ASEC Report 2월

® ASEC Report

2005. 03

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

브로피아 웜의 급속한 확산, 애드웨어로 감염되는 부베 바이러스..

2월은 평월보다 일수가 적고 설날연휴 등으로 인하여 PC 사용일수가 감소하여 악성코드로 인한 피해 및 신종 발견 건수가 전월에 비해 다소 감소하였다. 2월에는 처음으로 악성코드 피해 Top 10 안에 악성 아이알씨봇 변형이 랭크하였다. 그만큼 작년부터 꾸준히 피해를 입히고 있는 악성 아이알씨봇 변형에 의한 피해가 여전하다는 것을 의미한다. 2월 초에는 MSN 메신저를 통해 전파되는 브로피아 웜 변형이 발견됨과 동시에 한국을 비롯한 중국, 일본 등 아시아 지역에 많은 피해를 입혔다. 그러나 메신저 웜의 특징상 급속한 확산을 보인 만큼 단시간내에 소멸하였다. 하지만 브로피아 웜은 1월에 최초 발견된 이후 지금까지도 꾸준히 변형이 만들어지고 있으므로, 메신저 사용에 주의를 기울여야 하겠다. 2월에 발견된 스파이웨어 중에는 기존의 일반적인 스파이웨어 배포방식이 아닌 플래쉬 파일을 이용하여 스파이웨어를 배포하는 기법이 국내에서 발견된 점이 특이할 만하다. 2월에 마이크로소프트사에서 12개의 보안패치를 발표하였다. 이 중 MSN 메신저 등을 이용한 공격이 가능했던 PNG 처리 취약점으로 인한 원격코드 실행문제(MS05-009)는 취약점 발표 하루만에 공격코드가 공개될 만큼 악성코드 제작에 이용될 가능성이 매우 높았다. 2월 한달동안 세계적으로는 메일을 통해 전파되는 매스메일러에 의한 피해가 가장 많았다. 그러나 지난달과 마찬가지로 지역별로 피해가 많은 매스메일러에 다소 차이가 있는데, 한국과 일본은 넷스카이 웜이, 유럽은 자피 웜에 의한 피해가 가장 많았다. 반면 중국은 MSN 메신저를 이용하여 전파되는 브로피아 웜에 의한 피해가 많았던 것으로 보고되었다. 이달의 ASEC 컬럼에서는 2월에 발견된 애드웨어(스파이웨어)에 의해 감염되는 바이러스인 부베 바이러스를 계기로 본 애드웨어의 기술적 발전과 마이둠 웜 변형 사례를 통해 본 네트워크 시그니처 기반 탐지의 한계성에 대해 살펴보았다.

I. 2월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

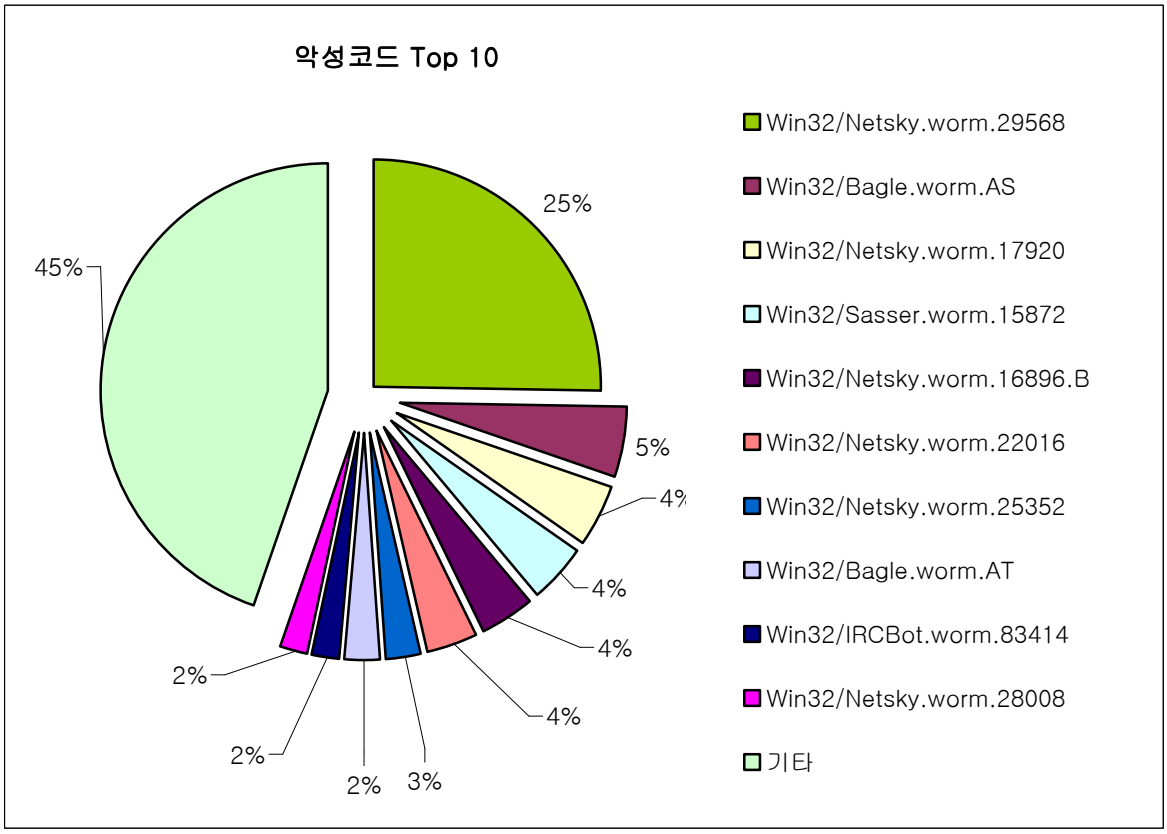
작성자 : 허종오 연구원(maha96@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	499	25.2%
2	New	Win32/Bagle.worm.AS	101	5.1%
3	-1	Win32/Netsky.worm.17920	86	4.3%
4	+1	Win32/Sasser.worm.15872	83	4.2%
5	-2	Win32/Netsky.worm.16896.B	76	3.8%
6	-	Win32/Netsky.worm.22016	73	3.7%
7	+2	Win32/Netsky.worm.25352	51	2.6%
8	New	Win32/Bagle.worm.AT	49	2.5%
9	New	Win32/IRCBot.worm.83414	39	2.0%
10	-2	Win32/Netsky.worm.28008	36	1.8%
		기타	886	44.8%
합계			1,979	100%

[표1] 2005년 2월 악성코드 피해 Top 10

안철수연구소로 신고된 2005년 2월 악성코드 피해 건수는 2005년 1월에 비해 소폭 감소한 1,979건이다. 지난달에 비해 다소 감소한 이유로는 2월 일수가 평월 보다 적은 28일이었으며 설날연휴로 인해 1주일간의 연휴가 있어, 기업사용자 및 일반사용자들의 PC 사용일수 감소로 실질적인 악성코드들이 활동할 수 있는 시간이 적었던 것이 주요원인으로 보인다.
2004년 한해 많은 변형이 발견되었던 악성 아이알씨봇(IRCBot) 웜은 2005년 1월에 예측했던 것처럼 증가 추세를 보였으며, 처음으로 10위권내에 악성 아이알씨봇 웜 변형이 진입하였다. 이는 특정 악성 아이알씨봇 웜으로 인한 피해가 꾸준히 증가하다는 것을 보여주고 있다.

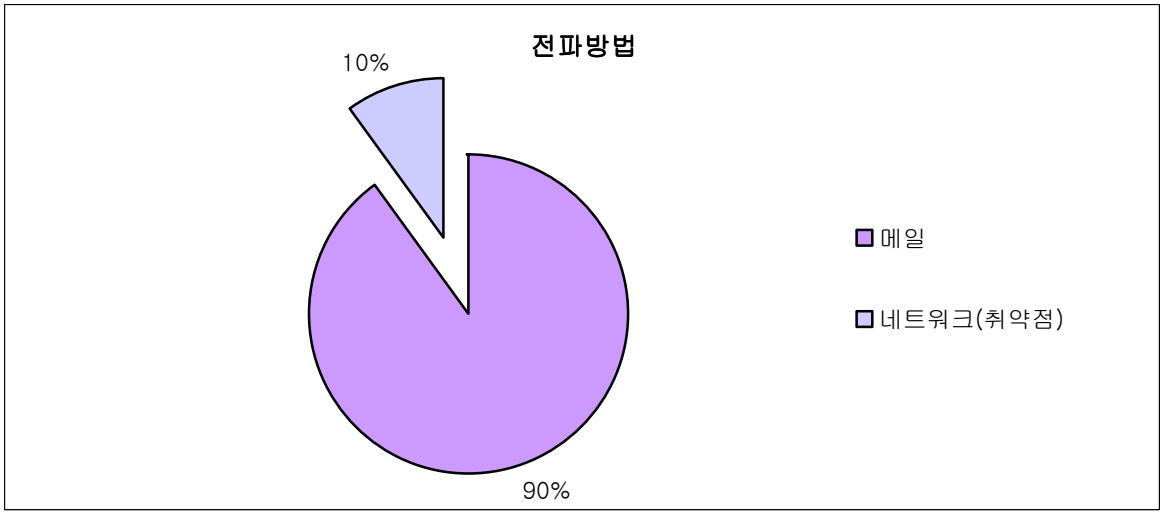
2월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.



[그림1] 2005년 2월 악성코드 피해 Top 10

2월 악성코드 Top 10 전파방법별 현황

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



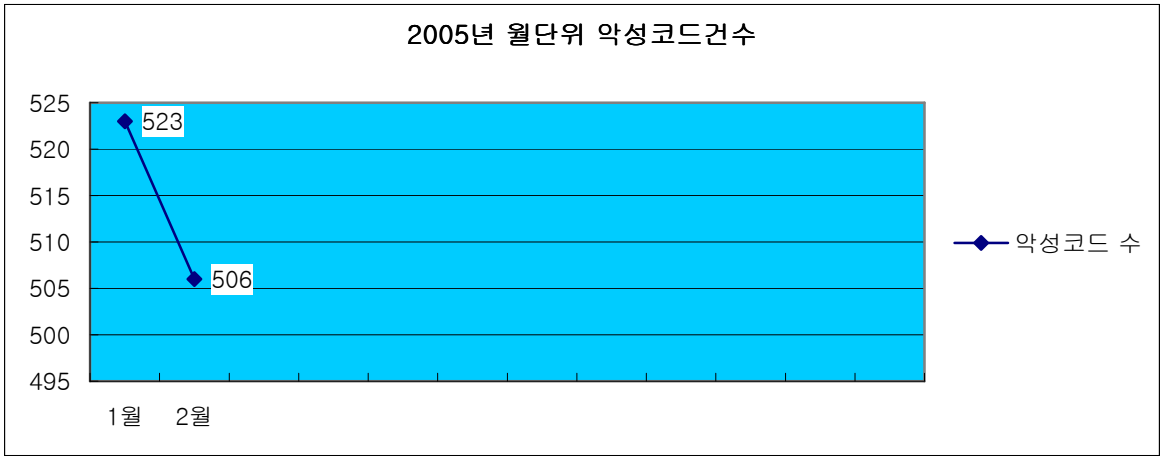
[그림2] 악성코드 Top 10의 전파방법별 현황

1월과 마찬가지로 2월에도 베이글 웜 변형에 의한 많은 피해가 보고되었다. 1월에는 베이글.Z 웜(Win32/Bagle.worm.Z)이 4위를 차지하였고, 2월에는 베이글.AS 웜(Win32/Bagle.worm.AS)이 2위를 차지하며 많은 피해를 주었다. 이처럼 베이글 웜의 변종이 많이 발견되는 이유는 스패머들과 결탁하여 검은 돈을 벌려는 일부 웜 제작자들이 소스가 공개된 베이글 웜의 코드(트로이목마 다운로드 URL, 문자열) 및 실행압축을 변경하여 꾸준히 변형을 만들어 내고 있기 때문이다. 일반적으로 베이글 웜은 이메일을 통해 전파되며 첨부파일을 실행하면 특정 호스트들로부터 트로이목마로 추정되는 파일을 다운로드 하고, 시스템 폴더에 설치된 파일은 TCP/UDP의 특정 포트를 오픈하며 다양한 확장자로부터 메일주소를 수집하여 자체 SMTP를 이용하여 웜 자신을 발송하는 특징이 있다.
이처럼 베이글과 같은 매스메일러 웜에 의한 피해가 여전히 많은 것은 악성코드가 점점 안티바이러스 제품에서 쉽게 진단되지 못하도록 지능화하고 되어가고 있고, 예전에 비해 스팸메일 및 매스메일러에 대한 사용자의 인식이 다소 증가하긴 하였으나 일부 사용자들은 매스메일러에 대한 경각심이 여전히 취약하기 때문으로 보여진다. 예방을 위해서는 사용자들이 의심되는 이메일을 열지 않는 습관을 가지고, 메일서버를 보유한 기업에서는 스팸메일을 차단할 수 있는 스팸필터 제품의 설치와 필터 기능 강화가 필요하다.

네트워크(취약점)를 통해 전파되는 유형은 여전히 전파방법의 일부를 차지하고 있다. 시스템에서 취약점을 원천적으로 제거하지 않으면 감염을 피할 수 없으며, 백신 프로그램으로 진단/치료한 후에도 또다시 재감염되는 증상이 반복되므로 시스템 보안패치를 주기적으로 실시하는 것이 최선의 대책이다.

월별 피해신고 악성코드 건수 현황

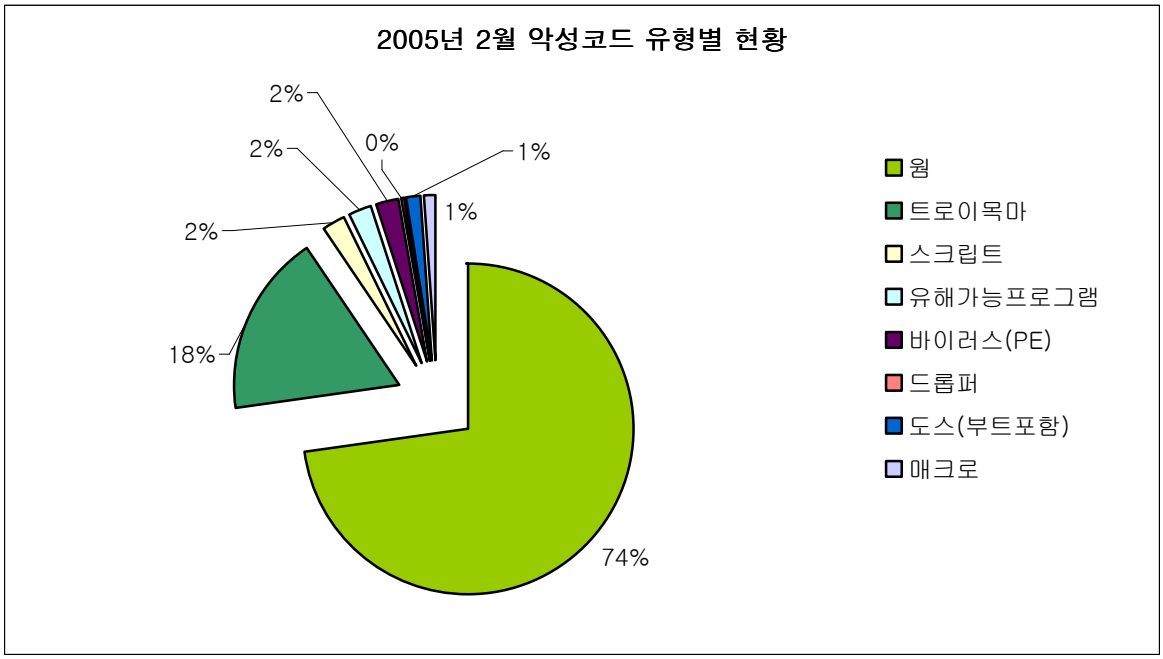
2월에 피해 신고된 악성코드는 506개이다. 이는 지난 1월에 비해 다소 감소한 수치이며, 설연휴 등으로 인해 악성코드들이 실제 활동할 수 있는 시간이 줄어든 것에 비하면 다소 미미한 수치의 감소이다.



[그림3] 2005년 월별 피해신고 악성코드 수

주요 악성코드 현황

악성코드 유형별 현황은 [그림4]와 같다.



[그림4] 악성코드 유형별 현황

다양한 종류와 많은 변형을 가진 웜이 1월에 비해 12%나 증가하며 급격한 증가세를 보였다. 그에 비해 트로이목마는 1월에 비해 8%나 감소하였다. 이는 일부 트로이목마(Agent, Downloader, Ranky, DDOS-Boxed)의 감소가 주요원인으로 분석되었다.

웜이나 트로이목마에 비해 미미한 수준이지만, 여전히 파일 바이러스(PE)에 의한 피해신고가 접수되고 있으며, 이는 바이러스에 취약한 시스템이 여전히 존재하는 것을 반증하고 있다. 여러 원인이 있으나 주로 사용자들이 P2P를 통한 파일 다운로드시 바이러스에 감염된 파일들을 받음으로써, 바이러스 감염이 지속되는 것으로 판단된다. 감염 예방을 위해서는 P2P 사용시 다운로드 한 파일에 대한 백신 검사 실시 및 사용자의 S/W 불법복제에 대한 경각심 고취가 필요하다.

(2) 신종 악성코드 발견 동향

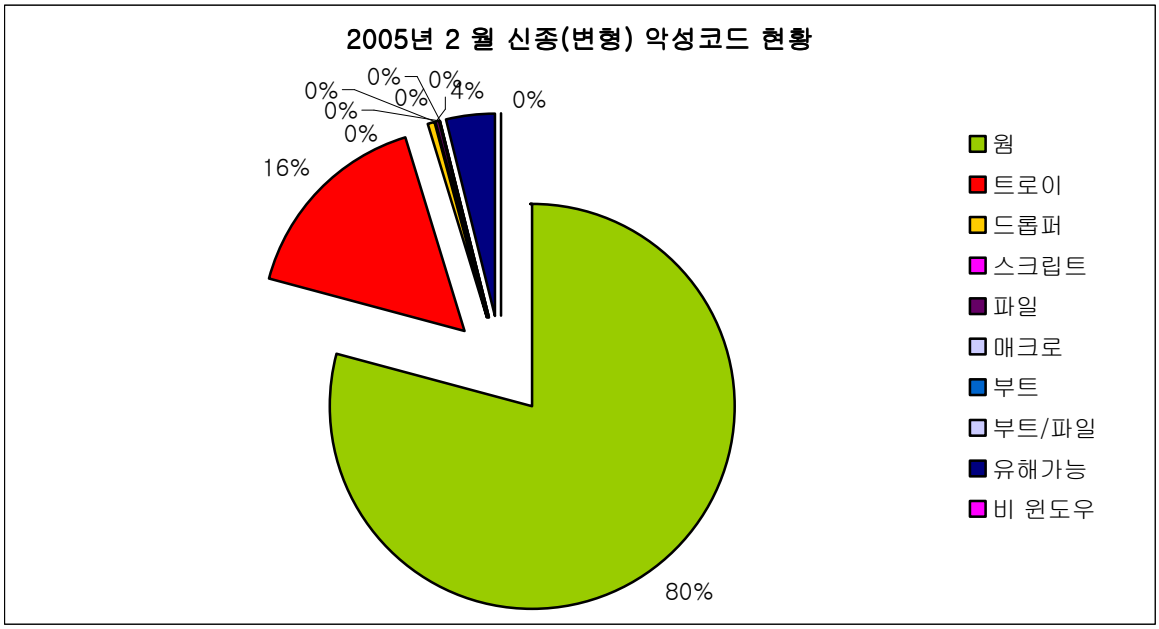
작성자 : 정진성 연구원 (jsjung@ahnlab.com)

2월 한달 동안 접수된 신종(변형) 악성코드의 건수는 [표1], [그림1]과 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
203	41	1	0	1	0	0	0	10	0	256

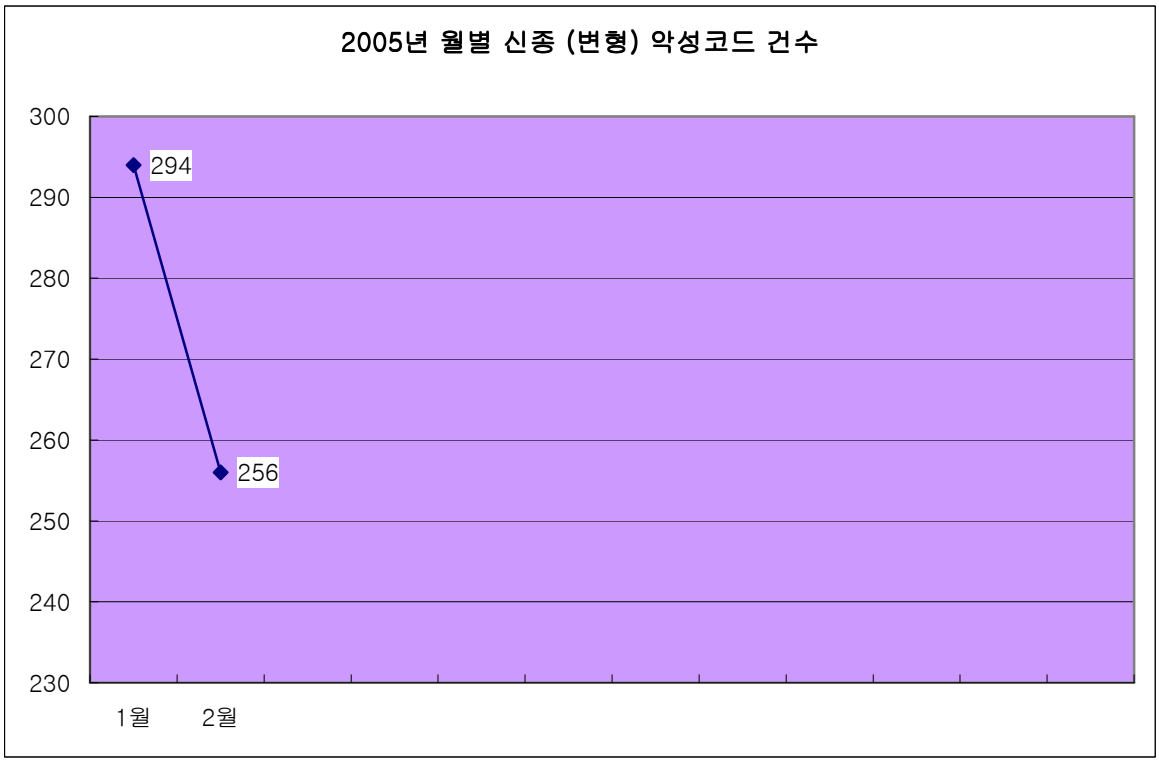
[표1] 2005년 2월 유형별 신종(변형) 악성코드 발견현황

1월과 비교해서 전체적으로 신종(변형)샘플은 약간 줄어 들었다. 특히 트로이목마 샘플이 지난달과 비교해서 큰 폭으로 감소하였다. 그 이유로는 몇몇 특정 트로이목마 샘플 변형들의 발견, 보고가 적었기 때문으로 추정하고 있다. 또한 악성 아이알씨봇(IRCBot) 웜은 지난달과 비교하여 매우 근소한 차이(+1)를 보이고 있어 지난달과 비슷한 양상을 보이고 있다.



[그림1] 2005년 2월 신종 악성코드 발견현황

악성 아이알씨봇은 위에서 언급한 것처럼 지난달과 비교해서 1건의 증가 정도 밖에 보이지 않는다. 악성코드 통계부분은 안티 바이러스 업체들마다 차이가 있을 수 밖에 없는데 여러가지 원인이 있지만 그 중 하나는 신고되는 샘플 종류에 있다. 보통 사용자들은 자신이 사용하는 안티 바이러스 제품에서 진단되지 않는 샘플을 신고한다. 그러므로 안티 바이러스 엔진에서 다양한 실행압축 해제 기능과 휴리스틱 진단 기능을 지원한다면 비이상적으로 확산되는 악성코드가 아닌 이상 접수되는 샘플의 수에 따라 통계의 수치가 달라질 수 있는 것이다.



[그림2] 2005년 월별 신종(변형) 악성코드 발견 현황

[그림2]는 월별 신종(변형) 악성코드 건수를 나타내고 있다. 1월과 비교해서 38건 줄어든 수치를 볼 수 있다. 이 역시 위에서 언급한 것처럼 다음 트로이목마 변형들의 샘플접수가 줄어든 것이 그 원인이라 하겠다.

- Win-Trojan/Agent
- Win-Trojan/DDoS_Boxed
- Win-Trojan/Downloader
- Win-Trojan/Rankey

2월 신종(변형) 악성코드 동향

이번달에도 몇가지 주목할 만한 악성코드들이 있다. 특히 국내를 비롯하여 세계적으로 MSN 메신저 웜인 브로피아 웜(Win32/Bropia.worm)이 급속 확산 되었으며, 이 글을 작성하는 현재에도 변형들이 발견되고 있다. 또 다른 특징으로는 애드웨어를 통한 바이러스 감염보고를 들 수 있다. 이 바이러스가 발견 되기 전까지 애드웨어를 통한 바이러스 감염에 대한 측은 있었지만 실제로 사용자로부터 샘플이 보고된 것은 처음 있는 일이다.

이메일 웜으로는 마이둠 웜(Win32/MyDoom.worm) 변형이 다수 발견되었다. 이 밖에도 기존 은폐형 코드가 아닌 다른 방법을 통해서 자신을 은폐하는 악성 아이알씨봇 웜 변형도 발견 되었으며, 국내 모 기업에서 온라인 게임의 트로이목마를 다운로드하는 바이러스에 대량

감염되는 사고도 보고되었다.

이번 달에 변형 및 새로이 발견, 보고된 악성코드 중 이슈가 있었던 것은 다음들과 같다.

▶ 브로피아 웜(Win32/Bropia.worm)

이 웜은 내부에 악성 아이알씨봇 웜을 포함하고 있다. 따라서 MSN 웜이 악성 아이알씨봇 웜의 전파 매개체가 된 것이다. 이 MSN 웜은 다음의 특이한 2가지 증상을 가지고 있다.

- 감염된 시스템에서 메신저의 현재 내 상태를 변경한다. (로그오프 등…)
- 감염된 시스템의 메인 믹서 볼륨을 초기화한다. (볼륨을 0으로 설정)

브로피아 웜은 1월중순에 첫 발견되었고 2월초에 발견된 변형 중 하나가 국내를 비롯하여 세계적으로 급속히 확산되었다. 다행히 MSN 웜 특성상 급속히 확산되어도 빠른 시간내에 감소하는 경향을 보여주어 우려할 만한 큰 피해가 발생하지는 않았다.

▶ 부베 바이러스(Win32/Bube.4350)

이 바이러스는 애드웨어(스파이웨어)에 의해서 감염되는 첫번째 바이러스로 알려져 있다. 바이러스의 구성은 단순한 편으로, 드롭퍼(Dropper)에 의해서 Explorer.exe만 감염시킨다. 바이러스는 윈도우 파일 보호 기능을 우회하지 않아 다음과 같은 폴더내 Explorer.exe파일을 모두 감염시켜 둔다.

- 윈도우 폴더
- 윈도우₩ServicePackFiles₩i386
- 윈도우 시스템₩dllcache

감염된 Explorer.exe는 특정 호스트로부터 애드웨어를 내려받아 설치하는 증상을 가지고 있다. 최근 들어 악성코드에 의한 애드웨어(스파이웨어)의 설치가 늘어나고 있다. 지금까지는 이메일 웜 또는 악성 아이알씨봇 웜이 애드웨어를 설치해 왔던 반면, 이 바이러스는 바이러스에 의해 애드웨어가 설치되는 첫번째 사례라 할 수 있다. 즉, 부베 바이러스는 애드웨어에 의해 설치되어 감염되고, 다시 또 다른 애드웨어를 다운로드하여 설치하는 형태의 첫번째 사례인 것이다.

▶ 마이둠 웜(Win32/MyDoom.worm) 변형

이번 달에 발견된 마이둠 웜 변형들은 기존의 것과 전파방법, 전파대상 및 증상이 유사한 편이지만, 기존의 마이둠 웜 변형들에서는 볼 수 없었던 다음 증상을 가지고 있으며, 이중 하나는 작년 여름경에 발견된 마이둠 웜에서 보았던 것과 같은 증상이다.

- int 0x2E를 이용한 커널모드 진입
- 가변적인 MIME 형식

유저모드에서 커널모드로의 진입 후 증상은 웜이 메일을 발송할 때 보여진다. 즉, 웜은 메일 발송을 위해서 시스템 기능을 사용하는 것이다. 이는 추정컨대 어플리케이션 레벨 방화벽의

TCP/IP 연결횟수 제한 등을 우회하려는 목적으로 보인다. 또 다른 증상은 작년에 발견된 마이둠에서 보였던 증상을 재현한 것으로, 가변적인 (첨부파일의) MIME 길이를 생성하는 것이다. 이는 0x0D, 0x0A 값을 불규칙적으로 집어 넣어 MIME 길이가 가변적이 된다. 이렇게 될 경우 시그니쳐 기반의 패킷 탐지 제품은 효율적으로 웜을 차단하기 어렵게 된다. 하지만 이러한 기법들이 이전에 알려진 형태여서 현재는 차단이 가능하다.

▶ 은폐형 악성 아이알씨봇(IRCBot) 웜

은폐형 악성 아이알씨봇 웜은 이미 작년 3월에 처음 알려졌다. 하지만 이번에 발견된 형태는 기존처럼 은폐형 코드를 내부에 가진 것이 아니라 별도의 커널 드라이버로 구성되어 있다. 그러나 이 커널 드라이버는 이미 작년에 V3 엔진에 추가된 형태와 동일하여 웜이 정상적으로 은폐되는데 그리 큰 효과를 주지는 못했다.

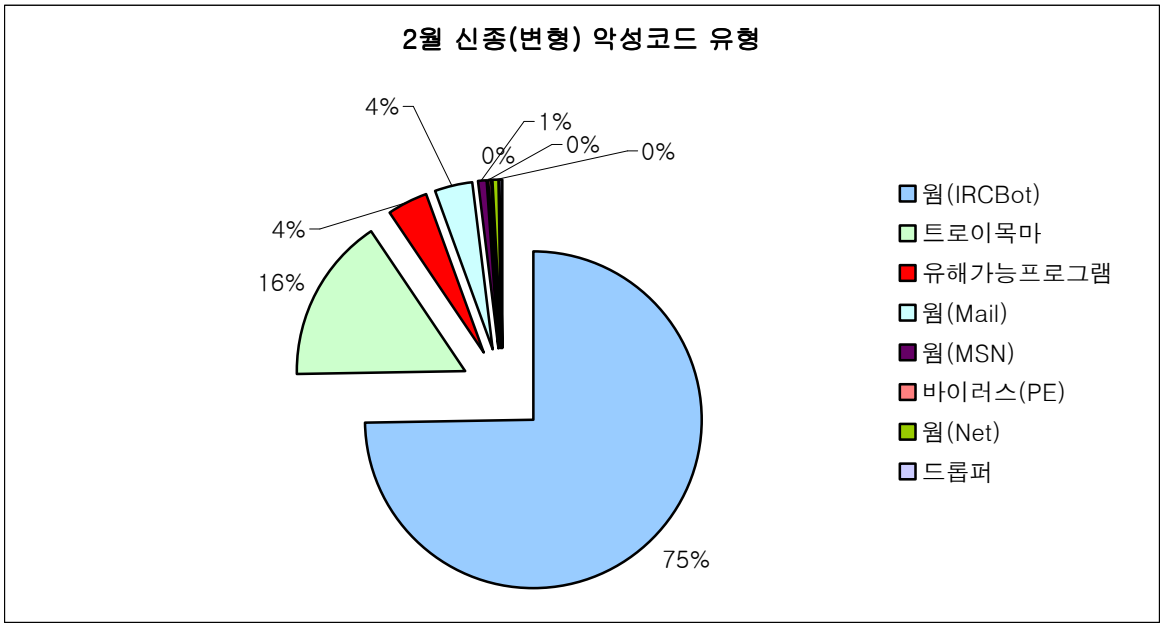
▶ 마이톱 웜(Win32/Mytob.worm)

다수의 변형들을 가지고 있는 이 웜은 악성 아이알씨봇 웜 증상을 가지고 있다. 일반적인 이메일 웜이기도 하지만 윈도우 취약점(MS04-011)을 이용하여 전파될 수도 있으며 특정 아이알씨봇 서버에 접속하여 마스터의 명령을 받을 수도 있도록 되어 있다. 이메일 웜이 이러한 증상을 가진 것으로는 처음 보고된 형태이다.

▶ 루키드 바이러스(Win32/Looked.67072)

이 윈도우 파일 바이러스는 국내 모 기업에서 다수 감염보고 되었다. 꽤 큰 크기를 가진 이 바이러스는 볼랜드 델파이로 제작되었다. 파일감염 증상 이외에 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마를 내려받아 실행하는 증상을 가지고 있는데, 이 증상을 수행하는 트로이목마는 DLL 파일이며 Explorer.exe에 Injection되어 동작된다. 바이러스는 암호가 없는 관리목적 공유폴더를 통해서도 전파 될 수 있으며 특이하게 윈도우의 특정폴더 내 파일들은 감염대상에서 제외되어 사용자는 감염여부를 쉽게 눈치채지 못 할 수 도 있다.

다음은 2월에 발견된 악성코드들을 유형별로 분류한 것이다.



[그림3] 2월 신종 (변형) 악성코드 유형별 현황

[그림3]의 악성코드 유형별 분류에서는 '바이러스(PE)'를 표시해두고 있는데 이것은 악성코드 유형중에 하나인 바이러스 부분에서, 윈도우 실행파일(PE 형식)을 대상으로 감염되는 형태를 말한다. 트로이목마의 비율이 악성 아이알씨봇 웜에 비해서 상대적으로 줄어든 것을 알 수 있다. 유해가능 프로그램들로는 다음과 같은 형태가 있었다.

- 원격 접속 프로그램류
- FTP 데몬류

이들은 유해가능 프로그램들 중 가장 많은 비율을 차지하는 형태이다. 정상적으로 사용될 때는 매우 편리한 프로그램이지만 사용자가 의도에 따라서 일부 설정만 변경한다면 충분히 악용될 수 있는 프로그램들이다.

악성코드 제작지별 현황은 1월과 마찬가지로 2월 역시 모두 외산이으로, 지난달과 동일한 양상을 보였다.

II. 2월 AhnLab 스파이웨어 동향

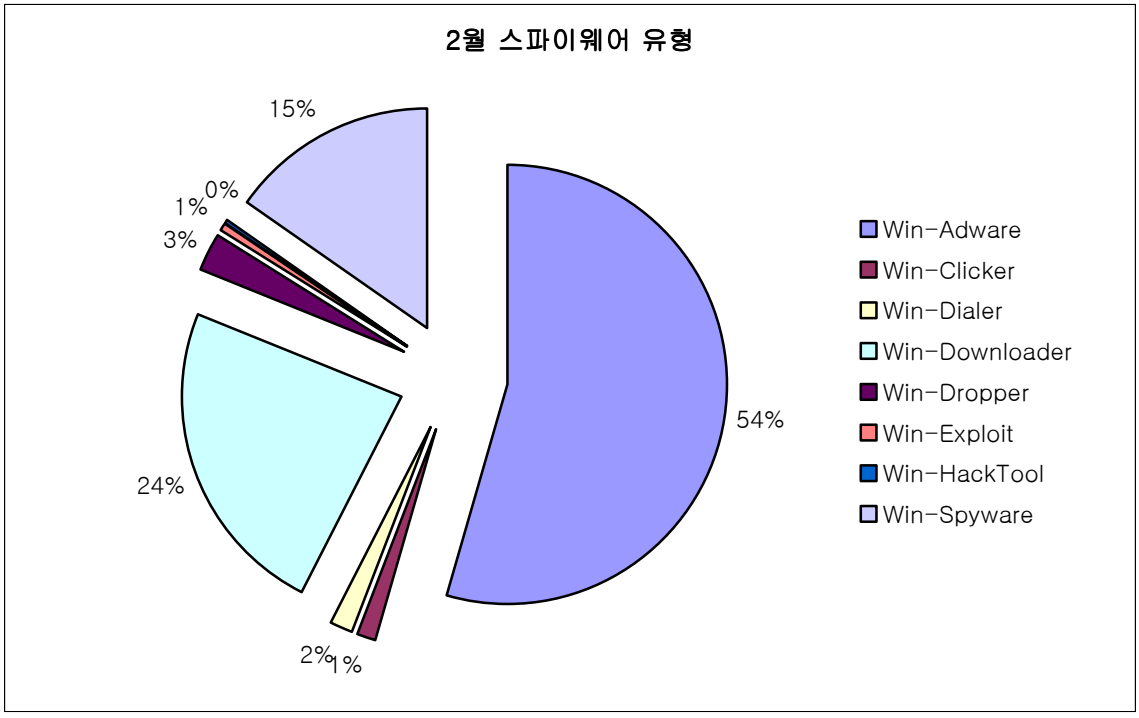
작성자 : 장혜윤 연구원(planet@ahnlab.com)

2월 한달 동안 접수된 스파이웨어[1] 건수는 [표1], [그림1]과 같다.

Adware	Clicker	Dialer	Downloader	Dropper	Exploit	HackTool	Spyware[2]	합계
380	9	12	166	19	4	1	107	698

[표1] 2005년 2월 유형별 발견현황

2월 한달동안 접수된 유형별 현황에서 볼 수 있듯이 Win-Adware, Win-Downloader, Win-Spyware가 주류를 이루고 있다.



[그림1] 2월 스파이웨어 유형별 현황

상위 10위권 안에 Win-Downloader가 5개 순위을 차지하고 있다. 이는 자체 전파기능없이 짧은 시간에 많은 스파이웨어를 배포하기 위해서 아직까지는 다운로더를 이용해서 원격지 서버로부터 여러 개의 스파이웨어를 받아 설치하는 방법을 사용하기 때문이다. 또한 원격지

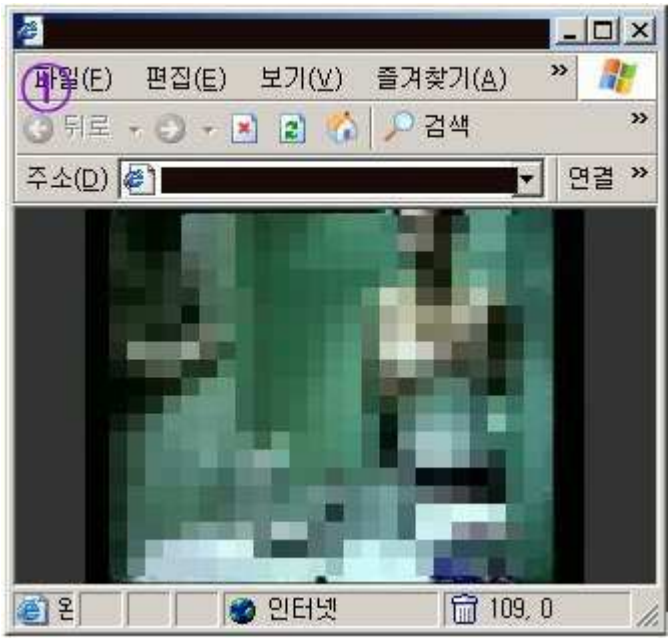
[1] "사용자가 설치 사실을 모르거나 정확한 용도를 모르고 설치하여 사용자를 불편하게 하거나 사생활을 침해할 수 있는 프로그램 및 데이터"를 말한다. Win-Adware, Win-Spyware, Win-Downloader 등 증상 및 파일 속성에 따라 분류된 진단 카테고리를 총칭하여 스파이웨어라 한다.

[2] 여기서 스파이웨어란 증상 및 파일 속성에 따른 진단명이다.

에 어떠한 파일이 있느냐에 따라 설치되는 스파이웨어 수가 틀려진다. 예로, 다운로더가 다운로더를 받아오는 경우를 생각해 보면 알 수 있듯이 적게는 1MB부터 많게는 수십 MB의 스파이웨어를 설치하게 된다. 이와 같은 경우 사용중인 시스템에 오류가 발생, 성능 저하로 인하여 사용하지 못하거나 수 많은 팝업 광고 창들이 발생하게 된다.
그러나 국내에는 아직까지 다운로더 기법을 사용하는 스파이웨어가 많지 않다. 거의 대부분 포털사이트 광고를 위해 시작페이지를 고정하거나, 바탕화면 등에 인터넷 바로가기 생성하거나, 특정 키워드 입력시 특정 사이트로 접속하는 방법을 사용하는 경우가 많은 반면, 외국은 국내와는 달리 다운로더 기법을 많이 사용하고 있으며, 스텔스(Stealth) 기법을 사용하여 설치된 파일의 일부분을 숨기는 등 국내와는 기술적인 차이를 보이고 있다. 이로 인해 외국 사이트에서 설치된 스파이웨어는 일반 사용자 눈으로 의심되는 파일 등을 찾기가 쉽지 않다.

최근 국내에서는 기존 배포 방식과는 달리 플래쉬 파일(*.Swf)을 이용하여 배포하는 기법이 발견되었다. 인터넷 웹 써핑을 하다보면 어느 웹페이지나 시각적 효과를 극대화하기 위해 플래쉬를 하나 이상 사용하고 있다. 특히 국내에는 카페 형식의 커뮤니티가 활성화되어 있는 점을 이용하여, 플래쉬 파일을 이용한 스파이웨어 설치 사례가 접수되었다.

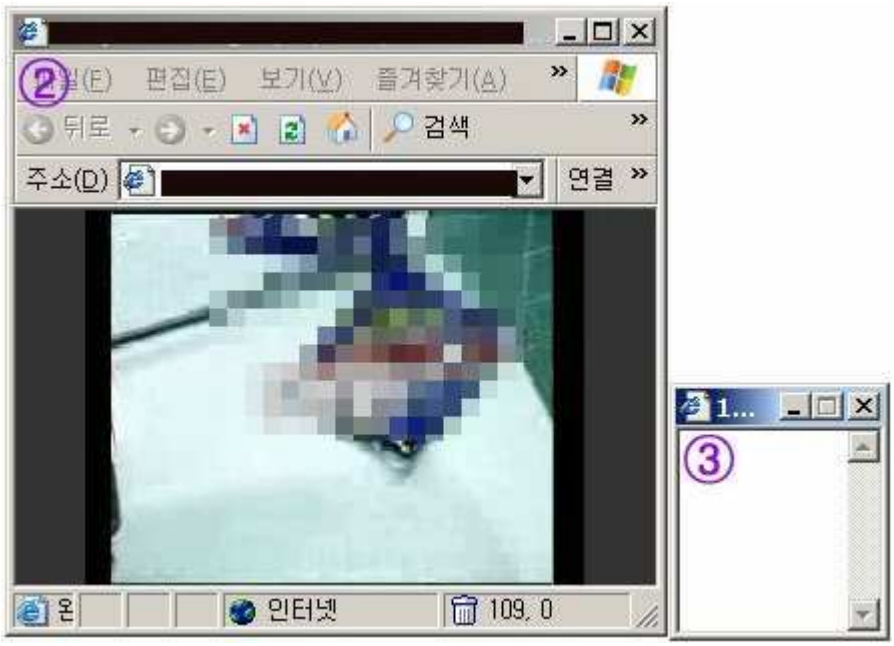
그 방법을 살펴보면 다음과 같다. 참고로, 플래쉬 화면은 특정 제품 광고 플래쉬인 관계로 임의로 모자이크 처리를 하였다.



[그림2] 정상적인 광고 플래쉬

① 정상적인 광고 플래쉬

플래쉬 파일을 이용하여 스파이웨어를 설치할 경우, [그림2]와 같이 처음에는 정상적인 광고 플래쉬를 보여준다.



[그림3] 원격지 파일 로드 및 팝업

② 설치할 Spyware Codebase 정보를 담고 있는 Html 파일을 불러올 플래쉬

[그림3]의 ②와 같이 정상적인 플래쉬 파일의 마지막 플레임에서 loadVariables 액션 스크립트를 실행하여 원격지에 있는 또 다른 플래쉬 파일을 데이터로 읽어 들인다

③ Codebase 정보를 담고 있는 Html

원격지에서 읽어 들인 플래쉬 파일은 getURL을 이용해서 [그림3]의 ③번 Html 파일을 팝업시키게 되고, Html 파일은 [그림4]와 같이 스파이웨어 ActiveX를 설치하게 되는 것이다.

[그림4] ActiveX 설치

아직까지 외국에 비해 국내 스파이웨어 기술은 걸음마 단계이지만, 점점 발전하고 있다는 것을 알 수 있다.

III. 2월 시큐리티 동향

작성자 : 김지훈 주임연구원(smallj@ahnlab.com)

이번 2월호에서는 최근 이슈가 된 MSN 메신저의 보안 위협, 다국어 도메인 이름 (IDN) 스푸핑 위협, 인터넷 사이트 보안장치 마련 시급성 등에 대해 얘기해 보기로 하겠다.

MSN 메신저의 보안 위협

지난 2월 마이크로소프트사는 12개의 보안패치를 발표하였다. 개념증명코드(Proof of Code)가 공개된 Office의 취약점으로 인한 원격 코드 실행 문제점(MS05-005), PNG 처리 취약점으로 인한 원격 코드 실행 문제점(MS05-009)을 포함한 '긴급' 수준의 8개, ASP .Net의 취약점으로 인한 인증 우회 문제점 (MS05-004)을 포함한 '중요' 수준의 3개, Windows SharePoint Sevices 및 SharePoint Team Serivces의 취약점으로 인한 사이트 간 스크립팅 및 스푸핑 침입 문제점(MS05-006)을 포함한 '보통' 수준의 1개이다.

▶ PNG 처리 취약점으로 인한 원격 코드 실행 문제점 (MS05-009)

이번 취약점은 PNG 이미지 포맷의 파싱을 이용한 것으로 2월 8일 공식적으로 보안패치를 제공했고, 2월 9일 관련한 상세정보와 공격코드가 공개되었다. 취약점이 발표된 지 하루 만에 공격코드가 공개되었을 만큼 이 취약점은 악성코드 제작에 사용될 가능성이 높았으며, 이로 인해 많은 피해가 발생할 확률이 매우 높았다. 한 보안업체에서 발표한 이 취약점 상세정보가 자칫 공격자들에게 이용당할 수도 있다고 우려한 마이크로소프트는 MSN 메신저를 강제로 보안업데이트 하도록 하는 등 발빠른 대응을 하였고, 이로 인해 이번 MSN 메신저의 PNG 취약점을 이용한 공격은 불가능하게 되었다.

MSN, 네이트온 등의 범용 메신저는 자신의 고객 및 친구 등의 인맥을 관리하고 사내 각 부서 및 직원 간의 업무연락 수단으로 광범위하게 사용되고 있다. 따라서, 메신저 소프트웨어의 결함은 기업 보안에 심각한 위협으로 이어질 수 있음을 상기하고, 기업형 메신저 솔루션의 도입, 보안 장비를 이용한 포트 차단 등의 보안정책을 강화하도록 한다.

다국어 도메인 이름 (IDN) 스푸핑 위협

Secunia (http://secunia.com/)는 Eric Johanson이 확인한 동형 이의어(homograph) 공격을 이용하는 다국어 도메인 이름(IDN) 스푸핑 테스트 결과에 대한 보안 권고문을 발표하였다.

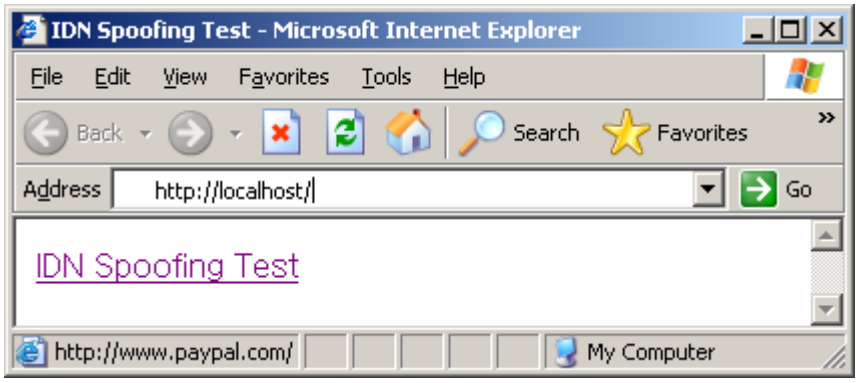
'다국어 도메인 이름'을 지원하는 대부분의 브라우저들이 이 취약점에 영향을 받는 것으로 보고되었다. 인터넷 익스플로러는 기본적으로 '다국어 도메인 이름'을 지원하지 않지만, IDN 플러그인 형태로 지원될 때는 영향을 받게 된다.

동형이의어 공격이란 유니코드상의 비슷해 보이는 문자를 이용하여 사용자로 하여금 정상적인 URL로 착각하게 만드는 방법이다.

다음은 정상적인 www.paypal.com 대신 키릴문자 a를 사용하는 www.paypal.com으로 이동하는 HTML 코드이다.

```
<a href="http://www.payp&#1072;l.com/">
IDN Spoofing Test</a>
```

이 코드를 웹 브라우저 상에서 실행한 화면이 [그림1]이며, 이는 영문자 a를 키릴 문자 a로 대체하였을 경우 문자의 모양이 비슷하기 때문에 사용자는 정상적인 www.paypal.com으로 이동하는 것으로 혼동하기 쉽다.



[그림1] 다국어 도메인 이름 스푸핑 화면

즉, 이를 이용하면 공격자가 악의적인 페이지를 만들고, 사용자로 하여금 웹페이지의 URL을 클릭하여 악의적인 페이지로 유도할 수 있다. 사용자는 자신의 개인 정보를 아무런 인지 없이 악의적인 페이지를 통해 입력하게 되며 이때 입력된 개인 정보가 공격자에게 쉽게 유출된다. 이러한 스푸핑 공격의 피해로부터 벗어나기 위한 가장 확실한 방법은 자신이 원하는 사이트에 방문하고자 할 때 특정 웹페이지의 URL링크를 클릭하지 않고 직접 URL 입력창에 직접 입력하는 방법 등이 있다.

최근 발표된 모질라 파이어폭스 1.0.1, 모질라 1.7.6, 모질라 베타 1에서는 이 취약점의 영향을 최소화하기 위해 IDN 기능은 지원하는 대신에 주소창엔 퓨니코드[1]의 형태로 표시되며 숨겨진 환경설정을 통해 이를 중지할 수 있다.

인터넷 사이트 보안장치 마련 시급

지난 1월말 국내의 한 인터넷쇼핑몰이 상품의 판매가격이 해커에 의해 1원, 2원, 3원으로 바뀌어 표시된 사건이 발생하였다. 이때 접수된 허위 주문이 무려 최소 수억원에 이르러 기업에 막대한 손실로 이어질 수 있었던 사고였다.

---

[1] 퓨니코드 (Punycode)
다국어 도메인을 인코딩하는 국제 표준으로, 문자 숫자 하이픈(-)의 3가지 코드로 주소를 조합해 다국어 도메인을 부호화한다.

홈페이지 변조 피해 사례는 사회적인 이슈를 반영하여 자신의 의지를 드러내기 위해 행해지는 경우도 많다. 최근 중국 게임 시장에 진출을 추진하던 국내 온라인 게임 업체의 홈페이지가 중국 해커 집단에 의해 변조되었고 중국 국기와 함께 한국 온라인 게임에 대한 중국의 견제를 엿볼 수 있는 경고성 문구가 포함돼 있었다. 반미 성향이 강한 아랍 계의 해커 집단에 의해 국내 인터넷 사이트의 홈페이지가 변조된 것 또한 이라크 파병국인 우리의 상황에 비추어 볼 때 사회적인 이슈에 의한 '악의적인' 해킹 피해로 파악해 볼 수 있다.

앞으로도 '자기과시'나 '악의적인 목적'의 형태로 국내외 기업에 대한 해킹 시도가 꾸준히 계속될 것이고 그로 인한 개인 및 기업의 정보 유출, 이미지 실추, 금전적 손실은 날로 증대될 것이다. 따라서, 중요한 정보가 관리되고 금전 거래가 이뤄지는 인터넷 사이트의 경우 의무적으로 보안시스템을 갖추도록 하는 내용의 법적 장치가 조속히 마련되어야 할 것이다.

Ⅳ. 2월 세계 악성코드 동향

2005년 2월 전세계 악성코드 동향에서 공통적인 현상은 메일을 이용하여 전파되는 매스메일러가 가장 많이 확산되는 것이다. 그러나 확산되고 있는 악성코드의 종류는 지역별로 차이를 보이고 있어, 한국과 일본의 경우 2월 한달동안 넷스카이 웜이 다른 매스메일러에 비해 월등하게 많은 감염 피해를 보이는 것에 비해 유럽의 경우 자피 웜이 가장 많이 확산되고 있는 것으로 나타났다.

매스메일러의 전파와 더불어 특이할 만한 사건은 중국에서 브로피아 웜에 의한 피해가 넷스카이 웜을 능가할 정도로 많이 발생한 것이다. 브로피아 웜은 2005년 1월 최초로 발견된 이후 여러 변형이 추가로 발견되고 있는 메신저를 통해 전파되는 웜이다. 주변 국가인 한국이나 일본의 경우도 브로피아 웜에 의한 피해가 있긴 하였지만, 중국의 피해에 비하면 미약한 수준이었다.

(1) 일본의 악성코드 동향

작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

2005년 2월 일본에서 가장 많이 전파된 악성코드는 넷스카이 웜(Win32/Netsky.worm)으로 전반적으로 매스메일러가 많이 확산되고 있는 상황은 전월과 비교하였을 때 크게 차이가 없다. 일본의 악성코드 동향에서 주요한 변화 중의 하나는 전월에 비해서 베이글 웜(Win32/Bagle.worm)과 마이둠 웜(Win32/MyDoom.worm)의 감염 피해 건수가 증가한 것인데, 이는 2월에 발생하여 확산된 새로운 변형들의 영향으로 보인다. 이외에도 최근 확산된 브로피아 웜과 같이 메신저를 통해 전파되는 웜이 일본에서 발견된 점도 주목할만 하다.

일본 유행 악성코드 유형별 발생현황

[표1]은 2005년 2월 일본에서 감염 신고된 악성코드의 통계를 나타낸 것이다. 표에서 알 수 있는 것처럼 넷스카이 웜의 감염 피해가 가장 많은 건수를 차지하고 있다. 넷스카이 웜에 대한 감염 피해는 전월과 비교하여 크게 변화가 없다.

또한 표에는 나오지 않았지만 2월에 새롭게 발견된 마이핍 웜(Win32/Myfip.worm)이나 브로피아 웜(Win32/Bropia.worm)과 같이 새롭게 발견된 악성코드에 의한 감염 피해도 접수된 것으로 나타났다.

브로피아 웜의 경우 마이크로소프트사의 MSN 메신저를 통해서 전파되는 악성코드로서, 처음 발견된 이후 현재까지도 여러 변형이 발생하여 유포되고 있다. 메일을 통해 전파되는 웜과 비교해서 소멸 주기가 짧은 메신저 웜의 특성상 지속적인 피해를 유발하지는 않지만 메신저에 제공된 파일을 다운로드하여 실행하거나 링크를 클릭할 경우 감염되고 메신저에 등록된 모든 사용자가 감염 대상이 되므로 단기간에 많은 사용자에게 전파되어 피해를 입힐 수 있다. 전체 자료에서 볼 때 일본에서는 브로피아 웜으로 인한 감염 피해가 많이 보고되지

않은 것으로 나와있으나 이러한 전파 형태를 가진 웜에 의한 감염 피해가 심각해질 수 있다.

Window/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Netsky	1,064	Xm/Laroux	13	VBS/Redlof	74
W32/Bagle	458	XF/Sic	3	VBS/Loveletter	9
W32/Mydoom	333	WM/Ethan	2	VBS/Fortnight	5
W32/Bagz	230	W97M/Opey	2	VBS/Soraci	2
W32/Klez	217	W97M/Tristate	1	VBS/Gaggle	1
W32/Zafi	215	WM/Cap	1	VBS/Gedza	1

[표1] 악성코드 피해 신고 현황 (출처: 일본 IPA)

악성코드의 감염 경로별 통계

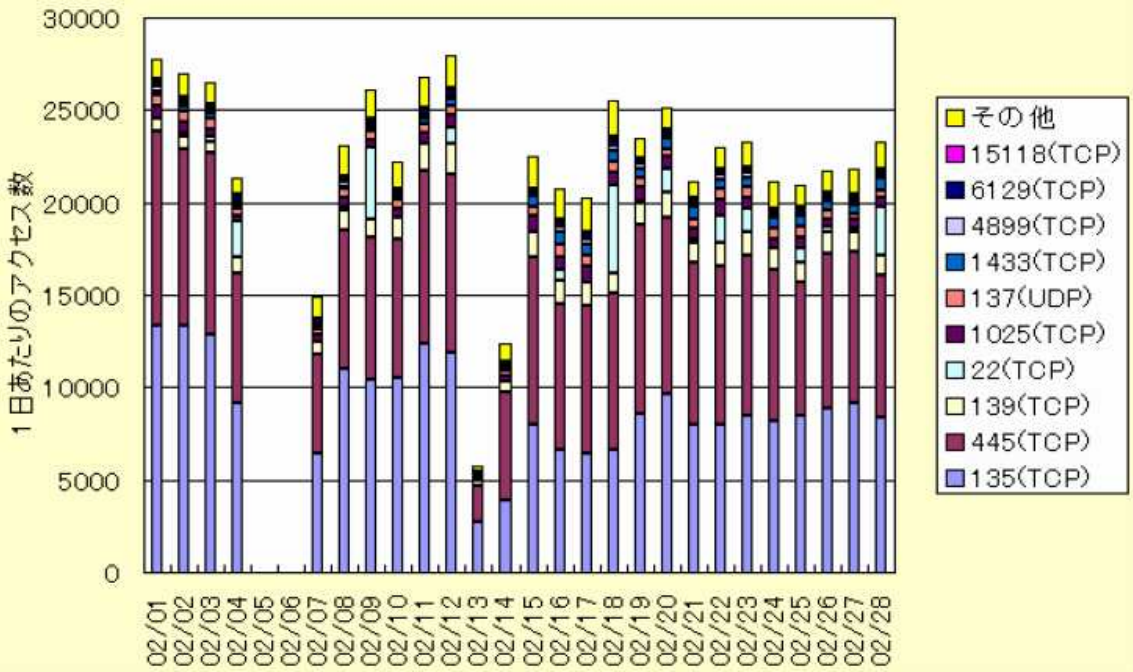
일본에서 가장 많은 피해를 입히는 것은 메일과 네트워크를 통해 전파되는 웜인 것으로 나타났다. 아래의 [표2]는 악성코드의 유형별 피해 건수를 나타낸 것이다. 표에서 나타난 것처럼 메일을 통해 감염된 경우가 거의 대부분임을 알 수 있는데 메일을 통해 전파되는 웜의 경우 사용자가 메일 사용에 조금만 주의를 기울이면 얼마든지 감염 예방이 가능하기 때문에 피해 예방을 위한 사용자의 주의가 필요하다.

감염경로	피해 건수					
	2005년 2월		2005년 1월		2004년 2월	
메일	4,111	99.1%	4,819	98.7%	1,654	95.4%
외부의 모체	0	0%	5	0.1%	19	1.1%
다운로드	0	0%	2	0%	17	1.0%
네트워크	39	0.9%	50	1.1%	34	2.0%
기타	0	0%	4	0.1%	9	0.5%

[표2] 악성코드 감염 경로 통계(출처: 일본 IPA)

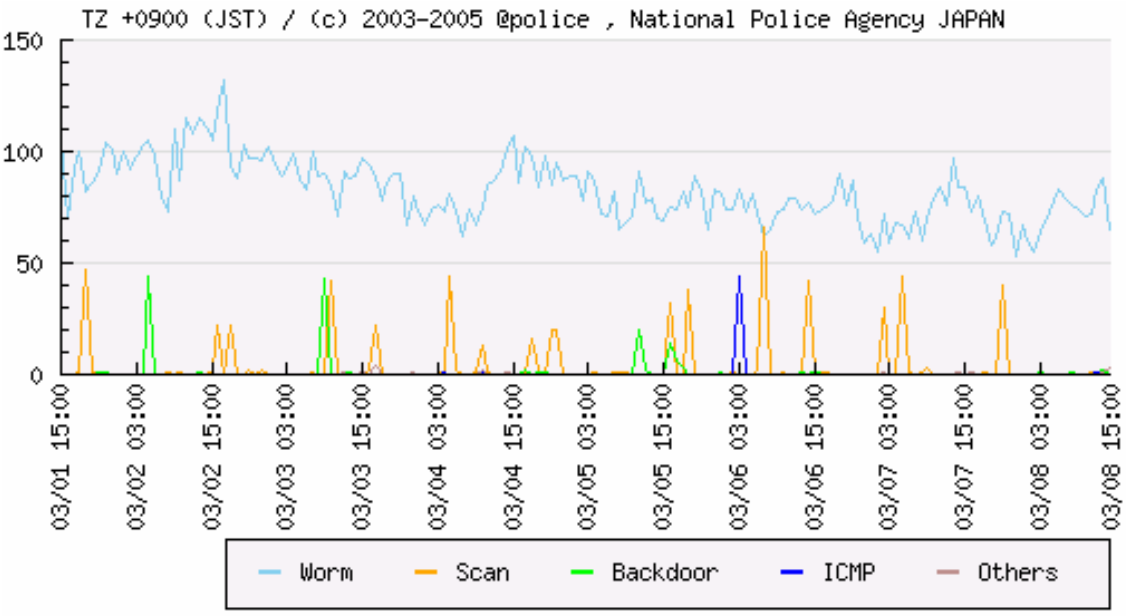
일본 네트워크 트래픽 현황

[그림3]은 일본의 주요 인터넷 거점에 대한 네트워크 트래픽을 통계로 나타낸 것이다. TCP 135 포트와 TCP 445 포트를 이용하는 트래픽이 매우 많은 것을 알 수 있다. 두 포트들은 윈도우 OS에서 사용되는 포트들이고 PC간 통신을 할 때 인증을 위해 사용되는 등 사용 빈도도 매우 높기 때문에 해당 포트들을 이용한 트래픽이 적지는 않으나, 최근 유행하는 아이알씨봇과 같은 웜들에서 이러한 포트들을 통한 공격을 시도하는 경우가 많이 발생하고 있다.



[그림3] 네트워크 트래픽 현황(출처: 일본 IPA)

[그림4]는 주요 네트워크 거점에 대한 공격패턴을 도표로 나타낸 것이다. 표에 나타난 것처럼 웜에 의한 공격이 가장 많은 양을 차지하고 있는 것을 알 수 있다. 인터넷을 이용하여 무작위적으로 대상 IP를 정하고 다수의 IP에 공격을 시도하는 웜의 특성으로 미루어볼 때 이러한 그래프는 당연한 결과라고 할 수 있다. 웜이 사용하는 공격 패턴은 누구라도 공격의 대상이 될 수 있다는 것을 의미하고 표에서 보는 것처럼 실제로도 많은 공격시도가 이루어지고 있기 때문에 감염으로 인한 피해 예방을 위한 대책 마련이 필요하다.



[그림4] 주요 네트워크 거점 공격패턴(출처: 일본 경찰청)

(2) 중국의 악성코드 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

2월 중국의 악성코드 피해 특징으로는 브로피아 웜(Win32/Bropia.worm)에 의해 많은 피해가 있었다는 것이다. 2005년 2월 중국 악성코드는 어떠한 모습들을 보이고 있는지 자세히 살펴보도록 하자.

악성코드 TOP 5

순위 변화	순위	CNCVERC
New	1	Worm_Bropia.F
↓ 1	2	Worm_Netsky.D
-	3	Worm_Bbeagle.J
-	4	Worm_AgoBot

[표1] 2005년 2월 CNCVERC 악성코드 TOP 4

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

[표1]은 중국 컴퓨터바이러스긴급대응센터(이하 CNCVERC)의 악성코드 TOP5이다. 중국 로컬 백신 업체인 라이징은 2주간이나 지속되었던 춘절(설날) 연휴로 인해 통계가 집계되지 않은 것으로 보인다. CNCVERC의 동향을 살펴 볼 경우 가장 큰 변화는 브로피아 웜(Worm_Bropia.F, V3진단명 Win32/Bropia.worm.188928)이 단기간에 1위로 올라섰다는 점이다. 이로인해 몇달째 1위를 차지하고 있던 넷스카이 웜(Worm_Netsky.D, V3진단명 Win32/Netsky.worm)은 브로피아 웜의 영향으로 인해 한자리 하락한 2위를 차지하고 있으며 러브게이트 웜(Worm_Lovegate.C, V3진단명 Win32/LovGate.worm)은 이번 달 순위에서 빠질 정도로 완전히 제외되었다. 그 외 3위와 4위는 지난 달과 비교하여 동일한 면을 보이고 있다.

신종 악성코드 동향

2월 중국의 신종 악성코드 동향 중 가장 큰 영향을 끼친 것은 앞서 언급했던 브로피아 웜이다. 이 웜은 감염된 시스템의 MSN 메신저에 등록된 친구목록의 모든 사람들에게 웜을 전달하는 확산 방법으로 인해 감염과 동시에 비교적 쉽게 이상 증상을 많은 사람들이 눈치 챌 수 있었다. 그러나 웜을 실행할 경우에는 웜 내부에 포함되어 있는 악성 아이알씨봇 웜이 설치되어, 이후에는 브로피아 웜에 의한 감염 보다는 악성 아이알씨봇 웜에 의한 공격과 피해가 더 우려되었다. 이러한 피해는 한국의 상황과 마찬가지로 중국 전역에서 MSN 메신저를 사용하는 사용자들로부터 많은 신고가 있으며 안철수연구소의 중국법인으로도 많은 신고와 문의가 있었던 것으로 보고되었다.

2월 한달 동안 안철수연구소의 중국 법인으로 신고된 악성코드들을 형태별로 분류하면 다음과 같이 구분된다.

순위	형태	퍼센트
1	Trojan	52 %
2	Backdoor	15.6 %
3	Dropper	15.6 %

[표2] 2월 AhnLab 중국법인으로 신고된 악성코드 형태별 분포

[표2]의 1위에서 3위까지는 모두 대분류상으로 트로이목마로 볼 수 있다. 이러한 트로이목마 류가 전체의 80%를 넘을 정도로 많은 양을 차지하고 있는 것이다. 그리고 웜은 총 5건 접수가 되었으나 이 중에서 1건은 리눅스 플랫폼에서 활동하는 스크립트 형태이다. 이러한 전체적인 분류로 보아서는 2월 접수된 신종 악성코드는 전통적으로 트로이목마가 많은 중국답게 트로이목마가 다수를 차지한 것으로 볼 수 있다.

브로피아 웜과 같이 인터넷 메시징 프로그램을 통해서 전파되는 악성코드가 올해 들어 자주 발견되는 것은 전세계적으로 많은 사람들이 인터넷 메시징 프로그램의 활용 빈도가 높다는 것을 보여주는 실례이다. 그러나 이에 반해 아직까지 많은 기업들과 개인 사용자들은 인터넷 메시징 프로그램의 보안에 대해서 심각한 수준으로 고민하고 있지 않은 것으로 보인다. 특히 손쉽게 파일 전송이 가능하다는 점은 오히려 기업 중요 정보 자산이 쉽게 외부로 유출될 수도 있다는 것임을 명심하여야 한다. 당분간 인터넷 메시징 프로그램을 이용하여 전파되는 악성코드의 감염은 계속될 것으로 예상되므로 주의가 필요하다.

(3) 세계 악성코드 동향

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

영국의 안티 바이러스 업체인 소포스(Sophos)의 2005년 2월 보고에 따르면 1위는 자피.D 웜 (W32/Zafi-D, V3진단명 Win32/Zafi.worm.11745)으로 30.8 %를 차지하고 있다. 이전에 발견된 변형인 자피.B 웜(W32/Zafi-B, V3진단명 Win32/Zafi.worm.12800)도 3위를 차지하고 있다. 자피 웜 변형이 한국을 포함한 아시아 지역에는 많은 보고가 되지 않은 것에 반해 유럽 지역에는 자피 웜 변형이 많이 확산된 것으로 볼 수 있다. 새롭게 진입한 악성코드로는 베이글 변형과 소버 변형(W32/Sober-K, V3진단명 Win32/Sober.worm.51688)이 있다. 베이글 변형과 소버 변형은 한국에서는 적은 보고가 되었거나 보고가 없었다.

러시아의 안티 바이러스 업체인 캐스퍼스키 연구소(Kaspersky Lab) 보고에 따르면 1위는 자피.B 웜이며 3위는 자피.D 웜으로, 소포스와는 순위가 반대이지만 역시 자피 웜 변형으로 인한 피해가 높은 순위를 차지하고 있다.

나머지 넷스카이 변형, 마이둠 변형의 확산은 전 세계적으로 동일한 상황으로 보인다

V. 이달의 ASEC 컬럼

(1) 부베로 본 애드웨어의 발전

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

부베 바이러스 등장

2005년 1월 중순 윈도우 실행 파일을 감염 시키는 바이러스로 진화(?)된 애드웨어가 등장하였다. 부베 바이러스(Win32/Bube.4350)로 불리는 이 바이러스는 감염된 컴퓨터에 사용자 동의 없이 인터넷에서 프로그램을 다운로드 해 실행하거나 레지스트리를 변경하는 기능을 가지고 있다. 부베 바이러스는 엄밀히 말하면 바이러스로 보기는 어렵다. 바이러스는 자신을 다른 파일에 감염시킬 수 있는 코드를 포함하고 있어야 하지만 부베 바이러스는 자신이 가지고 있던 일부 코드를 EXPLORER.EXE에 복사하고 감염된 EXPLORER.EXE 파일은 다른 파일을 감염시키지는 않는다. 따라서, 바이러스를 어떻게 정의하느냐에 따라 바이러스나 트로이목마가 될 수 있다. 실제로 안티 바이러스 업체에 따라 부베 바이러스를 바이러스로 분류한 곳도 있고 트로이목마로 분류한 곳도 있다. 과거에 바이러스가 로컬 시스템에서 단순히 실행 파일을 감염하는 행동에 국한하였으나 현재는 로컬 시스템 감염과 다른 악성코드나 애드웨어에서 인터넷을 통한 파일 다운로드로도 전파될 수 있어 자기 복제의 개념이 확대되었다. 부베 바이러스 역시 전파 경로가 다른 애드웨어였다. 애드웨어의 경우 경쟁 업체끼리는 상호 제거 대상이 되지만 협력 업체와는 배포 수단이 되고 있다. 제작 목적은 사용자 모르게 여러 애드웨어를 설치 후 해당 업체로부터 돈을 받는 것으로 보인다. 지금까지 바이러스, 웜, 트로이목마 등의 악성코드와 달리 애드웨어 제작 업체는 사용자 동의를 받는 형태로 설치되므로 법적으로 문제가 없다고 주장하고 있다. 따라서, 애드웨어 제작 업체는 애드웨어를 진단하는 안티 바이러스 업체나 안티 스파이웨어 업체에 항의하거나 소송을 걸기도 한다. 실제한 안티 바이러스 업체에서 모뎀으로 포르노 사이트에 접속하는 다이알러(Dialer)를 진단하자 해당 업체의 소송에서 부분 패소했으며 다른 안티 바이러스 업체로 하여금 법적인 문제로 다이알러에 대해서 보다 보수적인 진단 정책을 취하게 되었다. 일부 애드웨어 제작 업체들은 악성코드 제작자들과 연계해 악성코드에 감염된 시스템에 사용자 모르게 애드웨어를 인터넷을 통해 받아와 설치하고 있다.

발전하는 애드웨어

그럼 왜 바이러스 형태의 애드웨어를 제작했을까? 애드웨어 제작자가 안티 바이러스 혹은 안티 스파이웨어 프로그램의 진단을 회피하기 위한 목적으로 제작한 것으로 추정된다. 보통 안티 스파이웨어 프로그램은 파일 이름이나 MD5와 같은 파일 값을 이용해 진단한다. 하지만, 이런 방식은 실행 파일을 변경하는 형태에서는 무용지물이 된다. 현재 부베 바이러스는 바이러스로 분류되어 안티 바이러스 제품에서 진단 및 치료하고 있지만 안티 스파이웨어 제품들도 향후 파일 내용 검사 방식으로 개선되어야 할 것으로 보인다.

향후 전망

기술적으로 봤을 때 애드웨어의 등장은 악성코드와 정상 프로그램의 경계를 모호하게 만들었다. 하지만, 부베 바이러스의 경우 바이러스와 트로이목마의 구분도 어렵게 했다. 바이러스로 분류하는 측면에서는 파일 감염을 바이러스적 특징으로 보고 있으며 트로이목마로 분류하는 측면에서는 자기 복제를 하지 않는다는 점을 들 수 있다. 부베 바이러스의 경우 단순히 EXPLORER.EXE를 변경한 것으로 바이러스와 트로이목마의 경계상에 있다고 볼 수 있다. 또한 일단 부베 바이러스에 감염되면 설치되는 많은 애드웨어를 제거하기 위해 안티 스파이웨어 제품을 별도로 이용해야 한다.

애드웨어 제작 업체들은 기존 악성코드 진단 정책이나 법적인 문제를 피하기 위해 더욱 교묘해질 것으로 보인다. 만약 부베 바이러스를 포함하는 어떤 프로그램에서 프로그램 설치시 긴 사용자 약관에 '이 프로그램 설치시 시스템의 일부 기능을 광고 출력에 사용하며 시스템 파일 일부가 변형됩니다'로 표시할 때 또 다른 법적인 문제가 발생하지 않을까?

악성코드와 애드웨어 제작자들이 연계해 서로 공생하는 상황에서 어디까지가 악성코드이며 어디까지가 스파이웨어이냐는 논점은 더욱 불분명해지고 있다. 스파이웨어를 근절하기 위해서는 운영체제 차원에서의 보안 강화, 스파이웨어 정의와 규제에 대한 법률 제정, 사용자의 보안 인식 강화, 안티 바이러스 업체와 안티 스파이웨어 업체의 협력 및 불법적인 애드웨어를 배포한 업체에 대한 경찰의 지속적인 수사도 진행되어야 할 것으로 보인다.

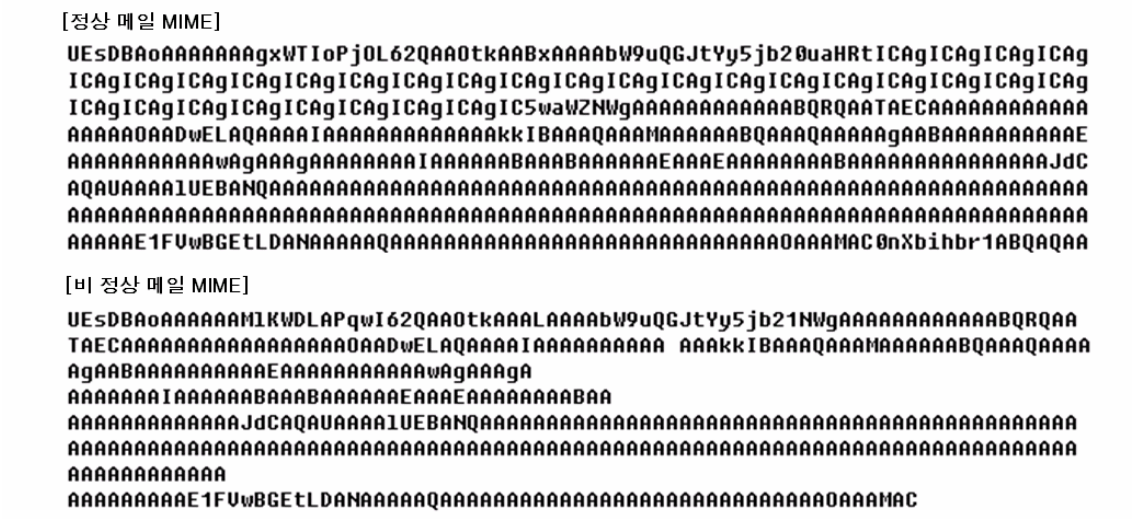
(2) 사례연구를 통해 본 악성코드의 도전 – 네트워크 시그니처 기반의 탐지는 어디까지인가?

작성자 : 정관진 주임연구원(intexp@ahnlab.com)

인터넷의 발전과 함께 다양한 보안 위협들이 발생하며 보안 소프트웨어, 장비의 발전도 함께 이뤄왔다. 이것은 악의적인 공격 행동 증가와 악성코드의 지능화 등 복합적인 위협이 증가함에 따라 자연스럽게 보안장비의 수요와 기술적 진보를 가져온 것이다. 하지만 악성코드의 관점에서만 보더라도 이러한 보안요소를 우회하기 위한 방법으로 역방향 쉘(Reverse Shell), 암호화 통신 등의 기법들이 악성코드에서 사용되고 있다. 이와 같은 우회기법들은 네트워크를 기반으로 한 시그너처 탐지에 어려움을 가중시키고 있는데, 어떤 문제점들을 가지고 있는지 한 사례를 통해 기술적으로 검토해 보고 시그너처의 한계를 조명해 보고자 한다.

최근 2월초 중에 발견된 마이둠.25771 웜(Win32/MyDoom.worm.25771)은 메일로 전파될 때 MIME(Multipurpose Internet Mail Extensions)[1]의 길이를 가변적으로 가지고 있다. RFC(Request For Comments)에서 정의하고 있는 MIME의 길이는 76바이트를 넘지 못하도록 하고 있으며, 일반적으로 메일로 전파되는 악성코드들은 72 또는 76바이트의 길이를 이용하고 있다. 하지만 이번 마이둠.25771 웜의 경우는 기존 MIME의 생성규칙을 따르지 않고 있어 네트워크 기반의 시그너처를 이용한 탐지에는 문제를 안고 있다. 문제의 원인은 이번 마이둠 웜이 메일을 보내기 위하여 MIME을 생성할 때 공백 또는 줄 바꿈 문자인 CRLF[2]를 특정 값의 연산에 따라 임의적으로 넣는다는 것이다. 다음은 정상적인 MIME과 가변적인 MIME 형태를 보여주고 있다.

[1] MIME은 전자우편으로 텍스트이외의 매체인 이미지, 소리, 동영상 등의 파일을 인코딩하여 전송하는 방식을 규정한 표준이다.
[2] CRLF(Carriage Return, Line Feed)를 뜻하는 것으로 줄 바꿈을 의미한다. ₩r₩n 으로 표현할 수도 있다.



[그림1] 정상적인 MIME과 가변적 길이를 가진 MIME의 비교

이러한 형태는 2004년 7월27일 발견된 마이둠.M 웜(Win32/Mydoom.worm.M)에서도 나타났는데 최근에 다시 등장한 것이다. 이와 같은 원인을 분석해 보면 제작자가 의도적으로 MIME 생성시 비 규칙적인 형태를 만들고 있다는 것을 알 수 있는데, 이것은 네트워크 시그너처를 기반으로 하는 보안 소프트웨어 또는 장비를 우회하고자 하는 것으로 추정된다. 기존 마이둠 웜이 MIME 생성시 사용한 코드를 보면 0x4C 길이가 되는 경우 004AE095, 004AE09D 지점에서 ₩r₩n을 넣어주어 다음 라인으로 MIME을 구성하게 된다. 여기서 0x4C는 10진수로 76 이므로 MIME의 한 라인 길이는 76 바이트가 되는 것이다.

```
004AE08C   FF45 F0          INC DWORD PTR SS:[EBP-10]
004AE08F   837D F0 4C       CMP DWORD PTR SS:[EBP-10],4C
004AE093   72 0D            JB SHORT avpproke.004AE0A2
004AE095   C60403 0D        MOV BYTE PTR DS:[EBX+EAX],0D
004AE099   43               INC EBX
004AE09A   897D F0          MOV DWORD PTR SS:[EBP-10],EDI
004AE09D   C60403 0A        MOV BYTE PTR DS:[EBX+EAX],0A
```

최근의 변형은 위 코드를 기준으로 임의의 연산을 하는 부분이 추가되었음을 다음 코드를 통해 알 수 있다. 특정 값으로 연산을 하고 00506723 지점에서 연산된 값을 통해 1인 경우에는 0x20(공백인 whitespace를 뜻함)을 입력하고, 00506731 지점에서는 2 또는 3의 값인 경우 0x0d와 0x0a(₩r₩n)을 입력하게 된다. 코드에서 나타난 조건분기 경우의 수를 보면 MIME을 구성할 시에 공백보다는 ₩r₩n 이 들어가는 비중이 더욱 높게 될 것이다.

```
00506719   B9 90010000    MOV ECX,190
0050671E   F7F9           IDIV ECX
00506720   83FA 02        CMP EDX,2
00506723   7D 09          JGE SHORT mydoom-o.0050672E
00506725   8B45 08        MOV EAX,DWORD PTR SS:[EBP+8]
00506728   C60403 20      MOV BYTE PTR DS:[EBX+EAX],20
0050672C   EB 11          JMP SHORT mydoom-o.0050673F
0050672E   83FA 04        CMP EDX,4
00506731   7D 0D          JGE SHORT mydoom-o.00506740
00506733   8B45 08        MOV EAX,DWORD PTR SS:[EBP+8]
00506736   C60403 0D      MOV BYTE PTR DS:[EBX+EAX],0D
0050673A   43             INC EBX
0050673B   C60403 0A      MOV BYTE PTR DS:[EBX+EAX],0A
0050673F   43             INC EBX
```

이와 같이 마이둠이 76바이트의 MIME을 생성하는 코드에 추가적으로 MIME의 구성이 일정치 않은 형태로 구성되는 루틴을 가지고 있어 일반적인 형태의 네트워크를 기반으로 하는 탐지에 있어서는 문제가 발생할 수 있다. 예를 들어, MIME의 일부를 시그너처의 탐지 패턴으로 사용했을 경우 해당 부분에 공백 또는 ₩r₩n이 들어가거나 임의적으로 들어간 값으로 인하여 전체적인 위치가 바뀌게 되어 offset이 변경될 수 있기 때문이다. 제작자의 이런 의도적인 행동은 시그너처 기반의 탐지를 우회할 수 있고, 가변적 길이의 MIME을 생성하여도 대중적으로 사용되고 있는 메일 클라이언트 소프트웨어들에서는 디코딩(Decoding)하는데 큰 문제를 가지지 않기 때문에 전파에 있어서 더욱 효과적인 방법이 될 수도 있는 것이다.

과거부터 보안제품의 기술들이 발달하며 이에 따라 악성코드들의 기법도 다양해지며 발전해왔다. 하지만 앞으로 네트워크를 이용하는 비중은 더욱 높아질 것이고 '보안'은 이제 중요한 변수가 될 것이며 앞서 살펴본 마이둠 웜의 경우와 같이 악성코드들의 지능화에 따른 여러 다양한 우회기법들이 일반화되어 사용될 것으로 예상된다. 이제 네트워크 기반의 시그너처는 제약사항들이 늘어나며 일반화되기 이전에 새로운 기법들과 지속적인 연구개발을 통해 효과적인 대처방안이 마련되어야 한다. 물론 네트워크 시그너처 기반의 탐지에는 한계가 존재하지만 이를 극복하고 연계될 수 있는 다른 대응방안 또한 함께 고려하여 시그너처 기반의 한계성을 보완해 줄 수 있는 요소가 검토되어야 할 것이다.