ASEC Report 5월

® ASEC Report

2006. 6

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. 5월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자: 이철수 연구원(lcstop@ahnlab.com)

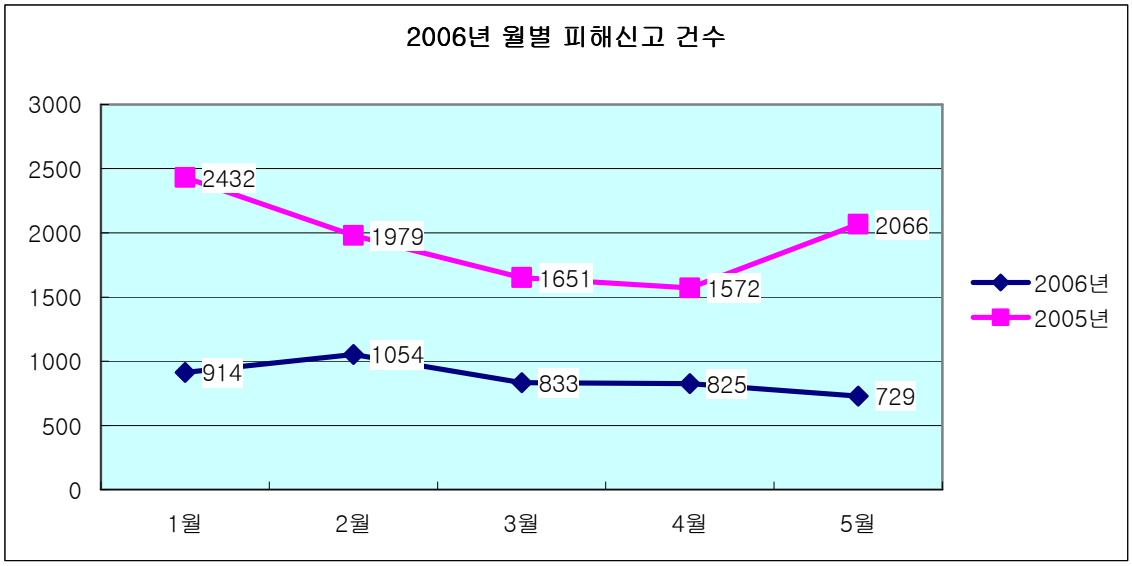
순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.Gen	170	23.3%
2	↑3	Win32/Bagle.worm.19666	26	3.6%
3	new	Win32/Zasran.worm.47138	9	1.2%
4	new	Win32/Bagle.worm.Gen	7	1.0%
5	new	Win32/Bagle.worm.27136	7	1.0%
6	new	Win-Trojan/Downloader.12288.S	5	0.7%
7	new	Win32/Maslan.C	5	0.7%
8	new	Win32/Bagle.worm.21700	5	0.7%
9	new	Win-Trojan/Vundo.38925	4	0.5%
10	new	Win32/DllBot.worm.28100.E	4	0.5%
		기타	487	66.8%
합계			**729**	100.0%

[표1] 2006년 5월 악성코드 피해 Top 10

5월 악성코드 피해 동향

2006년 5월 악성코드 피해 동향은 피해 Top 10 중 3위에서 10위까지 악성코드의 대부분이 5월에 발견된 신종(변형) 악성코드라는 점과 악성코드 피해건수가 2006년 들어 가장 적은 달이었다는 점이 특징이다. 2006년 5월 악성코드 피해건수는 총 729건으로, 이는 전년 동월 2,066건의 35.2%에 불과한 수치이다.

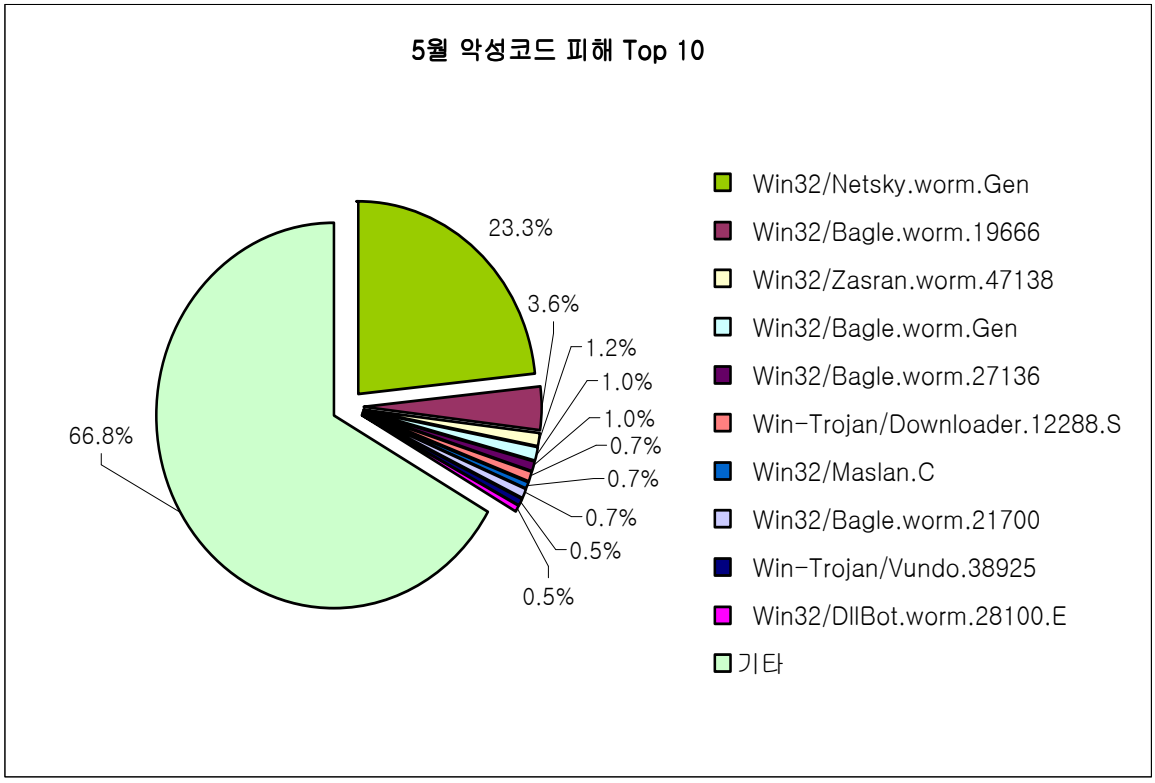
또한 5월 피해신고 된 악성코드 중 피해건수가 10건 미만인 악성코드는 전체 피해건수의 73.1%에 해당하는 533건으로, 5월은 다양한 악성코드로부터 피해가 접수되었으나 그 피해는 크지 않았던 것으로 보인다.



[그림1] 2006년 월별 피해신고 건수

악성코드 피해 Top 10 중 4종류의 베이글 웜이 순위를 차지하고 있으며, 전월에 많았던 조톱 웜과 마이톱 웜은 순위에서 사라졌다. 그러나 넷스카이 웜(Win32/Netsky.worm.Gen)은 여전히 Top 10의 순위 1위를 유지하고 있으며, 윈도우 실행 파일을 감염시키는 텡가 바이러스(Win32/Tenga.3666)는 3월과 4월에 증가 추세를 보이다가 5월에는 발견되지 않았다.

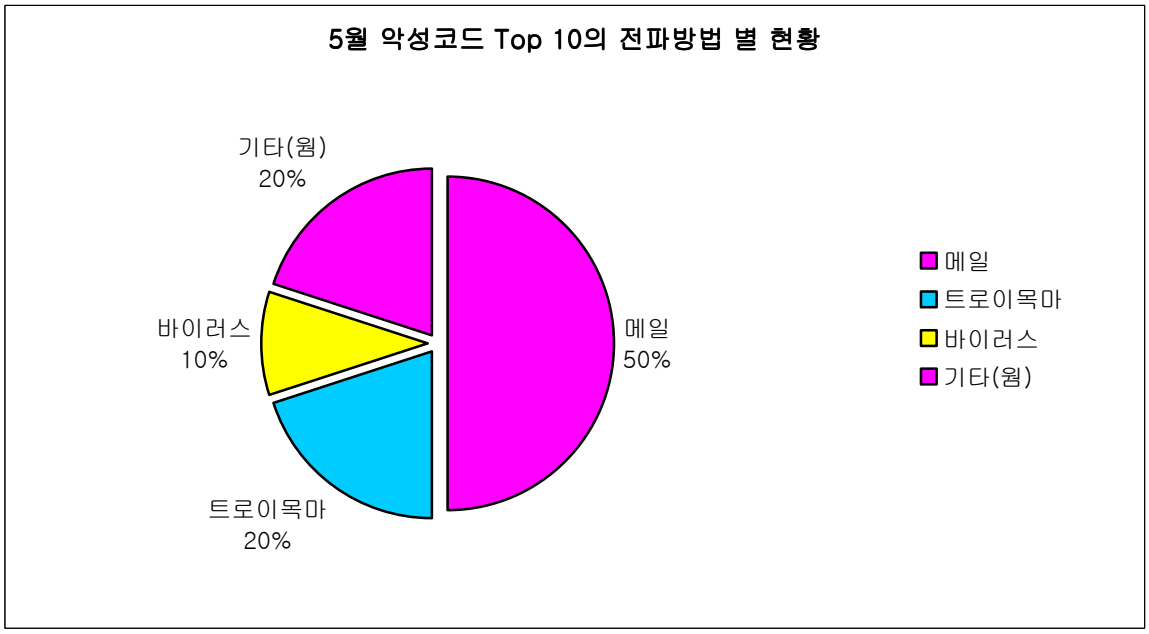
5월의 악성코드 피해 Top 10을 도표로 나타내면 [그림2]과 같다.



[그림2] 2006년 5월 악성코드 피해 Top 10

5월 악성코드 Top 10 전파방법 별 현황

[표1]의 Top 10 악성코드들은 주로 어떠한 감염 경로를 가지고 있는지 [그림3]에서 확인할 수 있다.

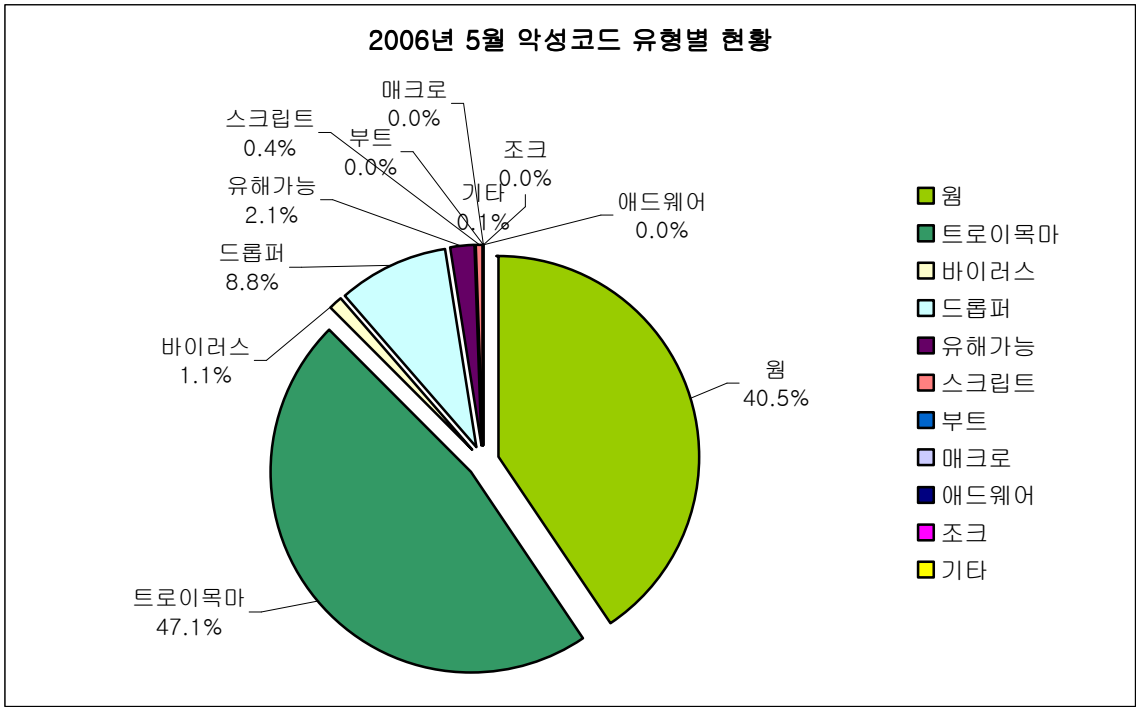


[그림3] 2006년 5월 악성코드 Top 10의 전파방법 별 현황

메일로 전파되는 특징이 있는 매스메일러는 50%, 트로이목마와 바이러스가 각각 20%, 10%를 차지했다. 특히 2006년 들어 계속 감소추세를 보였던 매스메일러는 4월에 일시적으로 증가추세를 보였으나 이내 5월 들어 다시 감소추세를 보였다.

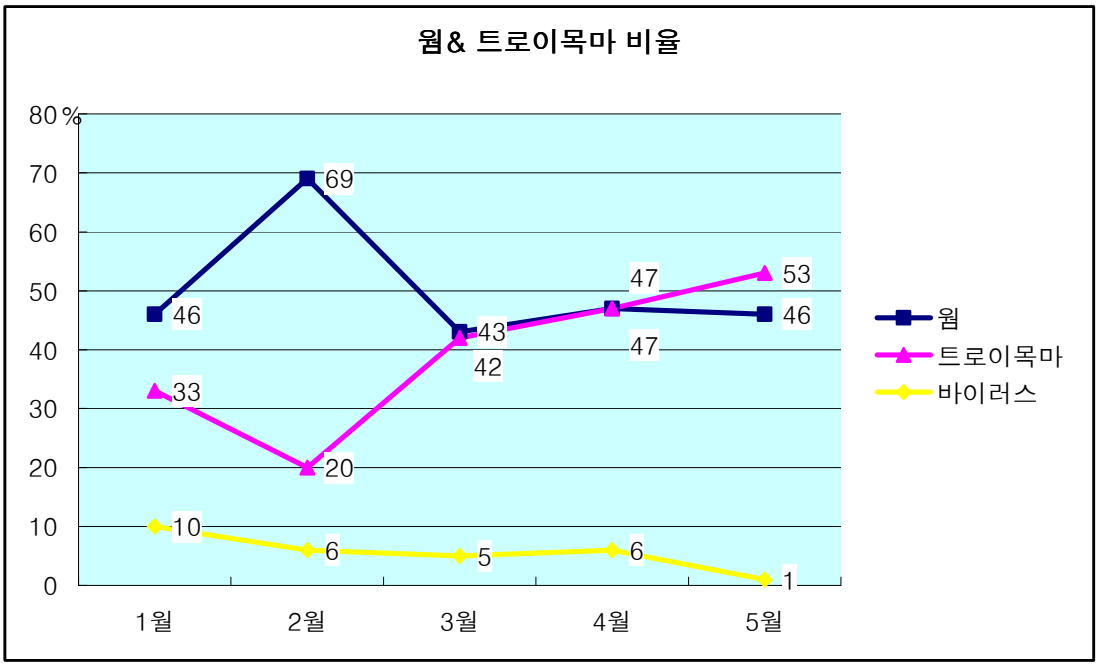
피해신고 된 악성코드 유형 현황

2006년 5월에 피해신고 된 악성코드의 유형별 현황은 [그림4]와 같다.



[그림4] 2006년 5월 피해 신고된 악성코드 유형별 현황

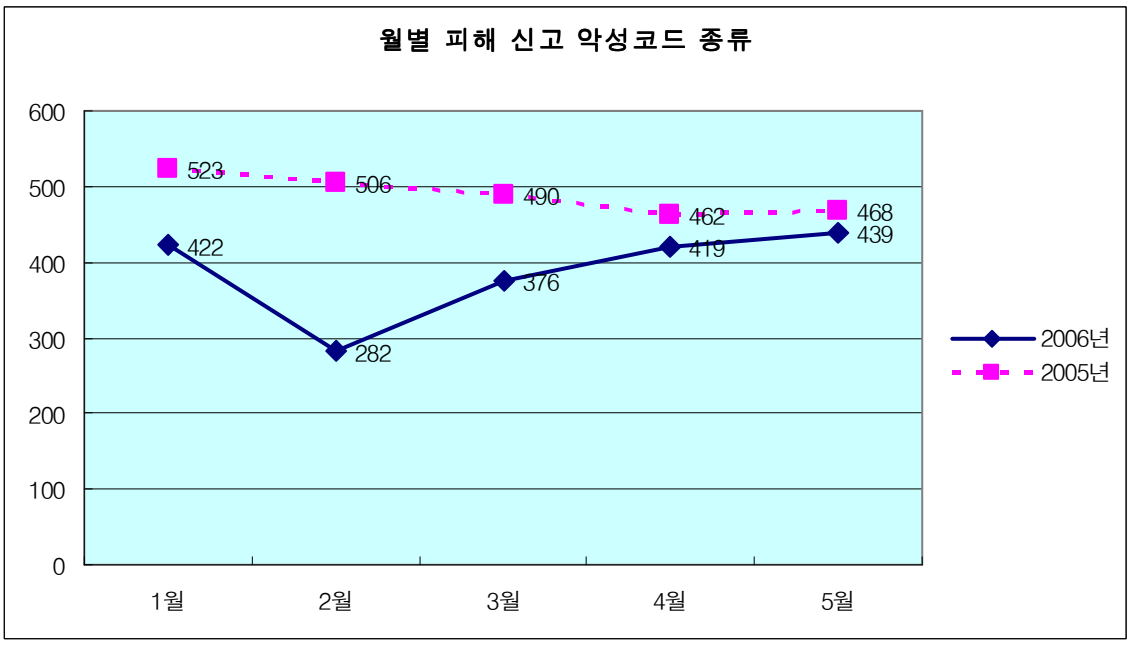
5월 피해신고 된 악성코드 유형 중 웜은 40.9%, 트로이목마는 47.1%씩을 차지하고 있는 가운데 드롭퍼와 바이러스가 각각 8.8%와 1.1%를 차지하였다. 지난해부터 트로이목마에 대한 피해가 증가추세를 보이더니 4월에는 웜과 트로이목마가 차지하는 비율이 동일하게 나타났으며, 5월에는 [그림5]에서 보는 것과 같이 트로이목마가 웜을 추월했다. 게임의 계정을 탈취하는 트로이목마의 피해는 전월에 비해 증가하였고, 특정 게임의 계정을 탈취하던 이전 형태와 달리 다수의 온라인 게임의 계정을 탈취하는 형태의 트로이목마로 인한 피해는 증가하였다. 일부 미디어 파일을 삭제하는 트로이목마가 발견 되기도 하였다. 바이러스에 의한 피해는 2월~4월에 비해 낮은 비율을 보이고 있다.



[그림5] 2006년 월별 웜, 트로이목마 피해신고 비율

월별 피해신고 된 악성코드 종류 현황

5월에 피해 신고된 악성코드 개수는 모두 439개로, 이는 전년도 동월에 비해 29건 정도 감소한 수치이지만, 2006년 2월 이후 지속적인 증가추세를 보이고 있어 앞으로 그 추세를 주의 깊게 지켜보아야 하겠다.



[그림6] 2005년, 2006년 월별 피해신고 악성코드 개수

(2) 신종(변형) 악성코드 발견 동향

작성자: 정진성 주임연구원 (jsjung@ahnlab.com)

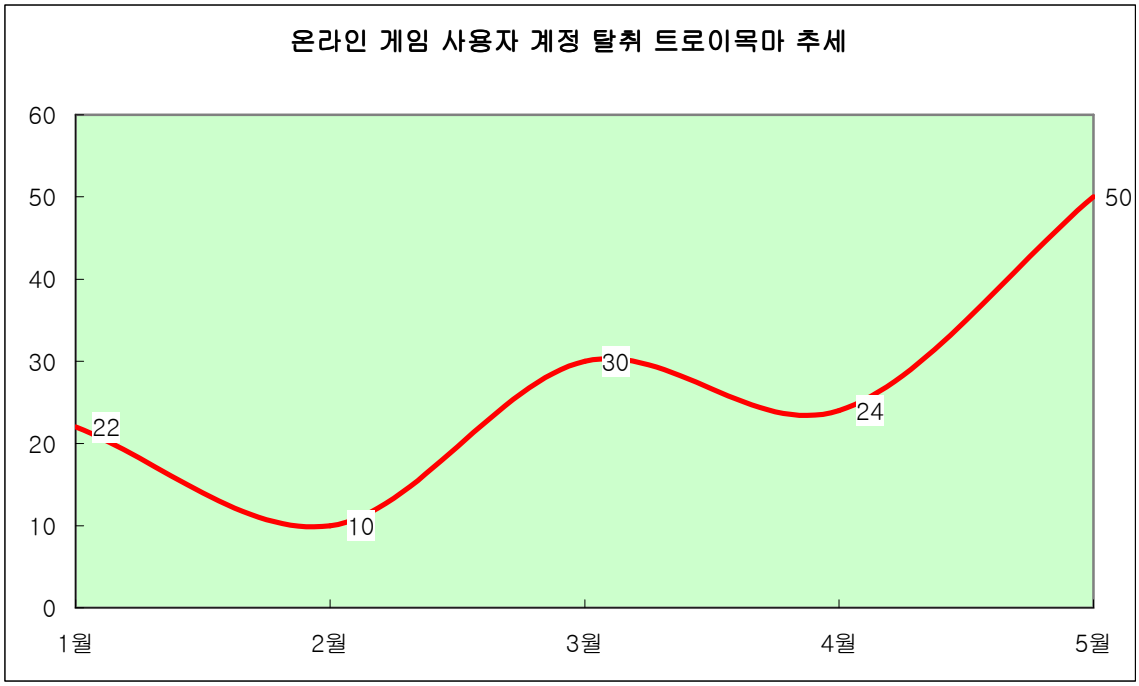
5월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1], [그림2]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
51	297	49	1	1	0	0	0	14	0	413

[표1] 2006년 5월 유형별 신종 (변형) 악성코드 발견현황

5월에는 올해 들어 가장 많은 413개의 악성코드가 발견, 보고 되었다. 특히 트로이목마의 수가 큰 폭으로 증가하였는데, 새로운 형태의 트로이목마보다는 기존에 알려진 트로이목마 변형 발견건수가 크게 증가하였다. 또한 트로이목마를 드롭(Drop) 하는 드롭퍼 (Dropper)도 트로이목마의 증가로 소폭 증가하였다.

[그림1]은 국내에 많은 피해를 주고 있는 온라인 게임의 사용자 계정을 탈취하는 악성코드에 대한 2006년도 월 발견 건수를 그래프로 나타낸 것이다.



[그림1] 온라인 게임 사용자 계정 탈취 트로이목마 현황

위에서 언급한 것처럼 기존에 발견 되었던 트로이목마들의 변형이 증가하면서 그 중 하나인 '온라인 게임의 사용자 계정'을 탈취하는 트로이목마도 증가 하였다. 전체 신종(변형) 악성코드 발견 증가의 큰 원인이었던, 5월에 많이 발견된 트로이목마 변형을 정리하면 다음과 같다.

► 휴피곤 트로이목마(Win-Trojan/Hupigon)

은폐기능을 가진 이 트로이목마는 중국산으로, 백도어 모듈을 인터넷 익스플로러에 인젝션(Injection)한 후 동작한다. 은폐기능 때문에 감염여부를 확인하기 어렵고 인터넷 익스플로러를 통한 외부 접속을 시도하므로 일부 TCP/IP 모니터링 프로그램에서는 이를 백도어에 의한 외부 접속임을 알아채지 못할 수도 있다.

► 리니지핵 트로이목마(Win-Trojan/LineageHack)

온라인 게임의 사용자 계정을 탈취하는 트로이목마 중 하나로 최근에는 실행파일을 감염 시키는 바이러스 형태도 보고 되었다. 이러한 형태는 감염된 파일을 실행하면 감염되지 않은 다른 파일도 감염시키고 트로이목마를 생성하거나 또는 특정 호스트에서 다운로드 받아와 실행하기도 한다. 동작방식은 트로이목마의 모듈을 실행중인 프로세스들에만 인젝션 한 후 특정 게임이 실행된 것을 인지한다. 그리고 사용자 계정을 훔쳐내어 특정 호스트로 80/TCP를 통하여 ASP 폼 메일 형태로 발송한다.

► 다운로더 트로이목마(Win-Trojan/Downloader)

일반적으로 특정 호스트로부터 트로이목마나 스파이웨어를 다운로드 하는 악성코드를 진단할 때 사용되는 대표적인 진단명이다. 증상은 특정 호스트로부터 파일을 다운로드 하여 실행하는 증상만 있다. 경우에 따라서 호스트 파일을 변조하기도 하는 등 다운로더 이외의 증상을 갖는 경우도 있다.

► 피씨클라이언트 트로이목마(Win-Trojan/PcClient)

중국산 트로이목마로 알려져 있으며 커널모드 은폐증상을 갖는다. 일반적인 백도어 증상을 갖는다.

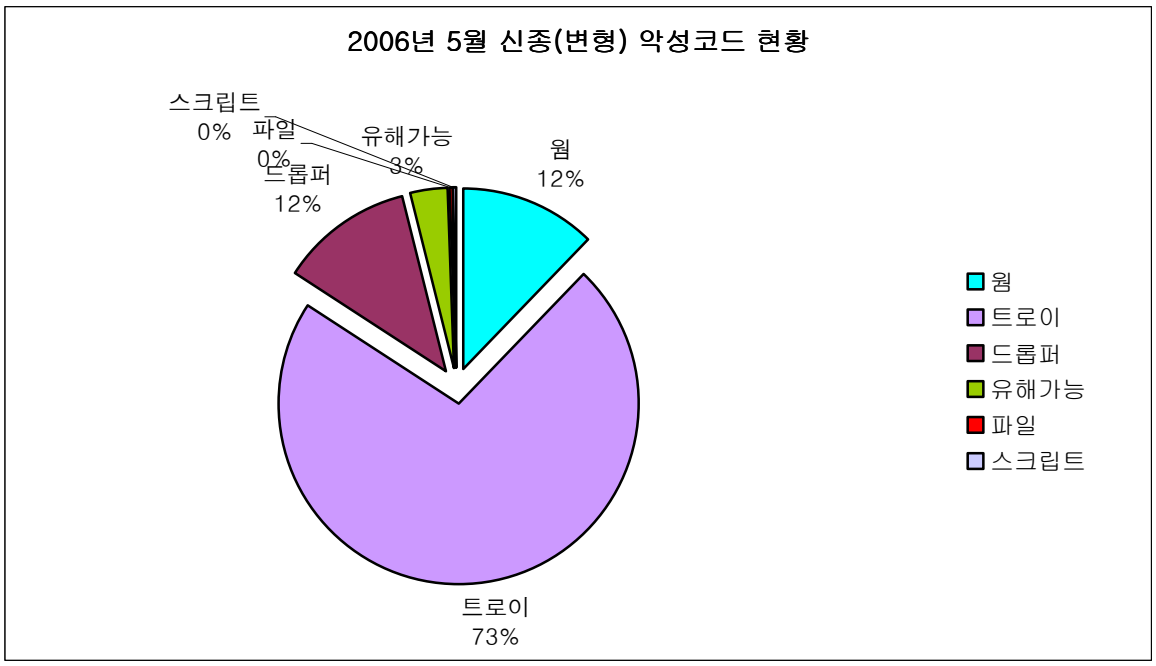
► 페이크얼럿 트로이목마(Win-Trojan/FakeAlert)

가짜 안티 스파이웨어류를 진단할 때 일반적으로 사용되는 진단명이다. 실제로 시스템에 문제가 없지만 거짓정보를 출력하여 사용자로 하여금 과금을 유도하게 한다. 주로 외산이 많으며 똑같은 프로그램이 UI 만 변경하여 일부 유해한 외국 사이트에서 설치 되거나 다운로더 트로이목마로부터 설치되는 경우도 많다.

► 즈롭 트로이목마(Win-Trojan/Zlob)

악의적인 트로이목마나 스파이웨어 등을 다운로드 하는 다운로더의 일종이다. 특징으로는 시스템 프로세스인 Winlogon.exe 에 자신을 쓰레드(Thread)로 인젝션 한 후 동작한다. 따라서 Winlogon.exe 가 파일을 다운로드 하고 실행하는 것으로 보이므로, 개인방화벽을 설치한 사용자도 이를 정상적인 동작으로 인식해 인터넷을 액세스하려는 접근제어 경고창에서 '허용'을 선택하여 설치되는 경우가 많다.

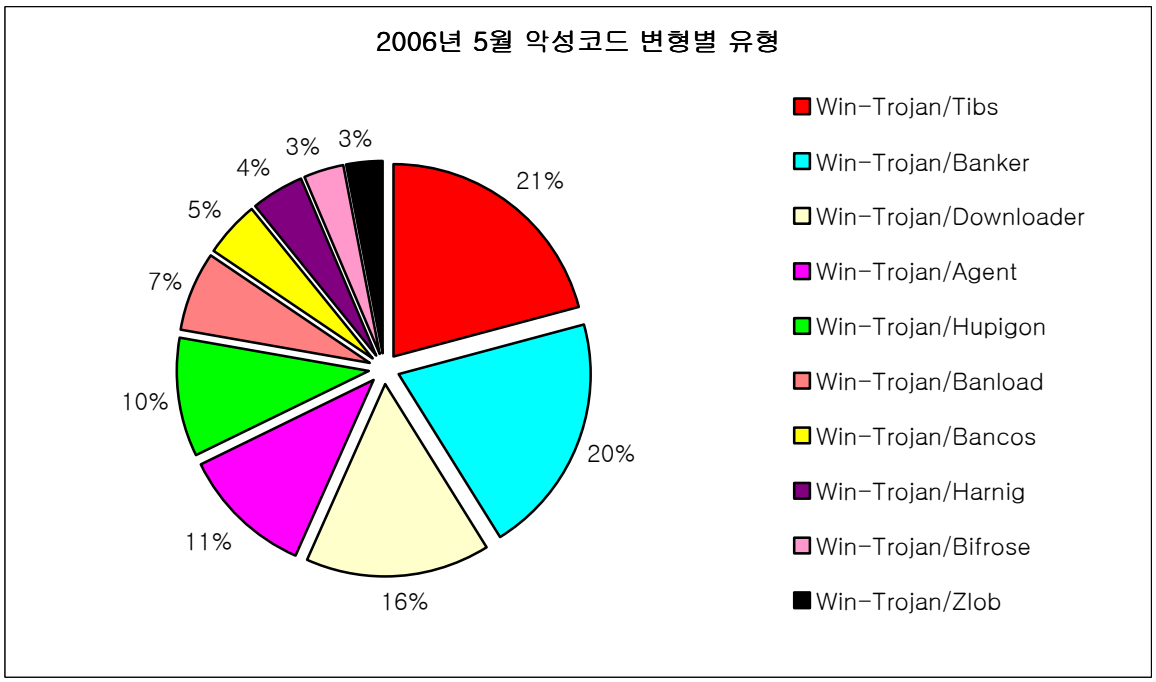
[그림2]은 5월 신종(변형)악성코드의 비율을 나타낸 것이다.



[그림2]2006년 5월 신종(변형) 악성코드 비율

트로이목마 비율은 지난달과 비교하여도 약 10% 정도 상승하였다. 웜은 지난달 18% 12% 로, 5월에는 소폭 하락하는 추세를 보였다.

다음은 5월달에 엔진에 추가된 악성코드에 Top 10 에 대한 비율을 확인해 보자.



[그림3] 악성코드 변형별 유형 및 분포율

이번달 트로이목마의 증가의 원인에서도 언급한 다운로더 트로이목마, 휴피곤 트로이목마, 즈롭 트로이목마 변형들이 눈이 띈다. 이는 정보유출에 대한 관심과 주의가 필요한 가운데 개인정보 유출을 노리는 '트로이목마' 가 증가 하고 있다는 것을 보여주는 것이다.

5월 주요 신종(변형) 악성코드 정리

2006년 5월에 발견된 악성코드 중 주요한 것을 살펴보면 다음과 같다.

► 랜섬 트로이목마(Win-Trojan/Ransom)

국외에서는 보통 '랜섬웨어(ransomware)' 라고 알려진 트로이목마이다. 일반적으로 오피스 문서나 프로그램 소스 파일 등의 사용자 데이터를 암호화 한 후 이를 풀 수 있는 비밀번호를 알기 위해서 '돈'을 요구하는 형태의 트로이목마를 일컫는다. 그러나 이번에 알려진 랜섬 트로이목마의 경우는 실제로 사용자의 데이터를 암호화하지는 않는다. 대신 불필요한 화면을 여러 개 띄운 후 시스템 리소스를 차지하게 되는데, 일반적으로는 이를 실행금지 시키기 어렵도록 해두었다. 따라서 감염되면 정상적으로 컴퓨터를 사용하는데 무리가 따르며 이를 해결하기 위해서는 일정금액을 제작자로 추정되는 이에게 보내야 한다. 아직 국내에서는 피해 사례가 보고 되지 않았다.

► 암호화된 채널을 지원하는 P2P와 이를 이용한 악성 아이알씨봇 웜

암호화된 채널을 이용하여 명령을 주고 받는 악성 아이알씨봇 웜이 보고 되었다. 이 악성코드는 암호화된 통신을 지원하는 P2P 기술을 사용하는 것으로 알려져 있다. 해당 P2P는 8/TCP를 사용하며 패킷 자체가 암호화 되어 있어 일반적으로 IPS, IDS 와 같은 어플라이언스에서 'bypass' 될 가능성이 높은 것으로 보고 되었다.

► 뎃낫 바이러스(Win32/Detnat) 변형

온라인 게임의 사용자 계정을 탈취하는 증상이 있는 트로이목마를 다운로드하고, 감염 전 원본 파일을 압축하여 바이러스 내부에 보관하는 등 치료하기 까다로운 뎃낫 바이러스 변형이 보고 되었다. 다행히 큰 피해는 없었지만, 실행파일을 감염시키는 증상이 있어 향후에는 좀 더 위협적인 형태의 변형이 출현할 가능성도 배제할 수 없다.

► 알려지지 않은 MS 워드 취약점

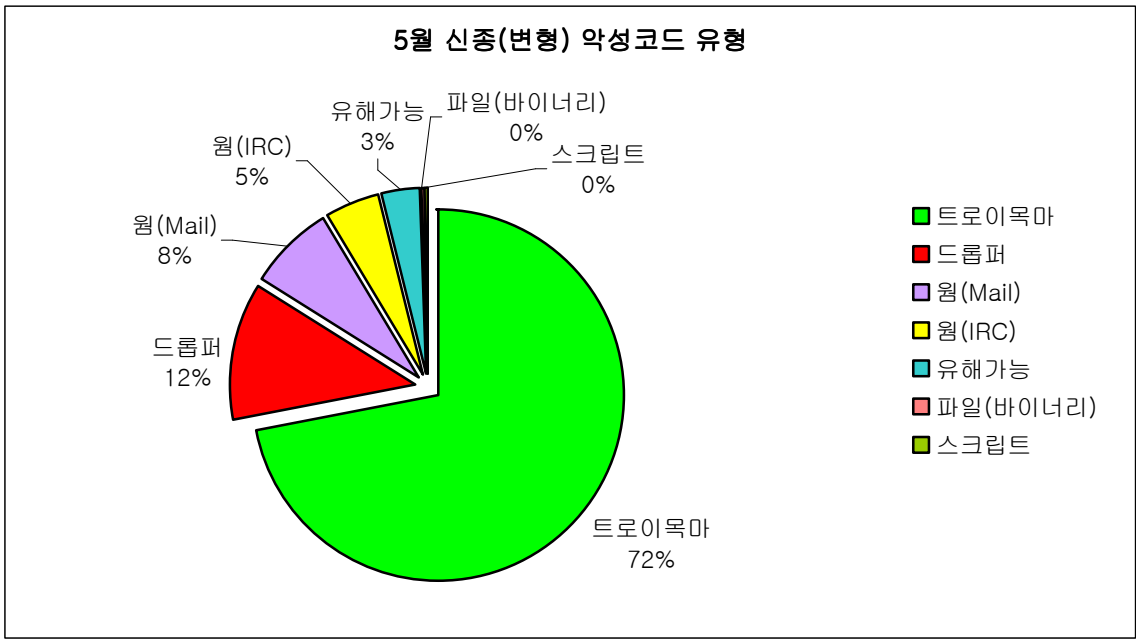
알려지지 않은 MS 워드 취약점이 포함된 워드 문서 파일이 발견되었다. 이 파일은 중국에서 제작된 것으로 추정되며, 이 문서에 포함된 MS 워드 취약점은 Smart Tag 데이터 구조의 유효하지 않은 크기 때문에 문제가 발생한다고 알려져 있다. 그러나 아직 MS의 공식적인 보안 패치가 발표되지 않은 상태이다. 이 취약점이 포함된 워드 문서는 광범위하게 확산 되지 않았으며 국외에서 일부 보고 된 것으로 보인다. 문서 내 포함된 악성코드는 은폐증상을 갖는 트로이목마이다. 일부 트로이목마는 OS 환경 때문인지 파일이 제대로 생성 되지 않는 문제점도 있었지만 역시 최근에 확인된 샘플은 한글 워드에서도 완벽하게 파일이 생성되고 시스

템이 트로이목마에 감염 되었다. 보안패치 이외에는 뚜렷한 방법이 없기 때문에 예방을 위해서는 사용하는 안티 바이러스 제품의 엔진을 최신으로 유지 시키는 것이 좋다. 대부분의 안티 바이러스는 취약점이 포함된 워드문서 자체를 진단한다. 또한 출처가 불분명한 워드 문서는 열어보지 않는 등의 주의를 기울이는 것도 필요하겠다.

► 자스란 웜(Win32/Zasran.worm) 확산

독일에서 제작된 것으로 추정되는 이 웜은 월드컵 티켓 관련 메시지를 일부 담고 있어서 화제가 되기도 하였다. 하지만 이는 극히 일부이고 웜이 자신을 메일로 보낼 때 사용하는 내용은 외설적인 내용이 대부분이다. 웜의 특징으로는 메일을 보낼 때 본문을 텍스트가 아닌 .gif 형태의 이미지로 보내며 암호가 설정된 ZIP 또는 RAR 형태의 압축파일로 자신을 첨부한다. 암호는 메일의 본문에 랜덤한 숫자로 표시되어 있다. 웜의 메인 모듈은 DLL 형태로 프로세스에 인젝션되며 특정 호스트에서 자신의 또 다른 변형을 다운로드 하기도 한다. 메인 모듈 자체는 실행 압축된 형태로, 발견된 변형 모두 조금씩 다른 형태를 보이고 있었다.

다음은 5월에 발견된 신종(변형) 악성코드에 대한 유형별 분포이다. 트로이목마가 차지하는 비율이 높아, 상대적으로 적은 비율을 차지하는 웜 유형에 대한 주의가 소홀해 질 수 있다. 그러나, 수동적인 감염형태를 보이는 트로이목마에 비해 웜은 발견되는 신종(변형)의 수는 작지만 자체 전파 능력을 통한 큰 확산력을 지니고 있어 사용자의 피해가 많이 발생하므로, 트로이목마 못지 않게 웜에 대한 피해에 대해서도 주의를 기울여야 하겠다.



[그림4] 5월 신종 (변형) 악성코드 유형별 현황

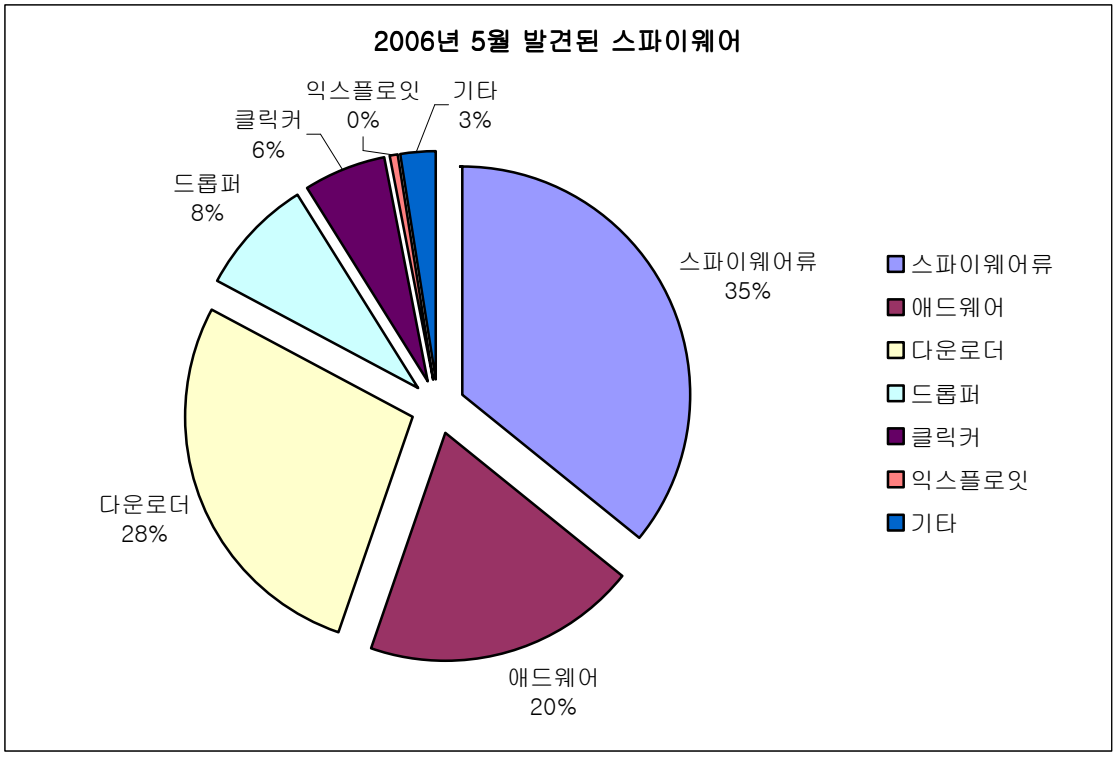
II. 5월 AhnLab 스파이웨어 동향

작성자: 박호진 주임연구원(hojinpk@ahnlab.com)

5월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표1], [그림1]과 같다.

스파이웨어류	애드웨어	다운로더	드롭퍼	클릭커	익스플로잇	기타	합계
236	129	183	55	38	3	17	661

[표1] 2006년 5월 유형별 신종(변형) 스파이웨어 발견 현황



[그림1] 2006년 5월 발견된 스파이웨어 프로그램 비율

5월에는 신종(변형) 스파이웨어[1]의 활동이 감소하였으며, 특히 스파이웨어류(Win-Spyware)[2]가 약세를 보였다. 드롭퍼는 하나의 실행파일에 다른 실행 가능한 파일을 가지고 있다가 특정한 시기에 지정된 폴더에 설치하여 감염시키는 패턴을 보인다. 특히 멀드롭(Win-Dropper/MulDrop)은 다수의 실행 가능한 파일을 가지고 있어, 다수의 스파이웨어를 감염시킬 수 있다.

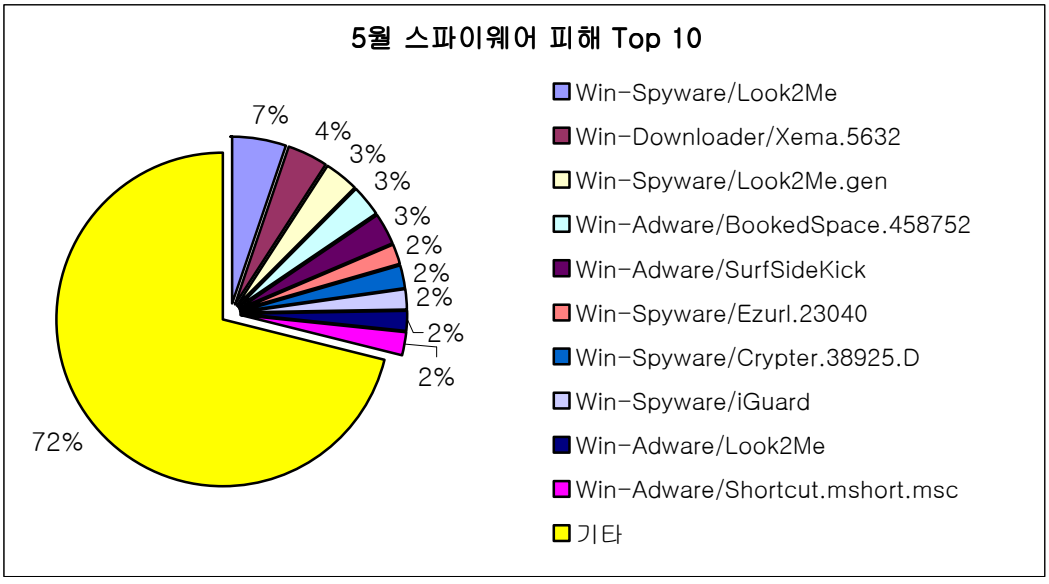
다운로더와 드롭퍼가 지난달에 비해 각각 3%, 6%의 증가를 보이고 있는데, 이는 5월초 즈롭 다운로더(Win-Downloader/Zlob), 즈롭 드롭퍼(Win-Dropper/Zlob)의 변형이 다수 발견된 것이 주요인이다.

[1] 스파이웨어(Spyware): 스파이웨어, 애드웨어 등을 총칭
[2] 스파이웨어류(Win-Spyware): 스파이웨어 카테고리상의 명칭

한편, 5월말에는 미디어티켓츠 애드웨어(Win-Adware/MediaTickets) 변종이 다수 발견되었고 클릭스프링 애드웨어(WIn-Adware/ClickSpring) 등 미디어티켓츠와 관련 있는 다른 애드웨어들도 발견되었다.

순위		스파이웨어 명	건수	비율
1	↑3	Win-Spyware/Look2Me	5	5%
2	New	Win-Downloader/Xema.5632	4	4%
3	↑5	Win-Spyware/Look2Me.gen	3	3%
4	New	Win-Adware/BookedSpace.458752	3	3%
5	↑2	Win-Adware/SurfSideKick	3	3%
6	New	Win-Spyware/Ezurl.23040	2	2%
7	New	Win-Spyware/Crypter.38925.D	2	2%
8	↑1	Win-Spyware/iGuard	2	2%
9	New	Win-Adware/Look2Me	2	2%
10	New	Win-Adware/Shortcut.mshort.msc	2	2%
		기타	69	71%
합 계			97	100%

[표2] 2006년 5월 스파이웨어 프로그램 피해 Top 10



[그림2] 2006년 5월 스파이웨어 피해 Top 10

5월 스파이웨어 피해 Top 10 에는 3가지의 룩투미 진단명이 순위를 차지하고 있는 등 룩투미 스파이웨어의 지속적인 강세가 이어지고 있다. 또한 5월에 순위에 새롭게 진입하며 4위를 차지한 북드스페이스(Win-Adware/BookedSpace.458752)는 윈도우에 BHO(Browser Helper Object)로 등록되어 인터넷 익스플로러와 같이 동작하며, 사용자가 인터넷 서핑 중에 팝업 광고창을 띄어 불편을 초래하는 특징을 가지고 있다.

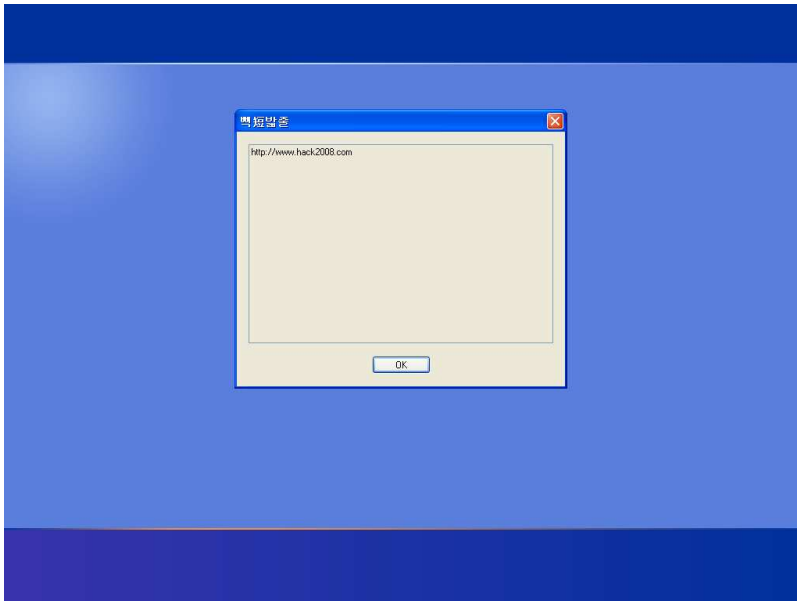
레지스트리 변경을 통해 윈도우 관리자 권한을 제거하는 스파이웨어

핵2008 (Win-Spyware/StartPage.Hack2008.15872)은 인터넷 익스플로러의 시작 페이지를 변경하고, 윈도우 로그인시 특정 메시지를 출력하는 등 윈도우 레지스트리를 변경하며, 특ㅈ경 레지스트리 값을 변경하거나 레지스트리 편집권한을 제거하여 변경된 레지스트리를 사용자가 수정할 수 없도록 하는 증상을 가지고 있다.

이 스파이웨어류는 [그림3]과 같이 시작프로그램에 등록되어, 윈도우가 시작될 때마다 악의적인 동작을 수행한다.

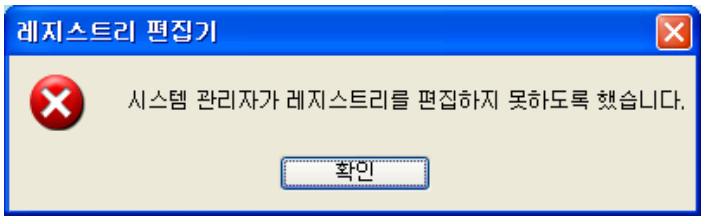
[그림3] 윈도우 시작프로그램에 등록된 결과

이 스파이웨어류가 실행되면 사용자 로그인시 [그림4]와 같은 메시지가 출력하는데, 이는 감염된 스파이웨어류와 관련된 사이트 URL을 표시하여 사용자로부터 불편을 야기시킨다.



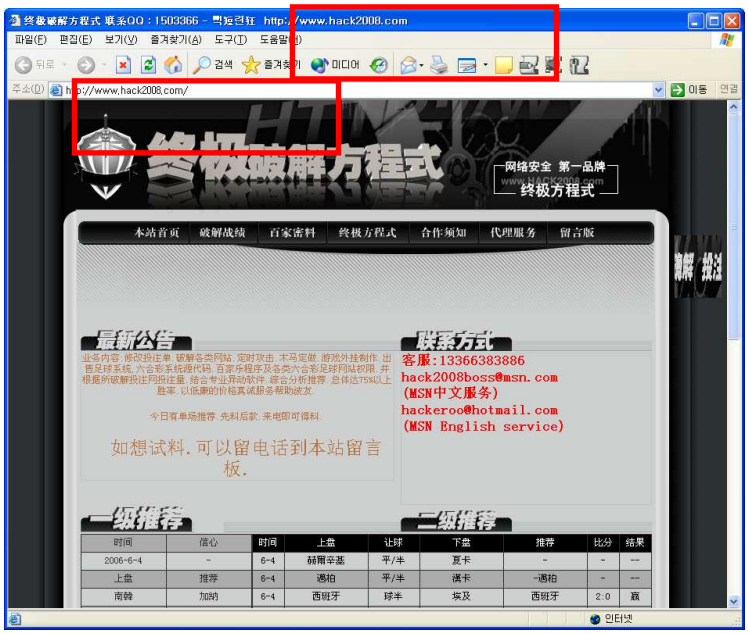
[그림4] 윈도우 로그인 시 특정 메시지 출력

또한 사용자가 레지스트리 값을 수정하기 위해 레지스트리 편집기를 실행하면 [그림5]와 같은 메시지를 출력하여, 사용자가 레지스트리를 수정할 수 없도록 한다.

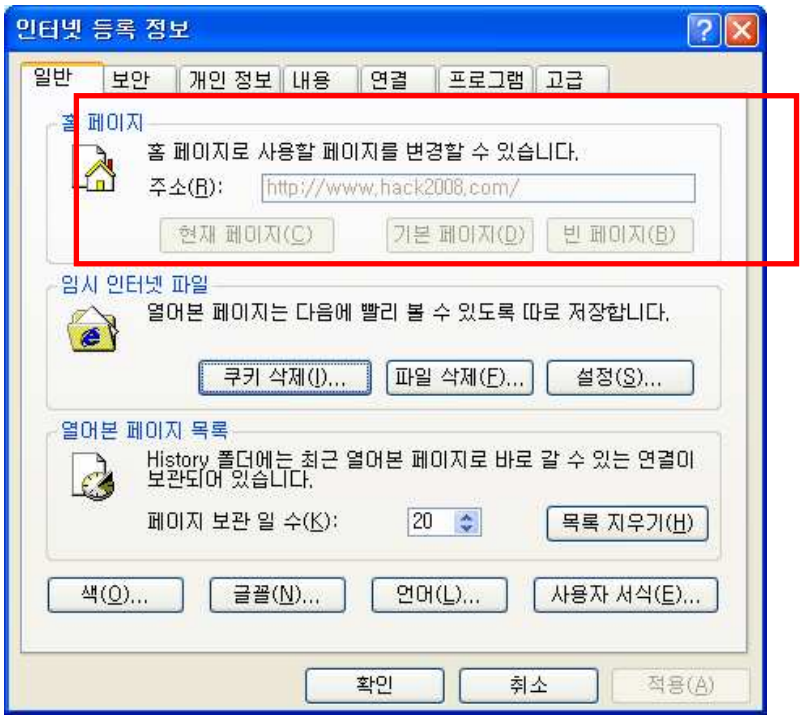


[그림5] 레지스트리 편집 금지 메시지

또한 인터넷 익스플로러를 실행할 때 나타나는 홈 페이지를 감염시킨 스파이웨어와 관련된 홈페이지로 이동시키고, 인터넷 익스플로러의 타이틀을 [그림6]과 같이 변경하며, 사용자가 이를 수정할 수 없도록 인터넷 등록정보에서 홈페이지 설정 관련 버튼을 [그림7]과 같이 비활성화 시킨다.



[그림6] 인터넷 익스플로러의 타이틀 바와 시작페이지 변경된 화면



[그림7] 인터넷 익스플로러의 홈 페이지 설정이 비활성화된 화면

이렇게 변경된 설정을 수동으로 해결하기 위해서는 다음과 같은 명령을 도스 창에 입력하여 레지스트리 편집기를 실행할 수 있도록 한 후, 레지스트리 편집기를 이용해 변경된 각 항목의 삭제하거나 변경하여야 한다.

```
C:₩>reg delete HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Policies₩System /v DisableRegistryTools
```

이렇듯 사용자가 조금만 부주의할 경우 스파이웨어가 PC에 설치되는 것은 쉽다. 또한 안티스파이웨어 제품이 설치되어 있는 스파이웨어는 제거해 준다 하더라도 사용자가 개인의 취향에 맞게 설정해 놓았던 옵션들을 다시 설정해야 하는 것 또한 여간 번거로운 일이 아닐 수 없다. 따라서 평소에 스파이웨어가 설치되지 않도록 다운로드되는 파일들을 꼼꼼히 살피며 주의를 기울이는 습관이 필요하겠다.

III. 5월 시큐리티 동향

작성자: 정관진 주임연구원(intexp@ahnlab.com)

올해 들어 작년과 달리 제로데이(0-day) 취약점이 공개되는 경우가 늘어났다. 일반적으로 보안업계에서는 취약점을 발견하면 발견자가 해당 업체에 발견사실을 통보하고 패치 또는 해결책이 나오기 이전까지는 공개적으로 발표하지 않는 것이 일반적이다. 그러나 근래 들어서는 이를 무시한 채 취약점을 바로 공개함으로써 사용자가 위험에 노출될 수 있는 가능성을 크게 높여주고 있다. 5월에도 마이크로소프트사 워드 프로그램의 취약점이 공개되면서 워드를 이용하는 사용자에게 또 다른 위협을 안겨주고 있다.
제로데이 공격의 증가는 공개되는 시점에 패치가 존재하지 않아 다른 취약점에 비해서 위험성이 크다는 것이다. 앞으로 이러한 행보는 계속 이어지리라 보이며 이번 워드 취약점 패치는 6월 마이크로소프트사의 정기 보안 패치 때 제공되리라 예상된다.

5월에 주요 취약점 현황[1]

이번 달에는 MS사의 정기 보안 패치가 총 3개 발표되었다.

위험등급	취약점	공격코드 유/무
MID	Microsoft Distributed Transaction Coordinator의 취약점으로 인한 서비스 거부 문제점(MS06-018)	무
HIGH	Microsoft Exchange의 취약점으로 인한 원격 코드 실행 문제점(MS06-019)	무
HIGH	Adobe사의 Macromedia Flash Player의 취약점으로 인한 원격 코드 실행 문제점(MS06-020)	무
HIGH	MS Word 0-day 취약점	유
HIGH	RealVNC Password Authentication Bypass 취약점	유

이 밖에도 많이 사용하고 있는 브라우저 파이어폭스의 취약점을 패치한 버전이 발표되었으며 MAC OS X , QuickTime 의 취약점 패치도 발표되었다. 또한 원격접속 프로그램으로 많

[1] 취약점 현황은 ASEC 의 보안전문가들에 의해 공격코드 유/무, 악성코드 활용가능성, 취약점의 위험도등 다양한 관점에서 판단하여 선별된 것으로, 사용자들의 주의가 필요한 것임을 나타낸다. 공격코드의 존재유무는 이 리포트를 작성하는 시점에서 인터넷 상에서 접할 수 있는 기준으로 작성되었다.

이 사용하고 있는 VNC 에 취약점이 보고되어 이에 대한 주의가 요망된다. 현재 VNC 의 공격코드가 넓게 퍼져 있는 것으로 보고되어 있다.

► MS 워드의 알려져 있지 않은 취약점을 이용한 트로이목마

MS 워드의 취약점을 이용하는 트로이목마가 보고 되면서 제로데이의 위험성을 다시 한번 보여주고 있다. 사용자는 해당 취약점에 대해 인지하고 있지 못한 만큼 아무런 의심 없이 워드 파일을 실행하게 되고 이를 통해 악성코드가 설치되는 것이다. 이번 취약점은 워드 XP 또는 워드 2003에 영향을 미치는 것으로, 서비스거부(DoS) 또는 임의의 코드실행이 가능하다.

취약점은 특정한 객체(Object)가 추가된 문서를 읽는 과정에서 포인터(Pointer)연산을 제대로 처리하지 않는 곳에서 존재한다. 사용자가 관리자 권한으로 로그인 되어 있는 경우 이 취약점을 악용한 공격자는 프로그램의 설치, 보기, 변경, 데이터 삭제 등과 같은 권한을 얻게 되어 시스템을 완전히 제어할 수 있게 된다. 하지만, 이 취약점을 이용한 공격에 성공하기 위해서는 사용자의 개입이 필요하게 된다.

이 취약점을 이용한 공격에는 조작된 파일을 사용자에게 메일 또는 웹으로 전달하여 사용자가 오픈하는 경우 임의의 코드를 실행할 수 있게 된다. 현재까지 몇몇 악성코드들[1]이 발견되었으며 한글 오피스 워드에도 해당 취약점이 영향을 미치는 것을 자체 테스트에서도 확인하였다.

공격자는 조작된 워드 파일 안에 실행시키고자 하는 쉘 코드를 위치시켜 임의의 명령어를 실행할 수 있게 된다. 이 글을 쓰는 시점까지 마이크로소프트사의 공식적인 패치는 발표되지 않았다. 다만 임시적인 해결책은 MS 워드 실행 시 Safe Mode(winword.exe /safe)로 실행하는 것이다. 이외 신뢰할 수 없는 워드 문서를 웹이나 메일에서 다운로드 하지 않는 것이 바람직하다.

► 간단히 알아보는 비스타(Vista) 의 새로운 보안 기능

윈도우의 차기 버전인 비스타 출시가 늦어지면서 이에 대한 궁금증이 더욱 커져가고 있다. 현재 2007년 2사분기에 출시예정인 윈도우 비스타는 지금보다 보안적인 면에서 많은 부분을 강화하였는데 간단히 살펴보면 다음과 같은 것들이 있다.

[1] Win-Trojan/Dropper.142848, Win-Trojan/Dropper.27648 등

(1) 윈도우 서비스의 강화

정책이 적용되어 권한이 제한되었다. 예를 들어, RPCSS 서비스가 레지스트리나 다른 파일을 제어할 수 없는 것과 같다.

(2) 버퍼오버런 방지 기능

윈도우 XP SP2 에서 DEP 라 불리는 기능으로, NX 기술 확장 및 오버플로우 방지기술이 포함되어 있다 (64bit 윈도우에서는 기본적으로 적용됨).

(3) 커널 패치 보호 및 드라이버 인증

커널 패치 방지 기술의 도입과 커널 드라이버의 디지털 인증을 도입한 것으로 현재 악성코드에서 사용하는 루트킷의 사용에 제한이 따를 것으로 보인다.

(4) 사용자 계정 권한 제어

관리자 권한을 분리하여 사용자는 사용자 권한만을 가지고 있게 되어 관리자 권한을 필요로 하는 명령어 수행 시는 인증이 필요하다.

(5) 새로운 로그인 아키텍쳐

(6) 다양한 보안 프로그램

윈도우 보안센터를 통해 악성코드 검색, 방화벽 등의 기능을 제공한다.

(7) IE7 의 보안적 기능 강화

권한이 최소화된 상태에서 동작하여 악성코드 설치에 제약이 따를 것으로 보이며 URL 데이터 처리과정에서 예상되는 공격을 감소시켰고 XSS 의 공격을 방지 한다. 또한 최근 늘어나고 있는 피싱(Phishing) 방지 기능 등도 포함되어 있다.

이외 여러 가지 보안적 기능들이 강화되었는데 비스타 출시 이후 과연 어떠한 보안적 변화가 생길지는 지켜볼 일이다. 현존하는 많은 문제를 예방할 수 있도록 디자인 되어 있지만 공격자는 새로운 공격기법들을 계속 찾아내는 만큼 아무리 보안적으로 뛰어난 소프트웨어가 나온다 하더라도 보안에 대한 사용자의 관심과 주의는 계속되어야 할 것이다.

Ⅳ. 5월 세계 악성코드 동향

2006년 5월 세계 악성코드 동향은 지난 4월과 비교하여 큰 변화를 보이지 않고 있다. 일본의 악성코드 동향에서는 여전히 매스메일러 웜들의 강세가 이어졌으며, 트로이목마가 정부기관이나 신문사를 사칭하여 메일로 배포되는 사고도 발생하였다. 이에 반해 중국의 악성코드 동향에서는 여전히 트로이목마 형태가 큰 강세를 보이며 웜 형태는 전혀 찾아 볼 수 없어, 유럽 지역과는 전혀 다른 양상을 보이고 있다. 유럽 지역의 경우에는 매스메일러 웜의 강세가 뚜렷한 반면 트로이목마 형태의 악성코드는 순위권에 전혀 포함되지 못하고 있다. 이러한 각국의 다양한 악성코드 동향을 바탕으로 일본과 중국 그리고 세계의 악성코드 동향을 살펴보도록 하자.

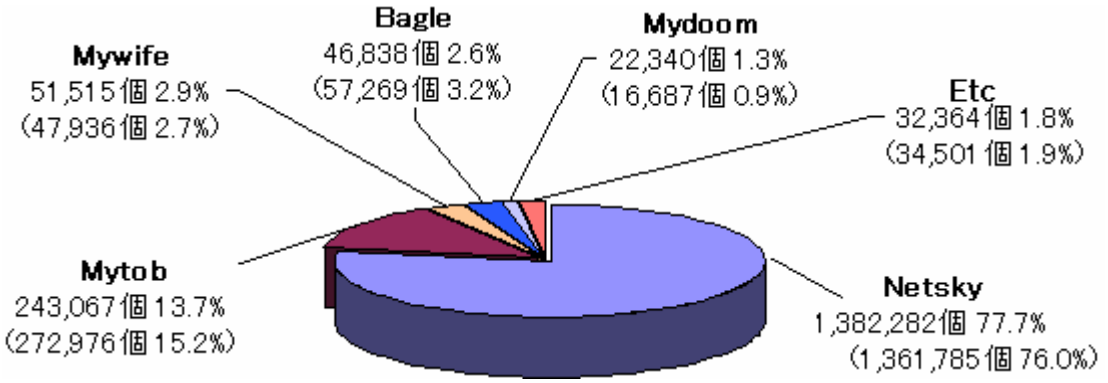
(1) 일본의 악성코드 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

최근 일본에서는 정부 기관이나 신문사 등에서 보낸 것처럼 위장한 메일을 이용하여 악성코드를 유포하는 사례가 발견되었다. 해당 악성코드의 경우 자체에 매스메일러의 기능을 가지고 있지 않으므로 많이 확산되지는 않았으나, 키로거와 백도어 기능을 가지고 있기 때문에 감염된 사용자의 경우 개인 정보 유출의 가능성이 매우 높다. 특히 첨부파일이 MS 오피스에서 사용되는 문서 파일이나 미디어 파일과 동일한 아이콘파일을 이용하고 있어 사용자들이 파일 확장자를 제대로 인지하지 못한 상태에서 실행할 경우 피해를 당할 가능성이 높다. 따라서 감염 피해 예방을 위해 발신자가 불분명하거나 첨부파일의 확장자가 exe나 pif 등 실행할 수 있는 형태의 파일이 첨부된 메일은 열지 말고 삭제하는 것이 중요하다. 또한 백신 제품을 이용하여 악성코드로 의심되는 파일을 검사해 보는 것도 피해 예방을 위해 바람직한 방법이다.

일본 악성코드 동향

2006년 5월 한 달 동안 일본의 악성코드 동향에서 가장 주목할 사항은 전 월과 비슷하게 전체적인 감염 피해가 점점 감소 추세를 나타내고 있다는 점이다. 이는 매스메일러 웜의 확산 피해가 줄어들고 있는 것이 원인으로 생각된다. [그림1]은 악성코드 유형 별 탐지 현황을 그래프로 나타낸 것인데 탐지 숫자에서 알 수 있는 것처럼 대부분의 악성코드의 탐지 건수가 전월과 비슷하거나 줄어든 것을 알 수 있다. 이러한 현상이 발생한 원인을 판단하기는 어렵지만 앞으로도 동일한 현상이 계속되는지 여부에 관심을 가질 필요가 있다.



[그림1] 악성코드 종류 별 탐지현황

2006년 5월 일본에서 가장 많은 확산을 보인 악성코드는 넷스카이 웜(Win32/Netsky.worm)이며 이는 전 월과 동일하다. 그러나 전 월에 이어 5월에도 감염 피해 수치가 연초에 비해 많이 하락한 것을 알 수 있다. 이러한 현상은 마이톱 웜(Win32/Mytob.worm)과 같은 다른 매스메일러들도 동일하게 나타나고 있다. 이외에도 순위에는 없지만 5월 말 경 새롭게 발견된 웜인 자스란 웜(Win32/Zasran.worm)의 감염 피해도 보고되고 있다.

Window/Dos Virus	금월피해 전월피해	Macro Virus	금월피해 전월피해	Script Virus	금월피해 전월피해
Win32/Netsky	888 826	Xm/Laroux	22 18	VBS/Redlof	31 26
Win32/Mytob	372 347	W97M/X97M/P97M/Tristate	8 8	VBS/Lovelette r	11 14
Win32/Mywife	284 221	XF/Sic	5 3	VBS/Soraci	1 2
Win32/Mydoom	280 258	W97M/Marker	1		
Win32/Bagle	244 216	WM/Cap	1		
Win32/Klez	175 169	X97M/Divi	1		

[표1] 악성코드 피해 신고 현황(출처: 일본 IPA)

악성코드의 감염 경로 별 통계

[표2]는 악성코드 감염 경로 별 통계를 나타낸 것으로써 메일을 이용해 전파되는 악성코드가 가장 많은 양을 차지하고 있는 것을 확인할 수 있다. 메일 이외에는 네트워크를 이용한

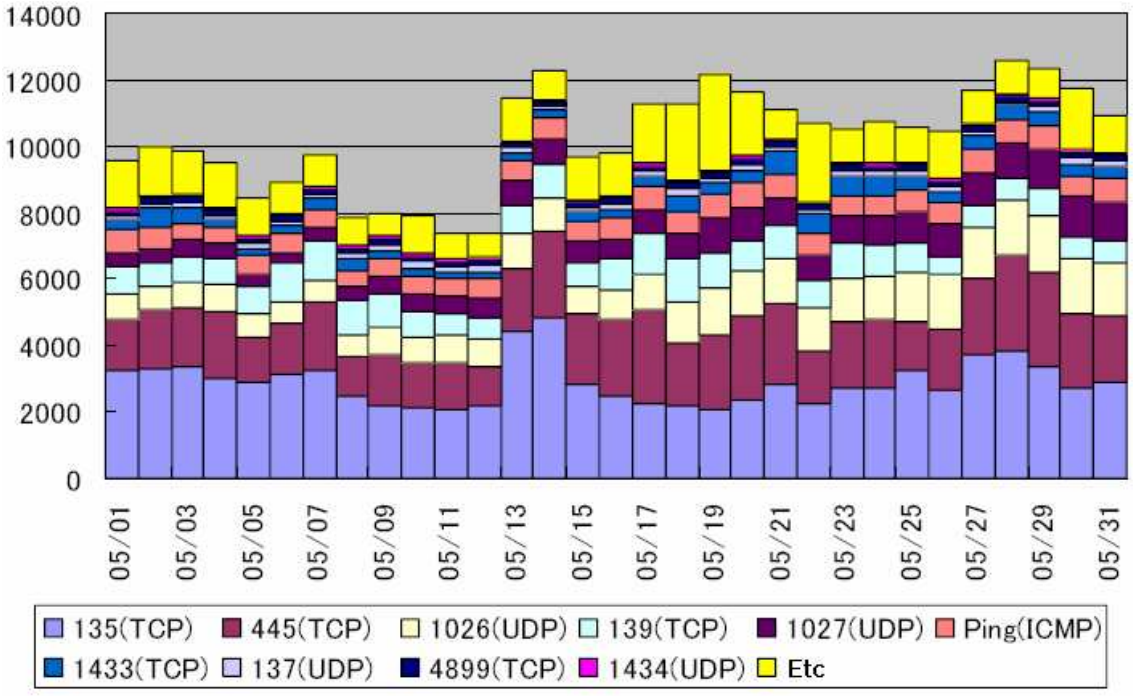
악성코드가 많이 발견되고 있음을 알 수 있다. 또한 총 합계가 전월에 비해 매우 많이 줄어든 것을 볼 수 있다.

감염경로	피해 건수					
	2006년 5월		2006년 4월		2005년 5월	
메일	3,552	97.3%	3,433	97.1%	4,943	98.4%
외부의 모체	0	0.0%	1	0.0%	5	0.1%
다운로드	0	0.0%	1	0.0%	2	0.0%
네트워크	98	2.7%	98	2.8%	59	1.2%
기타	1	0.0%	4	0.1%	12	0.2%
합계	3,651		3,537		5,021	

[표2] 악성코드 감염 경로 통계(출처: 일본 IPA)

일본 네트워크 트래픽 현황

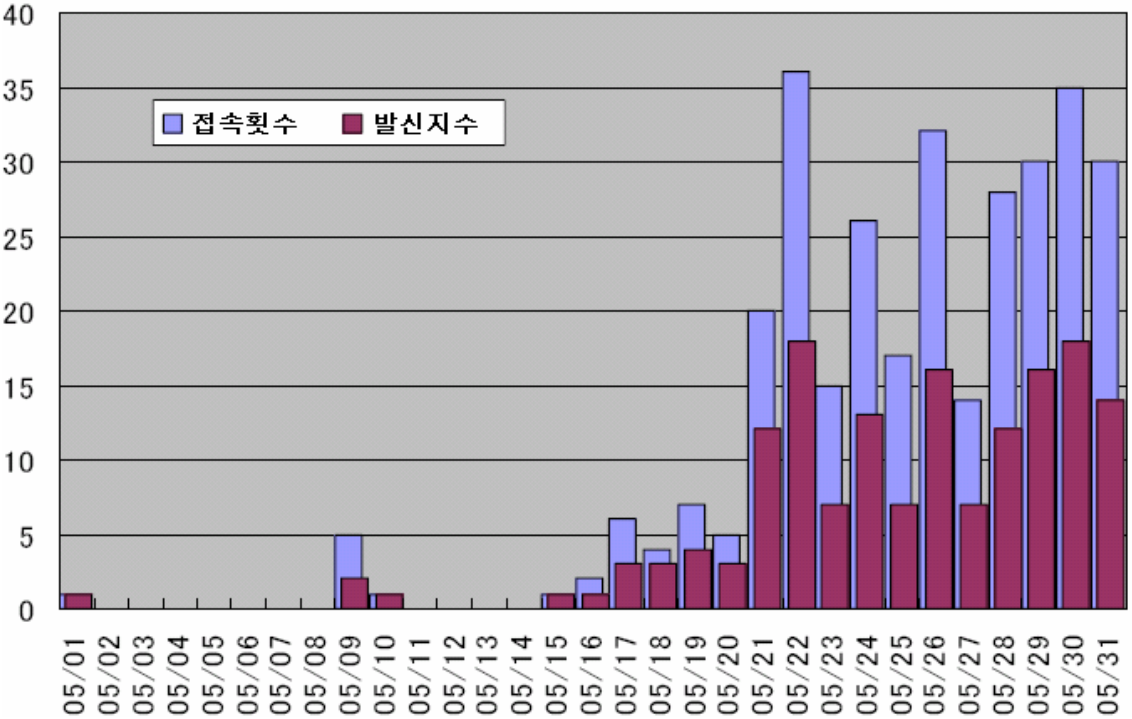
[그림2]는 2006년 5월 한 달 동안 발생한 일본의 네트워크 트래픽 현황에 대한 통계를 그래프로 나타낸 것이다. TCP 135번 포트와 TCP 445번 포트의 트래픽이 매우 많은 것을 볼 수 있는데 이 포트들은 윈도우 운영체제에서 사용되는 포트들로써 아이알씨봇과 같은 웜들이 윈도우 운영체제의 취약점을 감염 경로로 사용하므로 주의가 필요하다.



[그림2] 일본의 네트워크 트래픽 현황(출처: 일본 IPA)

[그림3]은 2006년 5월 일본에서 발생한 TCP 5900 포트의 비정상적인 트래픽 현황이다. 5

월 20일 이후 해당 포트로의 접근 시도가 급격하게 늘어나고 있음을 보여준다.



[그림 3] TCP 5900번 포트의 사용 현황

해당 포트는 원격 관리 툴인 RealVNC에서 사용하는 포트로써, 최근 RealVNC와 관련한 취약점이 발견되어 주의가 필요하다. 만약 악의적인 목적을 가진 공격자가 해당 취약점을 이용한 공격에 성공한 경우 원격에서 권한 획득이 가능하다. 일본 Cert에서는 해당 프로그램으로 인한 피해 예방을 위한 보안 경고문을 발표했다.[1]

[1] http://www.jpcert.or.jp/at/2006/at060005.txt

(2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

5월이 되면 중국인들은 대부분이 일주일간의 긴 휴일을 즐길 수가 있다. 이는 한국에서 근로자의 날이라고 불리는 5월 1일이 중국에서는 노동절이라 하여 긴 휴일을 가진다. 그러나 이러한 중국의 긴 휴일 속에서도 개인 정보를 노리는 트로이목마나 급속한 확산을 시도하는 웜의 피해는 여전히 지속되었다. 중국 로컬 백신 업체들의 동향을 살펴보면 전반적으로는 큰 변화가 없지만 지난 4월에 이어서 애드웨어를 다운로드 하거나 다른 악성코드들을 다운로드 하는 형태의 다운로더 트로이목마의 강세는 여전히 지속되고 있다.

악성코드 TOP 5

순위	순위 변화	Rising
1	-	Trojan.DL.Agent
2	-	Trojan.DL.QQHelper
3	-	Backdoor.Gpigeon
4	-	Trojan.DL.Small
5	-	Dropper.Agent

[표1] 2006년 5월 라이징(Rising) 악성코드 TOP 5

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

중국 로컬 백신 중에서 시장 점유율 1위를 차지하고 있는 라이징의 2006년 5월 악성코드 TOP 5를 살펴보면, 지난 4월과 비교하여 순위상의 변화는 전혀 없었으나 각각의 악성코드가 차지하는 분포적인 면에서 큰 차이는 아니지만 조금씩의 변화가 있었다.

순위	순위 변화	JiangMin
1	-	Adware/Downloader.QQHjit.gen
2	-	Adware/Downloader.QQHelper.gen
3	New	TrojanDownloader.Small.amj
4	New	Adware/Downloader.QQHelper.sa
5	↓1	Adware/Downloader.QQHelper.cb

[표2] 2006년 5월 강민(JiangMin) 악성코드 TOP 5

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

다음으로는 강민의 2006년 5월 악성코드 TOP 5를 보도록 하자. 강민의 악성코드 TOP 5 역

시 1위와 2위는 지난달과 동일하게 애드웨어를 다운로드하는 트로이목마가 차지했다. 그러나 3위와 4위는 다운로더 형태의 트로이목마가 새롭게 순위를 차지했다. 5위에는 지난 3월부터 꾸준히 순위 하락을 보이고 있는 애드웨어 다운로더 형태의 트로이목마인 Adware/Downloader.QQHelper.cb가 지난 4월보다 한 계단 하락한 모습을 보이고 있다.

주간 악성코드 TOP 5

순위	1주	2주	3주	4주
1	Trojan.DL.Agent	Trojan.DL.Agent	Trojan.DL.Agent	Trojan.DL.Agent
2	Trojan.DL.QQHelper	Trojan.DL.QQHelper	Trojan.DL.QQHelper	Trojan.DL.QQHelper
3	Backdoor.Gpigeon	Backdoor.Gpigeon	Backdoor.Gpigeon	Backdoor.Gpigeon
4	Trojan.DL.Small	Trojan.DL.Small	Trojan.DL.Small	Trojan.DL.Small
5	Dropper.Agent	Trojan.PSW.LMir	Trojan.PSW.LMir	Trojan.PSW.LMir

[표3] 2006년 5월 라이징(Rising) 주간 악성코드 순위

라이징의 2006년 5월 주간 악성코드 동향을 보면 1위에서 3위까지는 4주 동안 변화 없이 동일한 악성코드들이 차지하고 있는 것을 알 수 있다. 그러나 2주차에서 Trojan.PSW.LMir (V3 진단명 Win-Trojan/LmirHack) 트로이목마가 주간 순위 5위에 진입하여 5월이 끝나는 4주차까지 이어졌다. Trojan.PSW.LMir 트로이목마는 지난 3월 악성코드 TOP 5에서 4위를 차지하였으며 4월에 이르러서는 확산이 줄어드는 현상을 보여 4월에는 순위에 포함되지 않을 정도였었다. 하지만 이번 5월에는 다시 순위권에 진입 할 정도로 확산을 한 것으로 보여 다음 6월에는 어떠한 동향을 보일지 주의가 필요하리라 보여진다.

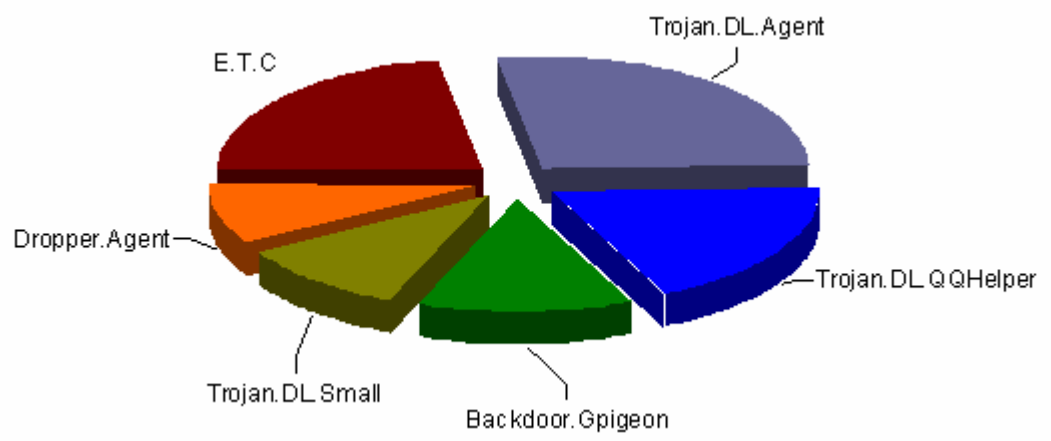
순위	1주	2주	3주	4주
1	Adware/Downloader.QQHjit.gen	Adware/Downloader.QQHjit.gen	Adware/Downloader.QQHelper.sa	Trojan/Klone.u
2	Adware/Downloader.QQHelper.gen	Adware/Downloader.QQHelper.gen	Adware/Downloader.QQHjit.gen	Adware/Downloader.QQHelper.sl
3	Adware/Downloader.QQHelper.cb	Adware/Downloader.QQHelper.cb	Adware/Downloader.QQHelper.ku	Adware/Downloader.QQHjit.gen
4	Adware/Downloader.QQHelper.gb	Adware/Downloader.QQHelper.gb	Adware/Downloader.QQHelper.gen	TrojanDownloader.Slime.f
5	Adware/Downloader.QQHres.gen	Adware/Downloader.QQhelper.gr	Adware/Downloader.QQHelper.sh	Adware/Downloader.QQHelper.to

[표4] 2006년 5월 강민(JiangMin) 주간 악성코드 순위

[표4]는 2006년 5월 강민의 주간 악성코드 순위 변화 표이다. 강민의 주간 악성코드 순위 역시 5월 3주차까지는 큰 순위 변화 없이 유지하고 있었지만 4주차에서 이르러서는

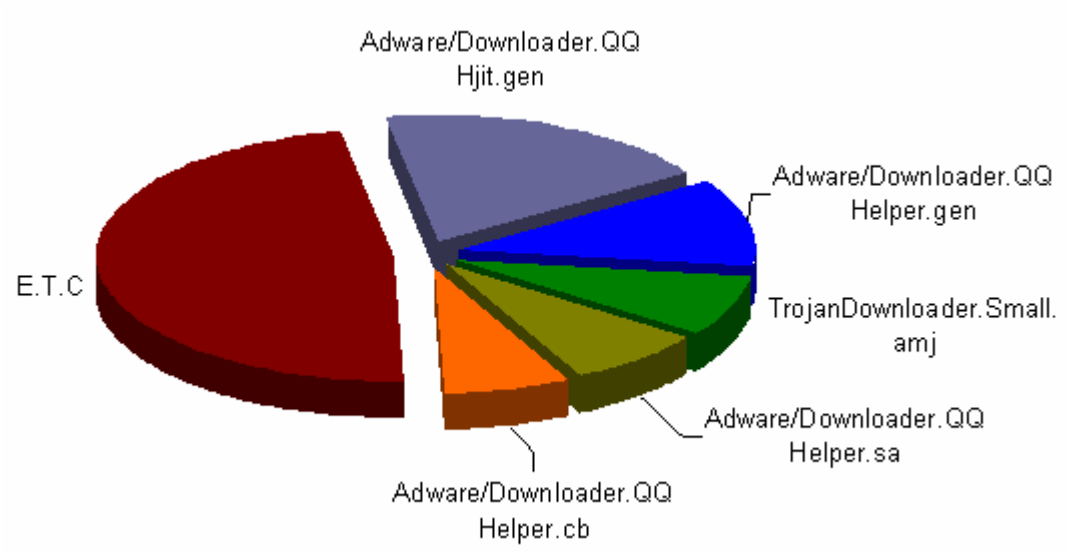
Trojan/Klone.u (V3 진단명 Win-Trojan/Klone)이 급격한 확산을 보이며 1위를 차지하였다. 이러한 현상으로 미루어 당분간은 Trojan/Klone.u 트로이목마의 감염에 주의를 하여야 할 것으로 보여지며 다음 6월에는 어떠한 확산 변화를 할 것인가에 대해서 지켜 봐야 할 것이다.

악성코드 분포



[그림1] 2006년 05월 라이징(Rising)의 악성코드 분포

5월 라이징의 악성코드 분포에서는 대부분의 악성코드가 분포면에서 증가한 것으로 분석되었다. 그러나 지난 4월에 유일하게 증가한 분포를 보였던 Dropper.Agent 만이 지난 4월 9.74%를 차지하였으나 이번 5월에서는 8.64%로 1.1%가 감소하였다. 이와 더불어 악성코드 TOP 5 순위권에 포함되지 못한 기타 악성코드 역시 지난 4월 23.4%에서 21.8% 로 대략 2% 정도가 감소하였다. 이와 같은 악성코드 TOP 5에 포함된 기존 악성코드들의 강세가 6월에도 유지될 것으로 보여지나 Trojan.PSW.LMir 트로이목마의 확산 변화가 어떠한가에 따라 전체적인 악성코드 동향에 변화를 줄 것으로 보여진다.



[그림2] 2006년 05월 강민(JiangMin)의 악성코드 분포

라이징의 악성코드 분포와는 달리 강민의 악성코드 동향에서는 악성코드 TOP 5에 포함된 악성코드의 분포가 급격하게 줄어든 것으로 보여진다. 악성코드 분포에서 가장 큰 변화를 보인 것은 기타에 포함된 악성코드들로, 지난 4월 전체 악성코드 분포에서 23.35%를 차지하였으나 5월에서는 전체 악성코드 분포의 절반에 가까운 47.64%를 차지하며 약 14% 증가한 현상을 보였다. 이와 같이 기타 항목에 포함된 악성코드 분포의 변화는 Adware/Downloader.QQHelper 변형과 Trojan/Klone.u의 변형이 기타 항목에 다수 포함되었기 때문으로 보인다.

(3) 세계의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

2006년 5월 통계 역시 지난 4월에 이어 여전히 매스메일러들이 순위권을 차지하고 있다.

영국 소포스의 2006년 5월 통계에 따르면 넷스카이 웜 변형 (Win32/Netsky.worm)이 1위를 차지하며 25개월 이상 피해 순위권을 차지하고 있으며 그 외 나이젬 웜 변형(Win32/Nyxem.worm)이 3위를 차지하고 있다. 그 외 마이톱 웜 변형(Win32/Mytob.worm) 2종이 새롭게 순위에 포함이 되었으며 기존에 알려진 마이둠 웜 변형(Win32/Mydoom.worm)도 새로 순위에 진입하였다.

.

카스퍼스키 연구소의 2006년 5월 통계 역시 지난 4월과 비교하여 큰 변화 없이 마이톱 웜 변형, 넷스카이 웜 변형, 러브게이트 웜 변형(Win32/LovGate.worm) 등이 순위권을 차지하고 있다. 새롭게 순위에 진입한 웜으로는 스카노(Scano)가 포함이 되어있다.

카스퍼스키 연구소의 온라인 2006년 5월 검사 결과 통계에 따르면 지난 4월 자료와는 달리 1위와 2위 모두 뱅커 (Banker) 변형들이 차지하고 있다. 그리고 10위권 내에 새로 순위에 진입한 악성코드는 모두 4종이며 모두 다운로더(Downloader) 형태가 차지하고 있다.

온라인 검사 결과 순위권에 든 20개의 악성코드 중 9개가 새롭게 등장한 악성코드이고 1개의 악성코드만이 순위권에 재진입하였다. 그리고 1위가 2.12%이며 순위권 외의 악성코드가 지난 달보다 4% 가량 증가한 80.02% 인 것으로 보아, 실제 시스템에 감염되어있는 악성코드는 다양하게 분포되어 있음을 알 수 있다.

V. 이달의 ASEC 컬럼 - 패키지형 스파이웨어 둘러보기

작성자: 장혜윤 연구원(planet@ahnlab.com)

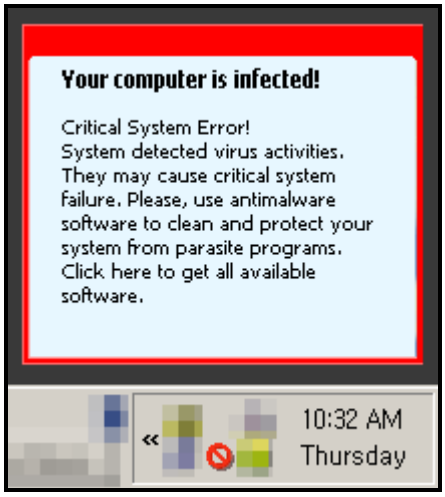
작년 후반부터 지속적으로 배포된 즈롭(Win-Downloader/Zlob)은 여러가지 증상을 맛 볼 수 있는 스파이웨어 패키지라고 할 수 있다. 자체 전파기능 없이 사용자가 메일 혹은 웹에서 실행 파일을 다운로드 해 실행하거나 다른 악성코드(웜, 바이러스, 트로이목마)를 통해 설치되는 것으로 보인다.

설치된 즈롭은 크게 아래와 같이 5가지 증상을 나타낸다.

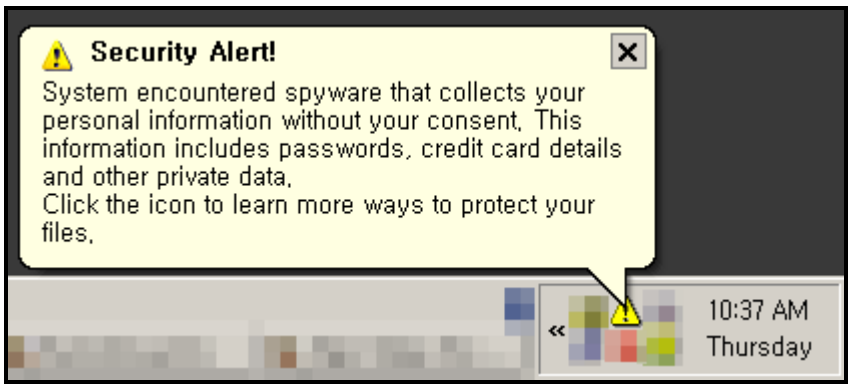
- 알림창으로 사용자의 클릭 유도
- 'Critical System Error!' 경고 다이얼로그 메시지 발생
- 트레이 아이콘 클릭시 허위 안티스파이웨어 설치/실행
- 트레이 아이콘 클릭시 허위 안티스파이웨어 사이트로 접속
- 광고 창 팝업
- 시작페이지 변경

사용자의 불안감을 조성하여 허위 안티스파이웨어 설치 유도

[그림1], [그림2]처럼 트레이 아이콘으로 등록되어 주기적으로 사용자의 PC에 스파이웨어가 감염되었다는 메시지를 발생시킨다. 이는 사용자를 불안하게 만들어 알림창을 클릭하게 하여, 허위 안티 스파이웨어 제품을 설치 및 설치할 수 있는 웹사이트로 이동하도록 한다.



[그림1] 트레이 아이콘의 알림메시지

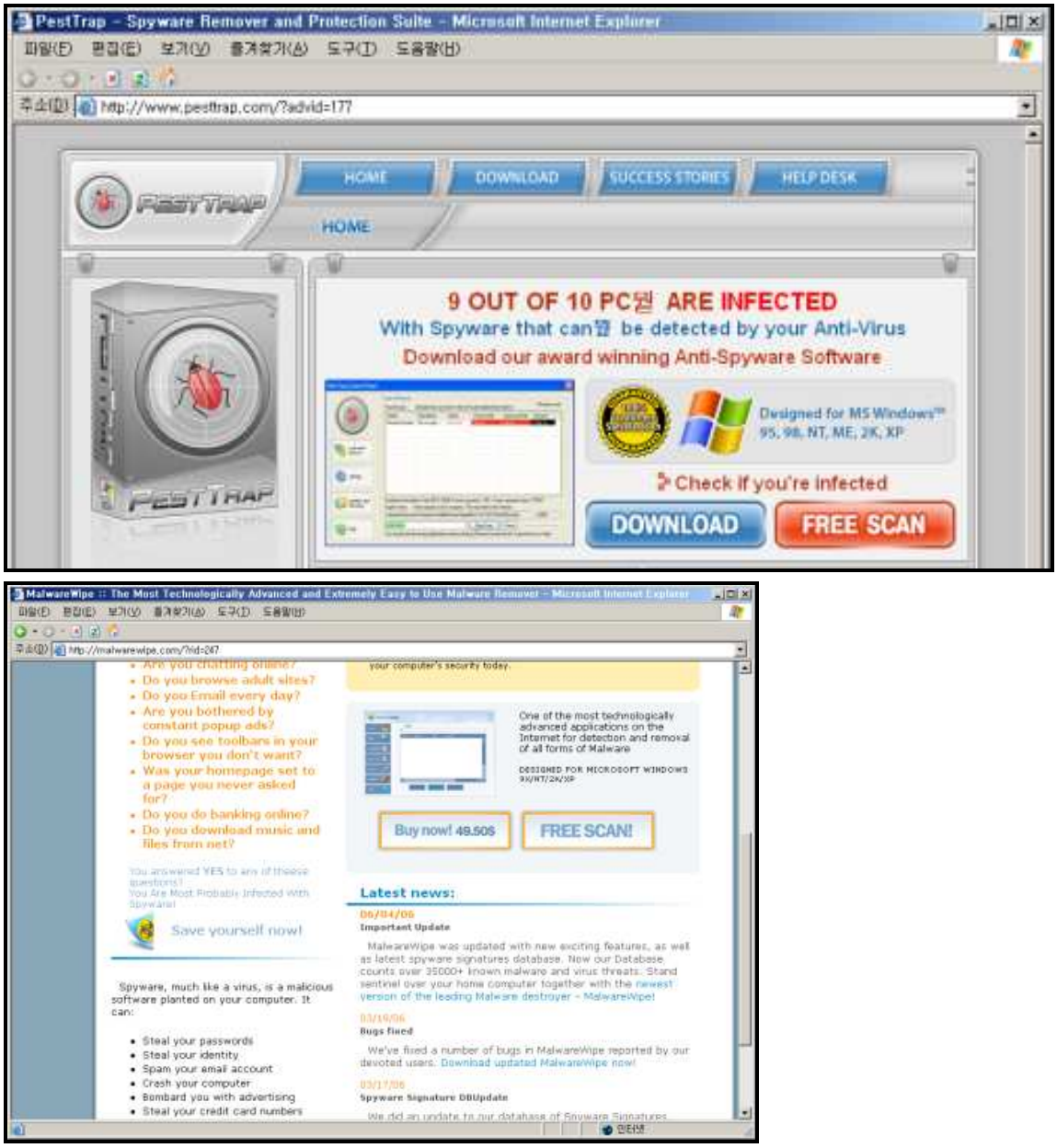


[그림2] 트레이 아이콘의 알림메시지

최초 트레이 아이콘 클릭 시에는 특정 사이트로부터 허위 안티 스파이웨어 제품을 설치하며, 다음부터는 설치된 허위 안티스파이웨어 제품을 실행한다.

사용자의 불안감을 조성하기 위한 또 다른 방법으로 사용자에게 시스템 에러 경고창[그림3]을 발생시켜, 클릭을 유도한다. 이때 '확인'을 클릭하면 [그림4]와 같이 허위 안티 스파이웨어 사이트로 접속하게 되는데, 이때 접속하게 되는 사이트는 매번 바뀐다.

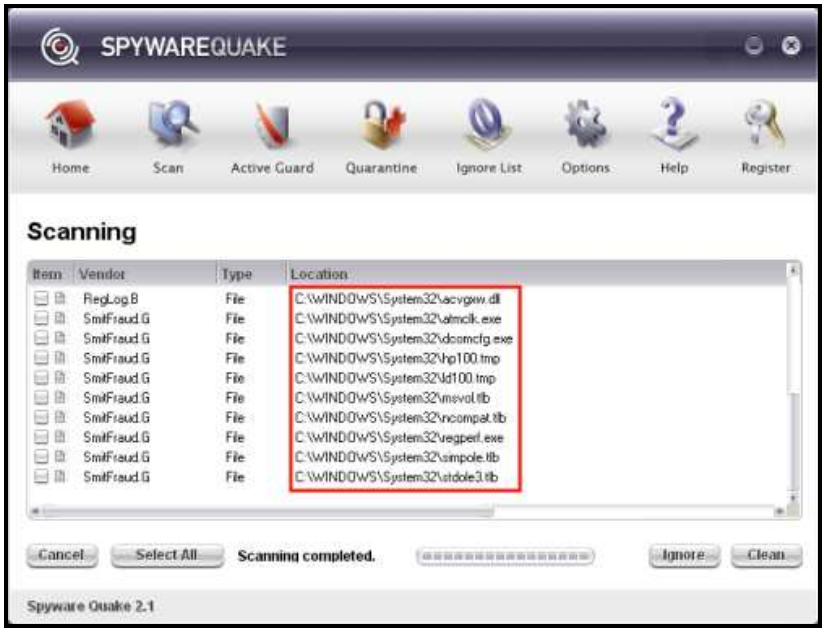
[그림3] 'Critical System Error!' 경고



[그림4] 알림창 클릭시 이동한 웹사이트 화면

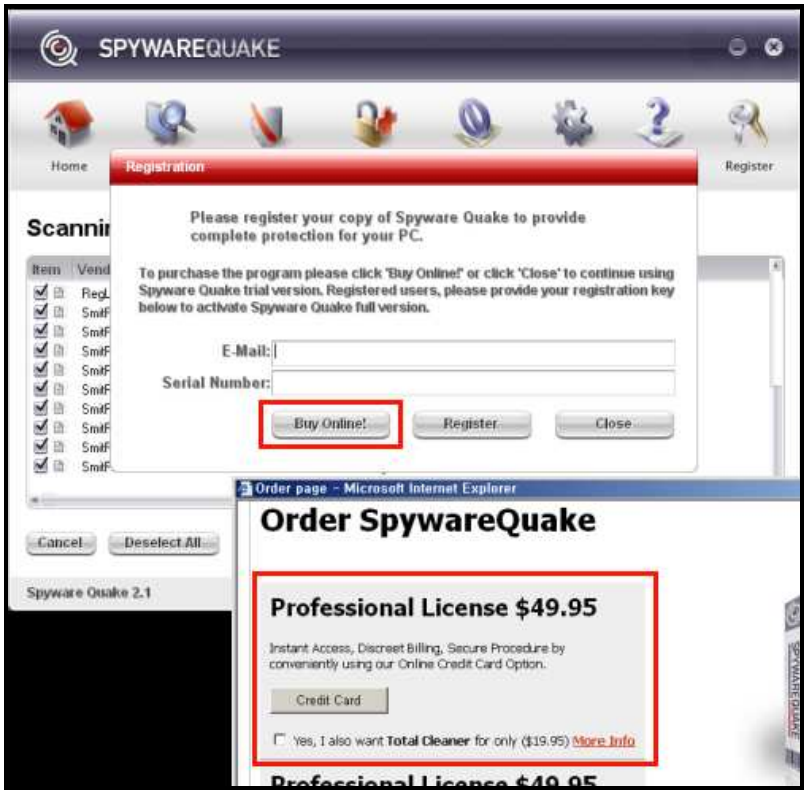
설치된 허위 안티 스파이웨어가 허위로 진단하여 결재를 유도

이동한 웹사이트에서 허위 안티 스파이웨어를 설치하면 스파이웨어케이크(SPYWAREQUAKE)가 설치되며, 이를 이용하여 시스템을 검사하면 [그림5]와 같이 즈롭으로 부터 설치된 구성요소 파일들을 진단하게 된다.



[그림5] 허위 안티 스파이웨어에서 즈롭 구성파일들을 진단한 화면

사용자는 진단된 스파이웨어를 치료를 하기 위해서 [SelectAll -> Clean]을 선택하지만, 허위 안티 스파이웨어인 스파이웨어퀘이크(SPYWAREQUAKE)는 치료를 위해 사용자에게 결제를 요구한다.



[그림6] 치료 시 결제를 요구하는 화면

감염된 PC에서 사용자를 귀찮게 하는 행동들

설치된 즈롭은 주기적으로 [그림7]와 같이 광고 창을 팝업 시키는데, 이때 매번 광고 주제가 바뀌며, 가끔 성인물 광고 창을 팝업하여 자녀를 둔 가정에서는 아이들에게 좋지 않는 정서적 영향을 끼칠 위험이 있다.

[그림7] 광고 팝업

맺으며

외국뿐 아니라 국내에서도 허위 안티 스파이웨어 제품들이 지속적으로 늘어나고 있다. 뿐만 아니라 이런 제품들은 제품 홍보 및 판매를 위해서 스파이웨어들이 사용하는 기법을 사용하여 광고 창 팝업 및 시작페이지 변경, 클릭 유도 등의 사용자 불편함까지 초래하고 있어 더 문제가 된다.

또한 예전에는 단순히 광고 창 팝업 등 한가지 증상을 가지는 스파이웨어가 많았지만, 근래에는 여러 가지 증상을 함께 가지고 있는 '패키지' 형식의 배포가 많이 이루어지고 있다. 이런 패키지 형식의 스파이웨어 설치 피해는 앞으로 더욱 증가할 것으로 예상되며, 여러 가지 불편한 증상이 함께 나타나기 때문에 심할 경우 사용자의 시스템을 무력화시키는 경우도 발생할 수 있어 주의가 필요하다.