ASEC Report 4월

® ASEC Report

2005. 05

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

다수의 마이톱 웜과 켈비르 웜 변형 발견…

4월은 3월에 비해 악성코드 피해는 다소 감소하고, 신종(변형) 발견건수는 다소 증가하는 현상을 보였다. 4월 악성코드 피해의 특징은 근 1년 동안 많은 피해를 입힌 넷스카이 웜에 의한 피해가 감소하고, MSN 메신저를 이용하여 확산되는 브로피아 웜, 메일을 통해 확산되는 마이톱 웜 변형에 의한 피해가 악성코드 Top 10 피해 순위에 등장했다는 것이다. 피해 악성코드 Top 10의 전파방법 별 유형을 살펴보면, 예년에 비해 MSN 메신저를 통해 확산되는 웜이 증가하였는데, 이는 다수의 켈비르 웜 변형, 브로피아 웜 변형 등이 발견되면서 MSN 메신저를 통해 확산되는 웜의 피해가 증가했기 때문인 것으로 보인다. 4월 발견된 신종(변형) 중 가장 특이할 만한 것은 역시 마이톱 웜과 켈비르 웜의 변형이 다수 발견되었다는 것이다. 특히 마이톱 웜 변형은 2월말에 최초 발견된 이후로 5월초 현재까지 약 80여 개의 변형이 발견될 정도로 단시간에 많은 변형이 발견되었다. 이런 현상은 한국 뿐 아니라 일본, 중국을 포함한 전세계적으로 나타난 현상으로, 당분간 마이톱 웜 변형에 의한 피해는 꾸준히 지속될 것으로 예측된다. 스파이웨어의 경우는 최근 들어 은폐 및 자기 방어 기능을 가진 것이 증가하고 있다. 이는 안티 스파이웨어 프로그램이 등장하면서 일반적으로 제거프로그램이 제공되지 않는 스파이웨어까지 검출, 삭제함에 따라 자신이 제거되는 것을 막귀 위해 자신을 보호하고 안티 스파이웨어 프로그램까지 무력화하는 기능을 포함하는 경향을 보이고 있는 것이다. 그 밖에도 4월에는 스파이웨어 구클이 발견되었는데, 이는 구글 사이트(www.google.com) 방문을 원하는 사용자가 오타로 googkle.com 사이트를 입력하여 방문할 경우, MS 취약점을 이용하여 약 30개 이상의 악성코드와 유해가능 프로그램을 설치하도록 하는 것이다. 그러나 이 스파이웨어는 발견즉시 해당 사이트가 폐쇄되어 많은 유포되지는 못하였다. 4월에는 8개의 MS 보안취약점에 대한 패치가 발표되었다. 그 중에서 IP 유효성 검사 취약점과 ICMP 연결 다시 설정 취약점은 이미 개념증명코드가 공개되어 이를 이용한 악성코드 제작가능성이 높으므로, 반드시 해당 취약점을 보유한 시스템은 패치를 적용하여야 하겠다. 그 밖에 이달의 ASEC 컬럼에서는 4월에 윈도우 XP 64비트 버전이 공식 출시됨을 계기로 64비트의 환경과 악성코드 감염 가능성에 대해 살펴보았다.

I. 4월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자 : 박철민 연구원(cmpark@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	240	15.3%
2	New	Win32/Bropia.worm.188928	123	7.8%
3	↑4	Win32/Sasser.worm.15872	63	4.0%
4	New	Win32/Maslan.C	61	3.9%
5	New	Win32/IRCBot.worm.83414	48	3.1%
6	↓3	Win32/Netsky.worm.25352	36	2.3%
7	↓3	Win32/Netsky.worm.17424	34	2.2%
8	-	Win32/Netsky.worm.18944.B	33	2.1%
9	↑1	Win32/LovGate.worm.128000	31	2.0%
10	New	Win32/Mytob.worm.61440	28	1.8%
		기타	875	55.7%
합계			1,572	100%

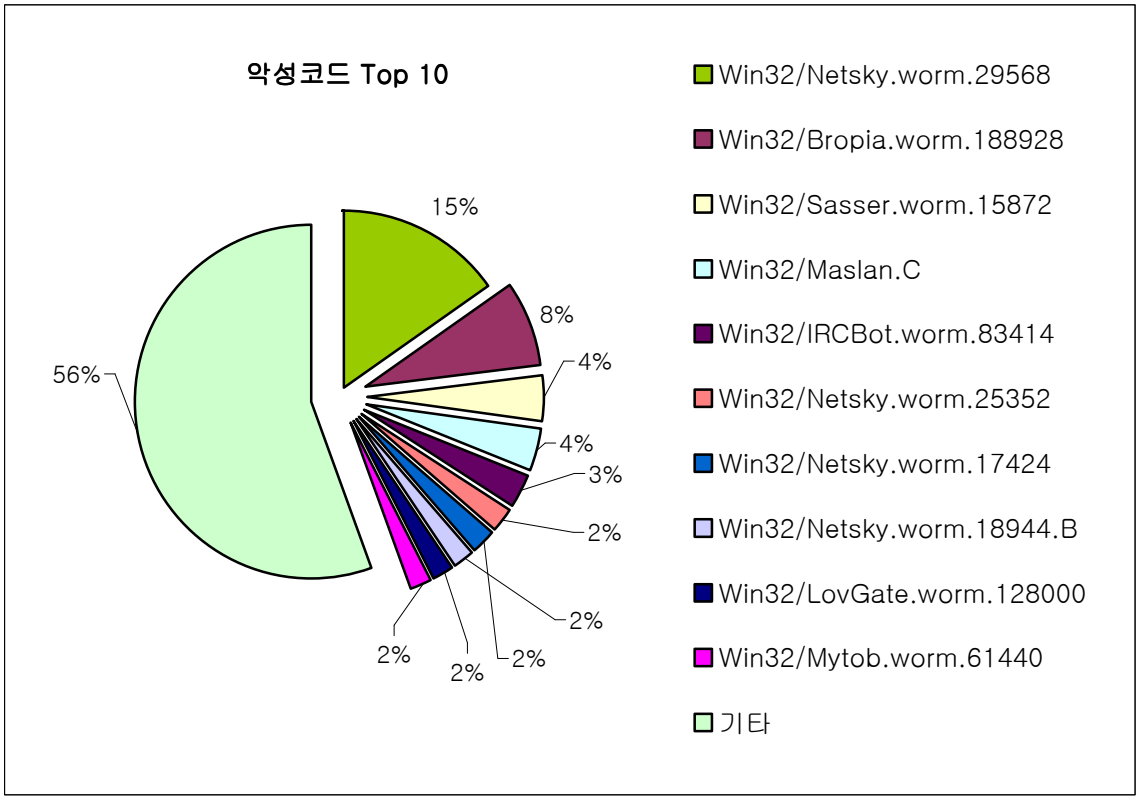
[표1] 2005년 4월 악성코드 피해 Top 10

4월 악성코드 피해 동향

2005년 4월 악성코드(바이러스, 웜, 트로이목마 등) 피해 건수는 2005년 3월에 비해 소폭 감소한 1,572건이다. 매월 악성코드 피해순위 1위를 차지하고 있는 넷스카이.29568 웜(Win32/Netsky.worm.29568)의 피해가 4월 들어 감소한 것과 V3에서 악성 아이알씨봇(IRCBot)류에 대한 진단/치료(삭제) 기능이 강화되어 악성 아이알씨봇 변형에 대한 피해가 감소한 것이 4월 악성코드 피해가 전반적으로 감소한 원인으로 추정된다.

4월 악성코드 피해 동향에서 특징적인 것은 메신저를 이용하여 전파되는 브로피아 웜(Win32/Bropia.worm.188928)이 Top 10에 등장함과 동시에 2위를 차지하고 있는 점이다. 이는 메신저 웜이 일반적으로 감염자의 메신저 리스트에 등록된 사용자에게 전달되기 때문에 메신저 사용자들이 지인으로부터 받은 메시지에 대해 경계심 없이 파일을 다운로드 하여 실행하거나 링크를 클릭하는데 기인한 것으로 보인다. 4월 악성코드 피해동향의 또 하나의 특징으로는 마슬란.C(Win32/Maslan.C)에 의한 피해가 증가하여 4위를 차지하였다는 것이다.

4월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.



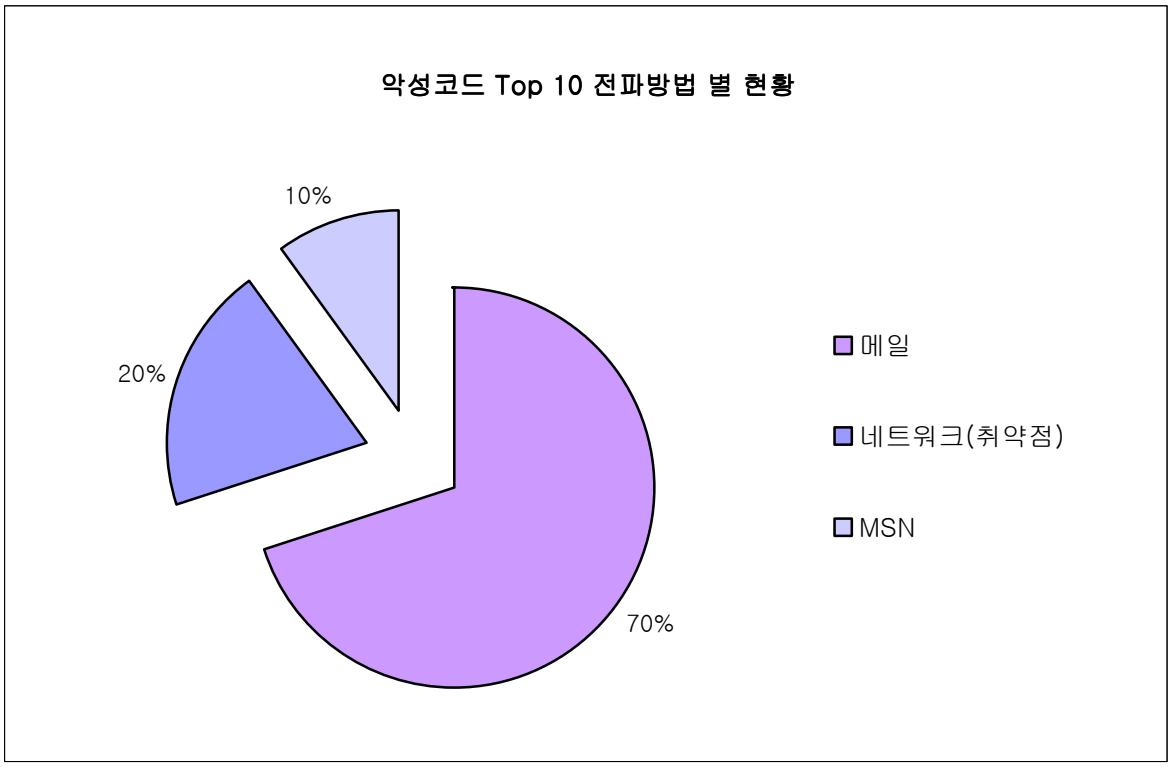
[그림1] 2005년 4월 악성코드 피해 Top 10

위에서 언급했듯이 넷스카이.29568 웜에 대한 피해문의가 현저하게 급감하였으며, 지난달에는 악성코드 Top 10에 넷스카이 변형들이 7개나 올라 왔었지만 이번 달에는 대부분 사라지거나 순위가 감소하였다.

반면, 마이톱.61440 웜에 의한 피해는 증가하였다. 이 웜은 3월에 발견된 이후 5월 초 현재까지 70개가 넘는 변형이 발견될 정도로 단기간에 많은 변형이 발견되어 광범위하게 확산되었다. 따라서 당분간 긴 생명력을 유지할 것으로 보인다.

4월 악성코드 Top 10 전파방법 별 현황

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



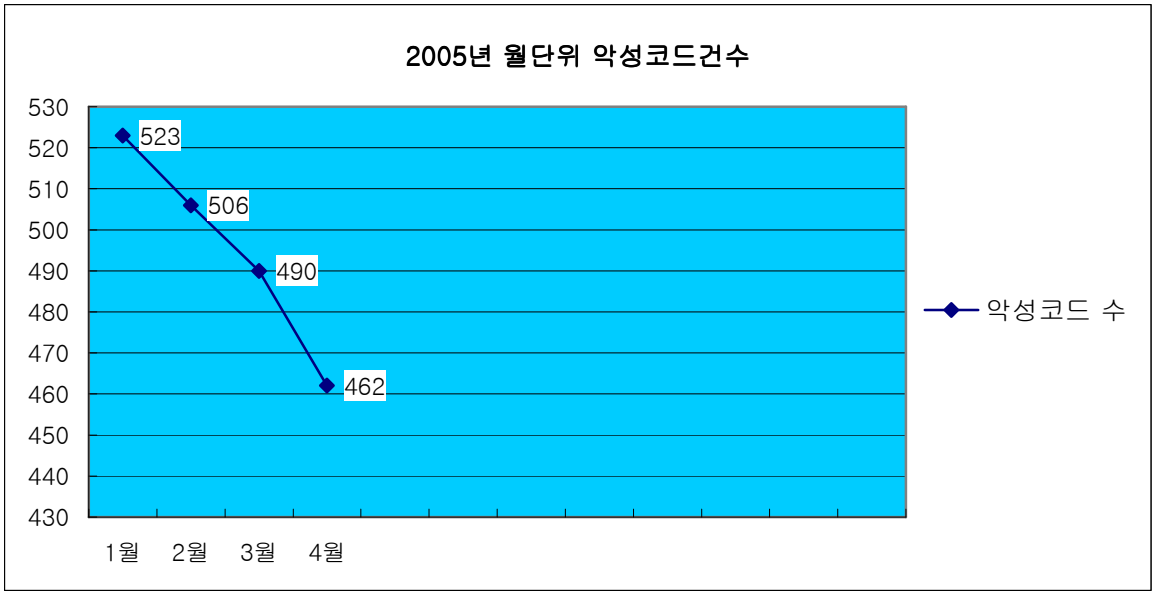
[그림2] 악성코드 Top 10의 전파방법별 현황

[그림2]에서 나타난 것처럼 악성코드가 이용하는 전파방법의 대다수가 메일을 이용하였으며, 이는 지난달과 비슷한 현황으로 여전히 매스메일러(Mass Mailer)에 의한 피해가 대부분을 차지하고 있음을 보여주고 있다. 또한 비중은 작지만 올해 들어 MSN 메신저를 이용하여 전파되는 웜이 예년에 비해 많이 발견되고 있어, 앞으로는 점점 메신저를 이용하는 악성코드가 늘어날 것으로 예측된다. 따라서 사용자들은 가까운 메신저 친구로부터 전송되어 오는 파일이나 링크는 친구가 보낸 것이 맞는지 확인한 후 다운로드 하여 실행 또는 해당 링크를 클릭하는 습관을 가지는 것이 중요하며, 혹여 다운로드 받았을 경우에는 실행 전에 최신엔진의 백신으로 검사하는 습관을 가져야 하겠다. 또한 네트워크(취약점)를 통해 전파되는 유형도 꾸준히 나타나고 있으므로, 자신이 사용하는 운영체제나 어플리케이션이 보유한 취약점에 대해 주기적으로 살피고 관련 취약점에 대한 보안패치를 적용하는 것 또한 게을리하지 말아야 하겠다.

월별 피해신고 악성코드 건수 현황

4월에 피해 신고된 악성코드는 462개이다. 지난 3월에 비해 소폭 감소하였으며, 이는 1월부터 지속적으로 감소하는 추세를 보이고 있다. 이는 V3 엔진의 악성 아이알씨봇 진단기능 향상, 지난해에 비해 전파력이 강한 악성코드의 발생이 상대적으로 적었던 것과 동시에 윈도우 XP SP2 등에서 기본으로 제공하는 방화벽의 사용 및 정기적인 보안패치 등 높아진 사용자

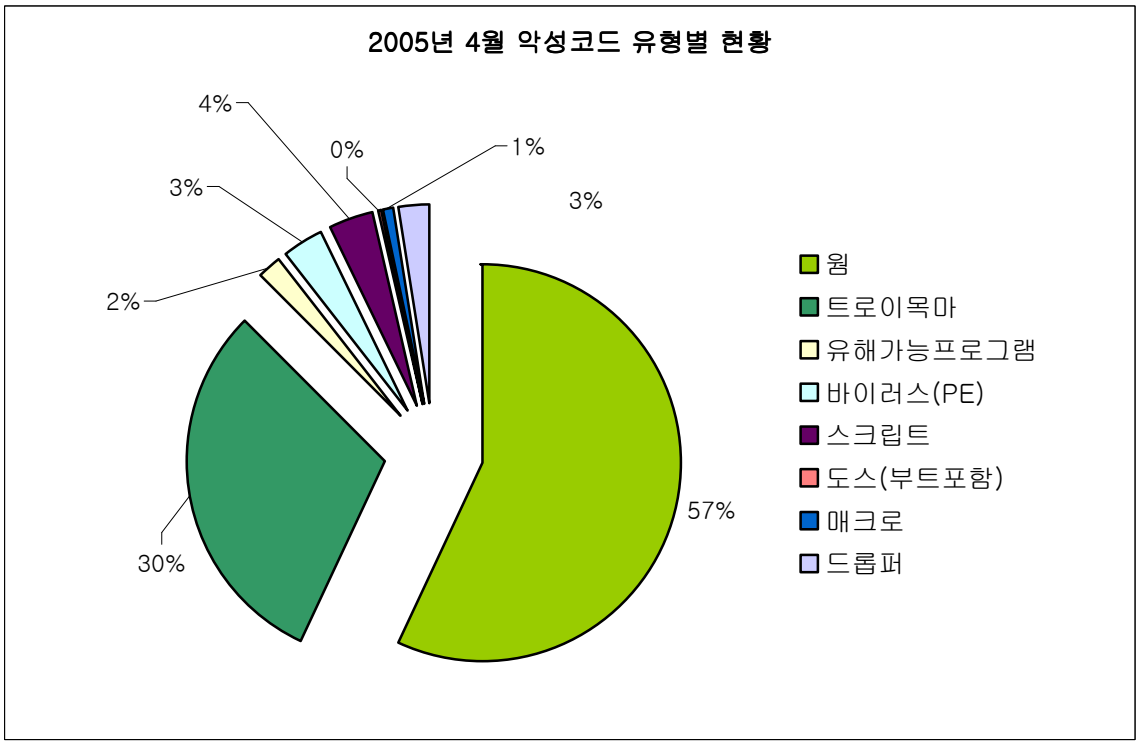
의 보안의식에 따른 것으로 보인다.



[그림3] 2005년 월별 피해신고 악성코드 수

주요 악성코드 현황

악성코드 유형별 현황은 [그림4]와 같다.



[그림4] 악성코드 유형별 현황

피해 악성코드의 유형별 현황에 있어서는 지난달과 비슷한 현황으로, 웜이 상대적으로 큰 비중을 차지하고 있다. 그 다음으로 트로이목마가 큰 비중을 차지하고 있다. 통상 트로이목마는 단독으로 시스템에 감염되지 않으며 웜이 감염된 후 시스템에 설치(드롭퍼)하는 유형이 많다. 이로 인해 웜의 감염 비율이 증가하면, 트로이목마의 감염 비율 역시 증가하는 현상으로 보인다. 더불어 웹 서핑시 주로 감염되는 스파이웨어도 트로이목마를 설치하는 증상을 보이고 있다.

다음은 이번 달에도 1위를 차지한 넷스카이 웜이 발송한 메일 본문의 마지막 부분이다.

```
++++ Attachment: No Virus found
++++ Norton AntiVirus - www.symantec.de
```

위에 나온 문구는 마치 첨부된 파일이 유명 안티 바이러스 업체의 검사를 통과한 아무런 문제가 없는 파일인 것처럼 그럴듯한 결과를 보여주고 있다. 이처럼 악성코드 제작자들은 메일을 이용하여 전파하는 기본적인 방법에 사회공학기법을 접목해서 사용자들을 속이고 있다. 이런 방법들은 지속적으로 사용자들에게 위협적인 존재가 되었고 앞으로도 계속될 것으로 보인다. 따라서 사용자들은 메일의 내용을 한번쯤은 의심해 보고, 첨부된 파일을 실행할 때는 악성코드를 예방하는 차원에서 V3로 검사한 후에 실행하는 습관을 가져야 하겠다.

(2) 신종(변형) 악성코드 발견 동향

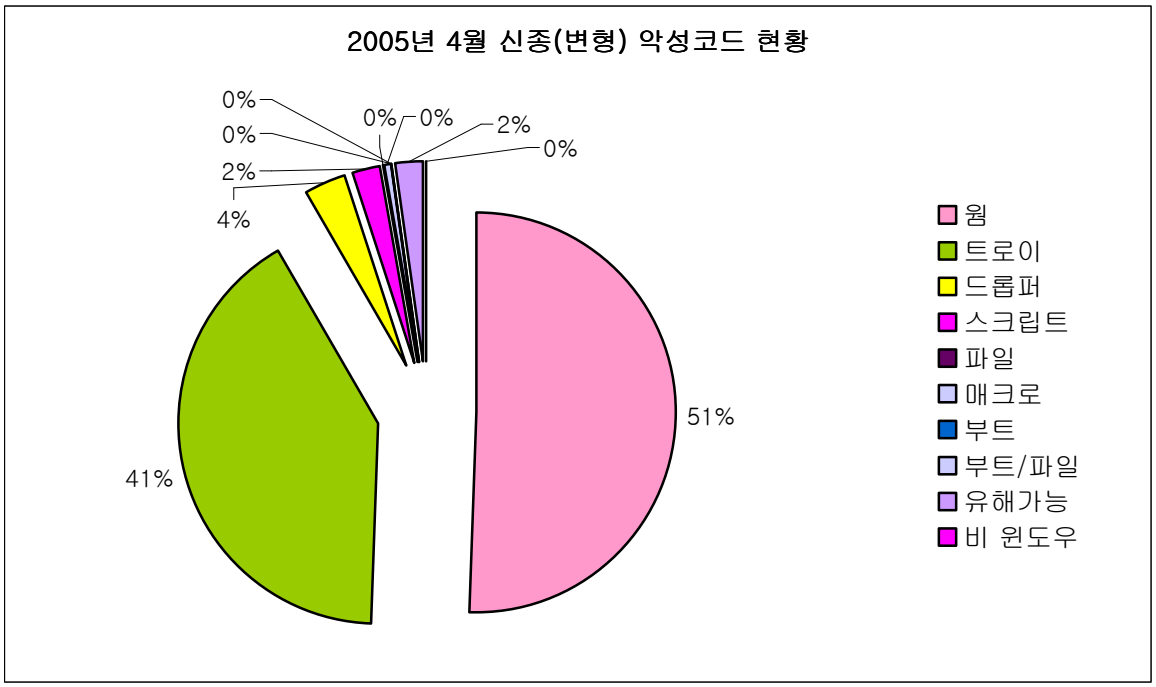
작성자 : 차민석 주임연구원 (jackycha@ahnlab.com)

4월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1]과 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	非윈도우	합계
114	92	8	5	0	1	0	0	5	0	225

[표1] 2005년 4월 유형별 신종 (변형) 악성코드 발견현황

2005년 들어 계속 감소되던 신종 악성코드 수가 4월에는 소폭 증가했다. 그 원인으로는 마이톱 웜(Win32/Mytob.worm)과 켈비르 웜(Win32/Kelvir.worm) 변형이 꾸준히 등장하여 확산되었고 트로이목마와 드롭퍼(Dropper)의 발견이 증가한 때문이다 향후 이 수치는 웜의 상당수를 차지하는 악성 아이알시봇(IRCBot)의 변형 추세에 따라 달라 질 수 있다. 변형 제작자들은 백신의 진단을 피하기 위해 백신이 잘 풀지 못하는 실행 압축 프로그램을 찾아 이용하고 기존 검색법으로 진단되지 않는 새로운 변형을 꾸준히 만들어 내고 있기 때문에 상황에 따라 수치가 증가할 수 있다..



[그림1] 2005년 4월 신종(변형) 악성코드 비율

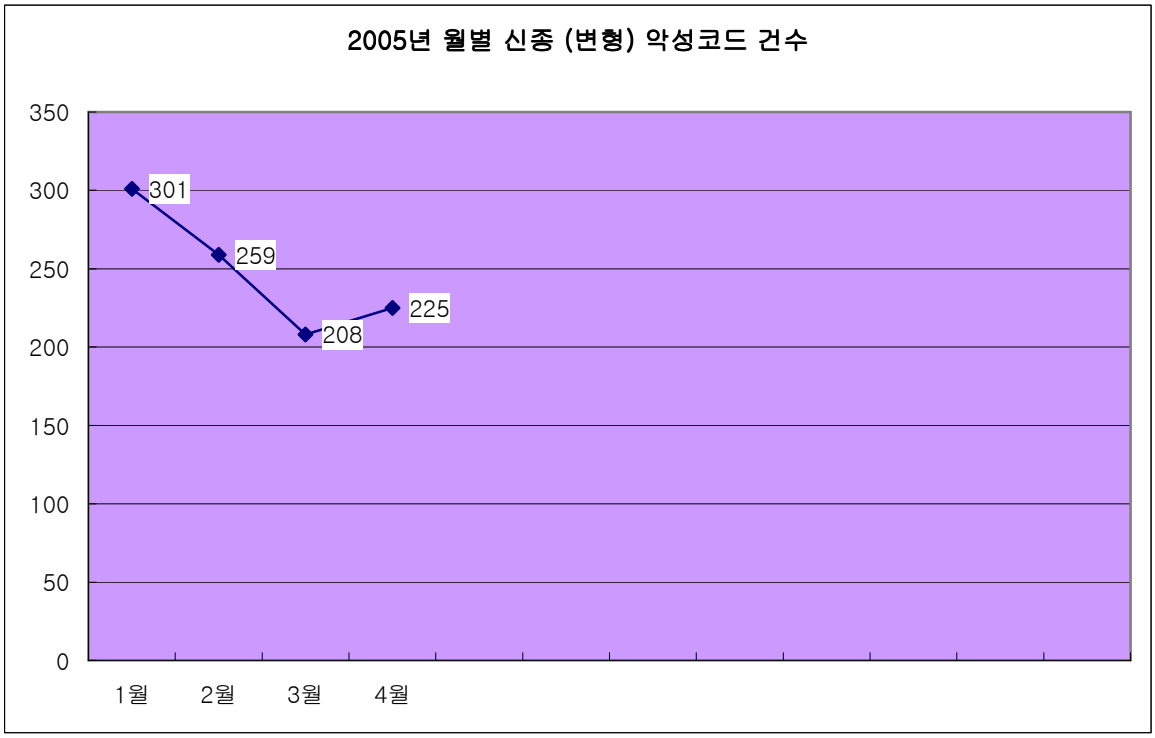
[그림1]은 4월 신종(변형)악성코드의 비율을 나타낸 것이다. 이번 달에도 웜과 트로이목마가 전체의 90% 이상을 차지하고 있다.

신종 트로이목마는 대체로 다음과 같은 유형으로 나뉠 수 있다.

- 백도어류 (Win-Trojan/HackDef, Win-Trojan/Nethief)
- 프락시 서버류(Win-Trojan/Ranky, Win-Trojan/Mitglieder)
- 다운로더류 (Win-Trojan/Downloader, Win-Trojan/Small)
- 시작 페이지 고정류 (Win-Trojan/StartPage)
- 애드웨어 연관류 (Win-Trojan/LowZones)

최근 몇 년간 유행하던 백도어류는 점차 자신의 존재를 숨기는 은폐기법(Stealth Technique) 혹은 루트킷(Rootkit)으로 불리는 형태가 증가하고 있다. 그 외 프락시 서버, 시작 페이지 고정, 애드웨어 연관 트로이목마는 금전적 이득을 위한 목적으로 제작되고 있다. 프락시 서버는 감염된 시스템을 이용해 스팸 메일을 발송하고 다운로더는 사용자 모르게 트로이목마나 애드웨어를 설치한다. 애드웨어와 연관된 트로이목마들은 사용자 시스템의 보안 설정을 낮춰 사용자 동의를 구하지 않고 애드웨어를 설치하도록 유도한다.

다음은 월별 신종(변형) 악성코드 건수를 나타내고 있다. 2월에 비해 3월에는 50개 가까이 감소하던 신종 악성코드 수가 소폭 증가한 것을 알 수 있다.



[그림2] 2005년 월별 신종(변형) 악성코드 발견 현황

3, 4월에는 이메일로 전파되는 마이톱 웜(Win32/Mytob.worm)과 MSN 메신저로 전파되는 켈비르 웜(Win32/Kelvir.worm) 변형이 지속적으로 보고되고 있다. 또한 사용자 시스템에 애드웨어 설치를 시도하는 트로이목마 등도 계속 보고 되고 있다.

4월 주요 신종(변형) 악성코드

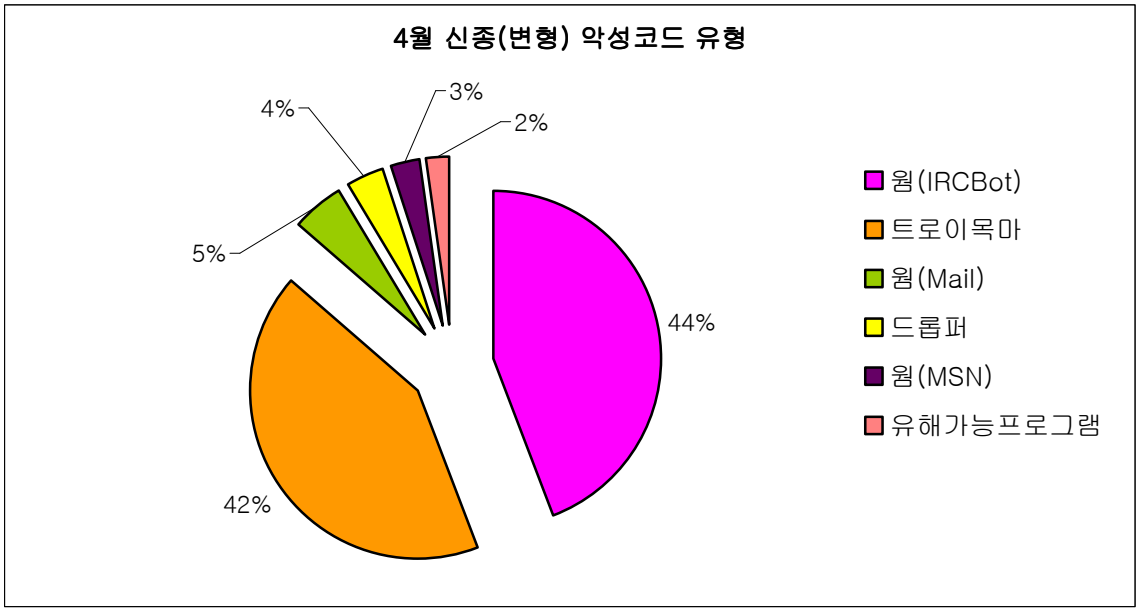
이번 달 이슈가 되었던 주요 악성코드를 뽑는다면 마이톱 웜과 켈비르 웜이다.

▶ 마이톱 웜(Win32/Mytob.worm)

이 글을 작성하고 있는 5월 초 현재도 계속 변형이 발견되고 있다. 2005년 5월 9일까지 발견된 마이톱 웜 변형은 80개 이상으로, 4월 초까지 20개 남짓임을 생각하면 4월 한달간 제작자가 많은 변형을 만들었음을 알 수 있다. 마이톱 웜은 마이둠 웜(Win32/MyDoom.worm)에 아이알씨봇 기능을 추가한 형태이다.

▶ 켈비르 웜(Win32/Kelvir.worm)

이 웜은 MSN 메신저를 이용하여 자신을 전파하며, 특정 호스트에서 악성 아이알씨봇 웜을 설치한다. 이러한 동작방식은 2월초에 많은 피해를 주었던 브로피아 웜과 매우 유사하다. 제작자는 악성 아이알씨봇을 이용해 애드웨어를 설치하는 것으로 확인되었으며 이 웜의 제작자 역시 애드웨어를 설치해서 금전적 이득을 얻으려는 것으로 보인다.



[그림3] 4월 신종 웜과 트로이목마 유형

2005년 4월의 신종 웜과 트로이목마 유형은 [그림3]과 같다. 악성 아이알씨봇이 웜의 대부분을 차지하고 있으며 MSN 메신저로 전파되는 웜이 소폭 증가했는데 이는 켈비르 웜의 변

형이 계속 등장하고 있기 때문이다.

4월은 조금씩 감소하던 신종 악성코드가 소폭 증가했으며, 마이톱 웜과 켈비르 웜 변형이 꾸준히 등장한 한달이었다. 특히 금전적 이익을 목적으로 제작된 트로이목마의 증가는 사용자들에게 많은 스팸 메일을 받게 하고 광고창을 보게 만들었다.

II. 4월 AhnLab 스파이웨어 동향

작성자 : 김정석 주임연구원(js_kim@ahnlab.com)

최근 들어 은폐 및 자기방어 기능을 가진 애드웨어나 스파이웨어의 종류와 수가 늘고 있다. 일반적으로 애드웨어나 스파이웨어는 직접적인 공격의 기능이나 확산 기능을 가지고 있지 않기 때문에 웜이나 바이러스와 같은 악성코드에 비하여 위험도가 떨어진다고 생각하기 쉽다. 하지만 애드웨어 또는 스파이웨어의 주요 기능인 팝업광고의 노출, 브라우저 설정의 변경, 백그라운드 프로세스의 실행만으로도 시스템 성능을 심각하게 저하시켜 가용성(Availability)을 크게 떨어뜨리며, 스파이웨어에 의해 사용자 정보가 유출되거나 자체적인 결함으로 인한 시스템 손상은 생각보다 훨씬 심각하다.

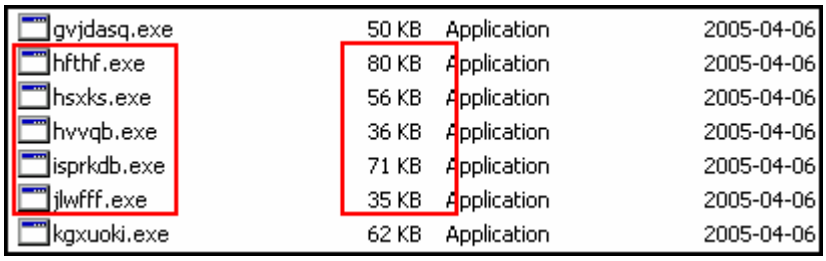
은폐 및 자기방어 기능을 가진 스파이웨어

애드웨어나 스파이웨어는 일반적으로 제거 프로그램을 제공하지 않기 때문에 수동으로 제거하기가 매우 어려웠으나, 안티 스파이웨어 프로그램이 등장함에 따라 애드웨어나 스파이웨어의 검출과 제거를 쉽게 할 수 있게 되었다. 그러나 최근 들어 발견되는 애드웨어, 스파이웨어는 이런 안티 스파이웨어 프로그램으로부터 자신이 제거되는 것을 막기 위해 자신을 보호하고 안티 스파이웨어 프로그램을 무력화하는 기능을 포함하고 있는 경우가 많아졌다.

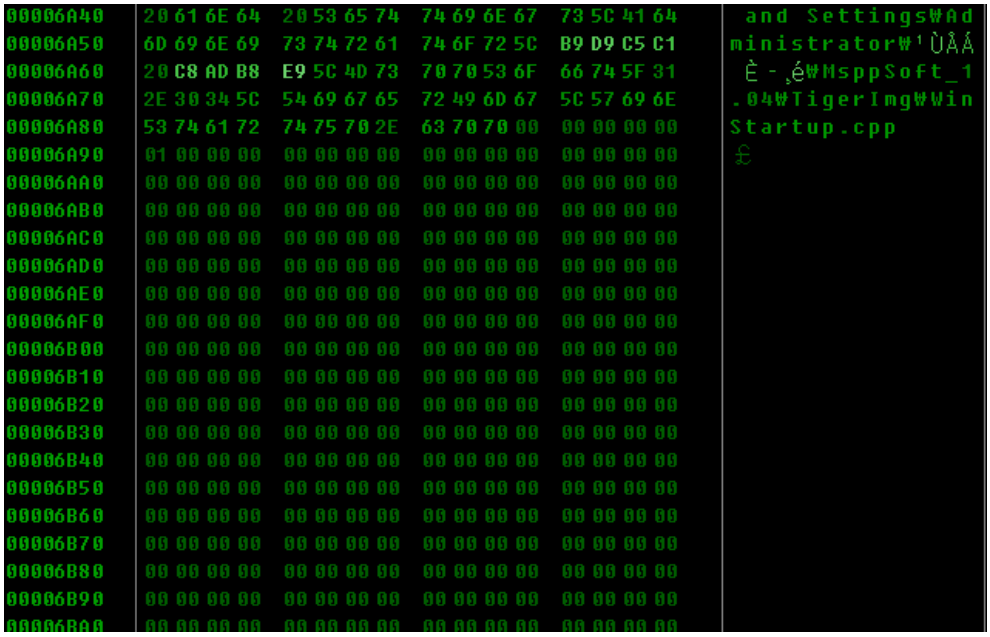
시작페이지를 고정하는 스파이웨어인 스타트페이지.vr(Win-Spyware/StartPage.vr)은 about:blank로 많이 알려진 스타트페이지(Win-Spyware/StartPage)의 수 많은 변형 중 하나이다. 스타트페이지.vr은 랜덤한 CLSID[1]와 파일이름을 사용하여 안티스파이웨어 프로그램의 검출을 피한다.

다운로더 한글로(Win-Downloader/Hanglo)는 애드웨어를 설치하는 다운로더이다. 다운로더 한글로는 안티 스파이웨어 프로그램의 검출을 피하기 위하여 파일이름을 랜덤하게 정하고 파일의 뒷부분에 의미없는 값을 덧붙이는 ZeroPadding 기법을 사용한다.

[1] CLSID 란?
OLE 클래스 개체와 관련된 A globally unique identifier (GUID)로, 서로 다른 벤더가 제작한 COM 개체에 대하여 이름 충돌을 피하고 위치투명성을 제공하기 위하여 CLSID를 이용한다. 윈도우에서는 ActiveX 콘트롤과 같이 동적으로 링크되는 콤포넌트를 이용하기 위하여 레지스트리에 CLSID를 등록하고 경로를 표시하게 된다. ActiveX 콘트롤을 이용하는 프로그램은 이름 대신에 해당 콘트롤의 CLSID를 이용하여 해당 콤포넌트를 호출하여 콤포넌트 이름에 의한 충돌을 피할 수 있다.
윈도우 레지스트리의 HKEY_CLASSES_ROOT의 하위키 CLSID에 각각의 CLSID가 등록되고 하위 키에 부가적인 정보를 표시하며 특히 InprocServer32키에 콤포넌트의 경로가 표시된다.



[그림1] 다운로드 한글로(Downloader/Hanglo)의 임의의 파일이름과 다양한 사이즈.



[그림2] 헥스 에디터(hex editor)로 본 다운로더 한글로 파일의 뒷부분

2005년 4월에 발견된 다운로더 델프.24577(Win-Downloader/Delf.24577)은 은폐기능을 사용하는 다운로더이다. 흔히 루트킷(Rootkit)이라고 불리는 은폐 기능을 가진 악성코드는 커널모드 드라이버를 사용하거나 윈도우 탐색기에 인젝션하는 방법으로 시스템 호출을 가로채 윈도우 탐색기에 나타나지 않는 방법을 사용한다. 다운로더 델프.24577는 자기 자신을 숨기기 위해 Browser Helper Object(BHO)[1]를 사용하는데, 설치되면 다운로더 델프.24577로 진단되는 DLL 파일을 윈도우 탐색기에서 볼 수 없다.

이러한 은폐 및 자기방어기능이 있는 애드웨어와 스파이웨어는 일단 설치되면 수동으로 제거하기가 매우 어렵다. 이를 예방하기 위해서는 안티 스파이웨어 프로그램에서도 안티 바이러스 프로그램(백신)과 같은 실시간 감시 기능이 요구된다.

[1] Browser Helper Object (BHO)
BHO는 마이크로소프트(Microsoft)에서 제공하는 윈도우탐색기와 IE 브라우저 기능을 확장하는 방법이다. DLL 형태로 만들어지며 IE 프로세스 내에서 동작하기 때문에 애드웨어나 스파이웨어는 BHO를 이용하여 여러 가지 악의적인 행동 – Address Redirection, 팝업노출, 윈도우 탐색기와 IE 브라우저의 특정 이벤트 가로채기 등 – 을 할 수 있다.

유사도메인을 이용한 스파이웨어의 설치

2005년 4월에 발견된 스파이웨어 구클(Googkle)은 유명 검색사이트 구글(www.google.com)방문을 원하는 사용자의 오타로 www.googkle.com 사이트를 방문하였을 때 IE 브라우저 취약점(MS00-037, MS04-028)을 이용하여 적어도 30개 이상의 악성코드와 유해가능 프로그램을 설치한다. 2005년 4월 26일 스파이웨어 구클에 대한 최초의 정보가 발표된 이후로 해당 사이트는 폐쇄되었다. 해당 도메인의 소유자는 러시아인이며, 동일인물이 아래의 유사도메인 리스트를 모두 소유한 것으로 보아 악성코드 배포의 목적으로 사용된 것으로 추정된다.

- msnm(dot)com
- gfoogle(dot)com
- ghoogle(dot)com
- googfle(dot)com
- luycos(dot)com
- msn1(dot)com
- passpport(dot)com
- xcnn(dot)com.

악의적인 목적으로 제작된 웹 사이트는 스팸메일이나 인기검색어를 등록하여 사용자의 방문을 유도하는 방법을 사용한다. 유사도메인을 이용하는 경우에는 적극적으로 사용자의 방문을 유도하는 대신 사용자의 오타로 방문을 기다리는 소극적인 방법을 이용한다. 그러나 두 가지 방법 모두 IE 브라우저 취약점을 이용하는 웹사이트에 방문하는 것만으로 위험도가 높은 악성코드가 설치 실행될 수 있기 때문에 각별한 주의가 필요하다.

이러한 악의적인 목적의 웹 사이트 방문에 의한 피해를 줄이기 위해서 사용자는 위와 같은 유사도메인을 사용하는 웹 페이지에 의도적으로 접근하지 말아야 하고, 항상 웹브라우저에 대한 취약점 패치를 확인해야 한다.

III. 4월 시큐리티 동향

작성자 : 김지훈 주임연구원(smallj@ahnlab.com)

이번 달에도 운영체제 및 응용 프로그램의 취약점을 이용한 보안 사고가 많은 것으로 보고되었다. 윈도우 운영체제와 관련한 보안 취약점 발표 후 보름이 채 지나지 않은 상황에서 6개 이상의 개념증명코드(PoC, Proof of Concept)가 쏟아져 나오는 등 제로데이 공격(Zero-day Attack)이 임박해오고 있음을 실감케 했다. 인터넷 사용자들의 다양한 기호를 반영하듯 인터넷 익스플로러 이외의 파이어폭스, 오페라 등의 웹브라우저에 대한 선호도가 늘어나고 있다. 이러한 흐름은 보다 많은 보안 위협에 노출되는 상황으로 자연스럽게 이어지고 보안 취약점을 이용하는 공격들도 다양하게 시도되고 있음을 주목해야 한다. 웹브라우저 벤더들의 방어기재 마련에 대한 노력이 절실히 요구되고 있다. 유닉스 운영체제 및 웹 응용 프로그램의 자체 취약점을 이용한 홈페이지 변조 사고 또한 꾸준히 증가되고 있는 점에서 웹사이트 운영자의 보안 의식이 여전히 부족한 것으로 드러났으며, 보다 적극적인 보안 장치의 마련이 시급한 것으로 판단된다.

마이크로소프트사, 2005년 4월 보안 업데이트 발표

마이크로소프트사는 심각도 등급 '긴급(5)', '중요(3)'를 가진 총 8개의 4월 보안 업데이트를 발표하였다. TCP/IP의 취약점으로 인한 원격 코드 실행 및 서비스 거부 문제점(MS05-019)에 관련된 취약점은 5개가 존재하는데 이중에서 IP 유효성 검사 취약점(CAN-2004-0048), ICMP 연결 다시 설정 취약점(CAN-2004-0790)에 대한 개념증명코드(PoC)가 이미 공개되었고, 기존 작성자의 개념증명코드(PoC)가 악용된 선례가 있어 이번 개념증명코드 또한 악성코드로의 발전 가능성에 대해 예의주시할 필요가 있다. 또한 마이크로소프트사의 제품 뿐 아니라 TCP/IP 기반의 중요 인프라 장비들에게도 영향을 미칠 수 있는 것이어서 좀 더 세심한 주의가 필요하다. 이 밖에도 윈도우 쉘의 취약점으로 인한 원격 코드 실행 문제점(MS05-016), 인터넷 익스플로러와 관련된 DHTML 개체 메모리 손상 취약점, 내용 관리자 메모리 손상 취약점 (MS05-020), Exchange Server 의 취약점으로 인한 원격 코드 실행 문제점 (MS05-021) 에 대한 개념증명코드(PoC)가 공개되었다.

마이크로소프트사, SP2 자동업데이트 차단장치 제거

기업들의 윈도우 XP 서비스팩(SP2) 보급률이 24%에 불과한 것으로 나타나고 있는 가운데 마이크로소프트사는 윈도우 XP SP2 보급에 박차를 가하고 있다. 지난해 8월 출시된 XP SP2를 자동업데이트 하면 운영체제의 방화벽 기능이 자동으로 작동되기 때문에 현재 동작중인 응용프로그램을 인식하지 못할 수도 있다는 의견이 제기되어 왔고, SP2가 다른 응용 프로그램들과 충돌하는 현상이 발견됨에 따라 기업 고객들에 한해 240일 동안 자동 업데이트를 차단할 수 있도록 해왔다. 그러나 이번 SP2 자동업데이트 차단장치 제거로 인해 보안성

이 뛰어난 SP2의 보급이 크게 증대됨으로써 윈도우 관련 보안사고 예방에도 크게 기여할 것으로 기대된다. 중소기업이나 가정용 사용자들은 이번 조치의 영향을 받지 않는다.

안전한 웹브라우저 만들기 노력

가장 많이 사용되는 웹브라우저 중에는 인터넷 익스플로러 다음으로 파이어폭스, 오페라가 있다. 웹 기반의 인터넷 환경에서 웹브라우저는 빼놓을 수 없는 도구가 된지 오래다. 이러한 웹브라우저 보안 취약성을 이용해 개인 사용자 컴퓨터에 유입되는 악성코드들이 크게 증가하고 있는 추세다. 보안업데이트를 통해 웹브라우저의 보안 취약점을 방어하는 활동 이외에 안전한 브라우저 제공을 위한 벤더들의 노력이 주목을 끌고 있다. 마이크로소프트사는 올 여름 바이러스나 스파이웨어, 피싱범죄에 대항하기 위해 다양한 보안 기능이 포함된 인터넷 익스플로러 7.0을 선보일 예정이다. 모질라 재단은 파이어폭스의 결함을 발견한 보안 연구자에게 포상금을 주어 그 활동을 지원하고 보상해주는 프로그램을 운영하고 있다. 오페라 소프트웨어는 인터넷에서 방문하는 사이트의 인터넷 보안 등급을 1~3등급으로 나누어 알기 쉽게 보여주고 보안 인증을 갖고 있는 웹사이트인지를 알려주는 브라우저를 발표했다. 이를 기반으로 인터넷 뱅킹이나 쇼핑 사이트에 대한 신뢰를 평가할 수 있는 수단이 가능해졌다.

한국정보보호진흥원(KISA), 홈페이지 개발 보안 가이드 배포

최근 발생되고 있는 대규모 홈페이지 변조 사고는 UNIX 운영체제와 PHP 언어를 사용하는 웹호스팅 서버환경에서 게시판 프로그램 취약점 등을 이용하여 발생되고 있다. 한국정보보호진흥원(KISA)에서는 꾸준한 증가추세를 보이는 홈페이지 변조 사고를 미연에 방지하고자 '홈페이지 개발 보안 가이드'를 제작하여 홈페이지와 인터넷침해사고대응센터(krCERT)를 통해 배포하고 있다. 지난 1월 7일에는 '홈페이지 대량 변조 발생에 따른 주의 경보'를 발령한 바 있다. 웹사이트를 운영하는 보안담당자는 PHP 언어의 외부 사이트의 소스 실행 금지 기능을 해제하고, 운영체제 및 게시판 프로그램은 항상 최신의 보안 패치를 유지하며, 인바운드(Inbound), 아웃바운드(Outbound) 트래픽 제한을 위한 호스트 기반의 방화벽을 운영하는 등 강력한 보안설정을 적용하여 보안사고 예방에 만전을 기하도록 한다.

개인 정보 유출 방지 대책 마련 시급

보안사고의 90% 이상이 의도적이라기보다는 실수에 의해 저질러지는 경우가 대부분이며, 내부자에 의한 정보유출 피해 사례는 전체 보안사고 가운데 비율이 약 70% 이상을 차지한다. 얼마 전 있었던 주요 기업의 대주주 신상 정보 노출 역시 내부자의 안일한 보안의식이 빚어낸 사건으로 기록된다. 최근 들어 학생 1백만 명의 개인정보를 입수하여 화상 강의 업체 등에 팔아 넘기는 등 개인 정보 유출 사고가 끊이지 않고 있다. 외부로 노출된 주민등록번호와 주소 등이 악의적인 사이트의 접속이나 범죄에 이용될 가능성에 대해서는 아직 구체적인 대응방안이 마련되어 있지 못한 상태이다. 주민등록번호가 인터넷 포털 사이트에서 회원가입을 위한 인증 수단으로 가장 흔하게 사용되고 있기 때문에 주민등록번호의 유출 빈도가 가장

높다. 행정기관과 공공기관의 홈페이지에 회원가입 시 주민등록번호 입력이 금지되고 인터넷 게시판에 주민번호가 게재되는 것을 막기 위한 입력방지 프로그램 설치도 의무화 될 예정이다. 앞으로 주민등록번호의 사용은 되도록 제한하도록 하고 주민등록번호를 대체할 다른 실명확인 수단을 모색하여야 할 것이다. 개인 정보 유출의 위험성과 익명성에 따른 위험성의 두 마리 토끼를 잡는 구체적인 방안들이 계속 이어지길 기대해 본다.

Ⅳ. 4월 세계 악성코드 동향

2005년 악성코드와 관련하여 전 세계에서 가장 큰 이슈가 된 사건은 마이톱 웜(Win32/Mytob.worm) 변형의 등장이다. 마이톱 웜은 2005년 2월말 최초로 전파되기 시작한 이래 여러 형태의 변형이 추가로 발견되고 있는 메일을 통해 전파되는 웜이다.
마이톱 웜의 확산 현상은 세계적으로 비슷한 추이를 보이고 있는 것으로 보인다. 악성코드 관련 업체인 중국의 컴퓨터바이러스긴급대응센터나 러시아의 캐스퍼스키 연구소의 경우 마이톱 웜을 2005년 4월 한 달 동안 가장 많이 확산된 악성코드로 발표했다. 1년이 넘는 기간 동안 가장 많이 확산되고 있는 넷스카이 웜을 능가한 수치라는 점에서 마이톱 웜의 향후 추이를 주목해야 할 필요가 있다..

(1) 일본의 악성코드 동향

작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

일본의 정보처리추진기구(IPA www.ipa.go.jp)에서는 2004년도 일본 국내의 악성코드 피해 현황에 대한 조사 자료를 발표했다. 이 조사는 일본의 5000여 일반 기업체와 지역단체 중 조사 대상을 무작위로 선정하여 설문지를 배포하는 방식으로 이루어졌다.

[표1]은 백신프로그램 사용 정도에 대한 통계 자료이다.

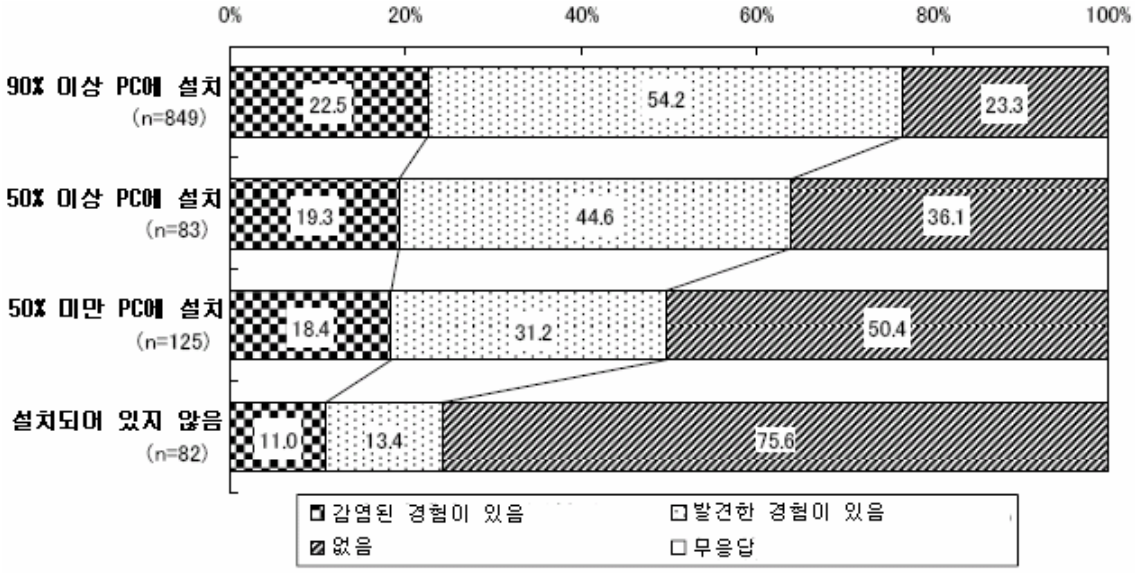
백신 사용도	90% 이상	50% 이상	50% 미만	설치 안됨	무응답
개인용 PC	73.8%	7.2%	10.9%	7.1%	1.0%
네트웍 서버	58.0%	4.4%	3.0%	7.4%	7.2%
로컬 서버	60.6%	5.5%	5.1%	25.0%	3.7%

[표1] 백신 프로그램 사용 현황

자료의 내용으로 미루어볼 때 개인용 PC에서 백신 사용률은 약 80%~90% 정도로 추정해 볼 수 있다. 그러나 개인용 PC의 백신 사용률에 비해 서버로 사용되는 시스템의 경우 백신 사용률이 매우 낮은 것을 알 수 있다. 개인용 PC는 대부분 윈도우 OS를 사용하지만 서버의 경우 윈도우 OS 이외에도 유닉스나 리눅스 등의 OS를 사용하는 경우가 많고 이러한 OS들은 상대적으로 감염 피해의 발생 비율이 적은 것이 서버용 시스템에서 백신 프로그램 사용률이 낮은 원인이 될 수 있을 것이다.

[그림1]의 통계는 기업의 자원을 보호하기 위한 백신 프로그램 사용의 필요성을 알 수 있게 해준다. [그림1]은 개인용 PC에서 악성코드의 발견 경험 유무에 대한 통계이다. 그림의 표에서 볼 수 있는 것처럼 PC에 백신 프로그램이 설치되어 있는 경우와 비교하였을 때 설치되어

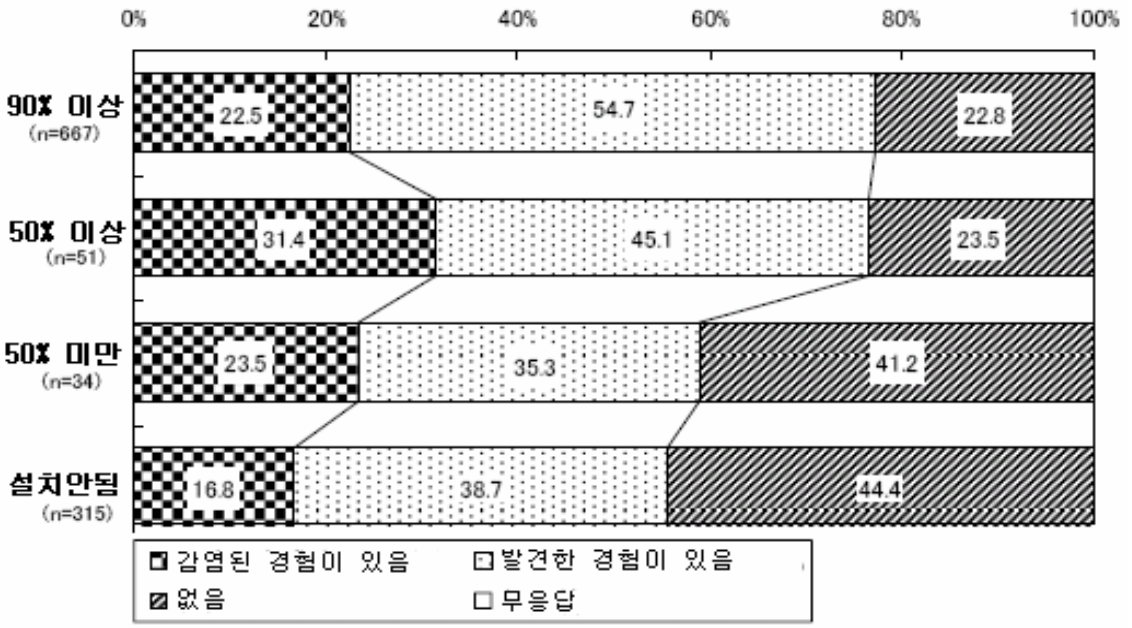
있지 않은 경우 악성코드 검출 정도가 크게 차이가 나는 것을 알 수 있다.



[그림1] 개인 PC의 악성코드 검출 현황

이 자료는 관리자가 감염을 인지한 것에 대한 설문을 실시한 것임을 감안해 보았을 때 백신 프로그램이 설치되지 않은 기업에서는 악성코드의 감염이나 보유 여부를 인지하지 못하였을 가능성이 매우 높다. 기업의 네트워크 환경이나 사업장의 특성에 따라 차이가 있겠지만 개인 PC의 경우 감염 비율이 크게 다르지 않을 것이기 때문이다. 백신 프로그램이 설치되어 있지 않은 PC에서는 악성코드의 발견 비율에 비해 감염 비율이 높은 것 또한 주목할 만 하다.

이러한 현상은 서버로 사용되는 시스템에 대해서도 크게 다르지 않다. [그림2]는 네트워크에 연결된 서버에서의 악성코드 발견 경험 유무에 대한 통계이다. 서버 시스템의 경우 관리자에 의한 관리가 이루질 것이므로 백신 프로그램이 설치되어 있지 않은 네트워크 서버의 경우 개인용 PC에 비해 악성코드가 발견된 비율은 상대적으로 높지만 백신 프로그램이 설치된 서버와 비교해 보았을 때는 수치가 낮은 것을 알 수 있다.

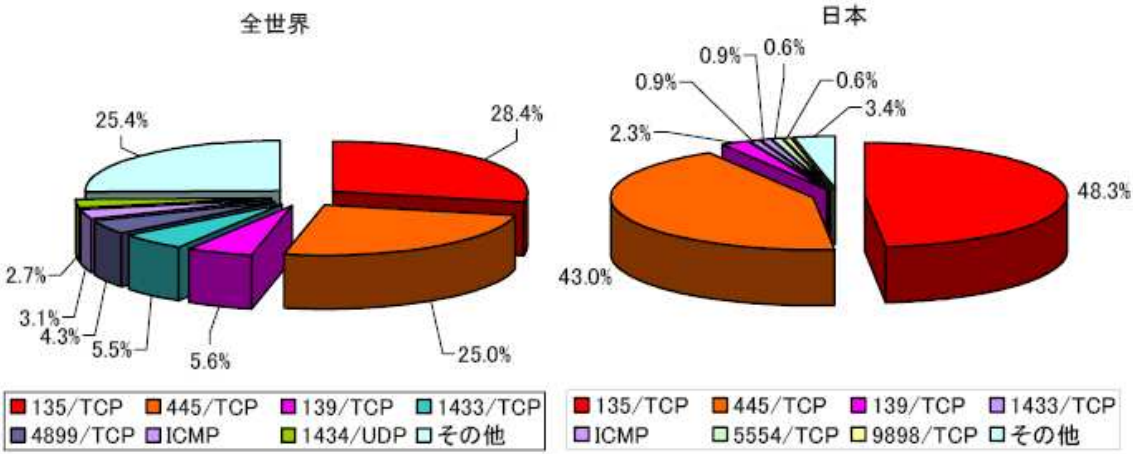


[그림2] 네트워크 서버의 악성코드 검출 현황

네트워크 트래픽 현황

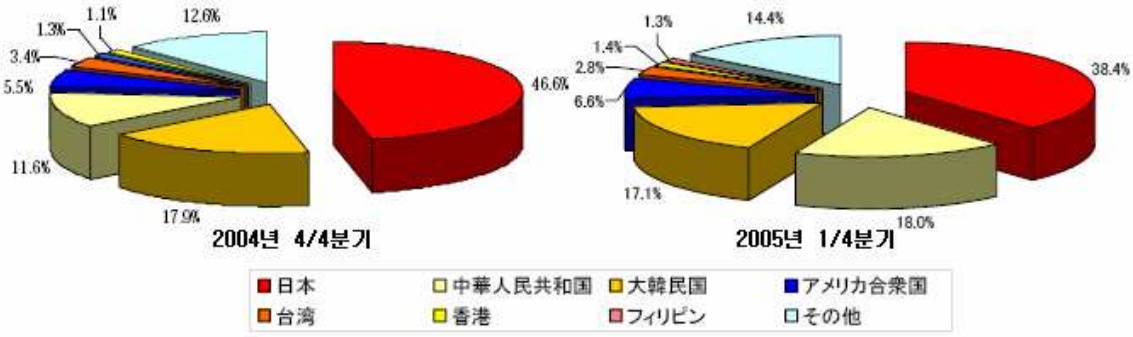
일본 경찰청에서는 2005년 1사분기에 발생한 네트워크 공격 현황에 대한 통계를 발표하였다. 통계의 내용은 일본의 주요 네트워크 거점에 설치된 방화벽과 IDS 등의 로그를 집계한 결과이다.

그림3]은 일본에서 발생한 네트워크 포트(Port)의 사용현황을 나타낸 것이다. [그림3] 왼편의 전세계 통계와 비교하여 보았을 때 일본의 경우 135 TCP와 445 TCP 포트를 통한 트래픽이 매우 많은 것을 알 수 있다. 두 포트는 윈도우 OS에서 사용되는 포트들이지만 최근 유행하는 아이알씨봇이나 새서 웜 등 OS의 취약점을 공격하는 악성코드에서도 사용되므로 주의가 필요하다.



[그림3] 네트워크 사용 포트 현황

[그림4]는 방화벽에서 관측한 네트워크 트래픽 진원지에 대한 통계자료이다. 2004년도에 비해 중국으로부터의 트래픽이 매우 늘어난 것을 알 수 있다. 이러한 트래픽 증가는 2월 말부터 3월 초에 이르는 기간 동안 MS-SQL 서버의 취약점을 이용한 공격이 급증한 것이 원인이다.



[그림4] 트래픽 진원지 통계

(2) 중국의 악성코드 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

4월 중국 악성코드의 동향은 1분기에 이어서 4월 역시 백쯔 웜(TrojanDroper.Worm.Bagz, V3진단명 Win32/Bagz.worm)이 1위를 유지하고 있다. 그럼 4월에는 어떠한 악성코드가 순위권에 진입을 하였는지 그리고 새로 발견되었는지 살펴보도록 하자.

악성코드 TOP 5

순위 변화	순위	Rising
-	1	TrojanDroper.Worm.Bagz
New	2	BackDoor.SdBot
↓ 1	3	Backdoor.Rbot
New	4	Trojan.PSW.QQPass
New	5	Backdoor.Huigezi

[표1] 2005년 4월 라이징(Rising) 악성코드 TOP 5

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

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

[표2] 2005년 4월 컴퓨터바이러스긴급대응센터(CNCVERC) 악성코드 TOP 4

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

[표1]과 [표2]는 중국 백신 업체인 라이징(Rising)과 컴퓨터바이러스긴급대응센터 (이하 CNCVERC)의 악성코드 TOP 5이다. 우선 라이징의 TOP 5부터 살펴보면 새로운 악성코드 3건이 새롭게 순위에 기록되었다. 새롭게 순위에 포함된 악성코드는 4월에 새롭게 발견된 악성코드는 아니며 기존에 발견되었으나 4월 들어 새롭게 순위에 포함된 것이다. 새롭게 순위에 진입한 악성코드 중에서 주목할 만한 악성코드는 Trojan.PSW.QQPass이다. 해당 악성코드는 중국 로컬에서 개발한 QQ 메신저를 전파 경로로 이용한다. QQ 메신저를 이용해서 전파되는 악성코드는 기존에도 발견된 형태들이 많았지만 Trojan.PSW.QQPass와 같이 순위권에 진입한 것은 2005년 올해 처음이다.

CNCVERC의 순위를 살펴보면 1분기 동안 1위를 지키고 있던 넷스카이 웜(Worm_Netsky.D,

V3 진단명 Win32/Netsky.worm)이 2위로 한 단계 내려가고 마이톱 웜(Worm_Mytob.X, V3 진단명 Win32/Mytob.worm)이 새롭게 1위를 차지하였다. 현재 까지도 마이톱 웜은 다양한 변형들이 발견되고 있어 주의를 요하고 있다.

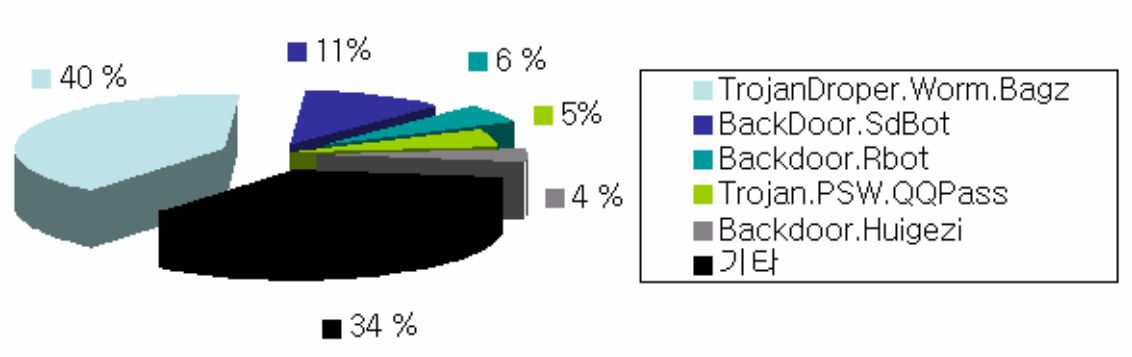
주간 악성코드 순위

순위	1주	2주	3주	4주
1	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz	TrojanDroper.Worm.Bagz
2	BackDoor.SdBot	BackDoor.Sdbot	Backdoor.PCshare	Trojan.PSW.QQPass
3	Trojan.Win32.Lineback	Trojan.Win32.Agent	Backdoor.Huigezi	Trojan.PSW.Lmir
4	Backdoor.Rbot	Backdoor.Rbot	Backdoor.Rbot	Trojan.Win32.Krepper
5	Trojan.PSW.Lmir	Trojan.PSW.Lmir	TrojanDropper.Win32.Delf	BackDoor.SdBot

[표3] 2005년 4월 라이징 주간 악성코드 순위

라이징의 주간 악성코드 순위 변화를 살펴보면 4주 동안 백쯔 웜이 1위를 차지하고 있는 것을 잘 알 수 있다. 그리고 백쯔 웜과 함께 꾸준히 순위에 등장하고 있는 BackDoor.SdBot, Backdoor.Rbot과 같은 악성 아이알씨봇 웜의 변형들(Win32/IRCBot.worm) 역시 순위권 내에 포함되어 있다. 그 외에도 순위권에 포함되어 있는 악성코드 중 특이할 만한 것은 Backdoor.PCshare이다. 해당 악성코드는 정상정인 프로그램인 원격제어 프로그램의 일부 또는 전체를 변형하여 사용하는 경우이다. 주로 드롭퍼 류와 같은 악성코드들에서 사용되는데 외부에서 감염된 시스템을 원격제어하기 위해서 사용되며 한국 또는 기타 지역에서는 정상 파일을 악의적인 목적으로 사용하는 문제로 인해 보안 업체들의 권고문들이 발표되기도 하였다. Backdoor.PCshare가 3주째에서 2위권으로 위치한 것으로 미루어 중국 내에서 원격제어 프로그램을 악의적인 목적으로 활용하는 악성코드의 확산에 주의를 기울일 필요가 있는 것으로 여겨진다.

악성코드 분포



[그림1] 2005년 4월 중국의 악성코드 분포

4월 중국 악성코드 분포를 살펴보면 지난달 전체의 절반이 조금 못 미치는 48%를 차지하던 백쯔 웜이 40%로 지난 달에 비해 8% 감소되었다. 순위상으로는 1위를 차지하고 있으나 전체 분포로 미루어 중국내의 확산이 조금씩 감소 추세를 보이는 것으로 분석된다. 그리고 악성 아이알씨봇 웜의 전체 분포 역시 지난 달에는 총 16%를 차지하였으나 이번 달에는 1% 증가한 17%를 차지하였다. 근소한 차이로 증가한 것으로 보일 수 있으나 1사분기 동안의 상황으로 미루어서는 현상 유지만 지속하고 있는 것으로 분석할 수 있다.
4월 악성코드 분포 전반을 살펴 볼 경우에는 기타에 포함된 다양한 트로이목마 류가 지난 달 24.5%에서 34%로 10% 가량 크게 증가한 것으로 미루어 중국 현지에서는 다양한 형태의 트로이목마가 새로운 위협의 형태로 발전하고 있는 것으로 추정할 수 있다.

4월의 중국 악성코드 동향은 기존의 백쯔 웜과 악성 아이알씨봇 웜들의 감염 수치가 조금씩 떨어지고 지난 달에 이어서 새로운 트로이목마 류가 많은 증가를 보이고 있다. 이러한 트로이목마 류의 증가는 전파력은 기존의 웜 류에 비해서 떨어지지만 감염으로 인한 개인 정보 유출 피해는 웜 보다 더 심각하다고 볼 수 있다. 이러한 위협에 대응하기 위해서는 시스템 사용자들 스스로 출처가 불분명한 파일 등에 대한 주의를 기울여야 한다. 5월에는 이러한 트로이목마 류로 인한 새로운 위협들이 어떻게 증가할 것일지 주목된다.

(3) 세계 악성코드 동향

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

205년 4월의 세계 동향으로 가장 특징적인 것은 많은 마이톱 웜 변형이 새롭게 등장한 것이다. 지난 1년간 피해 동향에는 넷스카이 웜(Win32/Netsky.worm), 마이둠 웜(Win32/MyDoom.worm), 베이글 웜(Win32/Bagle.worm) 등이 차지했고 유럽 지역에서는 자피 웜(Win32/Zafi.worm)이 상위권에 존재했다. 일년간 큰 변화가 없었지만 적게는 1개의 마이톱 웜 변형이 순위에 들었으며 러시아의 캐스퍼스키 연구소(Kaspersky Lab)의 순위에는 1위, 7위, 9위, 14위, 17위, 18위가 모두 마이톱 웜 변형이다. 향후 새롭게 급속히 퍼지는 웜이 등장하지 않는 이상 당분간 이런 체계로 진행될 것으로 보인다. 그 외 소버 웜(Win32/Sober.worm) 변형이 유럽 등지에서 많이 퍼졌지만 한글 윈도우 등의 비 영어권 시스템에서는 웜이 제대로 실행되지 않는 경우가 많아 아시아 지역의 피해는 적었다.

4월에는 휴대폰에서 많이 사용되는 심비안 OS 악성코드가 60여 개 이상 새롭게 등장했다. 다행히 대부분 자체 확산 능력이 없는 트로이목마로 실제 피해를 입힐 가능성은 낮아 보인다. 하지만, 최초의 휴대폰 웜인 카비르 웜(Cabir worm)이 이미 전 세계 20여 개국 이상에서 보고된 점으로 미루어 가벼이 간과할 일은 아니라 생각된다. 휴대폰은 컴퓨터보다 조작에 미숙하고 보안의식이 부족한 많은 사람이 많으므로 향후 휴대폰 악성코드는 많은 문제를 일으킬 수 있다.

.

V. 이달의 ASEC 컬럼 - 64비트 환경과 악성코드

작성자 : 정진성 주임연구원(jsjung@ahnlab.com)

2005년 4월 마이크로소프트(Microsoft, 이하 MS)는 윈도우 XP 64비트(Bit) 버전을 공식 출시하였다. 과거를 돌아보면 1981년 MS는 DOS를 시작으로 하여 윈도우 3.1까지의 16비트 시대가 있었다. 그리고 윈도우 9x부터 윈도우 NT(2000, XP)의 32비트 시대까지 데스크탑 OS는 총 24년이란 시간에 걸쳐 64비트 시대까지 맞이하였다. 앞으로 이 주기는 어떻게 될까? 빌 게이츠는 최근에 열린 MS 하드웨어 개발자 컨퍼런스에서 앞으로 10년은 64비트의 시대라고 얘기했다. 그럼 10년 후에는 128비트 OS가 나올 수 있을지도 모른다는 얘기도 된다.
새로운 OS와 고성능 CPU들이 나올 때 마다 지금 개인 사용자의 컴퓨팅 환경에 최신의 기술들이 필요한 것인지 되묻는 사람들이 많다. 일부 어얼리 어댑터(Early Adapter)들과 파워 유저들의 지적 호기심을 충족하기 위해서는 필요할지도 모르지만 대다수의 일반 유저들은 아직 64비트 윈도우의 출시는 물론 자신이 어떤 버전의 윈도우를 사용하는지 모르는 경우가 많다.

이번 컬럼은 64비트 환경과 악성코드에 대하여 정리해 보면서 어떤 위협이 예상되고 대응방안은 어떤지 간략히 정리해보기로 하겠다.

64비트를 지원하는 대표적인 x86 프로세서
데스크탑에서 64비트를 지원하는 CPU는 2003년 9월 AMD를 선두로 해서 인텔(Intel)도 올 2월에 공식적으로 EM64T(Intel Extended Memory 64 Technology)를 지원하는 프레스캇 코어 기반의 6xx 시리즈의 펜티엄4를 출시하였다. 인텔은 이미 일부 국가에서만 작년 4사분기말부터 EM64T기능이 포함된 펜티엄4F 시리즈를 출시한 적이 있었다. 하지만 틈새시장을 공략하려는 이 제품은 올해 단종시키고, 기존 펜티엄4 프레스캇 코어 기반의 5xx 시리즈에 EM64T를 포함하여 새 제품도 출시할 것이라고 발표했다. 인텔도 이로써 데스크탑 기반의 두 개의 CPU 제품군에서 64비트를 지원하게 되는 것이다.

참고로 인텔의 EM64T 제품은 Itanium/Itanium2 제품이 채용하는 IA-64 아키텍쳐(architecture)와는 달리 기존의 IA-32 아키텍쳐 코드를 확장한 것으로, AMD64 아키텍쳐 제품과 같이 64비트 OS, 어플리케이션에 대응하면서 기존의 32비트 환경과의 호환성이 유지되고 있다.

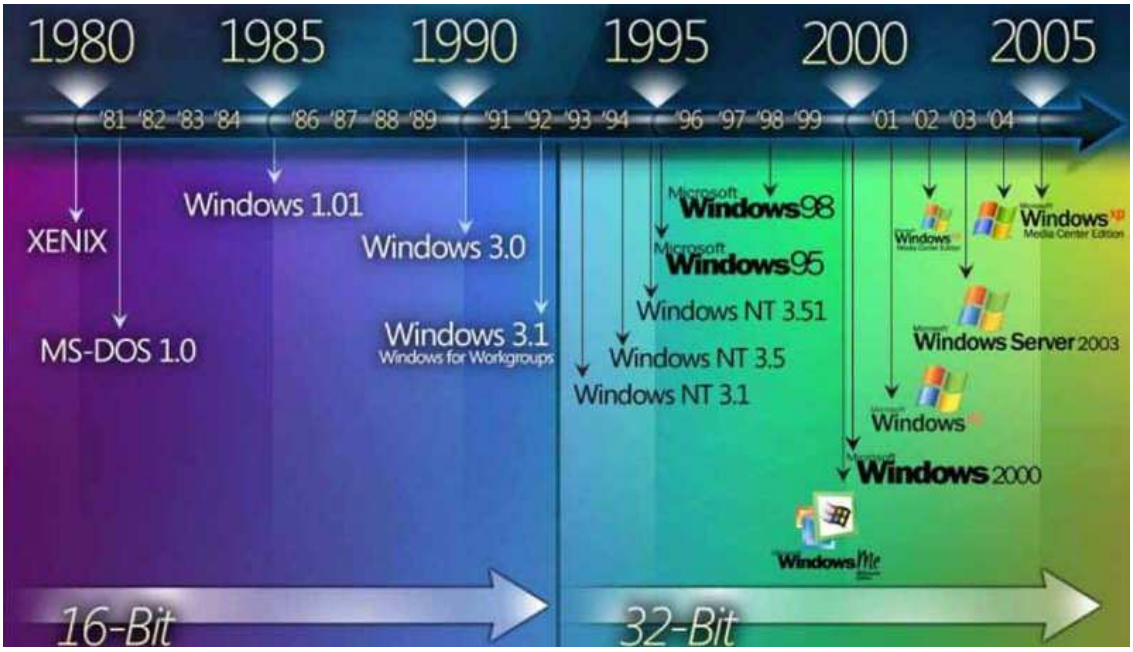
64비트 기술	제조사	CPU	사용환경
IA64	Intel	아이테니엄1,2	서버
AMD64	AMD	애슬론64	데스크탑
32/64 비트 기술	**제조사**	**CPU**	**사용환경**
32/64 비트 동시지원	Intel	제온-노코나 코어	서버
	Intel	펜티엄4,6xx-EM64T 펜티엄4,5xx-EM64T	데스크탑 데스크탑
	AMD	옵테론	서버

[표1] Intel & AMD 의 64비트 지원 CPU

대표적인 64비트 지원 OS

리눅스의 일부 커널들은 오래 전부터 64비트 지원을 하였고 윈도우의 경우 작년부터 베타 테스트를 통한 안정화를 거쳐서 올해 4월 윈도우 XP 64비트와 윈도우 미디어 센터 2005 64비트를 공개하였다.

윈도우는 언급한 것처럼 16비트 시대로부터 약 24년 만에 64비트 OS의 시대로 접어든 것이다.



[그림1] 마이크로소프트사의 OS 역사

인텔의 64비트 지원 CPU 출시에 맞춰서 공식 출시된 윈도우 XP 64비트의 경우 아직까지는 소비자의 구매가 활발하지 않다. 아직은 일부 어얼리 어댑터들이나 개발자 정도만 64비트

OS를 찾고 있는데 이는 32비트 OS가 출시 될 때처럼 드라이버와 응용 프로그램의 부족이 가장 큰 이유이다.

그런데 32비트 시대와는 달리 현재는 네트워크라는 인프라가 상당히 발전하였고 더 많은 사용자들이 H/W의 드라이버 제조사와 응용 프로그램 제작사에게 64비트 지원 드라이버를 요청하고 있다. 따라서 발빠른 그래픽 카드 제조사들은 이미 안정화가 된 공식 64비트 지원 드라이버를 내놓았고 이미지 편집으로도 유명한 S/W 제작사도 기존 제품을 64비트 지원이 되도록 하여 출시하였다. 또한 64비트 CPU와 OS의 장점을 가장 많이 볼 수 있는 게임업체와 3D 모델링 관련 업체들도 64비트 환경을 매우 선호하고 있다.

64비트 악성코드 전망

64비트 지원 OS와 관련 드라이버, 응용 프로그램들도 이제 막 출시되고 있는 가운데 벌써 64비트 악성코드를 점쳐보는 것은 무리가 아닌가 하는 분들이 있을 것이다. 하지만 이미 64비트 악성코드가 만들어져 있다.

감염 아키텍처	악성코드명
IA64	Win64/Rugrat.3344
AMD64	Win64/Shruggle.1318

[표2] 64비트 악성코드명

위 악성코드는 바이러스 유형을 가지고 있으며 IA64, AMD64 CPU와 그에 대응하는 64비트 윈도우 환경에서 정상적으로 감염활동을 한다. 이 바이러스들은 각각 작년 5월, 8월경에 발견되었다. 다행히도 일반 사용자로부터 보고된 경우는 아니고 악성코드를 제작하는 바이러스 제작자가 Proof of Concept으로 제작한 경우이다.

따라서 아직은 64비트 악성코드가 위 2개의 바이러스를 제외하고는 보고된 것은 없다. 하지만 64비트 OS 사용자가 늘어나고 개발환경도 갖춰진다면 32비트 시대에도 그랬던 것처럼 악성코드의 수는 점점 증가 할 것으로 보인다. 또한 상위버전은 언제나 하위버전에 대한 호환성을 가져야 하므로 지금의 32비트 악성코드는 64비트 윈도우 환경에서 별다른 문제없이 감염 활동을 일으킨다. 하지만 일부 유형의 악성코드들은 정상적으로 동작되지 못할 것으로 보는데 대표적인 것은 다음과 같다.

- PE 형태의 윈도우 실행파일을 감염시키는 32비트 바이러스
- 32비트 메모리 내 특정 영역에 대한 후킹을 시도하는 은폐형 악성코드들

64비트 바이러스는 이미 출현하였지만 64비트 윈도우에 대한 메모리 구조 등이 악성코드 제

작자들에게 분석되지 않았기에 아직은 64비트 은폐형 악성코드의 출현으로부터 안심할 수 있을 것으로 예상된다. 하지만 64비트 OS만의 특이한 지원(스크립트 등)으로 새로운 유형의 악성코드가 나타날 수 있는 점은 이미 안티 바이러스 컨퍼런스를 통해서 알려져 있다.

안티 바이러스 업체의 대응

위 글에서 64비트 OS가 정식으로 출시되기 전에 악성코드가 나와서 절망감에 빠졌던 분이 있다면 필자가 곧 얘기할 이야기를 듣고 희망감을 가졌으면 한다. 안철수연구소를 비롯한 대부분의 메이저 안티 바이러스 업체들도 이미 오래 전부터 64비트 악성코드와 환경에 대한 대비를 해두었다. 현재 64비트 지원 서버제품이 출시되어 판매되고 있으며 이는 다른 경쟁사도 마찬가지이다. 일단 64비트 환경을(IA64, AMD64) 지원하는 제품이 있으며 또한 위에서 기술된 64비트 악성코드들도 분석이 완료되어 엔진에 반영된 지 오래이다.
업체들마다 차이는 있겠지만 지금은 어떤 64비트 악성코드가 나와도 대응할 준비가 충분히 되어 있다는 것이다. 특히 64비트 환경에 대한 기존의 32비트 악성코드에 대한 테스트 등도 끝나 기존악성코드에 대한 대응도 준비 되어있다.

국내외 하드웨어 커뮤니티와 OS 커뮤니티에서는 64비트 CPU와 윈도우에 대한 벤치마크가 주를 이루고 있다. 또한 최근 CPU 기술인 멀티코어 CPU에 대한 끝없는 얘기도 쏟아지고 있다. 어얼리 어댑터들과 파워유저들의 전유물이라고만 여겨졌던 64비트 CPU와 OS는 점점 일반 사용자들이 접하기가 쉬워졌다. 이는 하드웨어 업체들의 가격 경쟁 등의 노력이 크다고 하겠지만 최신 기술을 이용하는 것이 이제는 일부 유저들 사이에서만 있는 것 같지는 않아 보인다.

사용하는 사람들이 많기에 그만큼 활동하는 악성코드도 많은 '윈도우'란 OS는 이제 64비트의 시대를 맞이하고 있다. 벌써 악성코드라는 얼룩이 묻어 버린 64비트 윈도우는 그 시작이 많은 사용자들에게 환영을 받고 있지는 않지만 이전 시대와는 다른 네트워크 환경과 지적 호기심이 높아진 사용자들로부터 환영 받는 날도 머지 않아 보인다. 또한 그에 따라 악성코드도 점차 모습을 드러낼 것으로 보여져 환경이 변했다고 해서 결코 안심할 수 없는 게 보안이라는 생각을 해 본다.