ASEC Report 5월

® ASEC Report

2005. 06

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

신종(변형) 트로이목마의 발견 및 피해 증가…

5월에는 4월에 비해 악성코드 피해신고 및 신종(변형) 악성코드의 발견이 증가하였다. 특히, 5월은 트로이목마, 드롭퍼의 발견과 피해가 급증하여, 1년 6개월만에 트로이목마 신종(변형) 발견건수가 웜의 신종(변형) 발견건수를 앞지르는 현상까지 나타났다. 그 원인으로는 스파이웨어(애드웨어) 다운로더, 프록시 트로이목마, 온라인게임 관련 트로이목마 변형의 증가를 꼽을 수 있다. 그 중에서도 리니지 게임 관련 트로이목마인 리니지핵 트로이목마 변형이 여러 건 발견됨과 동시에 많은 피해를 입혀 5월 악성코드 피해 Top 10 중 2위를 차지하였으며, 변조된 일본 및 한국의 유명 사이트 접속 시 다운로드되는 사건까지 일으켰었다. 5월 악성코드 피해의 또 한가지 특징은 4월과 마찬가지로 여러 종류의 마이톱 웜 변형의 발견과 피해이다. 악성코드 Top 10 중 5개를 마이톱 웜 변형이 차지하였으며, 이 마이톱 웜 변형들은 모두 5월에 발견된 것이었다. 한국, 일본을 비롯한 유럽지역도 마이톱 웜 변형으로 인한 피해가 많았던 한달이었으며, 그동안 백쯔 웜이 강세를 보이던 중국에서도 마이톱 웜에 의한 피해가 점차 증가하는 양상을 보였다.

5월은 4월에 비해 주목할만한 취약점이나 보안적 이슈가 적었던 한달이었다. '공인인증서가 해킹에 취약하다'라는 소식이 언론을 통해 전해지면서 이에 대한 우려가 높았었으나, 이는 공인인증서를 관리하는 특정 프로그램에 취약점이 존재하여 이것을 이용한 악의적이 행동이 가능하였을 뿐 공인인증서 자체의 안정성과는 무관한 것으로 밝혀졌다.

그 밖에도 5월에는 동영상에 스크립트 명령을 이용하여 스파이웨어를 설치하는 기법이 발견되어 주목을 받았다.

이달의 ASEC 컬럼에서는 일본과 한국의 유명 사이트를 해킹하여 온라인 게임인 리니지나 미르의 전설2의 계정과 비밀번호를 훔치는 트로이목마가 다운로드되도록 했던 사건과 변화되는 홈페이지 변조의 목적에 대해서 살펴보았다.

I. 5월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자 : 차형진 연구원(sharkjin@ahnlab.com)

순위		바이러스명	건수	%
1	-	Win32/Netsky.worm.29568	332	16.1%
2	New	Win-Trojan/LineageHack.37888.C	96	4.6%
3	New	Win32/Mytob.worm.59006	87	4.2%
4	-	Win32/Maslan.C	61	3.0%
5	↑5	Win32/Mytob.worm.61440	53	2.6%
6	New	Win32/Mytob.worm.29550	49	2.4%
7	New	Win32/Netsky.worm.17920	46	2.2%
8	↓2	Win32/Netsky.worm.25352	45	2.2%
9	New	Win32/Mytob.worm.51791	39	1.9%
10	New	Win32/Mytob.worm.44544.B	38	1.8%
		기타	1,220	59.1%
합계			**2,066**	**100%**

[표1] 2005년 5월 악성코드 피해 Top 10

5월 악성코드 피해 동향

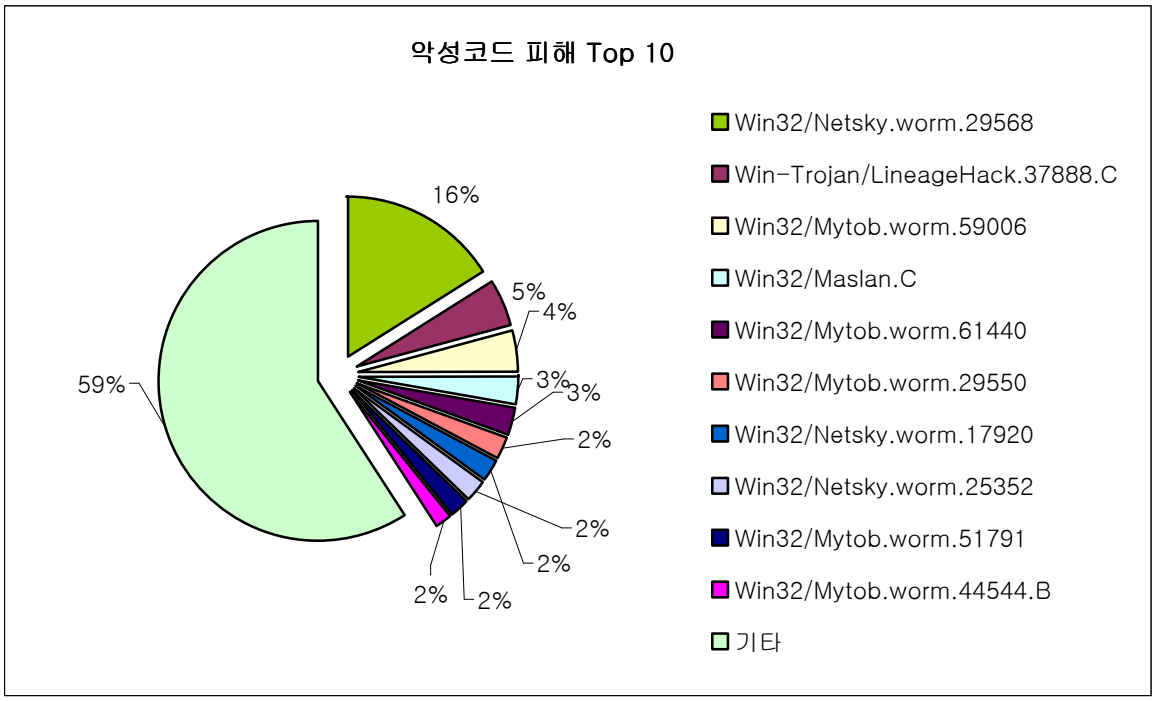
2005년 5월 악성코드 피해건수는 2005년 4월에 비해 대폭 늘어난 2,066건이다.
최근 감소 추세에 있다가 다소 증가한 이유로는 시스템 감염 후 메일을 통해 급속도로 전파되는 전통적인 대량 전송 메일 웜 유형의 증가, 사용자 정보를 빼내가는 트로이목마의 증가에 따른 것으로 보인다.

5월 악성코드 피해동향 중 주목할 만한 것은 리니지핵 트로이목마(Win-Trojan/LineageHack)의 변형인 리니지핵.37888.C 트로이목마(Win-Trojan/LineageHack.37888.C)가 5월에 발견됨과 동시에 피해순위 2위를 차지했다는 것이다. 이는 다양한 취약점을 이용하여 전파되며 감염속도도 매우 높기 때문이다. 이 트로이목마가 설치되면 특정 악성 프로그램이 실행되며, 실행된 특정 악성 프로그램은 또 다른 악성파일을 설치한다. 설치된 악성파일은 사용자가 입력하는 키보드 값을 가로채고, 이 정보를 하드 코딩 되어 있는 특정 메일 주소로 전송한다. 따라서, 개인정보 유출에 따른 피해의 심각성이 매우 높아, 앞으로 주의를 기울여 관찰할 필요가 있다.

5월 악성코드 피해동향 중 또 하나의 특징은 마이톱 웜(Win32/Mytob.worm) 변형에 대한

피해가 급증하여 Top 10 안에 무려 5개의 마이톱 웜 변형이 순위를 차지하고 있는 것이다. Top 10에 랭크된 5개의 마이톱 웜 변형은 모두 5월에 새로이 발견된 것으로, 이는 웜 변형에 대한 제작기간이 짧아졌으며, 확산도가 매우 높다는 것을 의미한다.

5월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.

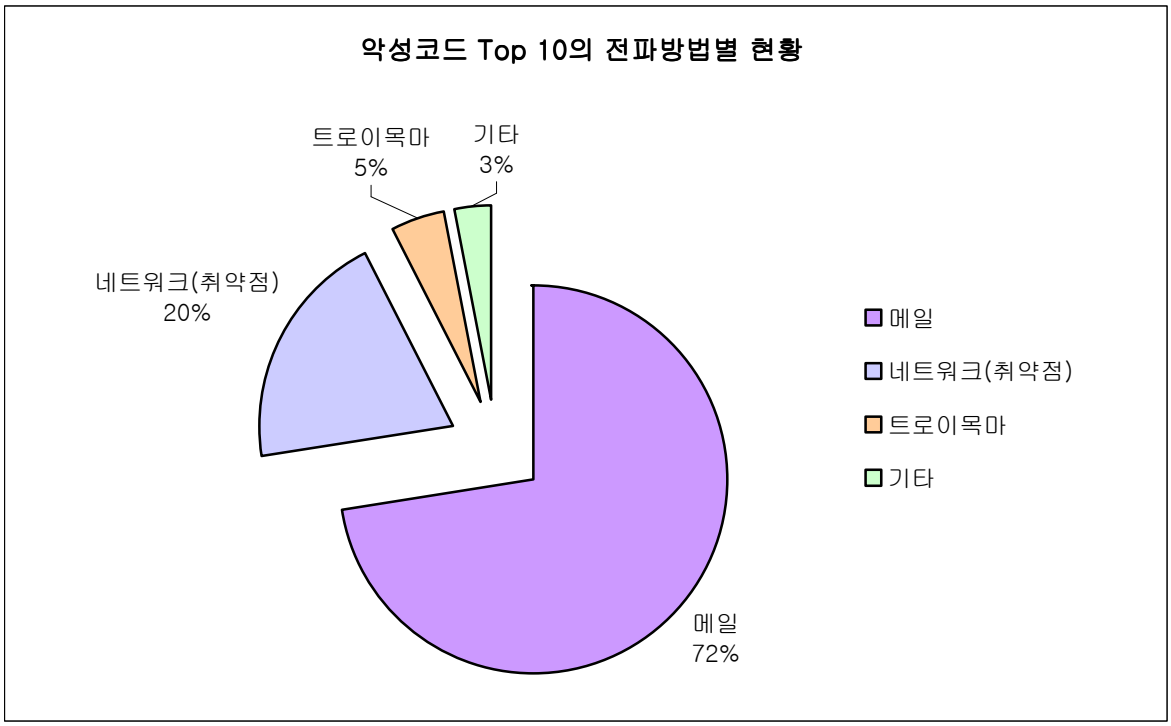


[그림1] 2005년 5월 악성코드 피해 Top 10

앞서 언급한 것과 같이 4월 중순부터 두각을 나타내기 시작한 마이톱 웜의 피해는 급격하게 증가하고 있으며, 새로운 변형이 발견되는 시기와 전파 속도 등 마이톱 웜의 라이프 사이클이 상당히 짧게 나타나고 있다. 이 웜은 현재 상당히 많은 시스템을 감염시켰으며 대량의 메일을 발송하여 전파하고 있어서, 당분간 Top 10 순위 권에 계속 머물 것으로 보인다.

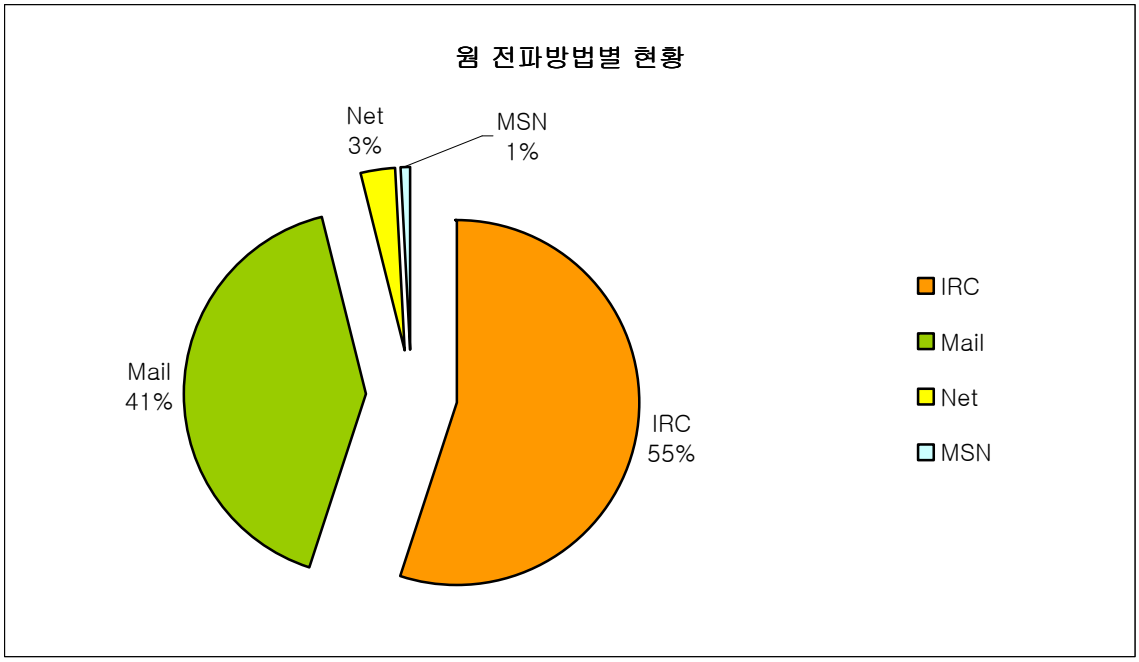
5월 악성코드 Top 10 전파방법별 현황

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



[그림2] 악성코드 Top 10의 전파방법별 현황

[그림2]에서 보여주는 것처럼 피해순위 Top 10에 랭크된 악성코드의 72%가 메일을 이용하여 전파되고 있다. 또한 네트워크(취약점)를 이용하여 전파되는 유형도 꾸준히 나타나고 있다. 특히 취약점을 이용하여 전파되는 트로이목마의 피해는 개인정보 유출과 직접적으로 연관되어 있기 때문에, 사용하고 있는 운영체제나 응용프로그램이 보유한 취약점에 대해 주기적으로 살피고 관련 취약점에 대해 보안 패치 적용 및 사용중인 백신을 최신엔진으로 업데이트하여 검사하는 습관을 가져야 할 것이다.

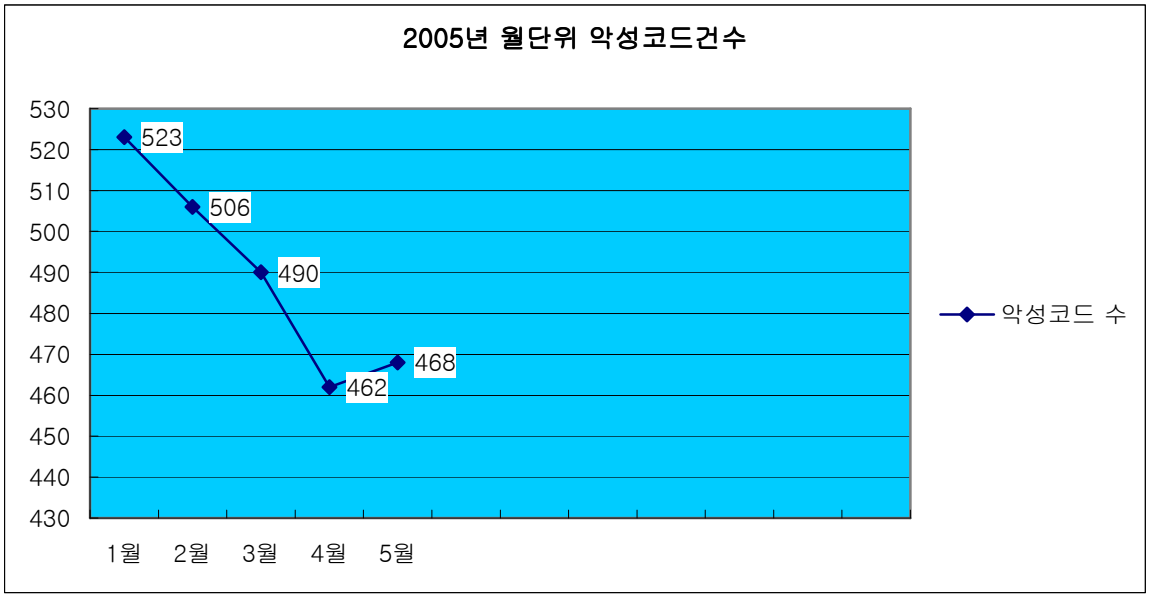


[그림3] 웜의 전파방법별 현황

[그림3]은 5월에 피해 신고된 웜의 전파방법에 대한 현황으로, 이메일(Mail)과 인터넷 채팅(IRC)이 96% 차지하는 것으로 집계되었다. 이는 이메일 사용 뿐 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

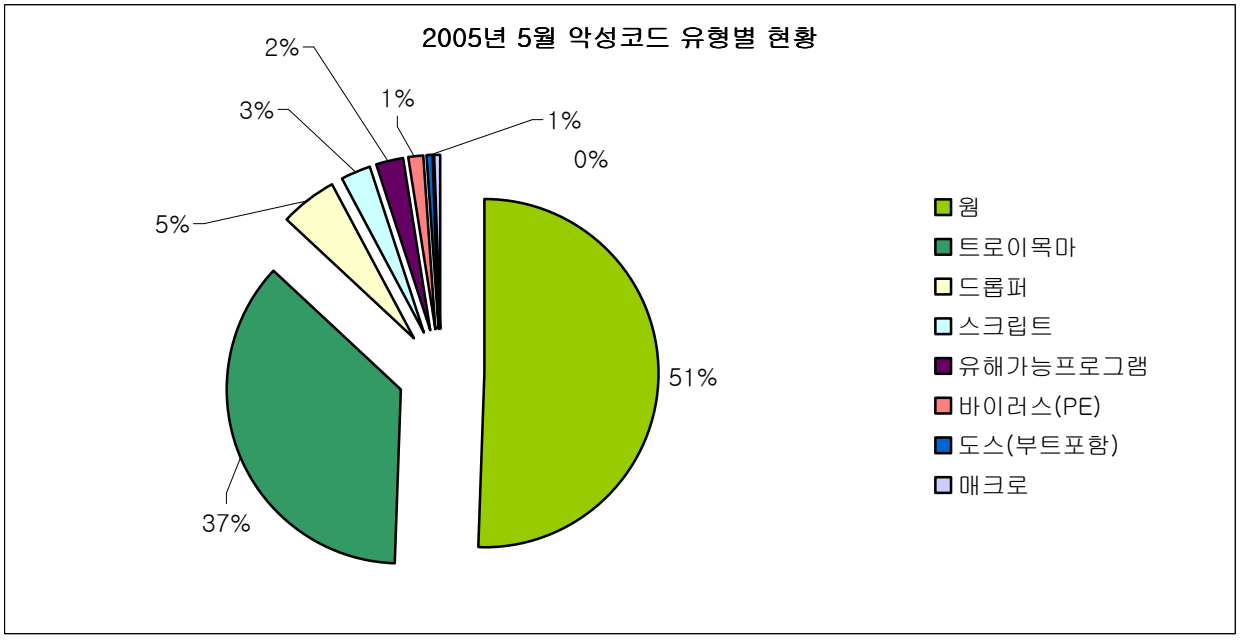
5월에 피해 신고된 악성코드는 468개이다. 지난 4월에 비해 다시 증가하였으며, 이는 마이톱 변형과 트로이목마의 피해로 인해 소폭 증가한 것으로 보인다.



[그림4] 2005년 월별 피해신고 악성코드 수

주요 악성코드 현황

악성코드 유형별 현황은 [그림5]와 같다.



[그림5] 악성코드 유형별 현황

5월에는 4월에 비해 웜이 6% 가량 감소한 반면, 트로이목마는 7% 가량 증가하였다. 이것은 리니지핵(LineageHack), 드롭퍼(Dropper), 로우존스(Lowzones), 다운로더(Donwloader)와 같은 일부 트로이목마의 증가가 주요원인으로 보인다. 또한 트로이목마를 설치하는 증상을

가진 웜이나 스파이웨어도 증가하고 있기 때문으로 보인다. 최근에는 고의적으로 트로이목마를 사용자 시스템에 설치하여 개인정보를 빼낸 뒤 금융적인 피해를 입히는 경우도 발생하고 있다. 이처럼 종합적, 지능적인 기능으로 사용자에게 피해를 입히는 트로이목마는 점차 증가할 것으로 보인다.

날로 심각해져 가는 개인정보 유출 위협으로부터 지켜나가기 위해서는 사용하고 있는 운영체제와 응용프로그램의 보안 패치 적용을 항상 최신으로 유지해야 한다. 또한 최신엔진으로 업데이트한 백신으로 주기적인 시스템 검사를 하는 습관을 가져야 하겠다.

(2) 신종(변형) 악성코드 발견 동향

작성자 : 정진성 주임연구원 (jsjung@ahnlab.com)

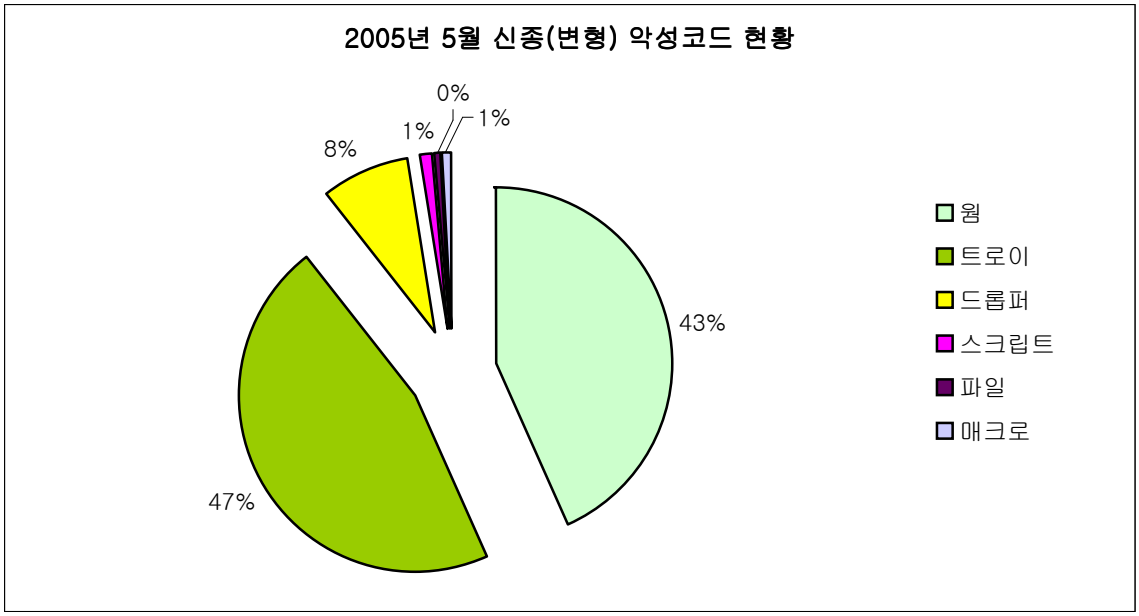
5월 한달 동안 접수된 신종(변형) 악성코드의 건수는 [표1], [그림1]과 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	非윈도우	합계
103	109	19	3	1	2	0	0	8	0	245

[표1] 2005년 5월 유형별 신종(변형) 악성코드 발견현황

신종 및 변형의 트로이목마 발견 건수가 지속적으로 증가하고 있다. 특히 이번 달은 트로이목마를 설치하는 드롭퍼의 증가도 눈여겨볼 만 하다. 특히 1년 6개월만에 신종 및 변형의 트로이목마 건수가 웜의 발견 건수를 앞지르는 현상을 보였는데, 이는 악성 아이알씨봇(IRCBot)이 취약점 등을 이용하여 자체 전파기능을 가지기 시작한 이후 처음이다.

[그림1]은 5월 신종(변형)악성코드의 비율을 나타낸 것이다. 역시 트로이목마 비율이 전체의 47%를 차지하고 있다.



[그림1] 2005년 5월 신종(변형) 악성코드 비율

이번 달 신종(변형) 악성코드 발견건수의 증가 원인이었던 트로이목마와 드롭퍼를 살펴보면 다음과 같다.

1) 트로이목마

- 에이전트 트로이목마(Win-Trojan/Agent)

- 다운로더 트로이목마(Win-Trojan/Downloader)
- 리니지핵 트로이목마(Win-Trojan/LineageHack)
- 페레 트로이목마(Win-Trojan/Pere)
- 피피도르 트로이목마(Win-Trojan/PPdoor)
- 랭키 트로이목마(Win-Trojan/Ranky)
- 스몰 트로이목마(Win-Trojan/Small)

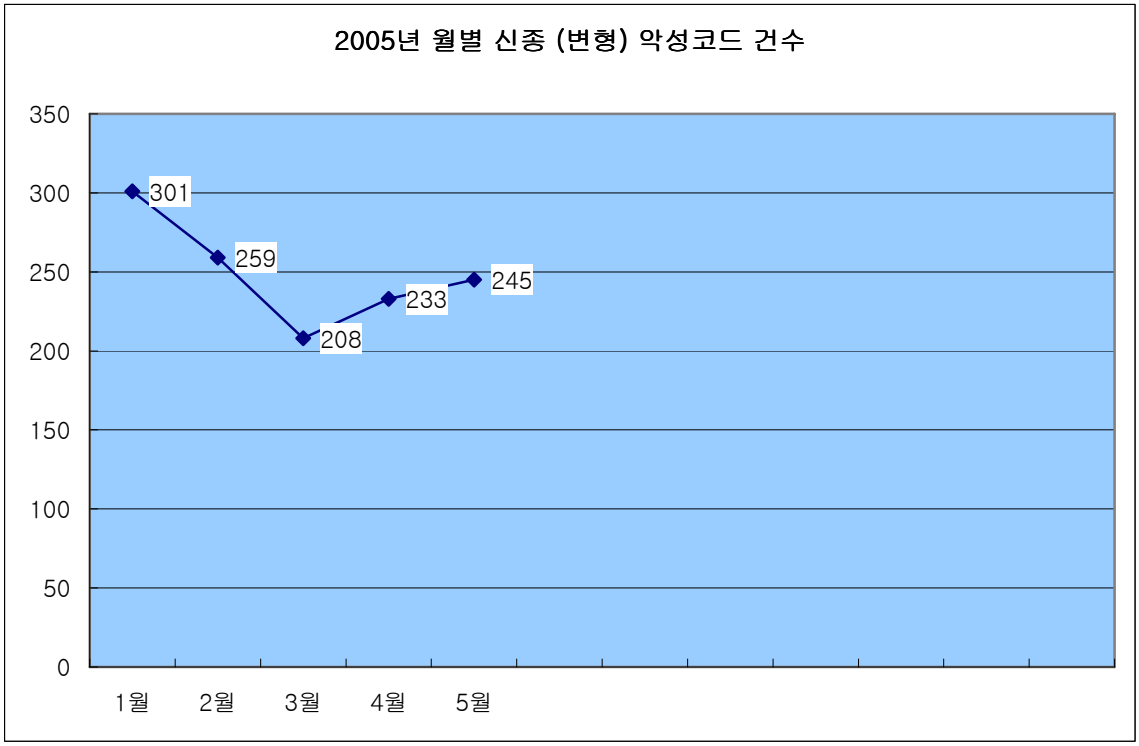
일반적으로 다운로더 트로이목마와 랭키 트로이목마, 스몰 트로이목마 등은 단독으로 실행되기 보다는 다른 악성코드 또는 스파이웨어와 함께 발견되었다. 또한 변형이 부쩍 증가한 트로이목마로는 리니지핵 트로이목마, 페레 트로이목마가 있다. 특히 이 트로이목마 중 페레 트로이목마 는 안티 바이러스 설치를 방해하거나 설치된 안티 바이러스 제품을 강제로 종료하는 증상을 가지고 있어서 국내에서 많은 피해 보고가 있었다.

2) 드롭퍼 (Dropper)

- 애드롭퍼 드롭퍼(Dropper/Adropper)
- 에이전트 드롭퍼(Dropper/Agent)
- 리니지핵 드롭퍼(Dropper/LineageHack)
- 멀티드롭퍼 드롭퍼(Dropper/MultiDropper)
- 인윈 드롭퍼(Dropper/Yinwin)

이번 달에는 악성코드를 임의의 폴더에 생성(Drop) 하는 드롭퍼의 종류가 다양해졌다. 특히 애드롭퍼 드롭퍼처럼 스파이웨어(애드웨어)를 생성하는 드롭퍼 변형의 수가 증가하였다. 또한 리니지핵 트로이목마를 생성하는 리니지핵 드롭퍼도 그 수가 증가하였다. 이 드롭퍼와 트로이목마에 대한 자세한 내용은 이번 달 주요 악성코드 정리 부분에서 살펴보도록 하겠다.

다음은 월별 신종(변형) 악성코드 건수를 나타내고 있다. 위에서 언급한 것처럼 최근 들어 트로이목마의 증가로 4월부터 발견된 신종 및 변형의 악성코드 건수가 증가하는 걸 알 수 있다.



[그림2] 2005년 월별 신종(변형) 악성코드 발견 현황

신종(변형) 트로이목마 증가의 원인으로는 스파이웨어(애드웨어)의 다운로더 및 프록시 트로이목마의 증가, 온라인 게임 관련 트로이목마 변형 증가를 들 수 있다. 이 두가지 유형의 악성코드를 통해 악성코드와 스파이웨어(애드웨어)의 유착관계를 어느 정도 유추해 볼 수 있다. 또한 온라인 게임의 사용자 계정을 탈취하는 트로이목마들도 결국은 탈취한 사용자 계정을 통해 금전적인 이득을 취할 수 있다는 것은 자명한 사실이고, 이를 통해 악성코드와 스파이웨어(애드웨어) 제작자들이 앞으로도 금전적인 이득을 취할 수 있는 악성코드 제작에 열을 올릴 것이라는 것을 미리 예상해 볼 수 있다.

5월 주요 신종(변형) 악성코드 정리

이번 달에 이슈가 되었던 주요 악성코드로는 지속적으로 변형이 보고된 마이톱 웜(Win32/Mytob.worm)과 특정 온라인 게임의 사용자 계정을 탈취하는 증상을 가진 리니지핵 트로이목마(Win-Trojan/LineageHack), 그리고 안티 바이러스 제품 등의 설치와 실행을 방해하는 증상을 가진 트로이목마가 있었다. 또한 중국에서 제작되어진 것으로 추정되는 CIH 바이러스와 유사한 파괴증상을 가진 야미(Win32/Yami.3027) 바이러스가 매스컴을 통해 보도 되었다. 그러나 이 바이러스는 실제로 일반 사용자들로부터는 보고 되지 않았다.

이슈가 되었던 악성코드는 다음과 같다.

► **리니지핵 드롭퍼(Dropper/LineageHack), 리니지핵 트로이목마(Win-Trojan/LineageHack)**

이 악성코드는 특정 온라인 게임의 사용자 계정을 탈취하는 증상을 가지고 있다. 해당 악성코드들은 이미 오래전부터 알려진 형태였다. 그러나 최근 들어 변형들의 발견 건수가 증가하고 있는데, 원인을 확인해 본 결과 유명 웹 사이트를 해킹한 후 해당 드롭퍼와 트로이목마를 다운로드 받도록 해두었기 때문이다. 해킹을 당한 사이트는 한국뿐만 아니라 일본에서도 확인되었다. 다음과 같은 동작원리를 가지고 있다.

1) 악성코드 제작자는 웹 사이트를 해킹하여 메인 페이지 내 특정 URL을 삽입해 둔다. 이 URL은 iframe 태그를 이용하고 그 크기를 0으로 하여, 사용자에게 보여지지 않게 해두었다.
2) 특정 URL로 지정된 호스트도 해킹된 것으로 추정하고 있으며 URL이 가리키는 경로에는 스크립트 파일이 올려져 있다. 이 스크립트는 인터넷 익스플로러 취약점(MS04-013)을 가지고 있어 패치가 안된 시스템이라면 해당 스크립트 명령이 자동으로 실행되도록 되어 있다.
3) 스크립트의 내용은 동일한 호스트에 올려진 chm 형식의 파일을 다운로드하여 실행하도록 되어 있다. chm 파일은 컴파일된 HTML 파일이며 내부에는 이미지와 같은 바이너리 파일뿐만 아니라 실행파일을 포함시킬 수도 있다. 그래서 이 파일내부에 리니지핵 트로이목마를 숨겨둘 수 있었다.
4) 실행된 트로이목마는 윈도우 타이틀 및 클래스명을 모니터링하여, 특정 게임이 실행되었다면 키로거 기능을 동작하여 온라인 게임의 사용자 계정을 로그 파일로 저장한 후 특정 메일주소로 발송하도록 한다.

이 악성코드들은 자체 확산력은 없지만, 웹사이트를 해킹한 후 드롭퍼를 유포하고 있기 때문에 5월에 피해문의가 증가하였다. 이는 드롭퍼와 트로이목마가 설치된 시스템들도 문제가 되지만 확산을 담당하는 취약한 시스템들도 문제가 되므로 감염된 악성코드의 치료도 중요하지만 취약한 시스템을 보안패치하고 관리하는 것이 중요하다.

► **페레 트로이목마(Win-Trojan/Pere)**

안티 바이러스 제품 및 모니터링 관련 프로그램의 실행을 방해하는 페레 트로이목마는 4월에 발견되었지만 그 변형이 5월에도 끊임없이 보고되었다. 이 트로이목마는 안티 바이러스 제품의 설치 및 실행을 방해하는 증상을 가지고 있으며, 트로이목마 자체는 목적이 불분명한 P2P 서버 역할을 하는 증상도 가지고 있다. 특히 트로이목마는 자신을 보호하려는 목적으로 프로세스에서 자신을 종료하면 이를 트로이목마가 사용하는 특정 DLL이 감시하여 해당 프로세스를 재실행한다. 또한 이 DLL은 정상 프로세스들에 삽입(Injection)되어 실행중인 상태에서는 종료하기 어렵다. 또한 트로이목마는 다형성 크립터(Crypter)를 사용하여 코드가 일정하지 않고 매번 다르다. 따라서 일반적인 진단방법으로는 진단이 안되며 다형성 코드를 풀

어내야만 변형들을 모두 진단해 낼 수 있다.

► 지피코드 트로이목마(Win-Trojan/Gpcode)

이 트로이목마는 러시아에서 제작된 것으로 추정하고 있다. 이 역시 변형으로 원형은 작년 12월쯤 보고되었다. 트로이목마는 다음과 같은 데이터를 PGP 방식으로 암호화 해둔다.

- asc, db, db1, db2, dbf
- doc, htm, html, jpg, pgp
- rar, rtf, txt, xls, zip

그리고 암호화된 데이터의 키를 사라는 내용이 담긴 텍스트 파일을 생성한다.

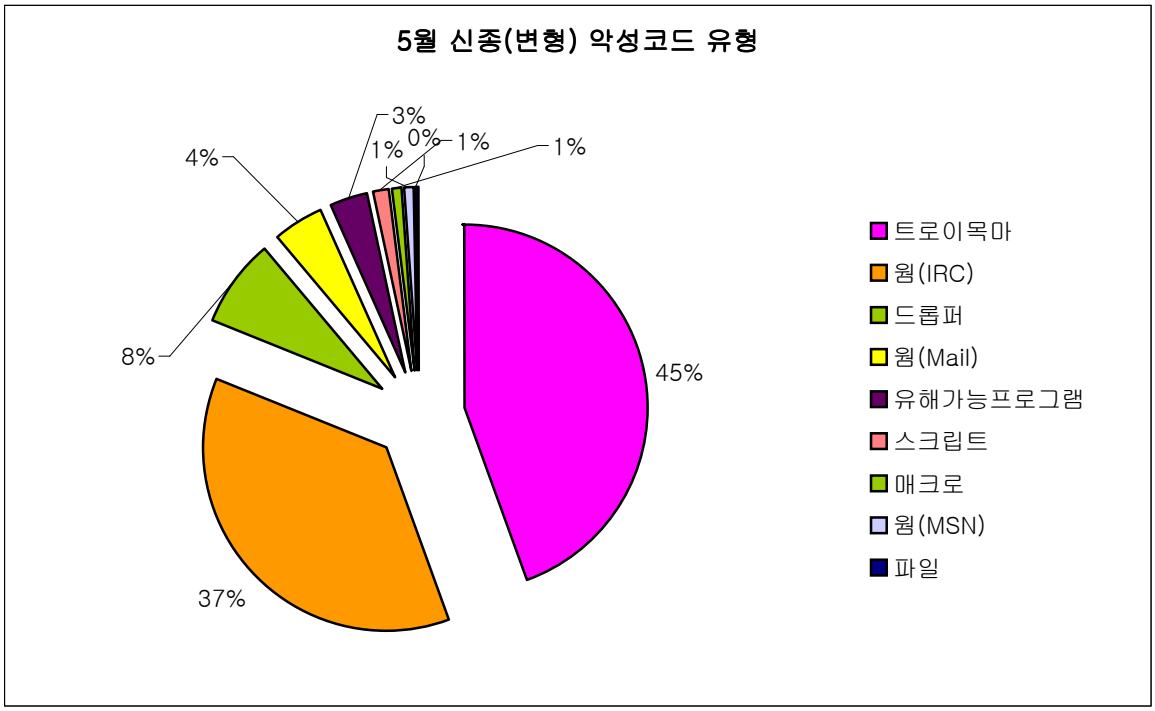
일부 매스컴에서는 이 트로이목마를 '랜섬웨어(RANSOM-WARE)'라고 보도되기도 하였다. 지금까지 악성코드는 사용자의 데이트를 삭제하는 등의 손상을 입혀왔다. 하지만 이 트로이목마는 지금까지와는 다른 방식으로 사용자에게 피해를 입히고 있는 것이다. 아직 이 트로이목마가 널리 확산되었다는 보고는 없다. 과거에도 일부 매크로 바이러스의 경우 감염된 문서에 암호를 설정하여 문서를 못쓰게 하는 경우가 있었으나, 지피코드 트로이목마와 같이 금전을 요구하지는 않았다. 향후 악성코드 피해 유형 중 이러한 악성코드에 의해서 발생하는 새로운 피해 항목이 만들어지지 않을까 예상해본다.

► 야미 바이러스(Win32/Yami.3027)

중국에서 제작된 것으로 추정되는 야미 바이러스는 매스컴을 통해 보도되기도 하였다. 다른 실행파일에 자신을 감염시키는 증상을 가진 야미는 오직 윈도우 XP에서만 정상적인 감염활동을 한다. 파일의 감염방식은 파일 내 빈 공간에 자신의 코드를 삽입하는 형식이다.

증상으로는 어떤 조건이 되면 롬 바이오스와 하드 디스크 특정 섹터를 바이러스 자신이 가지고 있는 특정한 문자열로 겹쳐쓰기하여 손상을 일으킨다. 이렇게 되면 해당 시스템은 부팅이 불가능하고 하드 디스크도 논리적인 손상을 입는다. 이 바이러스의 감염기법과 증상이 CIH 바이러스와 유사하다 하여 신 CIH 바이러스라고 매스컴을 통해서 처음 보고 되었으나 일반 사용자로부터 직접적인 감염보고는 없었다.

다음은 5월에 발견된 악성코드들을 유형별로 분류한 것이다.



[그림3] 5월 신종 (변형) 악성코드 유형별 현황

MSN 웜 변형이 꾸준히 보고 되고 있는데 이는 켈비르 웜(Win32/Kelvir.worm) 변형 때문이다. 유해 가능 프로그램들도 조금 증가했는데 이번 달 경우 취약점을 검사해 주는 툴들이 다수 포함 되었다. 이러한 취약점 검사도구는 해커들에게 남용되는 문제가 종종 발생하곤 한다. 유해가능 프로그램으로 분류된 프로그램들이 그렇듯 잘 쓰면 약이 되지만 악용되면 오히려 피해를 유발하는 문제를 일으킨다. 악성코드로부터의 예방도 중요하지만 유해 가능한 프로그램의 악용으로 다른 시스템이나 네트워크에 불법적인 검색을 통해서 피해를 입혀서는 안 되는 것도 중요한 일임이 틀림없다.

II. 5월 AhnLab 스파이웨어 동향

작성자 : 장혜윤 연구원(planet@ahnlab.com)

최근 국내에서 애드웨어 제작사를 단속하고 있어, 배포되는 국내 애드웨어 수가 줄어들고 있기는 하지만 아직까지 사용자를 교묘하게 속여 배포되는 경우가 발견되고 있다.

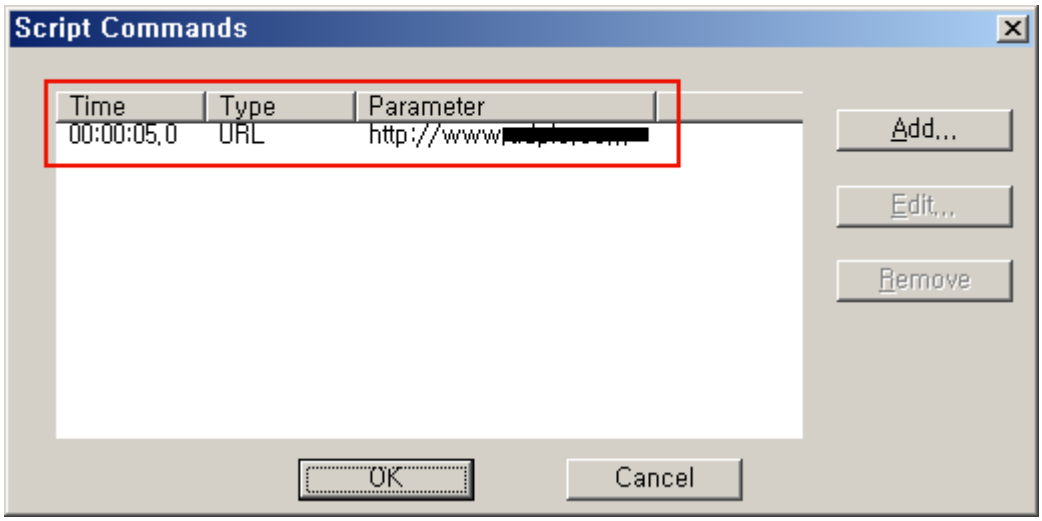
2월에 플래쉬 파일(*.swf)을 이용하여 배포하는 기법을 소개한 이후, 최근 이와 비슷하게 동영상에 스크립트 명령(Script Commands)을 이용하여 스파이웨어를 설치하는 기법이 발견되었다. 이 기법은 일반 사용자들도 쉽게 구현할 수 있을 뿐만 아니라, 사용자들에게 쉽게 배포할 수 있는 잇점을 가지고 있다. 또한 기본적으로 .WMV 파일을 재생하기 위해서는 'WMV-9 코덱'이 필요하며, 코덱이 설치되어 있을 경우 미디어플레이어(Media Player) 뿐만 아니라 다른 동영상 프로그램에서도 스크립트 명령(Script Commands)이 실행된다.

국내 모 업체에서 이 기법을 이용해서 여러 종류의 홍보용 동영상을 제작하여, 특정 웹 페이지에 Html 태그(<embed>[1], <iframe>[2])를 이용해서 ActiveX를 설치하는 사례가 확인되었다. 단순히 Html 태그를 이용해서 웹 페이지 접속 시 동영상 재생과 동시에 ActiveX를 설치하는 방법으로 배포 될 수도 있지만, 동영상 파일로 제작되었다는 점으로 미루어 볼 때 성인 동영상, 영화파일 등에 ActiveX 설치 URL을 삽입한 후 P2P(파일 공유 프로그램)를 이용해 배포될 수도 있다. 이럴 경우, 단시간에 여러 종류의 스파이웨어를 설치하는 동영상 파일이 수 많은 사용자들에게 배포될 수 있으며, 제작된 동영상은 [그림1]과 같이 윈도우 미디어 파일 편집기(Windows Media File Editor)로 확인할 수 있다.

[1] <embed>태그는 플래시나 동영상과 같은 멀티미디어 파일을 삽입하게 되면 동영상인 경우 윈도우 미디어플레이어, 플래시인 경우 쇽웨이브(Shockwave)라는 플러그인 프로그램들이 해당파일을 실행시켜 주는 것이다.
[2] <iframe>태그는 외부에 있는 문서나 페이지를 현재 있는 위치의 일부분에 삽입하는 것으로 문서내의 프레임이라 할 수 있다

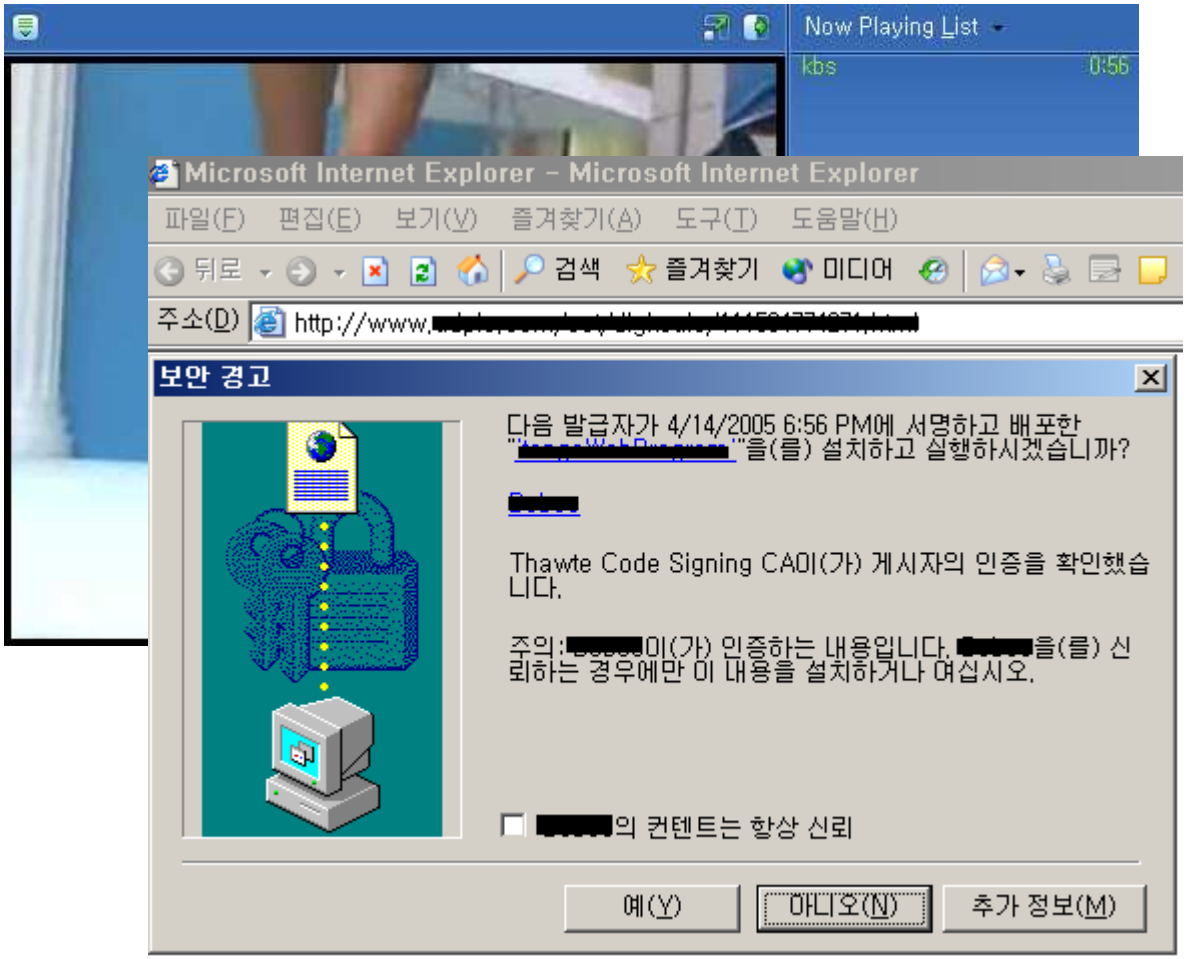
[그림1 윈도우 미디어 파일 편집기로 동영상 열기

동영상에서 사용하고 있는 스크립트 명령을 확인하기 위해서는 [그림1]에서 'Script Commands'를 클릭하여 [그림2]와 같이 스크립트 정보(Time, Type, Parameter)를 확인할 수 있다.



[그림2] 동영상 스크립트 명령 정보

[그림2]의 스크립트 명령 정보를 보면 5초에 [그림3]과 같이 URL 타입으로 되어 있는 인터넷 바로가기를 열게 된다.



[그림3] 동영상 재생 시 ActiveX 설치

대부분의 사용자들은 단순히 동영상을 재생한다고 생각하지만, 재생과 동시에 스크립트 명령에 입력되어 있는 정보에 따라 스파이웨어를 설치하기 때문에 관심을 갖지 않으면 설치과정을 눈으로 확인하기 힘들다. 또한 [그림3]처럼 단순 광고목적으로 ActiveX를 설치하는 경우도 있지만, 취약점을 이용한 URL이 링크되어 있으면 사용자에게 확인되지 않으면서 쉽게 개인정보를 유출하는 스파이웨어 및 바이러스 등을 설치할 수 있는 큰 문제점이 있다.

외국에서도 이와 비슷한 윈도우 미디어 플레이어(Windows Medie Player)의 디지털 저작권 보호 기능(DRM)[1]을 이용해서 사용자들에게 스파이웨어를 설치한 사례가 있다. 정상적인 인터넷에서 DRM 파일을 받게 되면 라이센스키도 함께 저장이 된다. 하지만 사용자를 속이기 위해서 P2P(eMule, KaZaA) 네트워크에 공유되어 있는 미디어 파일을 다운받아 실행할 때

[1] DRM(Digital Rights Management), 디지털 저작권 관리를 의미한다. 콘텐츠 제공자의 권리와 이익을 완전하게 보호하며 불법복제를 막고 사용료 부과와 결제대행 등 콘텐츠의 생성에서 유통, 관리까지를 일괄적으로 지원하는 기술이다.

특정 웹 페이지에서 라이센스 키를 받는 것처럼 사용자들을 유도해서 스파이웨어를 설치한다.

III. 5월 시큐리티 동향

작성자 : 정관진 주임연구원(intexp@ahnlab.com)

시간이 멈추지 않고 계속 흐르듯이 사이버 공간에서의 흐름도 끊임없이 변화하며 움직이고 있다. 새로운 소프트웨어, 새로운 취약점, 새로운 공격코드 등 새로운 것들은 계속 쏟아져 나오고 있는데, 이번 달의 시큐리티 주요 동향은 무엇인지 살펴보도록 한다.

5월에 발표된 보안 취약점 동향

5월에는 큰 보안 사건사고가 보고되지 않았으며, 매달 마이크로소프트사에서 발표하는 보안 패치도 4월의 것과 비교하면 큰 차이를 가지고 있다. 4월에는 긴급에 해당하는 것이 5개, 중요한 것이 3개였던 것에 비해 5월은 중요 등급에 해당하는 패치 하나만 발표되어, 2005년 5월은 주목할 만한 취약점이나 보안적 이슈가 적은 달로 평가할 수 있겠다.

이 중에서도 몇 가지를 짚어 보면 오픈소스 프로젝트 중 하나인 모질라의 파이어폭스(Firefox)와 관련하여 다수의 많은 공격코드가 공개되었고 TCP 스택과 4월에 보고된 MS의 취약점 공격코드가 공개되었다.

위험 등급	취약점	공격코드 유/무
HIGH	오픈소스 브라우저 FireFox 의 공격코드 다수 공개	유
MID	Microsoft Windows Explorer Remote Script Injection (MS05-024)	무
MID	Windows Message Queuing Service Overflow (MS05-017)	유
HIGH	Microsoft Windows COM Structured Storage Local Exploit (MS05-012)	유
MID	여러 Vendor 의 TCP Timestamp 취약점	유

[표1] 5월의 주요 취약점 현황[1]

5월 시큐리티 주요 이슈

오픈소스 브라우저의 사용증가에 따라 앞으로 가져올 위협을 전망해 보고 최근의 공인인증서 해킹 사건과 정부의 IT839 정책에 따라 준비되고 있는 IPv6의 위협에 대해서도 알아보자.

[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

► 오픈소스 브라우저의 취약점 증가

오늘날 가장 많이 사용되고 있는 브라우저는 단연 마이크로소프트사의 인터넷 익스플로러(Internet Explorer, 이하 IE)를 꼽을 수 있다. 브라우저의 시장 점유율을 조사하고 있는 Janco Associates Inc.에 따르면 2005년 4월 IE는 83.7%의 시장 점유율을 보이고 있다. 전 세계적으로 특정 브라우저의 시장 점유율이 80% 이상 차지하고 있다는 것은 엄청난 수치임에는 틀림없다. 하지만, 이에 대한 시장 판도도 곧 바뀌리라 예상된다. 바로 오픈소스 브라우저중의 하나인 파이어폭스(Firefox)의 점유율이 조금씩 증가되고 있고 현재 10%에 이르고 있기 때문이다. 이 조사기관은 다음 분기에는 25%까지 도달할 것으로 예측하고 있어 향후 브라우저 시장에 큰 영향을 줄 것으로 보인다. 브라우저의 시장점유율을 중요하게 여기는 이유는 시장점유율이 많다는 것은 사용자가 그만큼 많다는 것을 의미하며, 많은 사용자가 사용하는 브라우저의 취약점 발견은 그만큼 악성코드 제작자들이나 해커에게 매우 좋은 타겟이 되기 때문이다. 만약, IE에서 보안취약점이 발견되었다면 이는 상대적으로 시장 점유율이 낮은 파이어폭스에서 발견된 보안취약점 보다 미치는 영향이 상당히 클 것임은 자명한 일이다. 보안권고문을 발표하는 Secunia 사에 의하면 파이어폭스 1.1 의 권고문은 전체 18개로 평균 중간 정도의 위험등급을 가지고 있다. 이에 반해 IE 6.x는 81개의 권고문이 발표되었고 위험등급은 높은 등급에 해당된다. 파이어폭스가 18개중 5개가 패치되지 않았고 IE는 81개중 20개가 아직 패치되지 않았다. 물론, 권고문의 발표 개수와 평가방식 그리고 각 브라우저의 발표된 기간 등을 고려하면 어느 것이 더 보안적으로 안전하느냐 하는 것을 판단하기에는 올바른 척도가 되지 못한다. 하지만 이제 파이어폭스의 증가된 시장점유율을 보면 파이어폭스 또한 취약점 보고가 점점 증가되리라 예측되며 IE 뿐만 아니라 오픈소스 브라우저에 대해서도 보안적인 관심을 기울일 필요성이 높아지고 있다.

► TCP(Transmission Control Protocol) 취약점

TCP를 사용하는 여러 운영체제에 새로운 취약점이 보고되었다. 이 취약점은 서비스거부공격(DoS:Denial of Service)이 가능한 것으로 TCP의 성능향상을 위하여 소개된 TCP timestamp 와 PAWS(Protection Against Wrapped Sequence Numbers) 에 존재한다. 문제의 원인은 큰 수치의 조작된 timestamp를 처리하는 과정에서 발생된다. 이 취약점을 통해 특정 코드를 실행할 수는 없으며 DoS 상태만 가능하다. MS사의 운영시스템 경우 윈도우 XP 서비스팩2, 윈도우 서버 2003 서비스팩1 또는 MS05-019 패치가 적용된 시스템은 이 취약점에 영향을 받지 않는다.

► 공인인증서 해킹에 취약(?) 논란

'공인인증서가 해킹에 취약하다' 라는 소식이 처음 보고된 후 이에 대한 우려가 높아졌다. 언론들은 앞다퉈 이에 대한 소식을 다루었고 공인인증서가 취약하다는 내용에 사용자들은 걱정을 자아냈다. 하지만, 이번 사건은 공인인증서 자체의 안정성과는 무관한 것이다. 공인인증서를 관리하는 특정 프로그램에 취약점이 존재하여 이것을 이용한 악의적인 행동이 가능

하였을 뿐 '공인인증서'라는 전체에까지 확대 해석된 것은 잘못된 것이다.
다행히도 업체들의 발빠른 대응으로 큰 문제를 가져오지는 않았지만 이에 대한 문제를 한번 짚어 보도록 하겠다. 우선, 현재의 인터넷 환경구조에서는 공인인증서 관리 프로그램뿐만 아니라 많은 프로그램들이 이러한 위험에 노출될 수 있기 때문에 비단 공인인증서에만 초점이 맞춰질 이야기는 아니다. 사용자의 컴퓨터에 트로이목마가 설치돼 키보드 내용을 가로채는 등의 행위가 쉽게 이뤄질 수 있는 가능성이 있기 때문에 사용자들이 보안에 대한 인지가 있어야만 외부의 위험으로부터 본인의 자산을 지킬 수 있다. 아무리 뛰어난 보안 소프트웨어가 있다 하더라도 사용자의 방심은 보안사고로 이어질 수 있는 것인데 이것은 인간이라면 누구나 가질 수 있는 가능성이다.
다만 이번 계기를 통해 공인인증서 관리 프로그램 및 기타 소프트웨어들에 대한 보안적인 검토 그리고 일반 사용자들을 대상으로 한 보안 교육프로그램의 마련 등을 통해 세계적인 인터넷 강국으로서 인터넷의 활용측면에서도 안전하게 이용할 수 있는 준비가 필요할 것이다.

► IPv6 위협이 도래할 것인가?

마이크로소프트 운영체제인 윈도우 XP와 2003에 공격자가 서비스거부공격을 일으킬 수 있는 취약점이 보고되었다. 이번 취약점은 IPv6 TCP/IP 스택에 존재하는 것으로 차세대 인터넷 주소체계인 IPv6에서 발견되었다는 점이 특이할 만하다. 이것은 SYN 플래그가 설정되고 출발지 주소, 포트가 목적지 주소, 포트와 동일하게 설정되어 오는 패킷을 처리하는 과정에서 취약점이 존재한다. 여기서 사용된 공격기법은 과거 IPv4에도 있었던 Land Attack이라는 알려진 기술이다. 다만 IPv6에도 같은 기법이 보고되었다는 것인데, 향후 IPv6가 일반화되었을 경우 IPv4에서 이용되었던 다양한 공격기법들이 IPv6에서도 이용되고 IPv6 프로토콜 취약점이 대두될 가능성이 높다.
물론 아직 IPv6가 대중화되어 있지 않은 만큼 이에 대한 우려는 적지만 준비는 필요하다. 언젠가 인터넷 주소가 고갈되면 IPv6로의 이전은 불가피 할 것이고 정부에서 추진하고 있는 u-Korea 로드맵에 따르면 2011년부터는 IPv6 Only 망으로 전환 계획을 갖고 있기 때문이다. IPv6는 패킷의 헤더를 단순화 시켜 보다 직접적이고 단순화된 라우팅 기능을 제공하여 인터넷 트래픽의 효율성 증대를 가져오고 향상된 QoS(Quality of Serice)를 보장한다. 또한 IPSec을 기본으로 포함하고 있어 보다 향상된 보안성을 제공해 주고 자동 네트워킹 기능을 통해 다양한 이동기기들이 손쉽고 편리하게 네트워크에 접속할 수 있게 해주는 등의 여러 장점들을 가지고 있다.
현재 많은 OS(Operating System)및 응용프로그램에서 IPv6 구현을 완료하였고 향후 다가올 IPv6를 대비하고 있다. 이제 IPv6는 멀지만은 않은 기술로써 우리에게 더욱 가깝게 다가오며 앞으로 IPv6가 가져올 위협에 대해서 예측해 볼 필요성이 높아질 것이다.

IV. 5월 세계 악성코드 동향

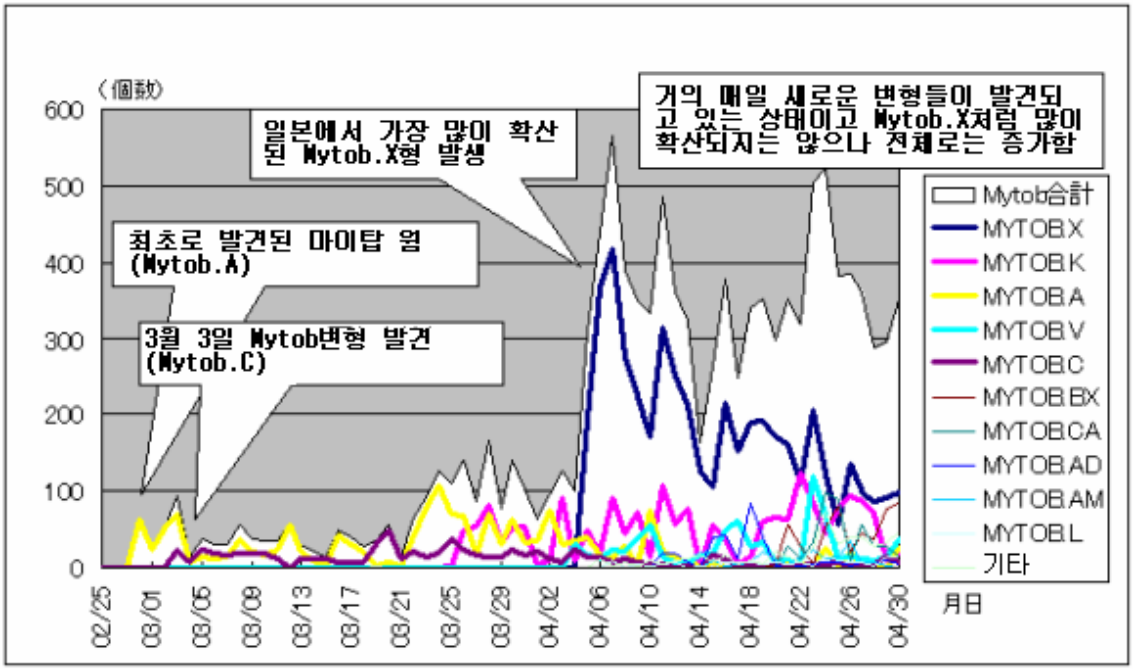
전 세계적으로 이번 5월은 메일로 전파되는 매스메일러 웜들이 강세를 보이고 있는 것으로 분석된다. 특히 유럽 지역에서는 마이톱 웜(Win32/Mytob.worm)의 여러 변형들에 의해서 많은 피해를 입은 것으로 알려졌으며, 일본 역시 마이톱 웜에 대한 주의를 각별히 요구하고 있다. 중국은 메일로 전파되는 백쯔 웜(Win32/Bagz.worm)이 강세를 보이고 있으나 5월경부터는 마이톱 웜의 피해가 점차 증가하고 있다. 그러나 이와 더불어 다양한 공격기법을 가지고 있는 트로이목마 역시 점차적으로 증가하고 있는 실정이다. 이러한 매스메일러들의 강세 속에서 중국과 일본 그리고 전세계적인 악성코드의 흐름이 어떻게 변해가고 있는지 자세한 내용들을 살펴보도록 하자.

(1) 일본의 악성코드 동향

작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

2005년 5월 일본에서 발생한 악성코드 관련 동향에서 주목할 점은 마이톱 웜의 감염 피해가 급격하게 증가한 것이다.

마이톱 웜은 메일과 윈도우 운영체제의 보안 취약점을 이용해 전파되는 악성코드로, 2005년 2월 말 최초 발견된 이후 많은 변형들이 추가로 발견되고 있다. 일본의 경우도 이러한 상황은 비슷하다. [그림1]은 마이톱 웜이 처음 발견된 시점인 2월말부터 4월까지 발생한 변형들에 대한 탐지 횟수를 나타낸 것이다. 4월에 이르러 급격하게 많은 양의 마이톱 웜 변형들이 발견된 것을 볼 수 있는데 이러한 상황은 5월에도 크게 달라지지 않은 것으로 보인다.



[그림1] 일본의 마이톱 웜 탐지 현황 (자료출처: 일본 IPA)

마이톱 웜은 기존의 매스메일러 기능에 더해서 아이알씨봇(IRCBot) 기능을 가지고 있어, 감염될 때 SMTP를 이용해 타 시스템에 대한 감염 시도를 하는 것과 더불어 보안 취약점을 공격하여 자신을 전파하려는 시도를 하게 된다.
전체 악성코드 감염 경로 중 메일이 차지하고 있는 비율이 매우 높다는 것을 고려해 보았을 때 매스메일러의 공격 패턴이 다양화된다는 것은 추가적인 피해의 발생 확률이 급증한다는 것이므로 다른 악성코드의 출현보다 더 심각한 문제일 수 있다.

일본 유행 악성코드 유형별 발생현황

[표1]은 일본의 IPA(정보처리추진기구)에서 2005년 5월 악성코드의 감염 통계를 표로 나타낸 것이다. IPA의 자료에 의하면 5월 한달동안 가장 많이 확산된 악성코드는 넷스카이 웜(Win32/Netsky.worm)이다. 넷스카이 웜의 감염 피해는 전월에 비해 100건 정도 증가하였으나 전체 감염 피해 건수로 비교했을 때 감염 피해의 증가는 미약한 수준이다.
5월 악성코드 감염 통계에서 주목할 점은 마이톱 웜의 감염 피해가 전월에 비해서 크게 증가한 것이다. 마이톱 웜 감염 피해 증가의 주요 원인은 여러 변형들이 계속 발견되고 있는 점일 것이다. 메일을 통한 전파뿐 아니라 윈도우 운영체제의 보안 취약점을 공격하는 기능을 가지고 있는 등 감염 경로가 다양한 점이 감염 피해가 증가하고 있는 원인으로 분석된다.

윈도우/도스바이러스	금월피해	매크로바이러스	금월피해	스크립트바이러스	금월피해
	전월피해		전월피해		전월피해
Win32/Netsky	1,128	Xm/Laroux	21	VBS/Redlof	86
	1,009		16		68
Win32/Mytob	584	XF/Sic	8	VBS/Loveletter	7
	302		4		8
Win32/Mydoom	446	W97M/X97M/Toraja	3	Wscript/Fortnight	6
	377		0		7
Win32/Bagle	336	Tristate	3	VBS/Soraci	5
	330		1		3
Win32/Lovgate	264	X97M/Divi	3	VBS/ FreeLink	2
	249		2		2
Win32/Klez	251	X97M/Cap	1	VBS/Gaggle	2
	255		2		0

[표1] 일본의 5월 악성코드 피해 신고 현황

악성코드의 감염 경로별 통계

[표2]는 악성코드의 감염 경로에 대한 통계를 나타낸 것이다. [표2]에서 알 수 있는 것처럼 악성코드 감염 경로로 가장 많이 이용되는 매체는 메일로써 이전과 비교해서 크게 차이가 없다.

감염경로	피해 건수					
	2005년 5월		2005년 4월		2004년 5월	
메일	4,943	98.4%	4,381	98.7%	5,311	97.6%
외부의 모체	2	0%	4	0.1%	11	0.2%
다운로드	5	0.1%	1	0%	2	0 %
네트워크	59	1.2%	51	1.1%	91	1.7%
기타	12	0.2%	3	0.1%	24	0.4%

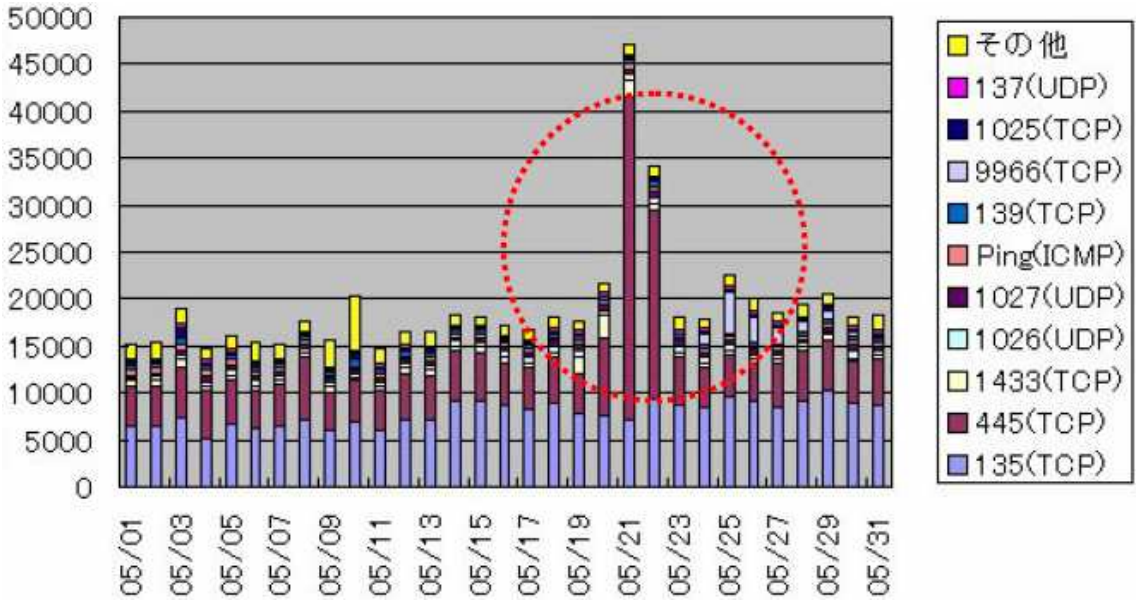
[표2] 악성코드 감염 경로 통계

일본 네트워크 트래픽 현황

[그림2]는 2005년 5월 한 달 동안 주요 네트워크 거점에서 발생한 네트워크 트래픽에 대한 통계를 나타낸 것이다. [그림2]에서 볼 수 있는 것처럼 TCP 135 포트와 TCP 445 포트의 네트워크 트래픽 양이 매우 많은 것을 알 수 있다. 두 포트들은 윈도우 운영체제에서 사용되는 포트들이다. 그러나 최근에 유행하는 네크워크 웜의 경우 이 포트들을 사용하는 윈도우 서비스의 취약점을 이용하여 불법적으로 권한을 획득하고 자신을 복제하려는 시도를 하는 공격이 빈번하게 발생하므로 주의가 필요하다.

5월 데이터에서 가장 주목할 점은 5월 20일을 전후로 TCP 445 포트의 트래픽이 갑자기 증가한 것이다. 이러한 현상이 발생한 원인은 스페인과 독일 등 유럽에서 5월 20일부터 24일까지 다량의 트래픽이 발생한 것이 원인이다. 발신자 주소도 대부분 상이한 것으로 미루어 공격이라기 보다는 국지적으로 유행한 악성코드 등이 원인일 가능성이 높은 것으로 분석된다.

이외에도 5월 19일부터 21일 사이에 TCP 1433 포트의 트래픽 역시 갑자기 증가했는데 이는 SQL 오버플로우 웜(SQL_Overflow)의 영향으로 추정하고 있다.



[그림2] 일본의 5월 네트워크 트래픽 현황

(2) 중국의 악성코드 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

5월 중국 악성코드의 동향은 여전히 백쯔 웜(TrojanDroper.Worm.Bagz, V3 진단명 Win32/Bagz.worm)이 가장 많은 분포를 차지하며 1위를 유지하고 있다. 그러나 악성코드 TOP 5의 순위 상으로는 1위를 유지하고 있는 것으로 보이나 주간 악성코드 동향과 전체 분포면에서는 서서히 감소 추세가 보이고 있다. 그리고 전 세계적으로 높은 확산을 보이는 마이톱 웜(Worm.Mytob, V3 진단명 Win32/Mytob.worm) 역시 중국 내에서 확산되고 있는 것으로 보이고 있다. 그리고 지난 달부터 등장한 다양한 형태의 트로이목마는 이번 5월 달에도 악성코드의 새로운 위협으로 등장하고 있다.

악성코드 TOP 5

순위 변화	순위	Rising
-	1	TrojanDroper.Worm.Bagz
↑ 3	2	Backdoor.Huigezi
New	3	Backdoor.Win32.Agobot
-	4	Trojan.PSW.QQPass
New	5	Worm.Mytob

[표1] 2005년 5월 라이장(Rising)사의 악성코드 TOP 5

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

순위변화	순위	JiangMin
-	1	Trojan/QQMsg.QQTail.Zigui.b
-	2	Trojan/QQMsg.Zigui.b
-	3	Trojan/WebImport
-	4	Exploit.MhtRedir
-	5	TrojanDownloader.Small.afz

[표2] 2005년 5월 강민(JiangMin)사의 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. 우선 라이징의 TOP 5부터 살펴보면 새로운 악성코드 2건이 새롭게 순위에 기록되었다. 새롭게 순위에 포함된 악성코드로는 아고봇 웜(Backdoor.Win32.Agobot, V3 진단명 Win32/AgoBot.worm)과 마이톱 웜이다. 아고봇 웜은 익히 알려진 바와 같이 악성 봇 웜의

변형 중 하나이며 현재까지도 꾸준한 확산을 보이고 있는 웜이다. 마이톱 웜의 경우에는 전 세계적으로 많은 확산을 보이고 있으면 현재까지도 다양한 변형들이 지속적으로 등장하여 많은 주의를 필요로 하고 있다.

중국 로컬 백신 업체 중 하나인 강민의 악성코드 TOP 5를 살펴보면 라이징의 순위와는 대조적으로 TOP 5 중 4위를 차지한 Exploit.MhtRedir를 제외하고는 모두 트로이목마가 차지하고 있다. Exploit.MhtRedir는 html 또는 chm 형태의 파일 실행 시 발생하는 윈도우 탐색기의 취약점을 이용하고 있다. 이 취약점을 이용하여 악성코드 제작자는 트로이목마 또는 웜을 실행할 수 있도록 만들고 있어 윈도우 보안 패치 적용에 대한 경각심을 다시 일으키고 있다.

주간 악성코드 순위

순위	1주	2주	3주	4주
1	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz
2	Backdoor.Huigezi	Worm.Netsky	Trojan.PSW.Lmir	Worm.Mytob
3	Script.DownLoader.Psyme.b	Backdoor.Win32.Agobot	Backdoor.Agobot	Backdoor.Huigezi
4	TrojanDropper	Backdoor.Huigezi	Trojan.PSW.QQDragon	Trojan.PSW.QQRobber
5	Worm.Netsky	Trojan.PSW.Lmir	Backdoor.Huigezi	Trojan.PSW.QQPass

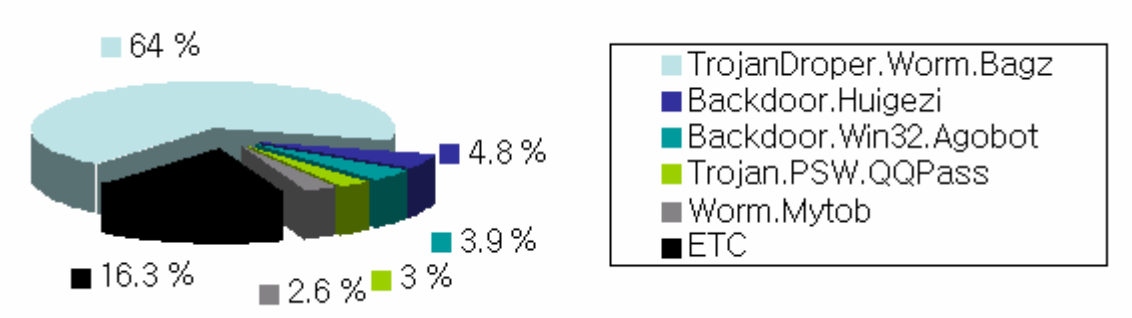
[표3] 2005년 5월 라이징(Rising)사의 주간 악성코드 순위

순위	1주	2주	3주	4주
1	Trojan/QQMsg.QQTail.Zigui.b	Trojan/QQMsg.QQTail.Zigui.b	Trojan/QQMsg.Zigui.b	Trojan/QQMsg.Zigui.b
2	Trojan/QQMsg.QQTail.Zigui.a	Trojan/QQMsg.Zigui.b	Trojan/QQMsg.QQTail.Zigui.b	Exploit.MhtRedir
3	Trojan/WebImport	Trojan/WebImport	Trojan/WebImport	Trojan/WebImport
4	TrojanDownloader.Small.afu	TrojanDownloader.Small.afu	Trojan/QQMsg.Zigui.a	TrojanDownloader.Small.afz
5	Exploit.MhtRedir	Exploit.MhtRedir	VBS/KJ	Trojan/Script.Seeker

[표4] 2005년 5월 강민(JiangMin)사의 주간 악성코드 순위

라이징의 주간 악성코드 순위를 살펴보면 TOP 5에서 1위를 차지한 백쯔 웜을 제외하고는 매주 다양한 악성코드의 순위 변화가 발생한 것을 알 수 있다. 1주와 2주차에서는 넷스카이 웜(Worm.Netsky, V3 진단명 Win32/Netsky.worm)이 많은 변화를 보였으나 3주차에 접어들면서는 급격한 감소를 보여 주었다. 앞서 높은 확산과 많은 변형으로 인해 주의가 우려된다고 설명한 마이톱 웜의 경우에는 4주차에 등장하자마자 2위를 차지하여 6월에도 현재와 같은 확산을 유지할 것으로 보여진다. 그리고 사용자의 계정과 암호를 가로채는 패스워드 스틸러 형태의 트로이목마들이 다수 순위에 등장한 것이 주목되며 지난 달까지 꾸준히 감염보고가 있었던 악성 아이알씨봇(IRCBot)의 경우도 아고봇 웜을 제외하고는 순위에 등장하지 않은 것으로 미루어 감소 추세를 보이고 있는 것으로 추정된다.
강민의 경우에는 다양한 형태의 트로이목마가 중국 내에서 많이 확산되어 있다는 것을 라이징에 비해 자세하게 나타내고 있는 것으로 보인다. 4주간의 순위 변화 모두 트로이목마에 의한 변화로만 기록되어 있으며 마이톱 웜이나 기타 악성 봇 들은 순위에서 찾아 볼 수가 없는 것이 라이징과는 또 다른 악성코드 동향을 예측할 수 있게 하였다.

악성코드 분포



[그림1] 2005년 5월 라이징(Rising)사의 악성코드 분포

2005년 5월 라이징의 악성코드 분포를 살펴보면 백쯔 웜이 전체 64%를 차지하고 있다. 지난 4월과 비교하여 24%나 증가한 수치를 보이고 있다. 그러나 주간 악성코드 순위 변화에서 설명한 것과 같이 점차 감소하는 추세를 보이고 있으므로 6월 악성코드 동향에서 어떠한 변화를 가져올지 주목된다. 5월 4주째에 등장한 마이톱 웜은 2.6%를 차지하고 있으나 전세계적인 흐름과 추세로 미루어 6월에는 더욱 높은 수치를 차지할 것으로 보여지고 있다. 기타를 포함한 나머지 악성코드들의 경우에는 전반적으로 분포상의 수치가 줄어든 것으로 분석된다.

(3) 세계 악성코드 동향

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

영국 소포스(Sophos)사의 2005년 5월 통계[1]를 보면 소버 웜(Win32/Sober.worm) 변형과 자피 웜(Win32/Zafi.worm) 변형이 각각 1위와 2위로, 피해 보고의 50% 이상을 차지하고 있다. 러시아 캐스퍼스키 연구소(Kaspersky Lab)의 통계[2]를 보면 마이톱 웜(Win32/Mytob.worm)이 1위를 차지하고 있으며 소버 웜 변형이 7위이다. 마이톱 웜은 2005년 2월 발견 이후 150개 이상의 변형이 발견되었다. 5월에 발생한 소버 웜 변형은 유럽 등지에서 많이 퍼졌지만 윈도우 한글 버전 등 비 영어권 시스템에서는 웜이 제대로 실행되지 않는 경우가 많아 아시아 지역의 피해는 비교적 적은 것으로 알려졌다. 유럽 업체들이 밝힌 상위권 순위 대부분은 소버 웜 변형, 자피 웜 변형, 마이톱 웜 변형, 넷스카이 웜(Win32/Netsky.worm) 변형 등 메일로 전파되는 웜이 대부분이었다.

한국과 일본의 유명 사이트가 해킹되어 트로이목마가 배포된 사건이 발생했다. 변조된 홈페이지는 MS04-013 취약점[3]을 이용해 트로이목마를 설치하므로 패치가 적용되지 않는 시스템이 이들 사이트에 접속하는 것만으로도 트로이목마가 설치된다. 수법이나 접속하려는 주소 등이 유사해 동일인 혹은 동일 그룹에서 유포한 것으로 추정되며 리니지 게임의 계정과 비밀번호를 유출하는 트로이목마인 리니지핵 트로이목마(Win-Trojan/LineageHack) 변형이 설치된다. 트로이목마 제작자는 훔친 리니지 게임의 계정과 비밀번호로 다른 사람의 게임 아이템을 훔쳐 사용하거나 온라인 게임 아이템 거래 사이트를 이용해 판매할 것으로 보인다.

이스라엘에서는 산업스파이 행위가 적발되었다. 이들은 경쟁사의 기밀을 빼내기 위해 전화도청뿐만 아니라 트로이목마가 담긴 CD 등을 통해 정보를 빼냈다. 여기에서 사용된 트로이목마는 핫월드 트로이목마(Win-Trojan/HotWorld)로 현재 다수의 변형들이 보고되었다. 트로이목마는 바이러스나 웜과 달리 자기 복제를 하지 않으므로 소수의 사람에게만 배포할 경우에는 발견 가능성이 매우 낮아진다. 악성코드를 이용한 돈벌이는 결국 산업스파이까지 확대되었다.

---

[1] 영국 소포스(Sophos)사의 2005년 5월 피해통계,
http://www.sophos.com/pressoffice/pressrel/uk/20050601topten.html

[2] 러시아 캐스퍼스키 연구소(Kaspersky Lab)의 5월 피해통계,
http://www.viruslist.com/en/analysis?pubid=164727154

[3] Microsoft Security Bulletin MS04-013,
http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx

V. 이달의 ASEC 컬럼 – 게임아이템 매매를 위한 홈페이지 변조사건

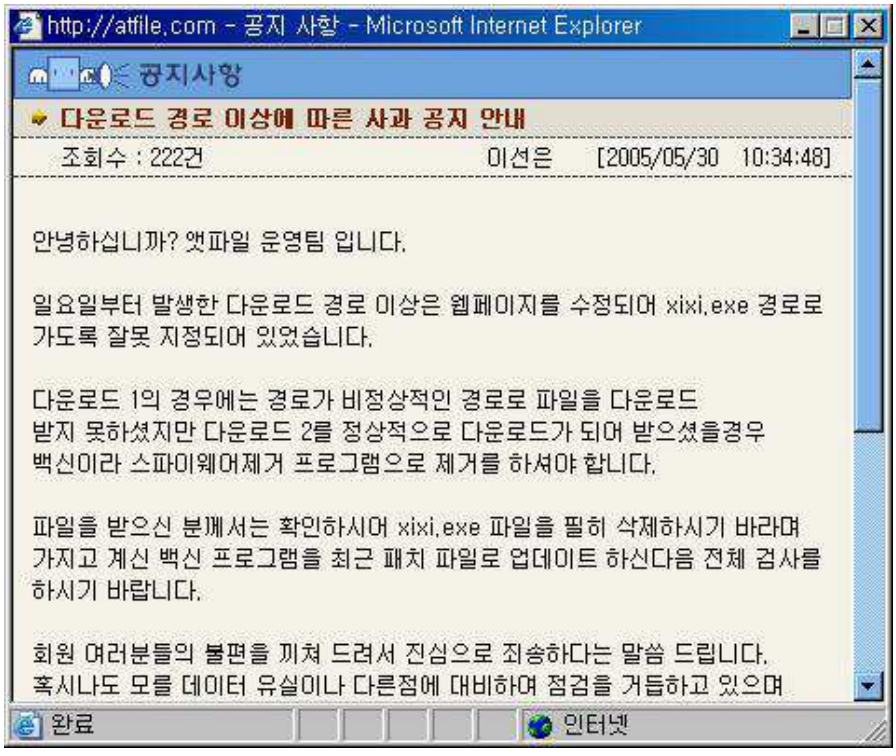
작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

2004년 말부터 엔씨소프트의 '리니지'나 위메이드의 '미르의 전설 2' 게임의 계정과 비밀번호를 훔치는 프로그램이 증가했다. 이들 프로그램은 한국의 대표적 온라인 게임으로 중국에서 많은 인기를 끌고 있다. 2005년 5월에는 한국과 일본의 유명 사이트를 해킹 해 리니지 계정과 비밀번호를 훔치는 트로이목마가 퍼졌다. 주요 사건과 홈페이지 변조의 목적에 대해 알아보겠다.

일본과 한국 사이트 해킹 사건

2005년 5월 16일 일본 최대의 가격 비교 사이트인 카카쿠 닷컴(http://www.kakaku.com)이 사이트 변조로 인해 약 일주일간 사이트를 폐쇄한다는 기자회견을 가졌다. 사용자가 이 사이트에 접속할 경우 특정 주소로 접속해 취약점을 통하여 패치되지 않은 시스템에 특정 파일이 설치되도록 했다. 설치되는 트로이목마는 V3에서 Win-Trojan/Delf.50688)과 Win-Trojan/Delf.23040.C로 진단된다.

한편 한국에서는 2005년 5월 29일 한국의 대표적 자료실인 앳파일(http://atfile.com)의 모든 자료 다운로드 주소가 특정 사이트의 xixi.exe로 변경되는 사건도 있었다.. 5월 30일 앳파일에서 조치와 함께 사과문을 올렸다.



[그림1] 앳파일의 사과 공지사항

6월 초 안철수연구소는 한국 MSN의 MSN 모바일 프리미엄 서비스 페이지에 접속하면 특정 주소의 icyfox.htm 파일이 로드되고 icyfox.exe 파일을 다운로드 받아 실행된다는 신고를 받았다. 6월 3일 마이크로소프트 포털사이트 MSN은 한국 MSN의 뉴스 사이트가 2일 해킹당해 악성코드가 설치됨에 따라 이를 제거하고 사이트를 복구했다고 3일 밝혔다. 처음에는 스파이웨어가 설치된다고 했으며 이후 외신에서 리니지 해킹 프로그램으로 알려졌다.
6월 6일에는 한국의 코리아닷컴(http://www.korea.com)의 자료실 주소가 변조된 한국 MSN에서 다운로드되던 주소와 동일하게 변조되었다. 이외 한국의 여러 사이트에서 홈페이지 변조가 보고되었다. 접속 주소와 파일명이 동일한 것으로 보아 한국 MSN을 해킹한 동일인 혹은 동일그룹으로 소행으로 추정된다.

취약점과 리니지 계정 훔쳐가기

한국과 일본에서 발생된 이들 홈페이지 변조 사건은 공통적으로 MS04-013 취약점을 이용해 패치가 적용되지 않은 시스템에서 해당 사이트에 접속할 경우 제작자가 원하는 프로그램을 실행할 수 있도록 했다. V3에서는 MS04-013 취약점을 이용하는 스크립트를 JS/Exploit-MhtRedir로 진단하며 이 취약점을 이용해 실행되는 악성코드 설치자는 리니지핵 드롭퍼(Dropper/LineageHack)로 진단한다. 설치되는 리니지 해킹 프로그램은 V3에서 리니지핵 트로이목마(Win-Trojan/LineageHack)로 진단되며, 이들 프로그램은 리니지 게임이 실행되면 사용자가 입력하는 계정과 비밀번호를 트로이목마 제작자에게 보내 사용자 정보를 유출한다.

범인은 리니지 유저들?

목표가 되는 리니지는 한국의 엔씨소프트(http://www.ncsoft.com)에서 제작한 게임으로 한국 외 여러 나라에서 서비스되고 있다. 한국뿐 아니라 중국, 일본 등의 아시아 지역에서도 다수의 사용자가 있다. 리니지 게임의 몇몇 아이템은 고가에 거래되고 있으며 리니지 계정과 비밀번호를 훔치는 것도 리니지 사용자가 가지고 있는 아이템을 자신의 계정으로 옮기거나 다른 사람에게 팔기 위한 것으로 보인다. 따라서, 이들 트로이목마 제작자는 리니지 게임 이용자이거나 리니지 게이머들과 결탁한 개인 혹은 그룹으로 보인다. 또한 리니즈 게임 해킹의 핵심 기능인 키보드 입력 내용을 저장하는 프로그램의 소스가 공개된 것으로 알려져 여러 사람이 리니지 계정과 비밀번호를 훔치는 프로그램을 제작할 수 있다.

게임/서버	물품내용	판매가격	종류	등록일시
리니지 > 01 데포루쥬	분 [총 1,000만/최소 200만]◇◆믿음+신용 아데... NEW	100만당 20,100원	게임머니	09:43:02
리니지 > 01 데포루쥬	분 [총 1,000만/최소 200만]◇◆믿음+신용 아데... NEW	100만당 20,100원	게임머니	08:43:02
리니지 > 01 데포루쥬	분 [총 1,000만/최소 200만]◇◆믿음+신용 아데...	100만당 20,100원	게임머니	2005/06/06
리니지 > 01 데포루쥬	분 [총 1,000만/최소 200만]◇◆믿음+신용 아데...	100만당 20,100원	게임머니	2005/06/06
리니지 > 01 데포루쥬	[판매] 이백만 (2,000,000) 아데나 팝니다.	38,000원	게임머니	2005/06/04
리니지 > 01 데포루쥬	분즉 [총 500만/최소 100만]5백만 개인아데나 파라...	100만당 19,000원	게임머니	2005/06/02
리니지 > 01 데포루쥬	분 [총 400만/최소 100만]4백만 분할판매	100만당 18,000원	게임머니	2005/06/02
리니지 > 01 데포루쥬	[판매] 일백만 (1,000,000) 아데나 팝니다.	19,000원	게임머니	2005/06/02
리니지 > 01 데포루쥬	분 [총 400만/최소 100만]4백만 분할판매	100만당 18,000원	게임머니	2005/06/02
리니지 > 01 데포루쥬	[판매] 이백만 (2,000,000) 아데나 팝니다.	37,000원	게임머니	2005/06/02
리니지 > 01 데포루쥬	[판매] 일백만 (1,000,000) 아데나 팝니다.	19,000원	게임머니	2005/06/01
리니지 > 01 데포루쥬	분 [총 400만/최소 100만]4백만 분할판매	100만당 18,000원	게임머니	2005/06/01
리니지 > 01 데포루쥬	완 [판매] 삼백만 (3,000,000) 아데나 팝니다.	57,000원	게임머니	2005/05/27
리니지 > 01 데포루쥬	완 [판매] 오백만 (5,000,000) 아데나 팝니다.	92,500원	게임머니	2005/05/20
리니지 > 01 데포루쥬	분즉완 [거래수량 : 800만]24시아덴마트	147,200원	게임머니	2005/05/19
리니지 > 01 데포루쥬	분 완 [거래수량 : 100만]아덴매니아	16,500원	게임머니	2005/05/17
리니지 > 01 데포루쥬	분즉 [총 200만/최소 100만]☆★스타 아덴★☆ 신...	100만당 19,000원	게임머니	2005/05/03

[그림2] 한국의 게임 아이템 거래 사이트

해킹 목적의 변화

과거 해킹과 악성코드의 제작 이유는 단순한 장난이나 실력과시가 대부분이었다. 하지만, 2004년부터 스팸 메일 발송이나 애드웨어 배포로 돈을 벌기 위해 악성코드를 제작한 사람들이 이제 게임 아이템 거래 등을 위해 특정 게임 해킹 프로그램을 만들고 이를 배포하기 위해 홈페이지를 변조가 증가하고 있다.