ASEC Report 8월

® ASEC Report

2005. 09

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

8월에는 지난 7월에 비하여 악성코드 피해 건수가 소폭 증가하였다. 특징적인 피해 동향은 MS05-039 취약점을 이용하는 Win32/Zotob.worm과 게임정보 유출시도용 Trojan인 Win-Trojan/Xema에 의한 피해 건수가 10위안에 들어온 것이다.

8월 피해신고 된 악성코드의 감염유형별 현황을 살펴보면 네트워크 취약점을 이용한 것과 메일을 이용한 것의 비율이 5:5의 비율인 것을 확인할 수 있다. 8월 신종(변형)발견 수치도 7월의 일시적인 하락 이후에 다시 증가 추세로 전환되었으며 피해신고와 마찬가지로 트로이목마의 발견이 강세를 보이고 있어, 전체 발견된 신종(변형) 중 53%를 트로이목마가 차지하고 있다. 8월 세계 악성코드 동향 중 일본의 경우는 넷스카이 웜과 같은 메일로 전파되는 웜이 확산되고 있는 것으로 분석되었다. 그러나 이와 반대로 중국의 경우에는 원격제어나 키로킹이 가능한 트로이목마 류의 큰 폭으로 증가하고 있는 것으로 분석되었다. 이러한 극동 아시아의 악성코드 분포는 메스 메일러와 트로이목마로 양극을 이루고 있는 반면 유럽 지역에는 일본과 유사한 메스 메일러가 대부분을 이루고 있으나 베이글과 마이둠 변형들은 큰 폭으로 감소하고 넷스카이 웜과 마이톱 변형들이 대부분을 차지하고 있다.

8월 스파이웨어 동향은 7월과 마찬가지로 애드웨어(Adware)의 발견 비율이 전체의 46%로 가장 높으며, 7월에 비해서 다운로더(Downloader)의 발견 비율이 감소한 반면 스파이웨어(Spyware)의 발견 비율이 증가한 것을 볼 수 있다. 또한 사용자 권리를 침해하는 '스파이웨어'에 대한 구체적인 기준안과 법률적인 처벌 근거가 마련됨으로써 스파이웨어 제작과 유포에 대한 행위가 상당수 줄어들 것으로 기대된다. 또한 그 동안 끊이지 않았던 백신, 안티스파이웨어 프로그램 제작 업체와 애드웨어, 스파이웨어 제작 업체와의 분쟁도 이번 스파이웨어 기준안 발표로 줄어들 것으로 예상된다

8월에는 4건의 윈도우 패치가 발표되었으며, MS05-039 취약점을 이용한 악성코드가 취약점 발표후 4-5일 이내에 출현하는 것으로 보아 zero-day 공격이 현실로 다가오고 있음을 알 수 있다. 또한 8월 15일 광복절을 기념하여 중국의 홍커들이 일본을 대대적으로 공격할 것이라고 예상되었으나, 실제로는 미미한 수준이었다.

이달의 ASEC 컬럼에서는 온라인 게임에서의 해킹 프로그램에 대한 내용으로 최근 문제가 되고 있는 온라인 게임의 사용자 계정을 탈취하는 종류의 악성코드에 관한 글이 아니라 게임 해킹 프로그램은 유틸리티를 사용하여 비정상적인 플레이를 하도록 하는 프로그램들에 대하여 살펴보았다.

I. 8월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자 : 조성준 주임 연구원(sjcho@ahnlab.com)

바이러스명	건수	%
Win32/Netsky.worm.29568	160	10.2%
Win32/Maslan.C	135	8.6%
Win-Trojan/Hanghack.44032	68	4.3%
Win-Trojan/Xema.31744.B	49	3.1%
Win32/Sasser.worm.15872	38	2.4%
Win32/Tenga.3666	38	2.4%
Win32/Zotob.worm.31744	38	2.4%
Win32/Mytob.worm.59006	36	2.3%
Win32/Netsky.worm.18944.B	33	2.1%
Win32/LovGate.worm.152576	29	1.9%
기타	940	60.1%
합	1,564	100

[표1] 2005년 8월 악성코드 피해 Top 10

8월 악성코드 피해 동향

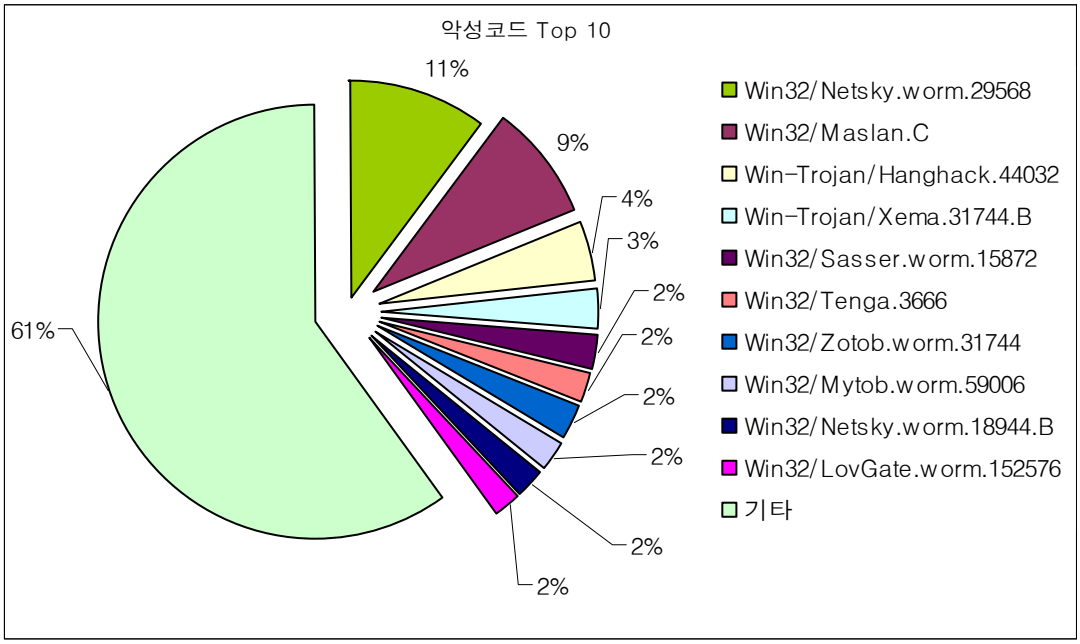
2005년 8월 악성코드 피해건수는 2005년 7월(1,497건)에 비해 소폭 늘어난 1,564건이다. 소폭 증가의 원인은 Top 10의 악성코드의 피해 건수는 약간 줄어 들고, 기타 변종 악성코드의 증가로 인한 것으로 보여진다.

8월 피해 동향의 특징으로 10위권 내에 악성코드인 Win32/Zotob.worm의 등장과 Win-Trojan/Xema의 진입이다.

Win32/Zotob.worm은 MS NT계열 OS의 플러그 앤 플레이의 취약점(MS05-039)이 공개됨에 따라 해당 취약점을 이용한 악성코드이며, IRCBot과 Mytob의 특징을 가지고 있다. 해당 웜이 발생시키는 취약점 공격 패킷으로 인해 패치가 되지 않은 한글 윈도우 NT 계열 시스템은 Services.exe 오류가 발생하며 시스템 리부팅 증상이 발생하는 특징을 갖고 있다.

Win-Trojan/Xema는 Win-Trojan/LineageHack과 유사한 게임정보 유출시도용 Trojan이며 웹사이트를 해킹하여 악성코드를 사이트에 심어 놓고, 해킹된 웹사이트는 악성코드를 유포하는 숙주 역할을 하게 된다. 해킹 당한 웹사이트에 접속한 시스템은 인터넷 익스플로러의 취약점(MS04-013, MS05-001)을 통하여 악성코드가 설치되고, 만약 해킹 당한 사이트가 인지도 높은 사이트일 경우 확산력도 함께 높아지는 특징을 갖는다.

8월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.

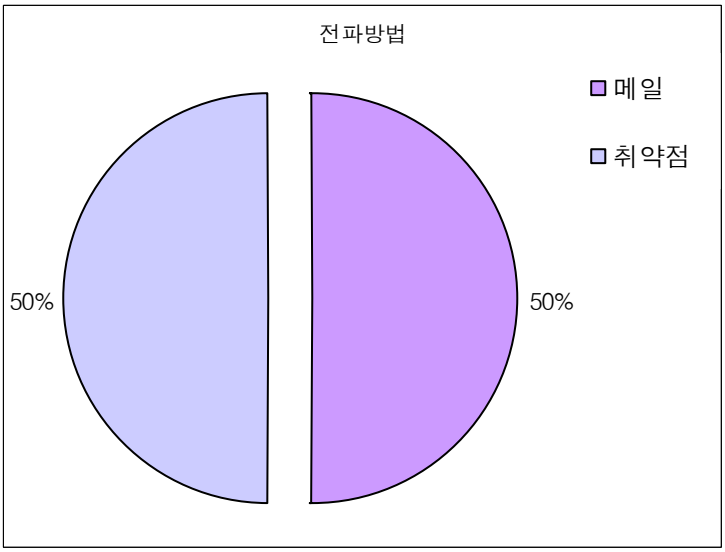


[그림1] 2005년 8월 악성코드 피해 Top 10

8월도 7월과 유사하게 10위권 내의 트로이목마가 두 자리를 차지하였고, 기타 악성코드의 비율이 대폭 늘어 났고 8월 달 Trojan.GameHack류의 변종의 수가 40여 개 넘게 등장한 것이 하나의 예이다.

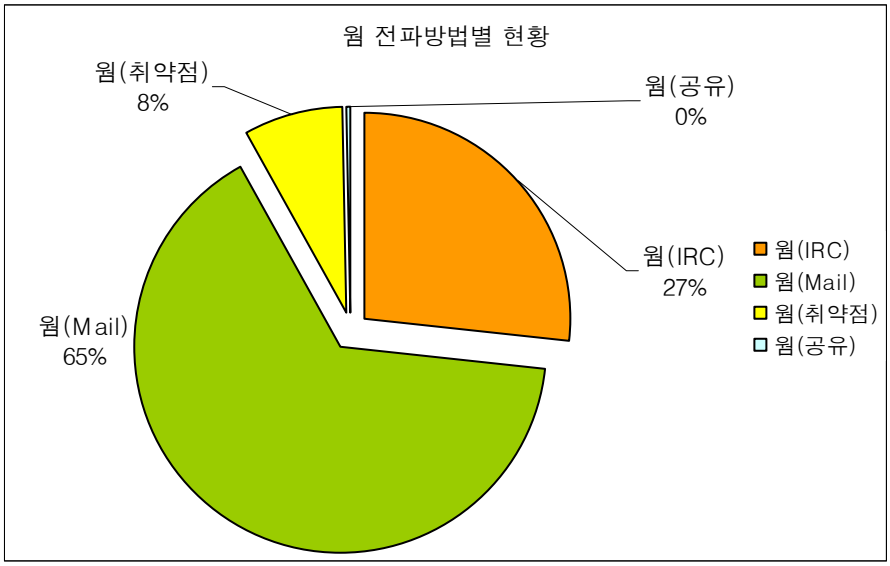
8월 악성코드 Top 10 전파방법별 현황

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



[그림2] 악성코드 Top 10의 전파 방법별 현황

[그림2]에서와 같이 피해순위 Top 10에 랭크된 악성코드의 50%가 메일을 이용하여 전파되고 있다. 지난 7월에 비해 메일은 10%가 감소하고 네트워크와 운영체제 취약점을 이용한 전파가 10%가 증가하였다. 8월에는 MS NT계열 OS의 플러그 앤 플레이의 취약점(MS05-039)이 공개된 부분도 취약점 이용 증가율에 영향을 주었다. 이에 대해 시스템의 취약점을 주기적으로 살피고 관련 취약점에 대한 보안패치를 적용해야 한다.

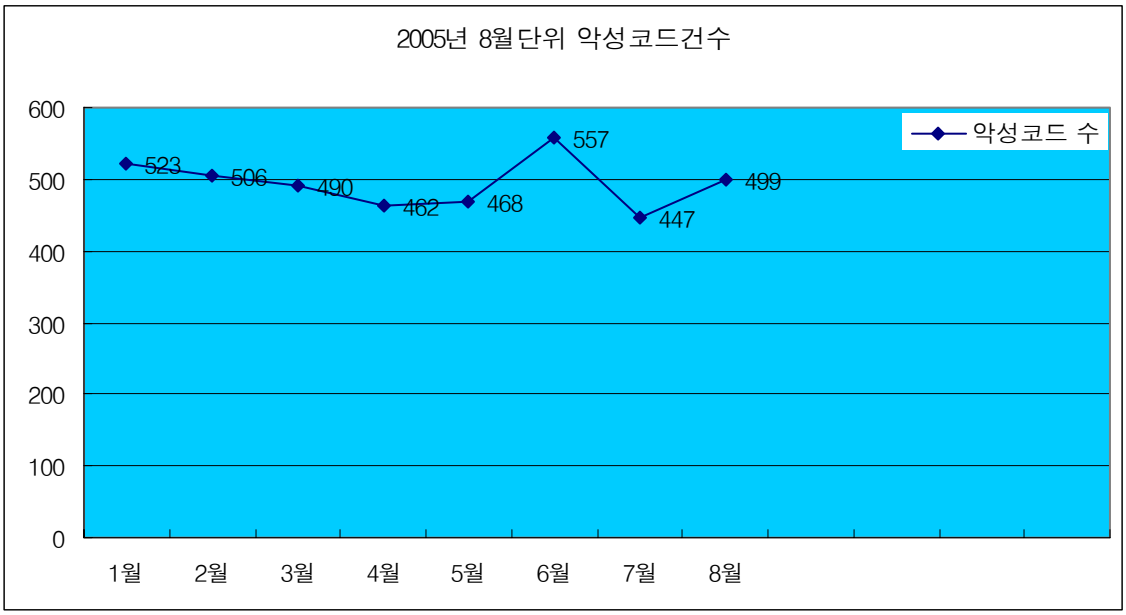


[그림3] 8월에 피해 신고된 웜의 전파방법 별 현황

[그림3]은 8월에 피해 신고된 웜의 전파방법에 대한 현황으로, 이메일(Mail)과 인터넷 채팅(IRC)이 92% 차지하는 것으로 집계되었다. 이는 지난 7월 달보다 2%가 감소한 수치이고, 취약점을 이용한 전파가 2%가 증가하였다. 취약점으로 전파되는 웜에 대해서 사전에 방지하기 위해서는 읽기/쓰기 공유 폴더 사용을 자제하고 최신 보안패치와 함께 관리 계정의 비밀번호를 영문, 숫자, 특수문자의 조합하여 웜의 침입을 막는 노력이 필요하다.

월별 피해신고 악성코드 건수 현황

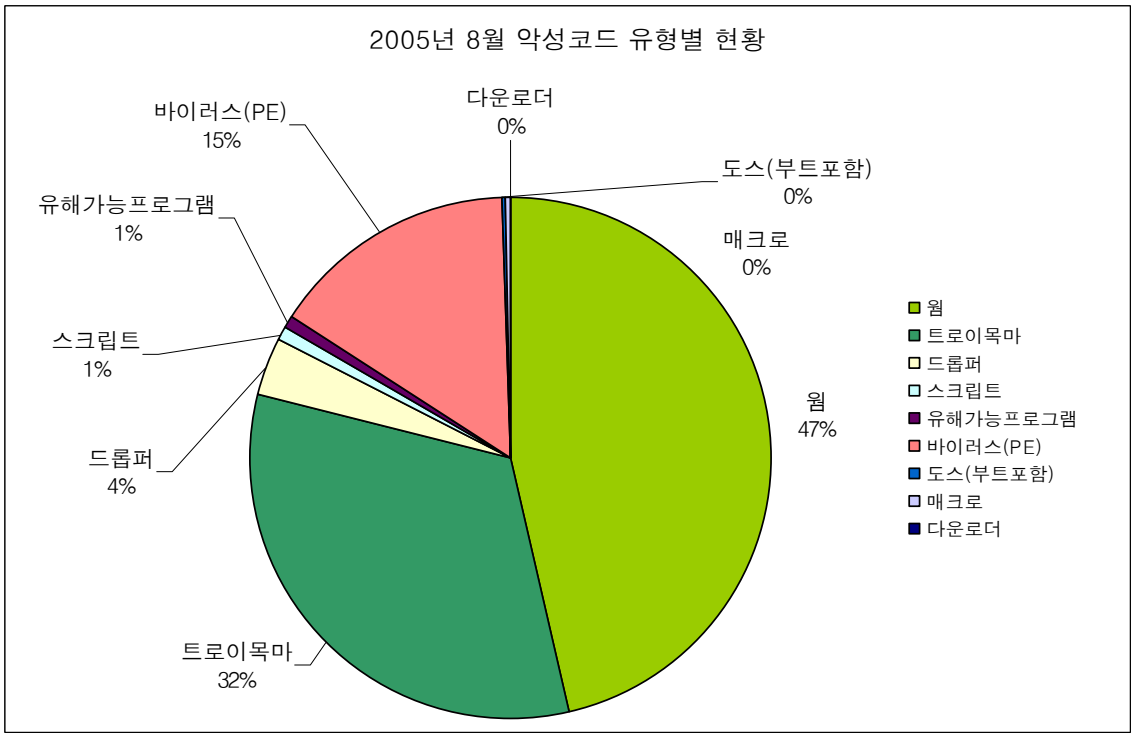
8월에 피해 신고된 악성코드는 499개이다. 트로이목마의 피해로 인해 증가한 것으로 보인다. 특히 기타 악성코드 부문에서 리니지 핵 변종 등 트로이목마 수치가 늘어났다.



[그림4] 2005년 월별 피해신고 악성코드 수

주요 악성코드 현황

악성코드 유형별 현황은 [그림5]와 같다.



[그림5] 악성코드 유형별 현황

8월에는 7월에 비해 웜이 5% 가량 증가한 반면, 비율상으로 트로이목마는 7% 가량 줄어 들었다. 트로이 목마 변종 수는 늘어 났지만, 전체 피해 비율은 줄어 들었다. 이는 보안패치

설치 및 백신의 최신엔진 업데이트 등 일반 사용자 보안 의식 발전 결과로 보여진다.

바이러스 비율이 꾸준히 증가하여 지난 7월에 비해 현재 7% 증가하였다. 이는 바이러스이지만 공유폴더 및 Netbios를 이용한 유포기능을 갖고 있는 Win32/Tenga.3666, Win32/Parite의 피해 신고 증가가 원인이다.

8월은 Win32/Zotob.worm과 Win-Trojan/Xema 의 Top 10위권 진입에서도 알 수 있듯이 취약점을 이용하는 악성코드의 증가와 함께 새로운 취약점 이용과 웹 사이트 해킹 등 보안의식의 중요성이 더욱 부각되었다고 볼 수 있다.

예방을 위해서는 우선 전산 관리자들은 주기적으로 웹 서버 등 중요 시스템의 보안 취약점을 사전에 체크하고, 최신 패치 프로그램을 설치하는 것이 중요하며, 일반 사용자들은 이런 종류의 피해를 막기 위해서 최신 보안패치와 함께 최신 버전의 백신프로그램으로 실시간 감시 기능을 사용하는 습관이 필요하다.

(1) 8월 국내 신종 (변형) 악성 코드 발견 동향

* 작성자: 정진성 주임 연구원 (jsjung@ahnlab.com)

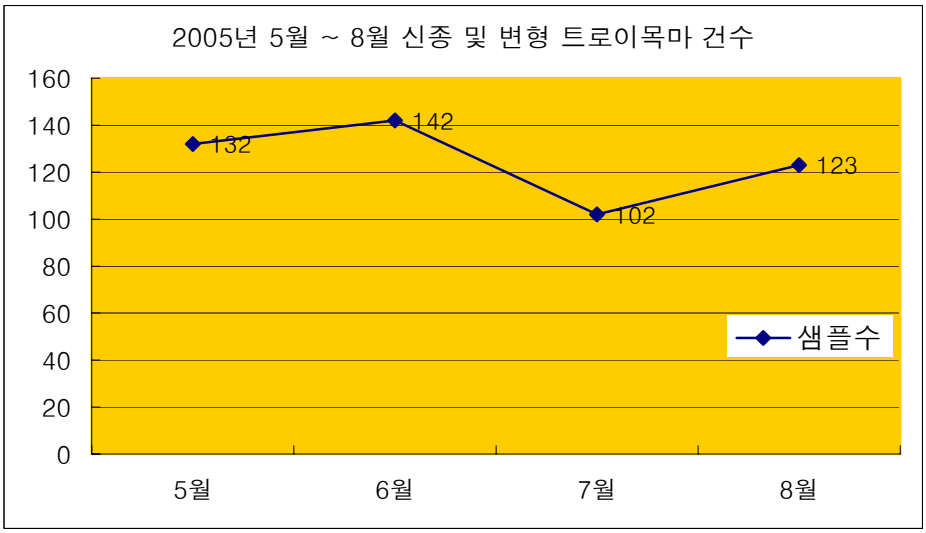
8월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1], [그림2]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비 윈도우	합계
70	123	29	2	1	1	0	0	10	0	236

[표1] 2005년 8월 유형별 신종 (변형) 악성코드 발견현황

8월은 7월과 비교하여 약간의 증가를 보였는데 원인으로는 트로이목마와 'IRCBot 웜' 이 증가하였다. 'IRCBot 봇' 은 특이할 만하게 증가한 수치는 아니나 트로이목마는 지난달과 비교하여 무려 23건이나 증가하였다.

다음은 8월까지 최근 4개월간의 국내고객으로부터 접수된 트로이목마의 샘플 수를 조사해보았다. 트로이목마의 증가는 올해 5월부터 시작 되었다. 그전까지는 'IRCBot 웜' 에 기인하여, 웜이 가장 많은 샘플접수건수를 보였다.



[그림1] 최근 4 개월간 트로이목마 발견건수

트로이목마의 증가는 여러가지 원인이 있겠지만, 국내 웹 사이트 해킹후 국내 온라인 게임 관련 트로이목마의 설치가 가장 큰 원인이라고 분석된다.

트로이목마의 증가추세는 비단 국내에만 보여지는 이상 현상이 아니다. 전통적으로 트로이목마는 다른 악성코드보다 수치 면에서 월등한 발견건수를 보였다. 즉, 웜은 발견 건수 자

체는 다른 악성코드보다는 많지만 트로이목마와 비교하였을 때, 발견 건수보다는 적고 동시 다발적으로 감염 및 피해가 큰 반면에, 트로이목마는 발견 건수가 다른 악성 코드에 비하여 다수 발견되지만, 웜보다는 국지적으로 발견되고, 그 피해 범위도 한정되어지는 것이 일반적이다.

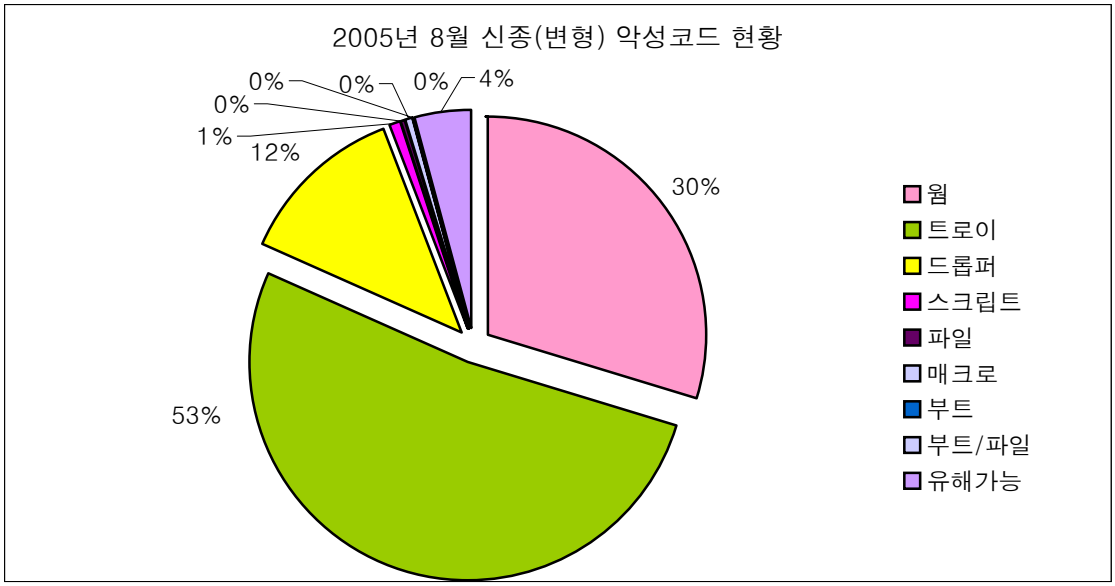
이번달에 트로이목마의 증가원인을 살펴보면 다음과 같다.

- Win-Trojan/Bagle 변형증가
- Win-Trojan/GrayBird 및 변형의 증가 (Win-Trojan/Hupigon)
- Win-Trojan/LineageHack 및 Win-Trojan/KorGameHack 등의 게임계정탈취 증상을 보이는 트로이목마 증가
- 그외 Win-Trojan/Downloader 증가

특히 Win-Trojan/GrayBird (이하 그레이버드 트로이목마) 변형과 이 소스를 변형하여 제작된 Win-Trojan/Hupigon (이하 휘피곤 트로이목마)가 특정 고객부터 다수 접수 되었는데 모두 중국산 트로이목마이다. 이 트로이목마는 스스로 확산하는 코드를 가지고 있지 않아 시스템에 누군가 불법적인 접근을 한 뒤 설치가 되었을 것으로 추정하고 있다.

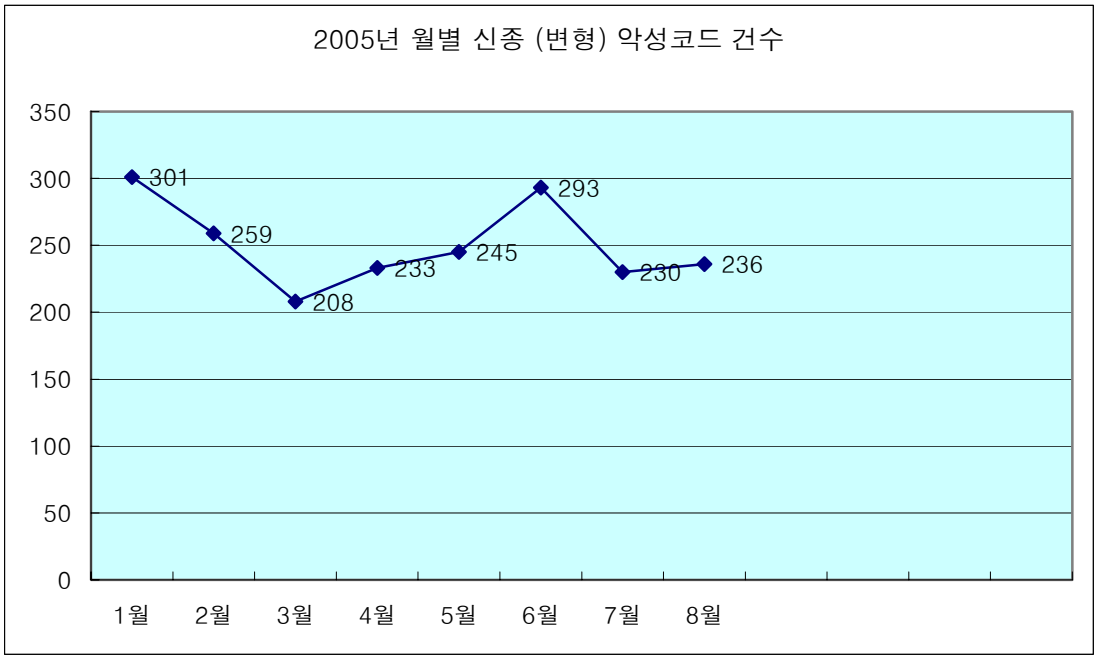
국내 온라인 게임의 계정을 탈취하는 트로이목마류는 지난 4월부터 끊임없이 변형이 발견, 보고되고 있으며 이번 달에도 다수가 보고 되었다.

[그림2]은 8월 신종(변형)악성코드의 비율을 나타낸 것이다. 트로이목마가 전체의 반 이상의 비율을 차지 하고 있다.



[그림2]2005년 8월 신종(변형) 악성코드 비율

다음은 국내고객으로부터 접수된 신종 및 변형의 악성코드의 건수를 나타내고 있다. 샘플은 국내고객 이외에 다양한 곳에서도 접수를 받고 있다. 실제로 매월 엔진에 추가되는 악성코드의 수는 이보다 훨씬 더 많은 수가 들어간다.



[그림3]2005년 월별 신종(변형) 악성코드 발견 현황

8월 주요 신종(변형) 악성코드 정리

이번 달에 최고의 이슈는 당연히 "MS05-039 취약점과 공격코드 (Exploit code) 공개 그리고 이를 사용한 악성코드의 대거 등장" 일 것이다.

* MS05-039 취약점(영문) 정보
http://www.microsoft.com/technet/security/Bulletin/MS05-039.mspx

* MS05-039 취약점(한글) 정보
http://www.microsoft.com/korea/technet/security/bulletin/MS05-039.mspx

일명 PnP 취약점으로도 알려진 이 것은 윈도우 2000 환경에서는 기존의 Win32/Sasser.worm 또는 Win32/Blaster.worm 이 이용했던 취약점만큼이나 매우 심각한 형태이다. 다행이라면 이 취약점을 이용한 공격코드가 모든 언어의 윈도우 2000 에서 동작하는 형태가 아니라는 점과 많은 사용자들이 이 취약점으로부터 비교적 안전한 윈도우 XP 환경이라는 점이었다.

공격코드가 공개된 후 이를 사용한 악성코드가 쏟아져 나왔다. 특히 그 동안 오래된 취약점만 이용해왔던 악성 IRCBot 웜이 이 취약점을 이용한 변형이 발견 되었으며 이메일과 취약점을 결합한 형태도 등장하였다.

이슈가 되었던 이번달의 악성코드는 다음과 같다.

▶ 윈도우 Vista 에 포함될 예정인 MSH 관련 악성코드

베타가 발표된 윈도우 XP 차기 운영체제인 윈도우 Vista (코드명 롱혼)에는 강력한 쉘 기능을 가진 환경과 이에 동작하는 스크립트인 MSH (Microsoft Command Shell)가 포함 되었다. 이 환경에서의 악성코드 제작이 가능할 것이라는 것은 일년 전쯤 안티 바이러스 컨퍼런스에서도 소개된 바 있다. 윈도우 Vista 의 MSH 환경에서 동작하는 첫 악성코드라는 타이틀을 거머쥔 이 악성 스크립트는 다행히도 MS가 서버 버전의 Vista에만 쉘 기능을 지원하기로 하여 일반 사용자에게 큰 피해는 주지 못할 것으로도 보인다.

▶ Win-Trojan/GrayBird 변형 (Win-Trojan/Hupigon)

중국산 트로이목마인 Win-Trojan/GrayBird (이하 그레이버드 트로이목마)는 구종의 트로이목마이지만, 그 변형이 계속 만들어져 배포되고 있다. 중국에 특정 사이트를 가지고 있으며 제작자는 새로운 변형을 만들어 업로드하고 있다. 환경 설정 파일 등을 통하여 이를 다운로드 받는 다른 악의적인 목적을 가진 사용자는 자신만의 변형을 만들고 이를 실행 압축하여 사용하고 있다. 트로이목마는 기본적인 백도어 기능을 가지고 있으며 자신을 은폐하거나 안티 바이러스의 진단을 방해하기도 한다.

▶ Win32/Zotob.worm

MS05-039 취약점을 이용한 가장 잘 알려진 Win32/Zotob.worm (이하 조톱 웜)은 취약점 발표 이후 얼마 되지 않은 시간에 발견된 악성코드이다. 비슷한 변형이 나와서 일부에서는 진단명 결정에 혼란을 주기도 하였다. 초기에 발견된 형태는 이미 알려진 Win32/Mytob.worm (이하 마이톱 웜)과 매우 유사하였기 때문이다. 변형여부에 따라 이메일 전파증상이 포함된 형태도 있다. 악성코드 형태로는 해당 취약점을 이용했다는 것을 빼고는 그리 특이할 만한 것이 없으며 이 악성코드 제작자는 체포된 것으로 알려졌다.

▶ Win32/Kelvir.worm.29226

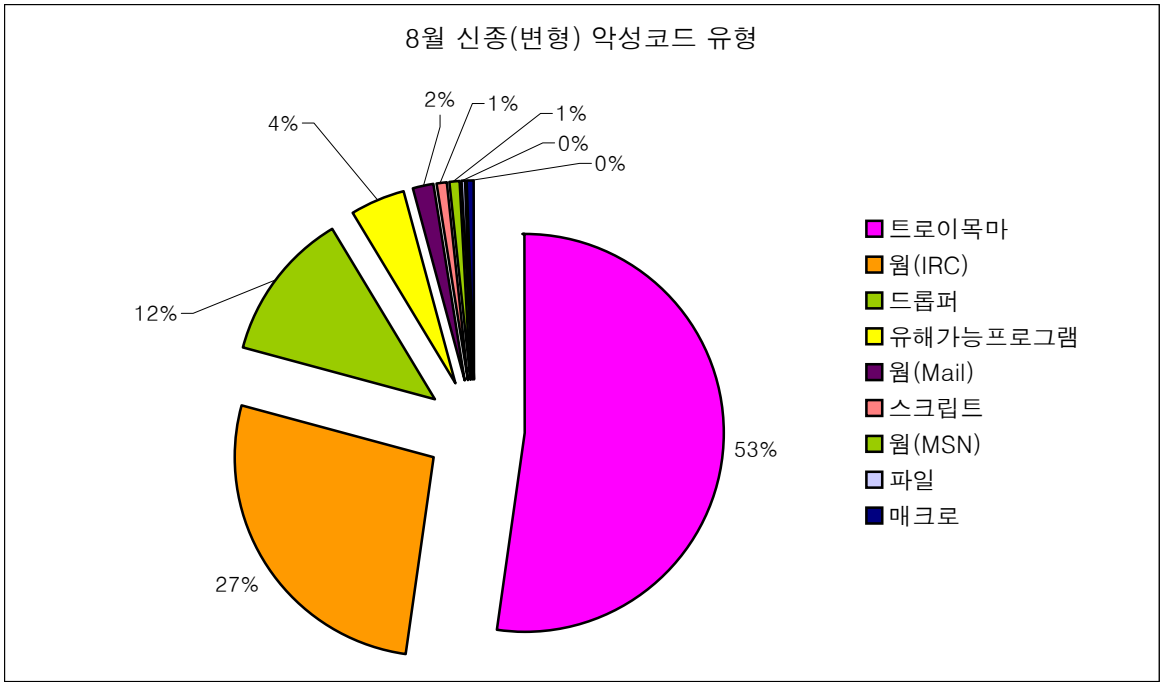
메신저로 전파되는 Win32/Kelvir.worm.29226 (이하 캘비르 웜) 역시 이전에 발견된 캘비르 웜의 변형중에 하나이다. 이 웜은 매스컴에도 소개되었는데 그 이유는 메신저로 자신을 다

운로드 하라는 메시지를 몇 개국의 언어로 보내기 때문이다. 일부 매스컴은 조금 과장된 표현을 사용하기도 하였는데 이것은 웜 내부에 숨겨진 문자열이 감염된 시스템의 윈도우 언어를 인지하고 보내기 때문에 가능한 것이다. 이외에는 기존 캘비르 웜과 다를게 없다.

▶ Dropper/MultiDrop.54808

국내에서 제작된것으로 확인된 Dropper/MultiDrop.54808 (이하 멀티드롭)은 유명한 게임인 StarCraft 의 맵핵을 Drop 하여 사용자를 속이고 내부적으로 스크립트 제작 툴킷으로 제작된 트로이목마를 실행하여 하드 드라이브의 로컬 드라이브를 삭제하도록 되어 있다. 스크립트 내부에는 국내 유명 개인 홈페이지 링크가 backward로 포함되어 있고 특정인을 비방하는 메시지를 담고 있었다.

다음은 8월에 발견된 신종 및 변형 악성코드들을 유형별로 분류한 것이다. 지난달에 이어서 파일 및 매크로 관련 악성코드가 이번 달에도 발견 되었다. X97M/Acute 라고 명명된 엑셀 매크로 바이러스로 인도네시아에서 제작된 것으로 추정되는 문자열과 SARS 관련 메시지를 담고 있었다. 올해 경우 작년보다 신종 또는 변형의 매크로 바이러스가 종종 보고 되고 있는데, 주로 국외에서는 워드 매크로 바이러스가, 국내에서는 엑셀 매크로 바이러스가 보고되고 있다. 국외에 비하며 극히 낮은 발견건수이지만 주로 기업 사용자들로부터 보고되며 피해를 주고 있어 당분간 주의가 필요하다.



[그림4] 8월 신종 (변형) 악성코드 유형별 현황

윈도우 실행파일을 감염 시키는 파일 바이러스 경우는 Win32/Hidrag.B 가 발견 되었다. 역시 구종의 윈도우 파일 바이러스이며 8월에 발견된 형태는 약간 수정된 변형이었으나, 바이러스의 감염기법이나 증상은 원형과 다르지 않았다.

올해 중반기부터 악성 IRCBot 웜에 치우쳐있던 악성코드의 유형이 2~3 년 전과 같이 트로이 목마가 강세를 보이고 다양한 형태의 악성코드가 보고되고 있어 과거의 악성코드의 Trend 가 다시 돌아오고 있는 것은 아닌지 추정해본다.

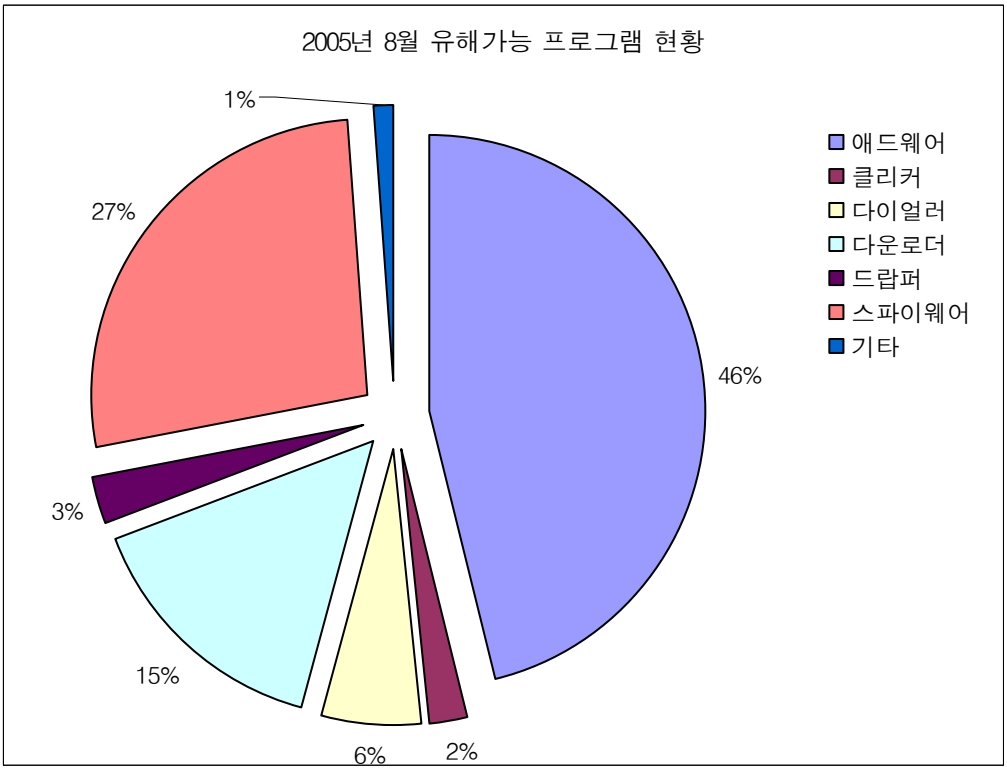
II. 8월 AhnLab 스파이웨어 동향

작성자: 김정석 주임연구원(js_kim@ahnlab.com)

8월 한달 동안 접수된 신종(변형) 유해가능 프로그램 건수는 [표1], [그림1]과 같다.

애드웨어	스파이웨어	다운로더	다이얼러	드롭퍼	클리커	기타	합계
189	110	62	24	11	9	5	410

[표 1] 2005년 8월 유형별 신종(변형) 유해가능 프로그램 발견 현황



[그림 1] 2005년 8월 발견된 유해가능 프로그램 비율

2005년 7월과 마찬가지로 애드웨어(Adware)의 발견 비율이 전체의 46%로 가장 높으며, 7월에 비해서 다운로더(Downloader)의 발견 비율이 감소한 반면 스파이웨어(Spyware)의 발견 비율이 증가한 것을 볼 수 있다.

8월 발견된 전체 애드웨어 189개 중 툴바(Toolbar) 형태의 애드웨어가 39개로 전체의 약 21%를 차지하고 있다. 특히 사용자 동의 없이 설치되어 IE 설정을 변경하고 다수의 광고를 노출하는 엘리트툴바(Win-Adware/ToolBar.EliteBar)에 대한 감염신고가 꾸준히 접수되고 있

으며 변형 또한 지속적으로 배포되고 있는 것으로 보인다.
사용자 동의 없이 바탕화면이나 IE 설정을 변경하고 스파이웨어에 감염되었다는 허위 경고 메세지를 노출하여 피에스가드(Win-Adware/Rogue.PSGuard) 같은 가짜 안티스파이웨어 프로그램의 설치를 유도하는 스파이웨어 애드클리커(Win-Clicker/Spywad)의 신종(변형) 프로그램의 피해사례도 꾸준히 보고되고 있다.

2005년 8월 30일 정보통신부에서 스파이웨어 기준안을 발표하였다. 이번 스파이웨어 기준안은 프로그램 동작의 측면에서 다음과 같은 7가지 행위를 하는 프로그램에 대해 스파이웨어로 규정하고 있다.

○ '스파이웨어'는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조 제2항의 규정에 의한 악성프로그램[1]의 일종임
○ 이용자의 동의 없이 또는 이용자를 속여 설치되어 다음 각호의 1에 해당하는 행위를 수행하는 프로그램은 '스파이웨어'에 해당됨

1) **웹브라우저의 홈페이지 설정이나 검색 설정을 변경 또는 시스템 설정을 변경하는 행위**
2) **정상 프로그램의 운영을 방해□중지 또는 삭제하는 행위**
3) **정상 프로그램의 설치를 방해하는 행위**
4) **다른 프로그램을 다운로드하여 설치하게 하는 행위**
5) **운영체계 또는 타 프로그램의 보안설정을 제거하거나 낮게 변경하는 행위**
6) **이용자가 프로그램을 제거하거나 종료시켜도 당해 프로그램 (당해 프로그램의 변종 프로그램도 포함)이 제거되거나 종료되지 않는 행위**
7) **컴퓨터 키보드 입력 내용이나 화면 표시 내용을 수집/전송하는 행위**

이번 정보통신부의 스파이웨어 기준안 발표로 스파이웨어를 전달 또는 유포하는 사람은 정보통신망법에 의거해 5년 이하의 징역 또는 5천만원 이하의 벌금형에 처해질 수 있다.

사용자 권리를 침해하는 '스파이웨어'에 대한 구체적인 기준안과 법률적인 처벌 근거가 마련됨으로써 스파이웨어 제작과 유포에 대한 행위가 상당수 줄어들 것으로 기대된다. 또한 그 동안 끊이지 않았던 백신, 안티스파이웨어 프로그램 제작 업체와 애드웨어, 스파이웨어 제작 업체와의 분쟁도 이번 스파이웨어 기준안 발표로 줄어들 것으로 예상된다.

[1] 악성프로그램 : 정당한 사유없이 정보통신 시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 프로그램

III. 8월 시큐리티 동향

작성자 : ASEC 분석2팀 / 정관진 주임연구원

어느덧 뜨거웠던 여름은 지나가고 가을의 햇살이 성큼 다가왔다. 가을의 햇살만큼이나 이번 달의 가장 뜨거운 이슈는 단연 마이크로소프트사에서 발표한 8월의 취약점 중 MS05-039 인 PnP(Plug and Play)서비스 취약점일 것이다. 해당 취약점이 공개된 이후 ASEC(AhnLab Security E-response Center)에서는 웜으로의 출현을 예상하였고 예상대로 공격코드가 나타나고 웜의 출현으로까지 이어졌다. 이와 같이 취약점이 공개되면 이를 이용한 악성코드가 나오기까지의 주기가 점점 짧아지고 있는 만큼 더욱 많은 주의가 필요하다. 이외에 8월15일 광복절과 관련하여 중국의 사이버 공격 등이 화두에 오르내렸다.

> 8월의 주요 취약점 현황

위험등급	취약점	공격코드 유/무
MID	“Msdds.dll” 라이브러리에 존재하는 원격코드 실행 취약점	유
MID	Microsoft Windows RDP(Remote Desktop Protocol) 서비스거부 공격 (MS05-041)	유
HIGH	인터넷 익스플로러의 COM Objects 관련 취약점 (MS05-038)	유
HIGH	Microsoft PnP(Plug and Play) 버퍼오버플로우 취약점(MS05-039)	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.

공격코드 공개 그리고 예측된 웜의 출현

현재의 악성코드 트랜드는 취약점이용 비중이 과거보다 높아졌다는 점이다. 이에 따라 사용 비중이 높은 마이크로소프트사(이하 MS)의 제품이 공격 대상이 되고 있는데, MS 에서는 매월 두번째 화요일에 보안 취약점 패치를 발표하고 있다. 8월 또한 마찬가지로 두번째 주 화요일인 9일에 총 6개의 패치를 발표하였다. 이중 PnP(Plug and Play)서비스는 원격지에서 임의의 명령어를 실행할 수 있는 취약점을 갖고 있는데, 다른 것보다도 악성코드에서 이용될 가능성이 높게 점쳐졌다. 그러한 이유로는 우선, 이전에 큰 이슈가 되었던 LSASS의 RPC 취약점과 같이 기본적으로 동작하는 서비스이기 때문에 영향을 받는 운영체제를 사용하고 있다면 공격의 대상에 포함된다는 점이다. 사용자의 개입이 없이도 공격의 대상이 되고 시스템 대상범위가 넓기 때문에 취약점을 이용한 악성코드가 나오기 좋은 조건을 갖추고 있다. 무엇보다 악성코드가 이용하기까지의 과정에 가장 중요한 역할을 담당하는 것이 공격코드의 공개다. 다음은 MS05-039 가 처음 공개되는 시점부터 악성코드가 나오기까지의 시간을 정리

한 것이다.

2005/08/09 MS05-039 MS 에서 보안취약점 권고문 공개
2005/08/11 MS05-039 첫번째, 두번째 공격코드 발견 (사용빈도 낮은 공격코드)
2005/08/12 MS05-039 세번째 공격코드 발견 (악성코드에서 이용한 코드)
2005/08/14 Zotob.A 웜 발견 (14일 밤)
2005/08/14 Zotob.B
2005/08/15 Zotob.C - Mass Mailer 기능 포함

9일날 MS 에서 권고문을 발표하고 3일만에 웜에서 이용한 공격코드가 공개되었다. 이후 공격코드가 공개된지 2일만에 Zotob 라 불리는 악성코드가 등장한 것이다. 취약점이 공개된 후 이를 이용한 공격코드가 나오기까지의 시간이 더욱 짧아지고 있다는 개념의 제로데이(0-day)에 더욱 다가가고 있고 이러한 비중은 앞으로도 더욱 높아질 것이다. 이번에 이용된 공격코드는 과거 블래스터 웜에서 이용한 공격코드 제작자가 공개한 코드로 코드와 취약점을 본다면 악성코드가 이용할 가능성이 상당히 높았던 경우였다. 물론, 이번 공격코드가 윈도우 2000에 한정되고 한글 OS 와 같은 시스템에서는 오프셋(Offset)의 위치가 정확하지 않아 60초 후에 시스템이 종료하는 에러 메시지가 나타나기도 하였지만, 향후 이번과 같이 웜의 확산에 크게 도움이 될 수 있었던 취약점의 경우는 관리자뿐만 아니라 일반 사용자도 각별한 주의가 필요할 것이다.

8월15일 광복절 중국의 대대적 사이버공격

8월15일은 1945년8월15일 일본의 식민지 지배에서 벗어난 것을 기념하고 더불어 대한민국 정부수립을 경축하는 뜻 깊은 날이다. 하지만, 이런 뜻 깊은 날에 중국 해커들이 광복절을 전후에 대규모로 일본 사이트에 대한 사이버 공격이 예정되어 있다는 소식이 전해졌다. 비록 대상이 일본 사이트이지만 한국 또한 주의를 기울이지 않을 수 없었다. 이유는 한국을 경유하여 일본을 공격한다는 계획이 있었기 때문인데 이것은 한국의 인프라가 많이 발전되어 있고 중국의 IP주소가 많이 차단되어 있는데 비해 한국은 그렇지 않다는 여러 가지 이유가 있었기 때문이다.

이러한 이유로 8월15일에 주요 기업 및 보안 업체에서는 만일의 사태에 대비하여 비상대응 체제에 들어가기도 하였지만 당일 날 별다른 사건은 발생하지 않고 하나의 해프닝으로 지나가 버렸다. 이제 사이버상에서의 이런 행동들이 쉽게 지나칠 수만은 없는 중요한 문제로 부각되고 있다. 국내의 많은 인프라들이 인터넷과 밀접해 지고 있기 때문이다. 보안은 한 순간만을 위해서가 아니라 지속적인 관심과 준비가 있어야 된다는 사실은 다시 한번 되새겨 보아야 할 것이다.

Ⅳ. 8월 세계 동향

8월 세계 악성코드 동향 중 일본의 경우는 넷스카이 웜과 같은 메일로 전파되는 웜이 확산되고 있는 것으로 분석되었다. 그러나 이와 반대로 중국의 경우에는 원격제어나 키로킹이 가능한 트로이목마 류의 큰 폭으로 증가하고 있는 것으로 분석되었다. 이러한 극동 아시아의 악성코드 분포는 메스 메일러와 트로이목마로 양극을 이루고 있는 반면 유럽 지역에는 일본과 유사한 메스 메일러가 대부분을 이루고 있으나 베이글과 마이둠 변형들은 큰 폭으로 감소하고 넷스카이 웜과 마이톱 변형들이 대부분을 차지하고 있다.

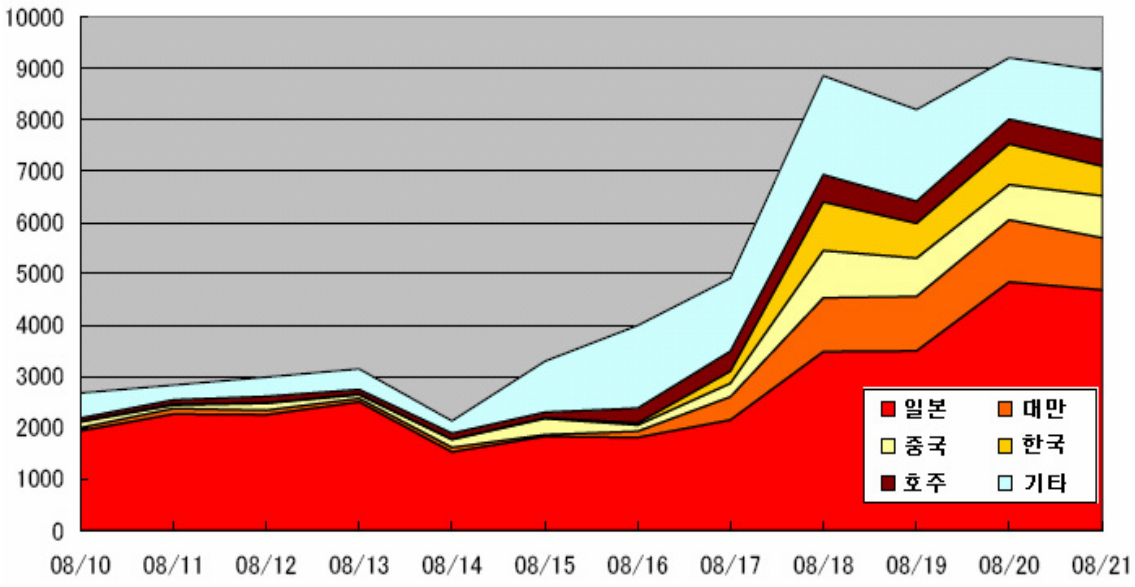
그리고 8월 15일은 세계 2차대전 종전으로 인해 일본의 패전으로 인해 중국과 한국이 독립된 날이기도 하다. 이 날을 기점으로 중국 해커 그룹들에서는 일본 우익단체들의 웹 사이트를 공격하는 계획이 알려져 주변 국가들에 대한 사이버 테러에 대한 경계심을 가지게 만들기도 하였다. 이러한 사항들을 바탕으로 8월 세계 악성코드 동향은 어떠한 변화가 있었는지 살펴보기로 하자

(1) 일본 악성코드 동향

작성자: 김소헌 주임연구원(sopara@ahnlab.com)

2005년 8월의 일본 보안 동향에서 가장 이슈가 되었던 사건은 중국 해커들의 공격시도이다. 일본의 보안관련 기관에서는 공격에 대비해서 보안 취약점에 대한 권고문을 발표하는 등 피해 예방을 위한 노력을 기울였고 우려했던 것과는 달리 일본에서 크게 피해가 보고되지는 않았다.

일본 보안 동향과 관련한 또 다른 이슈는 네트워크 트래픽의 비정상적인 증가이다. 아래의 [그림1]은 일본 경찰청(www.npa.go.jp)에서 발표한 8월 중순 일본의 TCP 445 포트를 통한 네트워크 트래픽 현황이다. 8월 15일을 전후하여 네트워크 트래픽이 급증한 것을 알 수 있다.

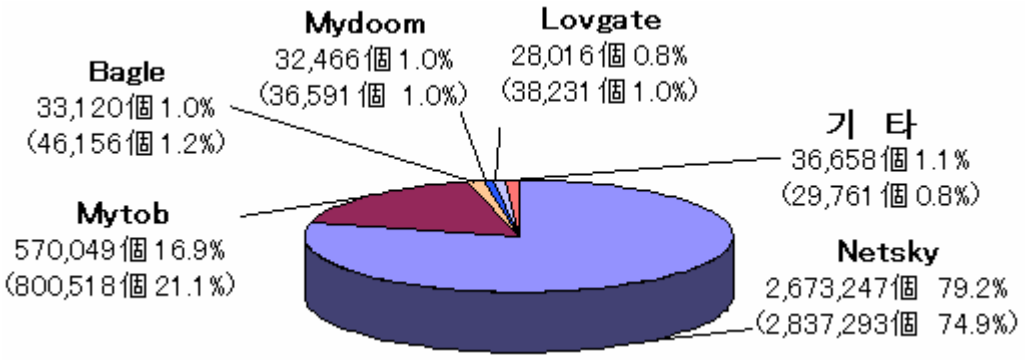


[그림1] 2005년 8월 TCP 445 포트 트래픽 증가 현황 <자료출처: 일본 경찰청>

이러한 현상이 발생한 원인에 대해서 정확하게 알 수는 없지만 비슷한 시기에 새로운 보안 취약점인 MS05-039 취약점을 이용한 웜 등 여러 형태의 악성코드가 유포된 것이 원인으로 추정된다.

1. 일본 유행 악성코드 유형별 발생현황

2005년 8월 일본의 악성코드 동향에서 주목할 점은 전월에 비해 전반적으로 악성코드의 확산도가 크게 감소한 것이다. [그림2]은 일본의 IPA(www.ipa.go.jp)에서 발표한 악성코드 통계 자료 중 일본에서 8월에 발생한 악성코드의 종류별 탐지 통계를 나타낸 것이다. [그림2]에서 볼 수 있는 것처럼 가장 많이 유포된 악성코드는 넷스카이 웜 (Win32.Netsky.worm)으로써 이러한 현상은 전월과 비교해서 크게 변화가 없다. 그러나 전반적으로 탐지된 악성코드의 양이 감소된 것을 알 수 있다.



[그림2] 악성코드 발견 건수 통계

아래의 [표1]은 2005년 8월 악성코드의 감염 통계를 나타낸 것이다. 넷스카이 웜에 의한 감염 피해가 가장 많은 것을 알 수 있는데 이는 전월과 비교해서 크게 차이가 없다. 그러나 전반적인 피해 수치가 전월에 비해 낮아진 것을 볼 수 있다.

Window/Dos Virus	금월피해	Macro Virus	금월피해	Script Virus	금월피해
	전월피해		전월피해		전월피해
Win32/Netsky	999	Xm/Laroux	11	VBS/Redlof	72
	1,125		9		59
Win32/Mytob	536	W97M/X97M/ P97M/Tristate	6	VBS/Loveletter	6
	638		8		10
Win32/Mydoom	352	W97M/Lexar	3	VBS/Soraci	5
	332				4
Win32/Bagle	303	W97M/Sting	3	Wscript/ Fortnight	4
	284				4
Win32/Klez	255	W97M/Divi	3	VBS/Internal	2
	230		4		2
Win32/Lovgate	213	WM/Sarsnan	3	VBS/Haptime	1
	249				1

[표1] 악성코드 피해 신고 현황

2. 악성코드의 감염 경로별 통계

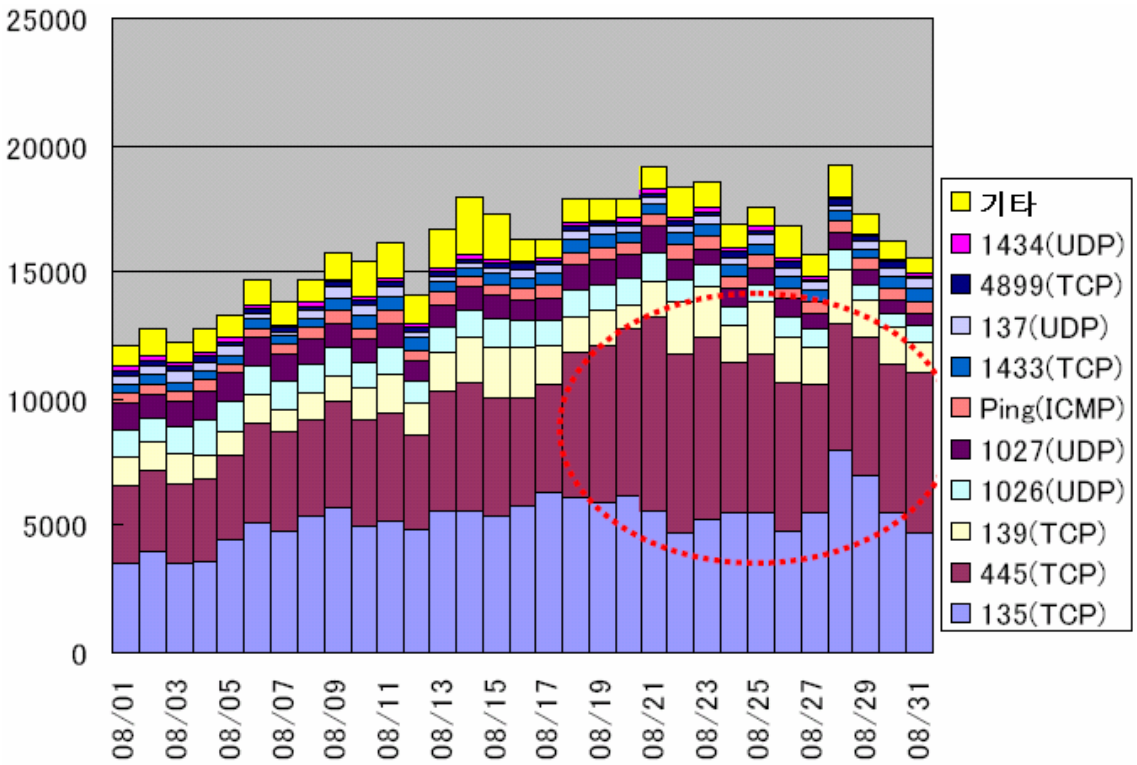
[표2]는 악성코드의 감염 경로 별 통계를 표로 나타낸 것이다. 악성코드의 감염 경로로 가장 많이 이용되는 매체는 메일로써 이는 전월과 동일하다. 전월과 비교해서 주목할 사항은 네트워크를 이용하는 악성코드의 감염이 많이 발생했다는 점이다. 이는 최근 보고된 윈도우 운영체제의 보안취약점을 이용한 웜의 공격이 증가한 것이 원인으로 분석된다.

감염경로	피해 건수					
	2005 년 8 월		2005 년 7 월		2004 년 8 월	
메일	4,290	96.00%	4,477	98.70%	5,004	98.30%
외부의 모체	4	0.10%	3	0.10%	6	0.10%
다운로드	1	0.10%	4	0.10%	5	0.10%
네트워크	171	3.80%	43	0.90%	65	1.30%
기타	4	0.10%	9	0.20%	11	0.20%

[표2] 악성코드 감염 경로 통계

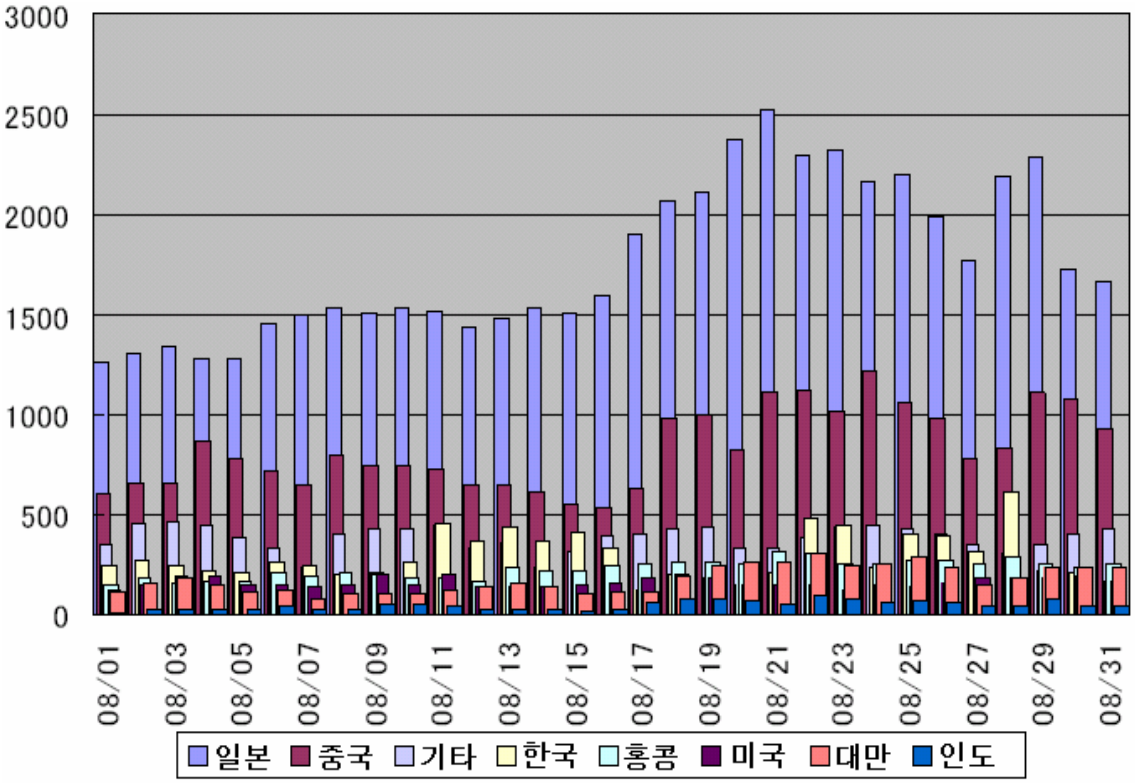
3. 일본 네트워크 트래픽 현황

2005년 8월 일본의 네트워크 트래픽 현황과 관련한 가장 큰 이슈는 TCP 445 포트의 트래픽이 급증한 것이다. [그림4]는 일본의 IPA에서 관측한 포트별 트래픽 현황이다. 8월 17일 이후로 해당 포트의 트래픽이 급격하게 증가한 것을 알 수 있다.



[그림3] 포트별 트래픽 발생 통계

[그림4]는 8월 한달 동안 발생한 국가별 네트워크 트래픽 통계를 보여준다. 8월 15일 이후로 전반적인 트래픽의 양이 증가한 것을 알 수 있다. 그러나 이러한 현상은 외부에서의 공격이라기 보다는 악성코드의 유포가 주 원인으로 추정된다. 그래프에서 볼 수 있는 것처럼 중국 이외의 다른 나라에서도 전반적으로 트래픽 양이 많이 증가한 것을 볼 수 있다.



[그림4]국가별 네트워크 트래픽 현황 <자료출처 : 일본 IPA>

(2) 중국 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

8월 중국 악성코드 동향은 지난 달을 기점으로 증가하기 시작한 악성 봇이 다시 줄어드는 추세를 보이고 있다. 이와 함께 루트킷(Rootkit) 형태의 트로이목마(V3 진단명 Win-Trojan/Rootkit)도 많은 수가 줄어 들었다. 그러나 지속적인 증가 추세를 보이고 있는 다양한 형태의 트로이목마는 이번 8월 달 역시 증가 추세를 보이고 있다. 그리고 이와 함께 원격제어 및 키로깅 형태의 트로이목마가 특히나 높은 증가 추세를 보이고 있어 개인 사용자들의 각별한 주의가 필요하리라 생각된다. 이러한 사항을 바탕으로 8월 중국에는 어떠한 동향의 변화가 있었는지 살펴보도록 하자.

1. 악성코드 TOP 5

순위 변화	순위	Rising
New	1	Trojan.PSW.LMir
↑ 1	2	Backdoor.Gpigeon
↓ 2	3	Backdoor.Rbot

↑ 1	4	Backdoor.Codbot
New	5	Worm.QQ.TopFox

[표1] 2005년 8월 Rising 악성코드 TOP 5

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

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

[표2] 2005년 8월 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 8월 악성코드 TOP 5이다. 먼저 라이징의 순위를 살펴보면 지날 달 순위에 포함되지 않은 엘미르핵 트로이목마(V3 진단명 Win-Trojan/LmirHack)의 급격한 증가가 8월 달의 가장 큰 이슈로 볼 수 있다. 그리고 그 뒤를 이은 원격제어 형태의 지피건 트로이목마 (V3 진단명 Win-Trojan/GrayBird, Win-Trojan/Hupigon)가 지난 달 보다 1계단 상승하며 지속적인 증가 추세를 보이고 있다. 그러나 이와 반대로 악성 봇 변형은 2계단 하락하면서 전반적인 감소 추세를 보이고 있으나, 감염 기법 등으로 미루어 네트워크 전반에는 아직도 많은 수의 악성 봇이 존재하고 있을 것으로 추정 된다. 마지막으로 5위를 차지한 Worm.QQ.TopFox는 중국에서 제작된 QQ 메신저를 통해서 전파되는 웜으로 감염된 사용자의 QQ 메신저 상에 등록되어 있는 사람들에게 특정 문구를 보내어 해당 문구를 클릭할 경우 웜이 실행된다.

강민의 순위에는 인터넷 익스플로러의 취약점을 이용하는 Trojan/Script.Seeker가 2계단 상승하면서 높은 증가 추세를 보이고 있다. 그러나 이와 반대로 악성 봇의 경우에는 라이징의 순위와 유사하게 감소 추세를 보이고 있다.

2. 주간 악성코드 순위

순위	1 주	2 주	3 주	4 주
1	Trojan.PSW.LMir	Trojan.PSW.LMir	Backdoor.Gpigeon	Trojan.PSW.LMir
2	Backdoor.Rbot	Backdoor.Gpigeon	Backdoor.Sdbot	Backdoor.Gpigeon
3	Win-Trojan/ GrayBird	Trojan.Clicker.AdShow	Trojan.PSW.LMir	Backdoor.Sdbot

4	TrojanDroper.Worm.Bagz	Backdoor.Sdbot	Worm.QQ.TopFox	Trojan.PSW.QQRobber
5	Backdoor.DxdBot	Backdoor.Rbot	Backdoor.Codbot	Backdoor.Rbot

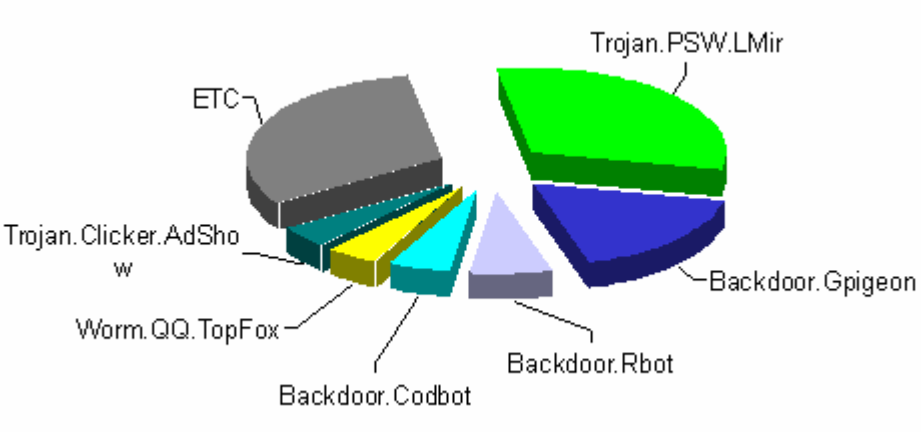
[표3] 2005년 8월 Rising 주간 악성코드 순위

순위	1 주	2 주	3 주	4 주
1	Backdoor/SdBot.atp.Rootkit	Trojan/QQMsg.Zigui.b	Trojan/Script.Seeker	
2	Trojan/Script.Seeker	Trojan/Script.Seeker	Trojan/QQMsg.Zigui.b	
3	Trojan/WebImport	Backdoor/SdBot.atp.Rootkit	Trojan/WebImport	
4	Trojan/QQMsg.Zigui.b	Trojan/WebImport	Backdoor/SdBot.atp.Rootkit	
5	TrojanDownloader.Agent.kk	Exploit.MhtRedir	Exploit.MhtRedir	

[표4] 2005년 8월 JiangMin 주간 악성코드 순위

주간 악성코드 순위를 살펴보면 라이징의 경우 엘미르핵 트로이목마는 3주 동안 지속적으로 1위를 차지하며 8월 한 달동안 지속적인 감염 신고가 있은 것으로 분석된다. 그리고 지피건 트로이목마 역시 8월 2주부터 급격한 감염 신고의 증가하기 시작한 것으로 보여진다. 엘미르핵 트로이목마와 지피건 트로이목마의 감염 증가는 당분간 지속될 것으로 보여지며 이에 따른 개인 사용자들의 각별한 주의가 필요하리라 예상된다. 7월부터 감소 추세를 보이기 시작한 백쯔 웜(V3 진단명 Win32/Bagz.worm)은 8월 1주차를 마지막으로 순위권 밖으로 밀려난 점으로 미루어 중국 국내에서 백쯔 웜에 의한 감염이 감소한 것으로 추정된다. 그리고 이와 함께 악성 봇 역시 8월 주간 순위 변화와 같이 전반적인 감염 활동이 감소하고 있는 것으로 분석된다.

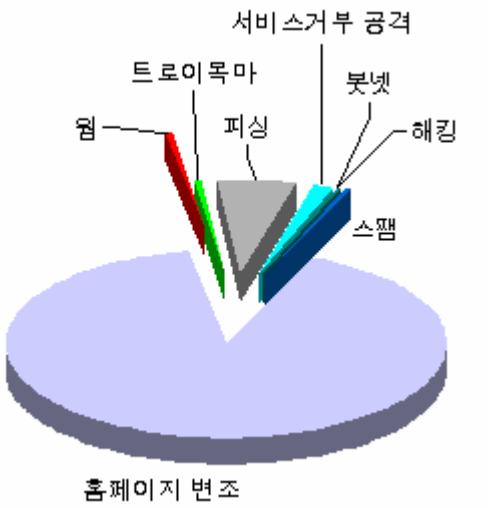
3. 악성코드 분포



[그림1] 2005년 8월 Rising의 악성코드 분포

위 [그림1]은 라이징의 8월 악성코드 분포도 이다. 해당 분포도의 엘미르핵 트로이목마가 전체의 31%를 차지하고 있다. 엘미르핵 트로이목마는 감염된 시스템의 모든 프로세스에 키로깅을 위한 라이브러리 파일을 인젝션하여 실행된다. 그리고 감염된 시스템의 사용자가 특정 온라인 게임 웹 사이트를 방문하게 될 경우 사용자의 계정과 암호를 후킹하여 특정 메일 주소로 전송하는 기능을 가지고 있다. 이러한 특정 온라인 게임의 사용자 계정과 암호를 취득하기 위해 제작된 트로이목마로는 엘미르핵 외에도 리니지핵 트로이목마(V3 진단명 Win-Trojan/LineageHack), 항핵 트로이목마(V3 진단명 Win-Trojan/HangHack)와 코게임핵 트로이목마(V3 트로이목마 Win-Trojan/KorGameHack) 등이 있다. 이러한 트로이목마는 개인에 의해 제작되기 보다는 조직적으로 제작되고 있으며 중국 언더그라운드 해킹 그룹 중에는 이러한 트로이목마 제작 프로그램까지 유포되고 있는 것으로 확인되었다. 확인된 바로는 엘미르핵 트로이목마의 주된 감염 경로는 보안이 취약한 웹 사이트에 트로이목마를 다운로드 하는 iFrame 링크를 첨가하는 기법을 쓰고 있다.

4. 보안 사고 통계



[그림2] 2005년 8월 CNCERT/CC의 보안사고 분포

[그림 2]는 중국 CNCERT/CC가 작성한 8월 중국 보안 사고 통계로서 지난 7월 77건이었던 홈페이지 변조는 1042건으로 급격한 증가치를 보였다. 홈페이지 변조 피해를 입은 시스템은 대부분이 리눅스 시스템이며 그 다음이 윈도우 2000과 윈도우 2003을 웹 서버로 운용하는 것으로 분석되었다.

(3) 세계 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

2005년 8월은 마이톱 웜(Win32/Mytob.worm) 변형의 극성과 지난 해 많은 피해를 입혔던 마이둠과 베이글 등 과거 웜들의 몰락으로 세대교체가 일어났다고 볼 수 있다. 또 8월 중순을 뜨겁게 달구었던 조톱 웜(Win32/Zotob.worm) 사건과 마이톱 웜과 조톱 웜의 제작자 검거 소식도 빼놓을 수 없다.

영국의 소포스(http:/www.sophos.com)의 2005년 8월 피해 통계[1]를 보면 1위는 넷스카이 변형이 차지고하고 있으며 나머지는 대부분 마이톱 변형과 유럽에서 많이 발견되고 있는 자피 웜(Win32/Zafi.worm) 변형이다.

러시아의 캐스퍼스키 연구소(http://www.kaspersky.com)의 2005년 8월 피해 통계[2]에 따르면 1위가 마이톱 변형, 2위가 넷스카이 변형이고 대부분이 마이톱 변형이 20위까지 순위에 포함된 것을 알 수 있다. 특히 2004년 초부터 많은 피해를 입혔던 마이둠 웜(Win32/MyDoom.worm)과 베이글 웜(Win32/Bagle.worm)은 순위에서 완전히 사라졌다. 하지만, 마이톱 역시 마이둠에 악성 IRC봇 기능을 추가한 기능 향상 버전으로 볼 수 있다.

2005년 8월 15일은 1945년 일본의 패망으로 한국과 중국에게 독립 60 주년 기념일이었다. 중국 해커가 일본 우익 관련 사이트에 해킹을 시도할 것이며 경유지로 한국을 이용할지도 모른다는 우려가 발생했다. 하지만, 평상시와 다른 일이 발생하지 않았지만 새로운 웜인 조톱(Win32/Zotob.worm)이 발견되었다. 이 웜은 마이톱 웜에 새롭게 발견된 MS05-039 취약점을 공격하는 기능을 포함했다. 새롭게 발견된 취약점인 만큼 패치가 적용되지 않는 시스템이 다수 존재했으며 ABC, CNN 등의 피해가 발생해 언론에 대대적으로 알려졌으며 마이크로소프트사에서도 관련 정보를 제공했다.[3] 하지만, 이 웜은 패치되지 않은 영문 윈도우2000 에서만 감염이 발생하므로 영문 윈도우를 사용하지 않거나 윈도우 XP 사용자는 감염되지 않으

[1] http://www.sophos.com/pressoffice/pressrel/uk/20050901topten.html
[2] http://www.viruslist.com/en/analysis?pubid=169665202
[3] http://www.microsoft.com/korea/security/incident/zotob.mspx

므로 비영어권 국가에서는 큰 피해가 없었으며 한국에서도 실제 감염은 보고되지 않았다. 다만, MS05-039 취약점을 공격 기법이 일반화되어 최근에 등장하는 대부분의 네트워크로 전파되는 악성 IRC 봇은 해당 취약점 공격 기능을 가지고 있으며 취약점 공격 기능이 개선되면 문제가 발생할 수 있다.

마이톱 웜과 조톱 웜을 제작 및 배포한 사람이 모로코와 터키에서 검거된 사건[1]이 있었다. 하지만, 이후에도 마이톱 변형이 계속 등장하고 있는데 제작자가 소스를 인터넷에 올려 많은 사람들이 변형을 양산해 내고 있는 것으로 보인다.

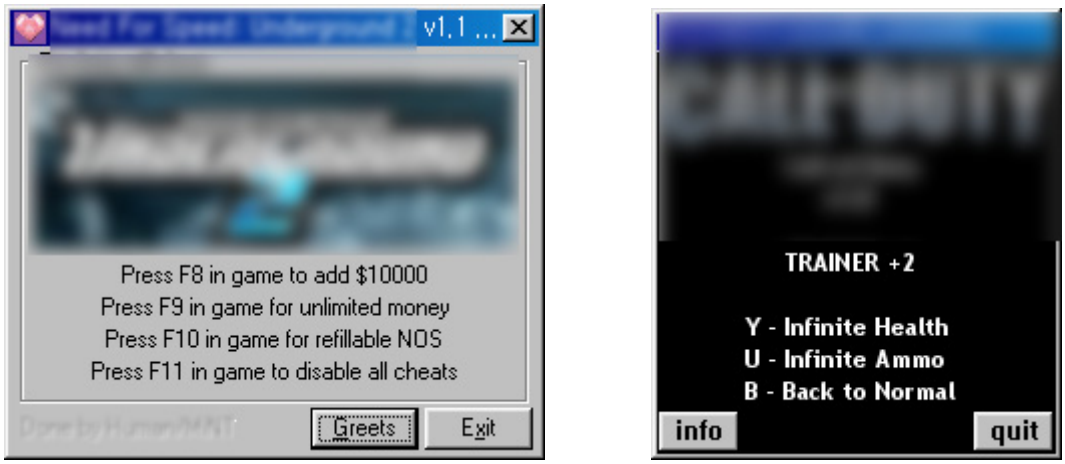
[1] http://blogs.washingtonpost.com/securityfix/2005/08/arrest_of_zotob.html

V. 이달의 ASEC 컬럼 - 온라인 게임 해킹 프로그램과 보안

작성자: 정진성 주임연구원(jsjung@ahnlab.com)

누구나 게임을 하다가 보면 막히는 곳이 있기 마련이고 이를 위해서든 아니면 다른 이유에서든 대부분의 패키지 게임들은 'Cheat Code'를 별도로 준비하여 게임을 원활히 진행할 수 있도록 한다. 물론 남용하면 그 재미가 반감되어 버리기도 하지만 온라인 게임은 컴퓨터를 상대로 플레이하는 것이 아니라 네트워크로 연결된 다른 유저들과의 경쟁을 하기 때문에 멀티 플레이 중 가능한 'Cheat Code'는 존재하지 않는다. 또한 게임진행을 매너없게 하는 불법 프로그램을 사용하는 것도 금지하고 있다.

단지 재미의 목적으로 게임을 조작한 것인데 이것이 과연 불법일까? 온라인 게임을 해킹 할 수 있는 프로그램은 어떠한 형태를 얘기하는 것일까? 일반적으로 이러한 프로그램들은 'Trainer' (최근에는 'BOT 또는 Hack' 이라고도 불리어진다.)라고 불리며 온라인 게임에서 이를 사용한 사람은 'Cheater' 라고 일컫는다.



[그림1] 유명게임의 Trainer

* 일반적으로 Trainer 는 해당 게임 캐릭터의 체력, 무기, 돈과 같은 게임 중에 필요한 데이터를 쉽게 조작해주는 프로그램은 일컫는다. 게임에 따라 다양한 기능의 Trainer가 존재한다.

* 일반적으로 BOT 은 (Robot 의 준말) 매크로와 유사하게 반복적인 형태의 진행을 자동으로 수행하거나 게임상의 타겟이나 방향 등을 유저의 개입 없이 자동으로 수행하는 것을 말한다. 대표적으로 FPS (First Person Shooting = 1인칭 슈팅 게임)류에서 AIMBot (타켓 자동조준봇)이 있다.

이번 달 컬럼의 주제는 바로 게임 해킹 프로그램에 대한 내용이다. 그러나 최근 문제가 되고 있는 온라인 게임의 사용자 계정을 탈취하는 종류의 악성코드에 관한 글이 아니라 게임 해킹 프로그램은 유틸리티를 사용하여 비정상적인 플레이를 하도록 하는 프로그램들에 대한 내용이다. 물론 게임 해킹 프로그램이란 용어가 정확하지 않은지도 모르지만(줄여서는 "게임 핵" 이라고도 표현한다), 여기서는 일반적으로 부르는 명칭을 그대로 사용하도록 하겠다.

본 글에서는 국내 패키지 게임 시장의 몰락의 배경과 게임과 보안은 언제나 공생관계 중이라는 약간의 내용을 곁들이도록 한다. 또한 과거의 게임 해킹 프로그램들은 어떠한 유형이 있었는지 알아보고 현재 온라인 게임 환경과 비교해보도록 한다. 그리고 이러한 게임 해킹 프로그램들은 어느 수준까지를 불법 프로그램으로 간주해야 하는지 고민해보고 이를 방어하는 솔루션들을 간단히 소개하도록 하겠다.

1. 국내 패키지 게임 시장의 몰락의 배경

현재 국내 온라인 게임이 성황을 이루고 있는 이유 중에 하나는 국내 게임 패키지 시장의 몰락이며, 이의 가장 큰 원인은 게임이 불법 복제, 유통되었기 때문이다. 국내 유수의 게임 개발사들은 불법유통이 그나마 적은 콘솔게임기의 게임을 개발하거나 휴대용 게임기의 게임들을 개발하는 등 적극적인 판로의 길을 가는 모습도 보였다. 여기서는 논외의 얘기이지만 콘솔게임의 타이틀도 복제되어 유통되거나 휴대용 게임기의 롬파일도 유통되고 있기 때문에 PC 게임처럼 패키지 시장이 몰락하지는 않겠지만 복제된 타이틀로 인한 정품 판매량 감소는 더 이상 두고 볼 일만은 아니 것 같다.

다시 PC 게임으로 돌아와 얘기를 해보면 오래 전부터 패키지 게임사들은 불법복제를 방지하는 차원에서 게임에 (플로피 디스켓 또는 CD) 락을 걸어 복제되지 않게 하거나 복제되더라도 정품으로 인식하지 못하게 하는 등 여러 가지 보안조치를 취하고 있다. 도스시절부터 게임을 즐긴 분이라면 'PANDORA' 와 같은 키 디스크 개념 또는 'EVERLOCK, HARDKEY' 와 같은 플로피 복사 방지 장치를 들어 봤을 것이다. CD 라는 저장매체의 등장으로 도스시절과 비슷한 Copy Protection 제품들이 CD 에서도 여럿 등장하였다. "SAFEDISK", 'STARTFORCE'. 'SecuROM' 등이 이러한 제품들이다. 또한 이 제품의 파일들은 리버싱 엔지니어링 되지 않기 위해서 파일을 분석하기 어렵게 되어 있기도 하며 CD 레코더나 공 CD 정보 등을 읽어와 복사여부를 판단하는 등 다양한 기술이 포함 되어 있다. 완벽하지는 않지만 불법복사를 방지하는 이 제품들로 하여금 게임과 보안은 오래 전부터 뗄래야 뗄 수 없는 관계를 유지해오고 있다.

2. 게임 해킹 프로그램의 궁극적인 목적?

오늘날의 온라인 게임시장의 보안은 어떠한가? 불법복제로부터는 해방되었던 온라인 게임은 가장 큰 복병 중 하나는 바로 게임 해킹 프로그램과 이를 사용하는 유저들이다. 이러한 문제가 되는 가장 큰 원인 중에 하나는 온라인 게임은 게임 내 다양한 승률 포인트를 이용하여 다른 아이템을 사거나 또는 이를 현금으로 거래할 수도 있기 때문이다. 이렇게 되면 그 피해는 게임을 즐기는 유저와 더 큰 피해는 게임 개발사들이 당하게 된다. 온라인 게임 개발사들의 수익원이 대부분 월 정액의 가입비 또는 유저들이 현금으로 구입하는 아이템 임을 감안할 때 이것을 승률 포인트 조작으로 얻을 수 있다면 평범한 유저들은 물론 개발사도 큰 피해가 온다.

* 본 글에서는 개인 또는 조직적으로 아이템을 현금 거래하는 것이 불법인지의 여부는 논의하지 않기로 한다.

대부분의 온라인 게임들은 아이템을 획득하기 위해서 일반적으로 현금으로 해당 아이템 사거나 게임을 하면서 얻어진 승률 포인트를 차감하여 아이템을 획득할 수 있게 한다. 일반 콘솔게임이나 패키지 게임이라면 단순히 게임을 하면서 얻어진 포인트로만 캐릭터의 레벨-업이나 아이템을 획득하지만 온라인 게임은 바로 '돈' 이 거래된다는 점에서 게임 해킹 프로그램 수요를 파악해버린 일부 유저들은 이점을 악용하여 자신이 개발한 프로그램을 버젓이 돈을 받고 팔고 있기도 하다. 또한 여기서는 논의하지 않기로 한 게임계정을 탈취하는 증상을 보이는 악성코드를 제작하고 유포하는 사람들의 목적은 무엇일까? 이들은 개인 또는 조직적으로 활동하기도 한다. 그렇다면 이 프로그램을 이용해서 부당행위를 하는 사람들과 이러한 프로그램을 만들어 파는 사람들의 목적은 한가지가 아니겠는가?

3. 게임 해킹 프로그램 유형

* 본 글에서는 가급적 자세한 게임 해킹 프로그램의 동작방식은 설명하지 않을 것이다.

우선 온라인 게임이나 멀티 플레이를 위해서 서버에 접속하지 않고 단지 내 컴퓨터에서 실행되는 게임을 살펴보자. 이러한 게임들을 대상으로 하는 게임 해킹 프로그램 유형은 다음과 같다.

- Trainer
- 범용 메모리 조작 프로그램

과거 패키지 게임의 해킹 프로그램이나 방법은 단지 게임의 재미를 위해서 사용되는 수준이었다. 그러나 일부 유저들의 온라인 게임들의 승률 포인트와 아이템을 이제 더 이상 게임의 재미를 위해서 갖는다기 보다는 '돈' 으로 거래하기 위해서 갖기 때문에 문제가 된다.

한편으로 패키지 게임들도 멀티 플레이를 위해서 게임서버를 두고 있다. 국외 일부 게임개발사들은 자사의 게임서버에 'Anti-Cheater' 서비스를 하여 멀티 플레이 중 매너가 없거나 불법 프로그램을 사용하는 유저들은 'Cheater'로 간주하고 접속을 끊는 등 일정한 룰을 가지고 있다. 이는 온라인 게임사도 마찬가지이다. 비정상적인 플레이를 하는 유저들의 아이디를 운영방침에 따라 관리하기도 한다.

패키지 게임에서의 멀티 플레이 중 발생할 수 있는 게임 해킹 프로그램들을 주로 'BOT'이라고 표현한다. 이러한 게임 해킹 프로그램의 사용은 게임의 유형마다 조금씩 다를 수 있겠지만 다른 유저와의 경쟁에서 자신을 유리하도록 도와주며 이를 통해 포인트 및 레벨-업 또는 소위 명예의 전당에 이름을 올리는 것이다. 단지 컴퓨터를 상대로 게임을 한다면 'Cheat Code'를 사용하여 플레이 할 수도 있을 것이다. 하지만 대부분의 게임들은 "Cheat Code"를 사용하면 게임 내 포인트 또는 레벨-업에 제한을 둔다. 그렇기 때문에 Trainer 또는 메모리 조작 프로그램 (또는 그 데이터)을 이용한다. 여기서부터 게임의 해킹 프로그램은 시작 되었다고 해도 과언은 아니다.

이러한 Trainer (또는 BOT) 와 메모리 조작 프로그램은 도스시절부터 존재해왔으며 지금 온라인 게임 해킹에도 그대로 계승되고 있다. 한가지 현재 온라인 게임 해킹 프로그램에서 안되는 형태가 있다면 세이브 파일이 로컬이 아닌 서버에 저장되므로 세이브 파일을 조작하는 형태는 현재 온라인 게임에서는 볼 수가 없다. 반대로 과거 게임 해킹 프로그램에서 볼 수 없었던 것은 패킷 스니핑을 통한 패킷 조작이다. 그렇다면 이러한 Trainer (또는 BOT) 나 메모리, 패킷 조작 프로그램들 과연 불법은 아닌가 하는 것이 관건이 된다.

4. 게임 해킹 프로그램 단지 재미만을 위한 필요악인가?

단지 자신의 시스템에서만 컴퓨터를 상대로 즐기는 게임의 해킹 프로그램은 Trainer 라는 단어의 정의대로 게임을 쉽고 재미있게 진행하도록 도와준다. 그리고 일부 메모리, 패킷 조작 프로그램들은 여러 가지 목적으로 사용될 수 있지만 이는 사용자의 마음먹기에 따라 다르다. 온라인 게임에서 이러한 프로그램들은 모두 게임 해킹에 특화되어 제작된 형태가 대부분이다. 이러한 프로그램들도 단지 자신의 시스템에서 컴퓨터를 상대로 게임을 플레이하는 것이라면 문제가 되지는 않을 것이다.

위에서도 언급한 것처럼 온라인 게임들은 다른 유저와 승률을 가지고 게임을 하는 것이다. 그러므로 비정상적인 방법이나 프로그램을 이용하여 승률을 조작하는 행위는 불법으로 간주될 수 밖에 없을 것이다. 필자는 온라인 게임 업체의 이러한 약관을 자세히 확인해보지는 않았으나 일반적인 상식 수준에서도 이와 같은 행위나 프로그램은 부당행위라고 얘기할 수 있지 않을까 한다. 이를 불법 (또는 불법 프로그램) 이라고도 표현 할 수 있겠지만 불법이라는 단어 자체가 왠지 법적인 구속력을 갖는 것처럼 들릴 수 있기도 하여 어려운 의미는

여기서는 논의하지 않기로 하겠다.

일반적으로 게임을 하다가 막히면 공략 집이나 'Cheat Code'를 사용하여 플레이 할 수 있다. 공략 집이나 Cheat Code는 불법이 아니지만 온라인 게임에서의 부정한 행위나 프로그램으로 자신의 승률을 올리는 것은 부당행위라 할 수 있겠다. 위에서도 언급한 것을 정리해보면 멀티 또는 온라인 게임 조작을 위해서 만들어진 Trainer, BOT, Hack 그리고 유저가 승률을 조작할 목적으로 사용하는 프로그램들도 게임사에서 보면 반드시 제지해야 할 프로그램일 것이다.

5. 게임 해킹 프로그램에 대한 대책

게임 해킹 프로그램에 대한 솔루션은 오래 전부터 출시되어 왔다. 이 솔루션들은 게임을 이용하는 일반 유저들을 위한 것이 아닌 게임개발사를 위한 솔루션이다. 일반적으로 유저들은 게임 해킹 프로그램과 이를 방어하는 솔루션 설치여부에 대하여 걱정할 필요가 없다. 일반 유저들이라면 게임 내에 이러한 솔루션이 있는지 인지하지 못한 경우가 대부분 일 것이다. 일반적으로 게임과 연동되어 동작되는 이 솔루션들은 게임시작 전에 부당행위를 위하여 사용되는 프로그램이나 Trainer, BOT, Hack 등을 감지하여 실행을 차단하고 이후에도 지속적으로 감시활동을 한다. 나아가서는 원천적으로 이러한 행위나 프로그램들로부터 게임을 지켜내기 위한 보호 방법을 사용하기도 한다.

그러나 일부 온라인 게임들이 해당 솔루션을 사용한 후부터 계속적인 도전을 받아온 건 공공연한 사실이다. 창과 방패의 싸움이라 할 수 있을 정도 이것은 컴퓨터 보안에서 거의 매번 나오는 이야기이니 게임의 보안도 예외일 수는 없다.

앞으로의 동향을 예상해보면, 게임 해킹 프로그램이나 이를 제작하는 방법 또는 메모리 또는 패킷 조작 프로그램을 사용하는 방법은 지금도 인터넷에 떠돌고 있으며, 앞으로 이러한 내용을 토대로 더 쉽게 프로그램 제작이나 부당행위 방법이 공개 될지도 모른다. 또한 악성코드와 유사한 방식으로 동작하여 솔루션들이 이를 대응하는데 지연시간을 발생하게 할 수 있을지도 모른다. 하지만 미래가 그리 어둡지만은 않다. 솔루션들도 이러한 동향을 충분히 인지하고 있을 것이며 악성코드 대응력으로 쌓았던 기술력을 바탕으로 어떠한 문제점도 충분히 해결할 수 있을 것이라고 생각된다.

게임 해킹 프로그램은 악성코드나 스파이웨어처럼 불특정 다수를 노리는 프로그램은 아니다. 그래서 어쩌면 컴퓨터 보안에 있어서 다소 소외되는 경향도 있고 많은 사람들이 모르는 경우도 아직 많다. 게임은 이제 더 이상 어린이들이나 하는 것이 아니라 것은 오래 전부터 인식 되었고 더 나아가 게임은 더 이상 '재미'로만 하는 것이 아닌 세상이 되어버렸다. 왠지 지나친 경쟁사회에 살고 있는 우리가 살아가면서 느끼는 시스템이 발전하고 세상이 변하

면서 겪는 현상이 아닌가 한다.