ASEC Report 8월

® ASEC Report

2006. 9

안철수연구소의 시큐리티대응센터(AhnLab Security Emergency 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.

I. ASEC Monthly 통계

(1) 8월 악성코드 통계

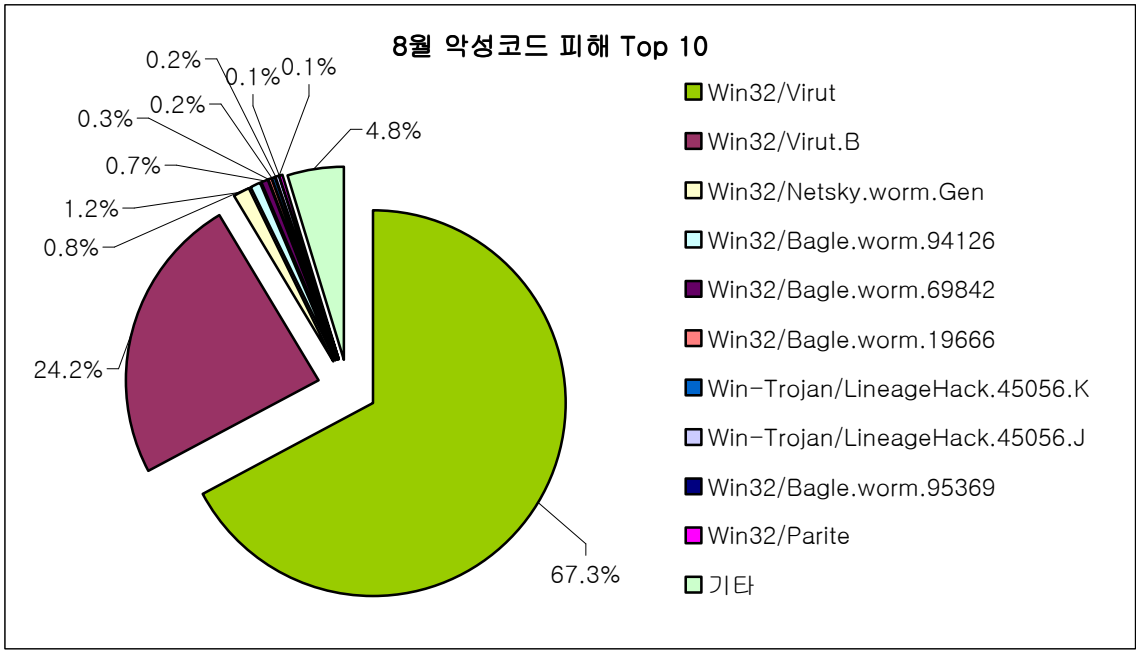
순위		악성코드명	건수	%
1	↑2	Win32/Virut	11,948	67.3%
2	↑3	Win32/Virut.B	4,293	24.2%
3	↓2	Win32/Netsky.worm.Gen	221	1.2%
4	New	Win32/Bagle.worm.94126	134	0.8%
5	New	Win32/Bagle.worm.69842	126	0.7%
6	New	Win32/Bagle.worm.19666	56	0.3%
7	New	Win-Trojan/LineageHack.45056.K	41	0.2%
8	↓6	Win-Trojan/LineageHack.45056.J	39	0.2%
9	↓5	Win32/Bagle.worm.95369	23	0.1%
10	New	Win32/Parite	19	0.1%
		기타	855	4.8%
합계			**17,755**	100.0%

[표1] 2006년 8월 악성코드 피해 Top 10

8월 악성코드 피해 동향

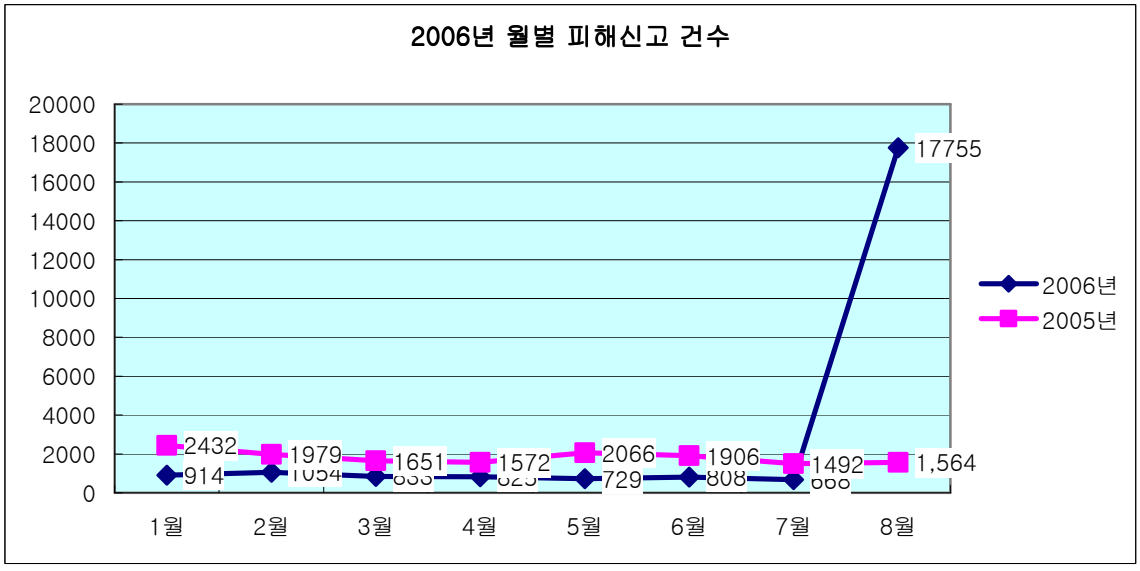
8월에는 윈도우 실행 파일을 감염시키는 바이럿 바이러스(Win32/Virut)과 그 변종인 바이럿.B 바이러스(Win32/Virut.B) 피해가 급증하였다. 또한, 7월 감소추세를 보였던 베이글 웜이 다시 10위권에 포함되었으며, 온라인 게임의 사용자 정보를 유출하는 리니지핵(Win-Trojan/LineageHack)변종이 7월에 이어 여전히 증가하고 있음을 알 수 있다.

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

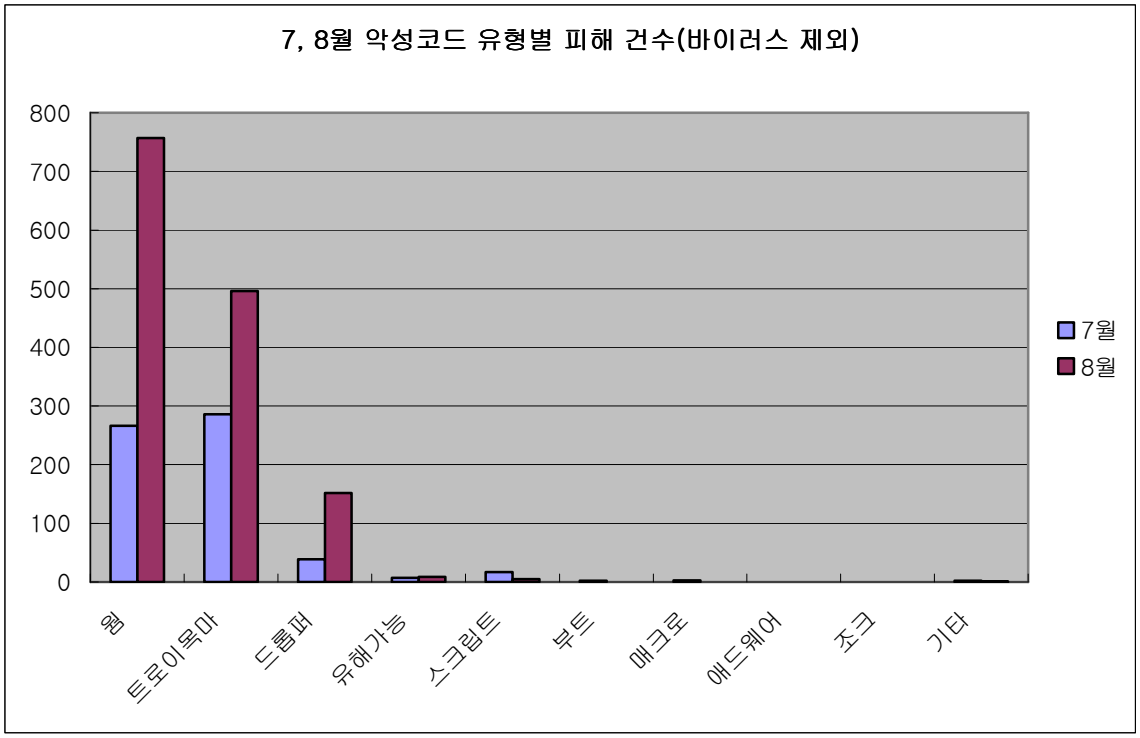


[그림1] 2006년 8월 악성코드 피해 Top 10

2006년 8월 악성코드 피해건수는 총 17,755건으로, 전년 동월 1,564건에 비해 약 11배 증가하였다. 급증의 원인은 바이럿 바이러스와 그 변종이 원인이다. 그러나, 8월에는 바이럿 바이러스의 피해뿐 아니라 다른 악성코드에 의한 피해도 전반적으로 전월에 비해 증가한 것을 [그림3]에서 확인할 수 있다.



[그림2] 2006년 월별 악성코드 피해신고 건수

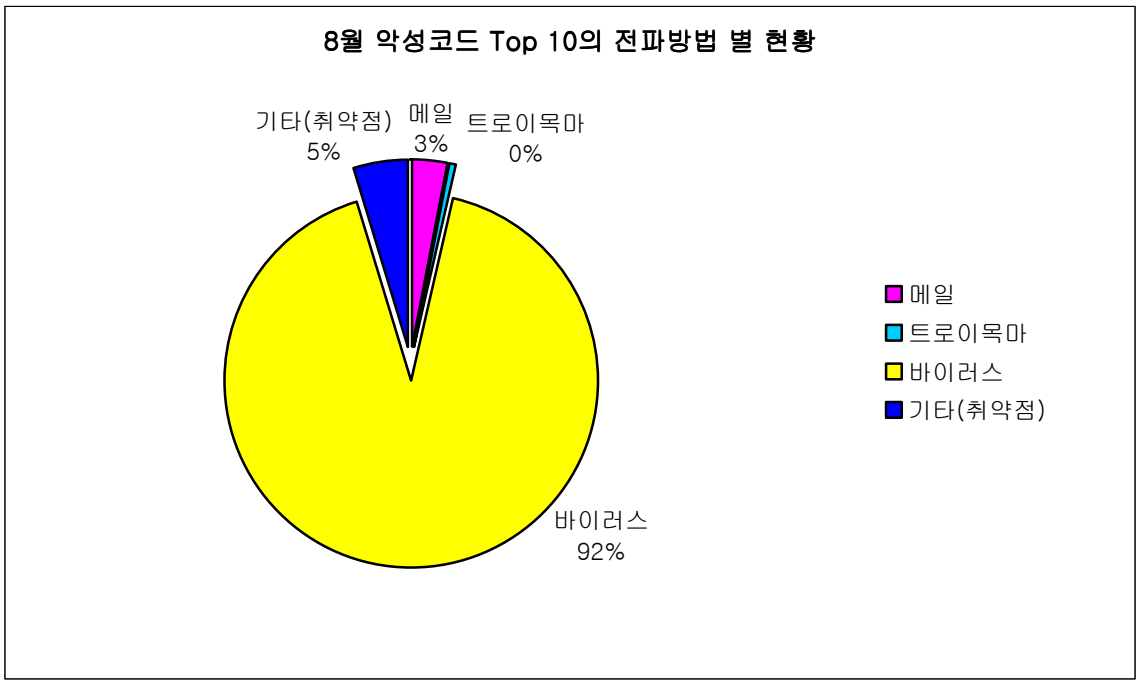


[그림3] 2006년 7, 8월의 악성코드 유형별 피해 건수(바이러스 유형 제외)

[그림3]은 8월 악성코드 피해 중 바이러스 유형을 제외한 악성코드 피해 건수를 7월과 비교한 자료이다. 웜, 트로이목마 및 드롭퍼의 피해가 7월에 비해 두배 이상 급증한 것을 알 수 있다. 트로이목마와 드롭퍼의 피해의 증가는 8월에 발표된 MS06-040 취약점을 이용한 악성코드의 증가가 그 원인이다.

8월 악성코드 Top 10 전파방법 별 현황

[표1]의 악성코드 피해 Top 10에서 확인된 악성코드는 [그림4]를 통하여 전파 방법을 확인할 수 있다.

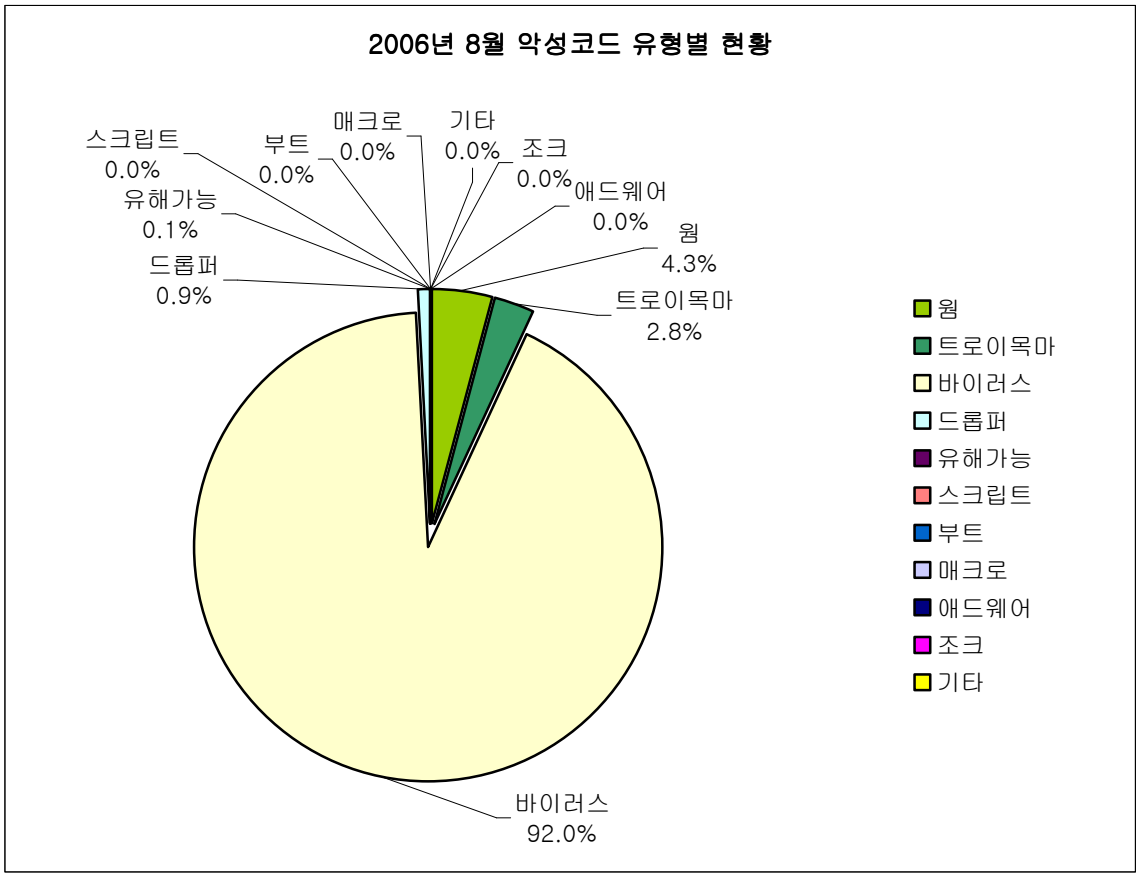


[그림4] 2006년 8월 악성코드 Top 10의 전파방법 별 현황

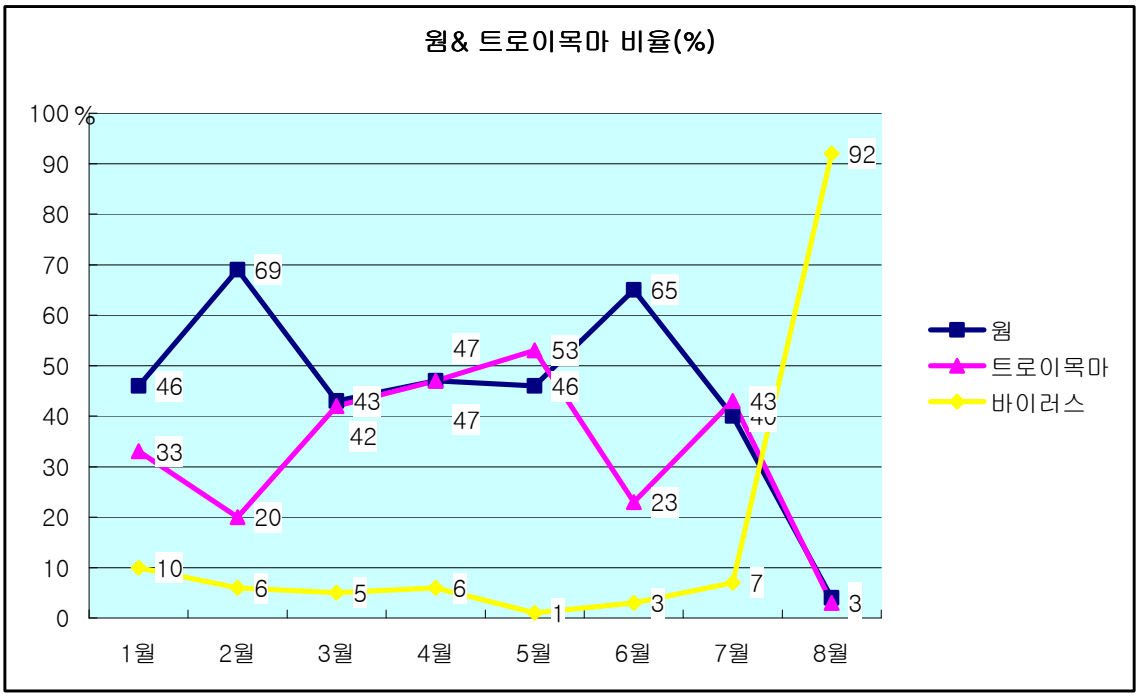
실행파일을 감염시키는 바이럿 바이러스로 인해 바이러스 피해 현황이 92%로 악성코드 피해 수의 대부분을 차지하고 있으며, 메일로 전파되는 특징이 있는 매스메일러는 3%, 트로이목마와 기타(취약점)가 각각 0.5%, 5%를 차지했다.

피해신고 된 악성코드 유형 현황

2006년 8월에 피해신고 된 악성코드의 유형별 현황은 [그림5]와 같다.



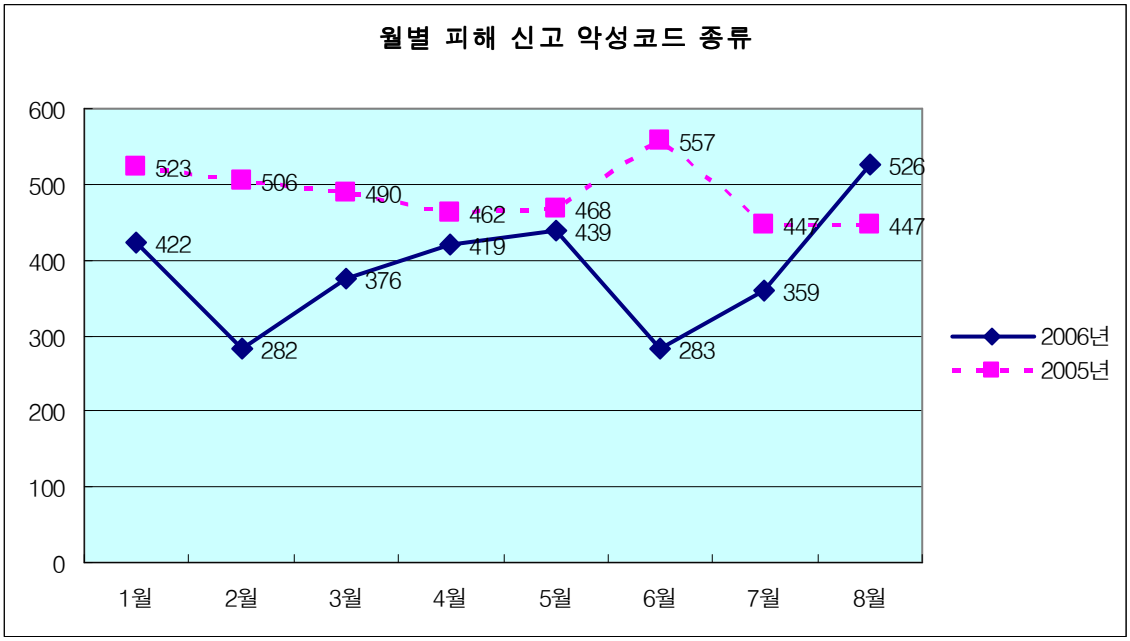
[그림5] 2006년 8월 피해 신고된 악성코드 유형별 현황



[그림6] 2006년 월별 웜, 트로이목마 피해신고 비율

월별 피해신고 된 악성코드 종류 현황

8월에 피해 신고된 악성코드 수는 모두 526개로, 이는 전년도 동월보다 다소 증가한 수치이다. 또한 7월에 이어 8월에도 피해신고 된 악성코드 수는 증가추세를 이어가고 있다. 이는 온라인 게임의 사용자 정보 유출과 관련된 악성코드 변형이 많이 발견된 것이 그 원인으로 보인다.



[그림7] 2005년, 2006년 월별 피해신고 악성코드 종류 개수

바이럿 바이러스[1] 피해신고 증가

8월에는 바이럿 바이러스의 피해신고가 매우 많이 접수되었다. 바이럿은 윈도우 실행파일을 감염시키는 바이러스로, 로컬 드라이브내의 *.exe, *.scr 확장자를 가지는 파일을 대상으로 감염시킨다. 전파 기능이 존재하지 않으며 감염된 파일을 실행할 때만 다른 파일을 감염시키지만, 바이럿에 감염된 트로이목마가 전파되면서 바이럿도 함께 확산되고 있는 것으로 조사되었다.

바이럿 바이러스는 시스템 커널 함수를 후킹하고 있어 완벽한 치료를 위해서는 메모리 치료가 선행되어야 한다. 안철수연구소에서는 바이럿의 손쉬운 치료를 위해 바이럿 전용백신[2]을 제공하고 있다. 따라서, 바이럿에 감염된 시스템 사용자는 안철수연구소 홈페이지의 [다운로드-전용 백신 다운로드]메뉴에서 바이럿 전용 백신을 다운로드 하여 치료하도록 한다.

---

[1] AhnLab, Win32/Virut (http://info.ahnlab.com/smart2u/virus_detail_4610.html)

[2] AhnLab, Win32/Virut 전용백신 (http://info.ahnlab.com/download/vaccine_view.jsp?num=55&pagecnt=1)

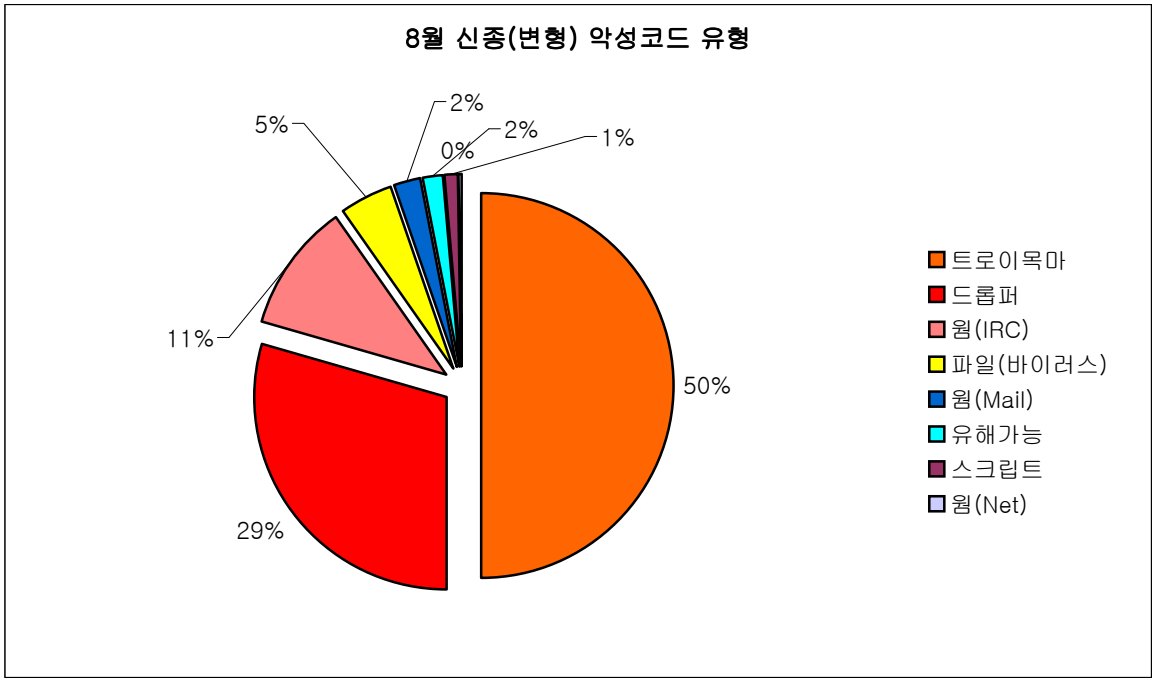
국내 신종(변형) 악성코드 발견 피해 통계

8월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표2], [그림8]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
41	153	90	3	14	0	0	0	5	0	306

[표2] 2006년 8월 유형별 신종 (변형) 악성코드 발견현황

8월은 전체적으로 전월 대비 신종(변형) 악성코드가 23% 증가하였다. 증가의 원인은 크게 2가지를 들 수 있는데, 그 중 하나는 MS06-040 서버 서비스 취약점 공격코드 등장과 이를 이용한 악성 IRCBot 웜의 증가이다. 또 다른 하나는 MS06-014 RDS.Dataspace Remote Execute-Exploit과 이를 악용한 스크립트 악성코드 증가로 인해 온라인 게임 계정을 탈취하는 트로이목마의 드롭퍼가 큰 폭으로 증가한 것이다. 8월에는 지난달에도 언급한 적이 있는 바이킹 바이러스(Win32/Viking)의 변형이 무려 14종이나 발견, 보고 되기도 하였다.

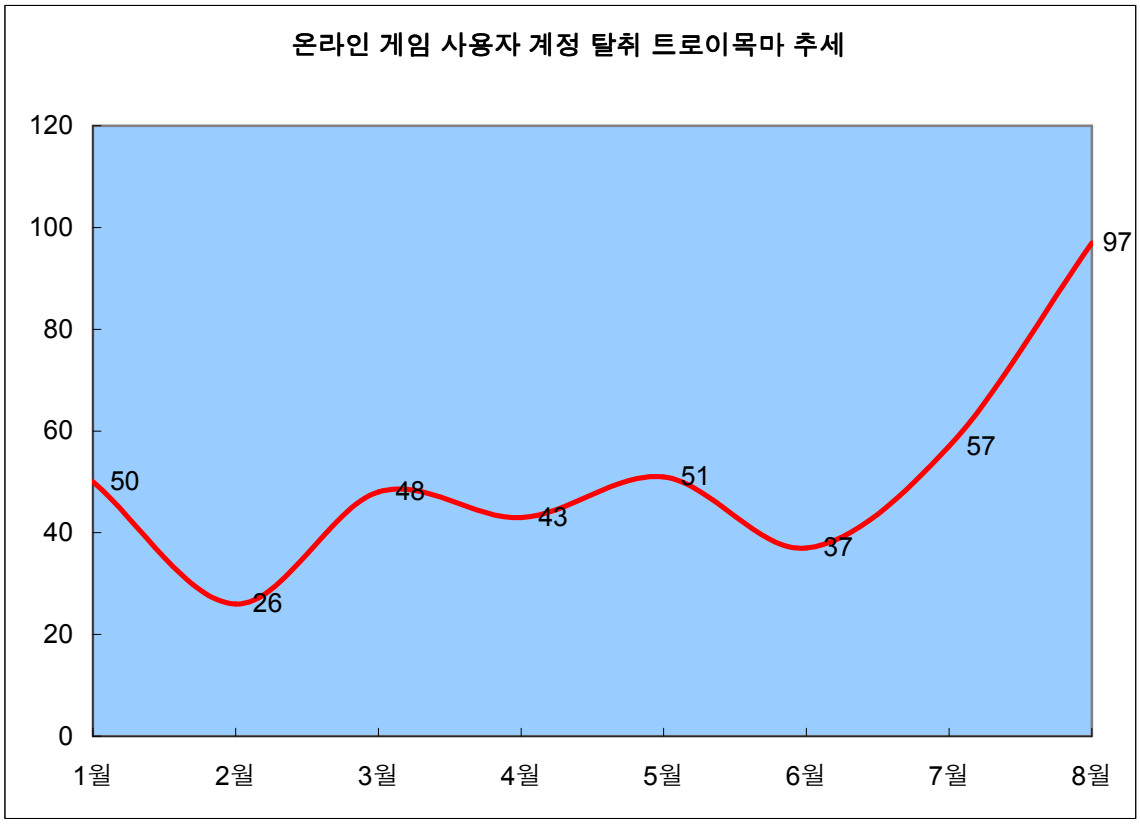


[그림8] 8월 신종(변형) 악성코드 유형

MS06-040 취약점과 공격코드의 등장으로 악성 IRCBot 제작자들은 이를 이용한 변형을 다수 유포하고 있는 것으로 보인다. 그러나 아직은 과거 2004년도 만큼 많은 수로 갑자기 늘어날 양상은 보이지 않고 있다. 이는 안티 바이러스 엔진 그리고 IDS, IPS 등에서 어느 정도 대응하고 있기 때문이며, 일부 윈도우 버전에서는 DoS 만 발생할 뿐 악성코드가 유입 되지 않기 때문이기도 하다. 그러나 새로운 실행압축 툴과 은폐기능을 갖는 악성 IRCBot 웜이 조금씩 증가하고 있어 그 추이는 좀 더 지켜보아야 하겠다.

바이킹 바이러스(Win32/Viking)의 경우도 변형이 국내 및 중국 등지에서 다수 보고되었다. 마치 바이러스 생성기가 있는 것이 아닌가 하는 추측이 들 정도로 변형이 계속 쏟아지고 있다. 이 바이러스는 중국발 웹 해킹의 피해를 당한 웹 사이트에 방문할 때 다운로드는 트로이목마에 감염된 채로 존재 한다. 이 바이러스의 감염이 증가한다는 것은 소위 '중국발 웹 해킹'의 피해를 입은 사이트가 증가하고 있다는 것을 의미하기도 한다.

다음은 중국발 웹 해킹의 주목적이기도 하며, 많은 변형이 발견, 보고되고 있는 온라인 게임의 사용자 계정을 탈취하는 악성코드에 대한 2006년도 월 발견 건수에 대한 그래프이다.



[그림9] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

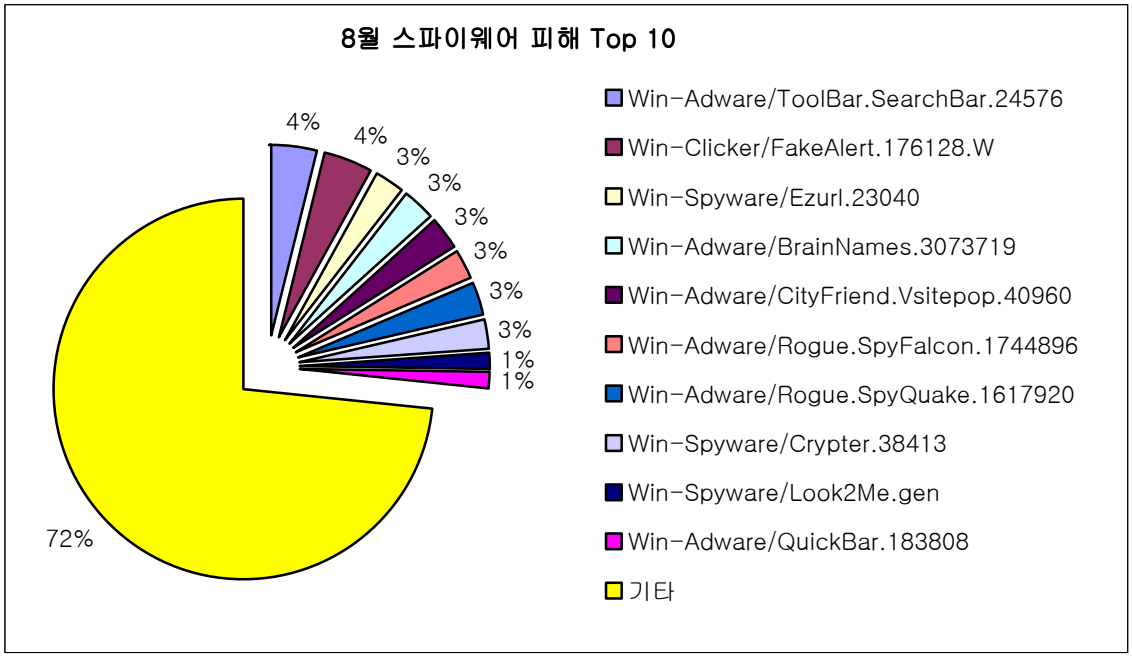
본글의 서두에서 언급 했던 것처럼 이번 달 역시 해당 트로이목마와 드롭퍼가 증가 하였다. 그 이유는 MS06-014 – RDS.Dataspace Remote Execute-Exploit로, 해당 취약점이 나온 후 이를 악용하는 스크립트 악성코드가 증가했고 이는 곧 드롭퍼의 증가로 이어졌기 때문인 것으로 추정하고 있다.

[1] 2006년 7월 자료와 비교해서 전체적으로 숫자가 증가하였는데, 이는 그 동안 통계를 트로이목마만 집계하였으나 8월부터는 트로이목마를 생성하는 드롭퍼까지 모두 통계에 포함했기 때문이다.

(2) 8월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	↑2	Win-Adware/ToolBar.SearchBar.24576	3	4%
2	New	Win-Clicker/FakeAlert.176128.W	3	4%
3	↓1	Win-Spyware/Ezurl.23040	2	3%
4	New	Win-Adware/BrainNames.3073719	2	3%
5	↓1	Win-Adware/CityFriend.Vsitepop.40960	2	3%
6	↓1	Win-Adware/Rogue.SpyFalcon.1744896	2	3%
7	New	Win-Adware/Rogue.SpyQuake.1617920	2	3%
8	↓1	Win-Spyware/Crypter.38413	2	3%
9	New	Win-Spyware/Look2Me.gen	1	1%
10	New	Win-Adware/QuickBar.183808	1	1%
		기타	55	72%
합계			75	100%

[표1] 2006년 8월 스파이웨어 피해 Top 10



[그림2] 2006년 8월 스파이웨어 피해 Top 10

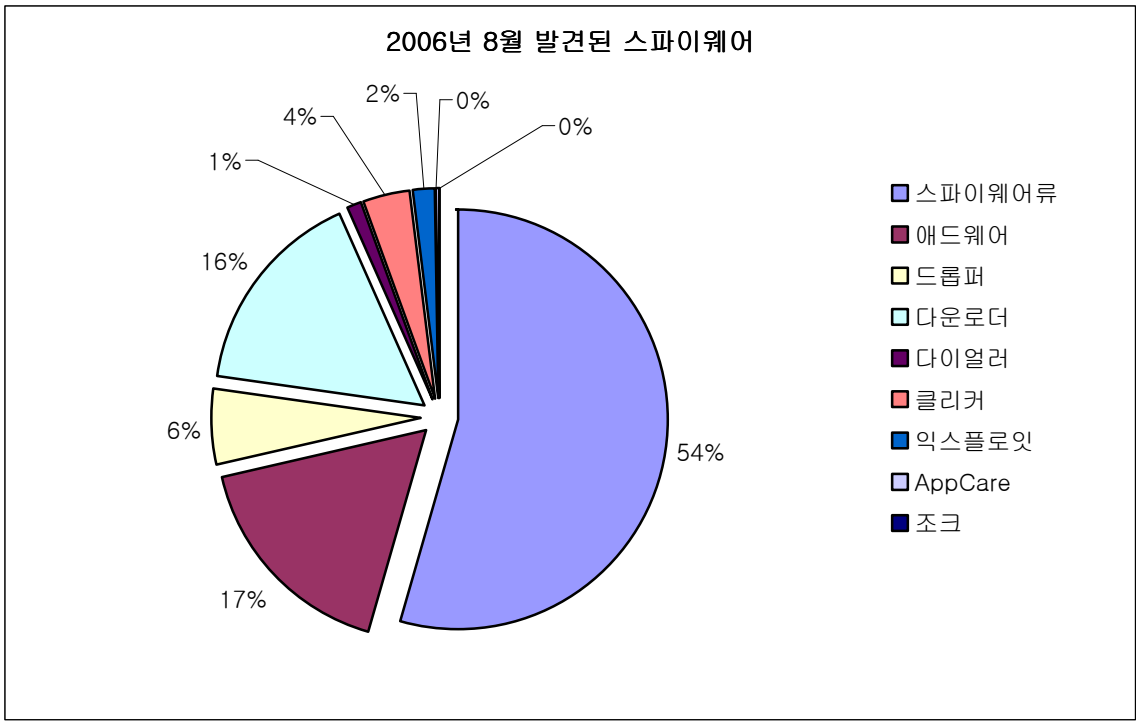
8월에는 총 75건의 스파이웨어 피해 사례가 접수되었으며 전월과 비교하여 비슷한 수준을 보였다. 가장 많은 피해 신고가 접수된 서치바(Win-Adware/ToolBar.SearchBar.24576)는 2006년 6월에 처음 발견되었으며, 불특정 웹 사이트에서 사용자 동의 없이 ActvieX로 설치된다. 7월과 8월에 지속적으로 피해 신고가 접수되고 있으며, 최근 많이 발견되고 있는 주소

표시줄 형태의 툴바로 만들어진 애드웨어이다. 8월에는 전체적으로 이지유알엘(Win-Spyware/Ezurl.23040) 등 국내에서 제작, 배포되고 있는 스파이웨어에 의한 피해가 전체 피해 Top 10의 절반을 차지할 정도로 두드러졌다.
허위 안티 스파이웨어 프로그램인 스파이팰콘(Win-Adware/Rogue.SpyFalcon.1744896), 스파이퀘이크(Win-Adware/Rogue.SpyQuake.1617920) 등의 허위 안티 스파이웨어에 의한 피해도 지속적으로 접수되고 있다.

8월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표2], [그림2]와 같다.

스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
259	81	28	76	5	18	8	1	0	476

[표2] 2006년 8월 유형별 신종(변형) 스파이웨어 발견 현황



[그림2] 2006년 8월 발견된 스파이웨어 프로그램 비율

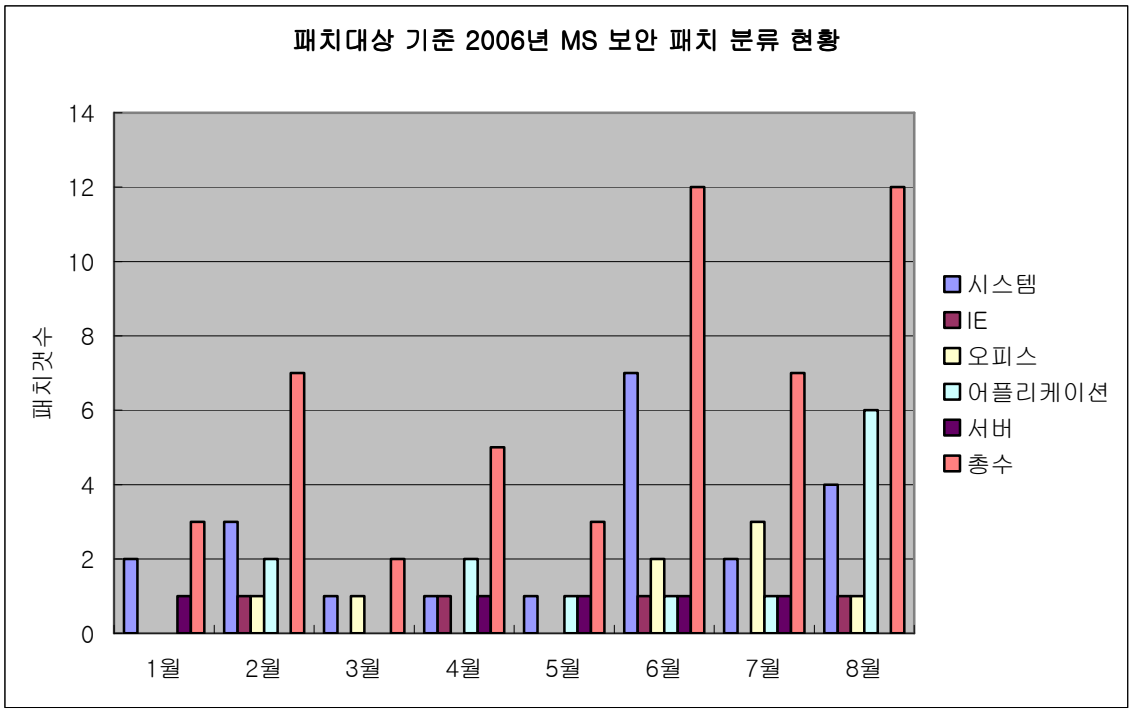
8월 발견된 신종(변형) 스파이웨어의 특징은 온라인게임 계정 유출 스파이웨어의 증가로 스파이웨어류가 지난달과 마찬가지로 가장 높은 비율을 보이고 있으며, 애드웨어 및 다운로더는 다소 감소하였다. MS 06-014 취약점을 이용하여 설치하는 리니지 스파이웨어 (Win-Spyware/PWS.Lineage) 등의 온라인 게임 계정 유출 스파이웨어 변형의 제작은 당분간 계속될 것으로 예상된다.

(3) 8월 시큐리티 통계

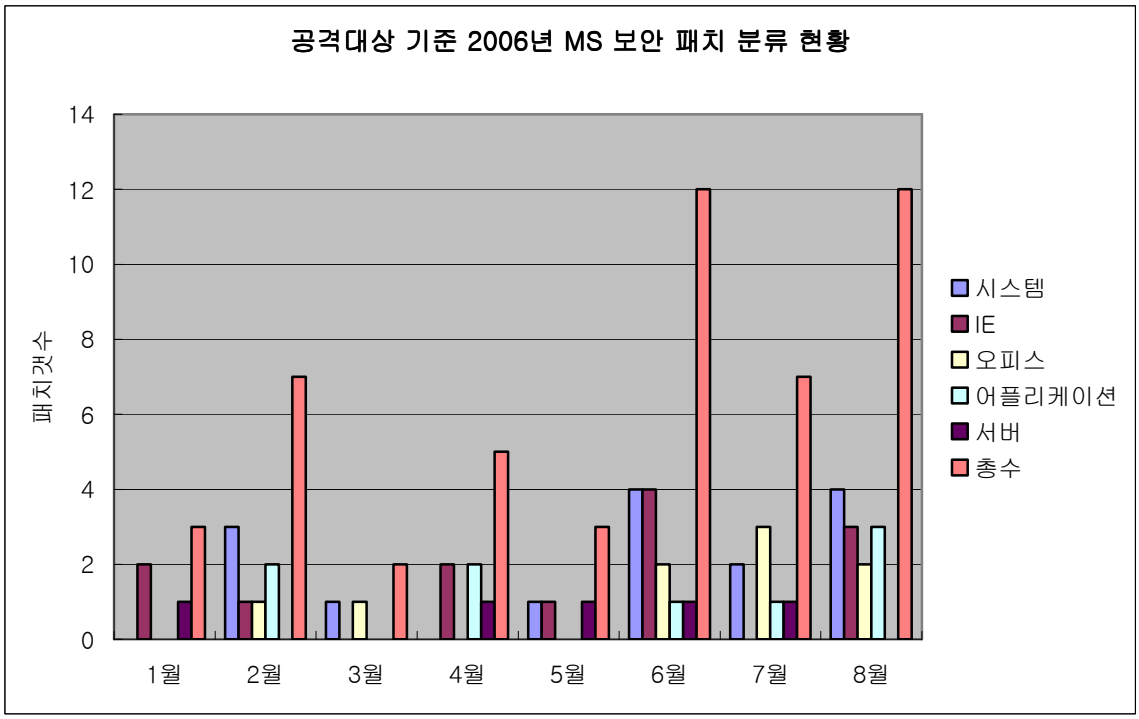
8월에 발표된 MS사의 정기 보안 패치는 총 12건으로 '긴급' 보안 공지 9건(MS06-040, MS06-041, MS06-042, MS06-043, MS06-044, MS06-046, MS06-047, MS06-048, MS06-051)과 '중요' 보안 공지 2건(MS06-045, MS06-049, MS06-050)이다. 인터넷 익스플로러 취약점을 보완하는 누적 보안 패치가 함께 발표되었으며, 지난 7월의 정기 보안 패치 7건보다 큰 폭으로 증가하였다.

이번 달에 발표된 보안 패치 중에서 가장 눈여겨 볼 수 있는 대목은 MS06-040인데, MS에서 보안 패치를 발표한지 5일 만에 해당 취약점과 관련 있는 악성코드가 발견되었으며, 현 시점에도 해당 취약점 공격코드를 악용한 IRCBot 변형의 피해신고가 꾸준히 접수되고 있다.

2006년 1월부터 8월까지 발표된 MS사의 보안 패치 현황은 [그림1]과 같다.



[그림1] 2006년 발표된 패치대상 기준 MS 보안패치 분류 현황



[그림2] 2006년 발표된 공격대상 기준 MS 보안패치 분류 현황(실제 공격활용 기준)

8월에 발표된 보안 패치는 오피스 제품 군에 영향을 미치는 보안 패치가 줄어든 반면 이외의 부문에서는 7월에 비해 증가한 것을 볼 수 있다. 특히 MS의 분류기준에서 최대 심각도가 '긴급'에 해당하는 보안패치가 다른 달에 비해 상대적으로 많고 취약점 대상이 시스템에서부터 어플리케이션까지 넓게 분포되어 있어, 다양한 외부 위협에 노출될 확률이 높다. 8월에는 뒤늦게 수정되어 제공된 보안패치가 있는 만큼 자신의 시스템에 최신패치가 적용되어 있는지 한번쯤 확인해 보는 것도 좋겠다.

II. ASEC Monthly Trend & Issue

(1) 악성코드 - MS06-040 취약점과 악성 IRCBot 웜

8월은 전통적으로 유독 대규모 피해를 입히는 신종 악성코드 출현이 많았던 달이었기에 안티 바이러스 업체들은 8월이 되면 긴장의 끈을 더욱 조이곤 한다. 올해 8월도 악성코드에서 이용될 가능성이 매우 높은 MS06-040 취약점이 발표되고 이를 이용한 악성코드가 발견되어 8월의 전통을 이어가나 싶었으나, 다행히 대규모 공격은 발생하지 않았다. 이 취약점과 더불어 몇 가지 이슈가 되었던 악성코드를 정리해 보자.

► MS06-040 서버 서비스 취약점 보고와 악성 IRCBot 출현

이 취약점은 과거 블래스터 웜처럼 대규모 공격에 매우 적합한 형태의 취약점이나, 과거보다 윈도우 보안이 강화되어 일부 윈도우는 DoS로 끝나버리는 형태이다. 뿐만 아니라, 공격코드가 나온 후 악성코드가 제작되는 것 또한 과거만큼 활발하지 않았다. 다만 안티 바이러스 로직의 일부를 알고 있는 제작자들이 악성 IRCBot 웜에 몇 가지 트릭[1]을 사용하여 안티 바이러스 엔진을 회피 하는 방법을 사용하고 있기는 하다. 그러나 이러한 변형도 이러한 트릭을 걷어 내면 웬만한 안티 바이러스 엔진에서 진단이 가능한 단순한 변형에 지나지 않았다. 공격코드 보고 후 이를 이용한 악성 IRCBot 웜이 전월 대비 135% 증가[2] 했지만, 이는 두 자리 이내에서 증가된 경우라 아직 우려할 만한 수준은 아니다. 앞으로 점점 이 취약점을 사용하는 악성 IRCBot 웜이 증가하고, 보다 일반화될 것으로 보인다. 그리고 이전에도 그랬던 것처럼 안티 바이러스 진단을 회피하는 형태도 꾸준히 증가 할 것으로 보인다.

► 바이킹 바이러스(Win32/Viking) 큰 폭으로 증가

지난 7월 리포트에서도 언급되었던 바이킹 바이러스가 8월에는 무려 14개의 변형이 발견 되었다. 이는 국내에서 발견된 변형만이며, 여기에 안철수연구소 중국법인으로부터 보고된 샘플까지 더 한다면 20개가 넘어선다. 바이킹 바이러스는 '중국발 웹 해킹'으로 인해 국내에 꽤 많이 확산 된 것으로 추정된다. 그렇게 추정하는 이유는 바이킹 바이러스에 감염된 트로이목마가 자주 목격 되었기 때문이다. 또 다른 원인 중에 하나는 공유폴더를 통한 전파이다. '쓰기'권한이 있는 공유폴더에 *.exe 형태의 확장자를 가진 파일이 존재할 경우 감염 되기 때문에 감염자가 여러 사람과 '파일서버'를 구성하여 공유한다면 확산은 매우 빠르게 이루어진다.

바이킹 바이러스의 변형이 언제까지 기승을 부릴 것인지는 알 수 없지만 계속적인 변형의 증가로 고객의 피해문의가 증가하고 있다. 참고로 일부 안티 바이러스에서는 바이킹 바이러

[1] 여기서 몇 가지 트릭이란 은폐된 프로세스와 안티 바이러스 엔진이 언팩을 지원하지 않는 실행압축툴을 말한다.

[2] 안철수연구소의 한국고객 신고 접수 통계기준

스를 웜으로 진단하고 있어 감염된 파일이 삭제되는 경우도 있으니 이 부분에 대해 주의를 기울일 필요가 있겠다.

► 온라인 게임 계정 탈취 목적의 드롭퍼 증가

MS06-014 취약점은 7월에 처음 보고 되었다. 그리고 이를 악용한 악의적인 스크립트가 덩달아 증가하기도 하였는데, 8월에는 드롭퍼가 상당수 증가하였다. 드롭퍼가 갑자기 증가한 이유는 명확하지 않지만 MS06-014 취약점이 그 한 원인으로 추정된다. 드롭퍼가 전월에 비해 증가했음에도 불구하고 8월에는 7월과 달리 취약점을 이용한 악의적인 스크립트가 크게 증가하지 않았다. 그러나 전월과 달리 8월에 발견된 스크립트는 여러 번 Crypt되어 있는 것이 특징이다. Crypt 된 코드를 풀어내도 이는 또 다르게 인코드되어, 안티 바이러스 엔진에서 진단이 어렵도록 하였다. 다행스러운 점은 드롭퍼에서 생성되는 트로이목마의 상당수가 기존 엔진에서 이미 진단되고 있어, 실질적인 피해는 크지 않았다.

► 스트레이션 웜(Win32/Stration.worm) 등장

국내와는 달리 해외에서는 스팸 메일을 통하여 악성코드를 유포한다는 소식을 종종 들을 수 있다. 이것이 누군가 고의로 보낸 것일 수도 있고 스팸 에이전트를 통해 발송할 수도 있지만, 일단 받는 주체가 제한된 불특정 다수이기 때문에 세계적으로 확산되지는 않는다. 또한 메일에 첨부된 파일 역시 트로이목마 형태가 일반적이다. 그래서 과거와 달리 이메일 웜이 세계적으로 확산 되는 현상이 오늘날은 매우 드문 일이 되어 버렸다.

그러나 해외 악성코드 피해 통계에서는 아직까지도 구종의 넷스카이 웜이나 마이둠 웜 등이 상위에 머물러 있곤 한다.

올 1월말에 세계적으로 확산 되어 이슈가 되었던 나이젬 웜(Win32/Nyxem.worm)이 주목을 받은 이후, 이렇다 할 이메일 웜이 없었는데 8월에 이메일로 확산되는 스트레이션 웜이 출현하였다. 이 웜은 짧은 기간에 다수의 변형을 만들어 냈고 국외에 상당수 확산된 것으로 보고되었다. 국내에서는 일부 고객에게서만 보고되었다.

이 웜은 특정 호스트로부터 파일을 다운로드 하고 실행하는데, 초기 분석 시에는 호스트에 업로드된 파일이 계속 업데이트 되기도 하였다. 이 파일은 사용자 정보를 탈취할 수 있는 트로이목마를 생성한다. 스트레이션 웜의 변형이 얼마나 제작되고 확산될 지는 예측하기 어렵지만, 단시간 내에 다수의 변형이 보고 되었고 확산된 수준으로 볼 때 이 웜의 다음 변형도 그러할 것이라고 조심스레 추정 해볼 수 있겠다.

(2) 스파이웨어 – IE 주소 표시줄을 교체하는 애드웨어

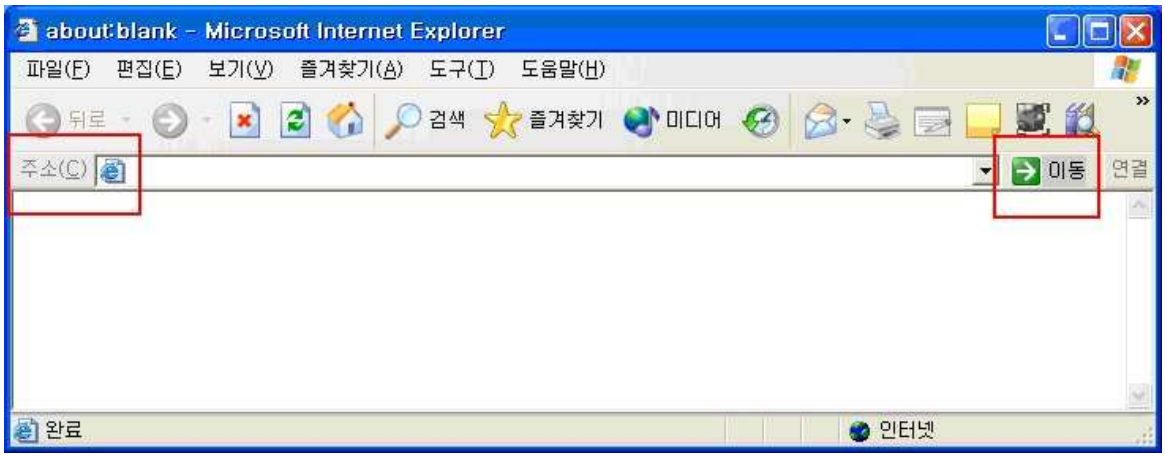
지난 달에 이어 8월에도 온라인 게임 계정을 유출하는 스파이웨어가 많이 발견된 가운데 국내에서는 몇 종의 애드웨어가 새로 발견되었다. 엔프로(Win-Adware/ToolBar.Npro), 와우바(Win-Adware/ToolBar.Wowbar), 더블유네이비(Win-Adware/ToolBar.Wnavy), 캐쉬온(Win-Adware/ToolBar.CashOn)이 8월에 발견된 대표적인 신종 애드웨어로 ActiveX 설치, 주소표시줄 형태의 툴바를 사용한다는 공통점이 있다. 주소 표시줄 형태의 툴바는 복잡한 특허관계가 얽힌 국내 '한글 키워드 서비스' 시장에서 특허를 침해하지 않으면서도 보다 손쉬운 방법으로 주소표시줄 검색 결과를 변경하는 기능을 구현하기 위하여 선택한 대안으로 풀이되며, 광고 수익을 올리기 위한 국내 애드웨어 제작 동향을 보여준다.

윈도우 환경에서의 툴바는 탐색기 또는 브라우저 기능 확장을 위한 도구모음으로 정의할 수 있다. 정상적으로 제작된 툴바는 브라우저의 검색기능을 확장하거나 특정 서비스 또는 어플리케이션의 브라우저와 연동하는 플러그인 등으로 유용하게 사용할 수 있다. 툴바는 BHO에 비하여 구현하는 것이 다소 까다로우나 BHO와 마찬가지로 탐색기 또는 IE 프로세스 내에서 동작하기 때문에 이벤트를 가로채거나 브라우저 사용내역을 감시하는 등의 악의적인 동작이 가능하다. 애드웨어 제작사는 광고링크를 포함하는 단순 도구모음에서 팝업광고 노출, 검색결과 변경 등의 다양한 툴바를 여러 가지 방법으로 배포해 왔다.
최근 국내 애드웨어 제작사들은 IE 주소표시줄을 흉내 낸 가짜 주소표시줄을 설치하는 툴바를 제작 배포하고 있다. 이런 툴바는 대부분 포탈사이트의 커뮤니티와 같은 불특정 웹 사이트에서 ActiveX 방식으로 사용자 동의 없이 설치되며 허위 안티 스파이웨어 프로그램의 번들로 설치하기도 한다.

가짜 주소표시줄을 설치하는 툴바의 공통적인 특징은 다음과 같다.

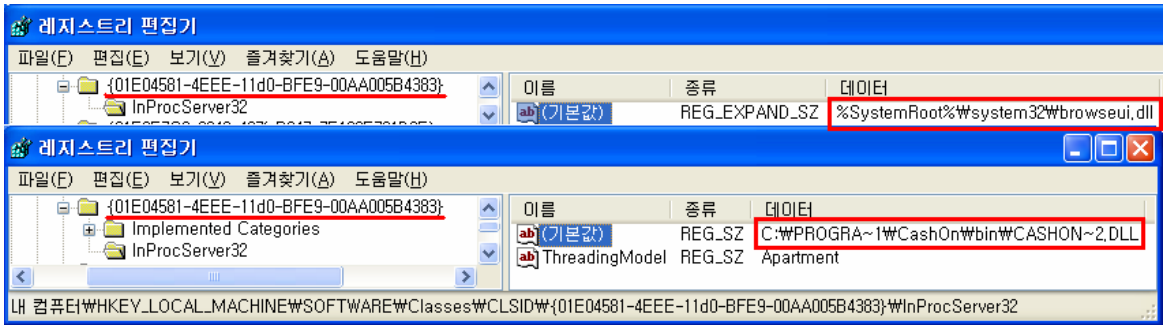
- 주소 표시줄 검색 결과 변경
- 광고를 포함하는 원하지 않는 웹 사이트의 검색결과 표시
- IE 브라우저 사용내역 감시
- IE 브라우저에 입력되는 키워드 감시
- 팝업 광고 노출
- IE 브라우저 성능 저하

[그림1]은 캐쉬온(Win-Adware/ToolBar.CashOn)이 설치된 후의 IE 주소표시줄 화면이다. IE 주소표시줄과 유사하게 제작되었으나 자세히 살펴보면, 툴바 텍스트가 다른 것 – IE 기본 주소표시줄의 텍스트는 '주소(D)'이다. – 과 '이동' 버튼의 색상이 다른 것을 확인할 수 있다. IE 기본 주소표시줄을 숨기거나 교체하기 때문에 자세히 보지 않으면 주소표시줄이 교체된 사실을 인식하기 어렵다.



[그림1] IE 주소표시줄이 변경된 모습

[그림2]는 IE 기본 주소표시줄이 가짜 주소표시줄로 변경된 후의 레지스트리 변화를 보여준다. IE 기본 주소표시줄을 포함하는 모듈인 browseui.dll을 CashOnBand.dll로 교체하였으며, CashOnBand.dll을 삭제하는 경우 IE에는 주소표시줄이 나타나지 않게 된다.



[그림2] IE 주소표시줄 CLSID와 동일한 CLSID를 사용

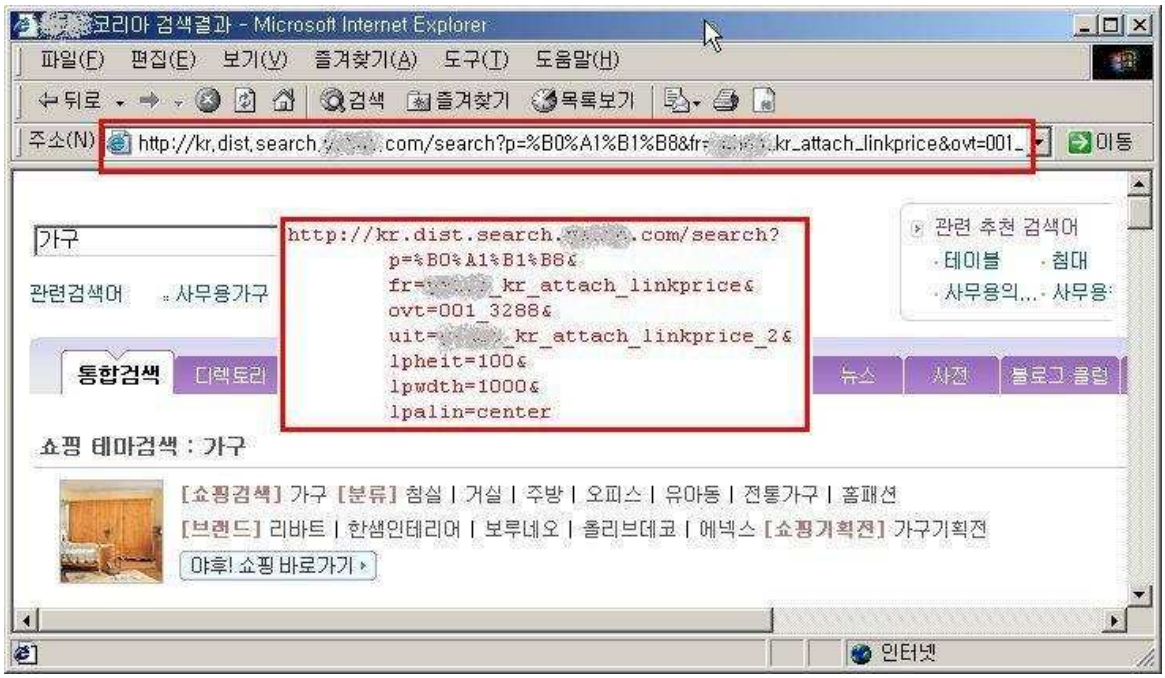
IE 주소표시줄이 보이지 않을 때는 윈도우 기본 IE 주소표시줄을 포함하는 browseui.dll을 등록 시켜 수동으로 주소표시줄을 복구할 수 있다.

```
C:₩WINDOWS₩system32>regsvr32 /i browseui.dll_
```

가짜 주소표시줄을 설치하는 툴바는 광고 목적으로 만들어진다. 주소표시줄에 입력되는 키워드에 대해 검색 결과를 변경함으로써 사용자는 원하지 않는 사이트에서 광고가 포함된 검색 결과를 보게 되며, 제작사는 광고 노출, 클릭 등의 동작이 일어날 때 광고주로부터 일정 금액의 광고료를 지급받는다. 불특정 웹사이트에 ActiveX 방식으로 무분별하게 배포하는 것도 불특정 사용자에게 광고를 많이 보게 하기 위해서이다.

엔프로(Win-Adware/ToolBar.Npro)는 IE 주소표시줄을 가짜 주소표시줄로 변경한 후 사용

자가 입력한 키워드를 이용하여 PPP(Pay Per Performance)[1] 광고를 통해 수익을 얻고 있다.

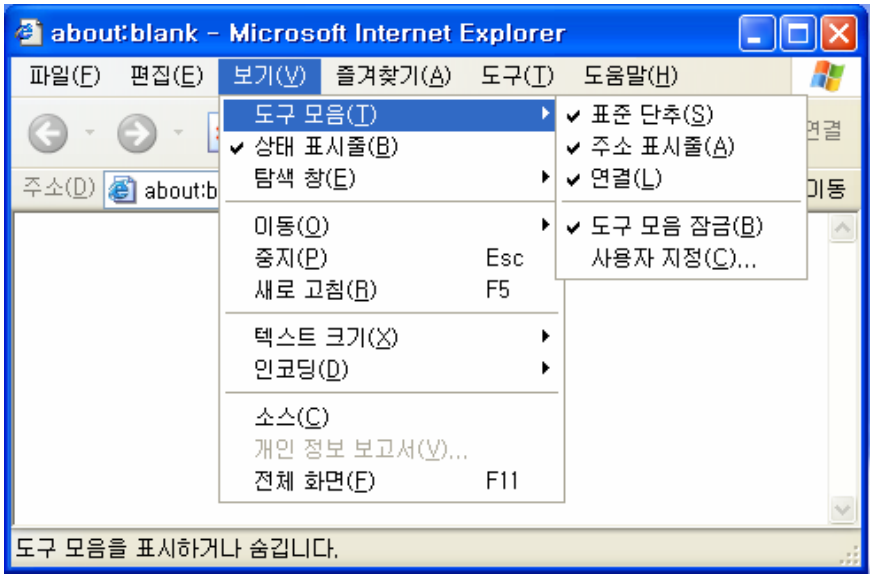


[그림3] 가짜 주소표시줄에 의해 변경된 주소표시줄 검색 결과

[그림3]에서 GET 방식으로 특정 웹 서버로 전송된 데이터에는 광고에 필요한 정보를 담고 있는 것을 확인할 수 있다.

'도구 모음'은 IE 5에서부터 소개되었고, 리바 컨트롤(Rebar Control)[2]에 여러 개의 툴바 컨트롤이 속해 있다. 윈도우에 설치된 툴바 컨트롤은 [IE]→[보기]→[도구 모음]에서 찾아 볼 수 있다.

[1] 광고주가 원하는 행위가 발생했을 때만 비용을 지불하는 방식
[2] 하나의 응용프로그램에서 별도의 뒷 배경을 가지고 하나 이상의 밴드를 포함할 수 있는 컨트롤을 말한다.



[그림4] IE 도구 모음

우선 IE 주소표시줄로 등록되기 위해서는 COM 객체로 작성되어야 하며 아래와 같은 레지스트리 경로에 해당 CLSID를 등록하고 파일 위치정보를 기록하면 자동으로 IE가 DLL을 로드한다.

Ordinal ^	Hint	Function	Entry Point
1 (0x0001)	0 (0x0000)	DllCanUnloadNow	0x000019C0
2 (0x0002)	1 (0x0001)	DllGetClassObject	0x00001A10
3 (0x0003)	2 (0x0002)	DllRegisterServer	0x00001A30
4 (0x0004)	3 (0x0003)	DllUnregisterServer	0x00001AA0

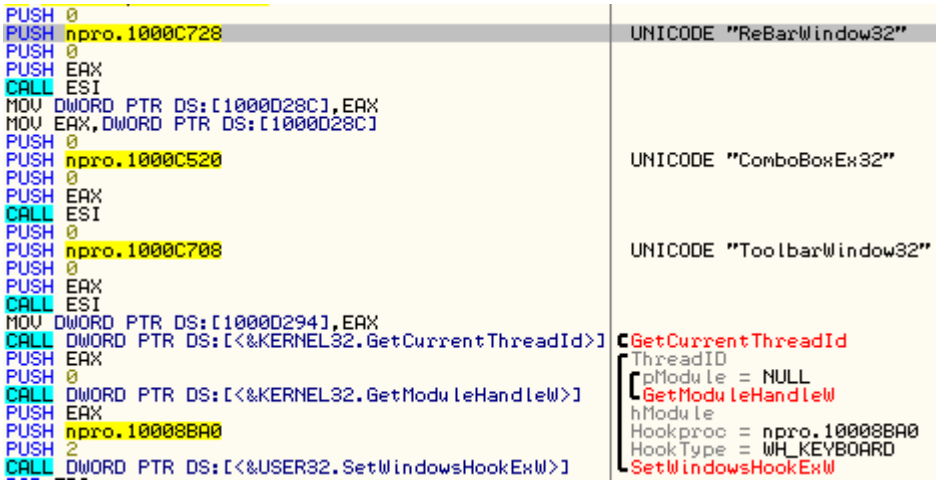
[그림5] COM 객체 외부노출 함수

기본적으로 IE 주소표시줄을 등록하기 위해서는 다음과 같은 레지스트리 경로에 COM 객체로 작성된 Dll을 등록한다.

```
- HKEY_CURRENT_USER
    Software
        Microsoft
            Internet explorer
                Toolbar
                    WebBrowser
                        {Your Band Object's CLSID GUID}

- HKEY_LOCAL_MACHINE
    SOFTWARE
        Classes
            CLSID
                {Your Band Object's CLSID GUID}
                    InprocServer32
                        (Default) = DLL Path Name
```

이런 애드웨어들은 자신이 설치되었다 하더라도 사용자가 해당 IE 표시줄을 사용하지 않고

윈도우 기본 IE 주소표시줄을 사용할 때를 대비하여 윈도우 기본 IE 주소표시줄에 사용자가 입력한 키워드를 가로채는 기능도 포함하고 있다.



[그림6] IE를 후킹하여 사용자가 입력한 키워드 가로체기

위 그림에서 ESI 레지스터에는 “FindWindowW” 함수를 가리킨다. IE 주소표시줄과 관련된 윈도우의 클래스명으로 윈도우를 찾아 키보드를 후킹하여 키워드를 가로채는 부분을 담당하고 있다.

(3) 시큐리티 - 8월의 보안취약점 동향 및 개인정보 유출 사건

이번 호에는 8월에 발표된 마이크로소프트사(이하 MS) 보안 패치들과 서버 서비스 원격 코드 실행 취약점 및 개인정보 유출 사고 등에 대해서 알아보도록 하자.

8월에 발표된 보안 취약점 동향

이번 달에 릴리즈된 MS06-040은 MS에서 보안패치를 공개한지 5일만에 악성코드[1]가 등장한 위협적인 취약점 공격으로 사용자 시스템에 적지 않은 피해를 가져다 준 것으로 분석되고 있다. 보안 취약점을 이용한 악성코드가 증가하고 있으며, 출현주기 또한 상대적으로 단축되고 있어 벤더에서 제공하는 보안패치의 신속한 적용이 시스템 피해를 최소화 할 수 있는 바로미터가 될 수 있겠다. 반면 MS06-042를 적용한 일부 시스템에서 인터넷 익스플로러 충돌문제가 보고되어 수정된 보안패치가 뒤늦게 재 배포 되는 해프닝이 있었다. 안전한 보안환경을 약속하는 보안패치의 신속 적용을 벤더들은 항상 강조하지만, 시스템 충돌을 야기하는 패치마저 함께 적용해야 하는지 사용자들을 잠시 고민에 빠지게 만든 8월로 기억될 것 같다.

위험 등급	취약점	개념 증명 코드
긴급	**MS06-040 서버 서비스의 취약점으로 인한 원격 코드 실행 문제점(921883)[2]** 클라이언트로부터 수신되는 서버 서비스를 처리하는 과정에서 검사되지 않은 버퍼로 인해 발생하는 오버플로우 취약점이며, 공격자는 SMB 연결 서비스를 통해 관리자 권한을 획득할 수 있다. 윈도우 2000 시스템은 취약점 공격을 받게 되면 60초 카운트 이후 재부팅이 발생하는 특징을 가지고 있다.	유
긴급	**MS06-042 인터넷 익스플로러 누적 보안 업데이트(918899)[3]** IE에서 발생하는 8가지 취약점을 위한 누적 보안패치인데, 패치를 적용한 일부 시스템에서 충돌현상이 보고되어 MS는 8월 29일 패치를 수정하여 다시 배포 하였다. 윈도우 2000 SP4 또는 윈도우 XP SP1기반에서 IE 6.0 SP1을 사용중인 시스템은 수정된 패치를 다시 적용해야 하는 수고가 필요하다.	무
긴급	**MS06-051 윈도우 커널의 취약점으로 인한 원격코드 실행 문제점(917422)[4]** Winlogon 프로세스가 활성화 될 때 동적 라이브러리의 로딩이 시스템 디렉토리보다 UserProfile 디렉토리가 우선하게 되는 결함으로, 조작된 DLL이 UserProfile 디렉토리에 위치할 때 관리자 권한을 획득할 수 있다.	무

[1] AhnLab, 워그 봇(Win32/WargBot.worm.9374)
(http://info.ahnlab.com/smart2u/virus_detail_4877.html)
[2] http://www.microsoft.com/korea/technet/security/bulletin/ms06-040.mspx
[3] http://www.microsoft.com/korea/technet/security/bulletin/ms06-042.mspx
[4] http://www.microsoft.com/korea/technet/security/bulletin/ms06-051.mspx

특정 응용프로그램에 국한되지 않고 수많은 범용OS에 타격을 입힐 수 있는 보안취약점은 악성코드 제작자들에게 대단히 매력적일 수 밖에 없어, 이를 응용한 악성코드는 수일 내에 어김없이 발견되곤 한다. 온갖 악성코드가 난무하는 외부 위협으로부터 안전을 보장받기 위해 방화벽, IDS, 백신 등의 많은 보안제품을 설치하는 것도 중요하지만, 각 벤더들에서 제공하는 보안패치를 성실히 적용하여 근본적인 원인을 제거해 주는 것이 내 시스템을 보호하는 가장 최선이자 최상의 방법이라 할 수 있겠다.

서버 서비스의 취약점(MS06-040)을 이용한 악성코드 위협

지난 5월과 6월 MS 오피스 프로그램을 대상으로 하는 제로데이 취약점이 기억에서 잊혀지기도 전에 이에 버금가는 악성코드가 출현하였다. 특히 윈도우 NT계열 시스템간의 통신 매개체로 사용되는 RPC[1] 프로토콜 취약점을 악용하므로 거의 모든 윈도우 시스템이 공격대상에 포함되는 매우 위협적인 취약점이라 할 수 있다.

서버 서비스는 파일, 폴더 및 주변장치 등의 공유를 지원하는 기능으로 services.exe를 통해 윈도우 시스템에서 기본 서비스로 동작한다. 클라이언트로부터 조작된 RPC 요청이 수신되면 서버는 services.exe의 구성요소인 netapi32.dll의 NetplsRemote() 함수 내에 NetpwPathCanonicalize를 호출하는데, 여기서 검사되지 않은 버퍼로 인해 스택 오버플로우가 발생하는 취약점이 있다. 현재까지 발견된 서버 서비스의 취약점(MS06-040) 공격에 따른 운영체제 별 영향은 다음과 같다.

서버 서비스의 취약점(MS06-040) 공격에 따른 영향

	재부팅	원격코드실행	서비스거부
윈도우 2000 SP4	O	O	O
윈도우 XP SP1	X	O	O
윈도우 XP SP2	X	X	O
윈도우 서버 2003 GOLD	X	X	O
윈도우 서버 2003 SP1	X	X	O

MS06-040 취약점 정보는 'III. MS06-040 취약점을 이용한 보안위협' 꼭지에서 보다 상세히 다루기로 하자.

캐빈 미트닉의 웹사이트 해킹사고

보안 컨설팅 회사를 운영중인 전설적인 해커 캐빈 미트닉의 웹사이트가 외부 침입에 의해 시작화면이 악의적인 문구로 변경되는 해킹을 당했다. 피해 당사자인 미트닉은 자신의 웹사이트를 호스팅하는 업체가 해킹을 당한 것이며, 내부에는 중요한 정보를 보관하고 있지 않기

[1] Remote Procedure Call : 네트워크 상의 다른 시스템에 서비스를 요청하는데 사용되는 프로토콜로서, 요청하는 프로그램이 클라이언트가 되고 서비스를 제공하는 프로그램이 서버가 되는 클라이언트/서버 모델을 사용한다.

때문에 심각한 피해는 없었다고 밝히며, 이번 사고에 대해 큰 의미는 두지 않는 모습을 보였다.

국내 결혼정보 회사 해킹한 피의자 검거

국내 결혼정보 회사를 해킹하여 회원정보를 취득하고, 회사 보안담당자에게 금품을 요구한 피의자가 경찰에 의해 검거되었는데, 피의자는 중국에서 유포된 SQL 인젝션(Injection) 자동화 툴을 사용하여 피해업체의 웹서버를 해킹한 단순 스크립트 키드[1]에 불과하였다. 이는 온라인에서 구한 해킹툴을 이용해서 손쉽게 침입 당하는 국내 웹사이트 보안의 현 주소를 단적으로 보여주는 사례라 하겠다.

위에서 언급한 사고는 80포트(HTTP)를 통한 웹해킹 중 SQL 인젝션 공격코드를 사용하였다. 이는 보안취약점과는 무관한 나쁜 프로그래밍 코드가 주 원인인데, 클라이언트로부터 입력된 값을 서버에서 제대로 검사하지 않기 때문에 발생한다. 웹 상에서 검사되지 않고 넘어온 입력값은 SQL Query문자열로 조합되고, 단순 조합된 Query문이 관리자 권한으로 실행될 경우 공격자는 웹서버를 장악하게 된다. SQL 인젝션이 발생하는 원인과 해결책을 정리하면 아래와 같다.

[요인1] 클라이언트로부터 입력되는 값을 검사과정 없이 그대로 사용한다.

- 입력 값이 숫자일 경우 IsNumeric() 함수 등을 통해 유효성을 검증한다
- 입력 값이 문자일 경우 특수문자는 정규표현식을 통해 검증하거나 치환한다
- 데이터베이스 쿼리에 민감한 키워드(EXEC XP_, EXEC_SP_, UNION SELECT...)를 검사한다

[요인2] 수신받은 입력값을 SQL Query문자열과 단순 조합하여 명령어로 사용한다.

- Query 빌드는 매개변수 Query를 사용하는 저장 프로시저로 구현한다

[요인3] Query가 SA 계정으로 실행되거나, 확장저장 프로시저로 시스템 명령의 전송이 가능하다.

- SA 계정을 삭제하거나 제거한다
- 시스템 명령이 가능한 확장 프로시저(xp_cmdshell, xp_regred, sp_adduser...)를 제거한다
- 권한을 최소화한 제한된 계정을 생성하여 데이터베이스 연결을 한다

보안성을 무시한 채 화려한 겉 포장만을 중시한 웹사이트는 사상누각과도 같아서 해커들의 아주 좋은 먹이감이 되고 만다. 자신이 운영중인 웹사이트는 웹해킹 공격에 안전한지 미리미리 점검하여 해킹사고의 또 다른 피해자가 되지 않도록 하는 것이 필요하겠다.

[1] 스크립트 키즈(Script Kiddies)
: 전문적인 지식없이 온라인상에서 해킹 툴을 찾아 악용하는 초보 공격자

III. MS06-040 취약점을 이용한 보안위협

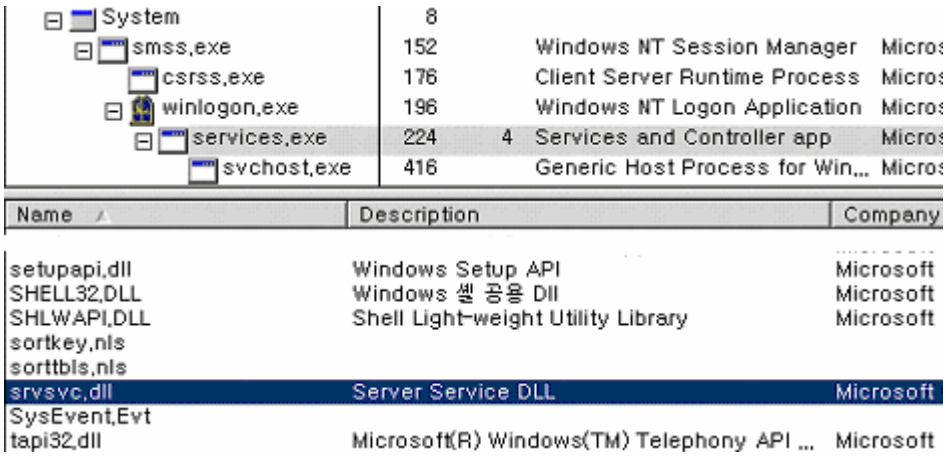
작성자: 이정형 주임연구원

마이크로소프트(이하 MS)사에서 발표한 8월 정기 보안패치에는 2006년에 발표된 취약점 중에서 가장 위협적인 서버 서비스의 취약점으로 인한 원격 코드 실행 문제점(MS06-040)에 대한 패치가 포함되어 있다. MS06-040은 작년에 많은 문제를 만든 PNP 취약점(MS05-039)과 예전에 많은 문제점을 일으켰던 LSASS 취약점(MS04-011), DCOM 취약점(MS03-026, MS03-029)에 필적하는 것이다.

MS06-040 취약점을 이용한 웜(워그 봇, IRCBot 변형)들이 최근 국내에 급속도로 확산되고 있으며, 윈도우 2000, 윈도우 XP, 윈도우 2003 이 MS06-040 취약점에 영향을 받는다.
이번 꼭지에서는 MS06-040에 대한 취약점 분석과 악성코드 위협, 이에 대한 대응책에 대해서 다루어 보기로 한다.

MS06-040 취약점 분석

서버 서비스는 RPC 지원, 네트워크를 통한 파일 인쇄 지원 및 명명된 파이프 공유를 제공하는 서비스로, services.exe 에서 관리를 하며 윈도우 시스템에서 기본 서비스로 동작을 하기 때문에 이번 MS06-040 취약점은 매우 위험하다. [그림1]은 서버 서비스 DLL 인 srvsvc.dll 이 services.exe 에서 동작을 하는 모습을 보여준다.



[그림1] srvsvc.dll 이 services.exe 에서 동작하는 모습

MS06-040 취약점은 원격에서 코드를 실행할 수 있는 취약점이 존재하는 것으로, 공격자는 관리자 권한을 획득할 수 있으며 프로그램의 설치, 보기, 변경, 데이터 삭제 등 해당 시스템을 완전히 제어할 수 있게 된다. 또한 이 취약점을 통해 해당 시스템들은 services.exe 등의 60초 카운트에 해당하는 서비스 거부가 발생할 수도 있다. 다만, 시스템 서비스들이 스택 보

호(Stack Guard) 옵션인 /GS로 컴파일 및 DEP 기능을 제공하는 윈도우 XP SP2와 윈도우 2003 SP1 에서는 실제 익스플로잇(Exploit)은 되지 않으며, 서비스 거부가 발생할 수 있다.

MS06-040 취약점이 무엇 때문에 발생을 하는지에 대해서 알아보자. 서버 서비스 DLL 인 srvsvc.dll 이 imports 하는 Net Win32 DLL 인 netapi32.dll 의 함수들은 아래와 같다.

```
750F28B1 5D NetApiBufferAllocate
750F181C A5 NetRegisterDomainNameChangeNotification
750F4F63 130 NetpwPathType
750F97D2 4D I_NetPathType
751094C3 12F NetpwPathCompare
750F8846 12D NetpwNameValidate
750F4EE9 12E NetpwPathCanonicalize
7510473C 9F NetMessageBufferSend
75106091 10F NetpLocalTimeZoneOffset
750F4B37 103 NetpGetComputerName
750F1DD5 10A NetpGetPrivilege
750F1F18 122 NetpReleasePrivilege
75105504 D8 NetUnregisterDomainNameChangeNotification
750F2C00 11A NetpNtStatusToApiStatus
75105E5A 102 NetpDeleteSecurityObject
75103F4D FF NetpCreateSecurityObject
750F2C97 F4 NetpAccessCheckAndAudit
750F8A45 12C NetpwNameCompare
750FA024 12 DsGetSiteNameW
750F2896 5E NetApiBufferFree
750F8732 12B NetpwNameCanonicalize
```

MS06-040 취약점은 srvsvc.dll이 imports하는 netapi32.dll의 NetpwPathCanonicalize 함수 등에 내부의 검사되지 않은 버퍼로 인하여 경로(Path) 처리 부분에서 버퍼 오버플로우가 발생하게 되는 것이다. 실제적으로 버퍼 오버플로우가 발생하는 부분은 netapi32.dll 에 존재하는 NetpIsRemote 함수 및 CanonicalizePathName 함수 등에서 해당 코드가 존재한다.

NetpIsRemote 함수와 CanonicalizePathName 함수는 wcscpy/wcscat을 사용할 때 변수의 크기를 사용하지 않거나, 변수를 잘못 처리함으로 인하여 버퍼 오버플로우가 발생한다. 인터넷 상에 공개된 익스플로잇은 NetpwPathCanonicalize 함수에서 호출하는 Canonicalize PathName 함수의 취약점을 이용하는 것이다. [그림2]와 [그림3]은 NetpIsRemote 함수(I_NetNameCanonicalize 함수에서 호출)와 CanonicalizePathName 함수의 코드들을 보여준

다.

```
.text:71B7BF10 loc_71B7BF10:                           ; CODE XREF: NetpIsRemote(x,x,x,x)+A130Tj
.text:71B7BF10                 mov     ecx, [ebp+arg_4]
.text:71B7BF13                 neg     eax
.text:71B7BF15                 sbb     eax, eax
.text:71B7BF17                 cmp     [ebp+arg_8], edi
.text:71B7BF1A                 mov     [ecx], eax
.text:71B7BF1C                 jz      short loc_71B7BF39
.text:71B7BF1E                 push    offset asc_71BA9C2C ; "\\\\\\"
.text:71B7BF23                 push    [ebp+arg_8]     ; wchar_t *
.text:71B7BF26                 call    ds:__imp__wcscpy
.text:71B7BF2C                 push    ebx             ; wchar_t *
.text:71B7BF2D                 push    [ebp+arg_8]     ; wchar_t *
.text:71B7BF30                 call    ds:__imp__wcscat
.text:71B7BF36                 add     esp, 10h
```

[그림2]NetpIsRemote 함수

```
.text:71B72BDB ; int __fastcall CanonicalizePathName(int,int,wchar_t *,wchar_t *,wchar_t *,int,int
.text:71B72BDB _CanonicalizePathName@20 proc near      ; CODE XREF: NetpwPathCanonicalize(x,x,x,x,
.text:71B72BDB
.text:71B72BDB var_416         = word ptr -416h
.text:71B72BDB var_414         = word ptr -414h
.text:71B72BDB arg_0           = dword ptr  8
.text:71B72BDB arg_4           = dword ptr  0Ch
.text:71B72BDB arg_8           = dword ptr  10h
.text:71B72BDB arg_C           = dword ptr  14h
.text:71B72BDB arg_10          = dword ptr  18h
.text:71B72BDB
.text:71B72BDB ; FUNCTION CHUNK AT .text:71B7C680 SIZE 0000008F BYTES
.text:71B72BDB
.text:71B72BDB                 push    ebp
.text:71B72BDC                 mov     ebp, esp
.text:71B72BDE                 sub     esp, 414h       ; wchar_t *
.text:71B72BE4                 push    ebx
.text:71B72BE5                 mov     ebx, ds:__imp__wcscat
.text:71B72BEB                 push    esi             ; wchar_t *
.text:71B72BEC                 xor     esi, esi
.text:71B72BEE                 cmp     [ebp+arg_0], esi
.text:71B72BF1                 push    edi
.text:71B72BF2                 mov     edi, ds:__imp__wcslen
.text:71B72BF8                 jnz     loc_71B7C680
.text:71B72BFE                 mov     [ebp+var_414], si
```

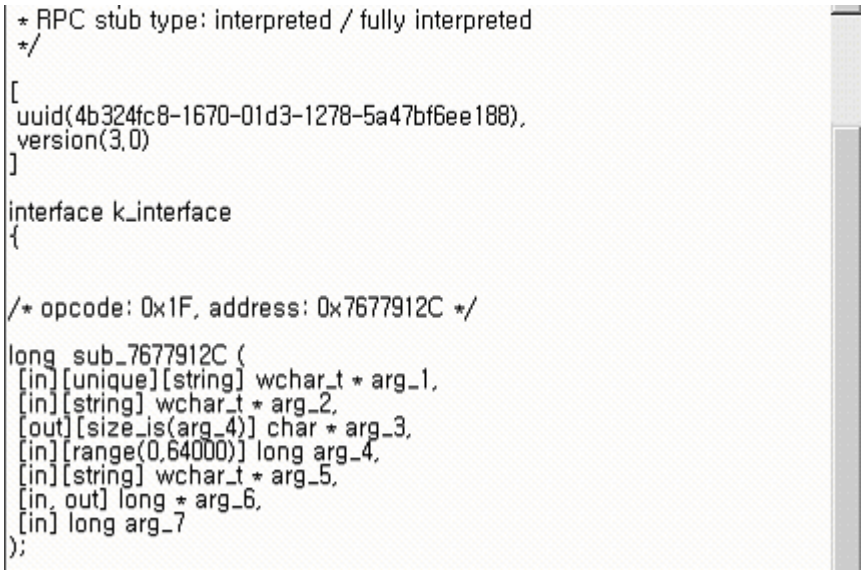
[그림3] CanonicalizePathname 함수

서버 서비스(srvsvc.dll)에서 제공하는 RPC Call 중에서 취약점을 가지고 있는 Call은 NetprPathCanonicalize 등이다. Srvsvc.dll의 관련 Interface 및 OPcode 는 [표1]과 같다.

Interface (srvsvc)	Operation number	Operation name
4b324fc8-1670-01d3-1278-5a47bf6ee188 v3.0	0x1f	NetprPathCanonicalize

[표1] Srvsvc.dll 의 관련 Interface 및 OPcode

또한 NetprPathCanonicalize 콜의 IDL(Interface Description Language)은 [그림4]와 같다.



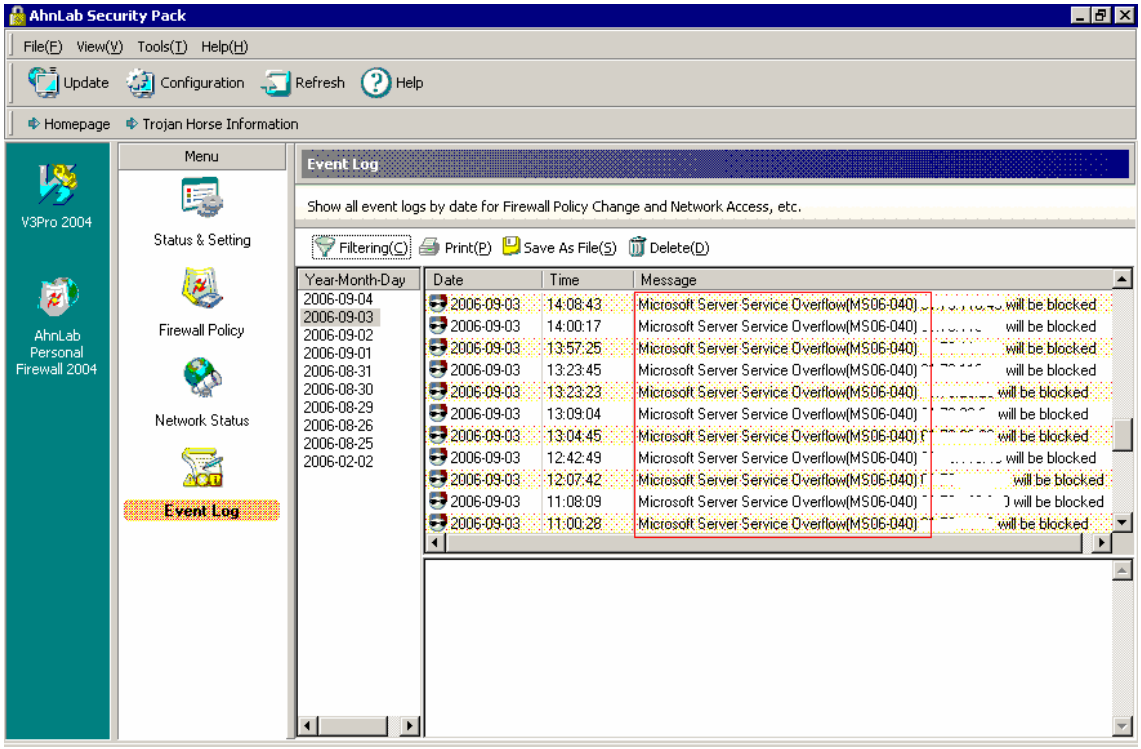
```
 * RPC stub type: interpreted / fully interpreted
 */

[
 uuid(4b324fc8-1670-01d3-1278-5a47bf6ee188),
 version(3.0)
]

interface k_interface
{


/* opcode: 0x1F, address: 0x7677912C */

long  sub_7677912C (
 [in][unique][string] wchar_t * arg_1,
 [in][string] wchar_t * arg_2,
 [out][size_is(arg_4)] char * arg_3,
 [in][range(0,64000)] long arg_4,
 [in][string] wchar_t * arg_5,
 [in, out] long * arg_6,
 [in] long arg_7
);
```

[그림4] NetprPathCanonicalize 콜의 IDL

MS06-040을 이용한 웜 전파

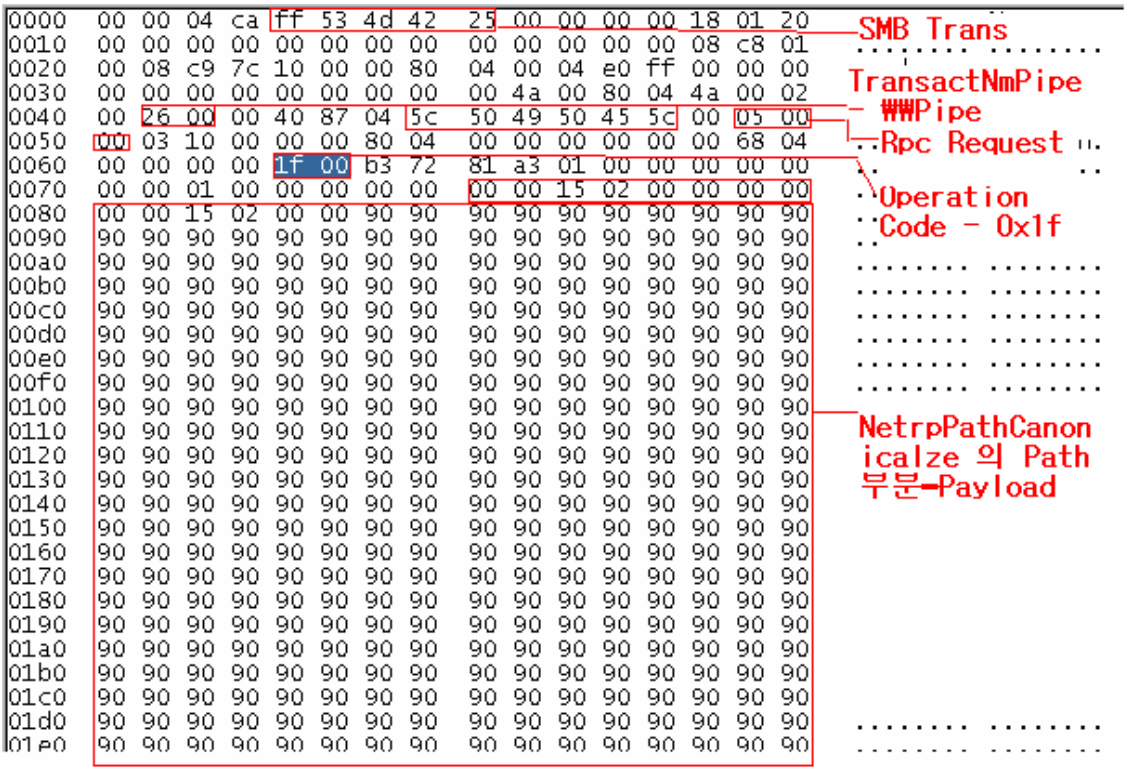
MS06-040에 대한 패치가 8월 9일 발표된 이후, 8월 10일 MS06-040을 이용한 공격코드가 발견되었으며, 이를 이용한 악성코드인 워그봇(Win32/WargBot.worm) 감염이 국내에서 처음 발견된 것은 8월 13일이었다. 그 후 점차 MS06-040을 이용하는 IRCBot 웜변형들이 발견되면서 8월 넷째주 부터는 급속도로 확산되기 시작하여 많은 피해가 발생하게 되었다. 피해 영향으로는 services.exe 60초 카운트 시스템 리부팅 및 웜 감염을 통한 다른 PC 공격, 그리고 기업 사용자들은 내부 네트워크 망이 급격히 느려지는 현상이 발생한다. 또한 이러한 웜들은 특정 IRC 서버에 접속하여 오퍼레이터의 명령을 받아 실행되거나 명령 없이 직접적으로 특정 포트를 통해서 해당 취약점으로 공격하는 방식을 이용한다.

[그림5]는 안철수연구소에서 운영중인 허니팟(Honeypot)을 통해서 TCP 445 포트를 통해 유입되고 있는 현재 국내에 확산중인 MS06-040 관련 웜의 차단정보를 보여주고 있다.



[그림5] AhnLab Personal Firewall 2004에서 MS06-040 관련 공격을 차단한 화면

MS06-040을 이용하여 전파되는 웜들은 CanonicalizePathName 함수의 취약점을 이용하는 패킷을 전송하여 해당 컴퓨터들을 감염시킨다. [그림6]은 해당 패킷의 일부분이다.



[그림6] MS06-040 공격 패킷의 일부분

MS06-40 대처방법

가장 좋은 해결책은 MS에서 제공하는 MS06-040 패치를 적용하여 해당 취약점을 제거하는 것이다. 운영체제 별로 해당하는 패치파일을 다운로드하여 설치하면 된다.

기업 사용자들은 방화벽 등에서 TCP 139 포트와 TCP 445포트를 차단함으로써 네트워크 상에서 웜의 유입을 방지할 수 있으며, 만약 웜에 의해 기업 네트워크에 문제가 생기면 게이트웨이 단에 존재하는 네트워크 보안 제품을 이용하여 웜이 발생하는 PC를 찾아 조치를 취해야만 한다. 보안 패치 방법과 더불어 백신 업데이트 및 개인용 방화벽 등을 사용하는 것 또한 필요하다. 끝으로 개인 사용자들은 윈도우의 다른 버전 보다 안전한 윈도우 XP SP2의 권장한다.

IV. ASEC이 돌아본 추억의 악성코드

혼란의 시작 – 카오스4 바이러스

1994년 7월 24일 alt.binaries.pictures.erotica 뉴스그룹에 한 파일이 업로드 되었다. 많은 사람들이 에로틱한 파일로 생각해 파일을 다운로드 받고 실행했다. 하지만, 뉴스그룹에 올려진 파일은 신종 카오스4 바이러스(Kaos4)[1]에 감염되어 있었다. 감염된 파일을 실행하면 현재 폴더와 경로로 지정된 실행 파일을 감염시키는 단순한 바이러스였다. 감염 능력이 떨어지는 비상주형 바이러스는 보통 특정 지역에서 잠깐 보고되고 사라지는데 인터넷 뉴스그룹을 통해 배포된 이 바이러스는 전 세계로 퍼졌고 8월에 국내에도 발견되었다.

1994년은 전 세계적으로 서서히 인터넷 붐이 불기 시작했고 웹 서비스가 아직 지금처럼 보편화되기 전으로 뉴스그룹이나 고퍼(gopher)가 주로 이용되었다. 보통 당시 도스 바이러스는 PC 통신이나 불법 복제로 전파되는 경우가 대부분이었다. 하지만, PC 통신은 특정 국가나 특정 지역에서 이용되는 경우가 대부분이라 바이러스가 널리 퍼지는 데는 한계가 있었다. 이에 전 세계 사람들이 사용하는 인터넷 서비스를 통한 바이러스를 배포는 기존 방법보다 진일보한 전파방법이었다.

악성코드 제작자들은 인터넷을 이용한 악성코드 전파를 시도했고 1996년에 안락사 바이러스(Euthanasia)[2]도 뉴스 그룹으로 배포되었고 1999년 1월에는 뉴스 그룹에 자신을 스스로 업로드하는 Happy99 웜[3]도 발견되었다. 뉴스그룹을 통해 전파되는 방법은 웹 서비스 가 대중화되어 뉴스 그룹 사용자가 줄어들고 메일로 전파되는 방법이나 취약점을 이용하는 방법이 더 쉽게 악성코드를 빨리 배포할 수 있어 현재는 거의 사라진 상태이다. 1980년대에도 대형 컴퓨터에서 활동하는 웜이 인터넷을 통해 전파된 경우가 있었지만, 1988년 이후 현대적 바이러스에서 개인 및 기업 사용자를 목표로 제작된 바이러스 중에는 카오스4 바이러스가 인터넷을 통한 첫 배포 사례로, 이는 현재와 같은 혼란의 시작이라고 볼 수 있다.

[1] AhnLab, Kaos4 (http://info.ahnlab.com/smart2u/virus_detail_5054.html)
[2] AhnLab, Euthanasia (http://info.ahnlab.com/smart2u/virus_detail_349.html)
[3] AhnLab, I-Worm/Happy99 (http://info.ahnlab.com/smart2u/virus_detail_387.html)