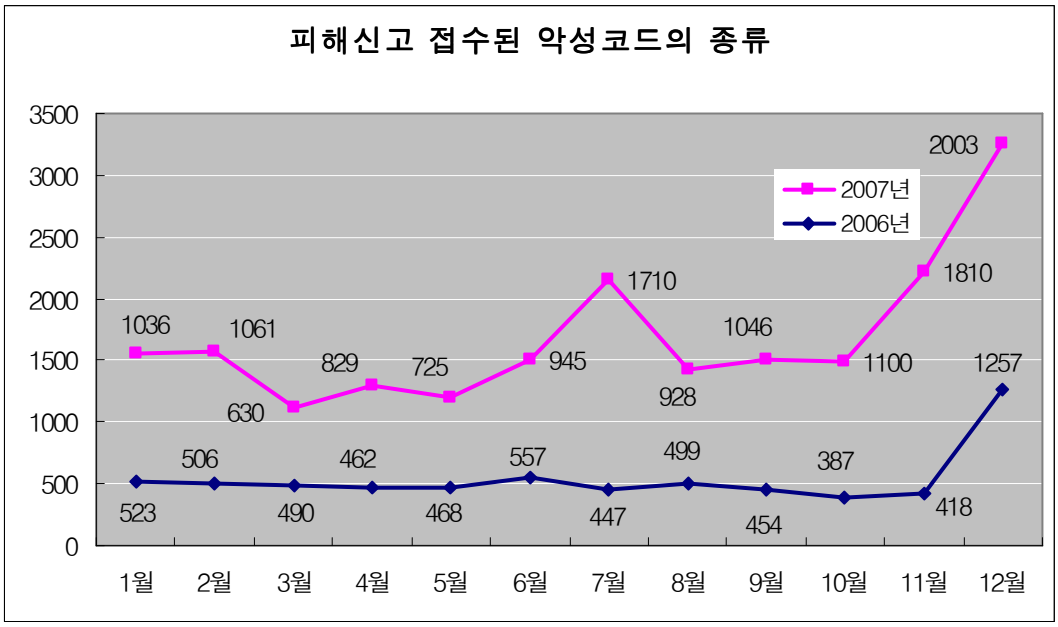
[그림 3-6]을 보면 2007년 악성코드 Top 20의 전파방법 중에 이동식 저장매체가 눈에 띄는데 이는 이동식 저장매체의 보편화와 이동식 저장매체를 시스템에 꽂을 경우 기본적으로 자동 실행되는 점에 착안하여 악성코드가 자신을 유포하는데 중요한 전파수단으로 사용했기 때문이다. 대표적으로 Win32/Autorun.wrom계열의 웜을 예로 들 수 있다.

Win32/Autorun.worm 중에는 안전모드관련 레지스트리 값을 조작하여 사용자가 안전모드로 부팅할 경우 블루스크린을 출력하게 하여 안전모드로 부팅하지 못 하도록 하며 자신을 강제 종료 시킬 경우 시스템을 재 부팅시키는 경우도 있었다.

IM(Instant Messenger)를 통한 확산의 비중이 극히 미비하나 여전히 악성코드가 확산되는 통로로 사용되고 있고 2007년 악성코드 피해 Top 20의 순위에 들지는 못 했지만

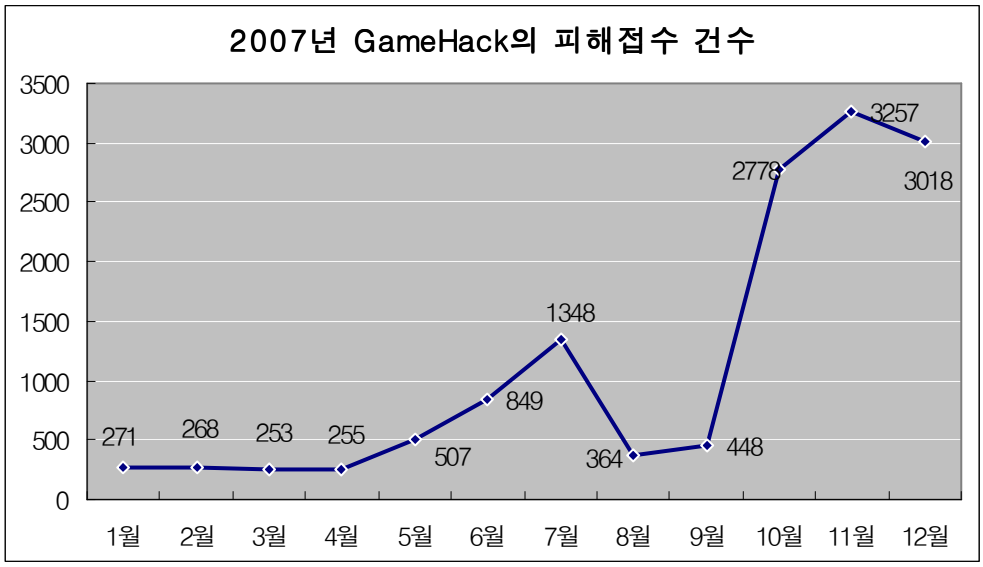
Win32/Zhelatin 웜계열이 이메일을 통해 확산되는매스 메일러(Mass Mailer)형 웜의 명맥을 겨우 유지하고 있으며 한동안 발견되지 않다가 크리스마스와 새해인사 관련하여 12월 말경 집중적으로 발견된 바 있다.

피해신고 접수된 악성코드의 종류, 2006 vs. 2007



[그림 3-7] 피해신고 접수된 악성코드의 종류

[그림 3-7]을 보면 2006년보다 2007년도에 피해신고 접수된 악성코드의 종류가 평균 2배 증가했음을 알 수가 있는데 이에 대한 원인은 앞에서 언급한 대로 잘 구축된 IT인프라와 악성코드 제작자들의 성향변화로 요약할 수 있으며 이동식 디스크의 보편화 등으로 인해 전파 방법 면에서도 많이 변화했기 때문이다.



[그림 3-8] 온라인 게임 관련 트로이목마(드랍퍼 포함) 피해접수 건수

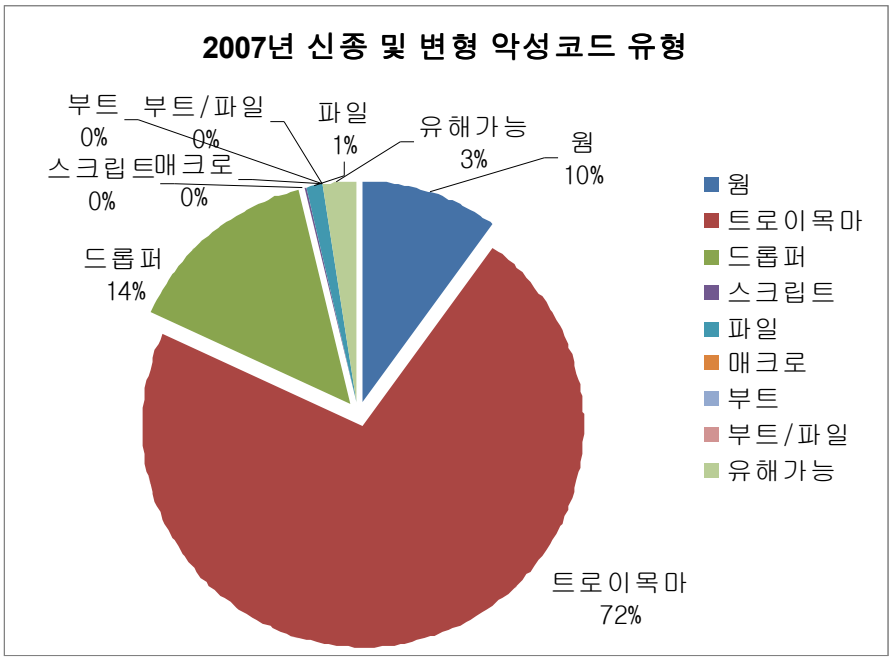
[그림 3-8]을 보면 10월부터 12월 사이에 온라인 게임 관련 트로이목마 및 드랍퍼에 의한 피해가 집중적으로 접수되었음을 알 수가 있다. 이는 여전히 유효한 웹 해킹과 결합된 악성코드 유포와 더불어 ARP Spoofing, 이동식 저장매체를 통해 확산방법이 추가되면서 이를 통해 확산되는 악성코드에 감염될 경우 또 다른 다수의 악성코드들을 다운로드 하는데 대부분이 온라인 게임 관련 트로이목마이었기 때문이다.

지금까지 언급한 내용을 종합해 보면 2007년 악성코드 피해동향은 ▶ 매스 메일러(Mass Mailer) 및 바이러스의 몰락의 가속화 ▶ 웹 응용프로그램의 취약성을 공격하는 웹 해킹의 심화 ▶ 금전적 이득을 노린 온라인 게임 관련 악성코드의 심화 등으로 요약할 수 있으며 2008년도 2007년과 유사한 형태의 악성코드 피해사례가 계속될 것으로 보인다.

2007년 신종 악성코드 동향

2006년 안철수연구소는 클라이언트를 대상으로 (공격하는) 왕성하게 감염 활동을 하는 악성코드의 증가에 대해서 언급 하였다. 대표적으로 실행파일을 감염 시키는 전통적인 파일 바이러스와 온라인 게임의 사용자 계정을 탈취하는 악성코드가 그것이다. 2007년에도 이러한 악성코드들의 동향은 전체적으로 크게 달라진 것은 없으나 패러다임은 변화하고 있다. 예로 작년에 기승을 부렸던 단순한 형태의 바이러스는 급격히 감소하고 진단, 치료하기 어렵고 복잡한 형태로 변모 하였다.

다음은 2007년 안철수연구소가 고객으로부터 접수한 샘플에 대한 악성코드 유형별 현황이다.



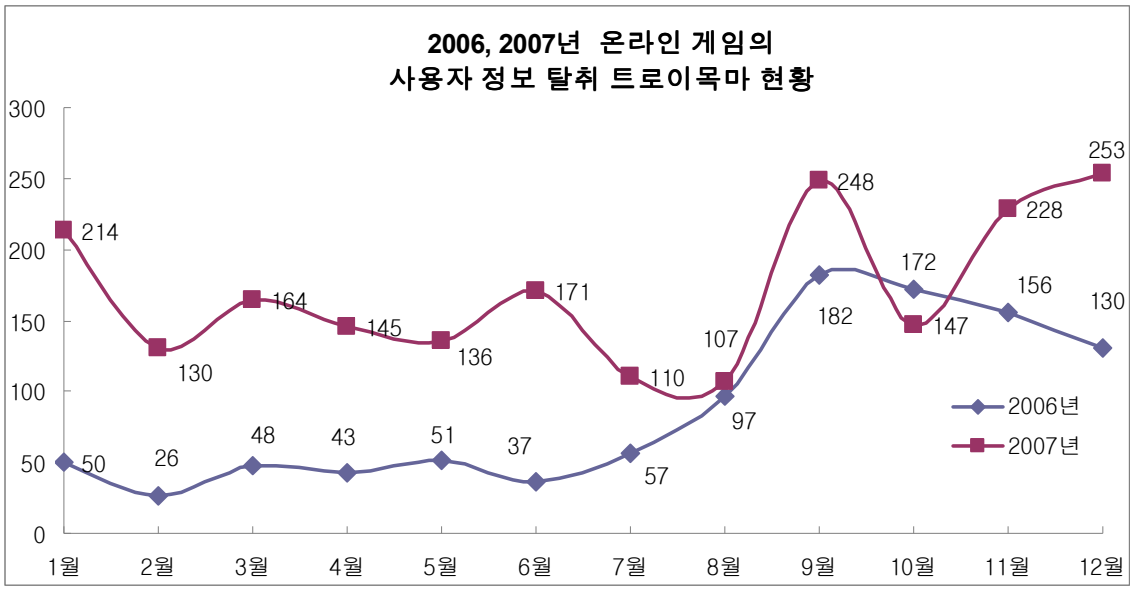
[그림 3-9] 2007년 국내발견 신종 및 변형 악성코드 유형

상반기와 마찬가지로 트로이목마의 비율이 매우 높으며, 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마 류의 악성코드 비율이 높은 편이다. 온라인 게임의 사용자 계정을 탈취하는 악성코드의 타겟은 국내 온라인 게임에서 중국이나 대만의 온라인 게임을 타켓으로 하는 등 그 양상이 변화 하고 있다.

그러나 국내에 취약한 웹 서버들이 악성코드를 다운로드 받을 수 있는 숙주로 사용되고 있는 것은 여전하다. 타켓이 중국이나 대만의 현지 온라인 게임으로 변화 했다는 것은 여러 가지 이유가 있겠지만 현지 온라인 게임 업체들의 게임 보안 솔루션을 도입하지 않았거나 또는 이를 우회 할 수 있도록 되어 있는 것으로 보인다.

다음은 해당 트로이목마 중에서 국내에 주로 이슈를 발생 하는 온라인 게임의 사용자 데이

터 탈취 트로이목마의 유형에 대하여 전년 수치와 비교해 보았다.



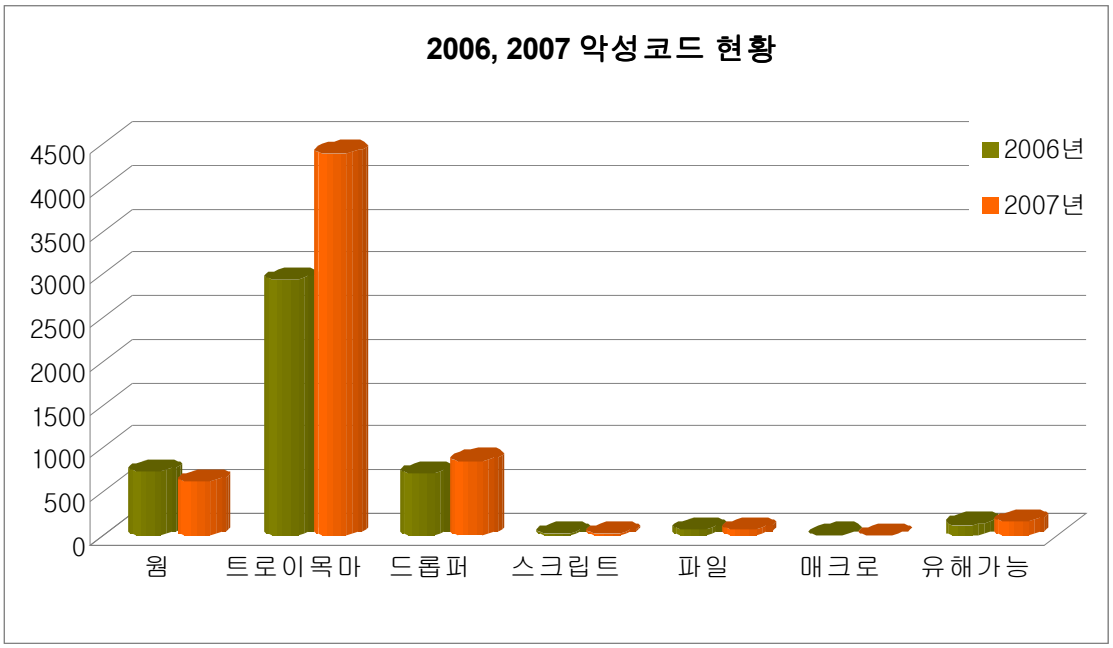
[그림 3-10] 2006, 2007 온라인 게임 트로이목마 현황

온라인 게임의 사용자 계정 정보를 훔쳐내는 트로이목마는 작년 동기 대비 96% 증가하였다. 국내의 경우 게임 보안 솔루션의 도입 또는 로그인 계정에 대한 보안 강화로 인하여 해당 악성코드가 주춤 하고 있는 것으로 판단 된다. 무엇보다도 중국, 대만 현지의 온라인 게임 이용자 증가와 더불어 인터넷 사용자의 증가도 악성코드 패러다임 변화에 어느 정도 기여를 한 것으로 보인다.

올해 중국산 악성코드의 또 다른 특징으로는 대량 다운로드 증상을 갖는 트로이목마와 ARP 스푸핑을 이용한 감염기법을 꼽을 수 있다. 대량 다운로더는 한번에 20 개 이상의 악성코드를 내려 받는다. 내려 받은 악성코드는 다시 또 다른 악성코드를 다운로드 한다. 이것은 대표적으로 온라인 게임의 계정을 훔쳐내는 악성코드를 설치하거나 다수의 애드웨어를 설치하는 등 시스템을 복합적으로 감염 시킨다. 이렇게 된 시스템은 마치 융단폭격을 맞은 것처럼 악성코드에 의해 쑥대밭이 되어 버리고 이를 다시 복구하기에는 어렵고 긴 시간이 소요된다.

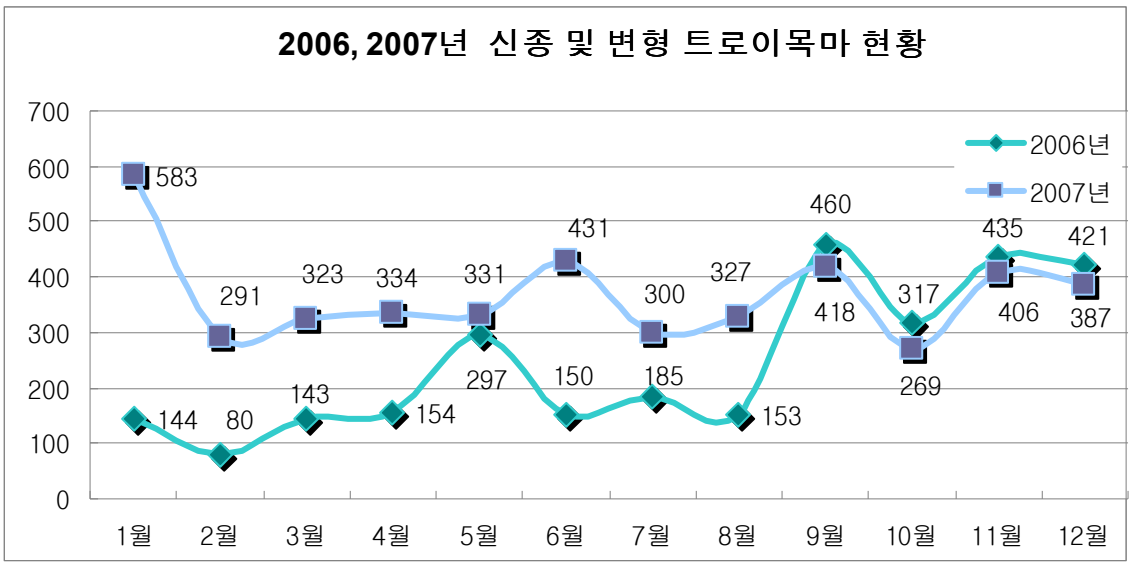
ARP 스푸핑 자체는 오래된 공격기법이지만 이를 악성코드 전파에 접목 시킨 것은 올해 큰 문제가 되었다. 해당 감염기법은 스푸핑을 하는 시스템이 마치 게이트웨이가 되어 네트워크 트래픽을 가로채고 이를 다시 요청 시스템에 돌려줄 때 보안이 취약한 웹 브라우저를 사용하고 있다면 악성코드에 감염 될 수 있다. 즉, 내가 감염됨으로써 주변의 다른 시스템들도 유해한 사이트나 악성코드가 숨겨진 웹 사이트를 방문하지 않아도 취약점이 있는 웹 브라우저를 사용하면 악성코드에 감염 될 수 있다.

다음은 작년과 비교한 신종 및 변형 악성코드 현황이다.



[그림 3-11] 2006, 2007 악성코드 현황

올해는 전년 대비 33% 의 악성코드가 증가 하였다. 많이 증가한 악성코드는 트로이목마와 드랍퍼로 각각 50%, 22% 가 증가 하였다.



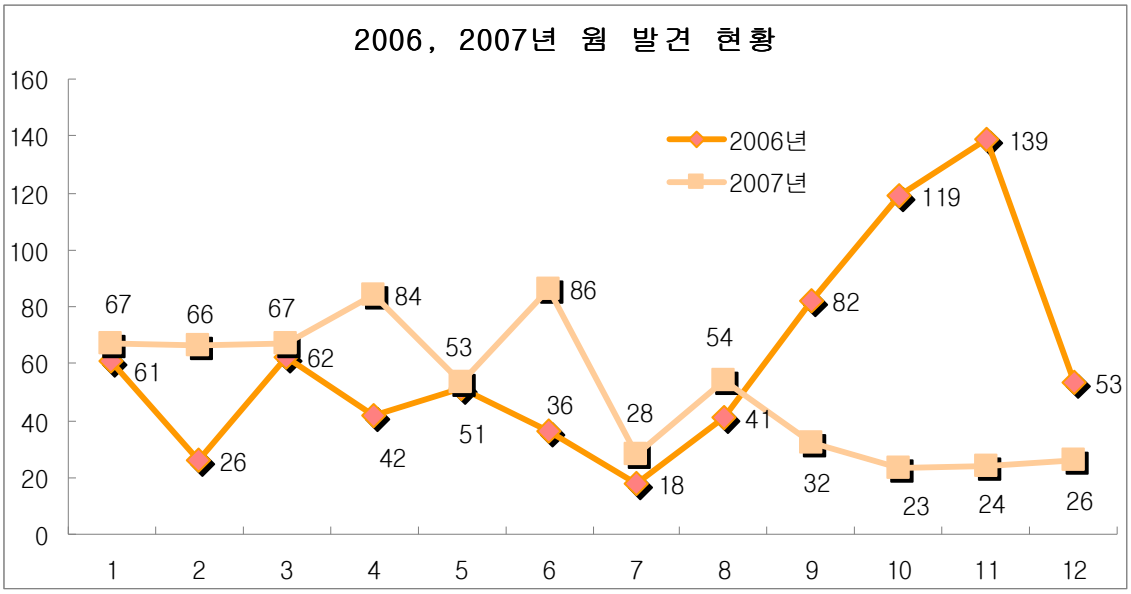
[그림 3-12] 2006, 2007 신종 및 변형 트로이목마 발견 현황

올해 발견된 악성코드중의 특징 중 하나가 악성코드의 생존시간 고도화 이다. 이를 세분화 하면 은폐기법 및 자기보호 고도화 나눌 수 있다.

은폐기법의 고도화는 이미 2006년에 전망되었고, 올해 현실화 되었다. 2008년에는 더욱 고도화 될 전망이다. 특히 시스템 파일 드라이버 또는 네트워크 드라이버내 DRIVER OBJECT 내 DISPATCHER TABLE 정보를 후킹하는 형태는 무력화하기 매우 어렵다. 그리고 자기보호기능이 강화 되어 자신이 발견 되어도 제거하지 못하게 하거나 마치 제거된 것처럼 속여 생존시간을 극대화 한 것 도 눈에 띈다.

악성코드 유형중 웜은 전년 대비 -13% 감소하였다. 가장 많이 감소된 웜은 악성 IRCBot 웜이다. 이 웜의 감소 원인으로는 더 이상 원격에서 공격이 가능한 윈도우 취약점 보고가 없으며 C&C (Command & Controls)라고 불리우는 공격자가 명령을 내리거나 제어 할 수 있는 호스트가 정보보호 기관들의 노력으로 대부분 차단 되는 등의 효과가 어느 정도 기인 한다고 생각 된다.

다음은 작년과 비교한 현황으로 특히 하반기 웜 유형의 수치가 줄어 들었다는 것을 알 수 있다. 물론 이 데이터는 국내 고객 접수 샘플만을 대상으로 하였으며 국내에 잘 보고 되지 않는 젤라틴 웜등은 국내 발견, 보고된 형태만 포함 되었고 국외로부터 접수된 유형은 제외하였다.



[그림 3-13] 2006, 2007 신종 및 변형 웜 발견 현황

올해는 특히 Autorun.inf 를 이용하여 자신을 자동으로 실행하는 형태의 악성코드가 큰 폭으로 증가 하였다. 이중에서도 웜 유형은 Win32/Autorun.worm으로 명명 되었는데 새로운 유형으로 자리매김 하였다. 대표적으로 이동식 저장장치를 노리고 있으며, 이는 마치 과거에 플로피 디스켓에 부트 바이러스가 감염되는 것과 유사하다. 더 위험한 것은 윈도우 운영체제

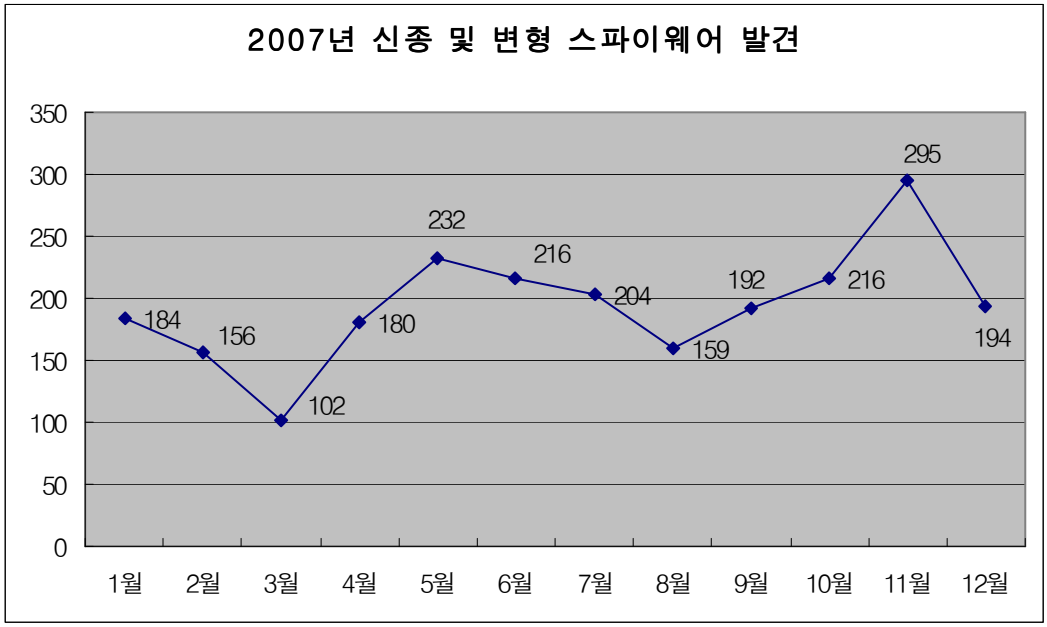
에서 이동식 저장장치로 인식되는 모든 장치가 감염 대상이 될 수 있어 매우 위험하다. 이 악성코드는 윈도우의 자동실행기능의 허점을 이용한 것이며 근래의 중국산 악성코드 대부분은 이 증상을 포함하여 자신의 감염대상을 넓히려 하고 있다.

(2) 2007년 스파이웨어 동향

2007년 신종 및 변형 스파이웨어 발견 동향

	스파이웨어	애드웨어	드랍퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
1월	62	38	29	42	4	6	2	0	1	184
2월	72	17	12	41	1	10	2	0	1	156
3월	48	17	10	20	0	5	2	0	0	102
4월	105	20	13	30	1	5	3	3	0	180
5월	143	29	5	46	1	4	1	3	0	232
6월	108	46	19	38	2	3	0	0	0	216
7월	63	50	17	65	4	5	0	0	0	204
8월	64	31	6	52	4	2	0	0	0	159
9월	91	37	12	40	6	6	0	0	0	192
10월	98	42	14	51	5	6	0	0	0	216
11월	99	61	15	112	3	5	0	0	0	295
12월	86	32	22	48	1	3	1	0	1	194

[표 3-4] 2007년 신종 및 변형 스파이웨어 발견 현황



[그림 3-14] 2007년 신종 및 변형 스파이웨어 발견 증감 현황

[그림 3-14]는 2007년 월별 신종 및 변형 스파이웨어 발견 현황을 보여주는 그래프이다. 1

월에서 12월까지 다소 기복을 보이는 가운데 전체적으로는 증가하는 모양을 볼 수 있다. 2007년 신종 및 변형 스파이웨어 발견 현황의 가장 뚜렷한 특징으로 상반기에는 온라인게임 계정 유출 목적의 스파이웨어가 많이 발견된 반면에 하반기로 접어들면서 국내에서 제작 배포되는 애드웨어의 수가 상대적으로 많이 늘어난 것을 들 수 있다.

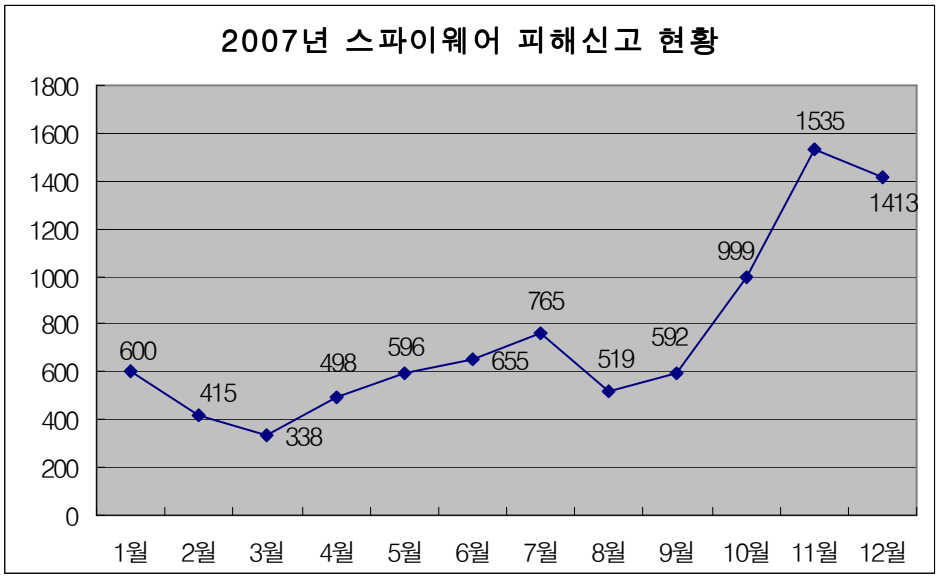
2007년 상반기는 중국발 해킹에 의한 웹사이트 변조와 이를 통한 온라인게임 계정 유출 목적의 스파이웨어 제작이 가장 활발한 시기였으며, 하반기에 접어들면서 신종 및 변형의 제작 배포는 다소 감소하였으나 여전히 큰 피해를 입히고 있다. 이들 온라인게임 계정 유출 스파이웨어는 제작 초기에는 국내 유명게임만을 타겟으로 한 반면 최근에 발견되는 것들은 국내 온라인게임 뿐만 아니라 중국/대만의 유명 온라인게임 또한 타겟으로 하고 있다. 보안 프로그램이 진단하는 것을 회피하기 위한 목적으로 다양한 변형이 양산되는 것도 이들 스파이웨어의 특징이다.

2007년 초까지 다소 주춤하던 국내 애드웨어 제작은 기존의 불특정 웹 사이트에서 ActiveX 컨트롤을 이용한 설치 방법에서 다운로더를 이용한 번들 설치 방법으로 변화함에 따라 하반기부터 증가하기 시작하였으며, 이들 애드웨어의 번들 설치만을 목적으로 하는 다운로더의 수도 상반기에 비해 하반기에 증가한 양상을 보인다. 2007년 상반기까지는 2006년에 이어 허위 안티-스파이웨어의 제작 배포가 활발하였으며, 하반기에 접어들면서 유명 쇼핑몰과 제휴하여 적립금을 제공하는 리워드 프로그램의 제작 배포가 활발하였다. 이들 리워드 프로그램은 툴바나 BHO 형태로 불특정 웹사이트에서 사용자 동의 없이 ActiveX 컨트롤을 이용하여 설치되거나 다운로더에 의한 번들로 설치되며, 찾아가지 않는 적립금을 주요 수익원으로 한다. 리워드 프로그램과 함께 제휴 쇼핑몰의 바로가기를 생성하는 숏컷(Shortcut) 계열의 애드웨어 설치 피해도 많이 발견되었다.

2007년 스파이웨어 피해 동향

	스파이웨어	애드웨어	드랍퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
1월	247	137	93	96	13	11	2	0	1	600
2월	188	81	24	96	6	17	2	0	1	415
3월	123	100	25	69	1	14	6	0	0	338
4월	233	94	52	81	2	23	7	6	0	498
5월	320	109	22	122	2	10	2	9	0	596
6월	279	166	46	139	8	16	0	1	0	655
7월	261	183	55	232	10	20	3	1	0	765
8월	197	105	43	156	12	6	0	0	0	519
9월	291	119	35	132	8	7	0	0	0	592
10월	632	131	38	180	7	11	0	0	0	999
11월	480	354	147	525	3	25	1	0	0	1535
12월	325	446	164	461	4	8	4	0	1	1413

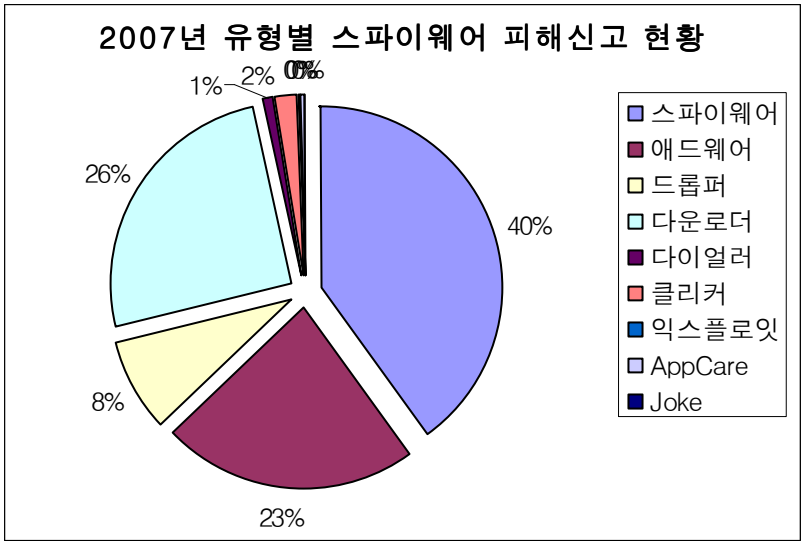
[표 3-5] 2007년 스파이웨어 피해 현황



[그림 3-15] 2007년 스파이웨어 피해신고 월별 증감 현황

[표 3-5]와 [그림 3-15]는 2007년 스파이웨어 피해신고 현황을 나타낸다. 9월까지 월 평균 500건 정도이던 피해신고 건수가 4/4 분기가 시작되는 10월부터 급증하여 월평균 약 1300건의 피해신고가 접수되었다. 신종 및 변형 스파이웨어 발견 현황과 마찬가지로 2007년 상반기 까지는 중국에서 제작 배포되는 온라인게임 계정 유출 목적의 스파이웨어가 피해 신고

의 상위를 차지하였으나 하반기로 접어들면서 국내제작 애드웨어의 피해신고 건수가 증가하면서 동시에 전체적인 피해신고 건수가 크게 증가하였다.



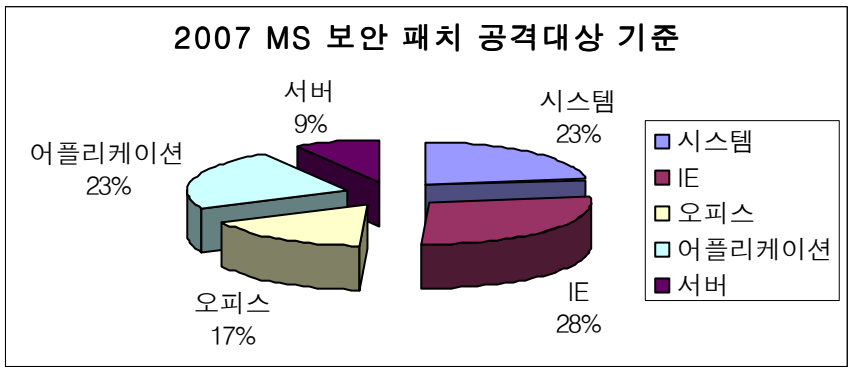
[그림 3-16] 2007년 유형별 스파이웨어 피해 신고 현황

[그림 3-16]은 유형별 스파이웨어 피해 신고 현황을 보여준다. 스파이웨어에 의한 피해 신고 건수가 가장 많았으며, 전체 피해신고의 약 40% 정도를 차지하고 있는 가운데 다운로더와 애드웨어가 그 다음으로 많은 피해를 입힌 것으로 나타났다. 온라인게임 계정 유출 스파이웨어의 피해는 2008년에도 지속될 것으로 생각되며, 2007년 하반기와 같은 추세가 지속된다면 2008년 상반기에는 국내제작 애드웨어의 피해가 더욱 증가할 것으로 예상된다.

(3) 2007년 시큐리티 동향

2006년에는 마이크로소프트사에서 발표한 보안 업데이트의 총 수가 78개를 발표한 반면에, 2007년에는 마이크로소프트사에서 발표한 보안 업데이트는 2006년 대비 약간 줄어든 69개를 발표하였다. 또한 긴급 보안 패치에 해당하는 것은 2006년에 49개, 2007년에는 43개에 해당한다. 2007년 3월달에 마이크로소프트사에 보안 패치를 발표하지 않는 달이 있어, 이러한 격차가 약간 벌어지게 된 것으로 파악된다.

2007년에 발표된 마이크로소프트사의 보안 패치를 분류 현황을 분석하면 아래와 같다.



[그림 3-17] 2007년 마이크로소프트 보안 패치 분류 현황

위의 [그림 3-17]을 보면, 2007년의 마이크로소프트 보안 패치의 주요 특징인 어플리케이션 취약점을 들 수 있으며, 어플리케이션, 오피스, IE(인터넷 익스플로러)에 관련된 보안패치가 전체 보안 패치 중 68%를 차지하고 있는 것을 알 수 있다. 어플리케이션 관련 취약점들의 대부분은 사용자들이 많이 사용하는 프로그램을 대상으로 하고 있으며, 악성코드 유포 및 특정 목적을 위해, 공격이 이루어 지고 있다. 이 중에서 기업 및 특정 시스템들을 공격하는 데는 오피스 관련 취약점들이 많이 이용되고 있는 것으로 파악되며, 2007년 발표된 오피스 취약점 관련 주요 목록을 살펴보면 아래와 같다.

MS07-014 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(929434)
MS07-015 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(932554)
MS07-023 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점 (934233)
MS07-024 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점 (934232)
MS07-025 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점 (934873)
MS07-036 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(936542)
MS07-037 Microsoft Office Publisher의 취약점으로 인한 원격 코드 실행 문제점(936548)
MS07-044 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(940965)
MS07-060 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(942695)

[표 3-6] 2007년 오피스 주요 취약점

2007년 9월에 발표된 마이크로소프트 오피스 2003 서비스팩 3 가 출시된 이후에 오피스 관련 취약점 또한 점차 줄어들고 있으나, 11월 달에 마이크로소프트 Access (.mdb)파일의 공격코드가 발표되었으며, 계속적인 주의가 필요하다. 오피스 취약점들은 악성코드가 포함되어져 메일이나 웹을 통해 공격하기 때문에, 신뢰하지 않는 사용자에게서 오피스 파일이 메일로 오는 경우에는 특히 주의가 필요하다. 또한, 오피스에 대한 보안패치는 반드시 오피스 홈페이지에서 보안 업데이트를 적용해야만, 클라이언트 시스템의 보안성을 강화할 수 있다.

[그림 3-17]을 보면 IE(인터넷 익스플로러) 취약점인 전체 28%을 차지하고 있는데, IE 취약점은 웹사이트 해킹 후에 악성코드 유포에 많이 사용되고 있다. 2007년에 발표된 IE 취약점 관련 주요 목록을 살펴보면 아래와 같다.

MS07-004 벡터 표시 언어의 취약점으로 인한 원격 코드 실행 문제점(929969)
MS07-008 HTML 도움말 ActiveX 컨트롤의 취약점으로 인한 원격 코드 실행 문제점 (928843)
MS07-016 Internet Explorer 누적 보안 업데이트(928090)
MS07-017 GDI의 취약점으로 인한 원격 코드 실행 문제점 (925902)
MS07-027 Internet Explorer 누적 보안 업데이트 (931768)
MS07-033 Internet Explorer 누적 보안 업데이트(933566)
MS07-042 Microsoft XML Core Services의 취약점으로 인한 원격 코드 실행 문제점 (936227)
MS07-045 Internet Explorer 누적 보안 업데이트(937143)
MS07-057 Internet Explorer 누적 업데이트 (939653)
MS07-069 Internet Explorer 누적 업데이트(942615)

[표 3-7] 2007년 IE 주요 취약점

IE (인터넷 익스플로러) 관련 취약점 보안 패치의 큰 특징은 하나의 패치 목록 안에 여러 개의 취약점에 대한 패치가 포함되어 있다. [표 3-7]의 목록 중에 악성코드 유포에 자주 사용된 취약점은 MS07-017 GDI ANI 파일 관련 취약점으로, 현재까지도 많이 악용되고 있는 실정이다.

이러한 통계는 2007년에 어플리케이션 취약점의 위협이 꾸준히 발생한 것으로 파악할 수 있다. 또한 ActiveX 관련 취약점도 증가추세에 있으며, 이 중에는 국내 ActiveX 보안 문제도 점차 늘어나고 있다. 어플리케이션 취약점 위협의 대표적인 사항은 대다수 사용자가 해당 어플리케이션을 사용하기 때문에, 미치는 영향이 크다고 볼 수 있다.

악의적인 공격자는 어플리케이션 취약점을 이용하여, 악성코드가 포함된 조작된 파일을 대량 메일로 전송하는 방식의 공격이 이루어지며, 악성코드 유포에 빈번하게 이용되었다. 비단 MS 사의 어플리케이션 취약점뿐만 아니라, Apple Mac OS X, ActiveX, 이미지 뷰어, 웹 브라우저, 이메일 클라이언트, 오피스, 메신저, 데이터베이스 등을 대상으로 공격이 다양화 되고 있으며, 2008년에도 어플리케이션 취약점의 위협이 보다 다양화될 것으로 보인다.

2007년 침해사고 현황 – 웹 사이트 공격 지속적인 증가

2007년 1월부터 12월까지 상반기 악성코드 유포를 위해 침해된 사이트 및 배포지 수의 평균은 131/50 이다. 침해사이트 수의 변화는 2007년 9월까지 계속 감소하다가 10월 이후 증가하는 것을 알 수 있는데 이것은 대상 탐색 사이트의 수가 증가하였기 때문이다. 탐색 사이트 별 침해지 비율을 0.37%로 1000개의 사이트중 적어도 3개 이상이 중국해커 등에 의해 침해되고 있다.

2007년 발표된 취약점 중 Internet Explorer를 사용해 악성 코드를 배포하는데 사용된 주요 취약점은 MS07-007과 MS07-017 총 2개이다. MS07-007 취약점의 경우 일부 플랫폼에만 적용 가능한 이유 등으로 악성코드 배포를 위해 거의 사용되지 못했던 데 반해 MS07-017의 경우 모든 플랫 폼에 적용가능하고 취약점을 이용한 악성 코드 배포도 매우 쉽기 때문에 현재 가장 큰 비중을 차지 하고 있다.

실제로 2007년 악성코드를 배포하기 위해 사용되는 취약점 별 비율을 살펴보면 MS07-017 취약점이 88/245로 전체의 약 36%이상을 차지하고 있다. 따라서 2008년에도 Internet Explorer와 관련한 새로운 취약점이 발표되기 전까지는 주로 사용되는 취약점은 MS07-017 취약점이 될 것으로 전망된다. 또한 2007년 후반기부터 점점 대중적으로 널리 사용되는 ActiveX 객체의 취약점을 이용한 악성 페이지도 조금씩 발견되고 있다. 그 동안 공격자가 공격한 취약점은 윈도우 운영체제나 IE에 집중되었으나 ActiveX객체가 많이 쓰이고 있는 국내 웹 사용환경의 특성상 ActviveX객체의 취약점을 이용한 사례도 간간히 발견되고 있다.

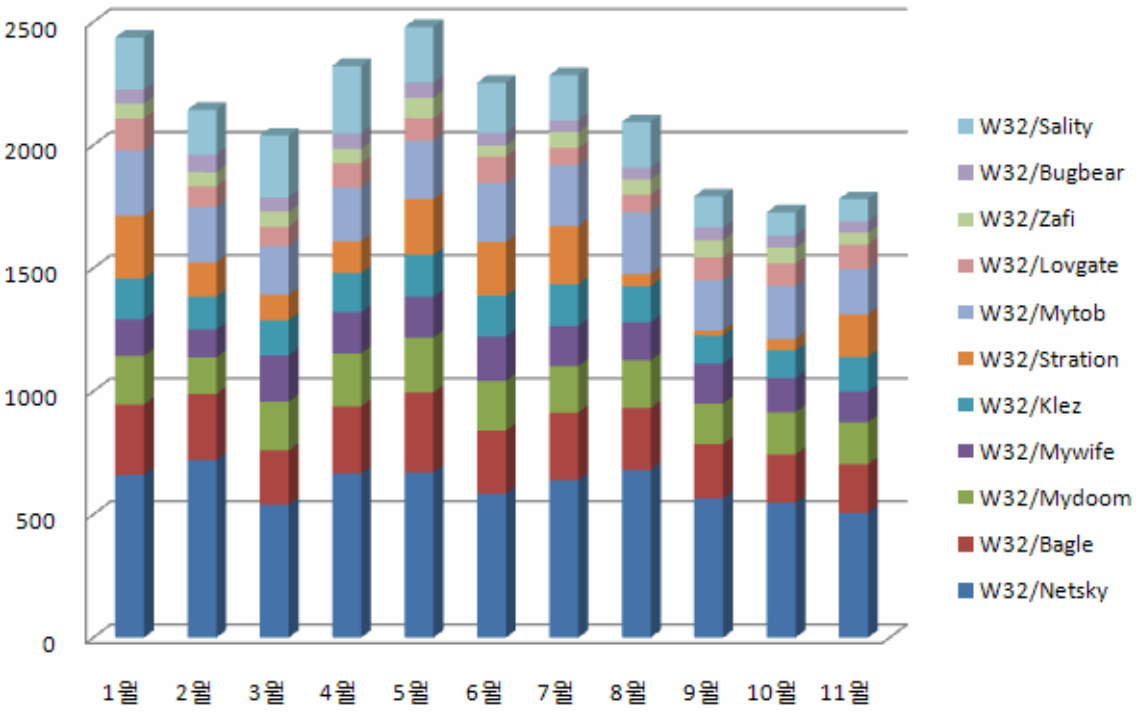
Mpack이나 Icepack등 웹 익스플로잇 툴킷이 대중화되면서 이를 이용한 침해사고의 사례도 조금씩 발견되고 있다. 웹 익스플로잇 툴킷을 사용하면 손쉽게 악성 웹 페이지 제작이 가능할 뿐만 아니라 AV 제품의 진단을 피하기 위한 고도화된 알고리즘을 사용할 수 있기 때문에 이를 이용한 공격코드 또한 점점 증가할 것으로 전망된다.

(4) 2007년 일본 악성코드 동향

2007년 일본에서 크게 이슈가 되었던 것들은 트로이목마 감염 피해가 전년도에 비해 증가한 것과 파일 공유 프로그램으로 인한 피해가 여전히 사회문제화 되고 있는 점을 들 수 있다. 피싱으로 인한 피해가 꾸준히 증가하여 사회적인 이슈가 되고 있는 것 또한 올 한해 일본의 악성코드 동향과 관련하여 주목할만한 점이다.

매스 메일러 웜의 감소 추세

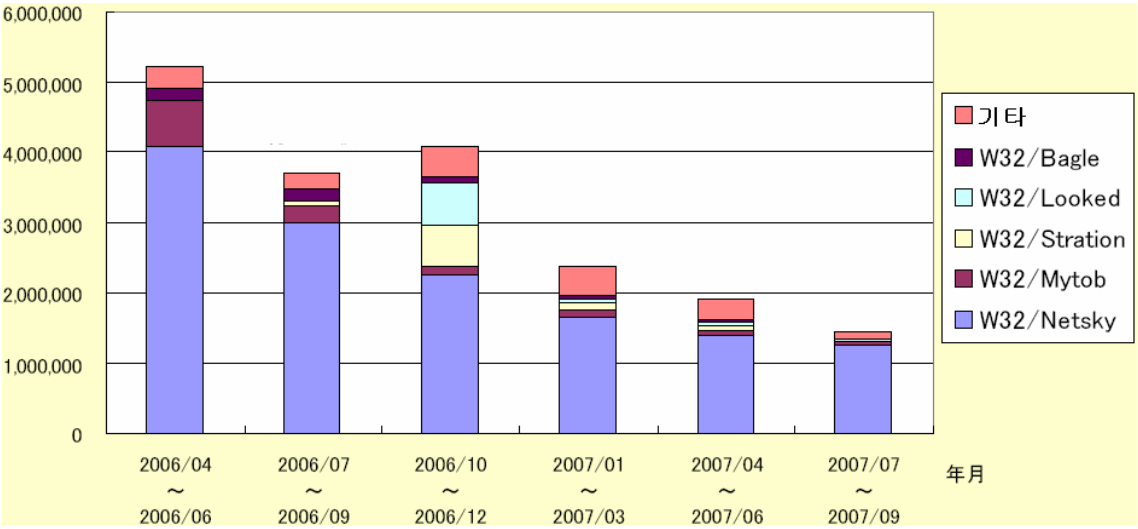
이메일은 불특정 다수에게 악성코드를 노출시킴으로써 감염을 유발시킬 수 있는 가장 편리하고 확실한 도구이다. 이러한 이유로 인해 전체 악성코드에 의한 감염 피해 중 매스 메일러에 의한 감염이 차지하고 있는 비율이 매우 높다. 그러나, 최근에는 웹 서버의 취약점을 이용하여 웹 사이트에 악성코드를 다운로드 할 수 있는 스크립트를 삽입하여 사용자들이 이를 받아가도록 하는 형태의 악성코드들이 많이 등장하고 있고 이로 인한 피해 또한 많은 것으로 보고되고 있으나 설치되는 대부분의 악성코드가 자가 전파력이 없는 트로이목마이거나 공유폴더 등 네트워크상의 취약점을 공격하는 경우가 대부분이므로 전파력이 높다고 볼 수는 없다.



[그림 3-18] 일본 IPA의 월별 악성코드 피해 통계

[그림 3-18]은 일본의 IPA(www.ipa.go.jp)에서 발표한 월별 악성코드 동향 보고서의 내용 중 악성코드 피해 통계를 취합한 것이다. 감염으로 인한 피해의 대부분을 차지하고 있는 것

이 이메일 웜들인 것을 알 수 있다. 도표에서 볼 수 있듯이 2007년 일본에서 가장 많은 피해를 유발한 악성코드는 넷스카이 웜이고 이는 몇 년 동안 변함이 없는 현상이다. 넷스카이 웜 뿐만 아니라 베이글 웜이나 마이둠 웜 또한 이메일 웜으로써 몇 년에 걸쳐 많은 피해를 유발하고 있는 악성코드들이다. 이러한 이메일 웜들의 감염 피해의 수치가 점점 감소하고는 있지만 몇 년에 걸쳐 지속적인 피해를 주고 있는 것으로 이메일 웜의 강력한 전파력을 가늠할 수 있다.



[그림 3-19] 분기별 악성코드 발견 통계

[그림 3-19]는 IPA에서 발표한 분기 별 악성코드 검출 통계이다. 이 데이터는 악성코드가 발견된 전체 개체수를 집계한 것으로 실제 악성코드에 감염되지 않은 경우를 포함하고 있고 같은 시스템에 동일한 악성코드가 중복해서 발견이 된 경우에도 각각의 개체수를 집계한 것이므로 악성코드 감염 피해 정도를 판단하기 위한 데이터로는 부적합하다. 그러나 얼마나 많은 양의 악성코드가 전파되고 있는지를 실감할 수 있는 자료로써의 의미를 가지고 있다.

[그림 3-19]의 자료에서 전파되는 대부분의 악성코드들이 이메일 웜이고 시간이 흐를수록 점진적인 감소 추세를 보이고 있는 것을 알 수 있다. 이러한 현상은 최근에 발견된 이메일 웜도 동일하게 나타나고 있는데 2007년 유행한 누워 웜(Win32.Nuwar.worm) 이나 젤라틴 웜(Win32/Zhelatin.worm)과 같은 이메일 웜은 많은 변형이 유포되고 있는 상태이지만 이로 인한 피해는 그리 많지 않은 것으로 보고되고 있다.

트로이목마 피해의 증가

올 한해 동안 악성코드와 관련하여 전세계적으로 가장 큰 이슈가 된 것 중의 하나는 트로이목마류의 급격한 증가를 들 수 있고 이러한 현상은 일본에서도 크게 다르지 않다. 일본의 경우 작년에 많은 피해를 유발한 애드웨어류가 감소한 반면 트로이목마로 인한 피해가 급격하

게 증가하였다.

순위	악성코드명	악성코드 유형	피해건수	발견일시
1	BKDR_AGENT	백도어	826 건	2003 년 8 월
2	TROJ_VUNDO	트로이목마	333 건	2004 년 11 월
3	JAVA_BYTEVER	기타	273 건	2003 년 5 월
4	TROJ_DLOADER	트로이목마	245 건	2004 년 7 월
5	TROJ_ZLOB	트로이목마	228 건	2005 년 11 월
6	BKDR_HUPIGON	백도어	213 건	2005 년 2 월
7	WORM_SDBOT	웜	204 건	2003 년 10 월
8	WORM_RBOT	웜	203 건	2004 년 3 월
9	ADWARE_BESTOFFERS	에드웨어	165 건	2006 년 7 월
10	EXPL_ANICMOO	기타	146 건	2007 년 3 월

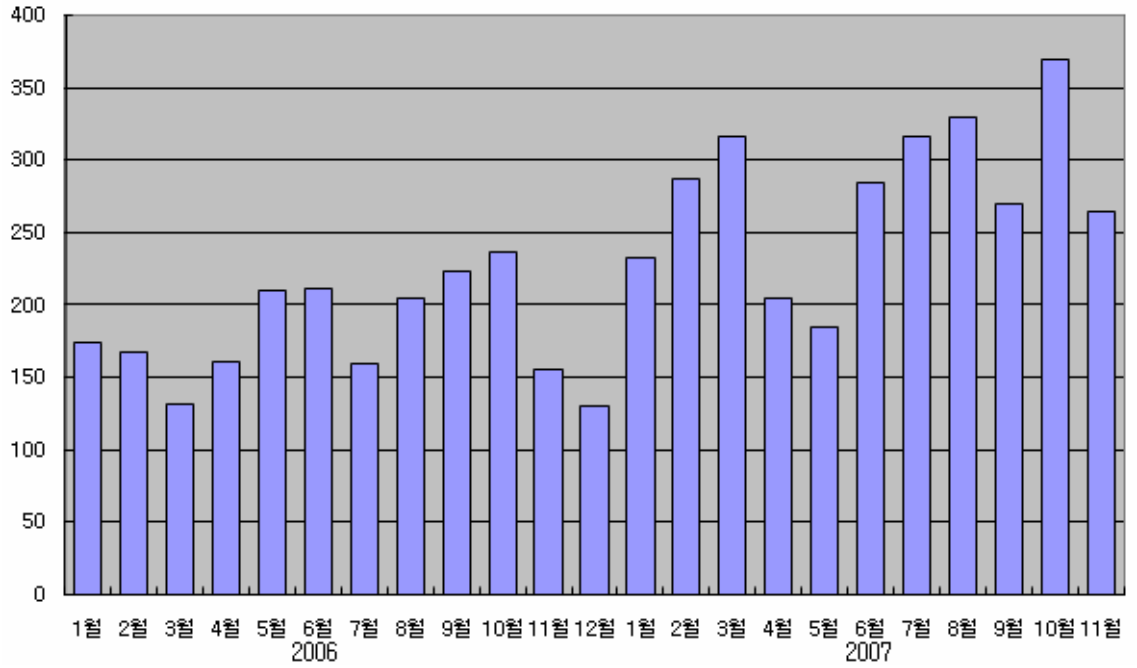
[표 3-8] 일본 Trendmicro의 2007년 바이러스 피해보고 리포트

위의 [표 3-8]은 일본 트렌드마이크로사(www.trendmicro.co.jp)에서 발표한 2007년 악성코드 피해보고 리포트의 내용 중 일부를 발췌한 것이다. 피해 집계된 내용에서 볼 수 있듯이 순위에 링크된 대부분의 악성코드가 백도어 등의 트로이목마류이다. 이러한 트로이목마류의 공통된 특징은 직, 간접적으로 개인 정보를 불법으로 취득하는 것을 목적으로 하므로 사용자의 주의가 필요하다.

트로이목마 이외에도 아이알씨 봇(Win32/IRCBot.worm)이나 에스디 봇(Win32/SDBot.worm)과 같은 봇류에 의한 피해 또한 많이 발생한 것을 볼 수 있는데 봇넷에 의한 네트워크상의 피해는 일본 내에서도 심각한 문제로 대두되고 있다. 일본에서는 봇에 대한 피해 예방을 위해 정부 기관과 통신사 ISAC이 주축이 되어 운영되는 사이버 클린 센터(www.ccc.go.jp)와 같은 단체가 만들어지는 등의 노력을 하고 있다.

피싱으로 인한 피해 증가

일본에서 가공 청구로 인한 문제는 피싱이나 보이스피싱과 같은 온라인 사기가 전 세계적으로 이슈화가 되기 전부터 온/오프라인상의 문제가 되어왔다.



[그림 3-20] 월별 부당청구 관련 피해 상담 통계

위의 [그림 3-20]는 일본의 IPA에서 월별로 집계한 부당청구 관련 상담 통계이다. 피해 건수가 시간이 갈수록 점점 늘어나고 있는 것을 알 수 있는데 일본에서는 출처를 알 수 없는 업체로부터 발송된 사용료를 납부하라는 엽서에서부터 불법 소프트웨어에 이르기까지 다양한 형태로 사용자를 유인하는 행위들이 발생하고 있다. 최근에도 원클릭 이라는 소프트웨어에 의해 성인사이트로 등록이 되고 이를 악용한 부당 청구로 인한 피해가 다수의 사용자들에게 발생하여 이슈가 된 사례가 있다.

Antinny 감염으로 인한 정보 유출

Antinny는 p2p 프로그램의 설정을 바꾸는 등의 동작을 수행함으로써 개인 정보를 유출하게끔 유도하는 트로이목마류의 일종이다. 일본에서는 Winny라는 p2p 기반의 파일 공유 프로그램을 많이 사용하고 있는데 Antinny에 감염된 PC로 인해 공개되지 않아야 할 정보가 Winny를 이용하여 무작위적으로 배포되고 그 중에는 국가의 군사 기밀이나 기업의 중요 정보가 공개는 경우도 있어서 사회적인 이슈가 되었었다.

(5) 2007년 중국 악성코드 동향

2007년 한 해 동안 중국의 악성코드 동향을 되돌아 보면 2006년도부터 진행되었던 악성코드의 국지화와 금전적인 목적을 위한 감염 시도가 더욱 심화되고 있는 실정이다.

악성코드 TOP 10

순위	JiangMin	점유율	수치
1	Checker/Autorun	3.54%	1221695
2	Exploit.ANIfile.b	2.18%	751630
3	Trojan/PSW.QQPass.qhf	0.84%	289433
4	Adware/Clicker.je	0.75%	261378
5	Adware/Adload.ad	0.47%	163005
6	Trojan/PSW.GamePass.frl	0.47%	162478
7	Adware/Agent.p	0.43%	149346
8	Trojan/PSW.GamePass.acuh	0.41%	141787
9	Adware/Boran.e	0.37%	128305
10	Trojan/Agent.psm	0.36%	126660

[표 3-9] 강민(JiangMin) 2007년 악성코드 TOP 10

2007년 중국의 악성코드 동향에서 가장 큰 변화로 꼽을 수 있는 것이 악성코드를 감염 시키기 위해 새로운 감염 기법의 등장으로 볼 수가 있다. USB 외장형 저장장치가 보편화되면서 웜이나 트로이목마의 악성코드의 형태에 구분 없이 중국뿐만 아니라 한국에서도 많은 문제점을 야기했던 Autorun.inf을 첫 번째로 꼽을 수 있는 감염 기법의 변화로 볼 수 있다. 2007년 2월에서 3월경부터 등장하기 시작한 Autorun.inf 파일을 이용한 감염 기법은 예전 플로피 디스크를 이용하던 시절을 연상시킬 정도로 심각한 문제로 대두되었다. 이러한 문제는 위 [표 3-9]의 강민(JiangMin) 2007년 악성코드 TOP 10에서 Checker/Autorun(V3 진단명 – TextImage/Autorun)이 1위를 차지하고 있다는 면에서 충분히 알 수가 있다.

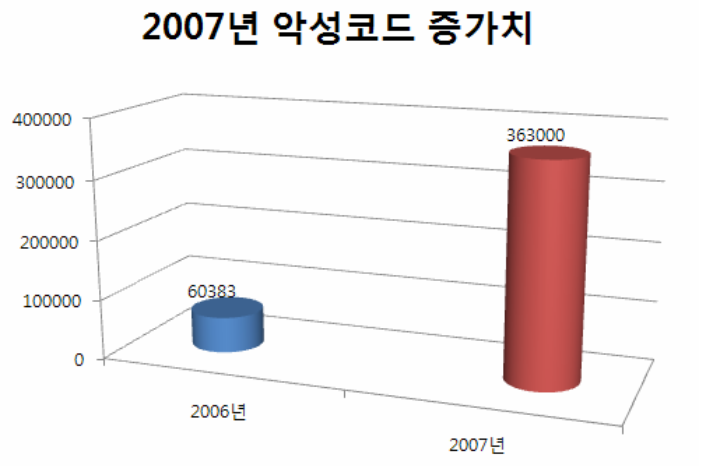
그 다음으로 심각한 위협으로 발전한 감염 기법을 본다면 바로 웹을 통한 악성코드의 감염을 들 수가 있다. 이는 중국 내에서만의 문제가 아니라 전세계적인 하나의 큰 흐름으로 발전하고 있는 실정이며 이러한 웹을 통한 감염 기법의 심화는 Exploit.ANIfile.b(V3 진단명 – Win-Trojan/ANIExploit.Gen)가 2위를 차지하고 있다는 것만으로도 충분히 알 수가 있다.

2007년의 중반 경부터 등장하기 시작한 ARP 스푸핑을 이용한 악성코드의 감염기법은 악성코드를 감염 시키기 위해 존재하는 악의적인 웹 사이트를 직접적으로 방문하지 않아도 악성코드에 감염될 수 있다는 점을 보여준 사례라고 할 수 있다.

감염 기법 면에서 본다면 앞서 서술한 3가지 기법들이 2007년 중국 악성코드 동향의 큰 축이었다면, 악성코드 형태별로 본다면 사용자 정보를 탈취하는 트로이목마가 가장 심각한 위협으로 볼 수가 있다. 이러한 형태의 악성코드는 2005년경부터 등장하기 시작하였지만 2007년의 경우를 본다면 공격의 대상이 한국에서 개발된 온라인 게임에서 벗어나 중국에서 개발된 온라인 게임으로 목표가 변경되고 있는 실정이다. 특히 Trojan/PSW.QQPass.qhf(V3 진단명 – Win-Trojan/QQPass.Gen), Trojan/PSW.GamePass.frl(V3 진단명 – Win-Trojan/OnlineGameHack)와 Trojan/PSW.GamePass.acuh(V3 진단명 – Win-Trojan/OnlineGameHack)이 각각 3위, 6위와 8위를 차지하고 있다 점에서 중국 내에서의 온라인 게임을 공격 대상으로 한 트로이목마는 2007년에 가장 활동이 활발했다고 볼 수 있다.

이러한 공격 대상의 변화에 대한 원인은 크게 2가지로 볼 수가 있는데 첫 번째로 국내 온라인 게임 개발 업체가 다양한 보안 기능 강화와 중국 내에서 개발된 온라인 게임의 아이템 거래 활성화로 볼 수 있다. 최근에 알려진 바에 따르면 중국 내에서는 이미 온라인 게임 아이템을 거래 할 수 있는 웹 사이트가 약 4만여 개에 이르며 중국인들이 가장 많이 사용하고 있는 QQ메신저를 통해서 QQ머니 라는 사이버 머니 역시 불법적으로 거래가 활성화되고 있다고 한다. 이러한 심각성은 2007년 2월 델보이 바이러스(Win32/Dellboy) 바이러스의 제작자로 알려진 리 준의 구속은 악성코드의 판매와 온라인 게임 사용자 계정 탈취를 위한 트로이목마 유포가 상업적으로 얼마나 많이 이용되고 있는지를 충분히 잘 보여주고 있는 사례로 들 수가 있다.

악성코드 형태별 증가치

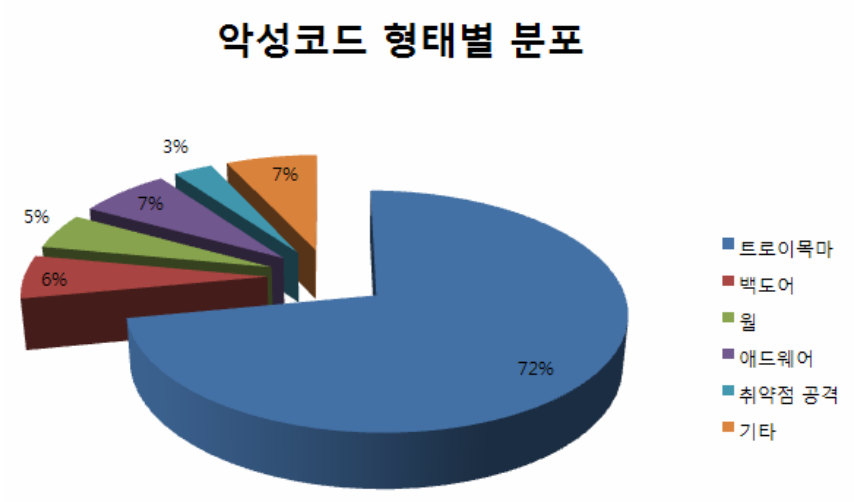


[그림 3-21] 강민(JiangMin) 2007년 악성코드 증가치

중국 로컬 백신 업체인 강민(JiangMin)의 발표에 따르면 2007년 한 해 동안 발견된 중국 내

악성코드는 총 363,000건으로 2006년 한 해 동안 발견된 60,383건 보다 6배에 이르고 있다고 한다. 이는 전 세계적으로 발견되는 악성코드가 수치적인 면에서 급격하게 증가하고 있는 현상 역시 중국 내에서도 동일하게 이루어지고 있다는 것을 잘 알려주고 있다.

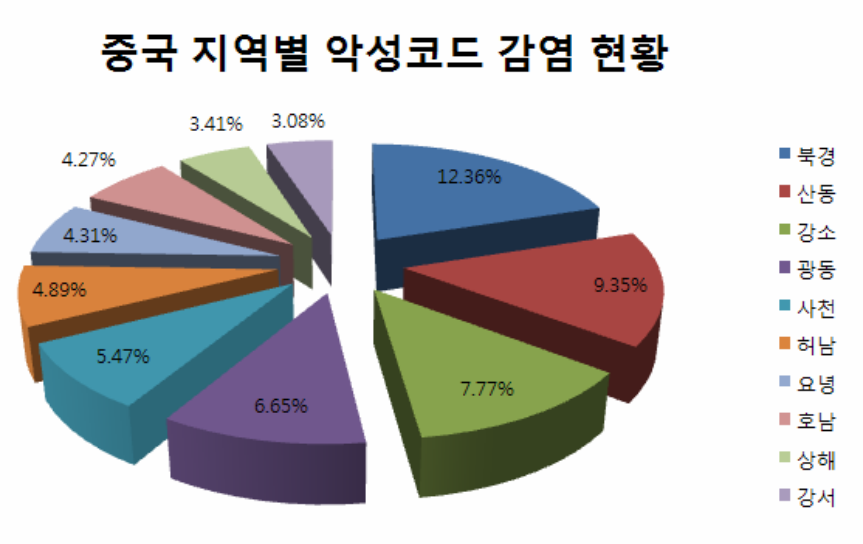
악성코드 형태별 분류



[그림 3-22] 강민(JiangMin) 2007년 악성코드 형태별 분포

악성코드의 형태면에서는 2006년에 이어서 2007년 역시 트로이목마가 절대 다수를 차지하고 있다. 이는 앞서 기술한 바와 같이 온라인 게임 아이템 탈취와 사용자 정보 탈취를 통해서 불법적인 재화의 거래가 가장 크게 작용하고 있기 때문이라고 볼 수 있다. 또 한가지 2007년도 악성코드 형태 면에서 특이점은 광고를 목적으로 제작되는 애드웨어 역시 크게 증가 한 것을 알 수 있다.

중국 지역별 악성코드 감염 현황



[그림 3-23] 강민(JiangMin) 중국 지역별 악성코드 감염 현황

2007년 중국내 지역별 악성코드 감염 현황은 이제까지 분기 별 동향에서 기술한 바와 크게 다르지는 않다. 컴퓨터와 네트워크 사용량이 많이 지역을 중심으로 악성코드 감염율이 특히 높은데 이러한 지역으로는 가장 많은 악성코드 감염을 보이고 있는 북경과 광주와 같은 큰 대도시가 포함되어 있는 산동의 순으로 이어지고 있다.

(6) 2007년 세계 악성코드 동향

2007년 세계의 악성코드 동향을 보면 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. 하지만, 이들 통계를 통해 국가별 차이를 알 수 있다.

영국 소포스(Sophos)의 통계를 보면 1,2 위는 모두 스크립트 악성코드가 차지하고 있다.[1] 메일로 전파되는 악성코드 역시 발견된지 3년이 지난 넷스카이 웜(Win32/Netksy.worm), 마이톱(Win32/Mytob.worm), 마이둠 (Win32/Mydoom.worm) 등이 순위를 차지하고 있다. 이는 여전히 과거 악성코드에 감염된 시스템이 존재하고 이들 시스템에서 메일을 발송하고 있기 때문이다. 2007년은 스트레이션 웜(Win32/Stration.worm), 젤라틴(Win32/Zhelatin.worm) 등이 계속 보고되었다.

러시아 카스퍼스키연구소(Kaspersky Lab)의 통계를 보면 1위는 역시 넷스카이 웜이 차지하고 있다. 넷스카이 웜은 2007년 내내 계속 순위권에 포함되어 있었다. 하지만, 실제 감염된 시스템 통계를 보면 바이럿 바이러스(Win32/Virut virus)가 상위권에 존재하고 있다. 바이럿 바이러스는 여러 국가에서 순위권 내에 있는 바이러스이다.

폴란드 아르카비르(ArcaVir)사의 통계에 따르면 1위는 국내에도 발견되었지만 널리 퍼지지는 않은 Win32/Jeefo 바이러스가 1위를 차지하고 있으며 여러 변형이 발견된 소로우 웜 변형이 (VBS/Solow)가 2위이고 소로우 웜 원형은 7위를 차지하고 있다. 특이한 점은 윈도우 95/98에서 활동하는 CIH 바이러스(Win95/CIH virus)가 9위를 차지하고 있다. 아마도 폴란드에서는 윈도우 95/98 사용이 여전히 많은 것으로 추정된다.[2]

슬로바키아 에셋(Eset)사의 2007년 통계에 따르면 1위는 스트레이션 웜 변형(Win32/Stration.worm)이다.[3] 357.2 개 메일 중 1개에서 발견될 만큼 압도적인 수를 차지하고 있다. 3위는 넷스카이 웜 변형이며 4위, 5위, 6위 모두 스트레이션 웜이 차지하고 있다. 에셋사의 통계는 기본적으로 메일을 통해서 파악되며 체코의 포털 사이트인 Seznam (http://www.seznam.cz/)의 메일을 모니터링하고 있기 때문에 체코 내에서 활동하거나 유입되는 악성코드의 통계로 볼 수 있다.

아이슬랜드 프리스크 소프트웨어(Frisk Software)에 따르면 지난 1년간 1위는 휴리스틱 진

[1] http://www.sophos.com/pressoffice/news/articles/2008/01/toptendec07.html
[2] http://www.arcabit.com/
[3] http://www.virusradar.com/stat_01_current/index_c12m_enu.html

단이므로 특정 악성코드는 아니다. 따라서 실제 악성코드 순위에서 1위는 나이젬 웜 변형(Kapser, Mywife 등)이며 2위는 소버 웜 변형, 마이톱 변형, 넷스카이 웜 변형 등이다.

인도 프로랜드(Proland)사의 통계에 따르면 1위는 Feebs 웜, 2위는 역시 넷스카이 웜 변형과 Reyds 웜 변형이다. 5위는 바이킹 바이러스 변형으로 보이는 Looked 바이러스이다.

루마니아 비트디펜더의 통계에 따르면 2007년 1위는 Trojan.Peed.Gen와 2위 다운로더 추정 트로이목마가 차지했다.[1] 하지만, 이 트로이목마들은 변형까지 포함한 진단이므로 실제 1위는 3위인 넷스카이 웜 변형이다. 5위는 나이젬 웜 변형인 나이젬.E 웜(Win32/Nyxem.E@mm) 이 차지했으며 나이젬 웜 변형이 유럽에서 널리 퍼졌던 것으로 보인다.

트렌드마이크로사의 통계에 따르면 지난 1년간 1위는 애드웨어의 일종인 Vundo 변형이다.[2] 하지만, 이 진단명도 의심 추정이므로 오진 가능성과 여러 변형을 단일 진단명으로 진단하고 있을 수 있다. 2위는 WORM_GAOBOT.DF, 3위는 WORM_SPYBOT.IS로 악성 IRCbot이 차지하고 있다. 악성 IRCbot은 최근 특정 지역에 소규모로 퍼지는 경우가 대부분이라 다소 특이한 수치로 보인다. 또한 2000년에 발견된 러브레터 바이러스(VBS/Love_Letter virus)가 5위를 차지하고 있어 특이한 결과이지만 대만계 다국적 기업인 트렌드로 통계를 보면 대만에서 러브레터 바이러스가 1위로 파악되어 대만 지역 사용자가 많다고 가정하면 특정 지역의 결과가 전체 통계에 영향을 준 것으로 보인다.

종합적으로 보면 2007년에도 국가별로 활동하는 악성코드 성향이 다르다. 대한민국은 온라인 게임 계정 탈취 트로이목마가 기승을 부리고 있지만 다른 나라에서 악성코드 통계에서는 순위 권에 없거나 몇몇 업체의 하위권에 분포할 뿐이었다.

핀란드 F-시큐어(F-Secure)사의 통계에 따르면 2007년까지 발견된 악성코드는 50만개 이며 2006년까지 발견된 약 23만개에서 1년 사이 2배가 증가한 엄청난 악성코드가 증가했다. 2007년까지 발견된 악성코드가 최소 50만개에서 최대 100만개까지 존재하는 것으로 보인다. 이는 유사 변형이 계속 제작되고 있기 때문에 통계가 부정확해진 것으로 보인다. 하지만, 확실한 건 2008년에도 악성코드 증가 수는 줄지 않을 것으로 보인다.

[1] http://www.bitdefender.com/NW647-world--BitDefender-Lab's-Top-10-Malware-List-for-2007.html
[2] http://itw.trendmicro.com/index.php?id=25

Ⅳ. 2007년 악성코드 주요 이슈 및 2008년 예측

(1) 2007년 악성 코드 주요 이슈

2007년 악성코드/스파이웨어 동향을 분석한 결과 새로 발견된 악성코드(바이러스, 웜, 트로이목마의 통칭)는 6,107개로 전년 동기 대비 33.6% 증가했으며, 스파이웨어는 6,527개가 새로 발견돼 지난해 동기 대비 8.6% 증가했다[1]. 2007년에 있었던 주요한 보안 이슈로는 ▶공격의 국지성 심화를 비롯해 ▶'사이버 블랙 마켓' 통한 대가성 범죄 급증 ▶웹사이트 해킹 심화 ▶허위 안티스파이웨어 급증 ▶좀비 PC 만드는 봇넷(BotNet) 기승 ▶이동저장장치 노린 악성코드 기승 ▶스파이웨어 전파 방법의 지능화 ▶악성코드 은폐 기법의 고도화 ▶ARP 스푸핑 해킹 기법과 악성코드의 결합 ▶애플리케이션 취약점 공격 다양화 등을 주요 이슈로 정리할 수 있다

(1) 공격의 국지성 심화: 악성코드의 국지성이 심화했다. 그 이유는 악성코드 제작자들이 금전을 얻고자 개인 정보 빼내는 데 목표를 두기 때문이다. 따라서 불특정 다수가 아닌 한 국가, 한 회사, 한 커뮤니티 사이트를 겨냥해 웹사이트를 해킹한 후 악성코드를 심는 일이 갈수록 급증하고 있다. 단적인 예로 특정 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 경우 올해 1800개가 발견돼 전년 동기 대비 95.9% 증가할 만큼 기승을 부렸다.

(2) '사이버 블랙 마켓' 통한 대가성 범죄 급증: 사이버 상에서 거래되는 가상의 재화를 현금으로 교환하는 일이 늘고 있다. 이에 따라 불법으로 재화를 거래하는 소위 '사이버 블랙 마켓'이 형성된 것으로 알려졌다. 최근 발생하는 대부분의 보안 위협은 '블랙 마켓'을 통해 현금을 얻는 데 목적이 있는 것으로 보인다. 여기서는 신상 정보 및 신용카드 정보, 온라인 게임 계정 등이 거래되고 있으며, 악성코드가 판매되는가 하면 봇넷이나 피싱, DDoS(분산 서비스 거부) 공격 등을 대가를 받고 해주는 것으로 알려져 있다.

현재 '블랙 마켓'이 가장 크게 활성화한 곳은 러시아와 중국이다. 우리나라는 중국 블랙 마켓의 영향력이 크게 미친다고 볼 수 있다. 특히 두 나라 사이에서는 대규모 다중사용자 온라인 롤플레잉 게임(MMORPG)에서 발생하는 아이템이 현금으로 거래되고 있어 게임 사용자의 정보가 매우 큰 가치를 갖는다. 따라서 이를 노리는 피해 규모도 상상을 초월할 것으로 추정된다.

(3) 웹사이트 해킹 심화: 웹사이트가 해킹을 당해 악성코드와 스파이웨어를 유포하거나 해당 웹페이지로 유도하는 역할을 하는 일이 많이 발생했다. 2007년 한 해 동안 2006개의 웹사이트가 악성코드/스파이웨어 유포지나 경유지로 이용됐다. 특히 인터넷 뉴스, 포털 사이트 등

[1] 스파이웨어 수치의 경우 2006년과 2007년의 통계 기준이 상이하여 정확한 증가수치를 의미하지 않는다.

방문자 수가 많은 웹사이트가 주된 해킹 대상이었다. 이는 다수의 취약한 PC에 악성코드를 설치할 수 있다는 점에서 가장 효과적인 방법이기 때문이다.

(4) 허위 안티스파이웨어 급증: 스파이웨어의 발견 및 피해 신고가 늘고 있을 뿐 아니라 허위 안티스파이웨어 또한 증가해 큰 피해를 주었다. 악성코드에 감염되었다는 허위 메시지를 보여주고 치료를 유도하는 허위 안티스파이웨어는 2006년에는 67개가 발견됐으나 2007년 11월 말 현재 186개로 3배 가까이 급증했다.

(5) 좀비 PC 만드는 봇넷(BotNet) 기승: 2007년 악성 IRC봇의 수는 2006년에 비해 다소 감소했다. 하지만 화상채팅 사이트, 게임 아이템 거래 사이트에 대한 DDoS 공격처럼 봇넷을 이용한 공격은 점차 대담해지고 있다. IRC 채널뿐 아니라 P2P를 이용하는 경우도 많아지고, 컴퓨터의 사양이 좋아짐에 따라 몇십 대에서 몇백 대의 좀비 PC만으로 DDoS 공격이 가능하기 때문에 피해는 갈수록 커질 것으로 전망된다.

(6) 이동저장장치 노린 악성코드 기승: 2007년은 이동저장장치(USB 플래시 메모리, 이동식 하드디스크)를 통해 전파되는 오토런(Autorun) 웜이 기승을 부렸다. USB 플래시 메모리 사용이 대중화함에 따라 악성코드 제작자들도 이를 노린 것으로 보인다. 현재 USB 플래시 메모리는 악성코드 전파 경로로만 이용되고 있지만 USB 플래시 메모리에 저장된 공인인증서 등의 정보 자체를 노린 악성코드도 등장할 수 있다.

(7) 스파이웨어 전파 방법의 지능화: 스파이웨어가 사용자의 동의를 거치지 않고 손쉽게 설치되기 위해 각종 지능적인 기법을 사용하고 있다. 다른 프로그램이 설치될 때 사용자 몰래 함께 설치되거나 동영상 플레이어 같은 특정 프로그램이 설치된 후 그 프로그램의 일부인 양 다운로드되기도 한다. 스파이웨어가 설치된 것을 인지하지 못하게 하거나 분석을 어렵게 하는 루트킷(root kit; 해커가 컴퓨터에 침입한 사실을 숨긴 채 관리자용 접근 권한을 획득하는 데 사용하는 도구)을 상용하기도 한다. 10월에 등장한 랜섬웨어는 동영상 플레이어 설치 후 화면을 크게 하는 데 필요한 프로그램인 것처럼 설치됐다. 사용자의 동영상 파일을 임의로 다른 폴더에 옮긴 후 실행하려고 하면 휴대전화 번호를 입력해 인증 절차를 거치게 하고, 7일 동안 해지하지 않으면 매달 자동 결제가 되도록 해 많은 피해를 낳았다.

(8) 악성코드 은폐 기법의 고도화 보안 제품의 성능 및 진단 기법이 향상됨에 따라 최근의 악성코드들은 보안 제품을 역분석해 진단을 회피하거나 무력화를 시도한다. 최신 기법에는 첫째, 종전에는 보안 제품의 프로세스를 종료하거나 파일을 삭제했으나, 최근에는 보안 제품이 정상적으로 동작하는 것처럼 보이지만 실제 기능은 중지시켜 사용자가 인지하기 어렵게 하는 기법이 있다. 둘째, 윈도 파일 보호 기능을 기존과 전혀 다른 방법으로 우회해 시스템 파일을 악성코드로 변경하는 기법이다. 셋째, 정상 행위와 악성 행위를 교묘히 섞어 보안 제품이 악의적인 행동을 탐지하지 못하게 하거나 잘못 탐지하도록 유도하는 방법이다.

(9) ARP 스푸핑 해킹 기법과 악성코드의 결합: ARP 스푸핑(Address Resolution Protocol Spoofing)은 동일 네트워크에 존재하는 공격 대상 PC의 IP 주소를 공격자 자신의 랜카드 주소와 연결해 다른 PC에 전달돼야 하는 정보를 가로채는 공격을 말한다. 어떤 PC에 ARP 스푸핑 기능을 가진 악성코드가 설치되면 약간의 조작으로 동일 구역 내의 다른 PC에 쉽게 악성코드를 설치할 수 있다. 이 기법 자체가 새로운 것은 아니지만 올해 상반기에 많은 피해가 있었다. 한편, ARP 스푸핑을 통해 VoIP 도청 등 데이터 변조를 쉽게 할 수 있어 기업 내부 네트워크 보안의 중요성이 부각되고 있다.

(10) 애플리케이션 취약점 공격 다양화 : 2007년에 나온 MS 보안 패치 중 애플리케이션(오피스, 인터넷 익스플로러, 일반 애플리케이션)에 관련된 것이 총 66%를 차지했다. 애플리케이션 취약점을 이용해 악성코드가 포함된 파일을 대량 메일로 전송하거나, 인터넷 익스플로러의 취약점을 통해 악성코드를 배포하는 사건이 빈발했다. MS사의 애플리케이션 취약점뿐 아니라, 애플 맥 OS X, 액티브X, 멀티미디어 플레이어, 이미지 뷰어, 메신저 등 사용자들이 많이 사용하는 애플리케이션들을 위협하는 요소도 늘었다.

2007년 악성코드 주요 이슈

올해 악성코드에 대한 키워드를 5가지로 요약해본다면 다음과 같다.

- 진단, 치료하기 복잡한 형태의 파일 바이러스 기승
- 대량 다운로더 트로이목마 피해 급증
- 은폐 및 자기보호 기법의 고도화
- 이동식 저장장치에 기생하는 악성코드 증가
- 중국발 악성코드 유형, 전파의 패러다임 변화

다음은 2007년 한해 주요 악성코드에 대해서 정리해 본 것이다.

► 실행파일 감염 바이러스 증가와 바이러스의 위험한 도전

판다 바이러스라고 일반인들에게 알려진 Win32/Dellboy (델보이) 바이러스 변형은 1/4 분기에 약 25종의 변형이 발견 되었다. 그러나 제작자가 구속된 이후 이 바이러스의 변형은 더 이상 보고 되지 않고 있다. Win32/Virut 변형 (C, D형) 그리고 Win32/Alman.C 바이러스는 매우 위험한 것으로 보고 있다. 먼저 이들은 분석 및 백신 제작을 지연 시킬 목적이 강하다. 복잡한 형태의 이들 바이러스 이전 변형과는 한 단계 업그레이드 된 형태이다. 특히 Win32/Alman.C 바이러스는 은폐기법이 적용 되었다.

Win32/Virut 은 그 복잡도가 작년에 발견된 원형 보다 한층 강화 되었다. 이 바이러스는 감염 후 특정 IRC 서버로 접속하여 팝업광고를 노출하는 애드웨어를 다수 설치 하기도 했다. 그리고 하반기에는 이 바이러스 변형으로부터 다운로드 되는 악성코드가 DDoS 공격에 사용되기 도 하였다.

► 악성코드의 은폐기법 및 자기 보호 기능 고도화

악성코드가 자신의 생존시간을 더 유지 하기 위해서 안티 바이러스의 프로세스를 종료하거나 파일을 삭제하는 건 일반화 되었다. 이제는 악성코드가 지능적으로 안티 바이러스나 보안 제품을 우회하여 진단을 회피한다. Win-Trojan/Rustock, Win-Trojan/Runtime 이라고 알려진 은폐형 스팸 메일러는 잘 알려진 안티 루트킷 제품이 메모리에 로드 되는 순간 이를 탐지하여 은폐 진단을 우회 한다. 또한 이들중 Win-Trojan/Runtime 트로이목마는 파일 시스템 드라이버와 같은 시스템 커널 드라이버의 DRIVER OBJECT 내 DISPATC HER TABLE 정보를 이용하여 자신을 은폐 하도록 한다. 또한 자신을 보호할 목적으로 레지스트리 복구기능 프로세스 종료 감지기능, 재부팅시 레지스트리 및 파일 재복구 기능등으로 자신의 생존성을 극대화 하였다.

► 리얼 머니를 노렸던 Win-Trojan/Banki

그 동안의 중국산 악성코드의 상당수는 국내 온라인 게임의 타켓으로 사용자 계정을 훔쳐내어 온라인 게임의 사이버 머니 또는 아이템을 훔쳐내는 등 피해를 주었다. 그러나 Win-Trojan/Banki (이하 뱅키 트로이목마) 라고 알려진 이 트로이목마는 국내 유명 은행의 인터넷 뱅킹 접속 사이트를 가장하고 사용자의 공인 인증서를 유출 한다. 사실 공인 인증서는 단순히 복사만 하면 다른 곳에서도 사용 할 수 있기 때문에 악성코드에서 이를 쉽게 이용 할 수 가 있었다.

► LSP (Layered Service Providers) 후킹을 이용한 정보 탈취

국내 온라인 게임의 사용자 계정을 탈취 하는 악성코드들중에서 유행처럼 LSP 를 이용하여 TCP/IP 핸들러를 삽입하고 Winsock2 의 연결을 변경하여 자신을 실행하고 정보를 훔쳐내는 형태가 단기간 증가 하였다. 이 악성코드 초기 발생시에는 일부 안티 바이러스 제품이 LSP 관련 레지스트리 값을 수정하지 않아서 악성코드 치료 후 인터넷이 안 되는 문제가 발생하는 오류가 있기도 했다.

► ANI 취약점을 이용하는 제로데이 공격 발생

ANI 취약점은 매우 심각한 제로데이 공격에 사용 되었다. 이 취약점은 윈도우 비스타와 인터넷 익스플로러 7 에서도 동작 되었다. 이것은 윈도우 애니메이션 커서와 아이콘 파일에 존재하는 취약점 이다. 이 취약점 공격코드가 알려지자마자 기존 중국 발 웹 해킹으로 공격 당한 국내 웹 사이트에서 악성코드를 전파 하려는 취약점이 이것으로 대부분 변경 되기도 했다. 이 취약점이 알려진 이후 중국산 악성코드를 광범위 하게 전파하는데 곧 잘 사용되었는데 이는 올해 기억되는 최악의 보안 취약점으로 생각 된다.

► AutoRun.inf 를 이용한 자동실행 급증

AutoRun.inf 파일의 위험성에 대해서 일반 사용자들은 제대로 인지 해야 한다. 물론 이 파일 자체가 악의적인 이라는 것은 아니다. 이동식 저장장치에 존재 하는 악성코드 복사본이 이 파일로 인해서 자동실행 되도록 된다는데 불필요한 의미가 있다. 즉, AutoRun.inf 와 여기에 자동 실행 되도록 명시 된 파일 (악성코드)이 DOS 시절 플로피 디스켓에 부트 바이러스가 감염 되는 것처럼 컴퓨터에 연결 되는 모든 이동식 저장장치가 감염 대상이라는 것과 이들이 자동실행 된다는 상황은 매우 위험하다고 하겠다.

► ARP Spoofing 공격으로 인한 악성코드 유포

이것은 처음 시도되는 중국 발 해킹의 형태라는 것이다. 이는 보안 패치가 안 된 경우라면 사용자 개입이 필요하지 않아도 악성코드를 감염 시킬 수 있다. 단지 사용자는 웹에 연결 했다는 이유 하나만으로 클래스가 동일한 서브넷에 Win-Trojan/MulDrop (MulDrop 이 전부 ARP Spoofing 공격도구를 의미 하지는 않는다.) 를 설치 후 약간의 세팅만으로 악성코드를 감염 시킬 수 있는 것이다. 물론 공격 받는 시스템은 인터넷 익스플로러의 보안 취약점이 존재해야 하지만 이것은 서브넷에 연결된 모든 (보안이 취약한) 시스템들을 감염 시키는데 있어서 매우 위협적인 방법 이다.

► MSN 메신저 웜의 기승

Win32/ShadoBot.worm, Win32/MSN.worm, Win32/MSGBot.worm 이라고 명명된 악성코드는 모두 MSN 을 이용하여 자신을 전파 시키는 웜이다. 올해 MSN 메신저를 비롯한 메신저로 전파되는 악성코드가 부쩍 증가 하였다. Win32/Stration.worm.Gen 의 일부 변형은 자신의 변형을 Skype 또는 다른 메신저로 전파 하기도 한다.

2005년도 비슷한 사례가 있었는데 Win32/Kevir.worm, Win32/Bropia.worm 이 그것이다. 그 당시에도 이 웜들의 다수 변형이 급격히 증가한 사례가 있다. 2005년의 MSN 웜과 오늘날 발견되는 MSN 웜과의 차이라면 BotNet 를 직접적으로 이용하느냐 또는 이용하지 않느냐에 차이다.

즉, 2005년에 극성을 부린 MSN 웜은 악성 IRCBot 웜을 다운로드 또는 내부에 별도의 실행 파일도 포함 하고 이를 실행하는데 주목적 이였다면 올해를 비롯하여 최근에 발견 되는 MSN 웜의 특징은 BotNet 직접 접속하고 IRCBot 기능과 자신을 전파 시키기 위한 수단으로 윈도우 OS 취약점을 이용하는 것이 아닌 MSN 메신저를 노렸다는데 있다. 또한 MSN 으로 자신을 전파 하려는 증상은 BotNet 에 접속 후 접속 한 채널의 공격자가 명령을 내려야만 동작하므로 메신저를 이용한 전파 증상이 재현 될 수도 있고 재현 되지 않을 수도 있다.

► Win32/Zhelatin.worm 의 기승

Win32/Zhelatin.worm 은 (Storm 웜으로도 불림) 잘 알려진 악성코드로 감염된 시스템의 안티 바이러스 및 보안 프로그램을 무력화 시키며 메일 주소를 수집하여 자신의 변형 및 스팸 메일을 발송한다. 또한 감염된 다른 시스템들과 암호화된 내용으로 오버넷이라고 알려진 일종의 파일 공유 관련 프로토콜을 이용하여 P2P 네트워크를 구성한다. 이는 감염된 시스템들만 사용되도록 private network 를 구성한 후 악의적인 사용자 또는 감염된 시스템들로부터 정보를 획득하여 특정 파일을 다운로드 및 실행 할 수 있도록 해둔다.

안티 바이러스로부터 진단을 회피하기 위해 암호화된 자신의 코드를 풀어 낼 때 바이너리에 하드코딩된 키값이 아닌 랜덤한 쓰레기 API 의 호출 한 후 리턴 되는 인자값을 복호화 키로 사용하는 동적인 방법으로 키값을 구해서 자신을 복호화한다. 이와 같이 동적인 키값을 사용하는 이유는 진단 또는 분석을 방해하도록 가상머신이나 에뮬레이터에서 자신이 실행 되지 않도록 하기 위해서이다.

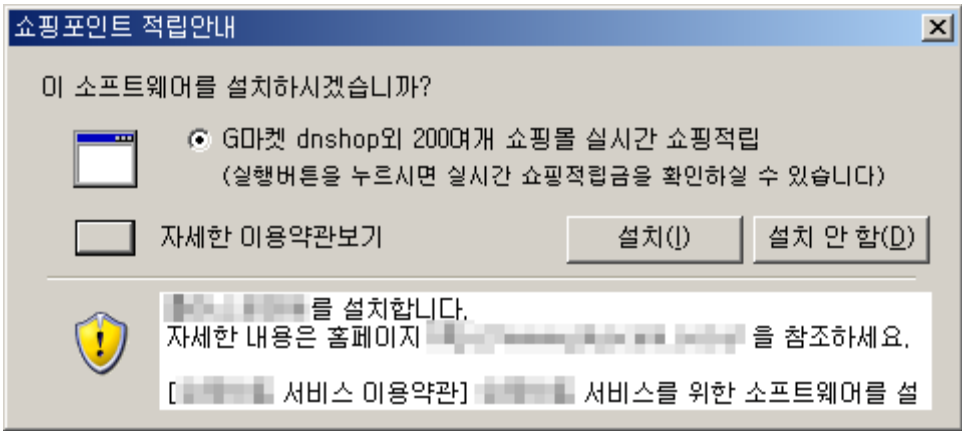
2007년 스파이웨어 트렌드 이슈

► 국내제작 스파이웨어의 증가

2007년에는 국내에서 제작 배포되는 스파이웨어의 종류와 피해가 전년도에 비하여 크게 증가하였다. 이들 국내제작 스파이웨어는 금전적인 이익을 목적으로 하는 애드웨어가 대부분을 차지하고 있는데, 수익모델은 다음과 같이 변화하고 있다.

2005년 - 직, 간접적인 광고 노출을 통한 광고 수익,
2006년 - 허위 안티-스파이웨어 배포를 통한 유료사용 유도,
2007년 - 제휴 쇼핑몰의 찾아가지 않는 적립금

2007년 상반기까지 많은 피해를 입혔던 허위 안티-스파이웨어는 하반기에 접어들면서 제작 배포가 둔화 되었으며, 하반기에는 유명 쇼핑몰과 제휴하여 적립금을 제공하는 툴바 또는 BHO 형태의 리워드 프로그램의 제작 배포가 활발하였다.



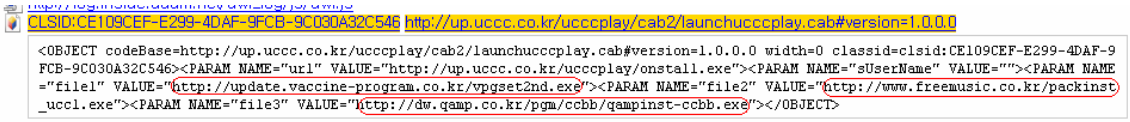
[그림 4-1] 리워드 프로그램의 설치 대화상자

애드웨어 제작 업체들 간의 경쟁은 대량 배포로 이어지며, 사용자 또는 경쟁사 프로그램으로부터 삭제를 방해하는 기능을 요구하게 되었고 점차 악성코드의 특징을 가진 애드웨어가 많이 제작 배포되고 있는 추세이다.

► 교묘해진 배포방법

인기 검색어 또는 실시간 검색어와 관련된 웹페이지 또는 블로그를 개설하여 ActiveX 로 설치를 유도하거나, 유행하는 동영상 낚시 게시물을 이용하여 스파이웨어 설치를 시도하는 등 사회적인 이슈를 스파이웨어 설치에 이용하는 사례가 많이 발견되었다. 유명 프리웨어 프로그램의 번들로 설치 되는 스파이웨어 또한 크게 증가하였으며, 유용한 프로그램으로 위장하

여 아예 사용자 동의를 받지 않거나 사용자를 교묘하게 속이는 스파이웨어도 여럿 발견되었다. UCC를 이용한 스파이웨어 설치는 2007년 스파이웨어 최대 이슈로 삼을만하다. 다운로더 유씨씨플레이 (Win-Downloader/UcccPlay)가 대표적으로, 선정적인 제목의 동영상과 이른바 '낚시 게시물'을 이용하여 ActiveX 컨트롤의 설치를 유도하며, 설치된 ActiveX 컨트롤은 다른 스파이웨어를 사용자 동의 없이 설치하는 다운로더로 동작한다. 2007년 11월 발견된 랜섬웨어로 알려진 스파이웨어 마이컴고가 다운로더 유씨씨플레이에 의해 설치되어 많은 피해를 입힌 바 있다.



[그림 4-2] 다른 스파이웨어를 번들로 설치하는 다운로더 유씨씨 플레이의 ActiveX 코드베이스

2007년 상반기에 많은 피해를 입힌 허위 안티-스파이웨어 프로그램의 설치를 유도하는 클리커 훼이크얼럿(Win-Clicker/FakeAlert) 또한 성인 동영상을 이용하여 설치 유도된다. 검색엔진을 통하여 해외에서 제작된 성인사이트에 접근하면 동영상을 보기 위한 코덱설치를 요구한다. 그러나 이렇게 설치되는 프로그램은 동영상 코덱과는 상관 없는 스파이웨어이다. 이렇게 설치된 프로그램은 스파이웨어에 감염되었다는 허위 경고메세지를 노출하며 사용자 동의 없이 로그 스파이락(Win-Adware/SpyLocked)과 같은 허위 안티-스파이웨어 프로그램을 설치한다.

[그림 4-3] 클리커 훼이크얼럿이 노출하는 허위 경고메세지

► 스파이웨어 대량 감염을 유발하는 다운로더

다운로더를 이용한 스파이웨어 설치가 크게 늘어난 것도 2007년 스파이웨어 동향의 한 특징이다. 다운로더를 이용하면 불특정 웹사이트를 이용하여 ActiveX 컨트롤을 이용하는 것 보다 효과적으로 스파이웨어를 설치할 수 있다. 스파이웨어 배포자는 스파이웨어 설치 당 일정

배당금을 제작사 또는 제휴마케팅 사이트에서 받게 되는데 설치 배당금을 늘리려는 목적으로 다운로더를 이용하여 제휴사의 스파이웨어를 대량으로 다운로드 하는 사례가 많이 발견되었다. 이들 다운로더는 원격지 제어서버에서 설치할 스파이웨어 정보가 포함된 리스트 파일을 다운로드 하고 이 파일에 포함된 제휴사의 다른 스파이웨어를 사용자 동의 없이 설치하게 된다.

► 바이러스 감염, 시스템 장애의 원인

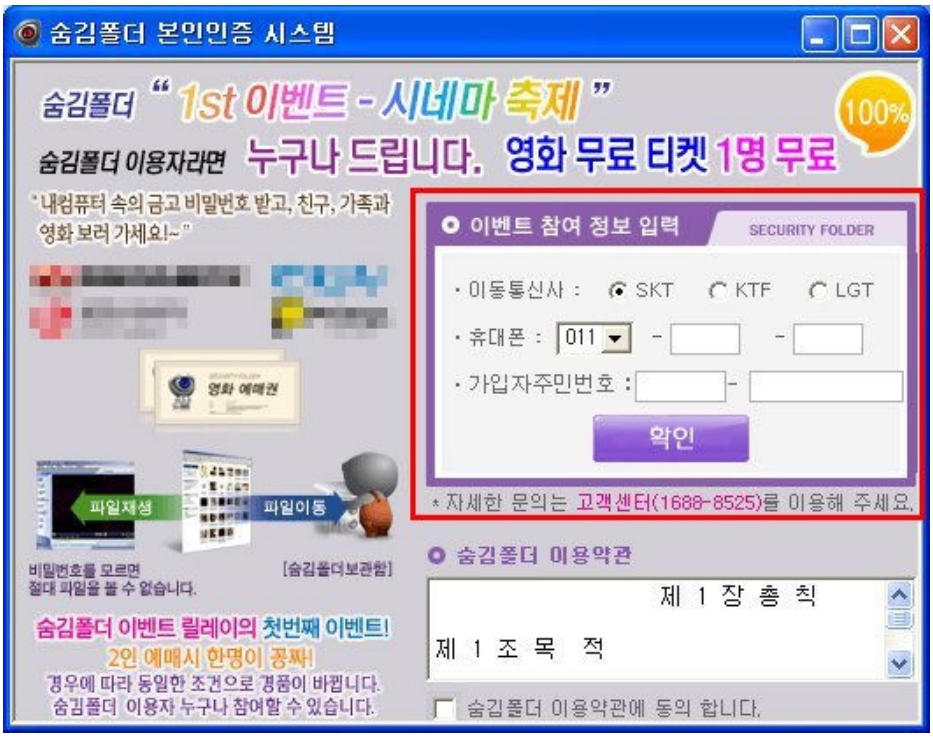
스파이웨어는 단순한 불편함 뿐만 아니라 심각한 시스템 장애를 발생할 수 있다. 2007년 발견된 일부 허위 안티-스파이웨어에 바이럿 바이러스(Win32/Virut)가 감염된 채로 배포되어 명목상 보안 프로그램이 오히려 바이러스 감염의 매개체로 사용되기도 하였으며, 일부 온라인게임 계정 유출 스파이웨어는 의도적으로 바이킹 바이러스(Win32/Viking)의 감염도구로 사용되기도 하였다. 검증되지 않은 프로그램에 의한 오류로 심각한 시스템 성능 저하, 시스템 장애를 발생시킨 사건도 발생하였는데, 일부 애드웨어의 오동작으로 인하여 중요 윈도우 레지스트리가 삭제되고 복구할 수 없는 심각한 시스템 장애가 발생한 사건도 있었다.

애드웨어 어도드(Win-Adware/Adod)는 IE 브라우저가 동작하지 않는 장애를 유발하였다. 애드웨어 어도드는 BHO로 동작하며 주소표시줄 검색결과를 변경하여 광고가 포함된 웹 페이지로 이동하는 기능을 수행하는데, 주소표시줄을 감시하는 과정에서 검증되지 않은 코드로 인하여 오류가 발생하였으며, IE 브라우저 동작이 정지하는 증상을 보였다.

► 스파이웨어 마이컴고

랜섬웨어로 알려진 스파이웨어 마이컴고(Win-Spyware/MyComGo)는 사용자 동의 없이 특정 문자열이 포함된 폴더를 은폐하는 루트킷(Rootkit) 드라이버를 설치한다. 스파이웨어 마이컴고가 설치되면 로컬 하드디스크에 저장된 동영상 파일을 검색하여 루트킷 드라이버가 은폐하는 폴더로 이동하며, 이렇게 옮겨진 파일을 이용하기 위해서는 마이컴고가 제공하는 관리 콘솔을 사용해야 하며 일정 기간이 지난 후 유료 사용을 요구한다.

다운로더 유씨씨플레이 (Win-Downloader/UcccPlay)에 의해 사용자 동의 없이 설치되는 마이컴고에 의해 많은 사용자가 금전적인 피해와 중요 동영상 파일을 분실하는 피해를 입은 것으로 추정된다. 마이컴고 설치 후 일정시간이 지난 후 동영상 파일에 접근하려고 하면 [그림 4-4]와 같은 '본인인증' 대화상자를 띄우는데 사실은 휴대전화 소액결제 대화상자이다. 루트킷 드라이버는 보안 프로그램 또는 경쟁사 프로그램에 의해 삭제되는 것을 방해하거나 사용자에게 설치된 사실을 숨기기 위한 목적으로 여러 스파이웨어에서 사용되기도 한다.

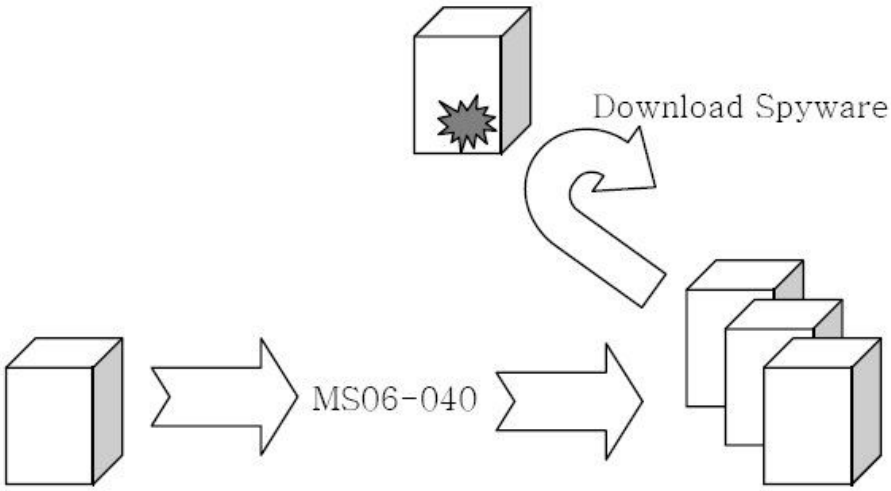


[그림 4-4] 스파이웨어 마이컴고의 유료결제 대화상자

► 온라인게임 계정 유출 스파이웨어의 피해

중국발 해킹으로 시작하는 온라인게임 계정 유출 스파이웨어의 설치는 사용자의 중요 정보를 해커에게 제공하는 위협 이외에도 설치 과정, 설치 된 이후에도 보안을 위협하는 여러 동작으로 인해 많은 피해를 입혔다.

다운로더 코게임(Win-Downloader/PWS.KorGame.48019)의 경우 IE 취약점을 공격하는 코드로 사용자 동의 없이 설치되며 다른 시스템에 확산하기 위하여 MS06-040 취약점을 공격하는 웜 기능을 수행한다. 이 외에도 ARP Spoofing 공격으로 인하여 전체 네트워크가 마비되거나 바이럿 바이러스(Win32/Virut) 바이킹 바이러스(Win32/Viking)와 같은 바이러스 감염 매개로 사용되기도 하였다.

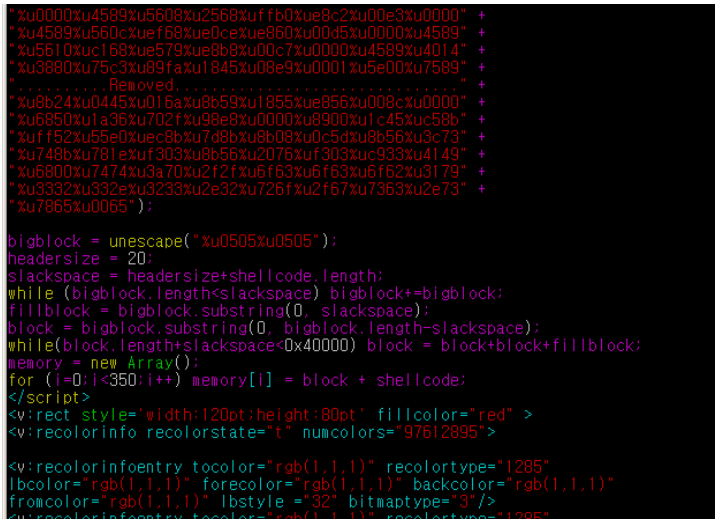


[그림 4-5] Win-Downloader/PWS.KorGame.48019 의 공격 개요

2007년 주요 취약점 이슈

► MS06-004 VML 취약점

VML 취약점은 1월9일 MS07-004 취약점 패치가 발표 되었고 얼마 지나지 않아 1월16일, 17일에 각각 공격코드가 공개되었다. 해당 취약점은 마이크로소프트사가 지원하는 VML(Vector Markup Language)컴포넌트 상에서 발생하는 Integer Overflow 취약점이다



[그림 4-6] MS07-004 취약점을 웹 사이트에 악용한 사례

► Sun Solaris 텔넷 인증 우회 취약점

지난 2월 12일 Sun 마이크로시스템사의 새로운 취약점 발표 소식을 듣고 많은 사용자들은 허탈함을 금치 못했을 것이다. 그 이유는 해당 취약점이 별다른 공격기술이나 공격도구 없이 단지 특정 옵션을 사용하는 것만으로 매우 치명적인 결과를 초래할 수 있는 단순한 취약점 이었기 때문이다. 이 취약점은 1990년대 중반에 발표된 rsh 취약점과 매우 유사하다

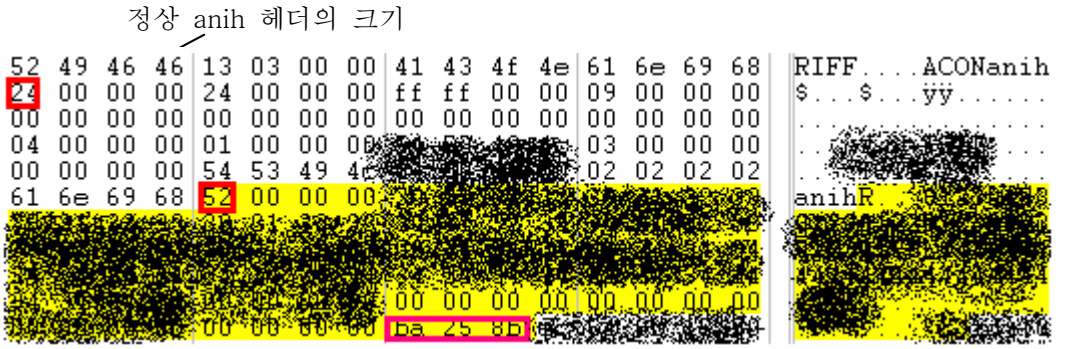
```
SECURE# telnet -l "-froot" <telnet server ip>
Trying <client_ip>...
Connected to <client_ip>.
Escape character is '^]':
#
```

► MS07-017 Animated Cursor Handling(ANI 파일) 취약점

2007년 3월 user32.dll 파일의 취약점을 이용한 제로데이 공격이 출현하였다. 이 취약점은

2005년에 발견된 취약점(MS05-002)과 동일한 곳에서 발견되어 결과적으로 과거 MS사의 패치가 잘못되었다는 것을 보여주었다.

MS05-002는 힙 오버플러우인 반면에, MS07-017은 사용자가 조작된 Animated Cursor 파일을 특정 어플리케이션에 로드할 경우 취약점이 존재하는 곳에서 버퍼 오버플로우가 발생하며 그 결과로 공격자는 임의의 코드를 사용자의 시스템에서 실행할 수 있다. 취약점이 존재하는 곳은 User32.dll의 LoadAniIcon 함수로 이 함수의 역할은 Animated Cursor 파일의 헤더를 파싱하고 해당 데이터를 처리하는 것이며 이 함수는 Animated File 을 로드할 때 실행된다.



[그림 4-7]. 조작된 animated cursor 파일 덤프

► MS07-029 MS DNS SRV 취약점의 악성코드화

MS07-029 취약점은 원격에서 코드를 실행할 수 있는 취약점이 존재하는 것으로, 관리자 권한으로 로그인 되어 있는 경우 공격자는 시스템을 제어할 수 있는 모든 권한을 얻을 수 있게 된다.
이 취약점은 DNS 서버 서비스에 바인딩 되어 있는 RPC 에 조작된 공격 패킷을 보내 임의의 코드를 실행할 수 있다. RPC 의 UUID "50abc2a4-574d-40b3-9d66-ee4fd5fba076" 의 DnssrvQuery 값(0x01 DnssrvQuery)을 설정하여 악용하는 것이다. 공개된 개념증명코드(Proof of Concept)에서는 포트바인딩 쉘코드(PortBind Shellcode)를 사용하여 MS DNS RPC서비스 취약점을 이용한 시스템 권한 획득이 가능함을 보여주었다. 또한, Windows 2000 서버의 DNS 서버를 공격하는 악성코드가 발견되기도 하여 그 위협의 심각성을 짐작케 하였다. (V3진단명: Win32/IRCBot.worm.199680.I)

► 마이크로소프트 오피스 취약점의 꾸준한 증가

오피스 프로그램은 대다수 사용자가 이용하는 응용 프로그램으로 스프레드 시트 프로그램인

엑셀(Excel),문서 작성/편집 프로그램인 워드(Word), 프리젠테이션 관련 프로그램인 파워포인트(PowerPoint), 데이터 베이스 관련 프로그램인(Access), 이메일 프로그램인 아웃룩(OutLook)등으로 구성되어져 있다.

MS 오피스 취약점은 이러한 오피스 프로그램 및 오피스 라이브러리에 버그(Bug)가 존재하는 것을 말한다.

사용자가 악의적으로 조작된 오피스 파일(File)을 읽는 과정에서, 사용자가 관리자 권한으로 로그인 되어 있는 경우 취약점을 악용한 공격자는 프로그램의 설치, 보기, 변경, 데이터 삭제 등과 같은 권한을 얻게 되어 시스템을 완전히 제어할 수 있게 된다. 하지만, 취약점을 이용한 공격에 성공하기 위해서는 사용자의 개입이 필요하다.

MS 오피스 프로그램이 기업의 많은 컴퓨터에 설치되어 있기 때문에, 위험의 심각도가 있다고 볼 수 있다.

MS Office는 다수의 애플리케이션으로부터 생성된 데이터를 하나의 파일에 포함시킬 수 있는 Compound Document File Format 을 갖는다. Compound Document file은 실제 파일 시스템과 유사한데, 데이터를 다수의 Stream(파일 개념)으로 분할하여 Storage(디렉토리 개념) 속에 나누어 저장한다. 다시 Stream은 작은 데이터 블록 단위인 Sector로 구분되는 데 반드시 연속되는 Sector들이 하나의 Stream을 이루는 것은 아니며 Stream의 구성은 Sector들의 연결 Chain(SID chain)으로 표현된다.

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

HEADER
SECTOR 0
SECTOR 1
SECTOR 2
SECTOR 3
SECTOR 4
SECTOR 5
SECTOR 6
⋮

일반적으로 MS 오피스의 취약점은 특정 오브젝트의 특정 필드에서 오버플로우 버그가 발생하거나, 오피스 공통 라이브러리에서 취약점이 발견되는 경우도 존재한다. 2007년 에 발표된

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

MS 오피스 취약점은 2007년 시큐리티 통계를 참고하도록 하자. MS 오피스 취약점은 2006년 상반기부터 본격적으로 나타나기 시작하였다. 2007년 MS 사의 보안 패치 취약점은 전체 대비 17%이다. 취약점을 이용한 공격에는 조작된 파일을 특정/불특정 사용자에게 메일 또는 웹으로 전달하여 사용자가 해당 오피스 파일(File) 읽는 경우 임의의 코드 또는 악성코드를 실행할 수 있게 된다.

악성코드는 V3 진단명으로 PP97M/Exploit-PPDropper, X97M/Exploit.Excel, X97M/Exploit.ControlExcel, W97M/Exploit-OleData 등이 존재하고, 오피스 문서 내부 코드에 트로잔(Trojan) 및 다운로더(Downloader)등이 포함되어져 있기도 하며, 최근에는 특정 오피스 취약점을 공격하는 자동 제작기가 중국에서 발견되기도 하였다.

외국뿐만 아니라 국내에서도 MS 오피스 취약점을 이용한 공격이 발생하고 있는데, 이러한 공격은 주로 특정 목적을 가지고 수행되는 것으로 보이며, 개인 및 기업등의 민감한 정보를 노리는 것으로 파악된다. MS 오피스 취약점은 제로 데이(Zero-Day) 공격에도 자주 사용이 되고 있기 때문에, 주의가 필요하다.

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

► 사회공학 기법인 전화사기(보이스 피싱) 극성

인간의 행동은 예측 가능하지 않기 때문에 사회의 절차나 제도, 사람의 심리등을 악용하여, 필요한 정보를 구하는 기법이 사회공학이다. 이러한 사회공학 기법을 이용한 보이스 피싱/전화사기가 극성을 보이고 있다.

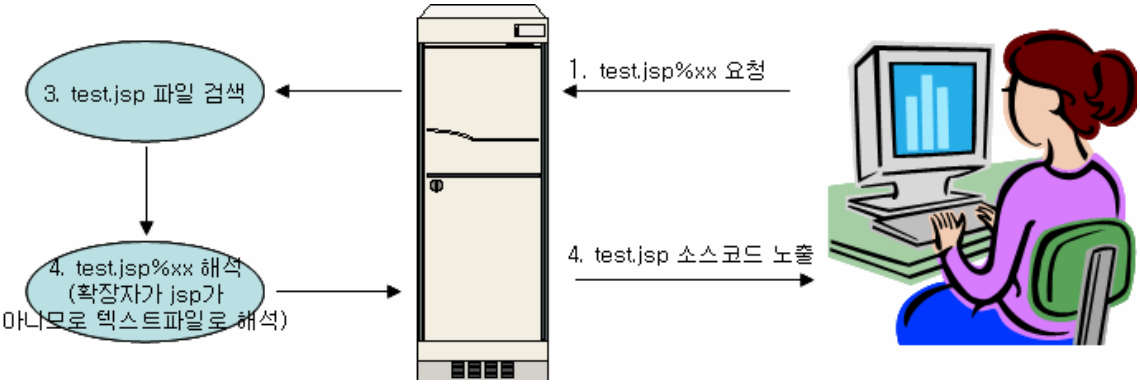
보이스 피싱/전화사기는 2006년 부터 꾸준하게 일어나고 있으나, 2007년에 들어서는 보다 교묘한 방법으로, 정부기관 및 기타 단체, 개인등을 사칭하여, 금품을 노리고 있다.

보이스 피싱/전화시기를 예방하기 위해서는 2007년 상반기에 금융감독원에서 발표한 “전화금융사기 피해를 막을 수 있는 8가지 수칙”을 참고하도록 하자.

- 전화로 개인정보 요구시 응하지 말 것
- "현금지급기로 세금 환급"도 사기
- 속아서 계좌이체 했다면 은행에 지급정지 신청
- 개인정보 알려줬다면 은행에 신고
- "나, 동창생인데.." 입금요구시 사실관계 확인
- 발신자 전화번호 확인해야
- ARS 사기전화 주의
- SMS 서비스 적극 이용

► 티맥스 미들웨어 제우스의 디렉토리 및 소스코드 노출 취약점

국가 사이버 안전센터 (NCSC)는 2007년 7월 16일 티맥스 소프트의 미들웨어인 제우스(JEUS)에서 디렉토리 파일 목록 및 JSP 소스코드가 노출되는 보안 취약점을 발표하였다. 제우스 미들웨어는 국내 많은 수의 정부기관과 금융기관이 사용하고 있고 소스코드 노출로 인한 제 2의 정보노출이 가능하다는 점에서 해당 취약점의 영향은 매우 크다고 할 수 있다



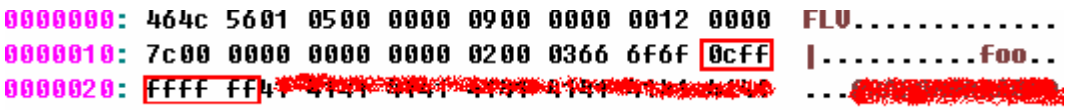
[그림 4-8] 제우스(JEUS) 보안 취약점

웹 어플리케이션에서 이와 같은 취약점이 발생하지 않도록 하기 위해서는 첫째, 어플리케이션의 모든 모듈의 문자열 처리 방법을 통일하고, 둘째 URL 인코딩 된 문자를 올바르게 필터링 하며 셋째, 펄과 같은 스크립트 언어를 사용할 경우 유저의 입력이 시스템 명령에 사용될 수 없도록 펄의 taint 모드와 같은 설정을 하도록 하는 것이 필요하다.

► 플래시 플레이어 취약점

2007년 7월 10일 플래시 플레이어가 가지고 있는 취약점이 발표되었다. 이 취약점은 플래시 플레이어가 사용하는 FLV 데이터 파일의 검증을 하지 못해 발생한다. 이 취약점은 웹 브라우저에서 사용가능한 플래시 플레이어의 특성상 불특정 다수의 사용자를 공격대상으로 할 수 있기 때문에 그 영향은 매우 크다고 할 수 있다.

일반적으로 FLV 파일은 파일헤더와 비디오, 오디오, 스크립트 데이터를 나타내는 일련의 FLV 태그로 구성된다. 다음 2개의 표는 각각 FLV 파일헤더와 태그 데이터를 나타낸 것이다. 모든 정수(integer) 데이터들은 빅엔디언(Big-Endian) 형식으로 저장되어 있다.



플래시 플레이어는 UCC 에서도 많이 사용되고 있고, 웹상에서 악성코드 배포에도 사용할 가능성이 많음으로 주의가 필요하며, 플래시 플레이어 취약점에 대한 보안 업데이트는 Adobe 사이트를 참고하면 된다.

► 은행 인터넷 뱅킹 문제점

2007년 하반기에 인터넷 뱅킹 보안 문제가 KBS 뉴스 방영 이후 수면위로 떠올랐다. 이 문제점은 게임 해킹 프로그램과 거의 유사하게 동작하며, 이 공격에 의한 피해는 인터넷 뱅킹을 이용하여 계좌이체를 할 경우 자신의 의도와는 다르게 공격자나 다른 계좌 이용자에게 금액을 이체 시킬 수 있다. 또한 보내고자 하는 이체 금액도 공격자 마음대로 조작이 가능한 것으로 나타났다. 아직까지 이를 이용한 악성코드등은 없으나 사용자의 각별한 주의가 요구된다.

인터넷 뱅킹 보안 문제는 이용자가 인터넷 뱅킹을 통해 계좌 이체를 할 경우 입력한 데이터는 메모리상에 남게 된다. 메모리상에 존재하는 데이터를 조작하여, 공격자 의도대로 자신의 계좌로 수정하거나 금액을 바꿀 수 있으며, 기타 보안 정보를 획득할 수 있다.

이를 대처하기 위한 방법으로는 인터넷 뱅킹을 사용하였을 경우 꼭 다시 한번 이체결과등을 확인하는 습관을 기르며, 윈도우 보안 업데이트 및 백신을 설치하여 악의적으로 설치된 프로그램을 치료하고 자주 업데이트하는 것이 좋다.

► Microsoft XML Core Services의 취약점으로 인한 원격 코드 실행 문제점 (MS07-042)

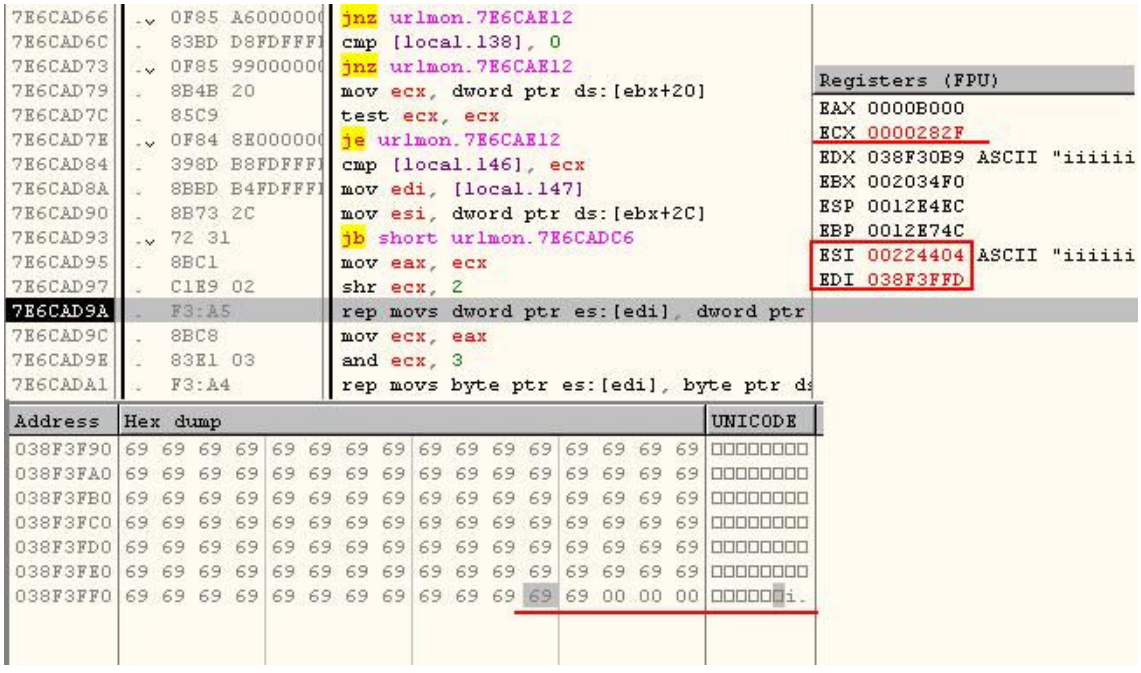
Microsoft XML Core Services(MSXML)는 JScript, Visual Basic Scripting Edition(VBScript), Microsoft Visual Studio 6.0을 사용하여 XML 1.0 표준을 준수하는 다른 응용 프로그램과 상호 운용성을 제공하는 XML 기반 응용 프로그램을 개발할 수 있도록 제공해 준다. 이러한 XML Core Services의 보안 취약점을 통해 공격자는 Internet Explorer(IE)를 통해 특수하게 조작된 웹사이트를 만들어 불특정 사용자를 공격할 수 있다. 공격자는 이로 인해 로그인 된 사용자의 모든 권한을 획득 할 수 있다.

이 취약점이 발생하는 substringData()는 offset값부터 시작하여 특정 길이만큼의 컨텐츠속 문자열을 반환해주는 함수로서, 해당 취약점은 substringdata()함수의 입력 파라미터를 사용하여 동적으로 할당할 메모리 공간을 계산하는 과정에서 발생하는 Integer Overflow가 그 원인이 된다. 이로 인하여 Memory Corruption이 발생하며 애플리케이션의 크래쉬(crash) 현상을 야기할 수 있다.

```
5d45f14c 8d141e          lea     edx,[esi+ebx]    ds:0023:80000000=????????
5d45f14f 3bd1            cmp     edx,ecx
5d45f151 7e07            jle msxml3!W3CDOMWrapper::substringData+0xbd (5d45f15a) [br=1]
```

► MS07-050 벡터 표시 언어의 취약점으로 인한 원격 코드 실행 문제점

Microsoft Windows에 구현된 VML(벡터 표시 언어)에 원격 코드 실행 취약점이 존재한다. VML(벡터 표시 언어)은 업무용 사용자 및 그래픽 디자인 전문가의 요구를 모두 만족하도록 웹에서 고화질 벡터 그래픽을 교환, 편집, 배포하는 XML 기반 형식이다. 이 취약점은 압축된 HTTP response 데이터를 받을 때 VML(vgx.dll)을 처리하는 과정에서 integer underflow를 일으키게 된다. 공격자는 특수하게 조작된 웹 페이지나 HTML 전자 메일을 구성하여 이러한 취약점을 악용할 수 있다.



► MS07-046 GDI의 취약점으로 인한 원격 코드 실행 문제점

그래픽 렌더링 엔진 GDI32.DLL 에서 특수하게 조작된 이미지를 처리하는 방식에 원격 코드 실행 취약점이 존재한다. 그리고, 이 취약점을 악용한 공격자는 프로그램의 설치, 보기, 변경,

데이터 삭제등과 같은 권한을 얻게 되어 시스템을 완전히 제어할 수 있다.

공격자는 특수하게 조작된 WMF을 파일을 전자 메일에 첨부하여 발송하거나 웹을 통하여 배포한 후 사용자가 해당 파일을 열게 되면 원격 코드가 실행되는등의 비정상적인 동작을 유발할 수 있다.

```
typedef struct _WindowsMetaHeader
{
  WORD  FileType;       /*Type of metafile (0=memory, 1=disk) */
  WORD  HeaderSize;     /* Size of header in WORDS (always 9) */
  WORD  Version;        /* Version of Microsoft Windows used */
  DWORD FileSize;       /* Total size of the metafile in WORDs */
  WORD  NumOfObjects;   /* Number of objects in the file  */
  DWORD MaxRecordSize;  /* The size of largest record in WORDs */
  WORD  NumOfParams;    /* Not Used (always 0) */
} WMFHEAD;

typedef struct _StandardMetaRecord
{
    DWORD Size;          /* Total size of the record in WORDs */
    WORD  Function;      /* Function number (defined in WINGDI.H) */
    WORD  Parameters[];  /* Parameter values passed to function  */
} WMFRECORD;
```

< Windows Meta File 파일 포맷 >

```
; START OF FUNCTION CHUNK FOR _AttemptWrite@12

loc_77E43726:
mov     ecx, [ebx+0Ch]
add     ecx, [ebp+arg_4]
mov     eax, [ebx+8]
cmp     ecx, eax
jbe     short loc_77E43757
```

Integer Overflow(정수 오버플로우) 발생 코드

► GOM 플레이어 원격 코드 실행 취약점

GOM 플레이어는 국내에서 가장 대중적으로 애용되고 있는 멀티미디어 플레이어이다. 이번 GOM 플레이어에서 발견된 취약점은 GOM 웹 컨트롤러(GomWeb3.dll)의 OpenURL() 메쏘드의 첫번째 인자인 sURL에서 버퍼의 크키를 체크 하지 않아서, 발생하는 스택 기반의 버퍼 오버플로우이다.

해당 취약점은 웹을 통해서 도용될 수 있으며 인터넷 익스플로러가 크래쉬(Crash) 되거나 공격자가 원하는 코드를 실행할 수 있다

GomManager Class

InprocServer32 : C:₩Program Files₩GRETECH₩GomPlayer₩GomWeb3.dll

ProgID : GomWebCtrl.GomManager.1

CLSID : {DC07C721-79E0-4BD4-A89F-C90871946A31}

OpenURL() 메쏘드가 호출되면 메쏘드에 넘겨진 URL 문자열은 **"/gm_embedding "** 문자열과 재조합된다. 이를 처리하기 위해서 함수 내에서 아래와 같이 로컬 스택에 0x208(520) 바이트 공간을 확보한다. 차례로 확보된 로컬 스택에 kernel32.lstrcatA 함수를 호출하여 "gm_embedding "과 전달된 URL을 복사하게 된다.

그러나, 이때 사용자 입력으로 전달된 URL의 길이가 "gm_embedding "(14)문자열을 제외하고 506 바이트 이상인 경우, 함수 내에서는 길이에 대한 유효성 검사를 전혀 수행하지 않기 때문에 본래의 로컬 스택 공간(520)을 초과하여 덮어쓰는 버퍼 오버플로우가 발생한다.

► DDoS 공격을 통한 서비스 거부 공격

"OO시까지 OO원을 입금하라. 그렇지 않으면..." 마치 영화 속 유괴범의 금품 요구 대사 같지만 이제 이러한 돈을 목적으로 하는 범죄는 비단 현실만의 얘기가 아닌 온라인 상에서도 자행되고 있다. 9월 말 아이템 베이, 아이템 매니아, 아이템 플포와 같은 온라인 게임 아이템 거래 사이트가 동시에 접속 불능이 되는 사태가 일어났다. 해당 사들은 접속 과다로 인한 통신장애라고 사유를 급히 밝혔지만, 실상 그 뒤에 돈을 요구하는 UDP Flooding DDoS 공격으로 인한 장애였던 것으로 밝혀졌다.

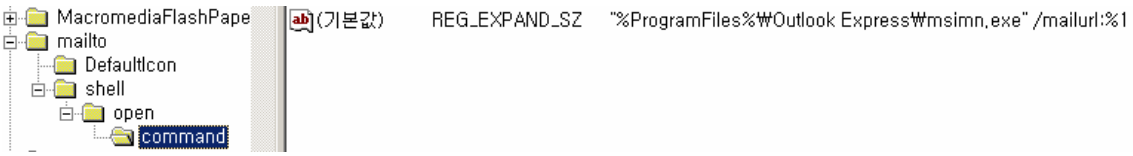
UDP Flooding은 다양한 DoS(Denial of Service) 공격의 일종으로 대량의 UDP 패킷을 이용하여 대상 호스트의 네트워크 자원을 소모함으로써 올바른 서비스를 중단시키는 공격을 말한다. DDoS 공격은 일부 취약한 호스트를 해킹하여 '좀비' 시스템으로 만들고, 이를 통해서 대량의 트래픽을 발생시킨다. 당시 공격에서도 최대 17G 정도라는 엄청난 양의 트래픽이 발

생되었고, 일반적인 장비로는 이를 막아낸다는 것이 불가능하다. 2007년 하반기에 발생한 사건뿐만 아니라 DDoS 공격은 성인,도박,화상 채팅 사이트 등 음성적인 서비스를 제공하는 업체를 대상으로 빈번하게 자행되고 있으나, 신고를 통해 사건을 조치하기 보다는 원하는 요구를 그대로 들어주고 있는 실정이다. 현재 DDoS 공격 패킷은 정상적인 트래픽 패킷과 구별하는 것이 쉽지 않지만 대응책으로는 Source Tracking, Packer Per Rate 설정, Syn Cookie/Proxy, Load Balancing, QoS 등의 방법을 이용하여,어느정도 방어가 가능하다. 그러나, 이러한 경우에도, 트래픽이 엄청날 경우 해당 ISP 와 더불어서 조치를 취하는 것이 효과적인 방법이다.

► MS URL 핸들링 취약점 (MS07-061)

지난 10월 초 마이크로소프트사는 Windows Server 2003과 Windows XP 상의 인터넷 익스플로러 7 버전에 대한 보안 권고문(Security Advisory 943521)[1]을 발표하였다. 해당 권고문은 다수의 사람들에게는 "PDF 제로데이 취약점"으로 더 많이 알려진 URL 핸들링 코드 실행 취약점에 대한 권고사항을 담고 있다. 이후 11월 달에 MS07-061 패치로 발표되었다.

Windows Shell은 "http","ftp", "mailto" 와 같은 URL 프로토콜 핸들러(Handler)를 사전에 등록하고, 사용자가 링크를 클릭할 때 해당 애플리케이션을 통해 자동으로 수행되도록 지원한다.



그러나, % 문자를 포함하는 URI의 경우 등록된 애플리케이션을 실행하지 않고, URI를 경로로 삼아 새로운 프로세스를 실행한다. 따라서, 다음과 같이 임의의 명령을 포함하는 URI를 웹 페이지에 삽입한다면, 이를 클릭하는 사용자들은 시스템에서 자연스럽게 계산기 프로그램을 수행하게 되는 것이다.

```
mailto:test%../../../../windows/system32/calc.exe".cmd
```

해당 취약점은 Adobe Acrobat Reader(PDF) 뿐만 아니라 Firefox, Outlook Express와 같이 스크립트를 수행할 수 있는 많은 다른 애플리케이션을 통해서도 이용될 수 있으며, 이미 공격에 응용된 PDF 파일 형태의 다운로더 악성코드가 신고 접수되었다.

1. 조작된 URI 에서 프로토콜을 확인한다. URI 에는 "blahblah%" 와 같은 문자열이 포함되어

[1] http://www.microsoft.com/technet/security/advisory/943521.mspx

있으므로 ShellExecute 함수는 해당 URI 문자열에서 프로토콜 이름을 얻어내는데 실패한다.

2. ShellExecute 함수는 URI 문자열을 파일이름으로 간주하여 파일 확장자를 추출한다. URI 문자열의 끝에는 .cmd 가 존재하므로 ShellExecute 함수는 파일 확장자를 .cmd 로 간주한다.
3. HKEY_CLASSES_ROOTW.cmd 레지스트리를 읽는다
4. CLASSES_ROOTWcmdfileWshellWopenWcommand 레지스트리를 읽는다. 이 때 아규먼트 치환에 사용되는 문자열을 "%1" %* 이다. [그림 5]
5. "%1"을 URI로 치환한다. 따라서 최종 인자는 "blahblah%/calc.exe".cmd" ; %*가 된다.
6. 치환된 문자열을 파라미터로 사용하여 CreateProcess 함수를 호출한다.
7. calc.exe(계산기 프로그램)이 실행된다.

[표 4-1] ShellExecute 함수가 조작된 URI를 처리하는 과정

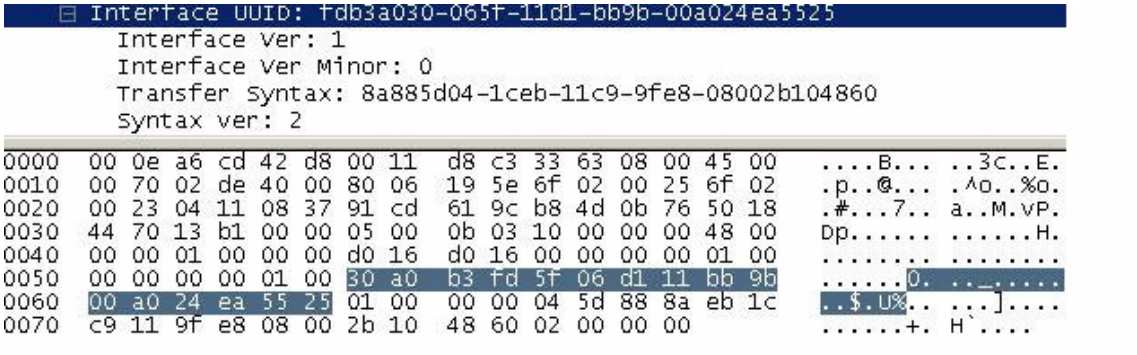
► Message Queuing의 취약점으로 인한 원격 코드 실행 문제점(MS07-065)

Microsoft Message Queuing은 다른 시간대에 실행 중인 응용 프로그램이 일시적으로 오프라인 상태일 수 있는 이기종 네트워크 및 시스템과 통신할 수 있는 기능이다. 또한 Message Queuing은 보장된 메시지 전달, 효율적인 라우팅, 보안 및 우선 순위 기반 메시징을 제공한다. 참고로 MSMQ 서비스는 TCP 2103, TCP 2105, TCP 2107 포트에서 기본적으로 동작한다.

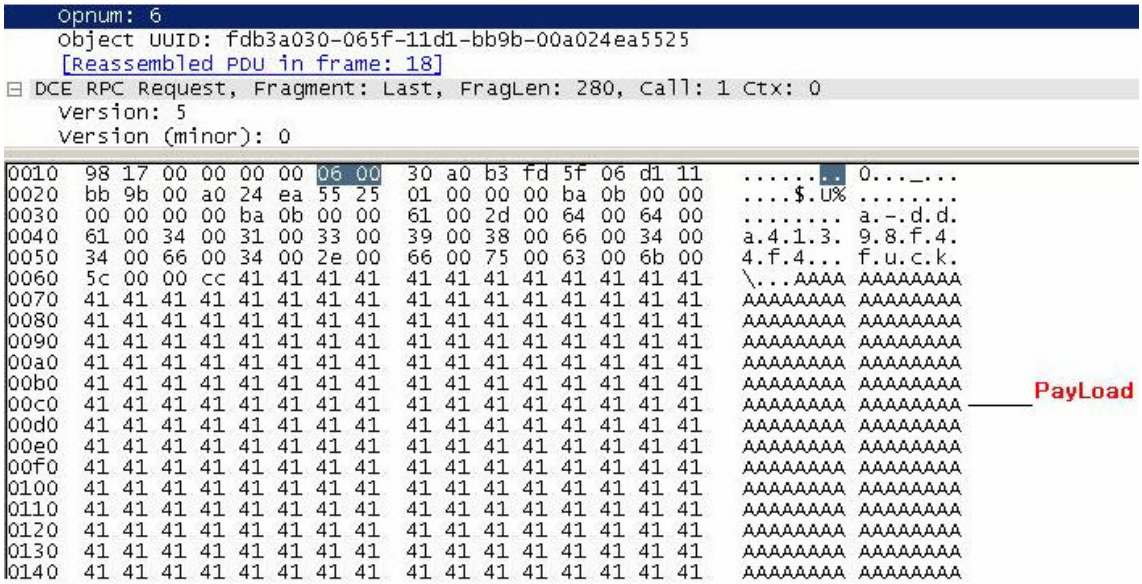
MS07-065 취약점은 원격에서 코드를 실행할 수 있는 취약점이 존재하는 것으로 공격자는 관리자 권한을 획득할 수가 있으며, 프로그램의 설치, 보기, 변경, 데이터 삭제등 해당 시스템을 완전히 제어할 수 있게 된다. 또한 이 취약점을 통해 60초 카운트에 해당하는 서비스 거부가 발생을 할 수도 있다.

Message Queuing 서비스에서 (mqqm.dll)에서 제공하는 RPC Call 중에서 취약점을 가지고 있는 Call 은 QMCreateObjectInternal 등이다. mqqm.dll의 관련 Inferface 및 OPcode 는 아래표와 같다.

Interface (srvsvc)	Operation number	Operation name
Fdb3a030-065f-11d1-bb9b-0a024ea5525	0x06	QMCreateObjectInternal



실질적으로 취약점이 발생하는 함수는 NetBiosName 관련 함수임으로, 이름 필드에 긴 문자열이 대입되면서 아래 패킷과 같은 버퍼 오버플러우가 발생하게 된다.



MS07-065 취약점의 주된 공격대상은 Windows 2000 서버군 제품들임으로, 특히 해당 서비스를 운영중인 서버들의 보안관리가 필요하다.

(2) 2008년 예측

2008년에는 ▶가상화 기술 이용 등 악성코드 은폐 기법의 고도화 ▶웹 해킹 증가 ▶사이버 블랙 마켓의 활성화 ▶스파이웨어의 악성코드화 ▶애플리케이션 취약점 공격 증가 ▶이동저장장치 노린 악성코드 기승 ▶UCC, SNS 등 웹2.0 서비스 통한 악성코드 전파 가속화 등의 위험이 예상된다.

(1) 가상화 기술 이용 등 악성코드 은폐 기법의 고도화: 악성코드 제작자는 악성코드를 은폐하기 위해 다양한 방법을 사용한다. 그 중 향후에 등장할 기법으로 가상화 기술(실제로 지니고 있는 물리 구조에 적당한 계층을 개입시킴으로써 더 일관성 있고 편리한 논리 구조를 갖게 하는 것)을 들 수 있다. 가상화 기술을 이용한 악성코드는 아직 나오지 않았지만 2005년에 개념을 증명할 정도의 형태로 루트킷(root kit)이 나온 바 있다. 당시에는 탐지가 어렵지 않고 동작에 불확실성이 있어 실제로 피해가 발생하지는 않았다. 하지만 자체 가상 머신을 가지고 해당 가상 머신에서만 동작하는 코드를 구현해 실행 압축을 해제하기 어렵게 만든 악성코드가 존재한다. 이런 악성코드는 보안 제품을 무력화할 수 있다. 2008년에는 이런 기법을 악용한 은폐 및 자기보호, 탐지하기 어렵게 더욱 고도화한 악성코드가 급증할 것으로 예상된다.

(2) 웹 해킹 증가: 웹 애플리케이션의 취약점을 이용해 해킹하거나 DDoS(Distributed Denial of Service; 분산서비스거부) 공격을 하는 일이 더욱 증가할 것으로 전망된다. 많은 웹사이트가 보안에 대해 고려되지 않고 개발되어 적용되기 때문에 보안에 취약한 상태여서 공격에 무방비 상태로 당할 가능성이 높다. 이를 통해 악성코드와 스파이웨어를 유포하거나 해당 웹 페이지로 유도하는 일이 전년에 이어 지속 발생할 것으로 보인다. 또한 DDoS 공격은 금전을 요구하기 위한 수단으로 이용되는 일이 더욱 많아질 것으로 예측된다.

(3) 사이버 블랙 마켓의 활성화: 가상의 재화를 현금으로 교환하는 '사이버 블랙 마켓'의 규모가 커질 것으로 전망된다. 여기서는 신상 정보 및 신용카드 정보, 온라인 게임 계정 등이 거래되고 있으며, 악성코드가 판매되는가 하면 피싱, DDoS 공격 등을 대가를 받고 해주는 것으로 알려져 있다. 이에 따라 여기서 거래 가치가 높은 악성코드나 해킹이 더욱 기승을 부릴 것으로 보인다. 또한 금전적 이익을 위해 불특정다수를 공격하는 것보다 특정 타깃을 노리는 국지적 공격이 증가할 것이다.

(4) 스파이웨어의 악성코드화: 국내에서 제작되는 스파이웨어 중 운영체제나 애플리케이션의 취약점을 직접 공격하거나 루트킷을 사용해 자신이 설치 또는 실행 중이라는 사실을 숨기는 프로그램은 많지 않았다. 그러나 앞으로는 스파이웨어를 통한 이익을 극대화하기 위해 취약점 공격, 보안 프로그램 무력화, 자기 은폐, 파일 감염 등 악성코드에 사용되는 기법이 많이 사용될 것으로 예상된다.

(5) 애플리케이션 취약점 공격 증가: 현재 MS사의 운영체제나 애플리케이션 취약점을 노리는 공격이 가장 비중이 높지만 그 수는 점차 줄어드는 추세이다. 반면 PDF, 애플 맥 OS X, 액티브X, 멀티미디어 플레이어, 이미지 뷰어, 메신저 등 사용자들이 많이 사용하는 애플리케이

션들에 대한 공격이 증가하고 있다. 이런 흐름은 2008년에도 이어질 것으로 예측된다.

(6) 이동저장장치 노린 악성코드 기승: 지난해에 이어 올해도 이동저장장치(USB 플래시 메모리, 이동식 하드디스크)를 통해 전파되는 악성코드가 기승을 부릴 것으로 전망된다. 특히 보안 USB가 등장함에 따라 이를 뚫거나 중요 정보를 빼내려는 악성코드가 등장할 가능성이 높다.

(7) UCC, SNS 등 웹2.0 서비스 통한 악성코드 전파 가속화: UCC가 악성코드 또는 스파이웨어를 배포하는 또 하나의 채널이 되고 있다. 동영상 플레이어의 일부인 양 설치를 유도하는 스파이웨어가 자주 발견되고 있으며 일반 동영상을 가장해 설치되는 스파이웨어도 적지 않은 실정이다. 이런 흐름은 2008년에도 지속될 것으로 보인다. 아울러 SNS가 주목 받기 시작하자 이를 이용한 악성코드가 기승을 부릴 것으로 전망된다. 이미 2006년에 미국 마이스페이스에서 프로필을 보기만 하면 친구 리스트에 특정인이 추가되도록 한 악성코드가 제작된 바 있다. 또한 1인 미디어인 블로그에 악성코드를 내려받게 유도하는 주소를 링크해놓는 일도 증가할 것으로 보인다.

한편, 향후 2~3년 후에 현실화할 이슈로는 VoIP를 겨냥한 DDoS 공격 및 도감청 본격화, 무선 인터넷 기기를 겨냥한 해킹 증가, 모바일 플랫폼인 안드로이드를 겨냥한 보안 위협 등장 등이 예측된다.

* VoIP 겨냥한 DDoS 공격 및 도감청 본격화: 2008년 1월 VoIP(Voice over Internet Protocol; 인터넷전화) 번호이동제의 시행으로 가입자가 증가할 것으로 예상된다. VoIP는 기존 공중전화망(PSTN; Public Switched Telephone Network) 대신 인터넷으로 음성 통화 서비스를 제공하기 때문에 보안 측면에서 위험성이 높다. VoIP 서비스의 서버를 DDoS 공격해 서비스를 중단하거나 서버의 데이터를 위변조할 가능성이 있다. 또한 전송되는 데이터를 도감청할 수 있으며 스팸의 또 다른 채널로 악용할 가능성도 매우 크다.

* 무선 인터넷 기기 겨냥한 해킹 증가: 현재 출시되는 대부분의 랩탑과 모바일 기기는 물론 PSP, 휴대용 게임기에는 무선 인터넷에 접속할 수 있는 기능이 들어있다. 그러나 이들의 접속을 허용하는 AP(Access Point)가 보안 설정을 하지 않은 경우가 많으며, 보안 설정을 했어도 WEP(Wired Equivalent Privacy; 유선 랜에서 제공하는 것과 유사한 수준의 보안을 무선 랜에 제공하기 위한 보안 프로토콜) 등과 같은 암호화는 쉽게 암호키를 알아낼 수 있다. 이런 네트워크에 접속하면 해당 네트워크에 접속한 컴퓨터의 각종 자료를 열람할 수 있을 뿐 아니라 ARP 스푸핑(Address Resolution Protocol Spoofing; 동일 네트워크에 존재하는 공격 대상 PC의 IP 주소를 공격자 자신의 랜카드 주소와 연결해 다른 PC에 전달돼야 하는 정보를 가로채는 공격) 또한 가능하다. 따라서 무선 인터넷 사용이 대중화함에 따라 보안 위협은 더욱 증가할 것으로 예상된다.

* 모바일 플랫폼 안드로이드 겨냥 보안 위협 등장: 구글을 비롯해 약 30여 개 업체가 연합해 만든 오픈 모바일 플랫폼인 안드로이드의 소프트웨어 개발 키트가 공개됐다. 이 플랫폼을

이용하면 모바일 기기를 제작할 때 제조 원가 절감을 비롯해 여러 이점이 있어 많은 업체들이 이를 적용할 것으로 예상된다. 아직 이 플랫폼을 적용한 제품이 출시되지는 않았지만, 안드로이드는 거의 모든 기능을 API(Application Programming Interface; 응용 프로그램 인터페이스)로 제공하고 있어 현재로선 악용될 소지가 매우 높다.

위에서 언급된 주요 예측에 대하여 몇가지 상세하게 살펴보면 아래와 같다.

- 악성코드의 고도화

악성코드가 지능적이고 더욱 복잡해졌다라는 얘기는 오래 전부터 있어 왔다. 그러나 앞으로는 악성코드의 고도화는 보안 제품의 향상된 날카로운 성능으로 말미암아 더욱 고도화 되는 추세이다.

즉, 진단기법의 향상은 악성코드 제작자들로 하여금 새로운 도전과제로 받아들여지며 역으로 이를 분석하여 진단기법을 회피하거나 무력화하는 시도는 더욱 고도화된 악성코드의 탄생을 의미 한다. 과거에는 안티 바이러스 기술이 악성코드 제작기법을 따라가면서 이를 분석, 방어 하는 것 이였다면 현재는 그 반대라 할 수 있겠다. 그들은 철처히 안티 바이러스 제품을 우회하고 무력화 한다. 그렇다고 해서 안티 바이러스 제품의 프로세스를 종료하거나 파일을 삭제 하지는 않는다. 이러한 방법은 오히려 고전이 되어 버렸다. 정상적으로 동작하는 것처럼 보이지만 안티 바이러스의 기능은 중지 되어 있기 때문에 사용자는 이를 알아채기 매우 어렵다.

또한 윈도우 파일 보호 기능을 기존과 전혀 다르게 우회하면서 시스템 파일을 악성코드로 변경하는 기법이 대중화 될 것으로 보인다. 저수준에 동작하기에 이를 탐지하기 위해서는 부단한 연구가 동반되어야 한다.

요즘 유행하는 안티 바이러스 제품의 행위기반 진단 역시 앞으로는 난항이 예상 된다. 정상행위와 악성행위를 교묘히 섞어 악의적인 행동을 탐지하지 못하게 하거나 안티 바이러스 제품으로 하여금 오탐을 극대화 하려는 시도가 예상 된다.

끝으로 주로 상용 파일 보호 제품에서 선보였던 가상화 기술이 악성코드 제작자들의 실행압축에서도 사용 될 여지가 많아 보인다. 이미 이러한 상용 제품을 크랙하여 악성코드 자신을 탐지하기 어렵도록 하는 유형은 많지만 이는 해당 제품을 단지 이용한 것에 불과하다. 따라서 향후에는 악성코드 자체에 가상화 기술을 적용하여 핵심 코드 부분을 분석하지 못하도록 방해하는 형태도 예상 된다. 또한 허니팟이나 자동분석 시스템을 공격하기 위하여 가상머신을 탐지하도록 설계된 악성코드의 대거 등장도 예상해 봄직 하다.

위해서 열거한 기법들은 이제 까지는 어려운 대상이 아닌 악성코드 마져도 모방 하고 있기 때문에 2008년에는 은폐 및 자기보호, 탐지 하기 어려운 더욱 고도화된 악성코드들의 출현이 잦아 질 것으로 보인다.

- 웹 사이트 공격 지속적인 증가

2007년 발표된 취약점중 Internet Explorer를 사용해 악성 코드를 배포하는데 사용된 주요 취약점은 MS07-007과 MS07-017 총 2개이다. MS07-007 취약점의 경우 일부 플랫폼에만 적용가능한 이유등으로 악성코드 배포를 위해 거의 사용되지 못했던 데 반해 MS07-017의 경우 모든 플랫 폼에 적용가능하고 취약점을 이용한 악성 코드 배포도 매우 쉽기 때문에 현재 가장 큰 비중을 차지 하고 있다.

실제로 2007년 악성코드를 배포하기 위해 사용되는 취약점 별 비율을 살펴보면 MS07-017 취약점이 88/245로 전체의 약 36%이상을 차지하고 있다. 따라서 2008년에도 Internet Explorer와 관련한 새로운 취약점이 발표되기 전까지는 주로 사용되는 취약점은 MS07-017 취약점이 될 것으로 전망된다. 또한 2007년 후반기부터 점점 대중적으로 널리 사용되는 ActiveX 객체의 취약점을 이용한 악성 페이지도 조금씩 발견되고 있다. 그동안 공격자가 공격한 취약점은 윈도우 운영체제나 IE에 집중되었으나 ActiveX객체가 많이 쓰이고 있는 국내 웹 사용환경의 특성상 ActviveX객체의 취약점을 이용한 사례도 간간히 발견되고 있다.

Mpack이나 Icepack등 웹 익스플로잇 툴킷이 대중화되면서 이를 이용한 침해사고의 사례도 조금씩 발견되고 있다. 웹 익스플로잇 툴킷을 사용하면 손쉽게 악성 웹 페이지 제작이 가능할 뿐만 아니라 AV 제품의 진단을 피하기 위한 고도화된 알고리즘을 사용할 수 있기 때문에 이를 이용한 공격코드 또한 점점 증가할 것으로 전망된다.

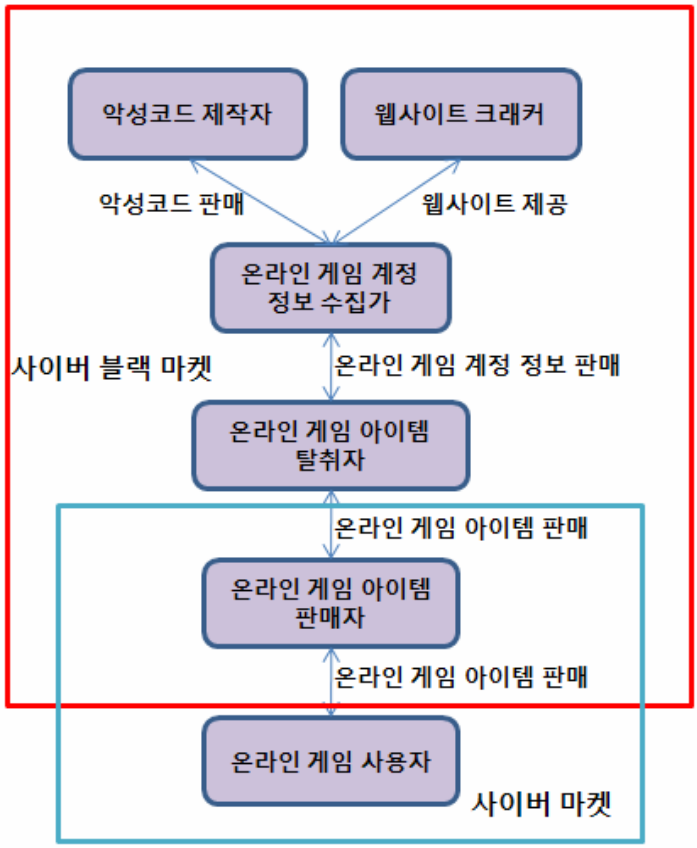
웹사이트 공격은 인터넷의 필수인 웹(Web)사이트를 공격하여, 수많은 사용자가 피해를 볼 수 있고, 방화벽을 우회할 수 있기 때문에, 방지책으로는 웹 서버 보안 패치 및 웹 어플리케이션의 보안 코딩 (Secure Coding)이 필요하고, 일반 사용자들은 해당 시스템의 보안 패치가 필수적이다. 이러한 웹사이트 기반 공격은 2008년에도 지속적으로 증가하리라 예상된다.

- 사이버 블랙 마켓의 활성화

2005년 여름을 즈음하여 중국에서 제작된 것으로 추정되는 온라인 게임 계정 정보를 탈취하는 악성코드가 한국에서 급증하기 시작하였다. 이렇게 급증하게 된 주요한 원인에는 한국에서 제작된 온라인 게임 중 해당 게임에서 사용되는 아이템이 현금 거래가 가능하다는 것에서 비롯된 것으로 알려졌다.

실제 이렇게 악성코드에 의해 불법적으로 탈취된 온라인 게임의 아이템이 얼마나 많이 어떻게 거래되는지는 분명하게 알려져 있지 않았다. 그러나 최근 연구되어 발표되는 정보 보안 관련 논문들 중 일부에서는 가장 주요한 원인이 사이버 재화들이 불법적으로 거래되는 사이버 블랙 마켓이 급격하게 성장하였기 때문으로 이야기하고 있다. 특히 사이버 블랙 마켓이 가장 활성화된 국가로는 중국과 러시아를 지목하고 있는데 한국의 경우에는 중국에서 활성화된 사이버 블랙 마켓의 영향력이 크게 미친다고 볼 수 있다.

중국의 사이버 블랙 마켓에서 주요하게 거래되고 있는 것은 앞서 이야기한 바와 같이 온라인 게임 아이템들이다. 이 를 탈취하기 위해서 중국의 사이버 블랙 마켓은 크게 악성코드 제작자, 웹 사이트 크래커, 온라인 게임 계정 정보 수집가와 온라인 게임 아이템 탈취자의 4가지 역할을 가진 인력 또는 조직이 중심이 되어 활동하고 있다.

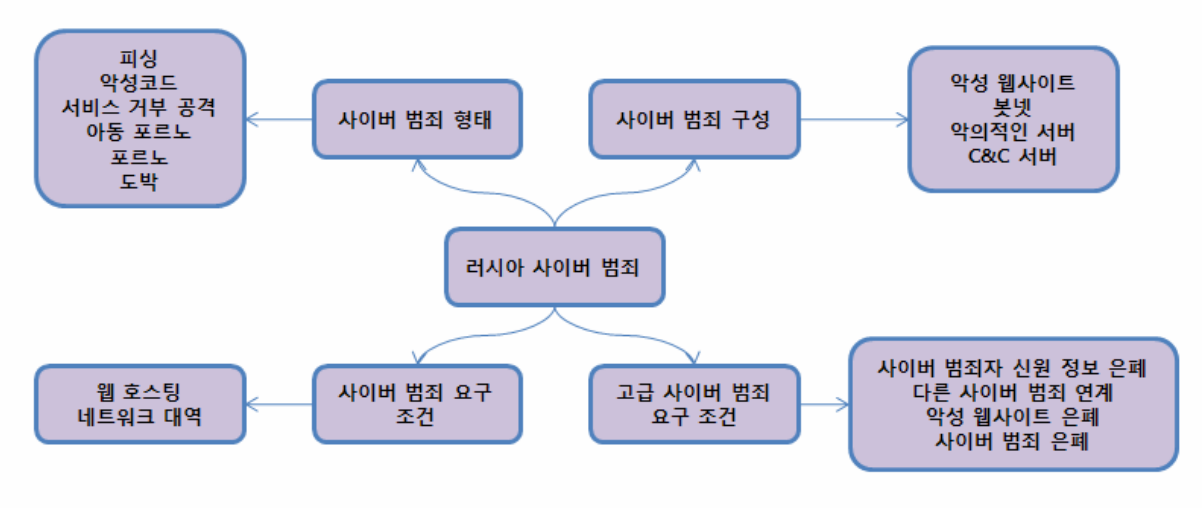


[그림 4-9] 중국 사이버 블랙 마켓의 구조

위 [그림 4-9]와 같은 순환 구조를 가진 중국의 사이버 블랙 마켓에서는 온라인 게임 사용자 정보를 탈취하는 악성코드가 최저 한화 1300원에서 최고 한화 130만원에 거래되고 있으며 이를 이용해 수집한 사용자 정보는 1개당 평균 한화 1300원 선에서 거래되고 있는 실정이다. 그리고 규모 면에서는 2007년 상반기 동안만 중국 내 약 40,000개의 온라인 게임 아이템 거래상들에 의해 평균 한화 2000원 선에서 약 1,220,000개의 온라인 아이템이 거래된

것으로 알려져 있어 얼마나 빠른 속도로 중국의 사이버 블랙 마켓이 성장하고 있는지를 예측할 수 있다. 이러한 추세로 본다면 2008년 역시 온라인 게임 사용자 정보를 탈취하기 위한 악성코드는 지속적으로 발견될 가능성이 상당히 높을 것으로 예측된다.

러시아의 사이버 블랙 마켓은 중국이 온라인 게임 아이템 판매를 통한 현금 획득을 중심으로 움직이고 있는 것과는 다르게 사이버상에서 현금을 획득할 수 있는 어떠한 형태의 재화들 모두가 거래된다는 면에서 중국의 것보다 확장된 형태를 갖추고 있다. 이로 인해 러시아의 사이버 블랙 마켓은 사이버 범죄의 형태를 띠고 있어 그 심각성이 크다고 볼 수 있다.



[그림 4-10] 러시아 사이버 범죄의 구조

이러한 러시아의 사이버 블랙 마켓의 구조를 도식화 한 것이 [그림 4-10]과 같다. [그림 4-10] 중 “사이버 범죄 형태”를 보면 중국의 사이버 블랙 마켓과는 다르게 피싱과 악성코드에서부터 포르노 및 도박 웹 사이트까지 온라인에서 수익을 거둘 수 있는 모든 불법적인 재화들이 이용되고 있는 것을 알 수 있으며 특히나 “고급 사이버 범죄 요구 조건”에서는 오프라인 세상에서 실제 범죄자들이 자신들의 범죄를 은폐하고 범죄 조직을 구성하는 것과 동일한 형태를 띄고 있다.

판매물	판매가
미국 신용카드 정보	$1 ~ $6
영국 신용카드 정보	$2 ~ $12
29,000개의 이메일 계정	$5
온라인 뱅킹 계정	$300
야후 메일 쿠키 익스플로잇	$3
야후 또는 핫메일 계정	$3

좀비 시스템	$6 ~ $20
피싱 웹 사이트	$3 ~ $5
검증된 페이팔(PayPal) 계정	$50 ~ $500
검증되지 않은 페이팔(PayPal) 계정	$10 ~ $50
스카이프(SkyPe) 사용자 계정	$12
월드 오브 워크래프트 사용자 계정	$10

[표 4-2] 러시아 사이버 블랙 마켓에서 거래되는 재화들과 판매가, 출처 - 시만텍

[그림 4-10]과 같은 구성을 가진 러시아의 사이버 블랙 마켓에서는 온라인 게임 아이템과 온라인 게임 사용자 정보가 주되게 거래되는 중국의 사이버 블랙 마켓과는 다르게 앞서 이야기한 바와 같이 온라인상에서 현금을 획득할 수 있는 어떠한 형태의 가상 재화를 모두 판매되고 있다. 이렇게 판매되고 있는 거래물들은 [표 4-2]에서와 같이 신용카드 정보에서 악성코드에 감염된 좀비 시스템까지 다양하게 거래되고 있어 그 규모면 에서는 중국의 사이버 블랙 마켓을 훨씬 뛰어넘는 형태를 보인다고 할 수 있다.

2008년 주요하게 관심을 가지고 지켜보아야 할 대상 중 하나가 바로 중국과 러시아의 사이버 블랙 마켓일 것이다. 이제까지 발생한 보안 사고들은 호기심이나 충동에 의한 것들이었다면 2008년에는 사이버 블랙 마켓에서 현금으로 거래를 위한 대가성 보안 위협이 크게 증가를 할 것으로 예측된다. 특히나 러시아의 사이버 블랙 마켓을 통해 온라인 상에서 현금으로 거래가 가능한 어떠한 형태의 재화 또는 정보라도 모두 거래가 이루어질 수 있다는 점으로 미루어 2008년에는 이 사이버 블랙 마켓을 통해서 새로운 형태의 보안 위협이 등장할 수 있을 것으로 예측된다.

- 이동저장 장치로 전파되는 악성코드 현황

안철수연구소 집계에 따르면 오토런(Autorun)이란 이름으로 이들 악성코드가 추가된 건 2006년 8월부터이다. 해당 악성코드는 비주얼 베이직 스크립트 작성된 형태였으며 2006년 12월 발견된 Win-Trojan/Autorun이 실행코드로는 처음이었다. 하지만, 국내에 본격적으로 유입되기 시작한 건 2007년 6월로 Win-Trojan/Autorun.25650, Win-Trojan/Autorun.14898 등을 시작으로 최근에는 거의 매일 새로운 유사 형태가 발견되고 있다. 대부분의 이들 악성코드는 중국에서 제작된 것으로 추정되며 주로 USB 메모리 사용이 많은 대학 등의 학교에서 극성인 것으로 알려져 있다.

단순히 악성코드와 autorun.inf 파일을 생성하는 형태가 아닌 새로운 기법을 이용하는 악성코드도 증가하고 있다. Win32/Autorun.worm.124370은 감염된 시스템에서 사용자가 악성코드를 삭제할 수 없도록 레지스트리 내용을 주기적으로 수정해 숨김 파일을 볼 수 없게 한다.

유사 방식으로 전파되는 Win32/Drom.worm 변형은 광고 출력을 하는 애드웨어(Adware) DLL 도 시스템에 설치한다. 결국 금전적 목적을 위해 이동 저장 장치를 통한 웜 전파 방법을 이용한 것이다. 국내에는 휴대의 간편성 때문에 USB 메모리에 공인인증서 등의 정보를 보관하는 경우도 많아 향후 이런 자료를 노린 악성코드도 등장 할 수 있다.

2008년에도 이동 저장 장치의 사용자 증가와 함께 이동저장 장치를 노린 악성코드들의 기승과 발전이 예상된다.