ASEC Report 1월

® ASEC Report

2006. 2

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.

I. 1월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자: 이재호 연구원(explod@ahnlab.com)

순위		악성코드명	건수	%
1	↑1	Win32/Netsky.worm.Gen	182	19.9%
2	↑3	Win32/Parite	42	4.6%
3	new	Win32/IRCBot.worm.Unknown	25	2.7%
4	↓1	Win32/Maslan.C	25	2.7%
5	↑3	Win32/Sasser.worm.15872	22	2.4%
6	new	Win32/LovGate.worm.143360	16	1.8%
7	new	Win32/LovGate.worm.Gen	11	1.2%
8	new	Win32/Mytob.worm.49281	11	1.2%
9	↓8	Win32/Sober.worm.55390	10	1.1%
10	new	Win-Trojan/Xema.67104	9	1.0%
		기타	561	61.4%
합계			914	

[표1] 2006년 1월 악성코드 피해 Top 10

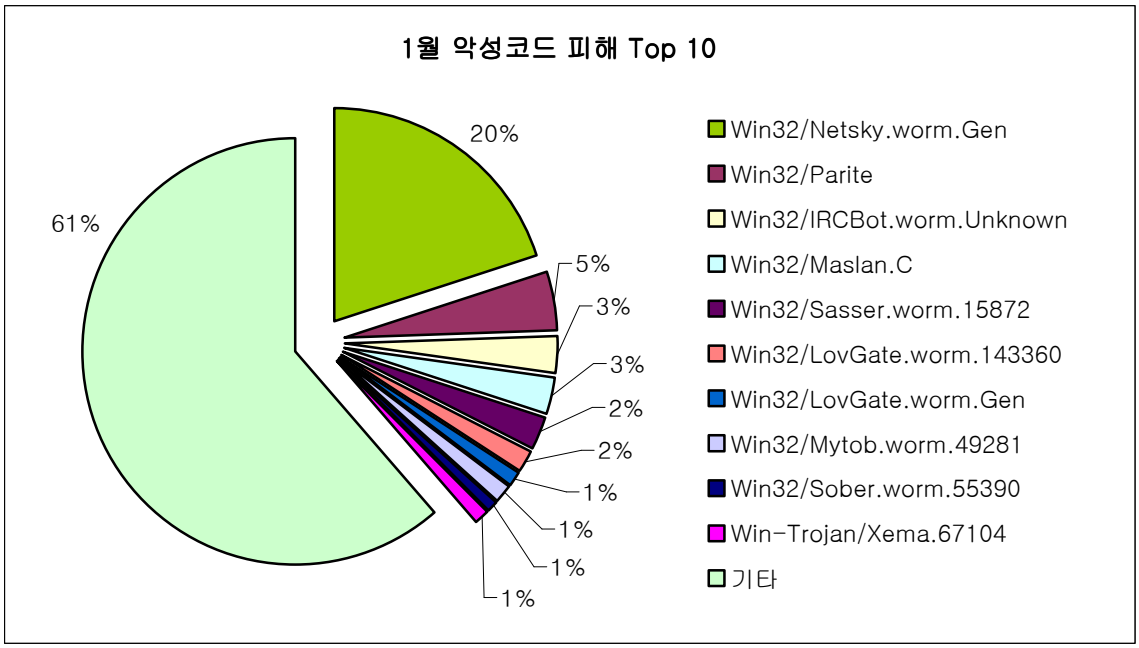
1월 악성코드 피해 동향

지난해부터 악성코드 피해신고가 지속적으로 감소하더니 급기야 2006년 1월 악성코드 피해 건수는 1,000건 미만인 914건을 기록하였다.

2006년 1월 악성코드 피해 Top 10을 살펴보면, 2005년 12월 1위를 차지하였던 소버.55390 웜(Win32/Sober.worm.55390)은 8계단이나 내려온 9위가 되었으나, 넷스카이 웜(Win32/Netsky.worm.Gen), 패리테(Win32/Parite), 마슬란.C(Win32/Maslan.C)는 여전히 상위권을 차지하고 있다. 또한 아이알씨봇 웜(Win32/IRCBot.worm.Unknown), 러브게이트 웜(Win32/LovGate.worm.143360, Win32/LovGate.worm.Gen), 마이톱.49281 웜(Win32/Mytob.worm.49281), 제마.67104 트로이목마(Win-Trojan/Xema.67104)는 악성코드 피해 Top 10에 새로이 진입하였다.

또한 자료에 나와있지는 않지만, 1월에는 특정 웹 사이트에서 악성코드를 유포하는 신고가 15건이나 발생하였다. 이는 이러한 방식의 악성코드 유포가 점차 증가하고 있으며, 앞으로도 한동안 계속 증가할 것임을 보여주고 있는 것이다.

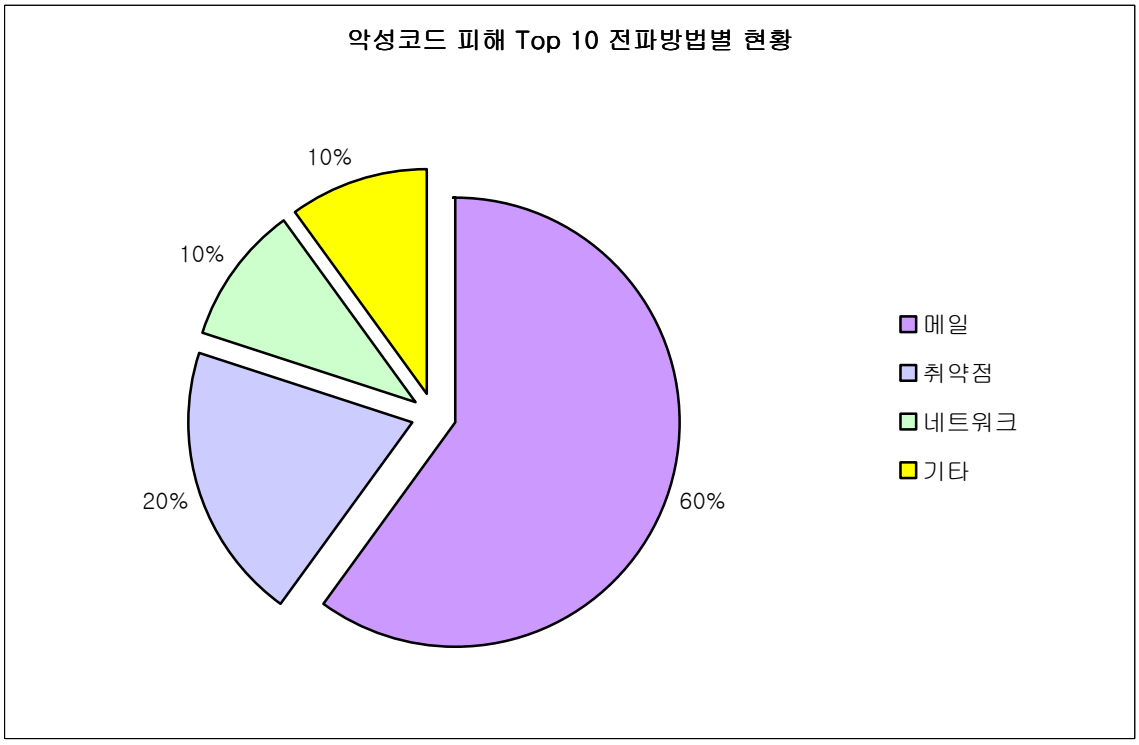
1월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.



[그림1] 2006년 1월 악성코드 피해 Top 10

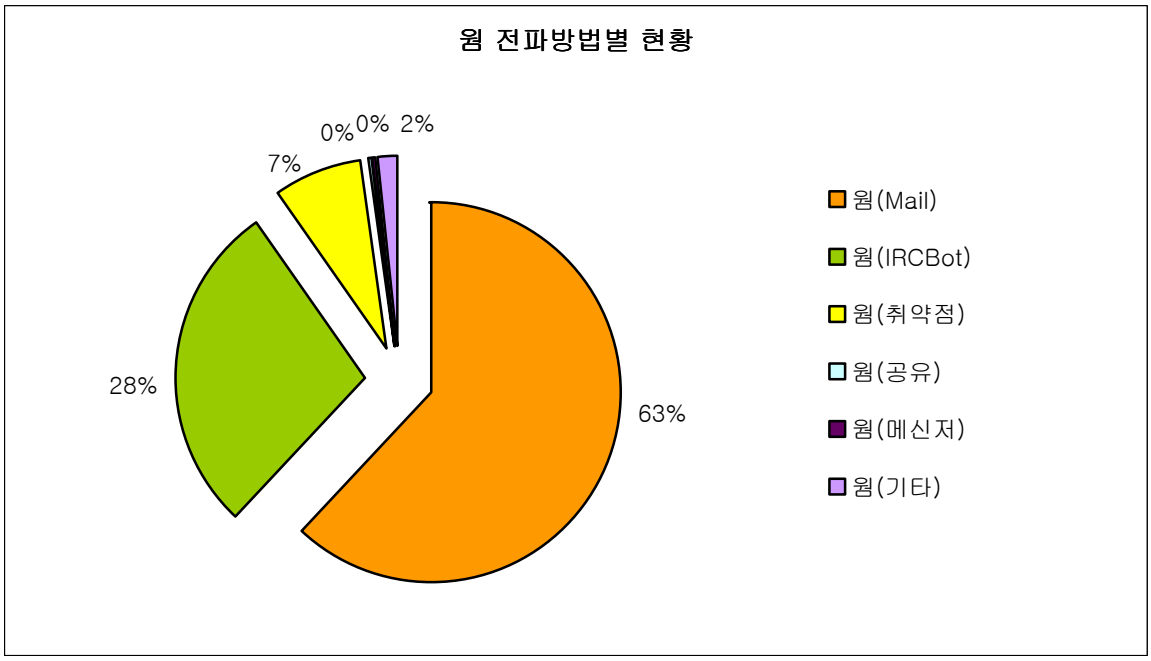
1월 악성코드 Top 10 전파방법별 현황

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



[그림2] 2006년 1월 악성코드 Top 10의 전파방법별 현황

매스메일러인 소버 웜과 넷스카이 웜은 감소 추세를 보이고 있으나, 또 다른 매스메일러인 러브게이트 웜이 새로이 출현하면서 지난달과 마찬가지로 Top 10에 랭크 된 악성코드의 60%가 메일을 이용하여 전파되고 있는 것으로 나타났다. 취약점을 이용한 전파방법은 전월에 비해 10% 증가한 20%를 차지하고 있다.



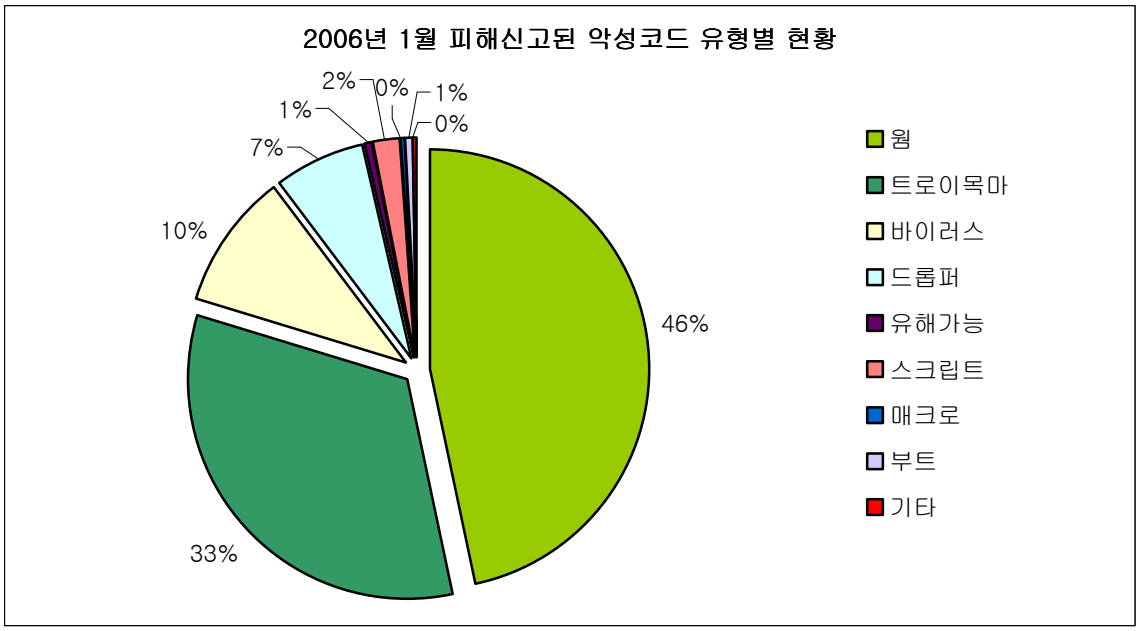
[그림3] 2006년 1월 웜의 전파방법별 현황

[그림3]은 1월에 피해 신고된 웜의 전파방법에 대한 현황이다.
이메일을 통해 전파되는 웜은 2005년 11월을 기점으로 10%씩 감소하기 시작하여 63%에 이르렀으며, 아이알씨봇 웜은 7% 증가하여 28%가 되었다. 이메일을 통해 전파되는 웜의 종류가 31개에서 23개로 감소하면서 메일을 통해 전파되는 웜이 감소하게 된 것으로 추정된다.

피해신고 된 악성코드 유형 현황

1월에는 전월에 비해 웜이 5% 가량 감소하여 46%를 차지한 반면, 드롭퍼, 트로이목마는 2, 3%씩 각각 증가하여 드롭퍼 7%, 트로이목마 33%를 차지하고 있다. 그리고 꾸준히 감소하고 있는 바이러스도 10%를 차지하고 있다.

악성코드 유형별 현황은 [그림4]와 같다.

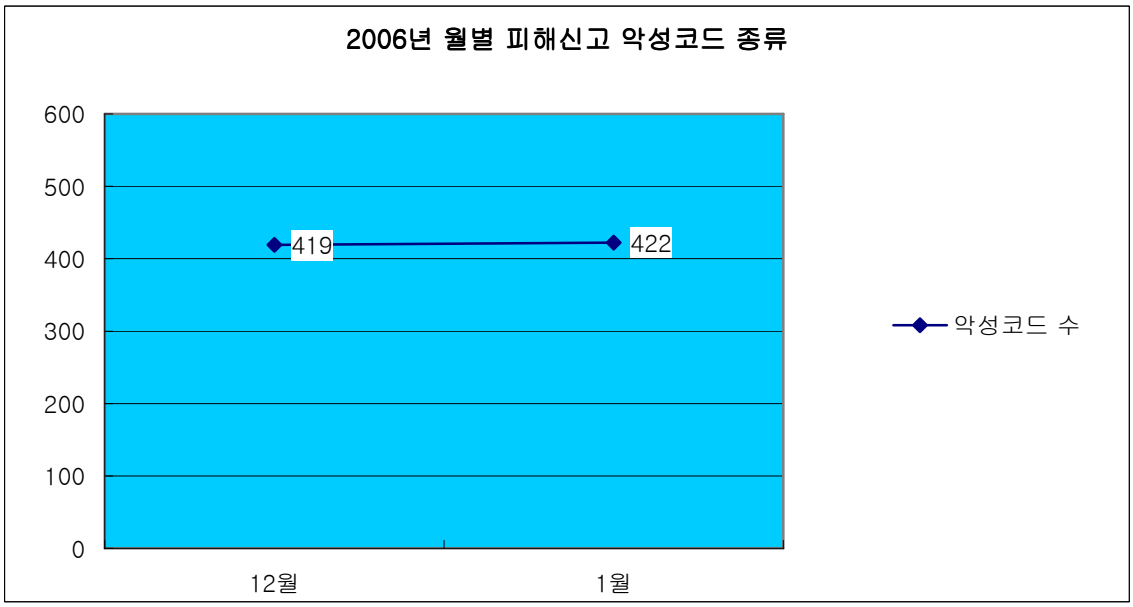


[그림4] 2006년 1월 피해 신고된 악성코드 유형별 현황

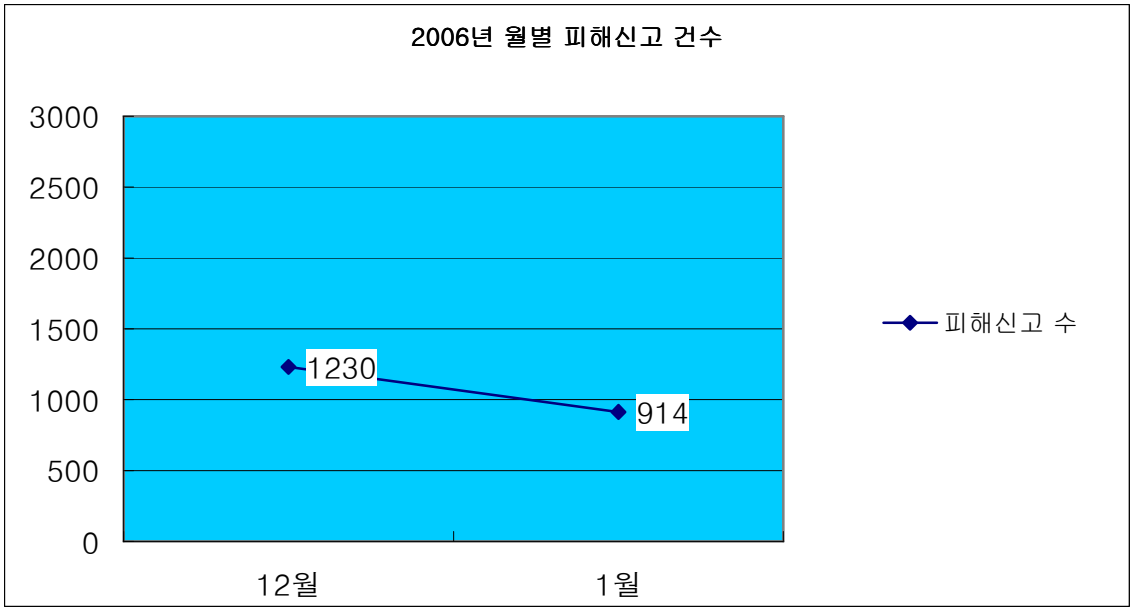
월별 피해신고 된 악성코드 종류 현황

1월에 피해 신고된 악성코드 진단명은 422개로, 지난 12월에 비해 3개 증가하였다.

피해 신고된 악성코드 진단명 중 웜은 다소 감소한 반면, 트로이목마와 드롭퍼는 각각 증가하여 전월과 비슷한 수치를 나타내었다.



[그림5] 2006년 월별 피해신고 악성코드 종류



[그림6] 2006년 월별 피해신고 건수

2005년도 악성코드 피해건수는 전반적으로 감소 추세를 보였다. 그리고 2006년 1월은 914건으로 최저의 악성코드 피해신고 수치를 보이고 있다. 이처럼 피해신고 악성코드 진단명 수는 전월과 비슷한데 반해 피해신고 건수가 급감한 것은 하나의 악성코드가 입히는 피해가 소수에 불과했다는 것을 보여주는 것이다.

(2) 신종(변형) 악성코드 발견 동향

작성자: 정진성 주임연구원 (jsjung@ahnlab.com)

1월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1], [그림1]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
61	144	44	1	2	0	0	0	6	0	258

[표1] 2006년 1월 유형별 신종 (변형) 악성코드 발견현황

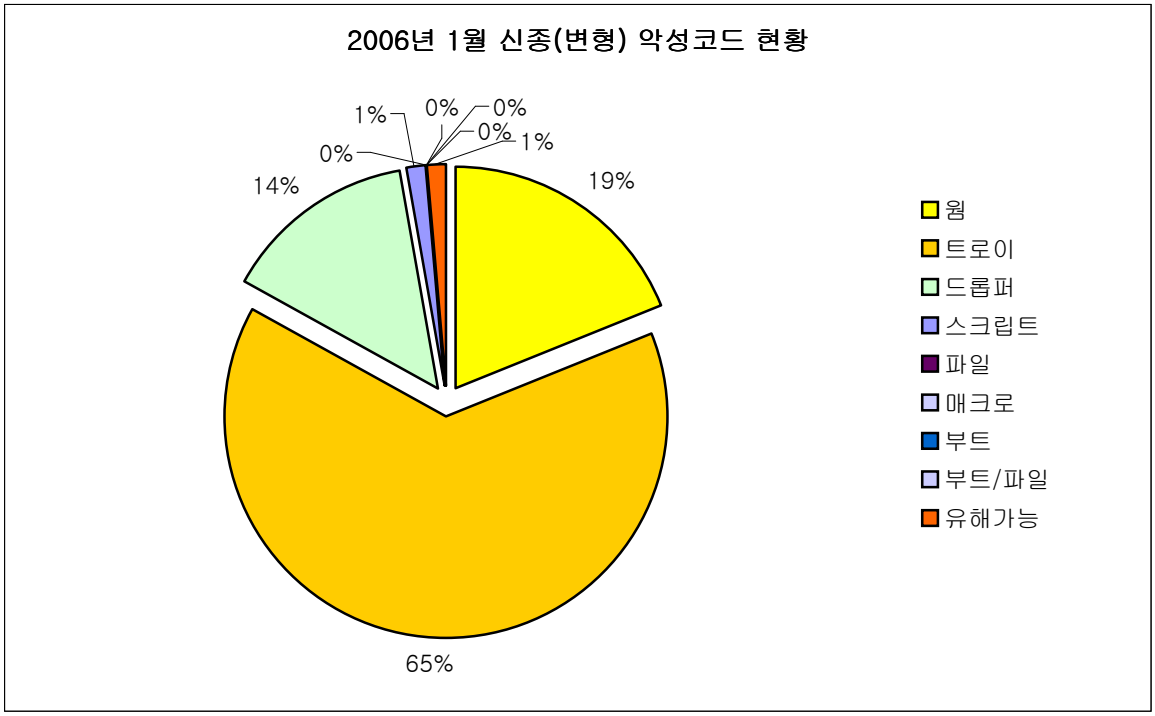
2006년 1월도 지난 2005년 12월과 비슷한 양상을 보이고 있다. 단지 그 수가 조금 줄어들었는데 특정 트로이목마들의 변형 수가 감소하였다. 이 트로이목마들은 크게 중국산 트로이목마와 베이글 트로이목마(Win-Trojan/Bagle)로 나눠진다. 변형이 감소한 트로이목마는 다음과 같다.

- 그레이버드 트로이목마(Win-Trojan/GrayBird)
- 리니지핵 트로이목마(Win-Trojan/LineageHack)
- 피씨클라이언트 트로이목마(Win-Trojan/PcClient)
- 베이글 트로이목마(Win-Trojan/Bagle) 시리즈

언급 했듯이 베이글 트로이목마 이외에 나머지는 중국산 트로이목마들이다. 이들은 중국발 해킹을 통하여 설치되거나 기존에 감염된 트로이목마들이 또 다른 변형을 다운로드하여 감염된다. 이러한 내용으로 추정해 본다면 중국발 해킹이나 이를 통한 트로이목마 유포 시도가 다소 줄어든 게 아닌가 추정된다.

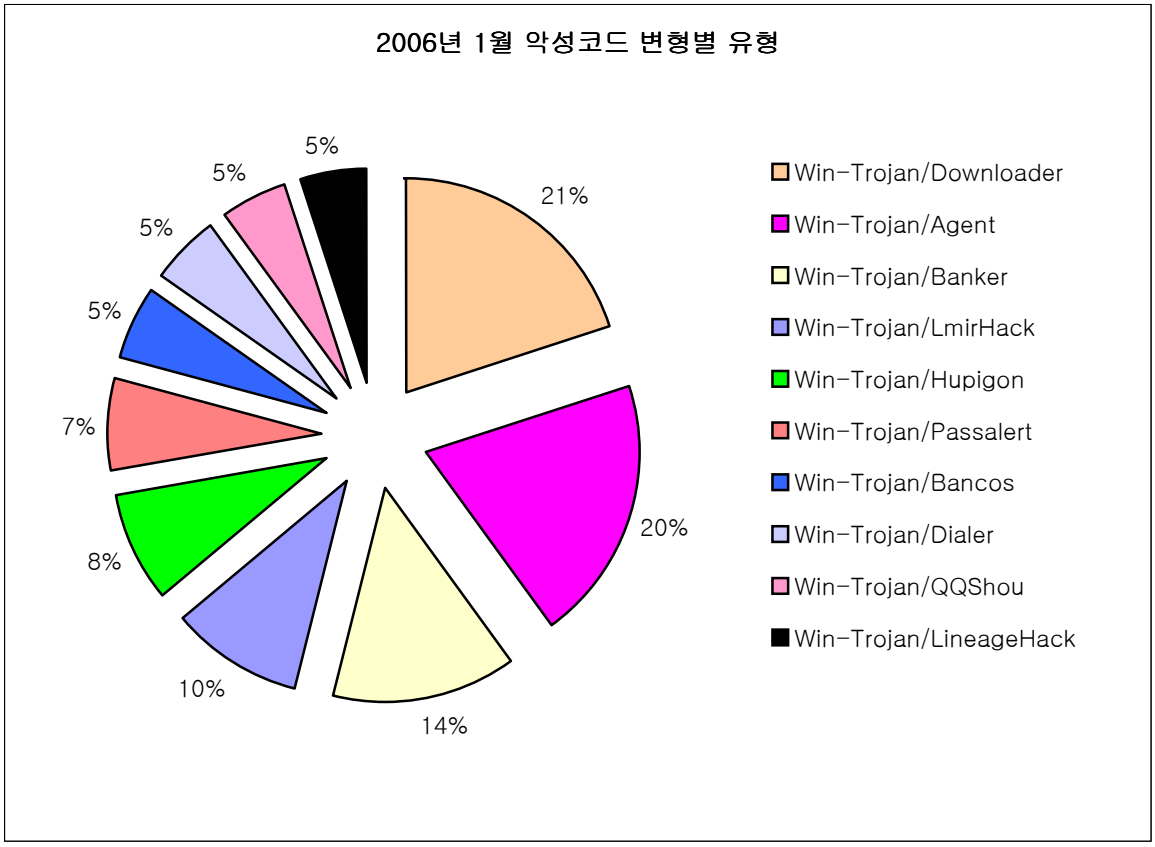
웜의 숫자는 지난 12월과 비교했을 때 소폭 증가하였다. 역시 악성 아이알씨봇(IRCBot) 웜의 변형이 가장 많으며 조금 다른 형태로 디엘엘봇 웜(Win32/Dllbot.worm)이라고 명명된 악성코드의 변형들이 발견되었다. 이 악성코드의 증상은 일반적인 악성 아이알씨봇 웜과 유사하지만 그 파일형태가 동적 라이브러리인 DLL 형태이다. 따라서 단독으로는 실행될 수 없고 드롭퍼에 의해서 드롭된 후 실행되거나 rundll32 또는 regsvr32로부터 실행될 수 있다. DLL 형태의 악성 아이알씨봇 웜은 이전에도 확인된 형태가 있으므로 새로운 것은 아니며 에스디봇 웜(Win32/SdBot.worm) 변형이 기승을 부릴 때인 2003년쯤 보고된 바 있다.

[그림1]은 1월 신종(변형)악성코드의 비율을 나타낸 것이다. 트로이목마가 차지하는 비율이 높은 것을 알 수 있다. 또한 트로이목마를 드롭하는 드롭퍼의 비율도 지난달에 비하여 증가하였다.



[그림1]2006년 1월 신종(변형) 악성코드 비율

드롭퍼의 형태는 PE 형태를 가진 실행파일과 .CHM 형태 등 크게 2가지로 나누어진다. .CHM 형태는 IE의 취약점을 이용하여 특정한 스크립트로부터 읽혀지고 실행된다. 이 형태는 압축된 HTML로, 내부에 실행 가능한 파일이나 이미지를 포함할 수 있다. 이 포맷자체가 문제가 되는 것은 아니며 이를 원격에서 권한 상승하여 로컬에서 임의로 실행될 수 있는 취약점이 존재하기 때문이다. 이 취약점은 매우 오래 전에 보고되었었다.



[그림2] 악성코드 변형 별 유형 및 분포율

[그림2]는 1월 엔진에 반영된 악성코드 중 가장 많은 변형을 가진 Top 10만을 집계해 본 것이다. 이 통계는 매월 엔진에 반영되는 모든 악성코드를 대상으로 조사한 내용이므로 국내를 비롯한 해외의 신종 및 변형의 악성코드 동향을 반영한 자료라 할 수 있다. 1월에는 다운로더 트로이목마(Win-Trojan/Downloader)가 가장 많은 변형이 보고되었다. 다운로더는 악성코드를 다운로드하는 것뿐 아니라 스파이웨어를 다운로드 받아오는 것도 포함한다. 다운로더 형태의 악성코드가 증가한 가장 큰 원인은 80/TCP를 이용하여 파일 다운로드를 하므로, 방화벽에서 차단되지 않기 때문이다. 과거의 악성코드들은 자신을 업데이트 하기 위하여 별도의 포트를 오픈하는 행동을 하였다. 하지만 이러한 포트들은 방화벽에서 모두 차단되었을 뿐 아니라 좋은 방법이 아니었다. 하지만 필터링 하기 어려운 80/TCP는 여전히 그들에게는 외부로부터의 연결이 자유로운 통로인 것이다.

1월 주요 신종(변형) 악성코드 정리

지난 12월말에 등장한 WMF 취약점 (MS06-001)을 악용한 관련 악성코드가 1월 내내 이슈가 되었다. 또한 오래 전부터 보고된 나이젬 웜(Win32/Nyxem.worm)의 변형이 국외에 광범위하게 확산되었고 특정 활동일에 파일을 손상하는 증상도 알려졌다.

이슈가 되었던 이번 달의 악성코드 및 주요사건은 다음과 같다.

► *.WMF 취약점과 관련 악성코드의 기승

보안패치가 공개되기도 전에 취약점을 이용한 악성코드의 등장으로 제로데이 공격이라고 불리던 MS06-001 취약점(그래픽 렌더링 엔진의 취약점으로 인한 원격 코드 실행 문제점)을 이용한 악성코드가 폭발적으로 쏟아져 나왔다. 수 많은 변형을 해결하기 위하여 대부분의 안티 바이러스 업체는 휴리스틱 엔진을 서둘러 제작하여 엔진에 포함시키기도 했다. 12월말과 1월 초 사이에 발견된 *.WMF는 스파이웨어를 다운로드 하는 형태가 대부분이었으나 시간이 지날수록 악성코드를 다운로드 하는 형태도 보고 되었다. 또한 취약점 코드와 공격자의 쉘코드를 합쳐 새로운 *.WMF를 만들어내는 도구도 등장하였고, 국내에서는 중국산 트로이목마를 다운로드하는 변형도 발견되었다. 중국의 악의적인 공격자 집단이 이미 자동화된 중국 발 해킹에 이 취약점이 포함된 *.WMF 파일을 이용했을 경우 큰 피해를 유발하는 상황이었다. 그러나 다행히 몇 건의 피해만 보고되었고, 크게 피해가 확산되지는 않았다.

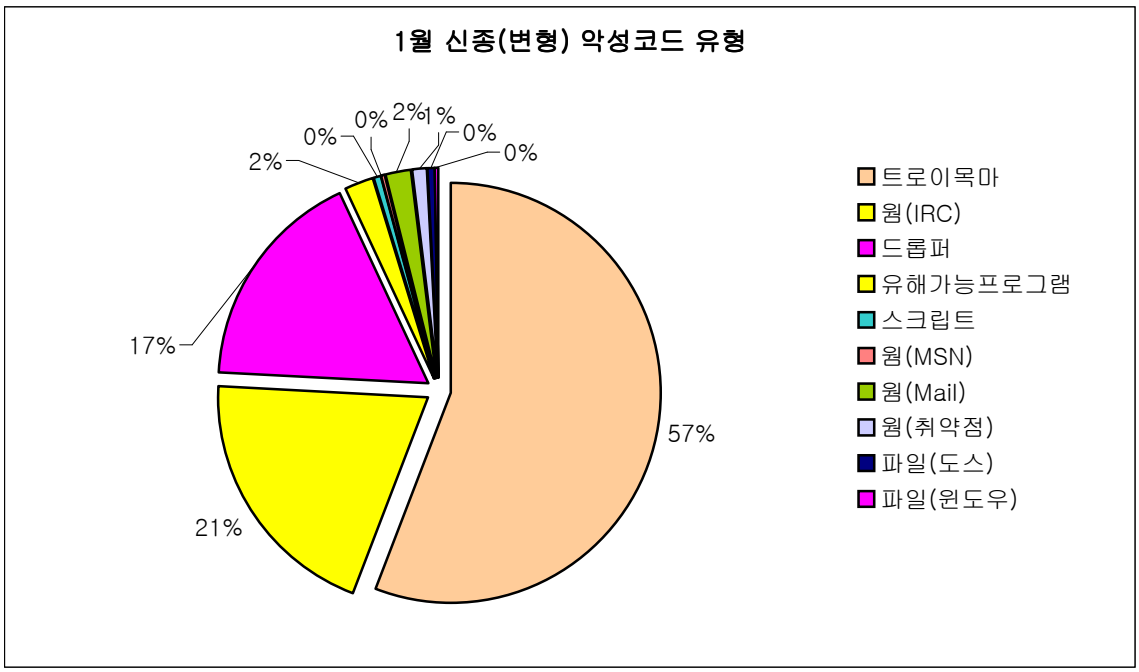
► 인스턴트 메신저를 이용하는 악성 아이알씨봇 웜

1월 중순 특정 메신저를 사용하는 고객으로부터 특정 웹 호스트가 명시된 링크가 담긴 메시지를 버디 리스트에 등록된 사람으로부터 받았으며, 메시지에 있는 링크를 눌렀을 때 어떤 파일이 다운로드 되려고 한다는 신고가 보고되었다. 확인결과, 취약점이 포함된 *.WMF 파일과 악성 아이알씨봇 웜이 발견되었으며, 공격자는 iframe 태그에 *.WMF 파일과 악성 아이알씨봇 웜 파일을 다운로드 받도록 해 둔 것이다. 따라서 패치가 안된 시스템에서는 조작된 *.WMF 가 실행될 경우 특정 FTP로부터 악성 아이알씨봇 웜을 다운로드 받게 되며, 취약점이 패치된 사용자도 다운로드 파일을 무심코 실행한다면 역시 감염되게 된다. 메신저를 이용하여 악의적인 링크를 보내는 방식의 공격은 이전에 발견되었던 웜에서도 사용되었던 방법이지만, 악성 아이알씨봇 웜이 여러 인스턴트 메신저까지 컨트롤 할 수 있게 되었다는 점에서 새롭다 할 수 있다.

► 나이젬 웜 확산과 특정 활동일

이 웜은 2년 전부터 보고되었으며 1월 중순에 발견된 것은 이 웜의 변형 중 하나다. 나이젬 웜(Win32/Nyxem.worm)으로 명명된 이 웜은 마이와이프 웜(W32/Mywife), 블랙말 웜(W32.Blackmal@mm) 등의 이름도 가지고 있다. 이 웜은 자신의 변형 중으로는 처음으로 특정일-매월 3일-에 오피스 문서파일이나 ZIP과 같은 압축파일들을 32Bit 크기를 갖는 특정 문자열로 덮어씌우는 증상을 가지고 있다. 이 웜은 주로 유럽지역에서 광범위하게 확산되어 큰 피해가 있을 것으로 예상되기도 했지만, 의외로 첫 피해가 예상 되었던 2월 3일은 이전 CIH 바이러스 활동일 때와 같은 큰 피해는 보고되지 않았다. 그 원인은 웜이 보고된 날로부터 첫 번째 피해가 예상되는 날까지 안티 바이러스 업체나 사용자들이 충분히 대응을 할 수가 있었기 때문으로 보이며, 각종 매스컴에서도 이 웜의 활동일에 대하여 경고하여 사용자들에게 충분한 주의를 주어 대처할 수 있었기 때문으로 보인다.

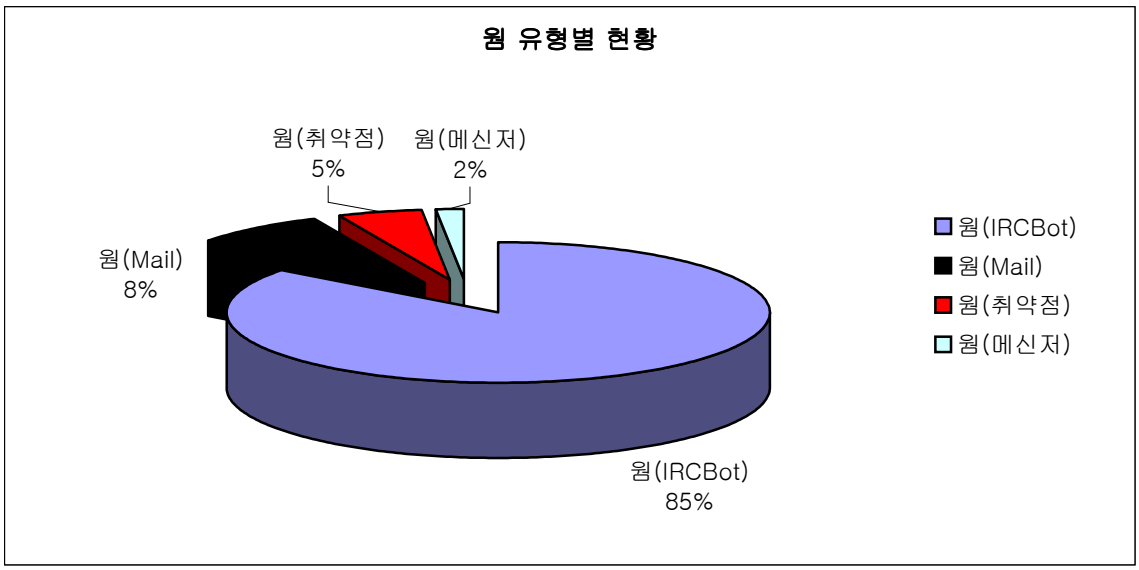
다음은 이번 달에 발견된 신종 및 변형 악성코드에 대한 유형별 분포이다.



[그림5] 1월 신종 (변형) 악성코드 유형별 현황

유형 중에 도스 파일 바이러스가 눈에 띈다. 도스 바이러스에 감염된 파일을 사용자부터 접수 받는 일은 흔하지 않은데, 1월에 HLLP.19920 라는 도스 바이러스가 발견되었다. 이 바이러스는 단순 기생형 바이러스로 *.EXE 만 감염되며 감염된 파일은 19920 바이트 증가한다.

[그림5]는 웜 유형을 종류별로 분류하여 본 것이다. MS 보안 취약점이나 관리목적 공유폴더 등으로만 전파되는 웜의 비율은 점차 줄어들고 있으며 이메일로 전파되는 웜 역시 그 종류라던가 그 확산도가 그다지 광범위하지 않다.



[그림5] 1월 신종 및 변형 웜 유형별 현황

그러나 악성코드들은 여전히 더욱 은밀하게 자신을 전송하여 시스템 및 사용자의 정보를 훔쳐내고 있다. 또한 광범위하게 확산되기 보다는 국지적으로만 확산되어 필요한 정보를 빼돌리고 사라지며 다시 필요하다면 자신이 감염된 시스템을 조정하여 업데이트하거나 다른 악성코드 형태로 출현하는 등 끊임 없이 자신을 확장, 유지하고 있다. 이러한 악성코드의 유형은 대부분 트로이목마 형태들이다.

올 1월도 지난해 12월과 마찬가지로 비슷한 악성코드 보고건수와 유형들이 집계 되었다. MS의 취약점 때문에 큰 이슈가 있었지만 보안패치도 예상보다 빨리 나왔고 여러 안티 바이러스 업체가 대응을 잘 했다는 평을 받고 있다. 악성코드의 출현을 미리 예상 할 수는 없지만 예방과 최소한의 피해를 위한 노력은 앞으로도 지속적으로 필요하다.

II. 1월 AhnLab 스파이웨어 동향

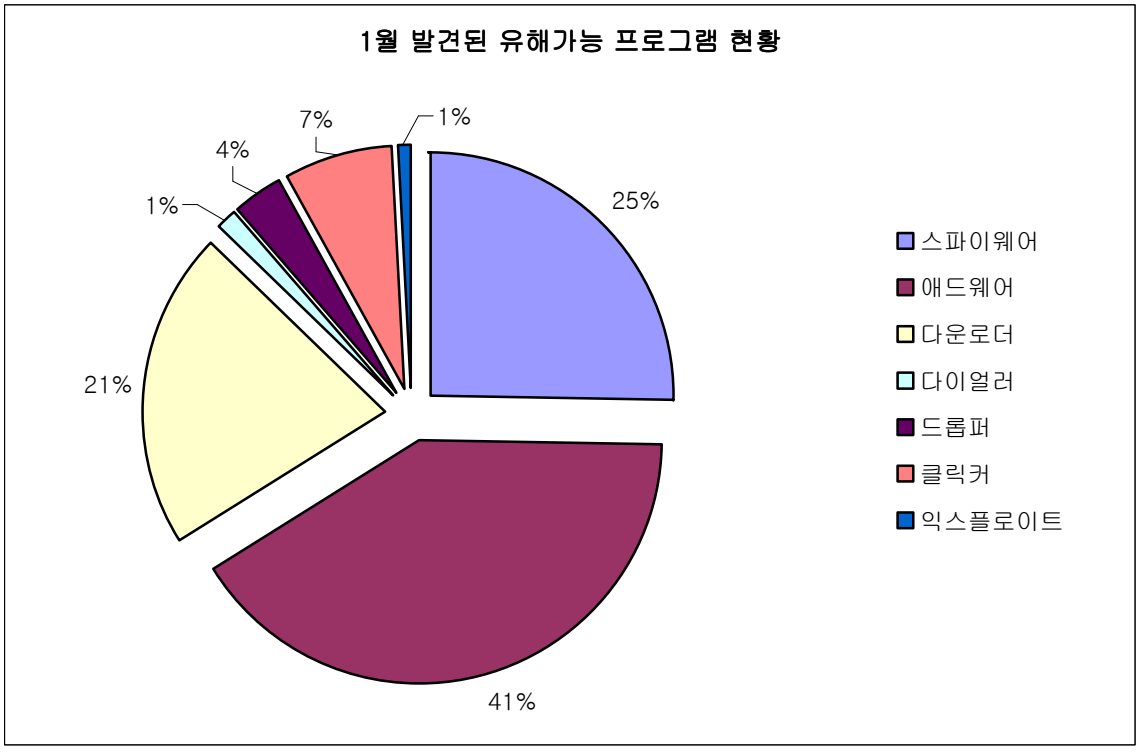
작성자: 박호진 주임연구원(hojinpk@ahnlab.com)

1월 한달 동안 접수된 신종(변형) 유해 가능 프로그램 건수는 [표1], [그림1]과 같다.

스파이웨어	애드웨어	다운로더	드롭퍼	클리커	익스플로잇	합계
108	174	89	15	30	4	426

[표1] 2006년 1월 유형별 신종(변형) 유해가능 프로그램 발견 현황

이번 달에 발견된 신종(변형) 유해가능 프로그램은 애드웨어가 스파이웨어 보다 많은 수를 차지하고 있다. 이는 Rogue(허위) 안티 스파이웨어의 꾸준한 증가와 바로가기 등 신규 샘플이 많이 접수되었기 때문이다.



[그림1] 2006년 1월 발견된 유해가능 프로그램 비율

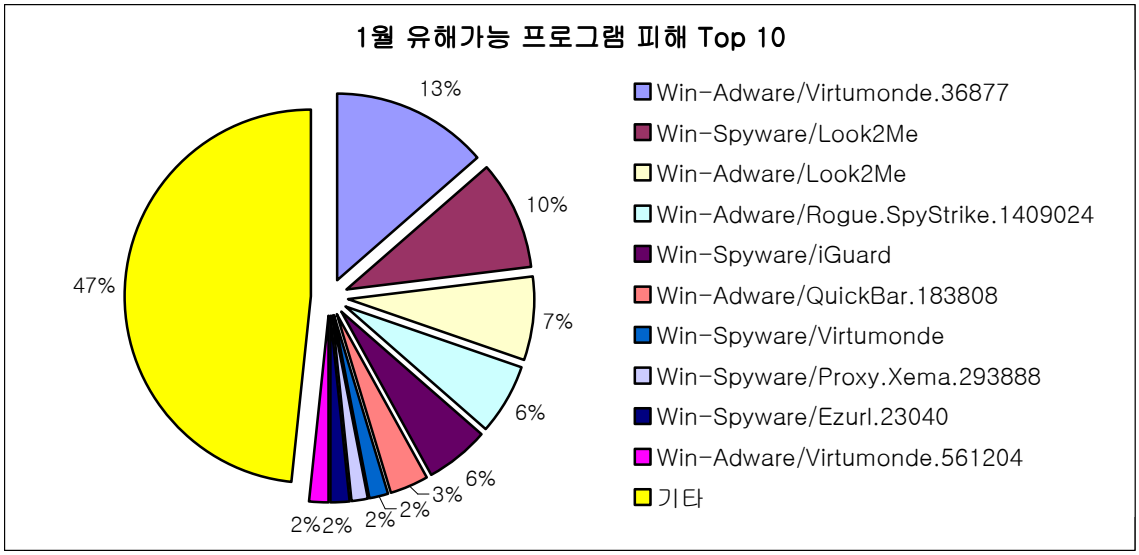
위 [그림1]에서 보는 바와 같이 유해가능 프로그램의 반 이상이 스파이웨어와 애드웨어로 구성되어 있음을 확인할 수 있다. 이는 스파이웨어와 애드웨어가 손쉽게 제작할 수 있기 때문으로, 사용자들의 정보를 빼내거나 어떤 식으로든 금전적 이윤을 얻으려고 하는 유해가능 프로그램들이 상당수 존재하고 있다는 것을 의미한다.

1월에 피해 신고된 유해가능 프로그램 Top 10을 살펴보면 [표2], [그림2]와 같다.

순위		유해가능 프로그램 명	건수	비율
1	-	Win-Adware/Virtumonde.36877	17	13.5
2	-	Win-Spyware/Look2Me	12	9.5
3	-	Win-Adware/Look2Me	9	7.1
4	-	Win-Adware/Rogue.SpyStrike.1409024	8	6.3
5	-	Win-Spyware/iGuard	7	5.6
6	-	Win-Adware/QuickBar.183808	4	3.2
7	-	Win-Spyware/Virtumonde	2	1.6
8	-	Win-Spyware/Proxy.Xema.293888	2	1.6
9	-	Win-Spyware/Ezurl.23040	2	1.6
10	-	Win-Adware/Virtumonde.561204	2	1.6
		기타	61	48.4
합계			126	

[표2] 2006년 1월 유해 가능 프로그램 피해 Top 10

1위를 차지한 버츄몬드(Win-Adware/Virtumonde)는 다운로더와 같은 다른 트로이목마나 스파이웨어에 의해 설치되는 것으로 추정된다. 이 애드웨어는 DLL파일의 형태로, 파일 이름과 CLSID는 랜덤한 값으로 생성된다. DLL파일이 BHO로 등록된 후, 탐색기를 실행하면 DLL이 Winlogon.exe에 인젝션(injection) 된다.



[그림2] 2006년 1월 유해가능 프로그램 피해 Top 10

2, 3위를 차지하고 있는 룩투미(Look2Me)는 이전부터 꾸준히 접수되고 있는 스파이웨어이지만, 4위를 차지한 로그.스파이스트라이크(Win-Adware/Rogue.SpyStrike)는 1월에 새롭게

발견된 허위 안티 스파이웨어 제품으로, 출시되자 마자 높은 순위를 보이고 있다.

이번 달에 있었던 스파이웨어 관련 사건들을 통해 스파이웨어 동향을 살펴보자.

WMF취약점을 이용하여 설치되는 다수의 스파이웨어 발견

WMF(Windows Meta File) 이미지 파일을 보는 것만으로도 감염시킬 수 있는 취약점(MS06-001)을 이용하여 스파이웨어 제작자들이 제마(Win-Clicker/Xema), 에이전트 다운로더(Win-Downloader/Agent), 멀드롭 드롭퍼(Win-Dropper/MulDrop)와 같은 스파이웨어들을 다수 발견되었었다.

허위(Rogue) 안티 스파이웨어들의 극성

이번 달에도 허위 안티 스파이웨어들의 기승은 그칠 줄 몰랐다. 허위 안티 스파이웨어는 주로 정상 파일, 정상 레지스트리를 오진하는 것으로, 이런 수법으로 사용자들에게 불안감을 조성하여 치료를 위한 결제를 유도하여 이윤을 챙기는 등 사용자에게 불안감을 조성하고 금전적인 손해를 입히는 프로그램이다. 특히 이번 달에는 애드웨어가 사용하는 레지스트리 키를 생성한 후 이를 진단결과로 보여주는 새로운 방법이 발견되었다.[1] 또한 기존에 스파이액스(SpyAxe)라는 허위 안티 스파이웨어 제품을 복제한 스파이스트라이크(SpywareStrike)가 발견되어 Win-Adware/Rogue.SpyStrike로 진단 추가하였다.

국내 최초의 루트킷(Rootkit)을 사용한 스파이웨어 발견

국내 특정 동영상 프로그램과 함께 번들로 설치되는 키워드 도우미 일종인 이지유알엘(Win-Spyware/Ezurl)이 바로 그것이다. 이 스파이웨어가 설치되면 루트킷을 이용하여 관련된 모듈을 은폐하고 사용자의 의도와는 무관하게 동작하여 악의적인 행동을 할 수 있다.
이미 지난해에 소니(Sony)에서 복사방지용 DRM 솔루션으로 루트킷을 이용하여 특정폴더를 숨겨 동작하도록 하였고, 이런 동작 방법을 이용한 악성코드들이 발견된 적이 있었으나, 국내에서 이런 수법의 스파이웨어가 발견되기는 처음이다.

[1] 안철수연구소의 안티 스파이웨어 제품인 스파이제로(SpyZero)에서는 이를 로그.비페스트(Win-Adware/Rogue.Befast)로 진단한다.

III. 1월 시큐리티 동향

작성자: 김지훈 주임연구원(smallj@ahnlab.com)

1월에 발표된 보안 취약점 동향

이번 달에는 마이크로소프트사(이하 MS)의 1월 정기 보안 패치가 총 3개 발표되었다. 모두 긴급 보안 공지(MS06-001, MS06-002, MS06-003)에 해당하는 것이므로 반드시 보안 패치를 적용하도록 한다. 이 중에서 MS06-001 보안 패치는 정기 보안 패치일(1월 10일)보다 앞선 1월 5일에 발표되었다. WMF 취약점의 심각성은 보안패치가 발표되기 전에 발표된 취약점이었다는 점에서 국내외 보안업계를 긴장시키기에 충분한 것이었다. 참고로, MS가 정기 보안 패치 예정일보다 앞서 발표한 사례는 2004년 12월 인터넷 익스플로러 누적업데이트(MS04-040)[1]를 들 수 있다. 이 보안 패치는 HTML 요소 취약점에 관한 것으로 보프라(Bofra)웜이 이 취약점을 이용하기도 하였다.

이번 WMF 취약점은 악의적으로 조작된 WMF 파일 생성 도구가 공개되는 등 일찍이 광범위한 악용이 예고되었었다. WMF 제로데이 공격(Zero-Day Attack)은 중국발 웹해킹 후 IFRAME 코드를 삽입하여 악성코드 유포에 활용되던 아웃룩 익스프레스(Outlook Express) 누적 보안 업데이트(MS04-013)[2] 취약점을 대체할 수단으로 부상하였다-실제로 다수의 스파이웨어나 키로거의 트로이목마 설치에 악용되었음. 또한, 기존의 매스메일러 및 메신저 전파 기능을 갖는 악성코드와 함께 연동하여 자신의 전파에 활용하기도 하였다. WMF 취약점에 대한 자세한 내용은 이달의 ASEC 컬럼 'WMF 취약점으로 본 잠재위협 요소들의 경고'에서 다루기로 한다.

1월의 주요 취약점 현황[3]

위험등급	취약점	공격코드 유/무
HIGH	그래픽 렌더링 엔진의 취약점으로 인한 원격 코드 실행 문제점 (MS06-001)	유
HIGH	포함 웹 글꼴의 취약점으로 인한 원격 코드 실행 문제점 (MS06-002)	무
HIGH	Microsoft Outlook 및 Microsoft Exchange의 TNEF 디코딩 취약점으로 인한 원격 코드 실행 문제점 (MS06-003)	무

[1] MS04-040, http://www.microsoft.com/korea/technet/security/bulletin/ms04-040.mspx
[2] MS04-013, http://www.microsoft.com/korea/technet/security/bulletin/ms04-013.asp
[3] 취약점 현황은 ASEC의 보안전문가들에 의해 공격코드 유무, 악성코드 활용가능성, 취약점의 위험도 등 다양한 관점에서 판단하여 선별된 것으로, 사용자들의 주의가 필요한 것임을 나타낸다. 공격코드의 존재유무는 이 리포트들을 작성하는 시점에서 인터넷상에서 접할 수 있는 기준으로 작성되었다.

► 윈앰프 플레이리스트 파싱 버퍼 오버플로우 취약점
(Winamp Playlist Parsing Buffer Overflow Vulnerability)

이번 달에는 또 하나의 제로데이 공격이 발표되어 보안 업계를 긴장시킨 일이 있었는데, 주요 음원 재생 도구의 하나인 AOL의 윈앰프(Winamp)에 버퍼 오버플로우 취약점이 존재하는 것이었다. 윈앰프의 in_mp3.dll 파일에서 플레이리스트(playlist)파일의 “File” 필드의 인자값에 지나치게 긴 스트링이 전달될 경우 버퍼 오버플로우가 발생하게 된다. 공격자는 이 취약점을 이용해 원격에서 피해시스템 내의 악의적인 코드 실행을 가능하게 한다. 실제 일반에 공개된 개념증명코드(Proof of Concept)에서도 악의적으로 조작된 플레이리스트 파일(.pls)을 통해 시스템 내의 전자계산기 프로그램인 calc.exe이 실행하도록 조정함으로써, 악성코드의 원격코드 실행가능성을 시사하였다.

다음은 일반적인 윈앰프의 플레이리스트 파일 포맷이다. (#은 숫자를 뜻함)

[playlist]	
File#=	파일의 위치 (예: File1, File2)
Title#=	디스플레이명
Length#=	실행시간 (초). -1 등의 네거티브 숫자인 경우 스트림을 의미.
NumberOfEntries=#	플레이리스트안의 엔트리 수.
Version=2	PLS 포맷 버전. 한 파일 내에는 동일 포맷만이 존재함.

공격자는 다음과 같이 악의적인 플레이리스트 파일(.pls)이 삽입된 IFRAME 코드를 삽입한 후 피해자로 하여금 웹페이지 방문을 유도하게 된다. 또한, 이메일 첨부물 형태로 전달하여 해당 파일의 실행을 유도할 수도 있다.

```
<html><body>
<iframe width="0" height="0" marginwidth="0" marginheight="0" border="0" frameborder="0" src="crafted.pls"></iframe>
</body></html>
```

윈앰프 5.12버전과 이전 버전의 사용자는 지금 바로 보안취약점이 수정된 최신 버전(Winamp 5.13)으로 업데이트 하도록 한다.

이 밖의 주요 음원 재생 도구로는 애플의 아이튠, MS의 미디어 플레이어, 리얼네트웍스의 리얼오디오를 꼽을 수 있다. 음원 재생 도구는 디지털 시대에는 없어서는 안될 필수품들로, 이미 상당한 고객층을 확보한 범용 프로그램이다. 따라서, 취약점 악용시 상당한 피해가 예상되므로, 보안취약점 발표 시 고객의 빠른 업데이트 대응이 필수적으로 동반되어야 한다.

► 오라클, 정기 보안 패치 발표

오늘날 데이터베이스는 기업 활동에 있어서 빠져서는 안 될 중요한 요소가 되었다. 데이터베

이스의 폭넓은 활용은 보안 위협의 주요 공격 대상이 될 수 있음을 의미한다. 최근에도 데이터베이스의 취약점을 이용한 공격 가능성이 소개된 바 있으므로, 각별한 주의가 요구된다.

최근 오라클은 8i, 9i, 10g 등 DB제품 로그인 과정의 보안 취약점을 포함한 데이터베이스와 서버 제품 등에서 발견된 다수의 취약점에 대한 1분기 정기 보안 패치를 발표했다.[1] 이번 정기 보안 패치에는 Database 부분 37건, Application Server 부분 17건, Collaboration Suite 부분 20건 등의 취약점이 포함되어 있다.

2006년도 오라클의 정기 보안 패치 일정은 다음과 같다.

- 17 January 2006
- 18 April 2006
- 18 July 2006
- 17 October 2006

데이터베이스 운영에 있어 필요한 몇 가지 보안점검 항목을 제안하고자 한다. 시스템 및 데이터베이스 관리자는 이번 점검을 통해 현재의 보안 수준을 되짚어보는 소중한 시간이 되었으면 한다.

- 초기 설치시 꼭 필요한 요소만 설치한다.
- 항상 최신의 서비스`팩을 유지한다.
- 디폴트(Default) 사용자와 테스트 DB는 제거한다.
- 관리자 이외의 사용자에게 필요한 권한만을 부여한다.
- 데이터베이스 및 중요 데이터로의 적절한 접근제어를 실시한다.
- 가능한 한 일반 사용자 권한으로 데이터베이스를 운영한다.
- 가급적 기본적인 통신 포트 이외의 것으로 변경하여 사용한다.

[1] http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html

Ⅳ. 1월 세계 악성코드 동향

2006년 1월 가장 크게 이슈가 되었던 것은 1월 중순 경 나이젬 웜이 세계적으로 많이 확산된 것이다. 나이젬 웜은 웜의 확산으로 인한 피해 이외에도 특정일에 파일을 파괴하는 특성을 가지고 있어서 추가피해가 예상되었으나 다행이 크게 문제가 되지는 않았다.
소버 웜이 파일 다운로드를 시작하는 1월 5일에 서버에 파일이 존재할 것인가 하는 것 또한 이슈가 되었다. 이미 많은 사용자들에게 소버 웜이 감염되었기 때문에 추가 피해 또한 매우 클 것으로 생각되어 여러 보안관련 기업과 단체들의 관심의 대상이 되었으나 실제로 파일이 업데이트되지 않아 해프닝으로 끝나게 되었다.
WMF 취약점을 이용한 악성코드들이 대거 유포된 점도 중요한 이슈이다. MS에서 패치가 제공하지 않은 상태에서 취약점을 이용한 악성코드가 발견되었고 다행이 심각한 피해를 주지는 않았으나 우려하던 제로데이 공격이 실제로 발생했다는 점에서 시사하는 바가 매우 크다..

(1) 일본의 악성코드 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

광고를 목적으로 하는 불법적인 애드웨어나 스파이웨어의 설치로 인해 피해를 당하는 PC사용자가 점점 증가하고 있는 것은 전세계적으로 공통된 현상이고 일본의 경우도 동일한 추세를 보이고 있다. 일본 트렌드마이크로(Trendmicro, www.trendmicro.co.jp)의 보고서[1]에 의하면 2006년 한 달 동안 일본의 고객에게서 가장 많은 피해 신고가 접수된 악성코드들의 대부분이 애드웨어와 스파이웨어임을 알 수 있다.

순위	악성코드명	악성코드유형	금월피해	전월피해	전월순위
1	SPWY_GATOR	스파이웨어	324	363	1위
2	ADW_SHOPNAV	에드웨어	147	128	2위
3	ADW_WEBSEARCH	에드웨어	101	37	없음
4	EXPL_WMF.GEN	보안취약점	80	1	없음
5	JAVA_BYTEVER.A	보안취약점	79	47	7위
6	TROJ_SMALL	트로이목마	65	38	10위
7	ADW_HOTBAR.H	에드웨어	57	57	6위
8	TROJ_ROOTKIT	트로이목마	57	70	4위
9	ADW_SBSOFT.A	에드웨어	55	33	없음
10	ADW_CMDDSKTOP.A	에드웨어	43	19	없음

[표1] 바이러스 감염피해 월간 리포트(출처: 일본 트렌드마이크로)

[1] http://www.trendmicro.com/jp/security/report/report/archive/2006/mvr060206.htm

최근 유행하는 애드웨어는 삭제 방지를 위해 은폐기법이나 보호기능 등 악성코드들에서 사용되는 기법들을 그대로 사용하는 경우가 많기 때문에, 일단 설치되면 쉽게 제거되지도 않아서 설치로 인한 피해가 지속되고 있다. 유포하는 방식도 과거에는 프로그램을 설치할 때 함께 설치되거나 특정 사이트에 접속 시 설치되는 경우가 많았지만 최근에는 블로그나 포털 사이트의 게시판 등과 같이 많은 사람들이 이용하는 불특정 웹사이트에 게시물을 가장하여 게재해 놓은 후 ActiveX의 형태로 다운로드 하여 설치하게 끔 유도하는 경우가 많으므로 웹사이트 이용 시 주의가 필요하다. 또한 프로그램 설치를 위한 동의를 묻는 창이 뜨는 경우 반드시 프로그램의 출처 등에 대한 확인을 하고 꼭 필요한 경우가 아니라면 되도록 설치하지 않는 것이 피해 예방을 위해 매우 중요하다.

일본 유행 악성코드 유형별 발생현황

2006년 1월 일본에서 가장 많이 확산된 악성코드는 넷스카이 웜(Win32/Netsky.worm)이었다.

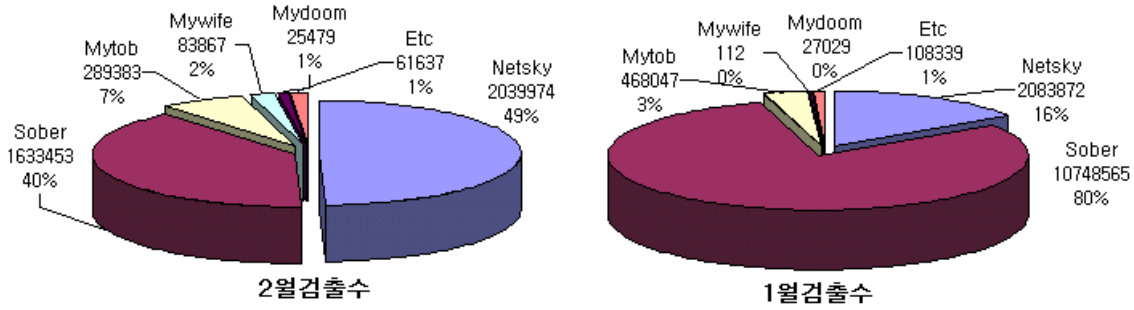
[표2]는 일본의 IPA(www.ipa.go.jp)에서 발표한 자료 중 악성코드 종류 별 감염피해 신고현황을 나타낸 것이다. 1월 한달 동안 넷스카이 웜의 피해 집계는 1,040건으로 이와 같은 수치는 전월과 비교해서 크게 변화가 없다.

Window/Dos Virus	금월피해 전월피해	Macro Virus	금월피해 전월피해	Script Virus	금월피해 전월피해
Win32/Netsky	1,040	Xm/Laroux	13	VBS/Redlof	42
	1,028		11		37
Win32/Mytob	630	XF/Sic	10	Wscript/ Fortnight	7
	570		3		
Win32/Sober	443	W97M/Bablas	4	Wscript/ Kakworm	3
	509		4		1
Win32/Bagle	313	X97M/Divi	4	VBS/Freelink	2
	304				1
Win32/Mydoom	242	WM/Cap	3	VBS/Internal	2
	289		237		
Win32/Lovgate	212	W97M/X97M/P97M/Tristate	2	VBS/Soraci	2
	203		9		3

[표2] 악성코드 피해 신고 현황

전월과 비교하여 마이톱 웜의 피해 건수가 증가한 것과 소버 웜의 피해 건수가 감소한 것은 특이할 만한 점이다. 특히 소버 웜의 경우 웜을 첨부한 메일을 다량 발송했던 전월에 비해서 그 양이 현저하게 감소하였다. [그림1]은 2005년 12월과 2006년 1월의 악성코드 검출 개수에 대한 통계이다. 넷스카이 웜 등 다른 매스메일러의 경우 수치의 변화가 거의 없는 반면

소버 웜은 월별 검출 개수가 현저하게 줄어든 것을 알 수 있다.



[그림1] 악성코드 검출 통계(출처: 일본 IPA)

실제 감염 피해가 감소한 비율에 비해 메일 검출 수치가 현저하게 낮은 것 또한 주목할 만하다. 이러한 현상은 악성 메일이 일본 국내뿐 아니라 국외에서도 다량이 유입되었음을 짐작할 수 있게 해 주는데, 소버 웜의 경우 12월 한 달 동안 전세계적으로 많은 피해 사례가 보고되었으나 현재는 피해 규모가 급격히 감소하고 있는 추세이고 이는 일본에서 나타난 현상과 유사하다.

악성코드의 감염 경로별 통계

[표2]는 악성코드의 감염 경로 별 피해 통계를 나타낸 것이다. 메일을 이용해서 전파되는 악성코드가 가장 많은 양을 차지하고 있는 것을 알 수 있다. 네트워크를 이용한 감염 피해 또한 이전에 비해 증가하고 있다.

감염경로	피해 건수					
	2006년 1월		2005년 12월		2005년 1월	
메일	4,385	97.5%	4,201	97.9%	4,819	98.8%
외부의 모체	0	0.0%	3	0.1%	2	0.0%
다운로드	4	0.1%	4	0.1%	5	0.1%
네트워크	109	2.4%	84	2.0%	50	1.0%
기타	1	0.0%	1	0.0%	4	0.1%
합계	4,999		4,293		4,880	

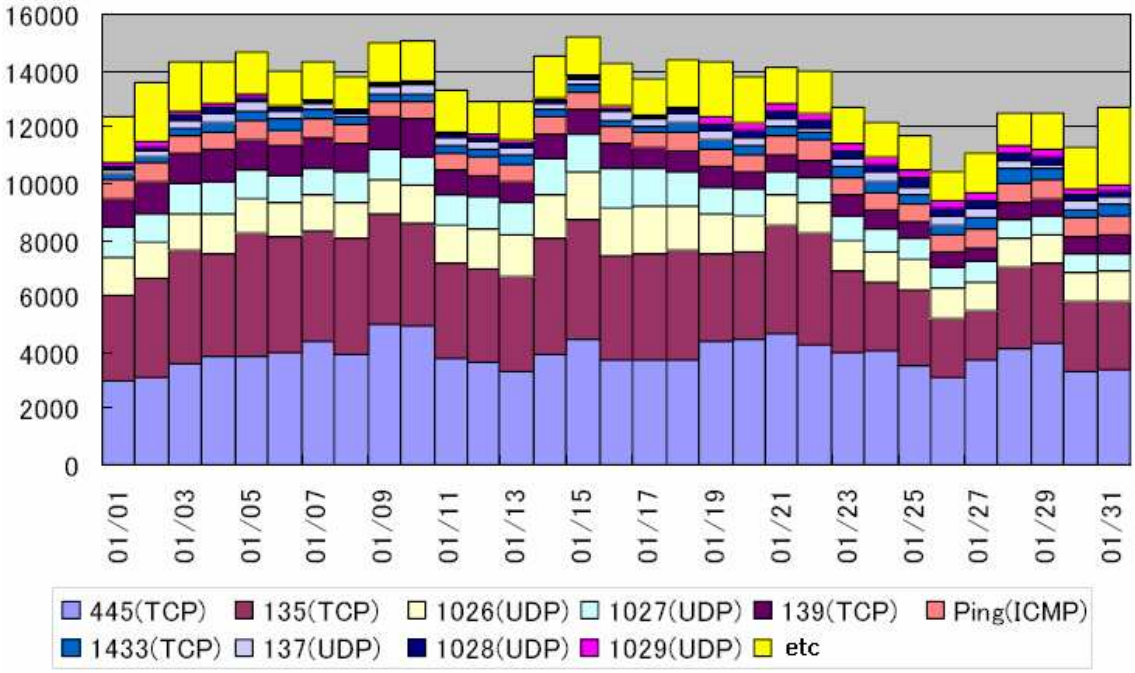
[표2] 악성코드 감염 경로 통계(출처: 일본 IPA)

일본 네트워크 트래픽 현황

[그림2]는 일본의 네트워크 트래픽 현황을 그래프로 나타낸 것이다. TCP135 포트와 TCP445 포트의 사용량이 매우 많은 것을 알 수 있다. 해당 포트들은 윈도우에서 기본으로 사용되는 포트들로써 최근에는 OS의 취약점을 이용하는 웜들에 의해 악용되기도 하므로 주의가 필요하다.

UDP1026 포트와 UDP1027 포트의 트래픽 또한 매우 많은 것을 확인할 수 있는데 두 포트들은 윈도우 OS의 메신저서비스에서 이용되는 포트들이다. 최근 일본에서는 윈도우메신저를

이용하여 광고메시지를 불특정 다수에게 전송하는 경우가 빈번하게 발생하고 있다.
대부분의 일반 사용자들은 메신저서비스를 사용하지 않는 경우가 많으므로 이러한 메시지를 받지 않기 위해서는 서비스를 중지시키는 것이 바람직하다.



[그림2] 일본의 네트워크 트래픽 (출처: 일본 IPA)

(2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

2006년 1월 중국 악성코드 동향에서 주목할 점은 2005년 가장 큰 흐름이었던 트로이목마의 강세가 계속해서 이어지고 있는 것인데 이러한 트로이목마의 강세는 웜에 의한 피해가 많은 다른 나라들과 뚜렷한 차이를 보이고 있다. 최근에는 애드웨어나 다른 악성코드의 다운로드를 시도하는 형태의 트로이목마 등 다양한 형태의 트로이목마가 등장하고 있으며 이러한 트로이목마의 확산 증가는 당분간 지속될 것으로 보여진다.

2005년 12월말에 등장한 마이크로소프트의 윈도우 메타 파일(WMF) 취약점(MS06-001) 역시 중국 내에서도 다른 악성코드를 전파하는 방법으로 사용되고 있으며, 특히 중국 내 언더그라운드 웹 사이트에서는 취약점을 악용한 윈도우 메타 파일을 제작할 수 있는 툴까지 배포하고 있는 것으로 확인 되었다. 그리고 매월 3일 감염된 시스템에 존재하는 특정 확장자의 파일들을 파괴하는 트리거로 인해 경계 주의가 있었던 나이젬 웜(V3 진단명 Win32/Nyxem.worm)은 유럽 등의 지역과는 달리 중국 내에서만은 감염보고가 거의 없었던 것으로 보고되었다.

악성코드 TOP 5

순위 변화	순위	Rising
↑ 1	1	Backdoor.Agent
↑ 1	2	Trojan.PSW.LMir
↓ 2	3	Backdoor.Gpigeon
New	4	Trojan.DL.Small
↓ 2	5	TrojanDownloader.Small

[표1] 2005년 11월 라이징(Rising) 악성코드 TOP 5

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

순위 변화	순위	JiangMin
New	1	TrojanDownloader.QQHelper.f
New	2	TrojanDownloader.Agent.ue
New	3	TrojanDownloader.Delf.sn
New	4	Trojan/INF.a
New	5	TrojanDownloader.Small.bbo

[표2] 2005년 11월 강민(JiangMin) 악성코드 TOP 5

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

[표1]은 중국 로컬 백신 업체인 라이징(Rising)에서 발표한 2006년 1월 악성코드 TOP 5 순위이다. 라이징의 순위에서는 2005년 12월 마지막 순위에서 1위를 차지하였던 Backdoor.Gpigeon(V3 진단명 Win-Trojan/GrayBird 또는 Win-Trojan/Hupigon)이 2계단 하락하여 3위를 차지하였다. 그 대신 Backdoor.Agent(V3 진단명 Win-Trojan/Agent)이 1계단 상승하여 1위를 차지하였고 그 뒤를 이어 Trojan.PSW.LMir(V3 진단명 Win-Trojan/LmirHack) 역시 1계단 상승하여 2위를 차지하고 있다. 이번 1월에 새로 순위에 포함된 Trojan.DL.Small(V3 진단명 Win-Trojan/Xema)는 2005년 8월 발견되기 시작하여 기타 악성코드에 포함될 정도로 감염보고가 많지 않았으나 1월에는 4위로 순위가 상승하였다. TrojanDownloader.Small(V3 진단명 Win-Trojan/Downloader) 역시 2계단 하락하여 5위를 차지하였다.

[표2]는 강민(JiangMin)에서 발표한 2006년 1월 악성코드 TOP 5 순위이다. 강민의 악성코드 TOP 5에서는 라이징의 순위와 달리 1위에서 5위까지 전부 새로운 악성코드로 등록되었다. 1위에는 TrojanDownloader.QQHelper.f(V3 진단명 Win-Trojan/QQHelper)가 차지하였다.

이 외에도 6위부터 10위를 기록하여 기타에 포함된 악성코드 중 웜은 라이징과 강민 두 업체를 통틀어서 강민 순위에 9위를 차지한 Backdoor/SdBot.atp.Rootkit(V3 진단명 Win32/IRCBot.worm)만이 있으며 나머지는 두 업체 모두 동일하게 트로이목마들이 차지하고 있었다. 라이징의 경우 2005년 12월까지 강세를 보이던 Trojan.PSW.QQRobber(V3 진단명 Win-Trojan/QQRob)과 Trojan.PSW.QQPass(V3 진단명 Win-Trojan/QQPass)은 7위와 9위로 큰 하락을 보였다. 이로 미루어 기존에 감염보고가 많았던 트로이목마들의 감염활동이 줄어들고 새로운 형태의 트로이목마들이 강세를 보이고 있는 것으로 분석된다.

주간 악성코드 순위

순위	1주	2주	3주	4주
1	TrojanDownloader.Small	TrojanDownloader.Small	Backdoor.Agent	Trojan.DL.Agent
2	Backdoor.Agent	Backdoor.Agent	Trojan.DL.Small	Trojan.DL.Small
3	Trojan.PSW.LMir	Backdoor.Gpigeon	Trojan.PSW.LMir	Trojan.PSW.LMir
4	Backdoor.Gpigeon	Trojan.PSW.LMir	Backdoor.Gpigeon	Backdoor.Gpigeon
5	Exploit.HTML.CodeExec	Exploit.HTML.CodeExec	Exploit.HTML.CodeExec	Dropper.Agent

[표3] 2006년 1월 라이징(Rising) 주간 악성코드 순위

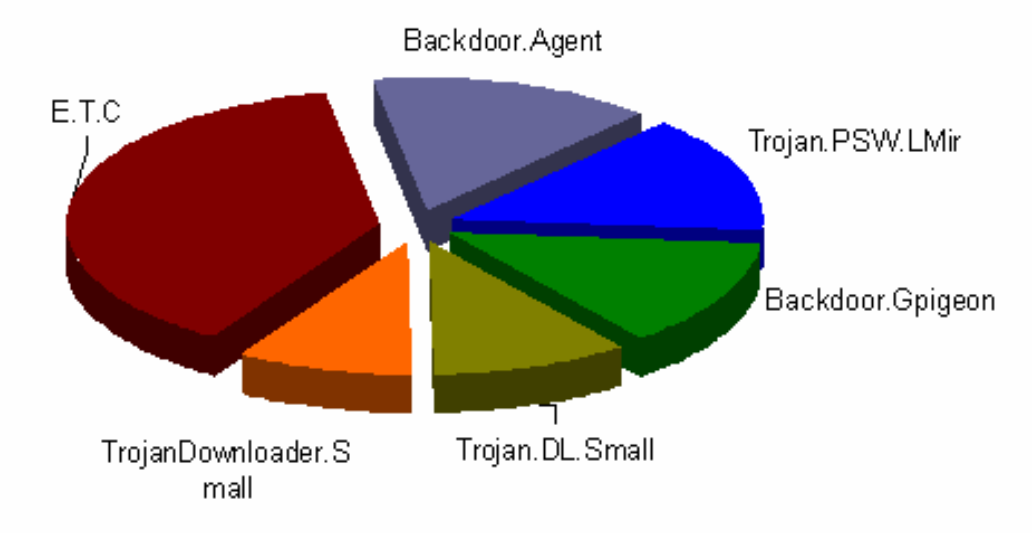
순위	1주	2주	3주	4주
1	TrojanDownloader.Agent.ue	TrojanDownloader.Agent.ue	TrojanDownloader.QQHelper.f	TrojanDownloader.QQHelper.f
2	Adware/Dmshell	TrojanDownloader.Small.bbo	TrojanDownloader.QQHelper.a	TrojanDownloader.Delf.sn
3	TrojanDownloader.Small.bbo	Trojan/INF.a	TrojanDownloader.Agent.ue	TrojanDownloader.Agent.uy
4	Trojan/INF.a	Trojan/HTADropper.ac	TrojanDownloader.QQHelper.b	TrojanDownloader.Agent.ue
5	Trojan/HTADropper.ac	Trojan/Maninex	TrojanDownloader.QQHelper.c	TrojanDownloader.QQHelper.a

[표4] 2006년 1월 강민(JiangMin) 주간 악성코드 순위

[표3]은 라이징(Rising)의 2006년 1월 주간 악성코드 순위이다. 2주차까지는 TrojanDownloader.Small이 1위를 차지하고 있었으나 3주차에서는 2위를 차지하고 있던 Backdoor.Agent가 1위를 차지하고 TrojanDownloader.Small은 주간 순위에서는 빠지게 되었다. 그리고 1주차와 2주차에서는 보이지 않던 Trojan.DL.Small은 3주차 2위를 차지하며 감염신고가 급격하게 증가하기 시작한 것으로 보고되어 4주째에서도 그 순위를 그대로 이어가고 있었다.

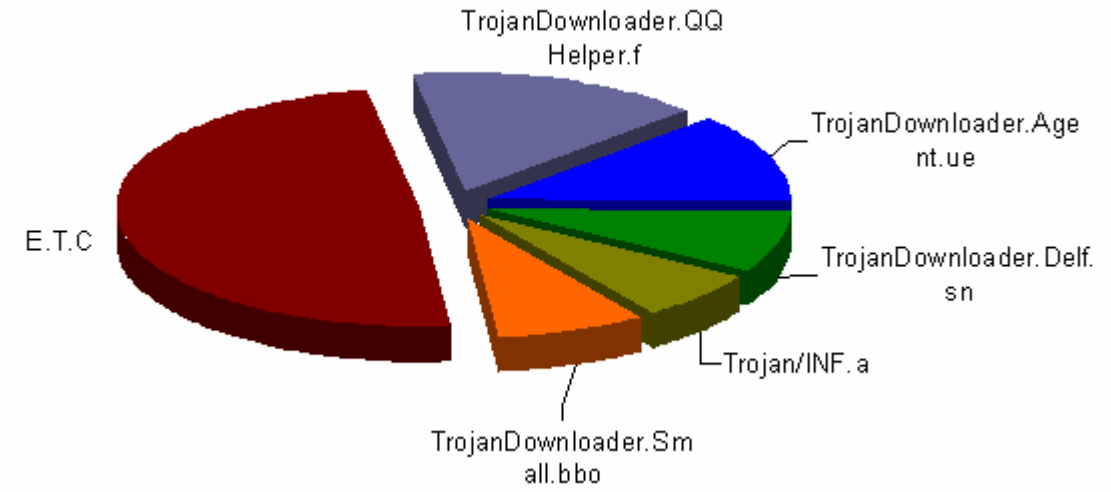
[표4]는 강민(JiangMin)의 2006년 1월 주간 악성코드 순위이다. 강민의 순위에서는 2주차까지는 특별한 변화의 조짐이 보이지 않았으나 3주째에서는 TrojanDownloader.QQHelper 변형들이 대거 등장하기 시작하였다. 3주차 순위에서 등장한 변형들은 총 4개로, TrojanDownloader.QQHelper.a, TrojanDownloader.QQHelper.f, TrojanDownloader.QQHelper.b, TrojanDownloader.QQHelper.c 이다. TrojanDownloader.QQHelper 트로이목마는 중국 내에서 사용되는 QQ 메신저의 이모티콘 등을 제공하는 프로그램으로 사용자를 속여 애드웨어를 다량으로 설치하는 다운로더 형태의 트로이목마이다. 이로 인해 3주차에서 급격한 신고보고가 있었던 것으로 분석된다.

악성코드 분포



[그림1] 2006년 01월 라이징(Rising)의 악성코드 분포

[그림1]은 2006년 1월 라이징의 악성코드 분포이다. 악성코드 TOP 5에 포함된 악성코드의 전체 분포는 61.61%를 차지하고 있으며 기타 악성코드가 38.39%를 차지하고 있다. 1위를 차지한 Backdoor.Agent, Trojan.PSW.LMir와 Backdoor.Gpigeon는 각각 14.6%, 14.31%와 13.45%를 차지하고 있어 분포 면에서는 큰 차이를 보이지 않고 있다. 38.39%를 차지한 기타 악성코드로는 Exploit.HTML.CodeExec(V3 진단명 HTML/CodeExec), Trojan.PSW.QQRobber(V3 진단명 Win-Trojan/QQRob), Trojan.DL.Agent, Trojan.PSW.QQPass(V3 진단명 - Win-Trojan/QQPass)과 Trojan.StartPage(V3 진단명 - Win-Trojan/StartPage)가 차지하고 있다.



[그림2] 2006년 01월 강민(JiangMin)의 악성코드 분포

[그림2]는 2006년 1월 강민 악성코드 분포이다. 강민의 악성코드 분포는 악성코드 TOP 5에 포함된 악성코드들의 분포는 50.14%를 차지하고 있으며 기타 악성코드가 49.86%를 차지하고 있어 라이징과는 달리 기타에 포함된 악성코드의 비율이 조금 더 높은 것을 알 수 있다. 1월 3주차에서 급격한 증가를 보였던 TrojanDownloader.QQHelper.f는 16.24%를 차지하여 가장 높은 분포를 보이며 TOP 5에 포함된 악성코드들과 분포 수치면에서도 큰 차이를 보이고 있다. 49.86%를 차지하여 기타에 포함된 악성코드로는 TrojanDownloader.QQHelper.a, Trojan/Maninex, Backdoor/Huigezi.nc(V3 진단명 Win-Trojan/GrayBird 또는 Win-Trojan/Hupigon), Backdoor/SdBot.atp.Rootkit(V3 진단명 Win32/IRCBot.worm)와 TrojanDownloader.QQHelper.c가 있다.

(3) 세계의 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

2006년 1월 악성코드 피해는 나이젬 웜 변형(Win32/Nyxem.worm.95690)[1]의 등장 외에는 큰 변화가 없이 여전히 소버 웜 변형, 넷스카이 웜 변형, 자피 웜 변형, 마이톱 웜 변형이 피해 순위 상위를 차지하고 있다.

나이젬 웜 변형은 1월 16일에 발견되어 대략 일주일이 지난 후부터 급격히 퍼지기 시작해 1월 말에는 순위가 1,2 위까지 올라갔었다.[2] 매달 3일에 문서 파일을 손상하는 나이젬 웜 변형은 피해가 우려되었지만 다행히 큰 피해는 보고되지 않았다. 특히 한국 등 아시아 지역에서는 나이젬 웜이 크게 확산되지도 않았다.

영국 소포스(Sophos)사의 1월 통계에 따르면 소버 변형이 44.9%로 압도적으로 1위를 차지하고 있다.[3] 나이젬 웜 변형은 4위로 새롭게 순위에 들어왔다. 독일의 H+BEDV사의 1월 통계에 따르면 소버 웜 변형이 1,2위를 차지하고 있다.[4] H+BEDV사의 통계에서 소버 웜이 2개 모두 왕성한 활동을 보이는 것은 소버 웜이 독일에서 제작되었기 때문으로 보인다.

1, 2위를 다투고 있는 소버 웜 변형이 1월 5일 파일을 다운로드하는 기능이 있어 많은 관계자들이 피해를 우려했다. 하지만, 언론 등에 알려지면서 악성코드 제작자가 부담을 느꼈는지 해당 주소의 서버에는 아무 파일이 올려지지 않았다. 소버 웜 변형은 발견 하루 전에 독일 경찰에서 새로운 소버 웜이 등장할 거라는 보도자료를 배포했는데 여전히 어떻게 경찰에서 웜의 배포 사실을 먼저 알았는지는 알려지지 않았다.

피해 순위에는 포함되지 않았지만 WMF 파일의 취약점을 이용해 사용자 모르게 악의적인 일을 하는 익스플로잇-WMF(Win-Trojan/Exploit-WMF)[5]을 이용한 일도 발생했다. 다른 악성코드를 다운로드 하게 변조된 WMF 파일이 메일, 메신저를 통해 보내졌으며 웹사이트 해킹 후 변조된 WMF 파일을 삽입해 두는 경우도 발생하고 1월 초에는 악성 아이알씨봇이 메신저를 통해 변조된 WMF 파일을 포함한 웹사이트로 접속을 유도하는 형태도 발견되었다. 다행히 현재 대부분의 백신에서 변조된 WMF 파일을 진단할 수 있으며 1월에 패치[6]가 발표되었다.

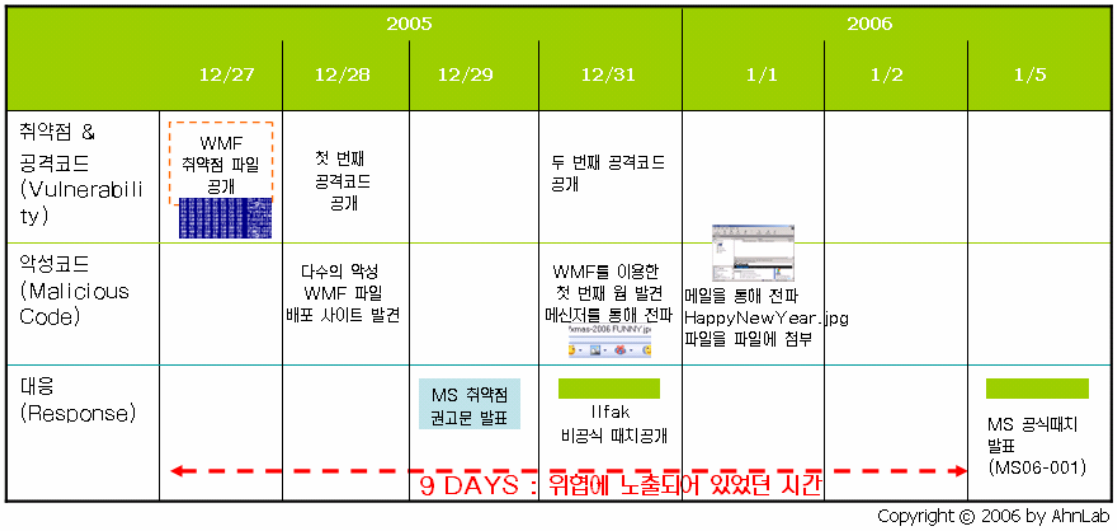
[1] http://info.ahnlab.com/smart2u/virus_detail_3503.html
[2] http://www.f-secure.com/virus-info/statistics/
[3] http://www.sophos.com/pressoffice/news/articles/2006/01/toptenjan06.html
[4] http://www.avira.com/en/news/January_Virus_Top_10.html
[5] http://info.ahnlab.com/smart2u/virus_detail_3231.html
[6] http://www.microsoft.com/technet/security/Bulletin/MS06-001.mspx

V. 이달의 ASEC 컬럼 – WMF 취약점으로 본 잠재위협 요소들의 경고

작성자: 정관진 주임연구원(intexp@ahnlab.com)

2005년의 마지막을 몇 일 남겨놓지 않은 시점인 12월 27일에 뜻하지 않은 한 통의 글이 보안 메일링리스트에 포스팅 되었다. 글의 내용인즉 새로운 취약점을 이용하는 것으로 추정되는 사이트의 주소였다.

해당 사이트에 접속하는 경우에는 수 많은 스파이웨어들이 설치되는데 그 근본적인 원인이 WMF(Windows Meta File) 이미지파일 안에 숨겨져 있는 특정코드 때문이었다. 사용자가 사이트를 방문하거나 또는 이미지 파일을 클릭하는 것만으로도 이미지파일 안에 숨겨진 특정코드가 실행돼 악의적인 파일들을 설치하게 된다. 이후 변형된 파일이 다수의 사이트에 등록되었고 공격코드 또한 공개되기 시작하였다. 시간이 지남에 따라 해당 취약점에 대한 정보가 세부적으로 밝혀졌고 악성코드가 해당 취약점을 이용하여 이메일, 메신저로 전파되는 웜으로까지 확산된 것이다. [그림1]은 해당 취약점이 발견된 시점부터의 주요사건을 표시한 것이다.



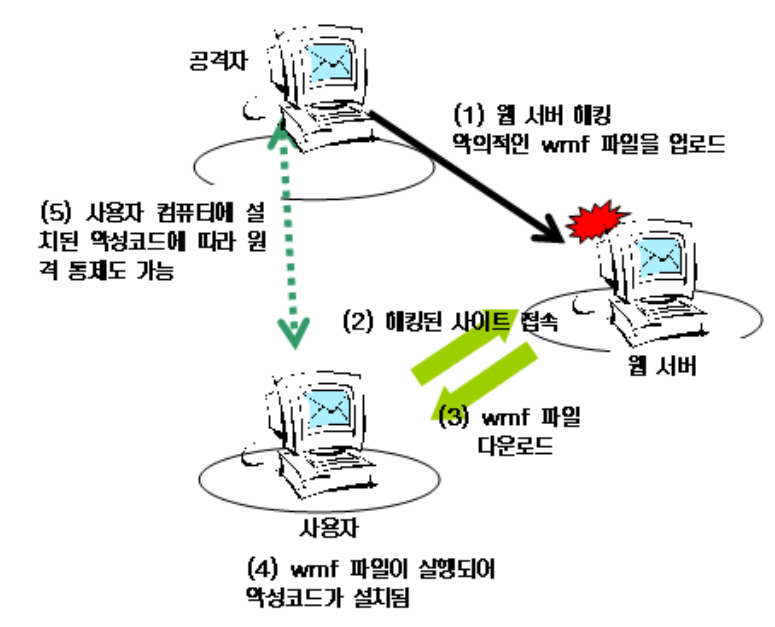
[그림1] WMF 취약점의 제로데이 TimeLine

해당 취약점이 보고된 후에는 언론에서도 큰 관심을 보였는데, 주된 이유로는 공식적인 패치가 존재하지 않았고 몇 년 전부터 우리들 귀에 익숙해진 제로데이라는 용어에 정확히 부합되기 때문이다. 즉, 취약점이 공개된 후 공격코드가 나오기까지의 시간이 점점 짧아지고 있다는 개념인데, 이번 WMF 취약점은 취약점을 이용한 악의적인 파일이 공개되면서 알려졌기 때문에 사용자들은 속수무책으로 해당 취약점에 노출될 수 밖에 없는 상태였다.

이 뜻은 결국 악성코드 또는 해당 취약점을 이용하여 악의적인 행동을 일으키기까지 최적의 시간임을 의미한다. 우선적으로 패치가 존재하지 않았다는 점이 가장 큰 문제이고, 윈도우 운영체제가 대상이라는 점, 취약점 자체를 이용하기가 어렵지 않고, 공격 코드 공개, 그리고

이런 악의적인 파일을 만들어 주는 도구까지 공개되어 누구나 쉽게 접근할 수 있었다는 점이다.

더불어 최근 들어 증가하는 웹 해킹에 WMF 파일을 이용한 해킹이 증가할 것으로도 예상되고 있어 이번 취약점을 통해 이용되는 경로는 다양해 질 것으로 보인다. 이미지 파일 자체에 취약점이 존재하는 형태이므로 (1) 메일에 파일 첨부 (2) 메신저를 통해 URL 전파 (3) 웹 페이지에 WMF 파일이 존재하는 IFRAME 태그 삽입 등 전파 경로가 다양해 질 수 있다. [그림2]는 웹 해킹을 통해 이뤄지는 과정을 나타낸 것이다.



[그림2] 웹 서버 해킹을 통한 WMF 취약점의 이용

이번 WMF 의 주요한 이슈들을 요약해 보면 크게 다음과 같다.

- 취약점이 발견된 후 이를 해결할 수 있는 패치가 존재하지 않았다.
- 취약점을 이용하는 공격코드 및 공격도구들이 알려졌다.
- 취약점은 WMF 이미지 파일에 존재하는 것으로, 다양한 방법으로 사용가능하였다.
- 패치가 나오기까지 9일 동안 사용자들은 취약점에 그대로 노출되어 있었다.
  물론 비공식적인 패치는 존재하였다.
- 취약점을 이용하는 악의적인 파일이 보고되었다.

일반적으로 취약점을 발견하면 해당 업체와 조율하여 패치가 다 준비되는 시점에서 발표시기를 정하는 것이 관례인데, 이번 WMF 사건의 경우 취약점을 악용하여 스파이웨어를 설치하는 파일이 알려지면서 WMF의 취약점이 드러나게 된 경우이다.

취약점은 12월말에 공개적으로 알려졌지만 언더그라운드 해커들 사이에서는 취약점을 공유하여 이전부터 사용하고 있었을 것으로 추정된다. 최근 보도된 기사에서도 12월 중반쯤 2,3개의 러시아 해커 그룹이 $4,000 달러에 취약점을 판매하려고 했었다는 내용이 실리기도 하였다.

이러한 위험성 때문인지 MS 사에서는 패치 일정인 1월 10일 보다 5일 앞서 1월5일에 패치를 발표하였다.

그럼 여기서 WMF 파일에 대해서 짚고 넘어가도록 하자. WMF 파일은 오래된 파일 포맷으로 Windows 3.x, Windows 95, 98 그리고 Windows NT 운영체제 때 사용되었던 파일이다. 이후에는 EMF(Enhanced Metafile)포맷이 사용되고 있어 WMF 파일은 현재 크게 사용되고 있지 않다. 그렇다면 왜 몇 십 년 전의 WMF 파일 취약점이 지금에 와서 사용되어 큰 문제가 되고 있는 것일까? 우선, 문제가 불거진 것은 그 위험성에 있어서고 필자가 언급하고 싶은 부분은 취약점의 발견시점보다도 과거의 오래된 포맷형태가 계속 유지되면서 최근에야 밝혀졌다는 점이다.

이 뜻은 앞으로 컴퓨터 사용이 계속 증대되면 소프트웨어, 파일포맷, 프로토콜 등은 과거 속에 잔존하면서도 계속 유지될 가능성이 높다는 것이다. 안전한 프로그래밍을 중시하지 않았던 과거에 제작된 소프트웨어나 프로토콜등이 현 시점에 중요한 보안 문제로 언급될 수 있기 때문이다. 과거 호환성을 위해 기능이 계속 유지되고, 소프트웨어 크기는 증대되면서 과거의 기능들이 위협요소로 존재할 수 있다.

앞으로도 소프트웨어의 기능은 다양해 지고 종류도 많아지면서 이러한 잠재적 위협요소들은 계속 누적될 것이다. WMF 취약점은 이에 대한 일종의 경고로 받아들여야 할지도 모른다. 그리고 제로데이의 상황이 과거에 비해 점차 증가되고 있어 향후 무방비로 외부에 노출되는 가능성이 더욱 높아질 것으로 예측된다. 그만큼 외부의 보안적 위협에 노출될 상황들이 점점 늘어나고 있다. 이제 우리는 새로운 보안적 위협을 대비할 수 있도록 준비하여야 할 것이다.