ASEC Report 7월

® ASEC Report

2005. 08

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…

7월에는 트로이목마의 발견과 피해가 지속적으로 증가하였다. 7월 악성코드 피해건수는 전월에 비해 소폭 감소하였으며, 피해신고 된 악성코드 수는 2005년 중 가장 적은 수가 접수되었다. 이는 전체적으로 ircbot과 mail로 전파되는 웜의 주춤한 것과 여름 휴가철의 시작으로 컴퓨터 사용률의 부분적인 감소로 인한 일시적인 현상으로 판단된다. 그러나, 트로이목마가 다양한 취약점을 이용하여 전파되어 전파속도가 빨라 웜에 비하여 상대적으로 피해 규모가 커지고 있는 상태이다.

7월 피해신고 된 악성코드의 감염유형별 현황을 살펴보면 네트워크 취약점을 이용한 것과 메일을 이용한 것의 비율이 4:6의 비율인 것을 확인할 수 있다. 7월 신종(변형)발견 수치도 ircbot의 감소로 인하여 일시적으로 하락하였으며, 이례적으로 바이러스에 의한 피해가 발생하였는데 7월 중순 이후 급속히 확산되었던 Tenga 바이러스가 있었다. 신종(변형)발견도 피해신고와 마찬가지로 트로이목마의 발견이 강세를 보이고 있어, 전체 발견된 신종(변형) 중 45%를 트로이목마가 차지하고 있다. 세계적으로는 넷스카이 웜의 확산이 눈에 띈다. 새로운 변종이 발견되지 않았음에도 여전히 강세를 보이고 있는 것은 넷스카이 웜의 강력한 전파력을 반증하는 것이다. 캐스퍼스키 연구소에서 발표한 악성코드 종류별 증가 추이를 보면 2003년과 2005년을 비교하여보면 트로이목마류는 6배, 휴대장비를 대상으로한 악성 코드는 5배, 유닉스용 악성코드는 약 3배 가량 증가하였다.

7월의 스파이웨어 동향은 다운로더가 다소 감소하고 애드워어가 약 34%를 차지한다. 국내에서 한글 인터넷 키워드 서비스를 제공하는 D사에서 안철수연구소를 상대로 스파이제로 판매 금지 가처분 소송을 내었으나, 기각되었다. 이는 국내외에 스파이웨어에 대한 정확한 기준이 없는 상태에서 신종 악성 프로그램인 스파이웨어에 대한 기준 정립 및 규제 기준 마련의 계기가 될 것으로 보인다.

7월은 전월에 비해 다소 적은 3건의 윈도우 취약점이 발표되었다. 그러나, 전부 보안등급이 '긴급'에 해당하는 취약점으로 이에 대한 보안패치를 적용하는 등 주의가 필요하겠다. 최근 불어진 불법 도청이 스니핑 기술을 통하여 사이버 세상에서도 가능하여 각별한 주의가 요망된다.

이달의 ASEC 컬럼에서는 최근 검거되어 재판이 진행 중이 악성코드 제작자들에 대한 처벌과 그 한계 및 범죄 조직과 악성 코드 제작자 간의 연계에 대하여 살펴보았다.

I. 7월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자: 차형진 연구원(sharkjin@ahnlab.com)

순위		바이러스 명	건수	%
1	-	Win32/Netsky.worm.29568	253	16.9%
2	↑1	Win32/Maslan.C	161	10.8%
3	↑3	Win-Trojan/LineageHack.37888.C	69	4.6%
4	New	Win32/Netsky.worm.17424	34	2.3%
5	New	Win32/Mytob.worm.48766.C	33	2.2%
6	New	Win-Trojan/LineageHack.330240	31	2.1%
7	New	Win32/Netsky.worm.18944.B	30	2.0%
8	↓6	Win32/Sasser.worm.15872	25	1.7%
9	New	Win32/Tenga.3666	24	1.6%
10	New	Win32/LovGate.worm.152576	24	1.6%
		기타	813	54.3%
합계			1,497	100

[표1] 2005년 7월 악성코드 피해 Top 10

7월 악성코드 피해 동향

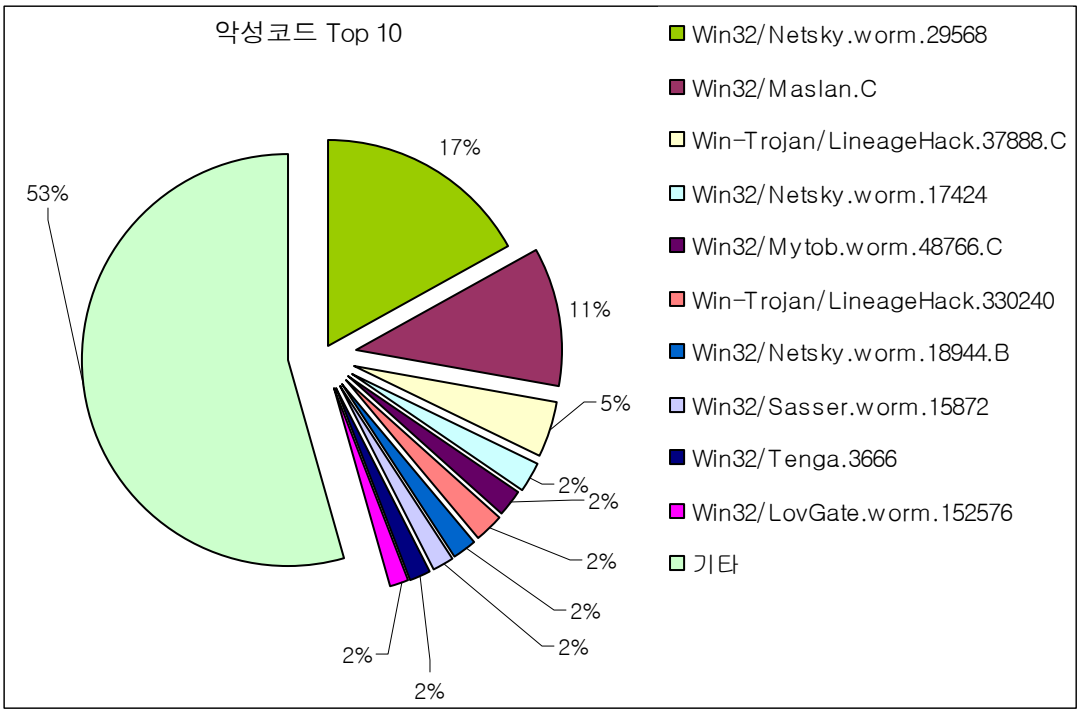
2005년 7월 악성코드 피해건수는 6월에 비해 소폭 줄어든 1,497건이다. 지난 달에 비해 감소 된 이유로는 악성 IRC 봇류의 변종과 피해가 감소된 데에 따른 것으로 보인다. 지난달과 비슷하게 Mass Mailer인 웜류도 변종이 다수 출현되긴 했지만 감염 피해는 상당수 줄어들었다.

7월 달에는 새로 진입한 악성코드가 무려 6개로, 이중 Mass Mailer 인 Mytob 변형은 올 초부터 지속적으로 나타나 피해를 주고 있으며, 2004년도에 많은 피해를 주었던 Lovgate 웜이 다시 진입한 것을 확인할 수 있다. Lovgate 웜은 메일 및 관리목적 공유 폴더 등으로 전파되는 것으로 분석되었으며, 이는 메일뿐만 아니라 윈도우 취약점을 이용한 악성코드 전파가 다시 증가되고 있음을 확인할 수 있다. 윈도우 MS04-011 취약점을 이용해 전파되는 Sasser 웜은 순위가 약간 떨어지긴 했지만 윈도우 취약점에 노출된 컴퓨터가 여전히 존재하고 있음을 보여주고 있다.

LineageHack은 5월경부터 발견되었으며, 변형과 감염확산도 증가로 Top10에 2개씩이나 등록되었다. 중국에서 제작된 것으로 판명된 LineageHack은 급속하게 확산되어 사용자에게 감염 피해를 입히고 있다. 특정 게임프로그램의 아이디와 패스워드를 훔쳐내는 것이 주목적이며, 8월에는 HangHack, ChunyHack, KorGameHack 등과 같이 유사한 트로이목마 변종도 다수 출현하였다.

일반적으로 트로이목마는 전파능력이 없는 것으로 알려져 있지만, 트로이목마류인 LineageHack은 윈도우 서버에서 실행되고 있는 IIS의 취약점을 이용하여 전파를 시도하는 것으로 분석되었다. 이 취약점에 노출된 웹사이트에 접근하는 다수 사용자를 감염시키고 있으며, 감염 속도와 피해가 더욱 증가되고 있는 추세이다.

7월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.



[그림1] 2005년 7월 악성코드 피해 Top 10

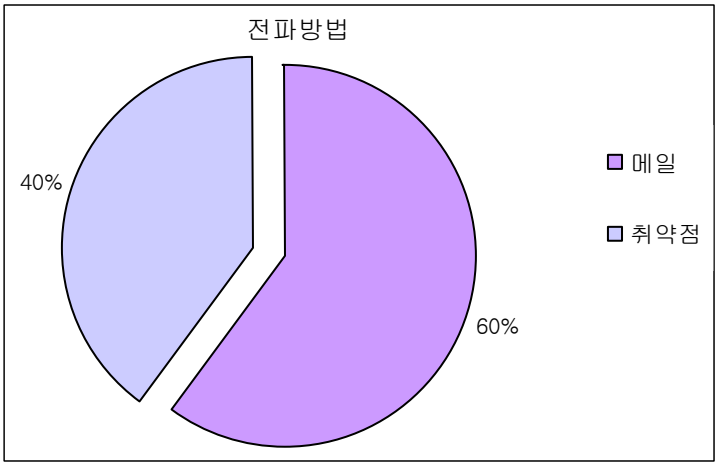
[그림1]과 같이 7월에는 트로이목마 뿐만 아니라 바이러스도 두각을 나타내고 있음을 알 수 있다. 2005년 중반기 이후부터 트로이목마뿐만 아니라 바이러스 피해도 증가하고 있으며, 특히 7월 중순에 발견되어 급속히 확산되고 있는 Win32/Tenga 바이러스(이하 Tenga 바이러스)가 대표적이다. Tenga 바이러스가 감염된 파일을 실행하면 윈도우 실행 파일인 PE 파일(Portable Executable)을 감염시키고, 감염된 파일의 날짜와 시간은 감염된 시점으로 변경된다. Tenga 바이러스도 해커가 고의적으로 특정 웹사이트에서 다운받을 수 있도록 하여 전파

를 시도하고 있다.

꾸준히 피해를 입히고 있는 Maslan.C는 메일로 전파되는 웜으로 감염 시 메일 발송 및 윈도우 취약점(MS03-026 , MS04-011)을 이용하여 감염대상 검색을 시도한다. 감염된 시스템은 느려질 수 있으며, 은폐 기법을 사용해 사용자로부터 바이러스 파일을 찾을 수 없게 한다.

7월 악성코드 Top 10 전파방법별 현황

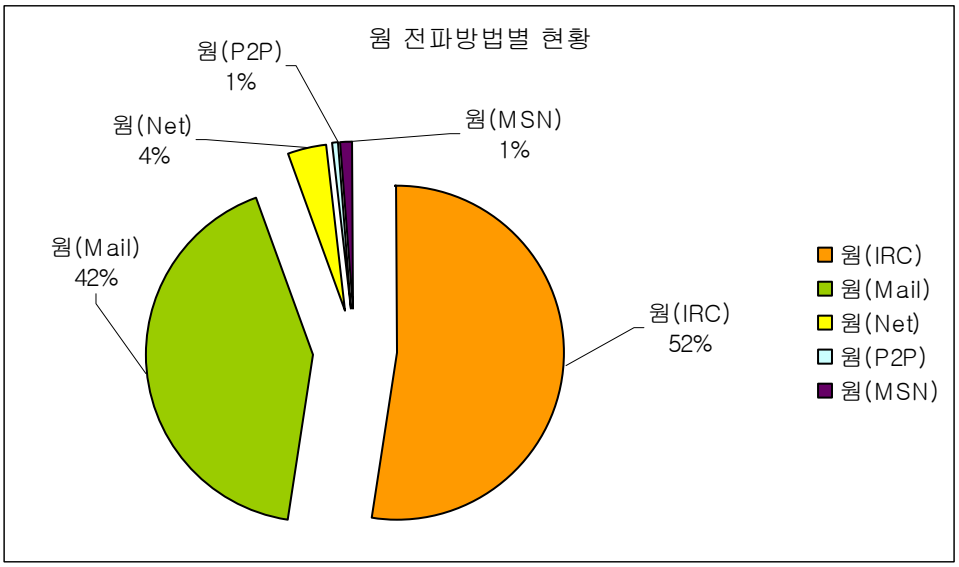
[표1]의 Top 10 악성코드들은 주로 어떠한 감염 경로를 가지고 있는지는 [그림2]에서 확인할 수 있다.



[그림2] 악성코드 Top 10의 전파 방법별 현황

[그림2]에서와 같이 피해순위 Top 10에 랭크된 악성코드의 60%가 메일을 이용하여 전파되고 있다. 지난 6월 달에 비해 메일은 10%가 감소한 것이다. 이는 네트워크와 운영체제 취약점을 이용한 전파가 10%가 증가했기 때문이다. 이 중 웹 서비스와 응용프로그램의 취약점을 이용하여 전파하는 비율이 매우 높아지고 있는 추세이다.

자신이 사용하는 운영체제와 응용프로그램이 보유한 취약점에 대해 주기적으로 살피고 관련 취약점에 대한 보안패치를 적용해야 한다.

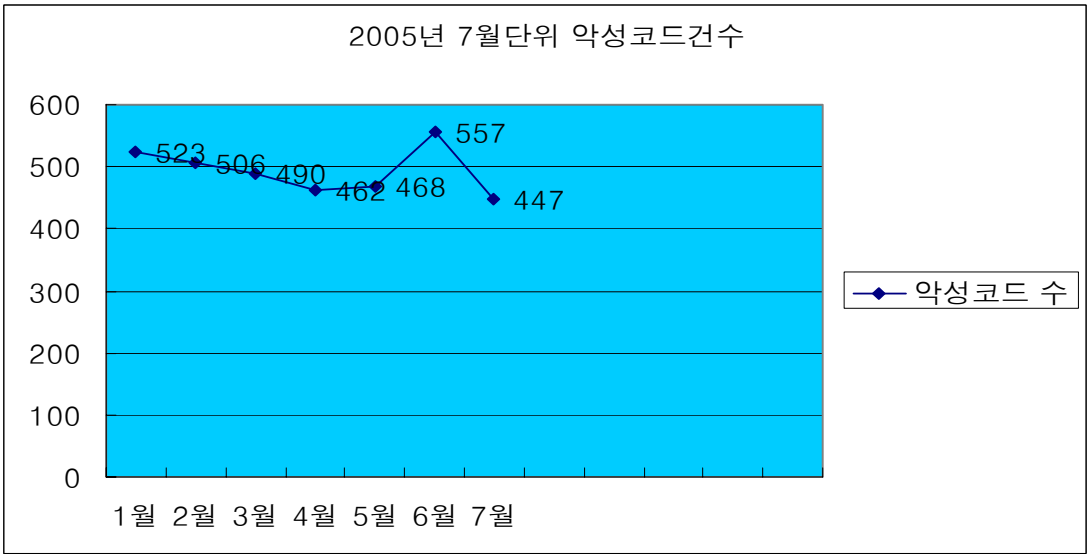


[그림3] 웜의 전파방법 별 현황

[그림3]은 7월에 피해 신고된 웜의 전파방법에 대한 현황으로, 메일(Mail)과 인터넷 채팅(IRC)이 94%를 차지하는 것으로 집계되었다. 이는 지난 6월 달보다 4%가 감소한 수치이다. 네트워크 취약점을 이용한 전파가 2%가 증가, P2P, MSN도 각각 1%씩 증가하였다.
네트워크 취약점과 P2P, MSN으로부터 전파되는 웜에 대해서 사전에 방지하기 위해서는 최신 엔진으로 업데이트된 백신제품의 실시간 기능을 항상 켜두고 사용하여야 한다.

월별 피해신고 악성코드 건수 현황

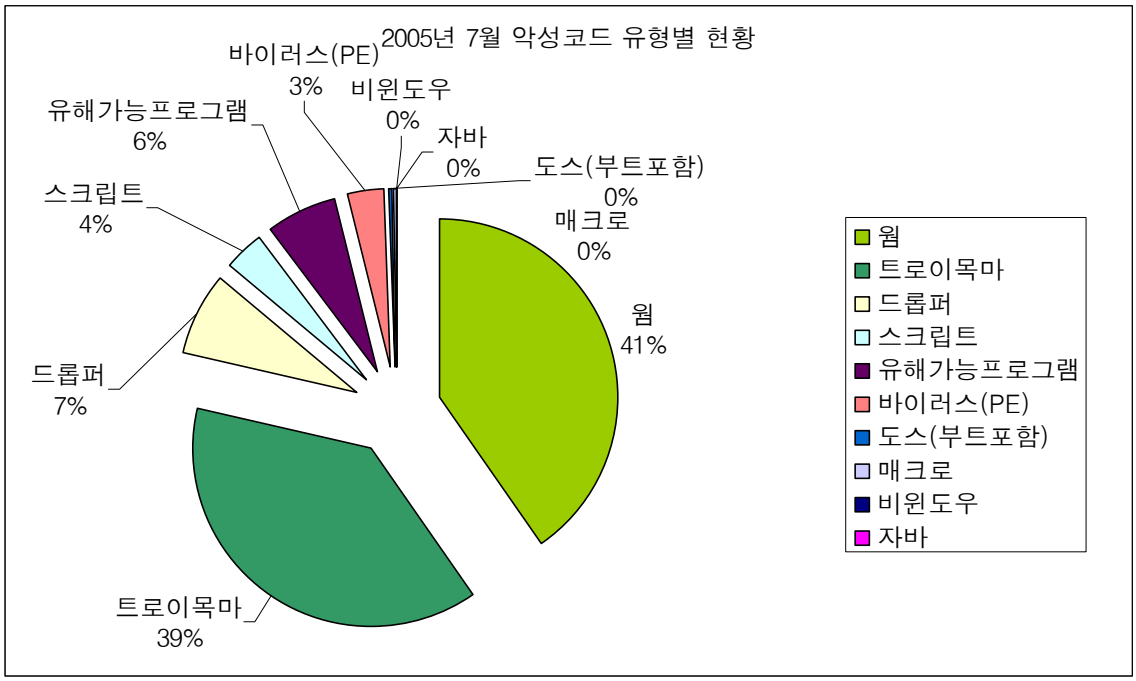
7월에 피해 신고된 악성코드는 447개이다. 2005년 가장 낮은 수치이며, 이는 웜에 대한 피해가 감소했기 때문으로 보인다. 전체적으로 악성 IRC봇과 메일로 전파되는 웜이 주춤한 것으로 보이며, 여름 휴가철로 인하여 컴퓨터 사용률이 부분적으로 감소하여 나타난 일시적인 현상으로 추정된다.



[그림4] 2005년 7월별 피해신고 악성코드 수

주요 악성코드 현황

악성코드 유형별 현황은 [그림5]와 같다.



[그림5] 악성코드 유형별 현황

7월에는 6월에 비해 유해가능프로그램이 2% 가량 증가하였으며, 바이러스부분도 소폭 증가하였다.

트로이목마와 바이러스의 공통적인 특징이 전파기능이 없이 악성코드를 수행하는데 있지만, 최근 파일 드롭, 웹사이트 접근 시 악성코드 파일다운 기능 등 다양한 방법을 동원하여 전파되고 있다. 이와 같이 다양한 취약점을 이용하여 급속도로 전파됨에 따라 감염피해는 위협적으로 증가되고 있다.

트로이목마류인 드롭퍼(Dropper), 다운로더(Downloader)가 지속적인 변형이 발견되고 있으며, 이로 인한 감염 피해가 지속되고 있는 것으로 보인다. 트로이 목마 중 LineageHack, HangHack은 한국에서 제작된 게임의 사용자 아이디와 패스워드를 훔쳐내는 것이 목적으로 하고 있으며, 금전적인 피해로까지 확산될 우려가 있다.

악성코드로부터의 피해를 줄이기 위한 예방책은 사용하는 운영체제와 응용프로그램의 취약점을 주기적으로 살피며 관련 취약점에 대한 보안패치를 바로 적용하는 습관을 가져야 하며, 백신을 설치하여 추가적인 신종 악성코드에 대응하기를 권한다.

(2) 7월 국내 신종 (변형) 악성 코드 발견 동향

* 작성자: 정진성 주임 연구원 (jsjung@ahnlab.com)

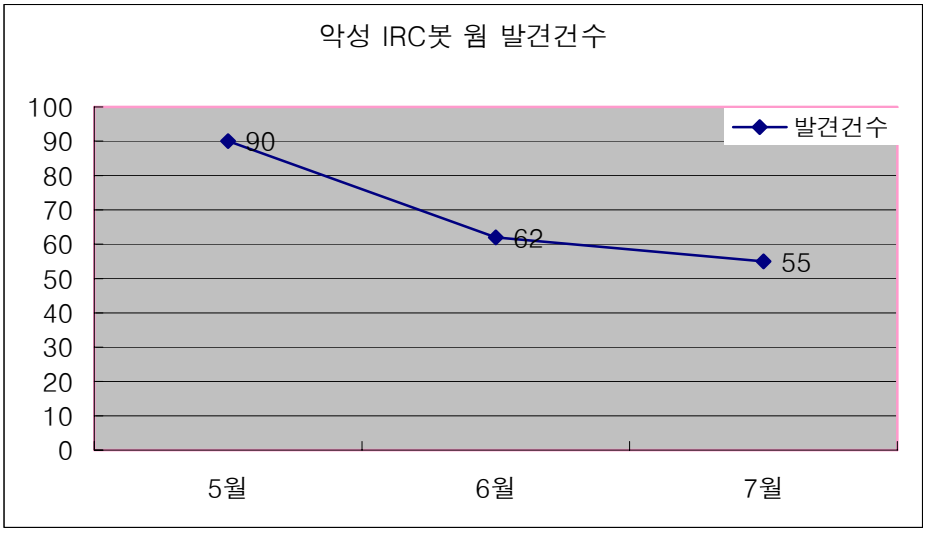
7월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1], [그림2]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비 윈도우	합계
63	100	29	7	1	1	0	0	26	0	227

[표1] 2005년 7월 유형별 신종 (변형) 악성코드 발견현황

이번 달은 지난달과 달리 전체적으로 악성코드 수가 줄어들었다. 특히 이번달의 악성 IRCBot 웜의 수가 많이 감소하였다. 이는 V3에서 실행압축을 해제하는 수가 지난달과 비해 늘어 났고 휴리스틱 진단 기능 등을 꾸준히 개선하고 있기 때문이다. 하지만 트로이목마의 비율은 여전히 웜 보다 많으며 이는 트로이목마의 증가 추세가 반영된 것이라 할 수 있겠다.

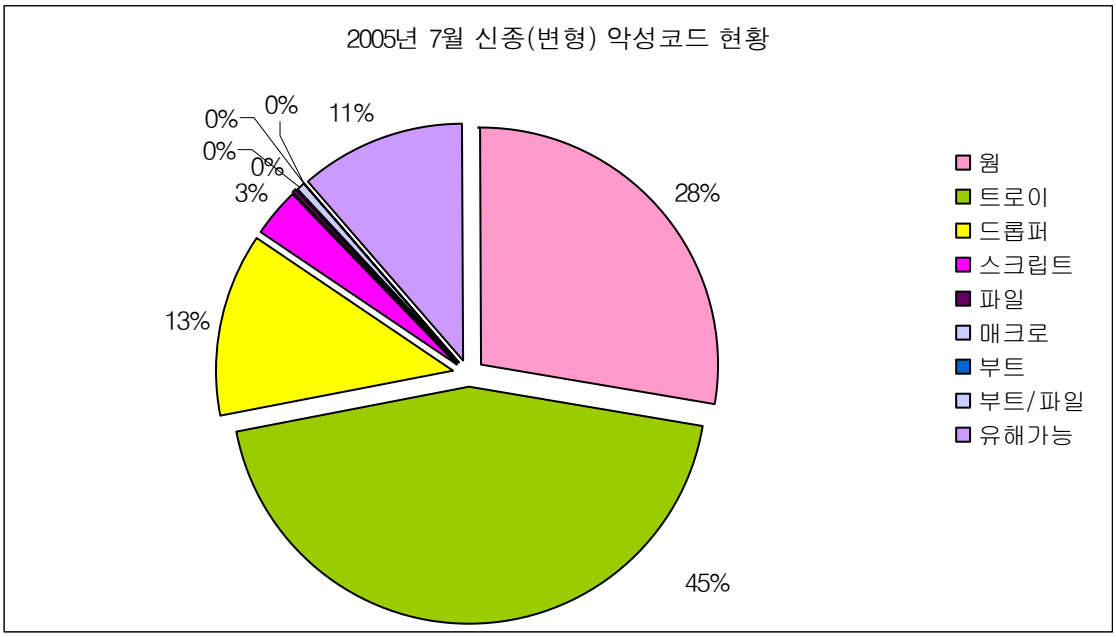
다음은 3개월간의 악성 IRC봇 웜의 발견건수이다. 참고로 이 자료는 국내 사용자로부터 접수된 악성 IRC봇 웜 샘플에 대한 자료이다.



[그림1] 3개월간 악성 IRCBot 웜 발견건수

최근 3개월간의 자료를 보듯이 해당 악성코드의 접수샘플수가 확연히 줄어드는 것을 볼 수 있다.

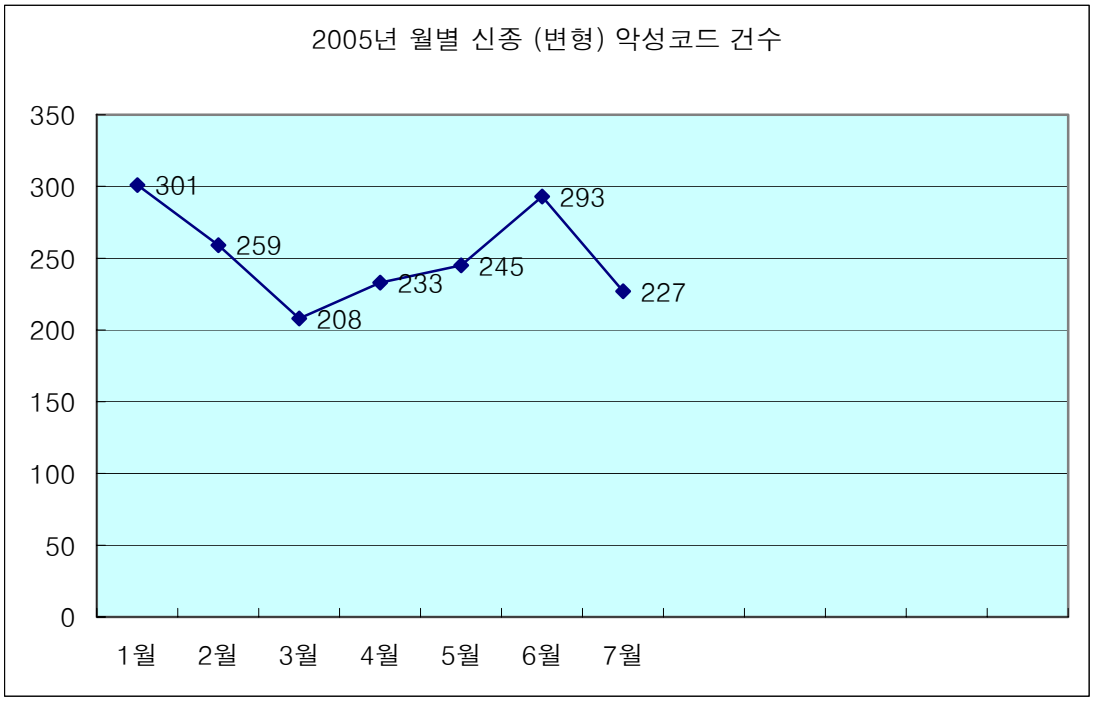
[그림2]는 7월 신종(변형)악성코드의 비율을 나타낸 것이다. 언급한 것처럼 역시 지난달에 이어 트로이목마가 비율을 차지하고 있다.



[그림2] 2005년 7월 신종(변형) 악성코드 비율

유해가능 프로그램의 비율도 올해 들어 가장 많은 11%를 차지 하고 있으며 FTP 데몬 프로그램 류와 프로세스 강제 종료하는 프로그램들이 증가 추세이다.
이번 달에 유해가능 프로그램으로 추가된 국산 상용 원격 관리 프로그램은 국내 한 고등학생이 국내 특정 은행 사이트를 가장한 가짜 웹 페이지를 만들어두고 이를 업로드 한 후 감염된 시스템을 해킹하는 사례가 발생하였고 해당 프로그램을 정상적인 프로그램으로 오인한 사용자들이 이를 실행하여 피해가 발생하였다..

[그림 3]은 월별 신종(변형) 악성코드 건수를 나타내고 있다. 지난 3월에 이어 다시 신종 및 변형의 악성코드의 수가 줄어들고 있는 것을 볼 수 있으며, 이는 대부분 악성 IRCBot 웜의 감소에 의한 것이다. 참고로 실제 제작되는 악성 IRCBot 웜의 감소가 아니라, 국내에서 신종으로 발견되고 접수된 샘플에 대한 통계이다. 즉, 여전히 악성 IRCBot 웜은 최고의 변형율을 보이고 제작되고 있지만, V3에서 실행압축을 해제하는 수가 지난달과 비해 늘어 났고 휴리스틱 진단 기능 등을 꾸준히 개선한 결과로 발견/접수되기 이전에 치료가 되기 때문으로 볼 수 있다.



[그림3]2005년 월별 신종(변형) 악성코드 발견 현황

7월 주요 신종(변형) 악성코드 정리

이번달은 다양한 형태의 악성코드가 이슈가 되었다. 특히 국내 금융권에서는 일부 상용 키로거 제품들이 오용되는 문제점이 확인되어 몇몇의 키로거들이 금융권의 권고로 인하여 엔진에 추가 되기도 하였다. 또한 이와 비슷한 사례로 상용 원격 관리 툴도 이를 남용하는 사례가 확인되어 엔진에 추가되었다. 이 유형들은 모두 유해가능 프로그램으로 분류되어 추가 되었으므로 일반적으로 정상적인 목적으로 해당 툴을 사용하는 관리자 및 담당자들은 큰 불편을 겪지는 않을 것으로 본다.

중국 해커들의 소행으로 추정되는 국내 웹 사이트 해킹이 여전히 문제시 되고 있다. 이들은 경제적인 이득을 목적으로 지속적으로 웹 사이트를 해킹하고 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마를 제작하여 해킹한 사이트에서 유포하고 있다.

자취를 감췄다고 생각이 들만큼 조용했던 윈도우 파일 바이러스 또는 이와 유사한 형태가 다시 기승을 부릴 조짐을 보이고 있다. Win32/Tenga 라고 명명된 바이러스는 웜으로 전파되어 광범위하게 확산 되었다. 또한 최근 악성코드 중 다른 파일에 대한 감염 기능은 없으나 파일자체가 마치 바이러스에 감염된 것처럼 조작된 경우가 있었다. 이는 안티 바이러스 진단 기능을 회피하는 형태로 일반적으로 진단코드를 작성할 경우 이런 류의 파일은 정상적으로 진단하지 못하는 경우가 발생하기도 한다.

이슈가 되었던 이번 달의 악성코드는 다음과 같다.

▶ Dropper/Exploit-1Table

이 악성코드는 MS 엑셀 및 워드의 취약점을 이용하여 실행된다. 특수하게 조작된 엑셀 또는 워드 문서파일 내 1Table 영역에 임의의 데이터 값을 넣어둔다. 사용자가 문서를 오픈시 임의의 데이터 값을 제대로 처리하지 못하여 버퍼 오버런을 발생하고 이때 악의적인 사용자가 지정한 임의의 코드가 실행되도록 한다. 국내 발견된 샘플은 워드문서가 특수하게 조작된 형태였다.

▶ Win-AppCare/SMPclient

상용 원격관리 프로그램인 이 툴은 국내 한 고등학생이 자신이 만들어둔 가짜 은행 웹 사이트 계정에서 다운로드를 하도록 유도했던 파일에 숨겨져 있었다. 즉, 임의의 설치파일을 만들어두고 파일을 설치시 해당 원격관리툴이 실행되도록 해두었다. 일반적으로 원격 관리 프로그램들은 안티 바이러스 제품에서 이를 진단하지 않는다는 점을 착안하여 범죄에 이용하였다고 피의자는 밝혔다. V3는 상용 프로그램을 감안하여 유해가능 프로그램으로 이를 추가하였다.

▶ Win32/Tenga.3666

이 바이러스는 MS 보안 취약점을 가진 윔에 감염된 채로 전파 되었다. 바이러스는 특정한 호스트로부터 다른 악성코드를 다운로드 한다. 이 글을 작성하는 현재 해당 호스트는 더 이상 접속되지 않는다. 바이러스에 감염된 파일은 약 3,666 바이트 증가하며 치료된 파일중 일부는 치료 후에도 바이러스가 수정해놓은 PE 파일의 특정 정보 때문에 크기가 100% 동일해지지 않는다.

▶ Win-Trojan/Rootkit.7168

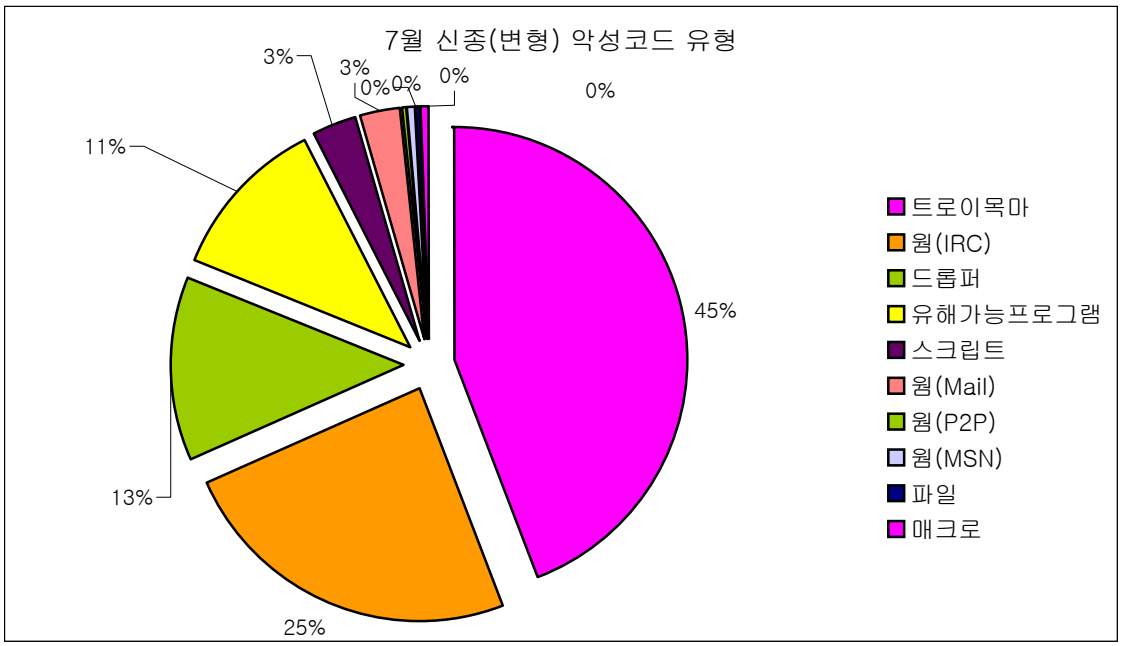
은폐증상을 가진 이 트로이목마는 단독으로 동작하지 않으며 특정 악성 IRC봇 윔으로부터 설치된다. 해당 윔의 프로세스 은폐증상을 갖는 이 트로이목마는 커널 드라이버 형태이다. 특정 IRC봇 윔들이 이를 사용하지만 진단방법은 동일하기 때문에 V3에서 모두 진단이 가능하다.

▶ Win-Trojan/SpamTool

국산 스팸 메일러인 이 트로이목마는 상용 통신 및 SMTP 라이브러리를 사용하고 있다. 특

히 SMTP 라이브러리가 없으면 스팸 메일을 정상적으로 발송하지 못한다. 메일 발송 데이터는 특정 호스트에서 다운로드 받아온다. 7월말에 발견 되었으며 계속적으로 변형이 제작 되어지고 있다.

다음은 7월에 발견된 악성코드들을 유형별로 분류한 것이다.



[그림4] 7월 신종 (변형) 악성코드 유형별 현황

다양한 유형의 악성코드가 발견된 것을 알 수 있으며 전체적으로 트로이목마, 웜, 드롭퍼, 유해가능프로그램 접수가 많았다. 웜은 악성 IRC봇 웜을 제외하고 이메일로 전파되는 웜이 그 다음으로 많았다.

II. 7월 AhnLab 스파이웨어 동향

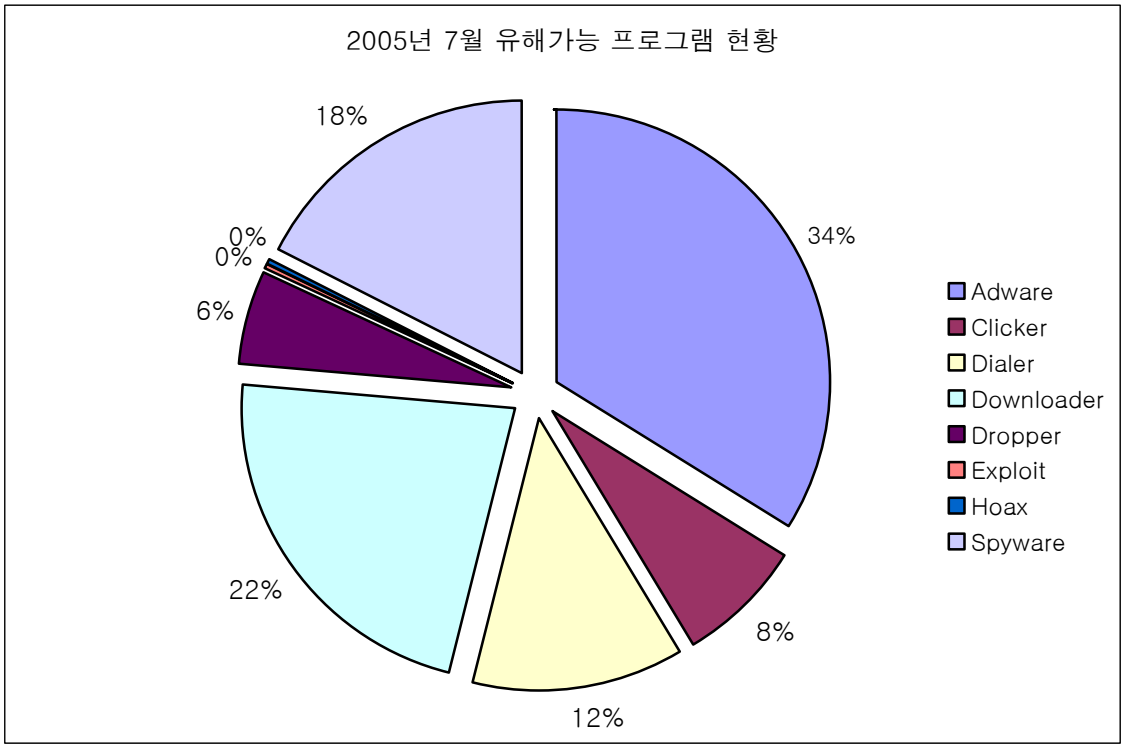
작성자: 장혜윤 연구원(planet@ahnlab.com)

7월 한달 동안 접수된 신종(변형) 유해가능 프로그램 건수는 [표1], [그림1]과 같다.

Adware	AppCare	Clicker	Dialer	Downloader	Dropper	Exploit	Hoax	Spyware
513	2	114	189	339	88	4	1	268

[표1] 2005년 7월 유형별 신종 (변형) 유해가능 프로그램 발견 현황

지난 6월과 비교해서 다운로더(Downloader)가 다소 감소하고, 애드웨어(Adware)가 증가한 것을 확인할 수 있다.



[그림1] 2005년 7월 발견된 유해가능 프로그램 발견 현황

7월에 발견된 스파이웨어 동향은 애드웨어(Adware)가 전체 유해가능 프로그램의 약 34%의 높은 비중을 차지하고 있다. 지난달에 이어 애드웨어(Adware), 다운로더(Downloader) 가 강세를 보이고 있다. 대부분의 유해 가능 프로그램이 다운로더(Downloader)로 설치가 되기 있기 때문에 높은 비중을 차지하며 앞으로도 계속 유지될 것으로 보인다.

7월 한달간 안철수연구소 신고센터에 접수된 유해가능 프로그램 문의 건수는 [표2]와 같다.

진단명	총건수	피해감염 접수건	단순문의 접수건
Win-Spyware/iGuard	87	83	4
Win-Spyware/StartPage.nk	3	3	0
Win-Spyware/Transponder.Nail	3	3	0
Win-Adware/Rogue.CZ	2	2	0
Win-Downloader/ISTbar.gen	2	2	0
Win-Downloader/ISTbar.ij	2	2	0
Win-Adware/DyFuCA	1	1	0
Win-Adware/Hanglo	1	1	0
Possible Policies Hijack	1	1	0
Win-Adware/NewDotNet	1	1	0
기타	2	2	0
총계	115	111	4

[표2] 2005년 7월 신고센터 토크로 유해가능 프로그램 문의 접수현황

접수현황에서 Top10 은 대부분 국외 유해가능 프로그램이 순위를 차지를 하지만, 몇 달 전부터 “Win-Spyware/iGuard” 가 1위를 차지하고 있다. 2005년 3월 ASEC Report 에도 소개 되었던 것으로 한글 키워드 시장을 둘러싼 경쟁으로 인해서 D사에서 배포되어 드라이버 방식으로 사용자 동의 없이 설치후, 백그라운드로 한글 키워드 도우미 프로그램을 설치후 사용자가 프로그램 추가/삭제에서 삭제를 하더라도 재설치하는 기능을 가지고 있다.

최근 한글 인터넷 키워드 서비스 업체인 D사에서는 안철수연구소를 상대로 “스파아제로” 배포금지 가처분 신청을 했지만, 재판부 판결에서 가처분 신청이 기각되었다. 재판부는 결정문에서 “D사 프로그램의 일부 구성 부분이 프로그램이 삭제된 뒤에도 자동으로 재설치되도록 하는 역할을 하고 있다”면서 이 구성 부분을 스파이웨어로 보는 안철수연구소의 판단에 잘못이 없다고 기각 이유를 밝혔다. 신종 악성 프로그램인 스파이웨어에 대해 법원이 처음으로 ‘차단 정당’ 결정을 내리면서 관련 개념 정립과 규제 기준 마련도 가속화될 전망이다.

또한 안철수연구소에서는 D사에서 배포된 일부 모듈에 대해서 Win-Spyware/iGuard로 진단을 하고 있지만, 타사에서는 D사에서 배포한 모든 모듈에 대하여 스파이웨어로 진단을 하고 있다.

III. 7월 시큐리티 동향

작성자 : 김지훈 주임연구원 (smallj@ahnlab.com)

7월에 발표된 보안 취약점 동향

이번 달에는 마이크로소프트사의 7월 정기 보안 패치가 총 3개 발표되었다. 3개의 보안 패치 모두 (MS05-035, MS05-036, MS05-037) 긴급에 해당하는 것이므로 반드시 보안패치를 적용하도록 한다. MS03-036은 ICC 프로파일 형식 태그 유효성 확인을 처리하는 방식 때문에 Microsoft 색상 관리 모듈에 원격 코드 실행 취약점이 존재한다. 공격자는 사용자가 악의적인 웹 사이트를 방문하거나 악의적인 메일 메시지를 볼 경우 원격 코드 실행을 허용하도록 악의적인 이미지 파일을 만들어 취약점을 악용할 수 있다. MS05-037은 COM 개체인 JView 프로파일러(Javaprxy.dll)는 인터넷 익스플로러에서 ActiveX 컨트롤로 인스턴스화될 경우 공격자가 영향을 받는 시스템을 완전히 제어할 수 있는 원격 코드 실행 취약점이 포함되어 있다. MS05-036과 MS05-037의 경우 개념증명코드(PoC)가 일반인에게 공개되어 있으므로 각별한 주의를 요한다.

> 7월의 주요 취약점 현황

위험등급	취약점	공격코드 유/무
HIGH	Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점 (MS05-035)	무
HIGH	Microsoft 색상 관리 모듈의 취약점으로 인한 원격 코드 실행 문제점 (MS05-036)	유
HIGH	JView 프로파일러의 취약점으로 인한 원격 코드 실행 문제점 (MS05-037),	유

* 취약점 현황은 ASEC 의 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.

► 사이버 불법도청의 위협으로부터 보호

최근 컴퓨터 사용자의 웹서핑, 이메일, 메신저 등의 인터넷 활동이 모니터링 될 수 있다는 기사가 언론에 보도되면서, 사이버 불법도청에 대한 네티즌의 걱정어린 관심이 대두되고 있다. 오래 전부터 대부분의 기업에서 기업 보안 등의 이유로 회사 임직원의 사전 동의를 전제로 인터넷 감시 솔루션을 도입해 사용해오고 있다. 이중 일부 몇몇의 솔루션들은 인터넷 온

라인을 통해 누구나 손쉽게 구할 수 있어 사이버 불법도청이 자행되고 있는 것이 아니냐는 우려를 뒷받침 하고 있다.

기업 내부의 네트워크 트래픽을 불법도청 하기 위해서는 기업 외부자가 해킹 공격을 통해 기업 내 전산망을 침투하는 과정이 필요하다. 악의적인 기업 내부자에 의한 가능성도 존재한다. 내부 전산망에 흐르는 암호화되지 않은 네트워크 정보는 제 3자, 즉 침투한 외부자 혹은 악의적인 내부자에 의해 그대로 노출될 위험이 있다.

내부 전산망에 연결된 모든 시스템의 보안 강화를 위해 기본적인 보안 원칙을 지켜나가는 일이 가장 중요하다. 시스템의 운영체제, 보안 프로그램은 항상 최신으로 유지하고, 불필요한 서비스는 중지시켜 해당 서비스에 대한 취약성을 사전에 방지하도록 한다.

중요한 정보의 유출을 차단하기 위한 가장 좋은 방법은 암호화 전송 프로토콜을 사용하는 것이다. 안전한 메세지 송수신을 위해서는 해당 프로그램에서 암호화 기능이 제공되어야 함과 동시에 사용자들이 이를 손쉽게 이용할 수 있도록 충분한 편이성이 제공되어야 한다.

► 보안, 백업 솔루션 업체와 고객 간의 신뢰 유지 필요

운영체제나 응용 프로그램은 사용 빈도가 높을 수록 보안취약점에 노출되기도 쉽다. 그동안 마이크로소프트사의 윈도우 운영체제에 대한 보안취약점이 많은 공격자로부터 노출되어 왔다. 운영체제의 보안취약점이 줄어듬에 따라, 대중적인 응용 프로그램들로 그 시선이 옮겨가고 있다. 백신 등의 보안 솔루션, 비니지스 연속성을 보장하기 위한 백업 솔루션 들도 예외가 될 수 는 없다. 최근 미국 라스베가스에서 열린 블랙햇 (http://www.blackhat.com/) 보안 컨퍼런스에서도 백신 솔루션에 대한 취약점 관련 내용이 시연된 바 있다.

기업, 개인은 보안, 백업 솔루션의 도입을 통해 해당 영역에 대한 강한 신뢰를 부여하고 있는 것이 사실이다. 이러한 믿음이 도리어 위협으로 작용될 수 있다는 점은 사용자에게는 충격적일 수 밖에 없다. 현존하는 어떠한 운영체제나 응용프로그램도 보안취약점으로부터 자유로울 수 없는 것이 사실이다. 따라서, 해당 솔루션 사용자는 보안취약점이 존재한다는 사실 자체만으로 제품에 대한 신뢰를 판단해서는 안될 것이다. 보안, 백업 솔루션 개발업체는 개발 단계마다 점검해야 하는 프로그래밍 고려 사항을 정리하여 개발 초기 단계부터 안전한 프로그램을 개발할 수 있도록 하여 보안취약점을 최소화하고, 제품 출시 이후에 발견된 보안취약점에 대해서도 악용되는 일이 없도록 빠른 사후 대응이 요구된다. 이러한 노력이 계속된다면, 보안, 백업 솔루션 업체와 고객 사이의 보이지 않는 신뢰의 끈은 꾸준히, 더 견고하게 이어져 나갈 수 있을 것이다.

► 인터넷 익스플로러 7 베타 1의 보안 기능

인터넷 익스플로러 7 (이하 IE 7) 베타 1은 XP SP2 상에서 지원되는 독립버전과 차기 운영체제인 윈도우 비스타 (코드명 롱혼) 에 기본적으로 내장되어 있는 버전의 2가지 형태로 제공되고 있다. IE 7 베타 1은 개발자들이 새로운 웹브라우저를 이용하여 그들의 기존 웹서비스에 대한 호환성을 테스트하기 위한 목적이 강하다. IE 7 베타 1의 가장 큰 특징은 코어 보안 아키텍처의 변화와 웹개발자를 위한 플랫폼의 향상을 들 수 있다.

IE 7은 사용자에게 안전한 브라우징에 대한 더 깊은 신뢰를 심어주고자 한다. URL 핸들링 보호, 크로스 도메인 스크립팅 공격 차단, 마이크로소프트사의 AntiSpyware 프로그램과의 연동, 인터넷 익스플로러 보호 모드 등의 보안 기능을 통해 악의적인 악성코드가 사용자 동의 없이 설치되거나 실행되는 것을 막아주고, URL 디스플레이 보호, 보안 상태 바 (Security Status Bar), 마이크로소프트 피싱 필터 (Phishing Filter)로 하여금 사용자가 악의적이거나 의심스러운 웹사이트를 쉽게 구별할 수 있도록 안전장치를 강화하였다.

이러한 보안 기능 이외에도 탭 브라우징, 툴바를 통한 인라인 검색, 사이즈 조정(Shrink-to-fit) 웹페이지 프린팅, RSS (Really Simple Syndication) 지원, 향상된 CSS (Cascading Style Sheets)와 투명한 PNG (Portable Network Graphics) 지원 등 사용자 편의성을 향상시킨 점도 눈여겨 볼만 하다.

IE 7 베타 1은 앞서서 언급하였던 것처럼 기존의 버전에 비해 보안 기능과 사용자 편이성 측면이 한층 향상되었다. 올해말 선보일 예정인 베타 2, 그리고 최종 버전에서도 많은 변화가 예견되고 있다. 인터넷 익스플로러 7가 인터넷으로의 안전한 항해를 돕는 조타수로서의 역할을 충실히 수행해주길 희망한다.

Ⅳ. 7월 세계 동향

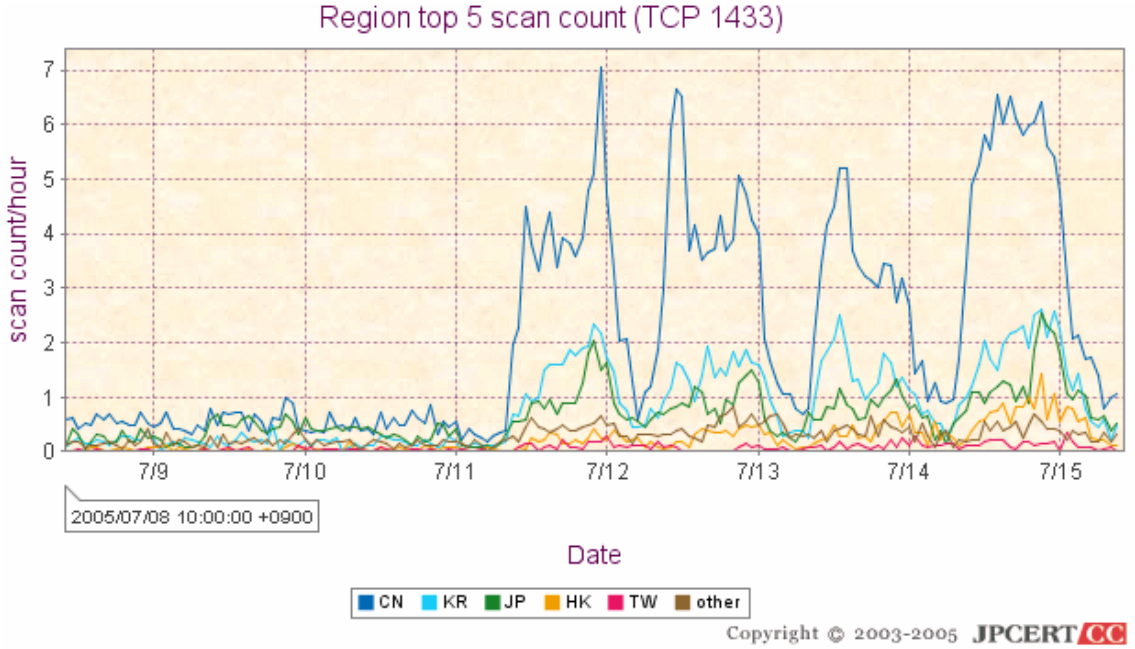
2005년 7월 세계 악성코드 동향과 관련한 주요 이슈는 전 세계적으로 넷스카이 웜의 확산도가 증가한 점이다. 유럽의 경우 6월부터 마이탑 웜의 확산도가 넷스카이 웜에 비해 더 높게 나타났었으나, 이번 달에는 넷스카이 웜이 가장 많이 확산된 것으로 집계되었다. 이러한 현상은 일본에서도 마찬가지였다. 넷스카이 웜의 경우 기존에 발견된 웜 이외에 새롭게 발견된 변형이 거의 없는 상태임에도 불구하고, 지속적으로 변형된 형태의 웜이 발견되고 있는 다른 웜들에 비해 확산도가 상승한 것은 넷스카이 웜의 강력한 전파력으로 인해 사용자의 감염 피해가 증가했다는 것을 짐작할 수 있게 해준다.

(1) 일본의 악성코드 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

2005년 7월 일본의 보안 동향과 관련하여 가장 큰 이슈가 되었던 사건은 TCP 1433 포트(MS SQL 에서 사용되는 포트)를 이용한 다량의 이상 트래픽이 발생한 것이다.
JPCERT/CC (www.jpcert.or.jp)의 발표 자료에 의하면 7월 11일에서 15일에 걸쳐 중국을 진원지로 하는 다량의 TCP 1433 패킷이 일본에 유입된 사실에 대해 피해 예방을 위해 사용자들의 주의를 당부하는 권고문을 발표하였다.
- JPCERT/CC의 권고문: http://www.jpcert.or.jp/at/2005/at050006.txt

[그림1]은 권고문의 내용 중 TCP 1433 포트의 진원지 별 트래픽 현황이다. 7월 11일 이후 중국을 진원지로 하는 트래픽이 급증한 것을 알 수 있다.
이와 관련한 자세한 내용은 아래의 네트워크 트래픽 현황을 참조하기 바란다.

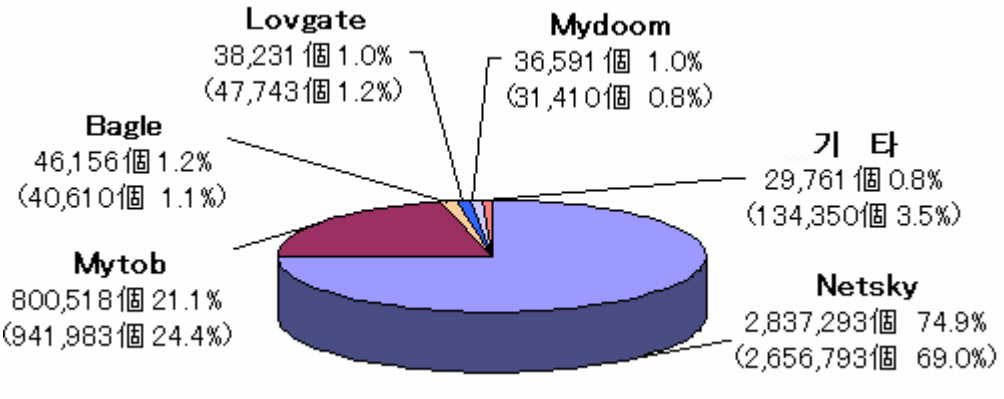


[그림1] JPCERT/CC의 진원지 별 TCP 1433 포트 트래픽 현황

일본 유행 악성코드 유형별 발생현황

2005년 7월 발생한 일본의 악성코드 동향과 관련하여 가장 주목할만한 사건은 넷스카이 웜(Win32.Netsky.worm)이 여전히 확산되고 있는 것이다. 이러한 현상은 전월과 비교해서 크게 변화가 없다.

[그림2]는 일본의 IPA에서 발표한 자료 중 일본에서 6월과 7월에 발생한 악성코드의 발견 개수에 대한 종류별 통계를 나타낸 것이다. 가장 많이 유포된 악성코드는 넷스카이 웜으로써 전월에 비해 유포되는 악성코드의 양이 매우 증가한 것을 볼 수 있다. 최근 넷스카이 웜의 새로운 변형이 발견된 사례가 거의 없음에도 불구하고 아직까지 이처럼 많은 양의 웜을 포함한 메일이 발송되고 있는 것은 대량의 메일을 지속적으로 유포하는 특징 때문으로 판단된다. 넷스카이 웜을 제외한 다른 악성코드의 경우 이전에 비해 대부분 감소하고 있는 것을 볼 수 있다.



[그림2] 악성코드 발견 건수 통계

아래의 [표1]은 일본의 IPA에서 발표한 자료 중 2005년 7월 악성코드의 감염 통계를 표로 나타낸 것이다. 넷스카이 웜에 의한 감염 피해가 가장 많은 것을 알 수 있다.

Window/Dos Virus	금월피해 / 전월피해	Macro Virus	금월피해 / 전월피해	Script Virus	금월피해 / 전월피해
Win32/Netsky	1,125 / 1,122	Xm/Laroux	9 / 8	VBS/Redlof	59 / 69
Win32/Mytob	638 / 699	W97M/X97M/ P97M/Tristate	8 / 3	VBS/Loveletter	10 / 13
Win32/Mydoom	332 / 352	X97M/Divi	4 / 8	VBS/Soraci	4 / 3
Win32/Bagle	284 / 316	W97M/Bablas	3 / 2	Wscript/ Fortnight	4 / 11
Win32/Lovgate	249 / 273	WM/Cap	1 / 3	VBS/Internal	2 / 1
Win32/Klez	230 / 265	WM/Concept	1 / 0	VBS/Haptime	1 / 0

[표1] 악성코드 피해 신고 현황

[그림3]의 넷스카이 웜과 관련한 데이터와 비교하여 보았을 때 발견되는 악성코드의 양에 비해 실제 감염 건수는 매우 적은 것을 알 수 있는데, [그림3]의 데이터의 경우 동일한 감염 시스템에서 지속적으로 악성코드를 유포하는 경우를 고려하지 않고 집계된 것이지만 [표1]의 데이터는 동일한 시스템에서 여러 개의 동일한 악성코드가 발견되는 것은 한 건으로 처리하였다는 차이가 있다.

그러나 실제로 감염된 시스템은 상대적으로 적은 양이라고 하더라도 PC 사용자에게 악성코

드 파일을 발송하는 것 자체가 감염의 위험 요소를 제공하는 것이고 실제로 넷스카이 웜이 비슷한 형태의 다른 웜들에 비해 훨씬 많은 감염 피해가 발생하는 주요한 원인 중의 하나가 다량의 메일을 발송하는 것이기 때문에 증감 추이를 지켜볼 필요가 있다.

악성코드의 감염 경로별 통계

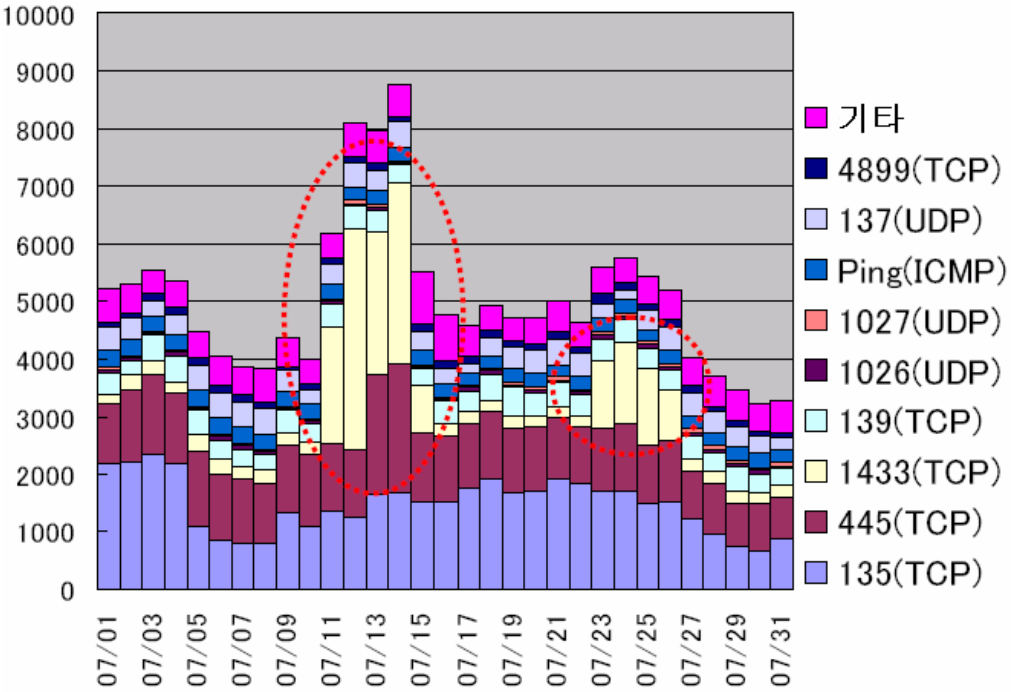
[표2]는 악성코드의 감염 경로 별 통계를 나타낸 것이다. 악성코드 감염 경로로 가장 많이 이용되는 매체는 메일로써 이러한 현황은 전월과 비교해서 크게 차이가 없다.

감염경로	피해 건수					
	2005 년 7 월		2005 년 6 월		2004 년 7 월	
메일	4,477	98.70%	4,850	98.40%	5,311	97.60%
외부의 모체	3	0.10%	4	0.10%	11	0.20%
다운로드	4	0.10%	9	0.20%	2	0%
네트워크	43	0.90%	57	1.20%	91	1.70%
기타	9	0.20%	8	0.20%	24	0.40%

[표2] 악성코드 감염 경로 통계

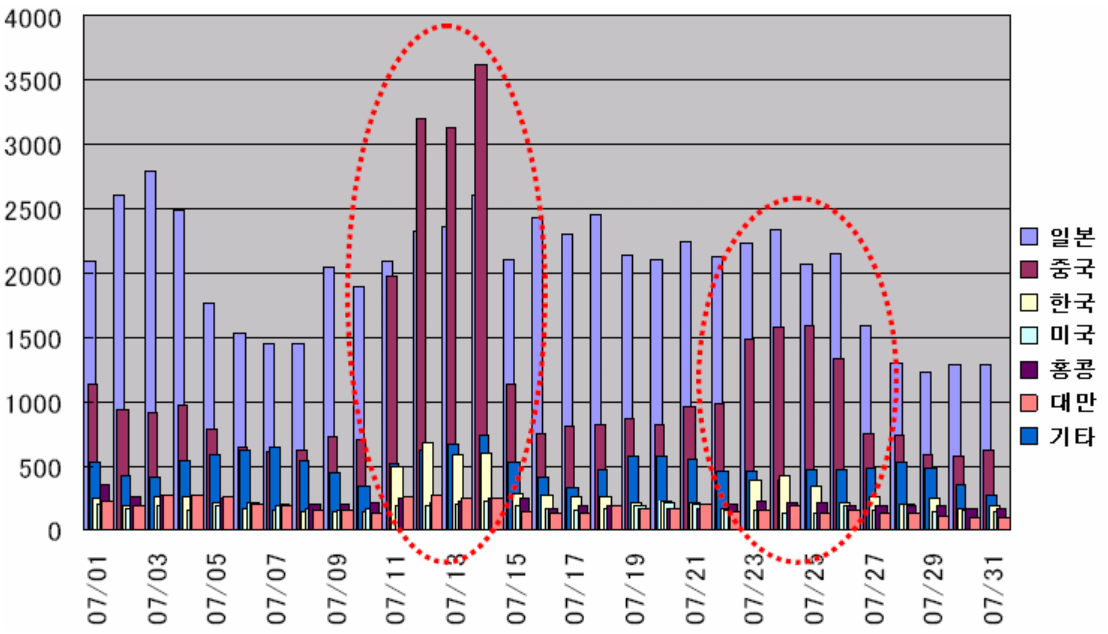
일본 네트워크 트래픽 현황

2005년 7월 일본의 네트워크 트래픽 현황과 관련하여 가장 큰 이슈는 중국을 발신지로 하는 TCP 1433 포트(MS SQL에서 사용되는 포트)의 급격한 증가이다. 아래의 [그림3]은 일본의 IPA (www.ipa.go.jp)에서 수집한 네트워크 트래픽의 발신지 별 포트 통계를 표로 나타낸 것이다. 표에서 주목할 만한 사항은 7월 11일과 23일 발생한 트래픽이 비정상적으로 급증한 것이다.



[그림3] 네트워크 트래픽 포트별 발신지 통계

[그림4]에는 7월에 발생한 네트워크 트래픽 발신지의 지역별 통계를 보여준다. 동일한 기간 동안 중국에서의 트래픽이 급증한 것을 볼 수 있다. 포트 정보 만으로는 어떤 유형의 트래픽이 발생한 것인지 알 수 없지만 제품의 보안 취약점을 이용한 공격이나 취약점 존재여부를 확인하기 위한 스캐닝이 발생했을 가능성이 매우 높은 것으로 생각된다.



[그림4] 네트워크 트래픽 발신지의 지역별 통계

이러한 비정상적인 네트워크 트래픽으로 인해 일본에서 직접적인 피해가 발생하지는 않은 것으로 판단된다. 그러나 최근 MS SQL과 관련한 취약점이 발표된 점 등으로 미루어 볼 때 취약점을 악용한 여러 형태의 추가적인 공격형태의 발생 가능성이 존재하기 때문에 주의가 필요하다. 일본 CERT에서도 이러한 현상에 대해 해당 포트를 통해 유입되는 네트워크 트래픽의 접근을 제한하는 등 취약점에 의한 공격 피해를 예방하기 위한 권고문을 발표했다.

(2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

7월 중국 악성코드 동향은 기존에 널리 알려진 악성 IRCBot 웜 변형(V3 진단명 Win32/IRCBot.worm)들이 다시 증가 추세를 보이고 있으며, 이와 함께 루트킷(Rootkit) 형태의 트로이목마(V3 진단명 Win-Trojan/Rootkit)의 감염 신고가 증가하였다. 그리고 원격제어 및 키로깅 기능 등을 가지고 있는 다양한 형태의 트로이목마의 다량 발견이 이번 7월 중국 악성코드의 특징으로 분석된다.

악성코드 TOP 5

순위 변화	순위	Rising
↑ 2	1	Backdoor.Rbot
↓ 1	2	TrojanDroper.Worm.Bagz
↑ 2	3	Backdoor.Gpigeon
New	4	Backdoor.Sdbot
New	5	BackDoor.Codbot

[표1] 2005년 6월 Rising 악성코드 TOP 5

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

순위 변화	순위	JiangMin
New	1	Backdoor/SdBot.atp.Rootkit
↓ 1	2	Trojan/QQMsg.Zigui.b
↑ 1	3	Trojan/Script.Seeker
New	4	Backdoor/Rootkit.Fu
New	5	Trojan/WebImport

[표2] 2005년 6월 JiangMin 악성코드 TOP 5

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

[표 1]과 [표 2]는 중국 로컬 백신 업체인 라이징(Rising)과 강민(JiangMin)의 7월 악성코드 TOP 5이다. 먼저 라이징의 7월 악성코드 TOP 5를 먼저 살펴볼 경우 지난 6월까지 1위를 지키고 있던 백쯔 웜(TrojanDroper.Worm.Bagz, V3 진단명 Win32/Bagz.worm)이 1계단 물러난 2위를 차지하고 3위를 차지하였던 악성 IRCBot 웜 변형(Backdoor.Rbot, V3 진단명 Win32/IRCBot.worm)이 1위를 차지하고 있다. 그 외에도 또 다른 악성 IRCBot 웜 변형들인 Backdoor.Sdbot과 BackDoor.Codbot 이 다시 순위에 진입하였다는 점도 특이 사항으로 볼 수 있다. 그리고 지난달 5위였던 그레이버드 트로이목마는(Backdoor.Gpigeon, V3 진단명 Win-Trojan/Gpigeon 및 Win-Trojan/GrayBird)는 3위로 순위가 상승하였다.

강민(JiangMin)의 TOP 5을 살펴 볼 경우에는 1위를 차지한 악성 IRCBot 웜 변형(Backdoor/SdBot.atp.Rootkit, V3 진단명 Win32/IRCBot.worm)은 라이징과 유사한 부분을 보이며 중국 내에서 악성 IRCBot 웜 변형들의 활동이 예전 보다 증가한 것으로 추정된다. 그러나, 기존 악성 IRCBot 웜 변형들과 다른 점은 루트킷(Rootkit) 형태의 트로이목마(Backdoor/Rootkit.Fu, V3 진단명 Win-Trojan/Rootkit) 역시 같이 증가하였다는 점이다. 라이징 순위에는 루트킷(Rootkit) 형태의 트로이목마가 포함되어 있지만 7월 달에 조금씩 증가 추세를 보이고 있는 분석되었다. 이러한 사항들은 최근 악성 IRCBot 웜이 자신을 은폐하기 위해서 은폐기능을 수행해주는 커널 드라이버 형태의 루트킷도 같이 생성하고 있어 악성 IRCBot 웜의 감염 신고와 함께 증가하고 있는 것으로 분석된다. 그리고 최근에는 은폐기능을 가진 휴피곤 드로퍼 또는 휴피곤 트로이목마(V3 진단명Dropper/Hupigon, Win-Trojan/Hupigon)와 같은 형태의 트로이목마들도 다수가 발견이 되고 루트킷 형태의 트로이목마도 같이 증가하는 것으로 분석된다.

주간 악성코드 순위

순위	1 주	2 주	3 주	4 주
1	Backdoor.Rbot	Backdoor.Rbot	TrojanDroper. Worm.Bagz	Backdoor.Rbot
2	Trojan.Spy. Keylogger	Trojan.PSW.LMir	Backdoor.Gpigeon	Backdoor.Gpigeon
3	Backdoor. Gpigeon	GrayBird	Backdoor.Rbot	TrojanDroper. Worm.Bagz
4	Trojan.Spy.Delf	Trojan.PSW. QQPass	BackDoor.Codbot	Trojan.QQ.Dragonjb
5	Worm.Mytob	Backdoor.Sdbot	Trojan.PSW.Lmir	Worm.Lebreat

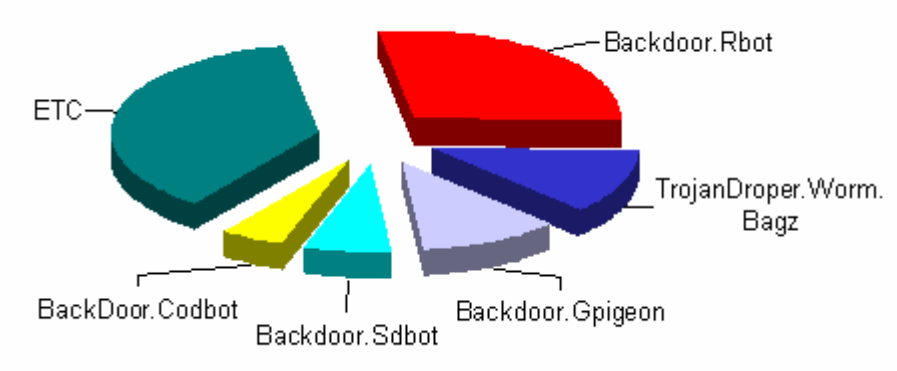
[표3] 2005년 7월 Rising 주간 악성코드 순위

순위	1 주	2 주	3 주	4 주
1	Trojan/QQMsg.Zigui.b	Trojan/QQMsg.Zigui.b	Backdoor/SdBot.atp.Rootkit	Backdoor/SdBot.atp.Rootkit
2	Trojan/Script.Seeker	Backdoor/SdBot.atp.Rootkit	Trojan/QQMsg.Zigui.b	Trojan/Script.Seeker
3	I-Worm/QQ.Porn	Trojan/Script.Seeker	Backdoor/Rootkit.Fu	Trojan/WebImport
4	Exploit.MhtRedir	Exploit.MhtRedir	Trojan/Script.Seeker	Trojan/QQMsg.Zigui.b
5	Backdoor/Rootkit.Fu	Exploit.HHCtrl.Jiaozhu	Trojan/WebImport	Backdoor/Rootkit.Fu

[표4] 2005년 7월 JiangMin 주간 악성코드 순위

주간 악성코드 순위를 살펴보면 TOP 5에는 기록되지 못했지만 주목할 만한 형태의 악성코드들로는, 먼저 엘미르핵 트로이목마(Trojan.PSW.Lmir, V3 진단명 Win-Trojan/LmirHack)를 들 수 있다. 엘미르핵 트로이목마는 특정 온라인 게임의 사용자 아이디와 암호를 훔치기 위해서 제작되었지만 주간 악성코드 순위에 기록될 만큼 많은 확산을 보이지는 않았었다. 하지만 최근 엘미르핵 트로이목마와 유사한 리니지핵 트로이목마(V3 진단명 Win-Trojan/LineageHack)까지 등장하여 많은 주의를 필요로 할 만큼 많은 확산을 보이고 있다. 리니지핵 트로이목마는 엘미르핵 트로이목마와 유사하게 특정 온라인 게임 프로세스가 실행되면 후킹 기능이 동작하여 해당 온라인 게임 사용자들의 계정과 암호를 메일을 이용하여 외부로 유출하는 기능을 하는 것이다. 기능적인 면으로 본다면 엘미르핵과 리니지핵 트로이목마는 크게 다른 부분이 없으나 유출하고자 하는 대상이 온라인 게임 사용자 계정이라는 점이 기존의 트로이목마와 다른 형태라고 볼 수 있다.

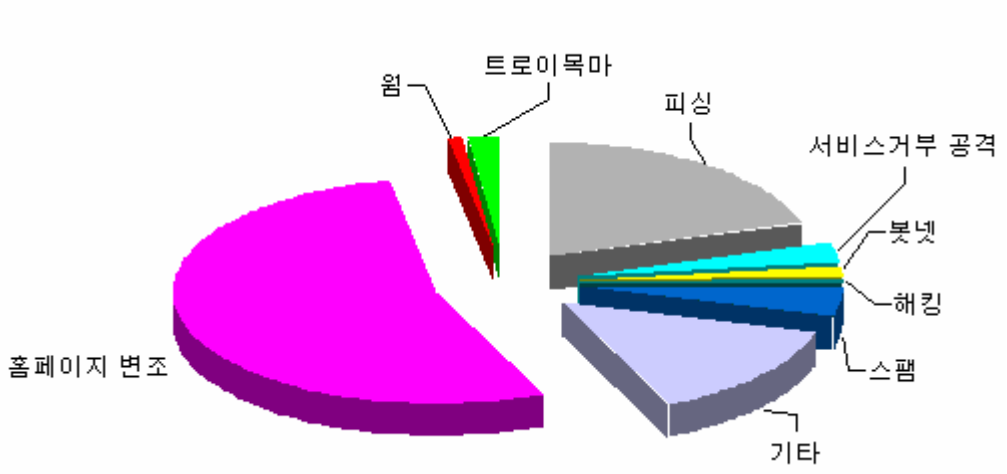
악성코드 분포



[그림 1] 2005년 7월 Rising의 악성코드 분포

위 [그림 1]은 라이징의 7월 악성코드 분포도 이다. 분포도를 살펴보면 지난 6월 1위를 차지한 백쯔 웜은 7월에는 17%에서 12%로 5% 감소한 반면 악성 IRCBot 웜은 7.9%에서 28%로 4배 가까운 증가치를 보였다. 이와 함께 그레이버드 트로이목마는 6%에서 11%로 2배 가까운 증가치를 보였다. 그러나 감염 신고가 높지 않은 다양한 형태의 트로이목마를 포함하고 있는 기타는 34%로 지난 6월 51%에서 전반적인 감소 추세를 보였다.

보안 사고 통계



[그림 2] 2005년 7월 CNCERT/CC의 보안사고 분포

위 [그림 2]는 중국 CNCERT/CC가 작성한 7월 중국 보안 사고 통계이다. 위 통계를 살펴볼 경우에는 7월 중국 내에서 발생한 컴퓨터 보안 사고는 홈페이지 변조가 77건으로 가장 높은 수치를 기록하였다. 다음으로는 피싱과 스팸 관련 사고들이 많이 발생하고 있는 점으로 미루어 중국 내에서도 금전적인 이득을 꾀하는 보안 사고들이 많이 발생하고 있는 것으로 추정되고 있다.

(3) 세계 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

2005년 7월 세계 악성코드 동향은 과거 웜의 재등장으로 요약할 수 있다. 영국의 소포스[1]와

[1] http://www.sophos.com/pressoffice/pressrel/uk/20050801topten.html

러시아의 캐스퍼스키 연구소[1] 모두 넷스카이 변형이 1위를 차지했으며 리스트의 대부분은 마이톱 변형(Win32/Mytob.worm), 자피 웜 변형, 마이둠 변형 등이 차지했다. 새로운 악성코드가 순위에 없는 이유는 최근에 등장하는 웜이 짧은 시간에 잠깐 확산되고 사라지기 때문으로 보인다. 그외 한 달에 발견되는 악성코드가 수천 개 이상이지만 대부분 전파 능력이 없는 트로이목마가 대부분이므로 과거에 널리 퍼진 악성코드가 지금도 강세인 것으로 보인다. 국내의 경우 중국 해커들의 웹사이트 변조를 통한 트로이목마 배포 영향으로 특정 게임 혹은 사이트의 계정과 비밀번호를 훔치는 트로이목마가 1위를 차지하고 있다.

캐스퍼스키 연구소의 유리 마쉐브스키(Yury Mashevsky)가 악성코드 종류별 증가 추이를 조사 발표했다. [2] 이 자료에 따르면 바이러스와 웜은 일정 수를 유지하고 있으며 개인 정보를 훔쳐가는 등의 트로이목마가 2003년 월 500개에서 2005년 5월에는 월 3000개에 육박하는 것으로 조사되었다. 회사간의 정책 차이로 다른 업체에서 악성 IRC봇 웜으로 분류하거나 다른 업체에서 스파이웨어로 분류하는 샘플도 트로이목마로 분류되어 있어 지나치게 샘플이 많은 것처럼 보일 수도 있지만 2년전과 비교하면 트로이목마가 많이 증가한 것을 알 수 있다. 또한 유닉스 악성코드가 2003년 월 12.67 개에서 2005년 35.20 개 발견되는 것으로 조사되었으며 휴대폰 등 휴대 장비에 이용되는 심비안은 2003년 월 1.42 개에서 2005년 월 7.4 개로 계속 증가 추세임을 알 수 있다. 이와 같은 트로이목마의 강세는 악성코드 제작자의 목적의 변화로 보인다. 악성코드 제작 목적이 과거 악성코드 확신을 통한 자기 만족에서 애드웨어나 스팸 메일 발송 등의 금전적 이득으로 바뀌면서 빠르게 확산되어 쉽게 자신이 들어나는 웜보다 최대한 은밀하게 사용자의 정보를 빼내가는 트로이목마를 이용하는 것이 더 효과적으로 판단하는 것 같다.

[1] Virus Top Twenty for July 2005
(http://www.viruslist.com/en/analysis?pubid=167966751)
[2] Watershed in malicious code evolution
(http://www.viruslist.com/en/analysis?pubid=167798878)

V. 이달의 ASEC 컬럼 - 악성코드 배포자 처벌

작성자 : 차민석 주임(jackycha@ahnlab.com)

7월에는 국내에서 악성코드 배포자 적발과 독일에서 새서 웜 제작자의 재판이 있었다. 이전에도 여러 악성코드 제작자 혹은 배포자가 재판을 받았지만 두 사건이 크게 주목받았다. 국내에서 중국 해커들을 고용해 온라인 게임 혹은 특정 웹사이트의 사용자 계정과 비밀번호를 훔쳐가는 악성코드 제작을 사주한 일은 다수의 사람들이 조직적으로 연계되었다는 점에서 충격을 주었으며 독일의 10대 청년인 스벤 야쉔(Sven Jaschan)의 재판은 2004년 최악의 악성코드로 불리는 넷스카이 웜(Win32/Netsky.worm)과 2004년 5월에 등장해 큰 피해를 준 새서 웜(Win32/Sasser.worm)의 제작, 배포자라는 점에서 주목받았다.

국제적 범죄 조직

2004년 안티 바이러스 연구가들은 악성코드 제작자들이 10대 들의 장난에서 점점 범죄화되고 있다고 우려했으며 피싱 등에 마피아 연루설 등도 제기되었다. 2005년부터 금전적 이득을 목적으로 하는 악성코드의 발견이 부쩍 증가했으며 국내에는 공인인증서 등의 각종 보안 기능으로 은행 해킹보다 상대적으로 손쉬운 게임 계정의 해킹이 증가하게 되었다. ASEC 리포트 2005년 5월 '게임아이템 매매를 위한 홈페이지 변조사건'에 대한민국과 일본 사이트를 해킹해 트로이목마를 배포한 사건이 소개되었다. 왜 중국 해커로 추정되는 사람들이 국내 게임과 국내 사이트를 목표로 했는지 의아해했지만, 2005년 7월 8일 지난 5월 하순부터 국내 주요 웹사이트를 해킹해 게임 아이디와 비밀번호를 몰래 빼가는 악성코드를 유포한 조직이 검거되면서 해결되었다. 이들은 중국 해커들에게 트로이목마 제작과 해킹을 사주한 것으로 밝혀졌다. 이 사건은 게임 아이템 거래 등이 실질적인 돈이 되며 컴퓨터에 대한 지식이 부족한 범죄 단체도 충분히 악성코드 제작에 개입할 수 있다는 것을 보여주었다. 향후 금전적 이득을 위한 다양한 범죄 단체의 연루가 진행될 것으로 보인다. 하지만, 검거 이후에도 유사 해킹 사건이 줄어들지 않고 있으며 최근에는 더 많은 게임과 더 많은 사이트의 계정과 비밀번호를 빼가는 프로그램으로 확대되고 있어 더 많은 조직이 존재하고 있는 것으로 추정된다.

스벤 야쉔 재판

2005년 7월 5일부터 새서 웜 유포자의 재판이 시작되었다. 스벤 야쉔(Sven Jaschan)은 컴퓨터 파괴 행위를 비롯한 모든 혐의를 인정했으며 그는 미성년자인 관계로 집행유예 21개월 판결을 받았으며 병원 등에서 30시간 봉사 활동을 할 것을 명령받았다. 스벤 야쉔의 재판에 대해서는 피해에 비해 처벌이 너무 가볍다는 의견이 많았다. 또 그는 재판 이전에 독일의 한 보안업체에 채용되어 해당 업체에 안티 바이러스 엔진을 제공하던 백신 회사에서 엔진 라이센스를 중단한 사건도 발생했다. 안티 바이러스 업계에서는 악성코드 제작자 채용을 금기시

하고 있기 때문이다.

처벌의 한계

스벤 야쉔의 집행 유해 판결 이후 바이러스 제작자를 사형시켜야 하는가에 대한 기사도 올라왔다. [1] 물론 지나친 비약이기도 하지만 악성코드 제작자의 대부분이 청소년임을 생각하면 성인에게 적용되는 처벌에 한계가 있다. 실제 과거 국내에서 적발된 바이러스 제작자들은 대부분 10대 청소년으로 불구속으로 끝나는 경우가 많았다. 단순한 처벌보다는 청소년들이 왜 악성코드를 제작하는지를 동기를 파악하고 환경을 개선하는 방안도 마련해야 할 것이다. 또한 최근 악성코드를 이용한 금전적 이득을 목적으로 범죄 단체들이 개입하고 있으므로 이들에 대해서는 국제적 공조를 통해 범인들을 잡아야 할 것으로 보인다

[1] Death penalty for virus writer (http://news.com.com/2061-10789_3-5785455.html?part=rss&tag=5785455&subj=news)