ASEC Report 6월

® ASEC Report

2005. 07

안철수연구소의 시큐리티대응센터(AhnLab Security E-response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스와 보안 전문가들로 구성되어 있는 조직이다.

이 리포트는 ㈜안철수연구소의 ASEC에서 국내 인터넷 보안과 고객에게 보다 다양한 정보를 제공하기 위하여 바이러스와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

SUMMARY

트로이목마의 발견과 피해 증가…

6월에는 트로이목마의 발견과 피해가 전월에 비해 증가한 한달이었다. 6월 악성코드 피해건수는 전월에 비해 감소하였으나, 피해신고 된 악성코드 수는 오히려 증가하여 2005년 상반기 중 최고의 수치를 보이고 있다. 이는 트로이목마 신종(변형)의 발견으로 인한 피해가 증가했기 때문인 것으로, 그 피해가 증가한 원인으로는 근래의 트로이목마는 다양한 취약점을 이용하여 전파되어 전파속도가 빠르다는 점을 꼽을 수 있다. 이로 인해 6월 피해신고 된 악성코드의 감염유형별 현황을 살펴보면 네트워크 취약점을 이용한 전파가 10%가량 증가한 것을 볼 수 있다. 6월 신종(변형)발견 수치도 올 3월 이후부터 꾸준히 증가 추세를 보이고 있다. 신종(변형)발견도 피해신고와 마찬가지로 트로이목마의 발견이 강세를 보이고 있어, 전체 발견된 신종(변형) 중 46%를 트로이목마가 차지하고 있다. 또한 6월에는 트로이목마뿐 아니라 드롭퍼와 유해가능 프로그램의 발견도 크게 증가하였다. 반면 세계적으로는 마이톱 웜의 확산이 여전히 강세를 보이고 있다. 또 하나 주목할 만한 것은 모바일 기기에 전파되는 콤워리어라는 모바일 웜의 등장이다. 이는 영국에서 최초 발견된 이후 여러 국가들에서 지속적으로 발견되고 있어 주의가 필요하다.

6월의 스파이웨어 동향은 다운로더가 전체 유해가능 프로그램의 약 33%를 차지할 정도로 증가한 것이 특징이다. 윈도우의 보안기능이 강화되고, 안티 스파이웨어 프로그램의 보급이 확산되면서 기존에 이용하던 브라우저의 취약점이나 ActiveX를 이용한 스파이웨어 설치가 어려워져, 다운로더를 이용하여 스파이웨어를 설치하는 경향을 보이고 있으며 이로 인해 다운로더가 6월에 크게 증가한 것으로 보인다. 또한 애드웨어나 스파이웨어에 의해 설치되는 안티 스파이웨어 프로그램이 증가한 것도 6월의 스파이웨어 동향의 하나로 꼽을 수 있다.

6월은 전월에 비해 많은 윈도우 취약점이 발표되었다. 특히 보안등급이 '긴급'에 해당하는 취약점이 3개나 발표되었으므로 이에 대한 보안패치를 적용하는 등 주의가 필요하겠다. 그 외에도 6월에는 외국에서 마스터, 비자카드 회원 개인정보 유출 사건이 있었으며, 국내 유명 사이트에 대한 해킹 사고가 지속적으로 발견되었다.

이달의 ASEC 컬럼에서는 6월초에 발생했던 인터넷 뱅킹 시스템을 해킹하여 고객의 예금이 인출된 사건을 통해, 상용 키로거가 가지고 있는 문제점과 인터넷 금융사고를 최소화하기 위한 보안수칙에 대해 살펴보았다.

I. 6월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자: 차형진 연구원(sharkjin@ahnlab.com)

순위		바이러스명	건수	%
1	-	Win32/Netsky.worm.29568	287	15.1%
2	New	Win32/Sasser.worm.15872	71	3.7%
3	↑1	Win32/Maslan.C	67	3.5%
4	↓2	Win32/Mytob.worm.59006	67	3.5%
5	-	Win32/Mytob.worm.61440	64	3.4%
6	↓4	Win-Trojan/LineageHack.37888.C	54	2.8%
7	-	Win32/Netsky.worm.17920	35	1.8%
8	New	Win32/Mytob.worm.46675	32	1.7%
9	New	Win32/IRCBot.worm.Gen	26	1.4%
10	↓2	Win32/Netsky.worm.25352	26	1.4%
		기타	1,177	61.8%
합계			1,906	100%

[표1] 2005년 6월 악성코드 피해 Top 10

6월 악성코드 피해 동향

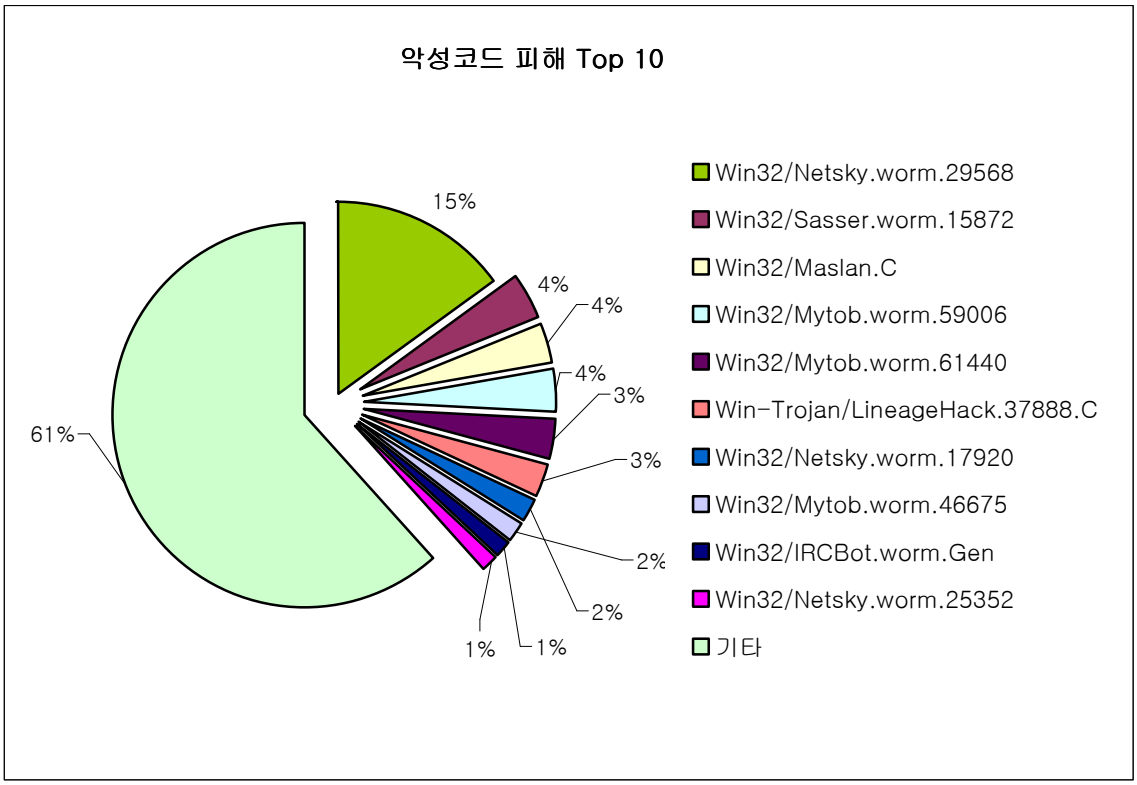
6월 악성코드 피해건수는 5월에 비해 소폭 줄어든 1,906건이다.
지난 달에 비해 피해건수가 감소한 원인으로는 아이알씨봇(IRCBot)류와 매스메일러(Mass Mailer)인 웜(Worm)류의 피해 감소로 인한 것으로 추정된다.

매스메일러인 마이톱 웜(Win32/Mytob.worm)은 12개 이상의 변형이 나타났지만 전파 속도와 피해 정도가 약하여 3위 밖의 순위를 차지하고 있다. 그러나 기능이 다양해져 IRC 채널에 접속하여 명령을 대기하는 것 외에도 레지스트리를 수정하여 윈도우 시작 시 자동 실행하거나 랜덤한 포트로 FTP 서비스를 실행하는 등의 동작을 취하고 있다. 웜의 제작기간이 단축되는 문제뿐만 아니라 기능이 복잡 다양해지는 것도 관심 있게 지켜볼 필요가 있다.

6월 악성코드 피해동향 중 주목할 만한 것은 여전히 1위를 고수하고 있는 넷스카이 웜(Win32/Netsky.worm)과 새로 2위에 진입한 새서 웜(Win32/Sasser.worm)을 들 수 있다. 특히 새서 웜은 윈도우 MS04-011 취약점을 이용해 전파되는데, 이는 아직도 윈도우 취약점에 노출된 컴퓨터가 많다는 것을 보여주고 있다. 윈도우 취약점에 의해 전파되는 웜이 급증하게 된 원인으로는 컴퓨터 시장 가격하락으로 값싸게 판매되는 컴퓨터 매출 성장과 상관관계가 있는 것으로 추정된다. 컴퓨터를 구입한 사용자는 반드시 네트워크를 차단한 채 운영체

제와 보안패치를 동시에 설치하는 자세가 필요하겠다.

6월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.

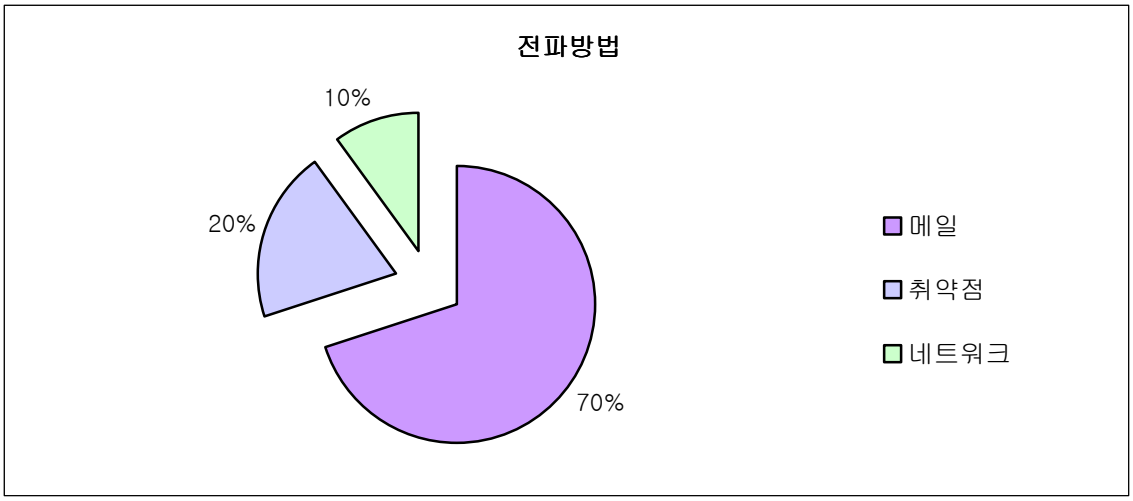


[그림1] 2005년 6월 악성코드 피해 Top 10

6월부터 두각을 나타내기 시작한 트로이목마는 그 감염 피해가 급격하게 증가하고 있으며, 새로운 변형이 발견되는 시기가 상당히 짧게 나타나고 있다. 트로이목마임에도 불구하고 전파속도도 상당히 빠른데, 그 이유는 다운로드, 드롭퍼, HTML 인젝션 등과 같은 다양한 취약점을 이용하여 사용자에게 감염시키고 있기 때문인 것으로 보인다. 예를 들면, 해커는 윈도우 운영체제에서 IIS 웹 서비스를 하고 있는 사이트에 악성코드를 삽입하고 사용자가 웹 페이지를 열람하는 순간에 감염시키도록 한다. 감염된 트로이목마는 대부분 게임 프로그램과 관련된 악성코드로, 사용자 아이디와 패스워드 정보를 가로채기 위한 목적이 다수였다.

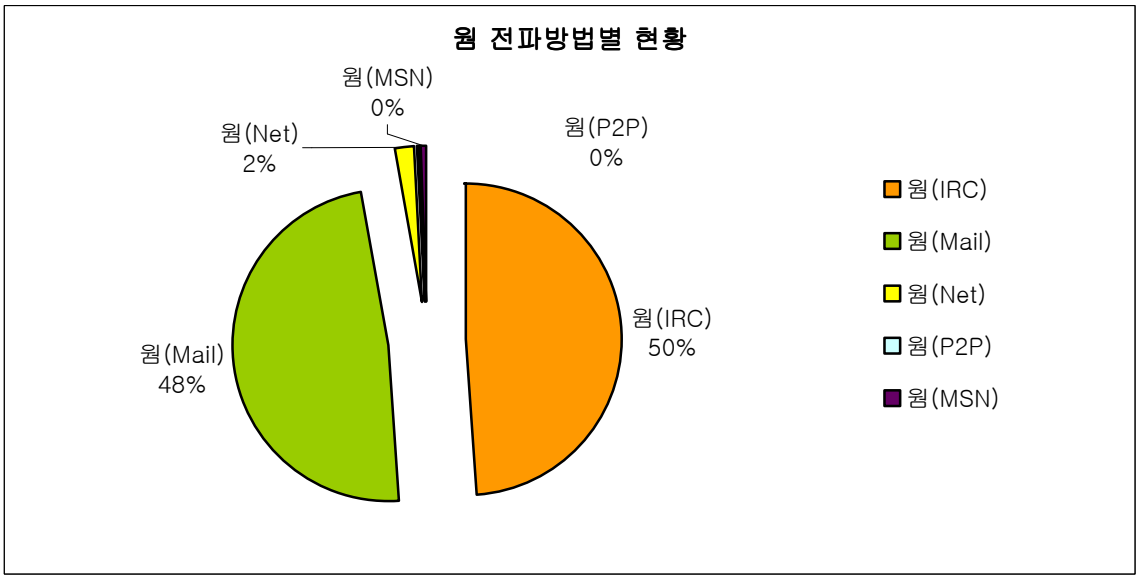
6월 악성코드 Top 10 전파방법 별 현황

[표1]의 Top 10 악성코드들은 주로 어떠한 감염 경로를 가지고 있는지 [그림2]에서 확인할 수 있다.



[그림2] 악성코드 Top 10의 전파방법 별 현황

[그림2]에서 보여주는 것처럼 피해순위 Top 10에 랭크된 악성코드의 70%가 메일을 이용하여 전파되고 있다. 이는 매스메일러에 의한 피해가 대부분을 차지하고 있음을 보여주는 것이다. 또한 지난달에 비해 네트워크, 취약점을 이용한 전파방법이 10%나 급증한 것도 주목할 부분이다. 이 중 웹 서비스와 응용프로그램의 취약점을 이용하여 전파하는 비율이 20%로 매우 높아졌다. 이는 이러한 취약점을 이용한 트로이목마로 인한 피해가 증가한 때문으로, 트로이목마가 전파방법이 전파방법이 점차 지능화되고 있다는 것을 보여주고 있다. 웹 서비스를 이용한 악성코드 전파는 개인정보의 피해로 이어질 수 있으므로 사용자의 각별한 주의가 필요하다. 무료 호스팅을 사용하는 인증되지 않은 사이트는 접근을 피해야 하며, 자신이 사용하는 운영체제와 응용프로그램이 보유한 취약점에 대해 주기적으로 살피고 관련 취약점에 대한 보안패치를 바로 적용하는 자세가 필요하다.

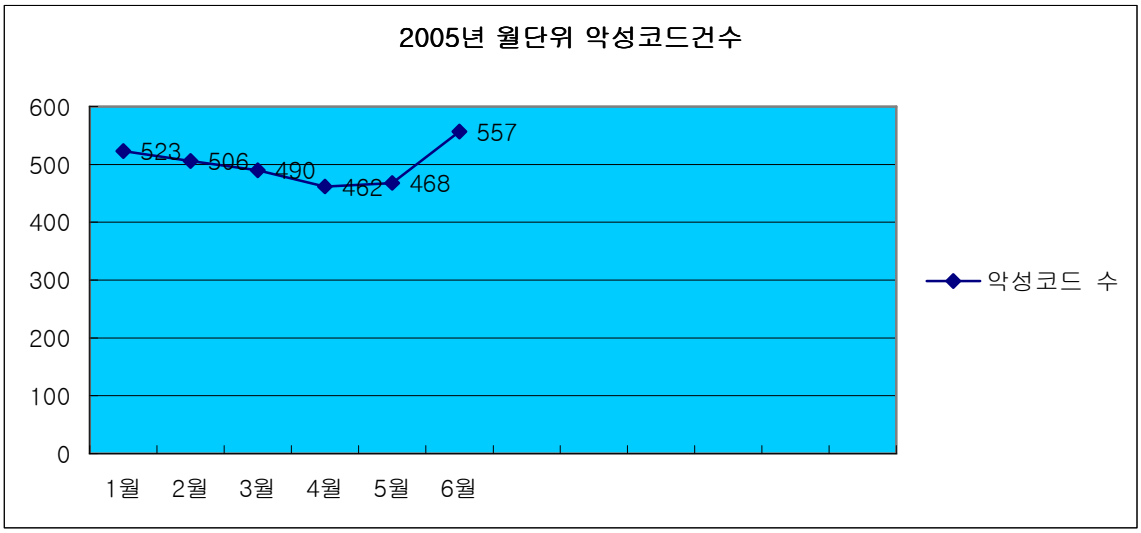


[그림3] 웜의 전파방법 별 현황

[그림3]은 6월에 피해 신고된 웜의 전파방법에 대한 현황으로, 이메일과 인터넷 채팅(IRC)이 98%를 차지하는 것으로 집계되었다. 이는 이메일 사용뿐 아니라 인터넷 채팅(IRC) 사용의 증가에 따른 현상으로 보인다. 따라서, 이메일을 확인하거나 인터넷 채팅(IRC)방에 접속할 때는 최신 엔진으로 업데이트된 백신제품의 실시간 기능을 항상 켜두고 사용하기를 권장한다.

월별 피해신고 악성코드 건수 현황

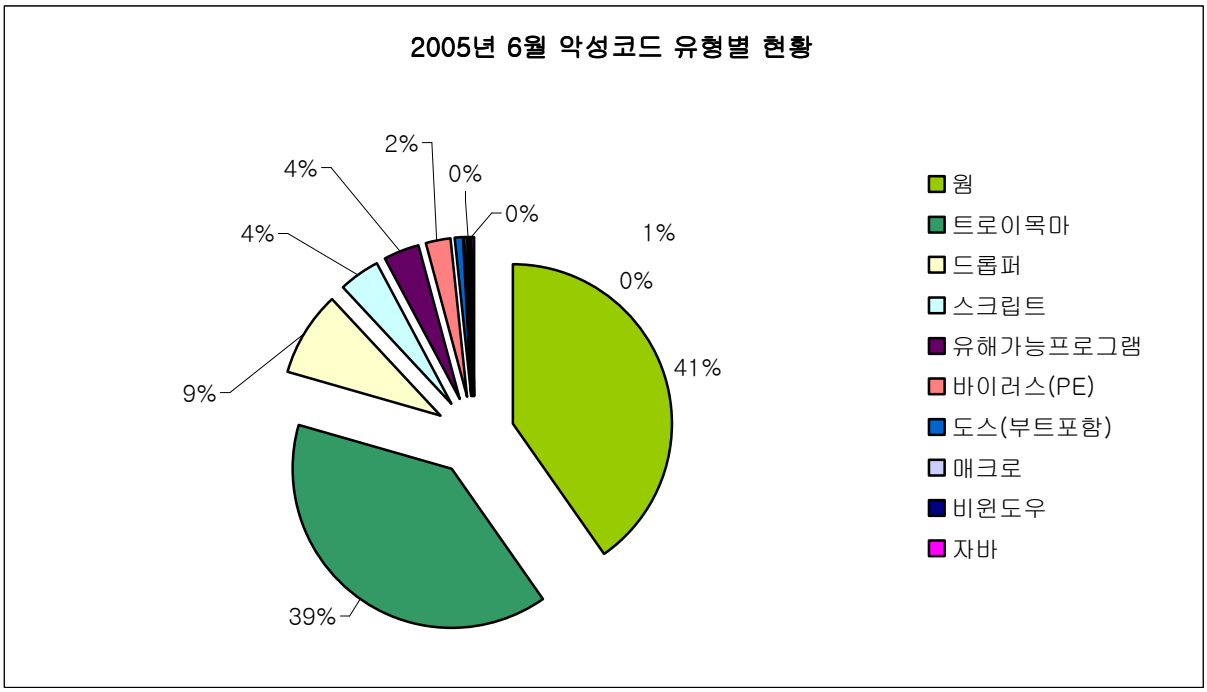
6월에 피해 신고된 악성코드는 557개이다. 상반기중 가장 높은 수치이며, 이는 마이톱 웜 변형과 트로이목마의 피해의 증가로 인한 것으로 보인다. 특히 리니지핵 변종과 다운로더, 드롭퍼 등 트로이목마 비율이 높아졌다.



[그림4] 2005년 월별 피해신고 악성코드 수

주요 악성코드 현황

악성코드 유형별 현황은 [그림5]와 같다.



[그림5] 악성코드 유형별 현황

6월에는 5월에 비해 웜이 10% 가량 감소한 반면, 트로이목마는 2% 가량 증가하였다. 이것은 리니지핵(LineageHack), 드롭퍼(Dropper), 다운로더(Donwloader), 스크립트와 같은 일부 트로이목마의 증가가 주요 원인으로 보인다. 트로이목마를 설치하는 증상을 가진 스파이웨어와 함께 취약점을 이용한 트로이목마 전파가 새롭게 등장한 것도 하나의 요인이다. 트로이목마를 사용자 시스템에 설치하게 하여 개인정보뿐 아니라 금융적인 사기 수법까지 동원이 되고 있어 문제가 심각해지고 있다. 앞으로도 취약점을 이용한 전파방법을 통해 지능적인 트로이목마 변형이 나올 것으로 보인다.

2005년 상반기 악성코드 피해 동향

지난 2004년 상반기의 피해문의가 기하 급수적으로 증가했던데 비해 2005년 상반기는 2003년도와 비슷한 수치의 피해문의가 접수되었다. 이는 2004년에 비해 아이알씨봇과 매스메일러에 대한 피해가 감소하였기 때문으로 추정된다.

2004년 상반기와 2005년 상반기의 안철수연구소가 피해신고 건수를 비교해 보면 [표1]과 같다.

구분	1 월	2 월	3 월	4 월	5 월	6 월	합계
2004 년	5,580	6,641	5,147	5,633	22,104	22,209	67,314
2005 년	2,432	1,979	1,651	1,572	2,066	1,906	11,606

[표1] 2004년, 2005년 상반기 월별 국내 악성코드 피해 신고 통계

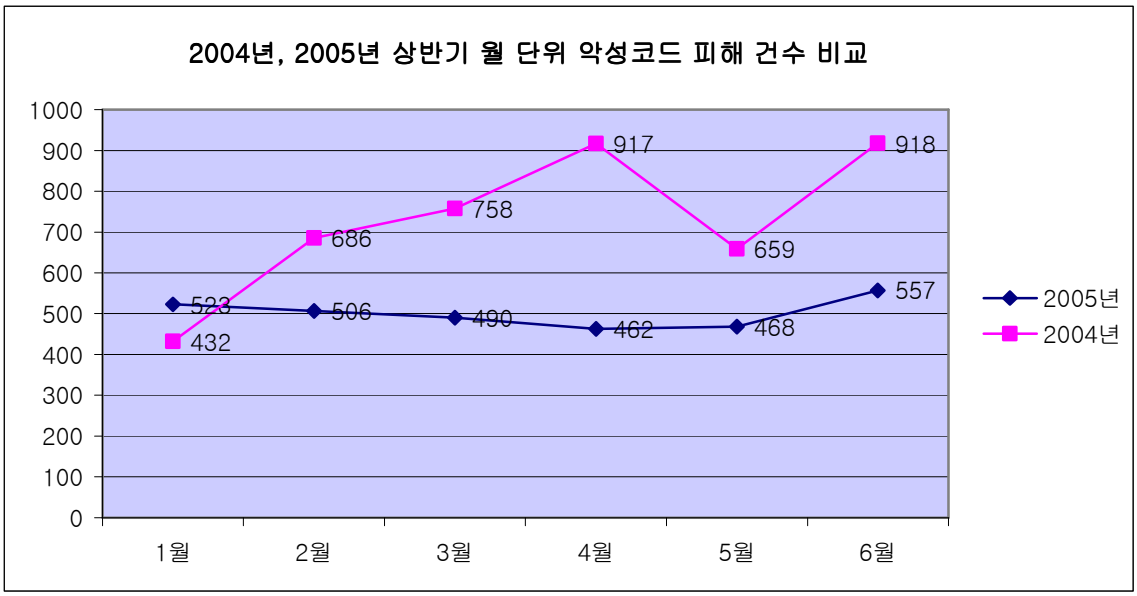
[표1]에서 보듯이 작년 상반기에 비해 올 상반기에 신고된 악성코드 피해문의는 55,708건이나 감소하였다. 이는 작년 피해건수의 17%에 달하는 수치로 2003년도 상반기의 악성코드 피해수치와 비슷한 수치이다. 2004년 후반기에 새서 웜, 아고봇 웜 제작자가 잇따라 검거되었고, 웜 제작자를 검거하기 위해 현상금까지 내거는 등의 노력으로 아이알씨봇류와 매스메일러 제작이 위축되어 2004년 상반기에 비해 피해건수가 대폭 감소한 것으로 보인다.

작년 상반기와 올해 상반기의 악성코드 피해 중 Top 10을 차지한 것을 정리해보면 매스메일러에 의한 피해문의가 많은 것은 작년 상반기와 비슷하다. 올해 초 새로 등장한 마이톱 웜의 등장이 주목할 만하다. 그러나 2004년 상반기 경우 Top 10에 속한 대부분의 악성코드들이 모두 매스메일러였던 것에 반해, 2005년 상반기에는 트로이목마와 윈도우 파일 바이러스 등이 순위에 진입한 것을 볼 수 있다. [표2]가 이를 잘 말해 주고 있다.

순위	2004 / 악성코드명	건수	2005 / 악성코드명	건수
1	Win32/Netsky.worm.29568	19,708	Win32/Netsky.worm.29568	2,452
2	Win32/Dumaru.worm.9234	11,130	Win32/Netsky.worm.17920	388
3	Win32/Netsky.worm.17424	6,571	Win32/Sasser.worm.15872	344
4	Win32/Netsky.worm.28008	2,805	Win32/Netsky.worm.25352	264
5	Win32/Netsky.worm.22016	1,922	Win32/Netsky.worm.22016	210
6	Win32/Netsky.worm.17920	1,747	Win32/Maslan.C	189
7	Win32/Blaster.worm.6176	1,645	Win32/Netsky.worm.16896.B	193
8	Win32/Netsky.worm.22016	801	Win32/Mytob.worm.59006	154
9	Win32/Bagle.worm.Z	686	Win-Trojan/LineageHack.37888.C	150
10	Win32/Netsky.worm.22016.C	684	Win32/Mytob.worm.61440	145

[표2] 2004년, 2005년 상반기 악성코드 피해 Top10 비교

[표2]에서도 알 수 있듯이 올해 피해 건수는 대폭 감소하여 매달 비슷한 피해 건수가 집계되는 것을 볼 수 있다. 특히 올해 상반기 중 6월 건수가 증가하고 있는 이유로는 트로이목마로 인한 감염 건수가 증가하고 있는 것으로 집계되었다.



[그림1] 2004년, 2005년 상반기 월 단위 악성코드 피해 건수

올해 상반기에는 트로이목마 류에 의한 피해 문의건수가 증가하고 있으며, 트로이목마 특성상 2004년도와 같이 피해가 대폭 증가하지는 않겠지만 전파 수법이 다양하고 지능적이어서 점진적으로 증가할 것으로 추정된다.

(2) 신종(변형) 악성코드 발견 동향

작성자: 정진성 주임연구원 (jsjung@ahnlab.com)

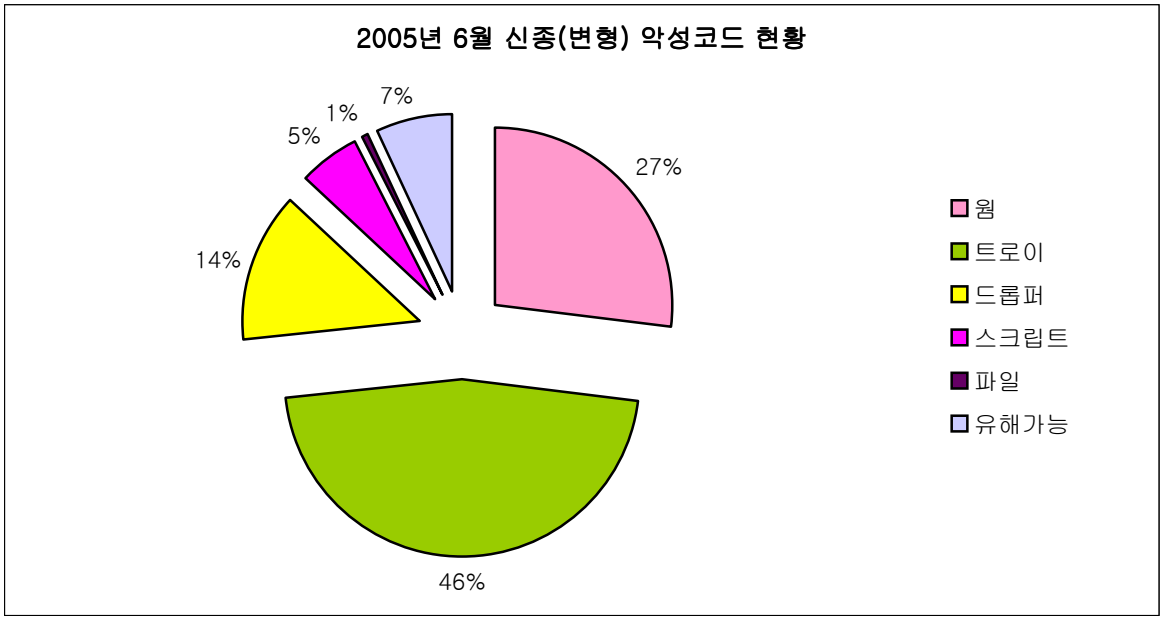
6월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1], [그림1]과 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	非윈도우	합계
79	136	40	16	2	0	0	0	20	0	293

[표1] 2005년 6월 유형별 신종 (변형) 악성코드 발견현황

트로이목마가 지난달에 이어서 강세를 보이고 있다. 더불어 트로이목마를 설치하는 드롭퍼도 증가하였다. 이러한 원인은 이전 동향에서도 설명한 것처럼 웜의 대다수를 차지하는 악성 아이알씨봇 웜의 샘플접수가 줄어든 것이 가장 큰 원인이다. 그러나 악성 아이알씨봇 웜 변형의 발견이 줄어들고는 있지만, 여전히 많은 양의 악성 아이알씨봇 웜 변형이 전세계적으로 보고 되어 있으므로 안심해서는 안된다. 또한 최근 들어 다시 찾아온 트로이목마의 증가도 눈여겨 볼 필요가 있다.

[그림1]은 6월 신종(변형)악성코드의 비율을 나타낸 것이다. 지난달에 이어 트로이목마 비율이 전체의 46%를 차지하고 있다.



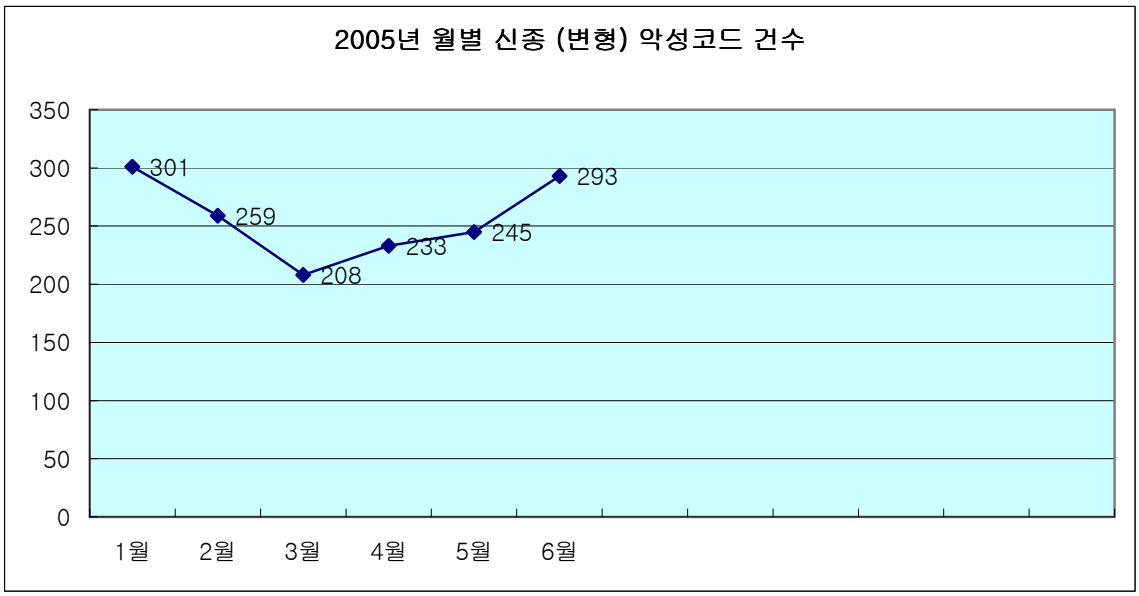
[그림1]2005년 6월 신종(변형) 악성코드 비율

이번 달은 드롭퍼(Dropper)와 유해가능 프로그램의 증가도 눈에 띈다. 전월 대비 드롭퍼는 60%, 유해가능 프로그램은 50% 가량 증가했다.
변형이 많았던 드롭퍼와 유해가능 프로그램은 [표2]와 같다.

드롭퍼(Droppper)	유해가능 프로그램
Dropper/ADropper)	Win-AppCare/ServU
Dropper/HangHack	Win-AppCare/HideWnd
Dropper/LineageHack	
Dropper/Paradrop	

[표2] 6월에 변형이 많이 발견된 드롭퍼와 유해가능 프로그램

[그림2]는 월별 신종(변형) 악성코드 건수를 나타내고 있다. 트로이목마의 증가로 인하여 4월부터 악성코드 건수가 증가한 것을 알 수 있다.



[그림2]2005년 월별 신종(변형) 악성코드 발견 현황

6월 주요 신종(변형) 악성코드 정리

이번 달은 세간의 이목을 끄는 특이한 악성코드는 없었지만 지난달에 이어서 여전히 국내 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마가 기승을 부렸다. 또한 이를 설치하는 드롭퍼, 그리고 드롭퍼를 자동으로 다운로드 하여 실행하는 보안 취약점이 존재하는 스크립트 파일들이 대거 발견되었다. 이 악성코드들은 국내 유명 웹 사이트들을 해킹한 후 원격의 호스트로부터 파일을 내려 받도록 링크를 심어 둔 형태로 확인되었다.

마이톱 웜(Win32/Mytob.worm)은 계속적으로 변형이 발견, 보고되었으며 일부는 다형성 악성 아이알씨봇 웜에서 사용한 다형성 크립터(Crypter)를 사용하는 형태도 발견되었다.

AOL (AOL Instant Messenger) 관련 메신저 웜도 5월에 이어서 6월에 다른 변형이 발견되었는데 이 웜도 악의적인 아이알씨(IRC) 서버에 접속하여 명령을 받는 형태로 되어 있다.

트로이목마 중에서는 여전히 에이전트(Agent), 다운로더(Downloader)도 다수 발견 되었다. 이외에는 MS05-011 취약점에 대한 공격코드(Exploit)가 공개되었다.

이슈가 되었던 악성코드는 다음과 같다.

► **애드롭퍼 드롭퍼(Dropper/ADropper)**

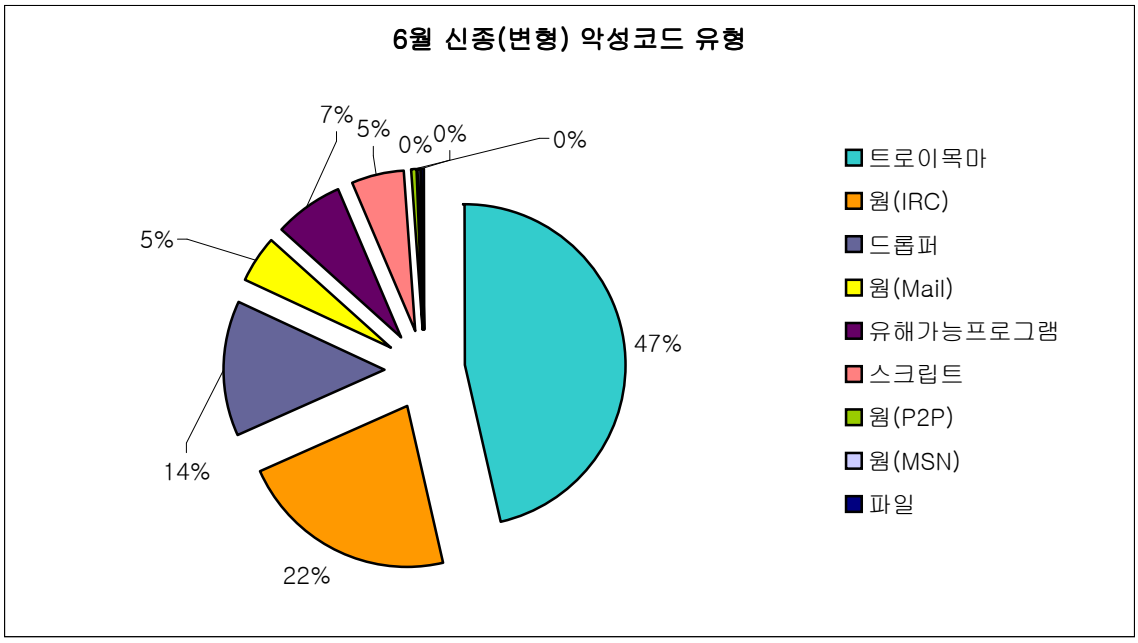
이 드롭퍼의 진단명은 일반적으로 스파이웨어(애드웨어) 관련 파일을 설치하는 악성코드를 지칭한다. 악성코드와 스파이웨어의 경계가 모호해졌으므로 이러한 드롭퍼들이 다수 증가하는 추세이다. 또한 이러한 유형을 안티 스파이웨어 제품에서만 대응하기보다는 안티 바이러스 제품에서도 적극적으로 대응하고 있는 추세이다.

► **Dropper/PWS-Rokw**

4월말부터 국내 유명 웹 사이트를 대상으로 조직적인 해킹이 시도되었다. 해킹목적은 특정 온라인 게임의 사용자 계정을 탈취하려는 목적이었다. 이러한 시도는 다른 온라인 게임들로 대상을 넓혀 갔으며 또한 국내 유명 포털의 사용자 계정을 훔쳐내도록 만들어진 Win-Trojan/PWS-Rokw도 발견, 보고 되었다.

지금까지는 특정 온라인 게임의 사용자 계정만을 훔쳐내도록 되어 있으나 최근에는 다수의 온라인 게임의 사용자 계정을 훔쳐내는 형태로 발전하였다. 이러한 악성코드들의 궁극적인 목적은 악성코드 제작자들이 훔쳐낸 계정을 이용하여 아이템을 획득하거나 판매하여 금전적인 이득을 노리는 것으로 추정하고 있다.

다음은 6월에 발견된 악성코드들을 유형별로 분류한 것이다.



[그림3] 6월 신종 (변형) 악성코드 유형별 현황

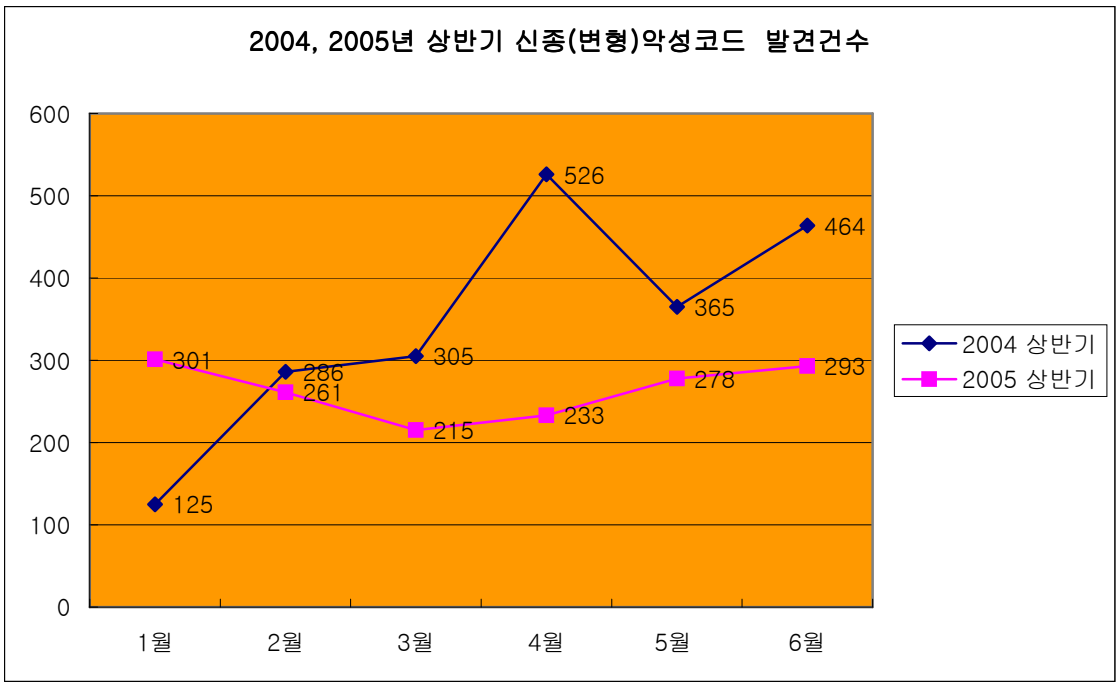
위에서 언급한 것처럼 6월 악성코드 유형 중 트로이목마의 비율이 두드러진다. 또한 여기에 드롭퍼와 유해가능 프로그램들의 비율도 전월에 비하여 높아졌다. 트로이목마들이 대부분 자체 전파기능이 없고 악의적인 목적을 가진 사용자에게 의해서 배포되고 이용된다고 볼 때

트로이목마의 피해가 상당히 많은 것을 알 수 있다.

2005년 상반기 악성코드 동향 및 정리

작년 한해 악성코드의 최대 이슈는 악성 아이알씨봇 웜이었다. 아마도 단일 악성코드로는 가장 많은 변형들이 발견되고 사용자들의 피해문의가 많았기 때문일 것이다. 올해도 악성 아이알씨봇 웜의 변형이 가장 많이 발견되었지만 안철수연구소를 비롯한 대부분의 안티 바이러스 업체들은 이 악성 아이알씨봇 웜을 대응하기 위한 충분한 방안을 모두 가지고 있어 작년처럼 수 많은 변형이 쏟아져 나와도 실행압축해제, 휴리스틱 검사 등으로 적시에 대응을 잘 하고 있는 것으로 보인다.

다음은 작년과 올해 상반기 신종 및 변형 악성코드에 대한 발견 건수를 조사해본 것이다. 이 악성코드들은 국내에서 고객으로부터 접수된 악성코드만 통계를 낸 것이다.



[그림4] 2004, 2005년 상반기 신종(변형)악성코드 발견건수

[그림4]에서도 알 수 있듯이 작년에는 2월부터 악성코드 수가 급격히 증가한 것을 알 수 있다. 증가 원인은 위에서도 설명한 것처럼 악성 아이알씨봇 웜 변형들 때문이다.
올 상반기 악성코드는 국내기준으로 하루 평균 51개의 신종 및 변형의 악성코드가 발견, 보고 되었다. 전년 동기는 하루 평균 66개였으므로, 작년에 비해 올해는 다소 감소한 수치를 보이고 있다. 올해 들어서는 3월에 악성코드가 주춤하는 듯 하였으나 트로이목마의 수가 증가함에 따라서 전체적인 악성코드 수도 증가하고 있다.

올 상반기 이슈가 있었던 악성코드 유형들을 나열해보면 다음과 같다.

- ► 메신저 웜 변형의 급격한 증가
- ► 이메일 웜 + 악성 아이알씨봇 웜 형태 등장
- ► 애드웨어를 통해서 감염되는 바이러스 등장
- ► 온라인 게임의 사용자 계정을 탈취하는 악성코드 증가
- ► MMS를 이용하여 전파되는 휴대폰 악성코드 보고
- ► 다양한 유형의 트로이목마 증가
- ► 봇넷(BotNet)

이 악성코드 유형을 간단히 정리해보면 다음과 같다.

► 메신저 웜 변형의 급격한 증가

올해 들어서 메신저 웜은 급격한 증가를 보여주었다. 그것도 단일 웜 하나의 지속적인 변형이 제작되었다. MSN 메신저로 전파되는 켈비르 웜(Win32/Kelvir.worm)이라고 명명된 이 웜은 그 동작형태는 매우 일반적이다. 다만 특이한 것은 이 메신저 웜이 악성 아이알씨봇 웜을 내부에 포함하고 있거나 특정 호스트로부터 다운로드 한다는 것이다. 즉, 악성 아이알씨봇 웜의 전파경로로 메신저가 새롭게 이용되고 있는 것이다. 켈비르 웜이 메신저 버디 리스트를 뒤져서 악성 아이알씨봇 웜을 다운로드하는 링크를 보내거나 웜 내부에 포함된 악성 아이알씨봇 웜을 실행하는 것 이외에 별다른 증상이 없다는 점이 이를 뒷받침해 주고 있다.

► 이메일 웜 + 악성 아이알씨봇 웜 형태 등장

마이톱 웜이라고 명명된 이 웜은 올 2월에 처음 발견, 보고 되었고 이 글을 작성하는 현재까지 수 많은 변형이 제작되었다. 마치 작년에 있었던 베이글 웜(Win32/Bagle.worm), 넷스카이 웜(Win32/Netsky.worm), 마이둠 웜(Win32/MyDoom.worm)이 경쟁적으로 변형을 만들어 냈던 것처럼 이 악성코드의 제작자는 재 컴파일 및 서로 다른 실행압축 툴의 조합으로 변형을 양산하였다. 이 악성코드가 주목받은 것은 바로 메일전파 이외에 제작자가 지정한 IRC 서버에 접속하는 증상이 있기 때문이다. 이메일 웜에 이와 같은 증상이 포함된 경우는 처음 있는 형태이다.

► 애드웨어(이하 스파이웨어)를 통해서 감염되는 바이러스 등장

스파이웨어는 지금까지 의도하지 않는 광고 정도만을 보여주는 성가신 프로그램이었다. 그러나 스파이웨어가 윈도우의 실행파일을 감염시켜서 지속적으로 스파이웨어를 다운로드하거나 윈도우의 보안관련 레지스트리를 변경하는 형태가 등장하였다.

부베 바이러스(Win32/Bube)라고 명명된 이 악성코드는 실행파일을 감염시키는 첫번째 스파이웨어로 보고되었다. 악성코드 제작자의 의도를 완벽히 간파할 수는 없지만 대부분의 안티스파이웨어 제품들이 파일의 크기와 특별한 해쉬 값만을 가지고 스파이웨어 유무를 판단하고 제거하므로 실행파일을 감염시키면 대부분의 제품에서 이를 대응하지 못할 것으로 판단하고 제작된 형태가 아닌가 추정해본다.

► **온라인 게임 사용자 계정을 탈취하는 악성코드 증가**

국내 온라인 게임의 인기가 높아져 해외에서도 서비스가 된 후부터 사용자 계정을 훔쳐내는 악성코드가 제작되고 있다. 이 악성코드 제작자들의 궁극적인 목적은 훔쳐낸 사용자 계정으로 사용자들의 아이템을 획득하여 이를 통한 금전적인 이익을 얻으려고 하기 때문이다. 온라인 게임 내 사용되는 아이템은 국내에서도 현금 거래가 되고 있기 때문이고 사이버 머니라고 불려지는 게임머니는 이를 통해서 실제 물품 등을 구입할 수 있기 때문이다. 이 트로이목마의 증가는 금전적인 이익을 노리는 최근 악성코드 제작자들의 제작 동기와도 일치하여 앞으로도 금전적인 이익을 노리는 악성코드가 증가할 것으로 예상되며 이는 곧 지속적인 트로이목마의 증가로 이어질 것으로 보인다.

► **MMS를 이용하여 전파되는 휴대폰 악성코드 발견**

블루투스(Bluetooth)는 단지 시작에 불과했다. 단거리 무선통신기술인 블루투스의 기술이 휴대폰에 탑재된 후 휴대폰 악성코드 제작자들은 불과 10M 이내의 전파력을 가진 이 기술에 더 이상 안주하지 못했다. 제한된 거리를 벗어 날 수 있는 방법은 MMS(Multimedia Messaging Service)였고 이를 이용하여 악성코드를 제작하였다. MMS를 이용하면 마치 메일에 첨부파일을 포함하여 발송한 것처럼 보낼 수 있기 때문이다. 거리의 제한이 없어진 MMS를 이용하는 악성코드가 나오기까지는 첫 휴대폰 악성코드가 나온 후 1년도 채 소요되지 않은 것으로 보고되었다.

► **다양한 유형의 트로이목마 증가**

더 이상 새로울 것이 없는 악성코드 유형이지만 최근 들어 악의적인 형태에 따라 분류되는 트로이목마가 늘었다. 주로 다음과 같은 유형들이다.

- 에이전트(Agent): 특정 호스트로부터 명령을 받아 악의적인 증상을 수행
- 프록시(Proxy): 감염된 시스템의 추적을 회피하려는 증상
- 피더블유에스(PWS): 윈도우 및 응용 프로그램의 암호를 훔쳐내는 증상
- 다운로더(Downloader): 특정 호스트에 업로드 된 파일을 다운로드하고 실행하는 증상
- 스타트페이지(StartPage): 인터넷 익스플로러 시작 페이지를 변경하는 증상
- 클릭커(Clicker): 특정 웹 사이트의 배너 등을 자동 클릭하게 하는 형태
- 백도어(Backdoor): 원격제어 증상을 가진 형태

올 상반기 트로이목마가 2003년 이후 다시 증가한 가장 큰 이유는 위에서도 언급된 것처럼 온라인 게임의 사용자 계정을 훔쳐내는 악성코드를 비롯하여 위 트로이목마들의 목적이 사용자 정보를 유출하여 이를 통한 유, 무형의 이익을 실현하고자 하는 악성코드 제작자들의 동기에 있기 때문이다.

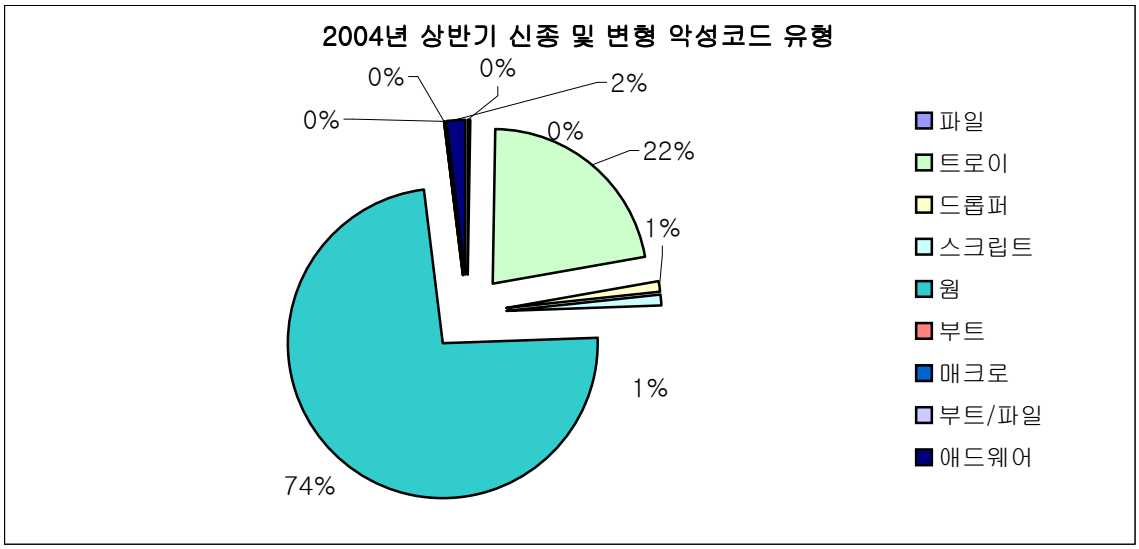
► **BotNet (봇넷)**

봇넷은 새로운 형태도 아니고 특정 악성코드를 지칭하는 것도 아니다. 봇넷은 네트워크에 연

결된 감염된 악성코드의 집합체이다. 봇넷은 미래 악성코드의 모습이라고 얘기하는 사람들도 있다. 악성 아이알씨봇 웜을 시작으로 베이글 웜까지 악성코드 제작자들은 자신이 감염시킨 시스템들을 원격에서 관리하고 이를 이용하여 악성코드를 전파하거나 다른 시스템을 공격, 또는 감염된 시스템의 제어권을 스팸 메일 발송자들에게 돈을 받고 팔려는 움직임이 이전부터 확인되었다. 좀비 시스템이라고 알려진 감염된 시스템들은 하나의 거대한 네트워크를 구성하여 위에서 언급한 것처럼 악의적인 목적에 다분히 이용될 소지가 크며 하나가 아닌 다수의 시스템들이므로 큰 피해를 가져올 잠재적 위험을 가진 형태라 할 수 있다.

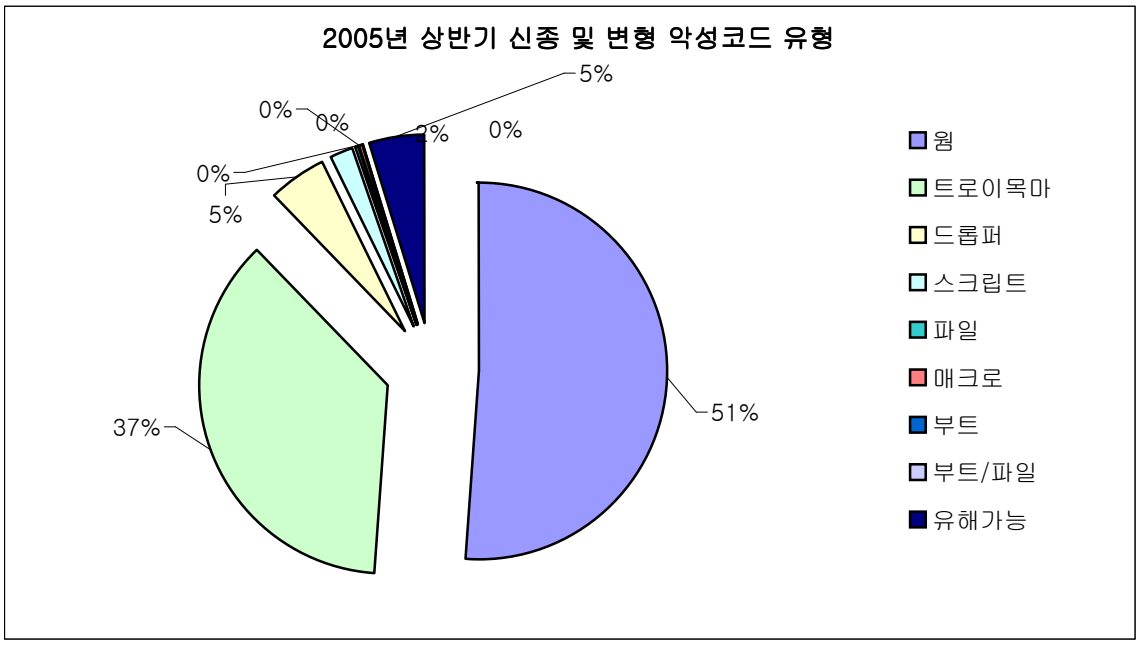
지금까지 상반기 이슈가 있었던 악성코드 형태를 알아 보았다. 상반기에는 다행히도 대규모의 악성코드 확산이라던가 MS 보안 취약점을 이용한 대규모의 공격은 없었다. 하지만 기존에 알려진 보안 취약점을 이용하여 악성코드를 전파하는 유형은 계속 보고되고 있다.
또한 은폐형 악성코드 및 진단/치료하기 까다로운 악성코드들도 여전히 사용자들이 괴롭히고 있다.

2004, 2005년 상반기 신종 및 변형 악성코드 유형은 다음과 같다. 2004년은 악성 아이알씨봇 웜의 증가로 웜의 비율이 상당히 높은 것을 알 수 있다.



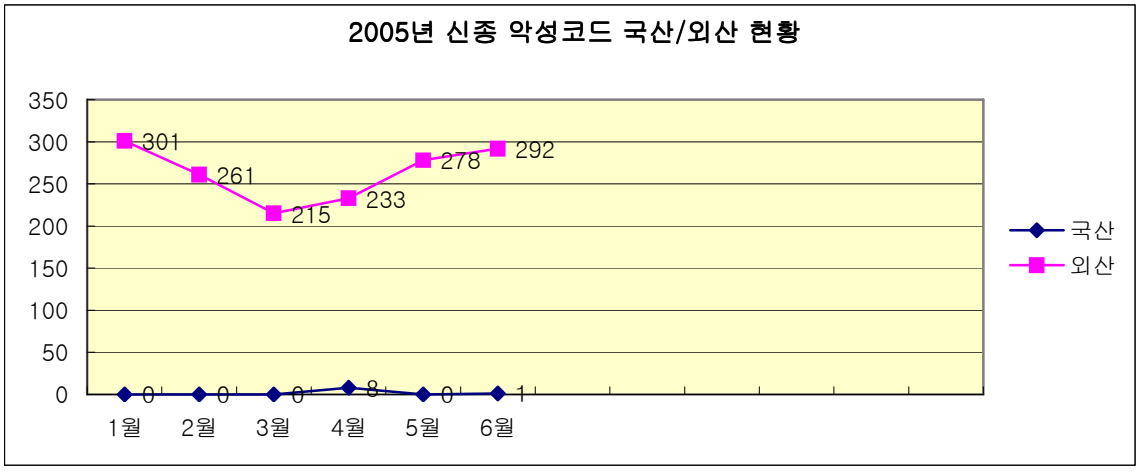
[그림5] 2004 상반기 신종 및 변형 악성코드 유형

반면, 2005년 상반기 경우 웜의 비율이 여전히 과반수이지만 작년 동기와 비교해서 트로이목마의 비율이 상대적으로 높아졌다. 이는 최근 다양한 증상을 가진 트로이목마의 증가를 단적으로 보여주는 예라 할 수 있겠다. 또한 상용 또는 셰어웨어 프로그램으로 제작 되었지만 사용목적에 따라서 악의적으로 사용될 수 있는 유해가능 프로그램들도 올해부터 통계를 내어본 결과 전체의 5%(75개)를 차지할 정도로 다양한 종류가 접수되었다.



[그림6] 2005 상반기 신종 및 변형 악성코드 유형

다음은 국내제작 악성코드 현황이다. 국내 제작 악성코드는 보고된 수가 저조하여 올해부터 별도로 ASEC 리포트에 기술하지 않았으나 상반기에는 그 동안 어떤 추세였는지 분석해보았다.



[그림7] 2005년 신종 및 변형 국산/외산 현황

상반기에 발견된 국산 악성코드들은 과거에 많이 보였던 스팸 메일러 형태가 주로 발견, 보고 되었다. 이외에도 배치파일로 만들어져 파일을 삭제하는 트로이목마 형태도 1건 보고되었다.

상반기 악성코드 신종(변형) 발견의 특징은 대규모의 악성코드 확산이나 취약점을 이용한 공격은 없었지만 여전히 많은 수의 악성 아이알씨봇 웜이 보고되고 있으며 커널 모드 드라이

버를 이용하여 은폐증상을 갖는 형태나 새로운 실행압축 툴로 팩킹된 형태가 대거 발견되었다는 것이다. 또한 MMS를 이용하여 전파의 한계를 뛰어 넘은 휴대폰 악성코드를 비롯하여 악성 아이알씨봇 웜 증상을 가진 이메일 웜과 메신저 웜이 등장하였다. 과거의 악성코드 추세의 강자였던 트로이목마가 다양한 증상을 가진 형태로 발전하고 금전적인 이익을 노리는 형태로 변모하여 수를 증가함에 따라 이 악성코드의 비율이 점점 높아지고 있는 것으로 2005년 상반기의 특징을 정리할 수 있을 것이다.

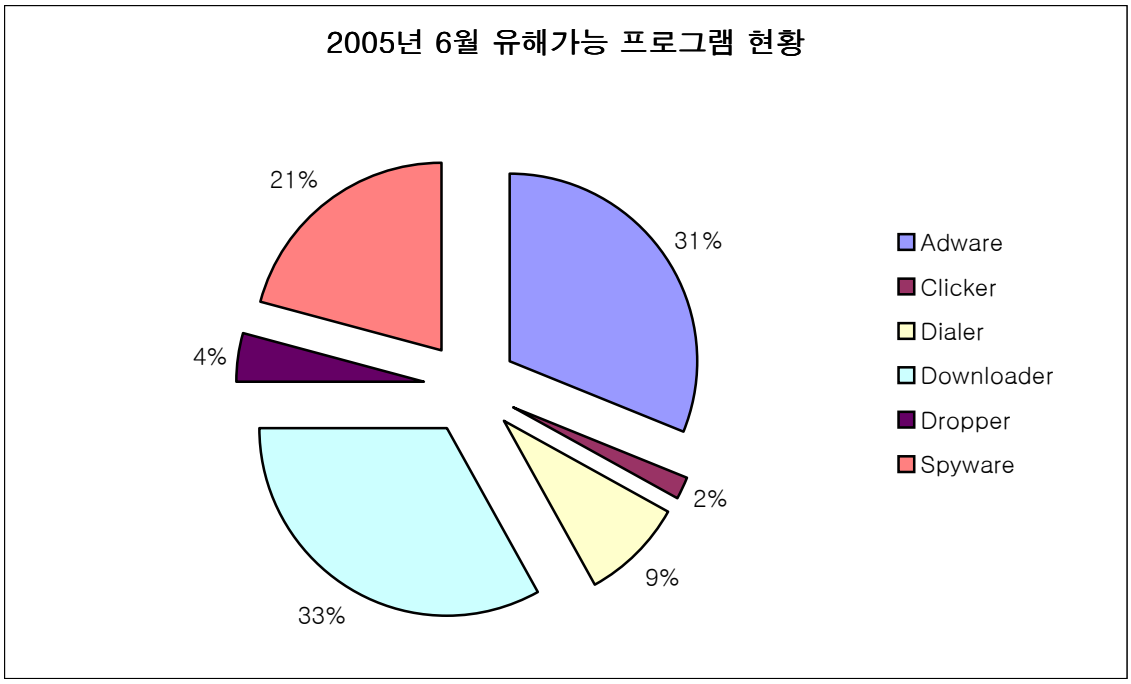
상반기에 정식 발표된 윈도우 XP 64비트로 하여금 곧 64비트 환경이 대중적으로 열리게 될 전망이다. 이에 관련된 악성코드의 등장은 이미 그 개념이 1년 전에 증명되었으며 그리 새로울 일은 아니다. 하지만 앞으로 있을지 모를 64비트 환경의 악성코드 증가와 휴대폰과 같은 모바일 기기에 대한 악성코드 수적증가는 다분히 예상해 볼 수 있다.

II. 6월 AhnLab 스파이웨어 동향

작성자: 김정석 주임연구원(js_kim@ahnlab.com)

6월에 발견된 스파이웨어 동향은 다운로더(Downloader)가 전체 유해가능 프로그램의 약 33%의 높은 비중을 차지하는 것이 가장 큰 특징이다. 일반적으로 자체 확산 기능이 없는 애드웨어나 스파이웨어와 같은 유해가능 프로그램은 설치의 대부분을 브라우저 취약점이나 ActiveX 를 이용한 설치에 의존하고 있다. 최근에는 다음과 같은 이유로 유해가능 프로그램의 배포가 어려워진 것도 트로이목마 형태로 동작하는 다운로더가 증가한 원인으로 생각된다.

- 인터넷 및 브라우저 보안 기능이 강화된 윈도우 XP 서비스팩2 사용자의 증가
- 안티 스파이웨어 프로그램의 보급
- 애드웨어, 스파이웨어 프로그램의 피해로 인한 사용자 보안 의식 향상



[그림1] 6월 발견된 유해가능 프로그램 동향

다운로더가 설치하는 유해가능 프로그램은 매우 다양하다. 많은 수의 다운로더가 또 다른 다운로더, 유해가능 프로그램의 드롭퍼(Dropper), 다이얼러(Dialer) 등을 다운로드하고 설치하며 아이에스티바(Win-Adware/ISTbar), 엔케이스(Win-Adware/nCase) 같이 널리 알려진 애드웨어를 설치하고 실행한다. 다운로더는 3KB~4KB의 아주 작은 사이즈로 드롭퍼나 다른 다운로더에 의한 설치가 용이하며, http나 ftp를 이용하기 때문에 방화벽 보안정책의 제한을

받지 않는다. 일반적으로 백그라운드로 실행되기 때문에 사용자가 인지하지 못하는 경우가 많고, 실행되는 것만으로 시스템 성능을 크게 떨어뜨리며, 팝업광고가 노출되고 브라우저의 시작페이지가 원하지 않는 사이트로 고정되는 등 전형적인 애드웨어나 스파이웨어의 감염 증상을 보이기도 한다. 특정 웹사이트를 신뢰하는 사이트(Trusted Sites)에 등록하거나 브라우저 보안 설정을 변경하는 등 시스템 보안에 큰 위협으로 작용한다.

6월에는 다운로더에 의해 설치되는 애드웨어에 의한 피해사례가 많이 접수되었다. 많은 피해를 입힌 애드웨어는 다음과 같다.

► 아이에스티바(Win-Adware/ISTbar)

성인컨텐츠를 포함하는 IE 툴바를 설치하고, 시작페이지와 검색페이지를 변경한다. ActiveX 또는 다른 여러 다운로더에 의해서 설치되며, 제어서버에서 임의의 프로그램을 다운로드하고 설치할 수 있다. 경쟁관계에 있는 다른 애드웨어의 제거를 시도하기도 한다.

► 미디어티켓츠(Win-Adware/MediaTickets)

전형적인 ActiveX 다운로더로서 다른 유해가능 프로그램을 설치한다. 미디어티켓츠가 다운로드 하는 프로그램은 용도를 속여서 설치를 유도하거나, 사용자가 동의하지 않아도 설치되기도 한다. 제어서버에 접속하여 임의의 프로그램을 다운로드하고 설치할 수 있다.

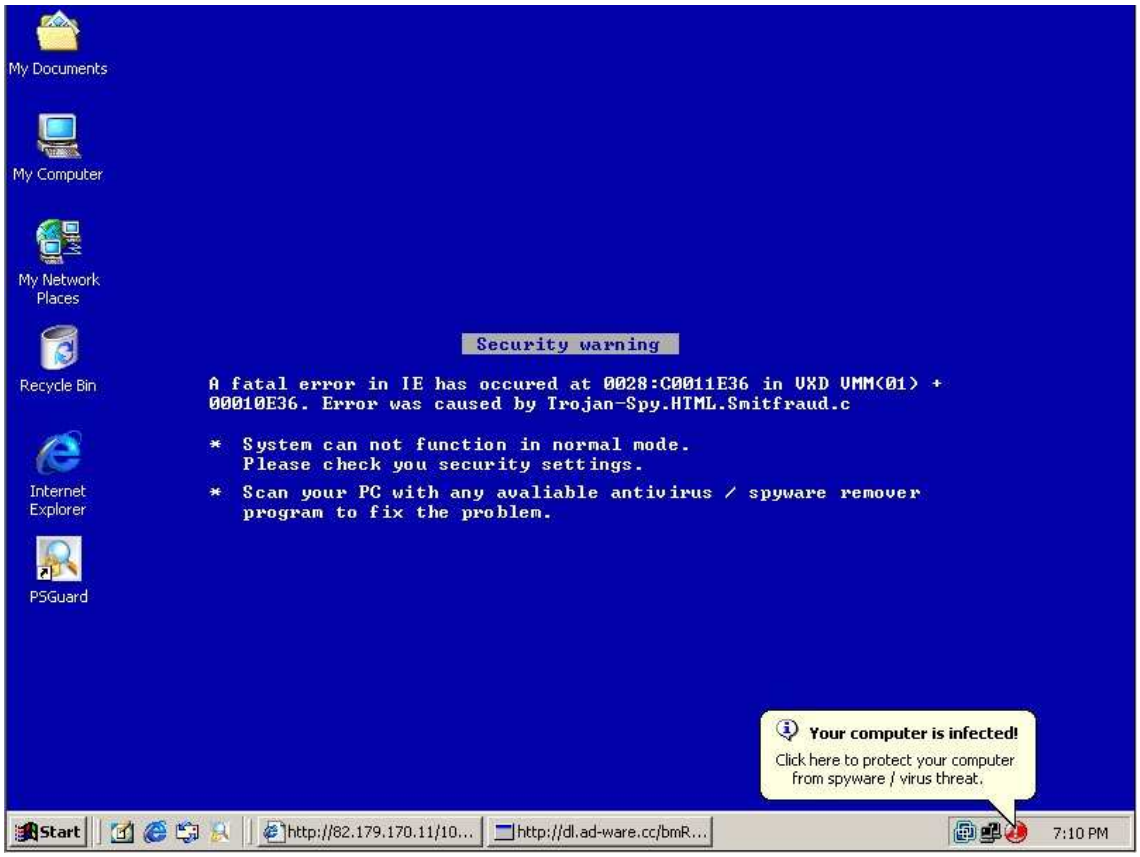
► 엔케이스(Win-Adware/nCase)

인터넷 무료 호스팅 서버를 이용한 ActiveX 형태로 설치되며 파일공유 프로그램, 무료게임 등의 번들로 설치되는 등 다양한 배포방법을 사용한다. URL에 포함된 주소나 키워드를 감시하여 180adsolution 관련 팝업광고를 노출한다.

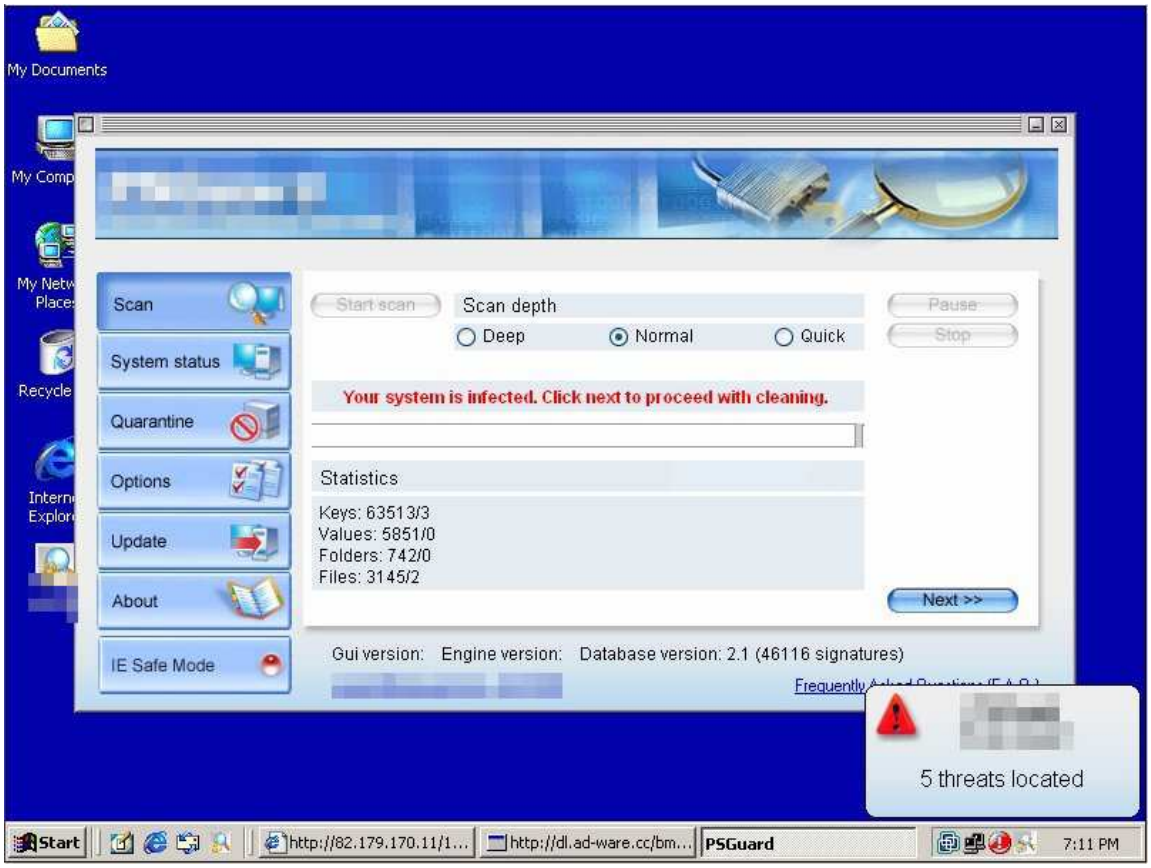
► 퓨리티스캔(Win-Adware/PurityScan)

성인사이트 광고를 통하여 설치되며, 2004년 초에는 유명 P2P 프로그램에 의해 번들된 형태로 설치되기도 하였다. 미디어티켓츠와 같은 다른 유해가능 프로그램에 의하여 설치되기도 한다. 사용자가 원하지 않는 팝업 광고를 노출하고 제어서버의 지시에 따라 다른 프로그램을 다운로드하고 설치할 수 있다. 사용자 시스템 정보를 제어서버에 전송하는 사생활 침해 기능도 가지고 있다.

애드웨어나 스파이웨어에 의해 설치되는 안티 스파이웨어 프로그램이 늘어난 것도 6월 스파이웨어 동향의 또 다른 특징이다. 스파이웨어에 의해 브라우저 보안설정이 변경되고 스파이웨어가 감염되었다는 팝업 메시지 또는 바탕화면 변경을 통한 전형적인 유해가능 프로그램 감염 증상을 보여주며, 사용자 동의 없이 설치된 안티 스파이웨어 프로그램이 실행되면 검사결과–허위검사 결과를 보여주는 경우도 있다-를 보여주고, 치료 시 과금을 유도한다. 이러한 안티 스파이웨어 프로그램은 유해가능 프로그램의 검출기능이 떨어지는 것이 보통이다.



[그림2] 스파이웨어에 의한 바탕화면의 변경



[그림3] 윈도우 시작 시 스파이웨어가 설치한 안티 스파이웨어 프로그램이 자동으로 실행

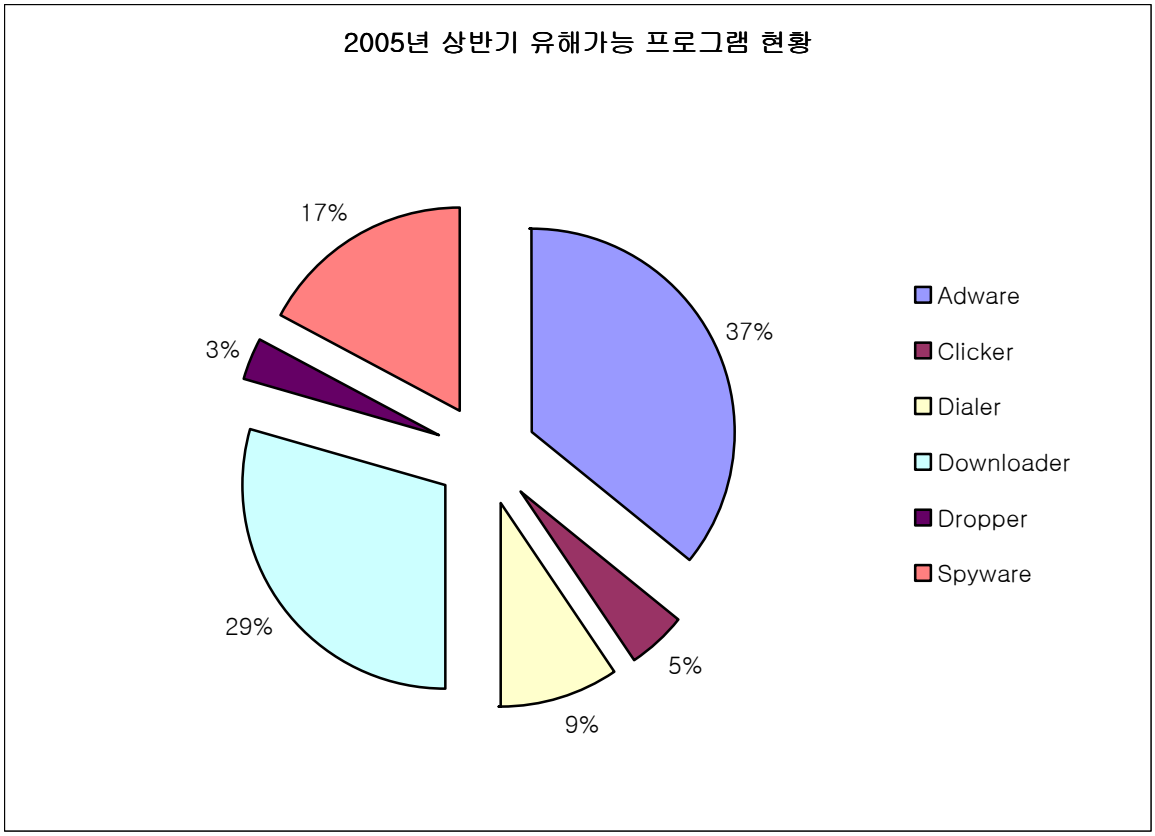
2005년 상반기 동향

2005년 상반기에는 직간접적으로 금전적인 이윤추구를 목적으로 하는 애드웨어와 스파이웨어의 제작과 배포가 크게 늘어났으며, 그 중 광고목적으로 제작된 애드웨어가 전체 유해 가능 프로그램의 약 37%로 큰 비중을 차지하고 있다. 웜이나 바이러스와 같은 전통적인 악성코드와 달리 애드웨어/스파이웨어와 같은 유해 가능 프로그램은 제작, 배포에 관한 법률적인 처벌 근거가 미비한 실정이었으나 최근에는 국내외적으로 무분별한 광고나 사생활을 침해하는 유해가능 프로그램에 대한 법률적인 처벌 근거를 만들기 위한 노력이 활발히 이루어 지고 있다.

유해가능 프로그램의 수적인 증가와 함께 악성코드에서 사용되는 다양한 기법이 애드웨어나 스파이웨어에도 사용되고 있다. IE 보안 취약점을 이용하여 사용자가 특정 웹 페이지를 방문하는 것 만으로 여러 가지 유해가능 프로그램이 설치되기도 하며, 안티 스파이웨어 프로그램의 검출을 피하기 위하여 임의의 이름을 사용하거나 루트킷[1]으로 불리우는 은폐기법을 사용

[1] 루트킷(Rootkit)
루트킷은 악의적인 목적으로 자신의 존재를 은폐하는 프로그램 또는 프로그램 도구이다. 바이러스, 트로이목마, 스파이웨어와 같은 악성코드가 사용자로부터 자신의 존재를 은폐하고 안티 바이러스 또는 시스템 관리 프로그램으로부터의 검출을 피하기 위해서 루트킷을 이용하기도 한다. 크게 커널모드(Kernel-mode), 유저모드(User-mode) 루트킷으로 나뉘며, 일반적으로 커널모드 루트킷이 검출과 제거가 더 어렵다.

하는 스파이웨어가 많이 발견되었다.



[그림3] 2005년 상반기 스파이웨어 유형별 현황

III. 6월 시큐리티 동향

작성자: 이정형 주임연구원(jungh@ahnlab.com)

벌써 2005년의 절반이 지나가고 있다. 시간은 화살처럼 빠르게 지나가고, 보안 분야는 방패와 창의 싸움이 늘 끊이지 않고 있다. 먼저 6월의 시큐리티 동향을 살펴보고, 2005년 상반기의 보안 동향을 살펴보기로 하자.

6월에 발표된 보안 취약점 동향

이번 달에는 마이크로소프사의 6월 정기 보안 패치가 총 10개 발표되었다. 6월달의 마이크로소프트사 정기 보안 패치는 지난 5월에 중요 등급에 해당하는 패치가 1개만 발표되었던 것에 비하면 많은 수가 업데이트되었다. 이 중에서 긴급에 해당하는 것이 3개 (MS05-025, MS05-026, MS05-027), 중요등급에 해당하는 것이 4개(MS05-029, MS05-030, MS05-031, MS05-032), 보통등급에 해당하는 것이 3개 (MS05-032, MS05-033, MS05-034)이다.

위험 등급	취약점	공격코드 유/무
HIGH	Internet Explorer 누적 보안 업데이트 (MS-0525)	무
HIGH	HTML 도움말의 취약점으로 인한 원격 코드 실행문제 (MS05-26)	무
HIGH	서버 메시지 블록의 취약점으로 인한 원격 코드 실행문제 (MS05-027)	무
MID	Outlook Express 누적 보안 업데이트	무

[표1] 6월의 주요 취약점 현황[1]

► 마스터, 비자카드 회원 개인정보 유출 사건

마스터, 비자카드 등의 고객정보를 담당하고 있는 카드 시스템스솔루션스사가 작년에 크래커로부터 공격을 당해 4,000만명 이상의 카드 사용자 정보가 노출이 된 것을 6월에 와서야 알게 되었다고 발표하였다. 이 여파에 의해 세계 각국에서 미국을 통해 물품을 구입한 경우에 피해를 입었을 가능성이 크다. 일본에서만 1000건, 1억엔 이상의 피해가 발생하였다. 우리나라는 아직까지 피해가 없는 것으로 밝혀졌지만 해당 카드 사용자들의 주의가 요구된다.

[1] 취약점 현황은 ASEC의 보안전문가들에 의해 공격코드 유/무, 악성코드 활용가능성, 취약점의 위험도등 다양한 관점에서 판단하여 선별된 것으로, 사용자들의 주의가 필요한 것임을 나타낸다. 공격코드의 존재유무는 이 리포트를 작성하는 시점에서 인터넷 상에서 접할 수 있는 기준으로 작성되었다

► **국내 유명 사이트에 대한 해킹 지속**

국내에 중국 크래커로 추정되는 사람에 의해 다수의 국내 사이트가 해킹을 당한 사고가 발생을 하였다. 또한 몇몇 사이트들은 다시 크래킹을 당하는 수모를 겪기도 하였다. 크래킹을 당한 사이트에는 해당 웹페이지에 악성코드를 넣어두고, 방문자가 해당 사이트 접속시 정보를 유출시키는 트로이목마가 자동으로 설치가 되며, 게임 사이트 접속 시 아이디와 패스워드를 특정 크래커에게 발송되게 된다. 이것은 게임 시에 사이버머니나 아이템 탈취를 위해 발생이 된 것으로 여겨지며, 개인 사용자들은 인터넷 이용 시 신뢰되지 않는 사이트에는 접속을 하지 말며, 반드시 인터넷 익스플로러 보안패치 및 AV 제품사용이 필요하다.

2005년 상반기 시큐리티 동향

취약점이 결합된 웜에 의한 보안 사고가 작년에는 많이 발생하였지만, 올해는 웹을 이용한 공격이 증가하였다. 특히 Web Attack은 예전부터 늘 문제가 되고 있다. 지난 6개월을 돌이켜보면, 1월에는 국내의 홈페이지가 대량 변조 당하는 사건이 발생하였고, 최근에는 국내 유수 업체들의 홈페이지가 해킹을 당하여, 게임사이트에 접속하는 정보를 훔쳐가는 악성코드가 발견되기도 하였다. 상반기의 다른 이슈로는 2월에 라우터(주니퍼, 시스코)쪽의 결함 소식과, 3월의 봇넷 증가 소식, 4월에 IE 보다 안전한 것으로 여겨진 파이어폭스의 취약점 소식, 5월에 Intel CPU의 HTT(Hyper Threading Technology)결함으로 인한 메모리 상에서 개인정보 유출 가능성, 6월엔 신용카드 업체가 해킹을 당해서 4천만명의 고객 개인정보가 유출이 된 사건 소식이 있었다.

SANS(www.sans.org)에서는 매년 그 해에 영향을 크게 미친 보안 취약점등에 대해서 Top 10 취약점 리스트를 발표하였지만, 올해부터는 보안 동향의 신속성을 위하여, 상반기, 하반기의 매 분기로 나누어 리스트를 공개하고 있다. 지난 6월 2005 년 상반기 Top 20 취약점 리스트[1]를 발표하였는데, 윈도우 취약점 및 리눅스/유닉스 등의 크로스 플랫폼 취약점을 함께 다루고 있다. 해당 리스트는 아래 표와 같다.

위험 등급	상반기 윈도우 취약점	공격코드 유/무
HIGH	윈도우 라이센스 로깅 서비스 오버플러우 (MS05-010)	유
HIGH	마이크로소프트 서버 메시지 블록(SMB) 취약점(MS05-011)	유

[1] SANS의 2005년 상반기 Top 20 취약점 리스트:
http://www.sans.org/top20/Q1-2005update/

HIGH	인터넷 익스플로러 취약점 (MS05-014 와 MS05-008) – 스파이웨어에서 많이 사용이 되고 있음	유
HIGH	마이크로소프트 HTML 헬프 ActiveX 컨트롤 크로스 도메인 취약점 (MS05-001) – 트로이목마에서 사용	유
HIGH	마이크로소프트 DHTML 에디트 ActiveX 원격실행 취약점 (MS05-013)	유
HIGH	마이크로소프트 커서, 아이콘 핸들링 오버플러우 (MS05-002) – 스파이웨어에서 많이 사용하고 있음	유
HIGH	마이크로소프트 PNG 파일 프로세싱 취약점 (MS05-009)	유

[표2] 상반기 주요 윈도우 취약점(출처:SANS)

위험 등급	크로스 플랫폼(Cross-Platform) 취약점	공격코드 유/무
HIGH	CA 라이센스 매니저 버퍼 오버플로우 (CAN-2005-0581, CAN-2005-0582, CAN-2005-0583)	유
HIGH	다양한 AV 제품의 버퍼 오버플로우 (CAN-2005-0249, CAN2005-0350, CAN-2005-0644)	유
HIGH	DNS 캐시 포이즈닝 취약점	유
HIGH	오라클 크리티컬 패치 업데이트 (CAN-2005-0298)	유
HIGH	다양한 미디어 플레이어들의 버퍼 오버플러우	무

[표4] 상반기 주요 비 윈도우 취약점(출처:SANS)

보안은 가장 작은 것을 소중히 여기는 데서 시작된다. 개인 사용자들은 해당 벤더의 보안패치를 정기적으로 체크하거나, 자동으로 업데이트 되게 설정해야 하며, 신뢰되지 않는 사이트로의 접속은 피하고, 꼭 필요한 보안제품(AV나 방화벽)은 사용하도록 하자.

Ⅳ. 6월 세계 악성코드 동향

2005년 6월 세계 악성코드 동향에서 가장 주목할 사항은 마이톱 웜의 확산이 크게 증가한 것이다. 마이톱 웜은 2005년 2월 말 최초로 발견된 이후 여러 형태의 변형들이 추가로 발견되고 있다. 마이톱 웜으로 인한 피해는 유럽에서 특히 심각한 상태이고 우리나라는 물론 일본과 중국에서도 이로 인한 피해가 점점 증가하고 있는 추세이다.
6월의 악성코드 동향과 관련하여 또 하나의 주목할 점은 모바일 기기에 전파되는 새로운 악성코드의 등장이다. 최근 발견된 모바일 웜인 콤워리어는 영국에서 최초로 발견된 이후 여러 국가들에서 지속적으로 발견되고 있으며 앞으로도 이러한 형태의 모바일 웜으로 인한 피해 사례는 계속 증가할 것으로 생각된다.

(1) 일본의 악성코드 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

개인 PC들간의 자료를 공유해 주는 파일교환 소프트웨어(이하 P2P 프로그램)는 다양한 정보를 쉽게 획득할 수 있다는 장점 때문에 많이 사용되고 있으나 이로 인한 피해 또한 심각한 상태이다.
정보 보안의 측면에서 볼 때 가장 문제가 되고 있는 것은 P2P 프로그램을 이용하여 악성코드를 유포하는 것이다. 일본의 경우 위니(Winny)라는 P2P 프로그램을 많이 사용하고 있으나 이 프로그램의 취약점을 이용하여 전파되는 안티니 웜(Win32/Antinny.worm)에 감염되어 개인 정보가 유출되는 사례가 빈번하게 발생하여 사회적인 이슈가 되기도 하였다.
일본 트렌드마이크로의 홈페이지에 발표된 감염 피해 바이러스 Top 10 정보에 의하면 안티니.A웜은 두 번째로 많이 퍼진 악성코드로 기록되어 있고 이외에도 2개의 안티니 웜 변형들이 포함되어 있는 것을 볼 수 있는데 이는 일본에서 P2P 프로그램으로 인한 피해의 정도를 알 수 있게 해 주는 단적인 예가 될 수 있을 것이다.
이러한 유형의 악성코드의 감염은 감염 자체로도 문제가 있지만 감염으로 인해 추가적으로 발생하는 피해가 더 심각하다.
안티니 웜의 경우 감염된 시스템에 설치된 P2P 프로그램의 설정을 변경하여 공유하지 않아야 할 데이터를 공유하게 만들거나 백도어를 설치하는 등 불법적인 형태로 사용자 데이터가 노출된 점이 일본 내에서 사회적인 이슈가 되었다. 기업에서 업무용으로 사용되는 시스템에서 이러한 P2P 프로그램을 사용하는 경우 보안 사고로 인한 기업 정보 유출의 가능성이 항상 잔존하고 있으므로 사용하지 않는 것이 바람직하고 방화벽과 같은 별도의 보안장비를 도입하여 이러한 프로그램의 사용을 막는 것이 피해 예방을 위해서 중요하다.

일본 유행 악성코드 유형별 발생현황

2005년 6월 한 달 동안 일본에서 발견된 악성코드 중 가장 많은 피해를 입힌 것은 넷스카이 웜(Win32/Netsky.worm)이다. [표1]은 일본의 정보처리추진기구(www.ipa.go.jp)에서 발

표한 6월 악성코드 피해 통계이다. 넷스카이 웜의 확산도는 전월과 비교해 보았을 때 크게 변화가 없는 상태이다. 다른 악성코드에 비해서 새로운 변형 발생횟수가 많지 않음을 고려해 보았을 때 넷스카이 웜의 감염 건수가 줄어들지 않는 것은 기존에 유포된 변형들의 확산도가 여전하기 때문으로 추정된다. 전월에 이어 6월에도 마이톱 웜(Win32/Mytob.worm)의 감염 피해가 증가하고 있는 것을 볼 수 있다. 마이톱 웜은 이메일과 네트워크를 통해 전파되는 악성코드로서 최근까지 여러 변형들이 발견되고 있다.

Window/Dos Virus	금월피해 전월피해	Macro Virus	금월피해 전월피해	Script Virus	금월피해 전월피해
Win32/Netsky	1,122 1,128	Xm/Laroux	8 21	VBS/Redlof	69 86
Win32/Mytob	699 584	X97M/Divi	8 3	VBS/Loveletter	13 7
Win32/Mydoom	352 446	XF/Sic	4 8	Wscript/Fortnight	11 6
Win32/Bagle	316 336	Tristate	3 3	VBS/Soraci	3 5
Win32/Lovgate	273 264	X97M/Cap	3 1	VBS/FreeLink	2 2
Win32/Klez	265 251	W97M/Marker	3 1	VBS/Netlog	2 2

[표1] 일본의 6월 악성코드 피해 신고 현황(출처: 일본 정보처리추진기구)

악성코드의 감염 경로별 통계

[표2]는 일본에서 발생한 악성코드의 감염 경로에 대한 통계이다. 악성코드의 감염 경로로 가장 많이 이용되는 매체는 메일로써 이는 전월과 비교해서 크게 차이가 없다.

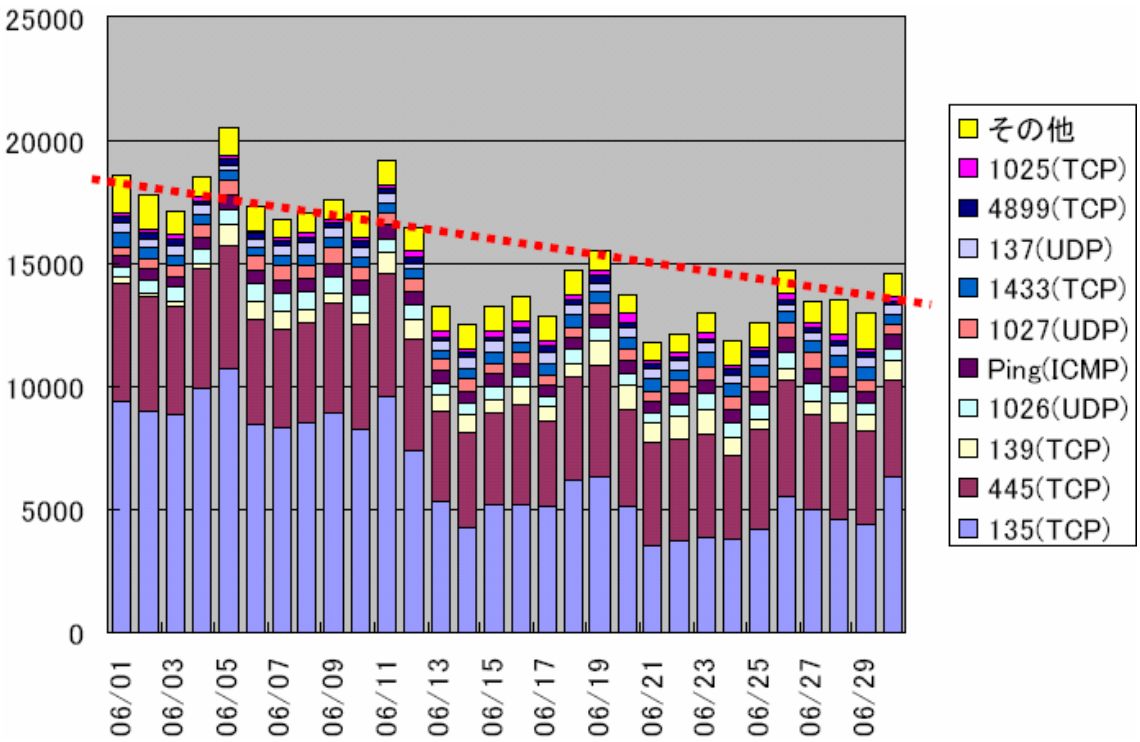
감염경로	피해 건수					
	2005년 6월		2005년 5월		2004년 6월	
메일	4,850	98.4%	4,943	98.4%	5,241	97.6%
외부의 매체	4	0.1%	2	0%	15	0.3%
다운로드	9	0.2%	5	0.1%	7	0.1%
네트워크	57	1.2%	59	1.2%	150	2.8%
기타	8	0.2%	12	0.2%	9	0.2%

[표2] 일본의 6월 악성코드 감염 경로 통계

일본 네트워크 트래픽 현황

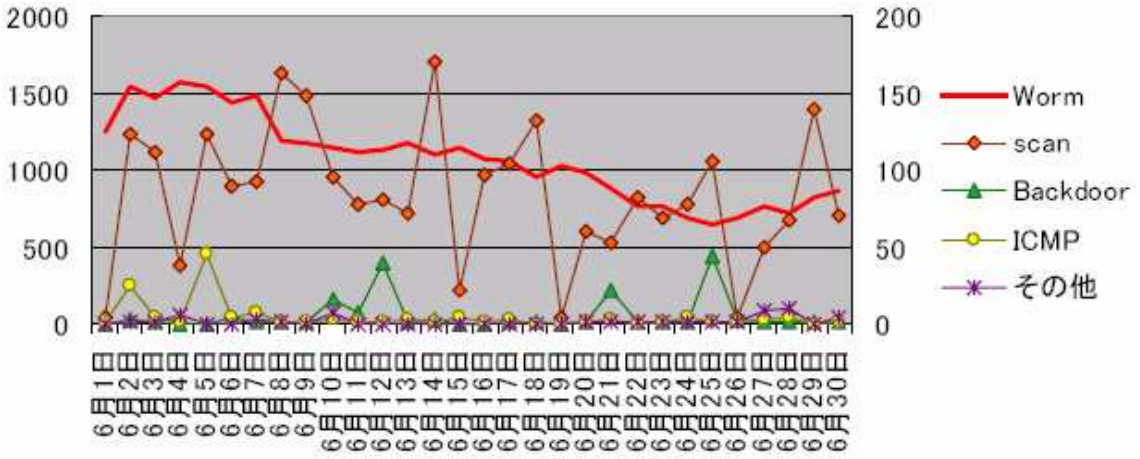
[그림1]은 2005년 6월 한 달 동안 발생한 네트워크 트래픽 사용량에 대한 정보이다. TCP

135 포트와 TCP 445 포트를 이용한 네트워크 트래픽이 매우 많은 것을 알 수 있다. 이 포트들은 윈도우 OS에서 인증을 위해 주로 사용되는 포트들이지만 아이알씨봇(IRCBot)과 같은 네크워크를 통해 전파되는 악성코드들에서 프로그램의 취약점을 이용하여 불법적으로 권한을 획득하고 자신을 복제하려는 시도를 하는 공격이 빈번하게 발생하므로 주의가 필요하다.



[그림1] 일본의 6월 네트워크 트래픽 현황

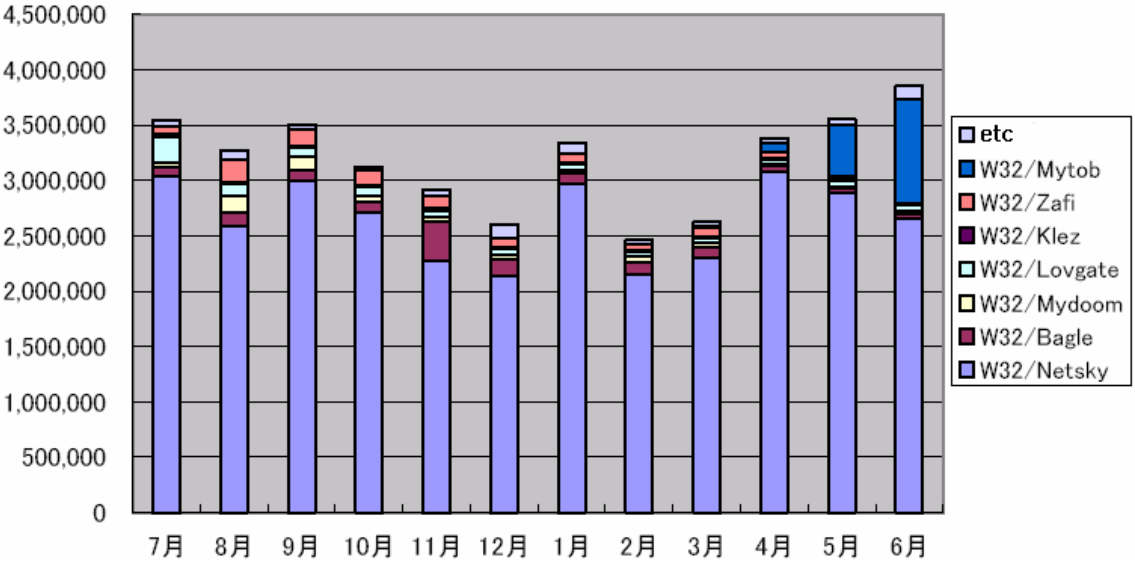
[그림2]는 일본 사이버폴리스(www.cyberpolice.go.jp)에서 발표한 공격 탐지 정보에 대한 통계이다. 웜에 의한 트래픽의 양이 매우 높은 것을 알 수 있다.



[그림2] 일본의 6월 공격 수법별 추이(출처: 일본의 사이버폴리스)

2005년 상반기 일본 동향

2005년 상반기 일본의 악성코드와 관련하여 가장 크게 이슈가 된 사건은 넷스카이 웜의 지속적인 확산과 마이톱 웜의 출현을 들 수 있다. [그림3]은 2005년 상반기 악성코드의 발견 통계이다.



[그림3]2005년 상반기 일본의 악성코드 발생 추이

[그림3]에서 볼 수 있는 것처럼 넷스카이 웜의 확산도가 가장 높은 것을 알 수 있다. 넷스카이 웜의 경우 처음 발견된 이후 여러 변형들을 유포하였고 현재까지도 그 영향력이 남아있는 상태이다.

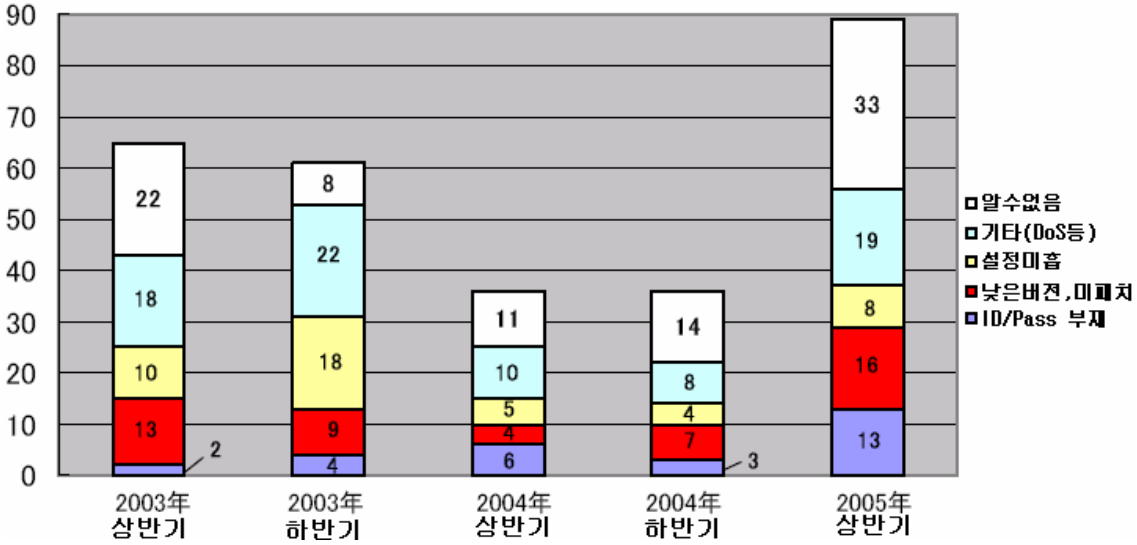
마이톱 웜은 2005년 2월 말 처음 발견된 이후 증가세를 보이지는 않았으나 5월에 들어오면서 여러 형태의 변형들이 발생하기 시작했고 현재도 이러한 증가세는 계속되는 추세이다.

이에 비해서 베이글 웜이나 마이둠 웜은 전년에 비해서 점차 감소세를 나타내고 있는 것을 알 수 있다.

[그림4]는 상반기에 발생한 보안 관련 피해 통계이다. 작년에 비해 보안 관련 피해가 매우 늘어난 것을 알 수 있다.

2005년 상반기에 주로 발생한 공격 형태는 과시를 위해 특정 사이트를 대상으로 공격을 시도했던 이전의 공격 형태에서 벗어나 피싱이나 키로거와 같이 개인 정보를 획득하여 이를 악용하려는 경향이 매우 강하게 나타나고 있다. 한국에서 특정 온라인 게임의 패스워드를 가로채기 위해서 제작된 백도어 프로그램이 무분별하게 제작되어 배포되는 것은 이러한 현상의 단적인 예이다.

이러한 현상은 개인과 기업의 정보 보호를 위한 대책을 세우고 이를 시행해야 할 필요성을 반증해 주고 있다.



[그림4] 일본의 2005년 상반기 보안 관련 피해 원인별 통계

(2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

6월 중국 악성코드의 동향은 여전히 백쯔 웜(TrojanDroper.Worm.Bagz, V3 진단명 Win32/Bagz.worm)이 가장 많은 분포를 차지하며 1위를 유지하고 있다. 그러나 지난 달부터 서서히 주간 악성코드 동향과 전체 분포면에서 감소 추세가 보이기 시작하여 6월에는 수치상으로는 현격하게 감소한 것으로 집계되었다. 그리고 지난 달 처음으로 순위에 등장한 마이톱 웜(Worm.Mytob, V3 진단명 Win32/Mytob.worm)이 한달 사이 급격히 증가한 것 역시 새로운 변화로 나타나고 있다. 지난 달부터 등장한 다양한 공격 형태의 트로이목마는 6월 역시 지날 달 보다 더욱 많은 새로운 형태의 트로이목마가 발견되었고, 이에 의한 피해가 예년에 비해 더 급증할 것으로 예상된다.

악성코드 TOP 5

순위 변화	순위	Rising
-	1	TrojanDroper.Worm.Bagz
↑ 3	2	Worm.Mytob
New	3	Backdoor.Rbot
New	4	Worm.Netsky
New	5	Backdoor.Gpigeon.5

[표1] 2005년 6월 라이징(Rising) 악성코드 TOP 5

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

순위 변화	순위	JiangMin
↑ 1	1	Trojan/QQMsg.Zigui.b
New	2	I-Worm/QQ.Porn
New	3	TrojanDownloader.Small.rn
New	4	Trojan/Script.Seeker
New	5	Backdoor/Jieba.2004

[표2] 2005년 6월 강민(JiangMin) 악성코드 TOP 5

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

[표1]과 [표2]는 중국 백신 업체인 라이징(Rising)과 강민(JiangMin)의 악성코드 TOP 5이다. 라이징의 순위를 참고로 할 경우에는 아이알씨봇(Backdoor.Rbot, V3 진단명 Win32/IRCBot.worm)과 넷스카이 웜(Worm.Netsky, V3 진단명 Win32/Netsky.worm)처럼 기존에 알려진 악성코드들이 순위권에 재진입한 것이 눈에 띈다. 순위권에 재진입한 것으로

미루어 수치상으로는 많지 않지만 중국 내에서는 아직까지 감염 활동이 지속적으로 이루어지고 있는 것으로 보여진다. 이번 달 순위상으로 가장 큰 변화를 이룬 것은 다양한 변형의 등장으로 전세계적으로 높은 감염 활동이 있었던 마이톱 웜(Worm.Mytob, V3 진단명 Win32/Mytob.worm)이다. 마이톱 웜은 지난 5월 통계에서는 5위로 최초 등장하여 이번 6월에는 3계단이 상승한 2위로 기록되었다. 이러한 순위상의 변화로 미루어 마이톱 웜은 중국 내에서도 많은 감염활동이 있는 것으로 분석된다. 5위로 새롭게 순위상에 진입한 그레이버드 트로이목마(Backdoor.Gpigeon.5, V3 진단명 Win-Trojan/GrayBird)는 중국 현지에서 제작된 백도어의 일종으로 감염된 시스템을 원격제어 하는 등 다양한 악의적인 기능들을 수행할 수 있다. 알려진 바로는 제작자는 원격제어 프로그램 형태로 개발하였으나 악의적인 크래커에 의해 이를 변형하여 사용되는 것으로 추정된다.

강민의 순위는 지난 5월과 비교하여 전체적인 순위상에서 많은 변화가 있었다. 지난 달 1위인 Trojan/QQMsg.Zigui.b를 제외하고는 2위에서 5위까지 모두 새롭게 순위에 진입한 악성코드들이다. 전체 순위만을 놓고 비교해 본다면 웜에 의한 감염 활동 보다는 트로이목마에 의한 감염 활동이 상대적으로 높다.

주간 악성코드 순위

순위	1주	2주	3주	4주
1	TrojanDroper.Worm.Bagz.d	Worm.Mytob	Backdoor.Rbot	Backdoor.Gpigeon
2	Trojan.PSW.Lmir	Trojan.Clicker.Agent	Worm.Mytob	Trojan.DL.Swizzor
3	Worm.Email.LovGate.af	Worm.Netsky	Backdoor.Gpigeon	Backdoor.Rbot
4	TrojanDroper.Worm.Bagz	Backdoor.Agobot	Worm.QQ.TopFox	Backdoor.Codbot
5	Worm.Netsky	Backdoor.WinterLove	TrojanDroper.Worm.Bagz	Worm.QQ.TopFox

[표3] 2005년 6월 라이징(Rising) 주별 악성코드 순위

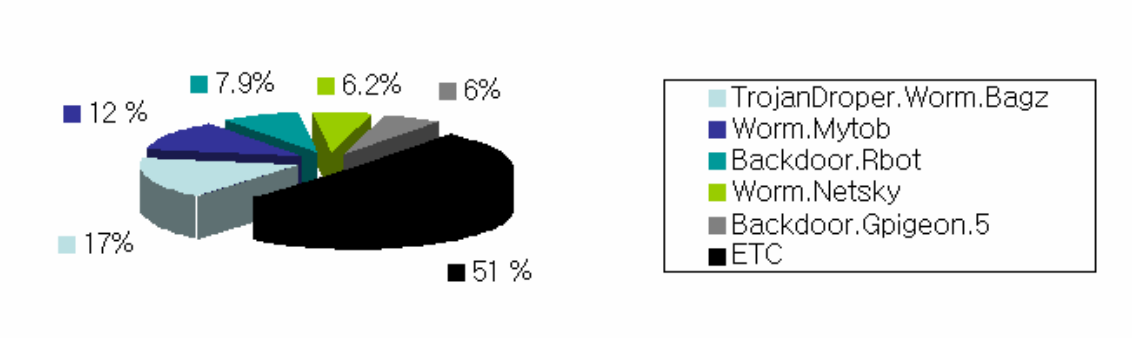
순위	1주	2주	3주	4주
1	Trojan/QQMsg.Zigui.b	Adware/ToolBar.Iebar.c	Adware/ToolBar.Iebar.d	Trojan/QQMsg.Zigui.b
2	TrojanDownloader.Small.rn	Adware/ToolBar.Iebar.d	Adware/ToolBar.Iebar.c	I-Worm/QQ.Porn
3	I-Worm/QQ.Porn	Trojan/QQMsg.Zigui.b	Trojan/QQMsg.Zigui.b	Backdoor/Rootkit.Fu
4	Backdoor/SdBo	I-Worm/QQ.Porn	Trojan/PSW.Mir7	Trojan/Script.See

	t.atp.Rootkit		005.cf.b	ker
5	TrojanDownloader.Small.ore	TrojanDownloader.Small.rn	I-Worm/QQ.Porn	Backdoor/Jieba.2004

[표4] 2005년 6월 강민(iangMin) 주별 악성코드 순위

[표3]과 [표4]는 중국 백신 업체인 라이징(Rising)과 강민(JiangMin)의 주간 악성코드 순위이다. 먼저 [표3]의 라이징 주간 악성코드 순위의 눈에 띄는 변화로는 넷스카이 웜, 마이톱 웜과 그레이버드 트로이목마이다. 넷스카이 웜의 경우 6월 1주차부터 2주차 까지는 지속적인 증가를 보였으나 3주차에 이르러서는 다시 순위 권 밖으로 밀리는 현상을 보였다. 이에 반해 마이톱 웜의 경우에는 2주차에 주간 순위 1위로 등장하여 3주차에서는 2위로 밀린 후 다시 4주차에서는 순위 권 밖에 밀려났으며 그레이버드 트로이목마의 경우에는 3주차에 처음 등장하여 4주차에서는 주간 순위 1위를 차지할 정도로 증가세 보이고 있다. 다음 7월에는 그레이버드 트로이목마가 어떠한 변화를 이어나가게 될지 그리고 어떠한 트로이목마가 새롭게 등장할지 주목된다.

악성코드 분포



[그림1] 2005년 6월 라이징의 악성코드 분포

전체 악성코드 분포는 이제까지 악성코드 분포와 다른 형태를 보이고 있다. 월간 악성코드 TOP 5에 포함되지 않을 정도로 감염 활동이 미비한 트로이목마들이 대거 등장한 것이다. 이로 인해 전체 악성코드 분포에서 기타에 포함되는 악성코드가 전체의 절반이 넘는 51%를 차지하고 있다. 여기에 포함되는 트로이목마들은 감염 신고가 대부분이 1자리 수를 차지할 정도로 피해건수는 미미하다. 여기에 포함되는 대표적인 악성코드로는 엘미르 트로이목마(Trojan.PSW.Lmir, V3 진단명 Win-Trojan/LmirHack), 윈터러브 트로이목마(Backdoor.WinterLove, V3 진단명 Win-Trojan/WinteLove) 등이 있다. 이러한 트로이목마들의 공통적인 특징은 웜과 달리 급격한 확산을 목적으로 하는 것이 아니라 개인 정보와 중요 데이터 유출이 주목적을 이루고 있다. 지난 6월에 발생한 온라인 뱅킹 사건에 이용된 악성코드 역시 사용자가 입력하는 키보드 입력 값을 외부로 유출하는 키로깅 기능을 가지고 있는 트로이목마였던 만큼 이에 대한 각별한 주의가 필요하다.

2005년 상반기 중국 동향

2005년 벌써 절반이 지난 7월에 이르렀다. 지난 상반기 중국의 악성코드 흐름을 이야기 한다면 단연 메일로 전파되는 매스메일러가 강세였다고 볼 수 있다. 그러나 이러한 흐름도 시간이 흐르면서 다시 트로이목마의 강세로 이어지고 있다. 그렇다면 월별로 어떠한 악성코드가 발견되어 피해가 발생하였는지 한번 살펴보도록 하자.

월	1월	2월	3월
	TrojanDroper.Worm.Bagz	Worm_Bropia.F	TrojanDroper.Worm.Bagz
월	4월	5월	6월
	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz

[표1] 2005년 상반기 라이징(Rising) 월별 악성코드

[표1]은 중국 백신 업체인 라이징(Rising)의 월별 악성코드 TOP 5 중 1위를 차지한 악성코드를 나타낸 것으로, 중국 악성코드의 상반기 동향은 백쯔 웜의 감염 활동이 절대적이었던 것으로 분석된다. 백쯔 웜은 메일로 전파되는 특성으로 인해 단시간에 많은 감염 활동이 있었다.

월별로 어떠한 악성코드의 흐름이 있었는지 살펴 보도록 하자. 1월에는 새로운 베이글 웜(Worm_Bbeagle, V3 진단명 Win32/Bagle.worm)의 변형 발견으로 인하여 2004년과 같이 매스메일러들의 급격한 증가에 따른 많은 피해가 발생할 것으로 예상되었다. 그러나 2월에는 매스메일러에 의한 피해가 증가하기 보다는 MSN 메신저를 이용하여 확산되는 브로피아 웜(Worm.MSN.Bropia, V3 진단명 Win32/Bropia.worm)의 갑작스런 등장으로 인해 많은 피해가 있었다. 브로피아 웜은 MSN 메신저를 이용하여 친구목록에 등록된 모든 사람들에게 악성 아이알씨봇 웜을 다운로드하는 링크를 발신하여 브로피아 웜에 의한 피해와 함께 악성 아이알씨봇 웜에 의해 피해도 같이 증가하게 되었다. 3월에는 기존 백쯔 웜과 악성 아이알씨봇 웜의 영향력이 다시 증가하였다. 그러나 이와 함께 스타트페이지 트로이목마(Trojan.Win32.StartPage, V3 진단명 Win-Trojna/Starepage)가 서서히 증가하기 시작하여 중국 내에서도 애드웨어와 스파이웨어의 위협이 본격적으로 진행되기 시작한 것으로 분석된다. 4월에는 백쯔 웜이 여전히 순위상으로는 1위를 차지하고 있지만 서서히 감염 활동이 감소하고, 다양한 공격 기법과 감염 기법을 가진 트로이목마가 서서히 증가하고 있었다. 이로 인해 트로이목마가 웜보다 더 많은 수치를 차지하기 시작하여 트로이목마에 의한 피해가 증가하였다. 5월에는 전세계적으로 다양한 변형들에 의한 피해가 발생하였던 마이톱 웜의 피해가 중국에서도 서서히 증가하여 백쯔 웜 만큼 많은 감염 활동을 보이기 시작하였다. 그리고 4월에 이어 다양한 트로이목마들이 지속적으로 발견되고 있었다. 6월 역시 마이톱 웜의 급격한 감염 활동 증가와 함께 그레이버드 트로이목마와 같은 원격제어 형태의 트로이목마의 감염 활동이 증가하기 시작하여 개인 정보 유출 등의 피해가 우려되었다.

(3) 세계 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

영국의 소포스(Sophos) 통계를 보면 2005년 6월은 상당수의 새로운 악성코드가 순위에 올랐다. 거의 일년 가까이 상위권에 존재하던 넷스카이 웜(Win32/Netsky.worm), 자피 웜(Win32/Zafi.worm)이 조금씩 순위가 떨어졌다. 특히 자피.D 웜의 순위가 2위에서 8위로 급격히 떨어지고 대부분의 자리를 마이톱 웜 변형(Win32/Mytob.worm)이 차지했다.[1] 러시아의 캐스퍼스키 연구소(Kaspersky) 통계 역시 마이톱 웜의 변형들이 순위에 진입했다.[2] 핀란드의 F-시큐어(F-Secure)사는 휴대폰 악성코드인 콤워리어(Commwarrior)가 영국에서 발견되어 전세계 15개국에서 발견되었다고 보고했다.[3] 모바일 악성코드는 꾸준히 발견되고 있으며 조금씩 전세계로 퍼져나가고 있는 것으로 보인다.

2005년 상반기를 정리하면 자피.D 웜과 넷스카이 변형이 압도적으로 1, 2위를 차지하고 있다. 이는 상반기에 이들 웜의 강세가 컸기 때문으로 보고 있다. 소포스는 상반기 동안 7,944개의 새로운 악성코드를 발견했으며, 작년 대비 59%의 증가를 보이고 있다고 보고했다.[4] 악성코드의 수치는 계속 증가 중이며 작년 이후 악성코드와 스파이웨어 등의 각종 보안 위협이 증가하면서 폭발적인 증가세는 계속 될 것으로 예상된다.

[1] http://www.sophos.com/pressoffice/pressrel/uk/20050701topten.html
[2] http://www.viruslist.com/en/analysis?pubid=166511024
[3] http://www.f-secure.com/weblog/archives/archive-062005.html
[4] http://www.sophos.com/pressoffice/pressrel/uk/midyearroundup2005.html

V. 이달의 ASEC 컬럼 - 인터넷 뱅킹 사고

작성자 : 차민석 주임연구원(jackycha@ahnlab.com), 양하영 연구원(hyyang@ahnlab.com)

2005년 6월은 인터넷 뱅킹 사고로 떠들썩했다. 한 초보 해커가 오래된 백도어를 이용해 인터넷 뱅킹으로 돈을 인출한 사건이 발생한 것이다. 인터넷 뱅킹 사건과 풀어야 할 문제에 대해 알아보겠다.

인터넷 뱅킹 사고

2005년 6월 초 한 은행의 인터넷 뱅킹 시스템이 해킹을 당해 고객의 예금이 인출되는 사건이 처음으로 발생했다. 해커는 PC방에서 인터넷 카페에 재테크와 관련된 글을 올리고 해킹 프로그램을 설치하도록 하였다. 피해자는 해킹 프로그램을 재테크와 관련된 프로그램으로 생각하고 자신의 컴퓨터에 설치하였다. 해커는 이 해킹 프로그램을 통해 피해자의 인터넷 뱅킹 접속 정보를 알아낸 뒤 통장에서 5천만원을 인출했다.

해킹 방식

해커가 사용한 해킹 프로그램은 넷데블(Win-Trojan/NetDevil)로 알려져 있으며 이 프로그램은 2002년에 발견되었고 대부분의 백신 프로그램에서 이 프로그램을 진단 할 수 있다. 해킹 프로그램은 피해자의 컴퓨터에 설치된 뒤 피해자가 인터넷에 접속하면 입력한 키보드 정보를 실시간으로 가로채는 `키 스트로크(key stroke)' 방식을 사용했다. 이를 통해 해커는 인터넷 뱅킹에 사용하는 아이디, 패스워드, 특정 번호의 보안카드 코드표를 알아냈다.
일반적인 경우, 해커가 사용자의 아이디와 패스워드 정보를 알아냈다 할지라도 인터넷 뱅킹 시 사용하는 보안카드의 3-4자리 숫자는 수십 개의 숫자 중 매번 요청하는 번호가 다르기 때문에 피해가 발생하기 어렵다. 또한, 연속적으로 3회 이상 틀린 번호를 입력할 경우 해당 은행을 직접 방문하여 새로운 보안카드를 발급받아야 거래가 가능하다. 하지만, 이번 사건의 경우, 해커는 한 두개의 보안카드 번호를 알아낸 뒤 반복적인 로그인/로그아웃 수행을 통해 인출에 성공했을 것으로 보인다. 피해 발생 후 해당 은행은 잘못된 번호 입력 시 로그아웃 후에도 틀린 보안카드 번호 입력 횟수 정보를 유지하여 반복적인 작업으로 피해가 발생하는 것을 막도록 조치하였다. 또한, 해당 은행 사이트에 접속 시 키보드 보안 프로그램이 자동 설치되도록 하여 사용자가 입력한 키보드 정보가 유출되는 것을 방지하였다.

상용 키로거

인터넷 뱅킹 사고 이후 인터넷 뱅킹이 과연 안전한가에 대한 의문이 제기되었다. 이에 몇몇 전문자들이 인터넷 뱅킹의 안전성에 대해 문제가 있다고 밝혔다. 모 시사 프로그램에서는 키로거 프로그램을 이용해 인터넷 뱅킹시 입력하는 로그인 정보와 보안 카드 번호를 알아냈다. 이때 사용한 프로그램은 상용 키로거 프로그램으로 알려져 있으며, 상용 키로거는 자녀나 직원의 컴퓨터 사용 내역을 확인하기 위해 사용되는 정상프로그램이다. 상용 키로거는 감시 당

하는 사람 모르게 실행되어야 하므로 사용자로부터 자신의 존재를 숨기는 등의 기능을 가지고 있는 것이 많다. 또 키로거 기능을 막는 안티 키로거 프로그램에 대해서도 대비가 되어 있는 경우가 많다. 따라서 이런 프로그램을 악용할 경우 다른 사람의 계정, 비밀번호나 신용카드 번호 등 개인 정보를 유출할 수 도 있다.

안철수연구소 대응

안철수연구소는 상용 키로거의 악용이 우려되어 사용자 선택 시 상용 키로거를 Win-AppCare/Keylogger로 진단하고 있다. 하지만, 진단하는 제품이 상용 제품이라는 것과 '해당 상용 제품을 정상적으로 사용하는 사용자의 혼란을 어떻게 해결해야 하는가' 하는 문제가 남는다. 인터넷 뱅킹을 이용하는 사람들 중 대부분은 보안에 대한 지식이 없는 사람들이며 보안 프로그램에서 어떤 프로그램이 위험하다고 했을 때 해당 프로그램의 정확한 용도를 모르는 경우가 대부분이며 이때 그냥 무시하거나 반대로 지나치게 겁을 먹을 수도 있다.

사건을 정리하며

기술적으로 세상에 완벽한 보안은 있을 수 없다. 다만 보안 제품과 이용자의 보안 수칙 실행으로 보다 안전한 컴퓨터 이용을 할 수 있다. 이번 사건에 이용된 해킹 프로그램도 기존 보안 프로그램에서 막을 수 있었지만 사용자가 보안 제품을 사용하지 못한 점, 사용자 불편을 우려해 강제로 보안 프로그램을 사용하지 않게 하고 허점이 존재한 인터넷 뱅킹 시스템이 함께 만들어낸 사고였다. 사건 이후 은행에서는 사용자 편리성보다 보안을 보다 우선시할 계획이라고 한다. 하지만, 강화된 보안은 사용자의 불편을 야기하므로 은행과 보안 업체도 보안 수준에 고민을 가지고 있다. 특히 상용 키로거와 원격 제어 프로그램을 보안 프로그램에서 진단할 경우 발생하는 고객 혼란도 만만치 않을 것으로 보인다. 이외 별도의 인증 방법, 일회성 비밀 번호 등 다양한 보안 방안이 논의되고 있다.

인터넷 금융거래 보안수칙 10계명

완벽한 보안은 없다. 그러나 다음의 10가지 보안수칙을 습관화하여 이행한다면 인터넷 금융거래 시 발생할 수 있는 보안사고를 최소화할 수 있을 것이다.

1. 출처가 불분명한 이메일이나 첨부파일은 열지 말고 삭제하기

이메일 확인 시 발신인이 불분명하거나 수상한 첨부 파일은 열지 말고 모두 삭제한다. 무심코 확인하는 과정에서 바이러스, 웜, 트로이목마 등에 감염될 수 있다.

2. 보안 프로그램의 설치 및 활용하기

인터넷 금융거래에 이용하는 PC에 백신 프로그램 및 PC 방화벽을 설치하고 실시간 감시 기능을 활용하여 해킹 및 바이러스 등의 보안위협에 대비하도록 한다. 또한 자동 업데이트 기능을 이용하여 최신 엔진으로 항상 업데이트해 놓아야 한다.

3. 안전하지 않은 PC에서 인터넷 금융거래 이용하지 않기

PC방 등 누구에게나 개방된 컴퓨터에서는 가급적 인터넷 금융거래를 하지 않도록 한다. 그러나 부득이하게 PC방 등 개방된 컴퓨터에서 사용해야 경우에는 백신 및 PC방화벽이 설치 실행되는 곳에서만 이용한다.

4. 비밀번호는 영문, 숫자 등의 조합으로 6자리 이상 설정하고 주기적으로 변경하기

로그인 계정의 비밀번호는 영문/숫자/특수문자 조합으로 6자리 이상으로 설정해야 하며 주기적으로 변경해 사용하는 습관을 갖는다. 타인이 쉽게 추정할 수 있거나 영문으로 유추하기 쉬운 단어를 사용해서는 안 된다. 타인이 쉽게 추정할 수 있는 비밀번호의 사용 예로는 주민등록번호, 전화번호, 생일날짜, 차량번호 등의 개인 정보를 들 수 있다.

5. 최신 윈도우 보안패치 적용하기

윈도우 운영체제 사용자는 최신 윈도우 보안 패치를 모두 설치해야 한다.

6. 피싱(Phishing) 사기 이메일 조심하기

개인정보, 계좌정보 등을 요구하는 수상한 이메일의 경우 신종 금융사기 수법인 피싱(Phishing)을 먼저 의심해 각별한 주의를 해야 한다. 금융기관으로부터 개인정보, 계좌정보 등의 업데이트나 정보 변경을 요구하는 이메일을 받으면 클릭하지 말고 해당 금융기관 사이트에 가서 직접 확인해야 한다.

7. 수상한 사이트는 방문하지 않고 안티 스파이웨어 사용하기

믿을 수 없는 사이트는 방문하지 않으며 수상한 프로그램을 다운로드 하지 말아야 하며 자신의 PC는 주기적으로 스파이웨어 검사를 실시해 깨끗이 사용해야 한다.

8. 인터넷 금융거래와 계좌 비밀번호 별도 적용하기

인터넷 금융거래 비밀번호와 계좌 비밀번호는 반드시 다르게 사용해야 한다.

9. 불법복제 프로그램 사용하지 않기

바이러스나 해킹의 위험에 노출되기 쉬운 불법복제 프로그램은 사용해서는 안 된다.

10. 메신저로 자료 교환 시 백신으로 검사하기

메신저나 P2P 프로그램을 통한 자료 교환 시 바이러스 등 악성코드 감염 파일이 전달될 수 있으니 백신 프로그램으로 감염 여부를 반드시 검사한 후 이용해야 한다.

안전한 인터넷 금융거래를 위해서는 금융기관 및 쇼핑몰 등 업체들의 보안 강화는 물론 개인 사용자들도 보안수칙을 준수하는 등 각별한 주의가 필요하다. 금융거래 보안수칙을 꼭 지켜 자신의 소중한 자신을 안전하게 관리해야 할 것이다.