ASEC Report 2월

® ASEC Report

2008. 3

안철수연구소의 시큐리티대응센터(AhnLab Security Emergency response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스 분석 및 보안 전문가들로 구성되어 있는 조직이다.

이 리포트는 ㈜안철수연구소의 ASEC에서 국내 인터넷 보안과 관련하여 보다 다양한 정보를 고객에게 제공하기 위하여 바이러스와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

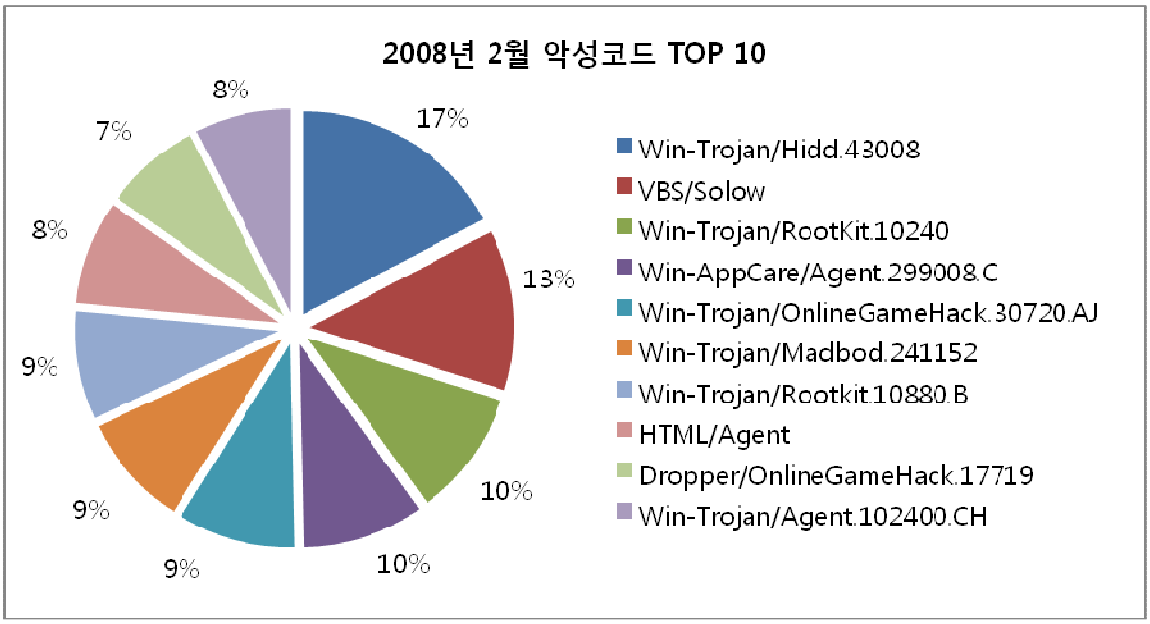
I. ASEC 월간 통계

(1) 2월 악성코드 통계

순위		악성코드명	건수	%
1	new	Win-Trojan/Hidd.43008	50	17.2%
2	new	VBS/Solow	37	12.8%
3	new	Win-Trojan/RootKit.10240	29	10.0%
4	new	Win-AppCare/Agent.299008.C	28	9.7%
5	new	Win-Trojan/OnlineGameHack.30720.AJ	27	9.3%
6	new	Win-Trojan/Madbod.241152	26	9.0%
7	new	Win-Trojan/Rootkit.10880.B	25	8.6%
8	new	HTML/Agent	24	8.3%
9	new	Dropper/OnlineGameHack.17719	22	7.6%
10	new	Win-Trojan/Agent.102400.CH	22	7.6%
합계			290	100.0%

[표 1-1] 2008년 2월 악성코드 피해 Top 10

2008년 2월 악성코드 피해 Top 10에 랭크 된 피해 건수는 290건으로 2월 한달 총 피해건수(3,254건)의 약 11%에 해당한다. 온라인 게임관련 정보취득용으로 제작된 악성코드가 주류를 이루던 지난 1월과는 사뭇 대조적인 모습이다. 온라인 게임 정보취득을 목적으로 하는 공격의 시발점이 되는 중국과 상대적으로 공격대상이 되었던 한국이 최대 명절인 설을 맞이하는 기간이며, 한국 교육 문화에서도 개학과 졸업 등의 변화의 시기이기도 한, 2월은 수치상으로는 상당히 안정적인 인터넷 환경이 유지된 시기였다고 볼 수 있다.



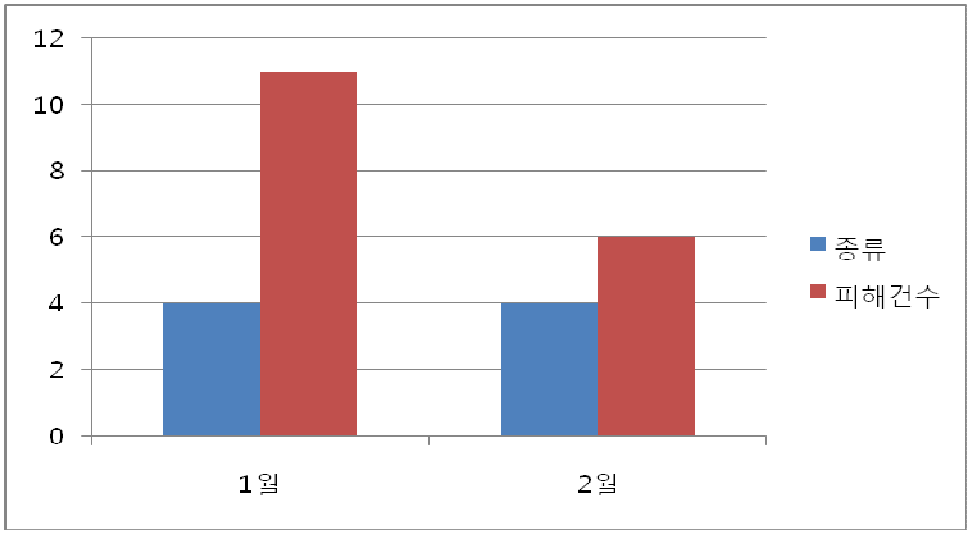
[그림 1-1] 2008년 2월 악성코드 피해 Top 10

눈여겨 볼 만한 것은 1위의 Win-Trojan/Hidd.43008과 2위의 VBS/Solow이다. Win-Trojan/Hidd.43008은 그 자체만으로는 악성코드라고 보기 어려울 수 있는 평범한 프로그램이지만, 이를 악용하는 악성코드들이 다양하게 등장하고 있다. 자신을 숨겨서 사용자 몰래 동작해야하는 스파이웨어들이 주로 이것을 악용하는 것이 추세이므로 Win-Trojan/Hidd.43008이 발견된 PC에서는 추가적으로 존재하는 애드웨어는 없는지 검사하는 습관이 필요하다.

최초 발견 당시 보다 진화된 모습을 취하고 있는 VBS/Solow를 V3에서는 발견되는 시점에 분석하여 진단값을 추가하던 방식에서 다양한 분석을 통해 악성코드로 판단할만한 형태를 지닌 파일을 사전에 진단하는 형태로 변화하여 사용자들의 피해를 최소화 하는데 초점을 맞추고 있다

이상 2개의 악성코드에 대해 사용자들의 각별한 주의가 필요하며, V3IS2007을 통한 진단/치료 후에도 이상증상이 발견될 경우에는 즉각 안철수연구소에 신고하여 조치 받을 것을 권한다.

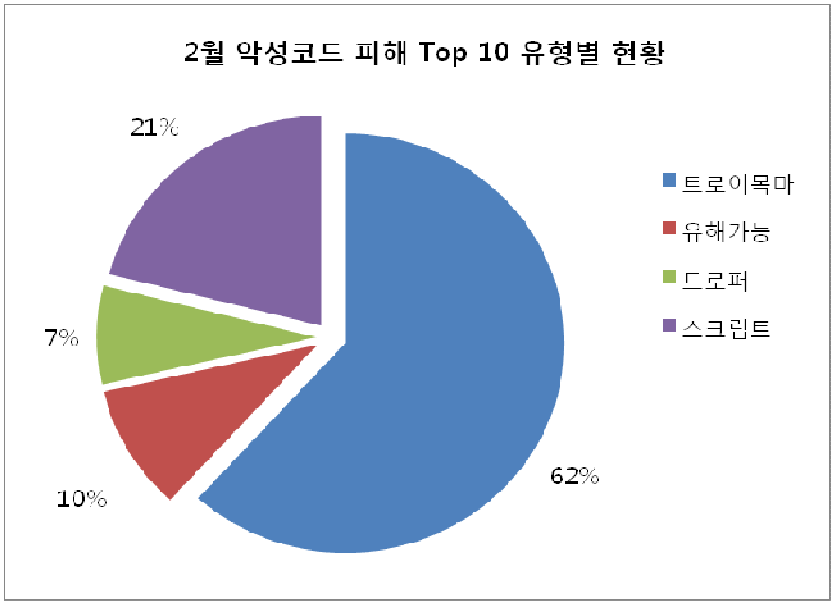
순위에는 포함되어 있지 않으나 최근 MSN을 통해 전파되는 MSNBot이 잠재적으로 동작하고 있는 것으로 보인다. 사용자들의 보안의식이 높아져 많은 피해가 없을 것으로 기대하고 있으나, 아직도 검증되지 않은 파일을 다운로드 받아 실행하는 사용자들이 많은 것 같다.



[그림 1-2] MSNBot 발견건 수 및 피해신고 건 수

MSNBot은 주로 압축된 이미지파일의 형태로 전파되며, 압축해제 후 이미지파일을 클릭하게 되면 실행된다. 이것이 피해를 크게 하는 원인은 자신이 잘 알고 있는 MSN 내의 친구가 파일이 보내기 때문이다. 일단 확인되지 않은 파일은 실행하기 전 백신을 통해 진단/치료 해 볼 것을 권한다. 진단되지 않더라도 의심스러울 경우에는 반드시 안철수연구소에 의뢰하여 확인 받을 것을 권하는 바이다. 이런 과정이 복잡하다면 해당 메시지를 보낸 친구가 영문메시지로 말을 하고 압축된 이미지 파일을 보내올 경우, 보낸 파일이 무엇인지를 되물어보는 정도의 습관을 가지는 것이 좋겠다.

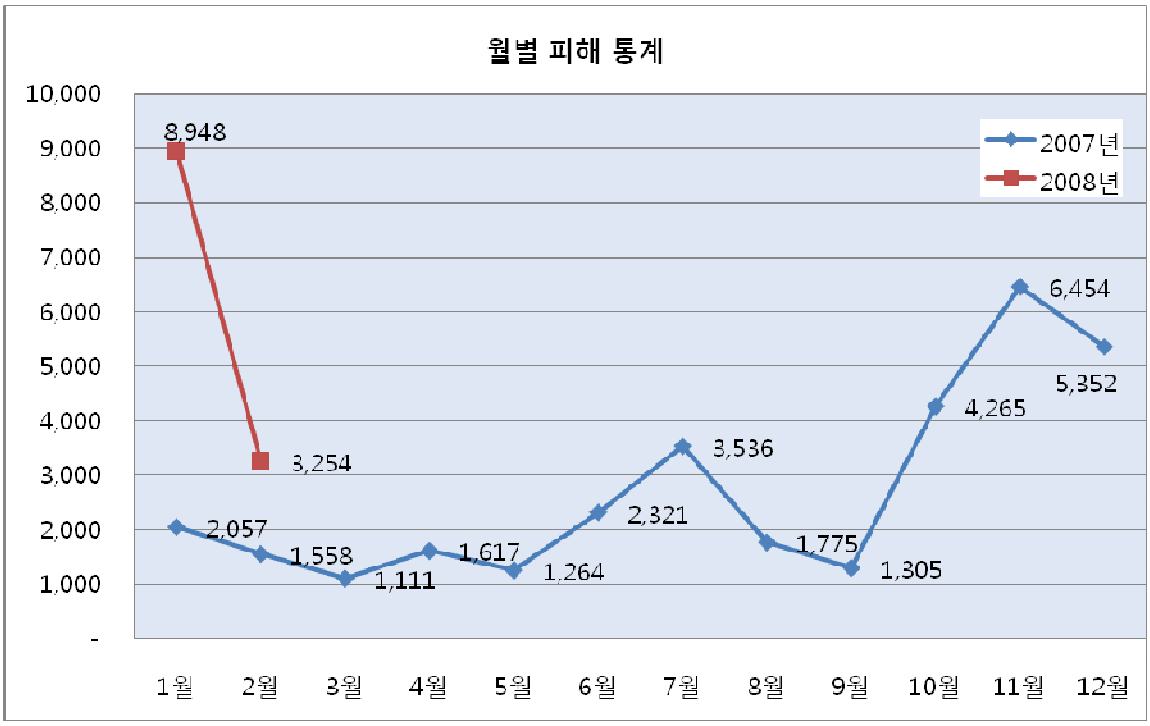
악성코드 피해 Top 10의 유형별 현황



[그림 1-3] 악성코드 피해 Top 10의 유형별 현황

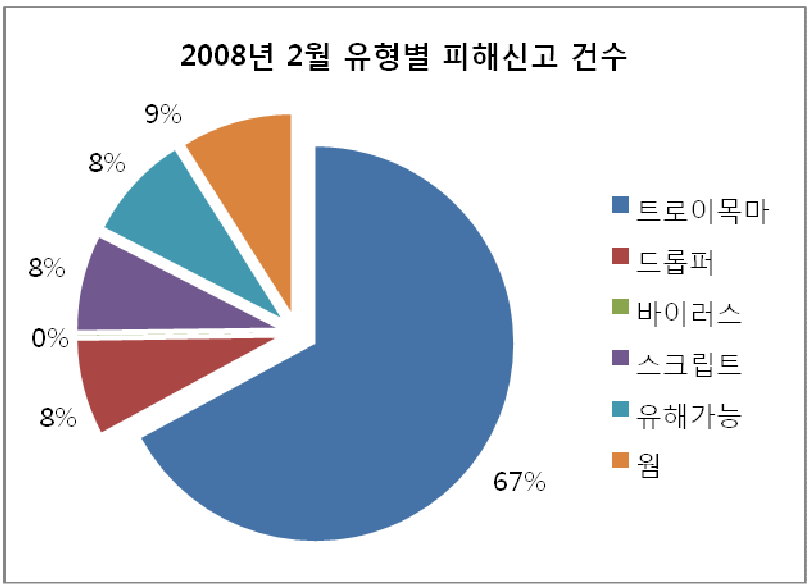
여전히 트로이목마로 인한 피해가 다수를 차지하고 있다. 트로이목마는 특성상 스스로 전파되는 기능이 없고, 그 스스로가 악의적인 목적으로 제작된 것이므로 삭제하면 대부분 문제가 해결된다. 주로 공개된 게시판을 통해 설치되거나 검증되지 않은 파일을 이용할 때 설치되므로, MS 보안패치를 통해 OS의 취약점을 보완하고, PC방화벽을 통해 파일의 실행을 방어하는 것이 필요하다. 안철수연구소의 그레이제로 서비스를 통해 네티즌들을 통해 작성된 파일 정보를 확인해 보는 것도 좋은 방법이 될 수 있다.

월별 피해신고 건수

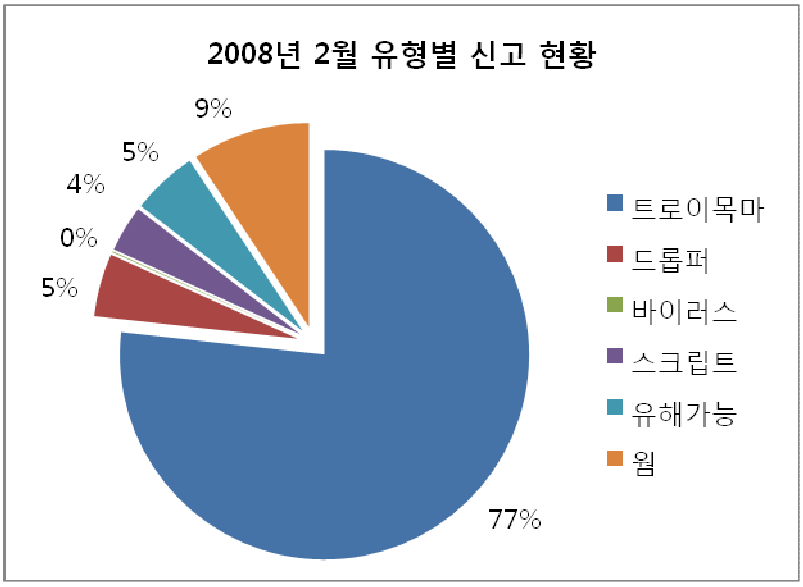


[그림 1-4] 2007,2008년 월별 피해신고 건수

수치상으로는 지난해 7월의 피해통계와 비슷하나, 같은 해 10월부터 12월까지의 증가한 피해수치를 기초로 볼 경우 평균을 밑도는 수치임을 알 수 있다. 급격히 증가한 2008년 1월과 급격히 감소한 2월의 수치만으로 2008년을 예상하는 데 무리가 있을 것이다.



[그림 1-5] 2008년 2월 악성코드 유형별 피해신고 건 수



[그림 1-6] 2008년 2월 피해 신고된 악성코드의 유형별 현황

지난 3개월간의 유형들을 비교해 보면 2월 한달 간 접수된 악성코드 피해와 그 유형은 줄어들었으나 유해가능 프로그램과 스크립트는 오히려 증가한 것을 볼 수 있다. 이것이 2월에 국한된 것일지, 향후 동향변화의 지표가 될 지 아직은 확인할 수 없다

다만, 스크립트 형태를 취하고 있는 악성코드가 새로운 악성코드의 대안처럼 제시되고 있고, 이것을 악용하는 다양한 시도가 시도되고 있다는 점에 주목할 필요가 있다. 또한 현재는 유해가능 프로그램으로 분류되어 사용자의 선택에 의해 사용/제거 되는 프로그램이 나도 모르는 어느 한 순간에 트로이목마로 변신하여 PC사용에 불편을 초래할 수도 있다.

다양한 정보와 편리함을 제공하는 프로그램들이 홍수처럼 쏟아져 나오고, 국경을 초월한 정보의 이동은 사용자들의 호기심을 자극하기에 충분하다. 내가 원하는 정보를 얻기 위하여 일반적인 PC사용자들이 원할만한 정보를 거짓으로 흘리는 것은 그리 어려운 일이 아닐 것이다. 앞서 잠시 언급했던 절친한 친구의 메신저를 통해 들어오는 압축된 그림파일은 가장 좋은 예가 될 수 있다. 친구가 보낸 압축된 그림파일을 열어보는 것은 위험한 행위가 아니라고 판단되겠지만 이젠 이것마저도 위협받는 시대이다. 파일 전송전/후에 백신을 통한 파일검사는 반드시 수행할 것을 권하며, 가급적 이런 것은 PC 사용의 습관처럼 여기는 것도 필요하다.

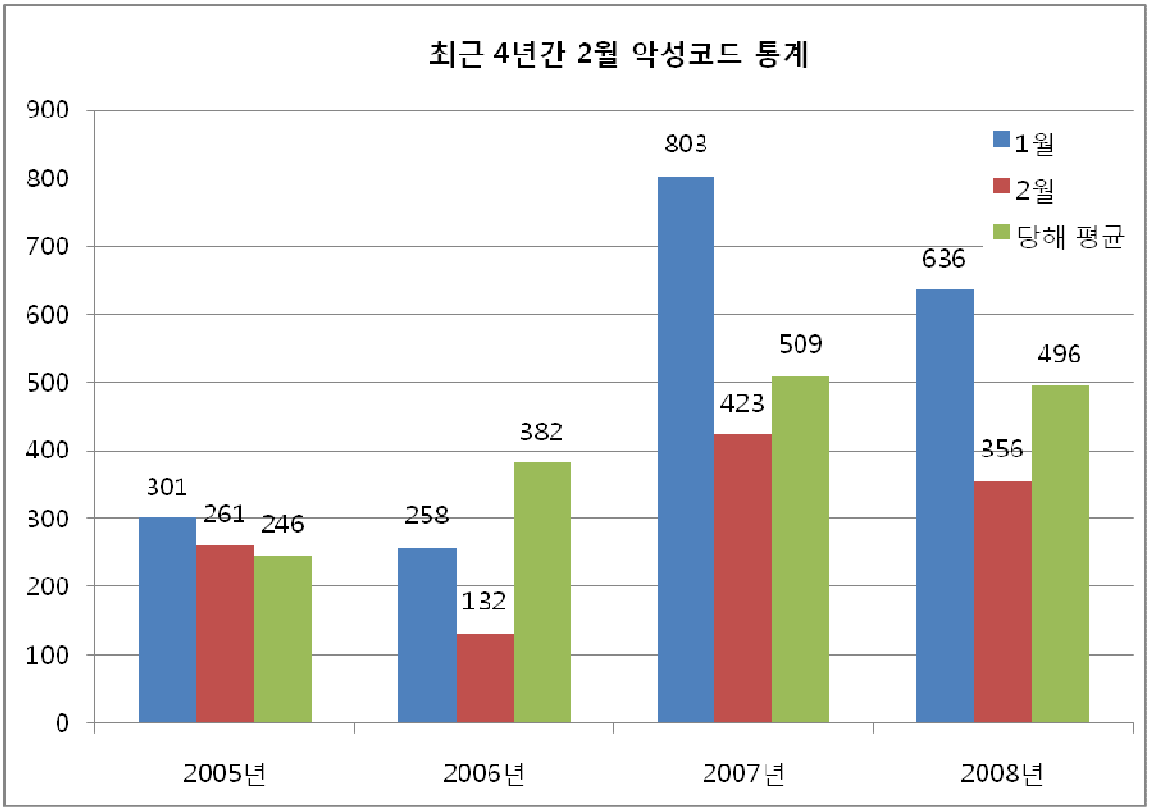
국내 신종(변형) 악성코드 발견 피해 통계

2월 한달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 1-2], [그림 1-7]와 같다.

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
12 월	26	387	80	1	5	0	0	0	9	0	508
01 월	47	471	107	2	1	0	0	0	8	0	636
02 월	43	281	21	3	3	0	0	0	5	0	356

[표 1-2] 2007년 ~ 2008년 최근 3개월간 유형별 신종 (변형) 악성코드 발견 현황

이번 달은 전월과 비교하여 발견된 악성코드의 수가 큰 폭으로 줄어들었다.(-44%) 이는 어느 정도 예상된 것으로 우리나라가 중국 발 악성코드에 큰 영향을 받고 있다는 사실이 다시 증명되었다고 하여도 과언이 아닐 것 이다. 다음은 중국 발 해킹 그리고 악성코드의 영향이 가시적으로 느껴졌던 2005년부터 올해까지의 1,2월 악성코드와 당해 년도의 평균수를 비교한 것이다.

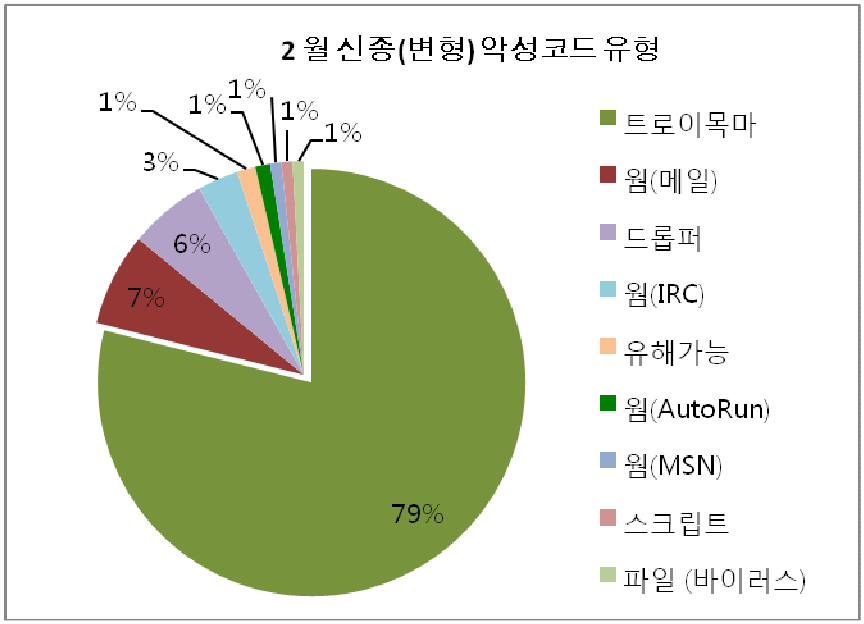


[그림1-7] 최근 4년간 1,2월 악성코드 통계

2월에 보통 음력설이 있고 이는 우리나라에서 최대 명절일 뿐만 아니라 중국에서는 '중국의

새해'로 표현 될 정도로 최대 명절이다. 따라서 이 기간 동안 소위 중국 지역의 '작업장' 이라고 불리는 곳에서 악성코드 제작/유포 또는 이를 이용한 데이터 갈취 등이 현저히 줄어 든다고 판단 된다. 따라서 중국, 대만 또는 국내에 거점을 둔 중계서버에 올려진 악성코드에 대한 업데이트 또는 사용자들의 감염 횟수도 줄어 들기 때문에 2월은 다른 어느 달 보다 그 수가 적다고 추정 할 수가 있다.

다음은 이번 달 악성코드 유형을 상세히 분류한 것이다..



[그림 1-8] 2008년 02월 신종 및 변형 악성코드 유형

이번 달에는 메일로 전파 되는 Win32/Zhelatin.worm 변형이 많았다. 특히 발렌타인 데이 관련 내용을 위장하여 수 많은 변형이 유포 된 것으로 보인다. 역시 변형인 자신을 진단 하지 못하도록 기존 진단 방법을 우회하는 모습이 역력 했다.

드롭퍼 역시 중국쪽의 영향으로 전월 대비 -80% 가까운 감소를 보였다. 따라서 제일 많은 비중을 차지는 하는 트로이목마와 드롭퍼의 비율이 가장 큰 하락폭을 보였다.

이번 달은 3종의 바이러스가 발견, 보고 되었는데 다음과 같다.

- Win32/Diskgen.L
- Win32/DunDun
- Win32/Sality.L

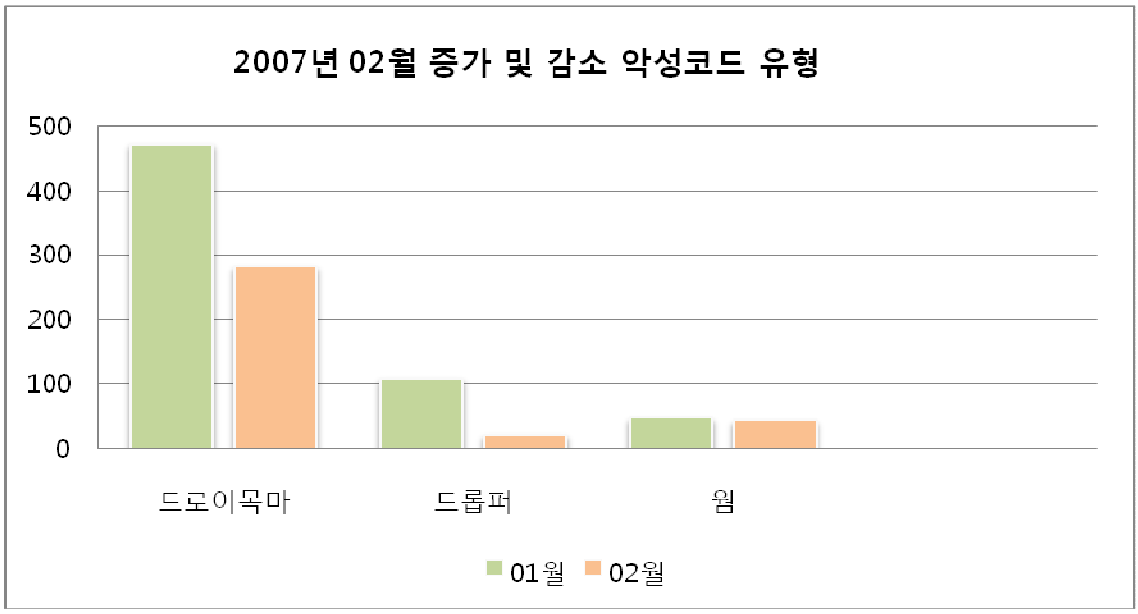
Win32/Diskgen 바이러스는 많은 변형을 가지고 있다. 이 글을 작성하는 현재 15개의 변형

이 나왔다. 이 바이러스는 중국산으로 추정 되며 2006년과 2007년 초 많은 피해를 입혔던 Win32/Viking, Win32/Dellby 바이러스의 연상하게 한다. 이 바이러스에 대한 내용은 Trend & Issue 에 다루기로 하겠다.

Win32/DunDun 바이러스는 중국에서 보고 되었다. 그리복잡하지 않은 다형성 바이러스며 후위형이다. Explorer.exe 의 특정 메모리 영역에 자신의 코드를 Inject 하고 CreateFileA 함수가 호출 될 때 자신의 코드로 CALL 하도록 되어 있다.

Win32/Sality.L 은 기존에 알려진 Win32/Sality 바이러스의 변형중 하나이다.

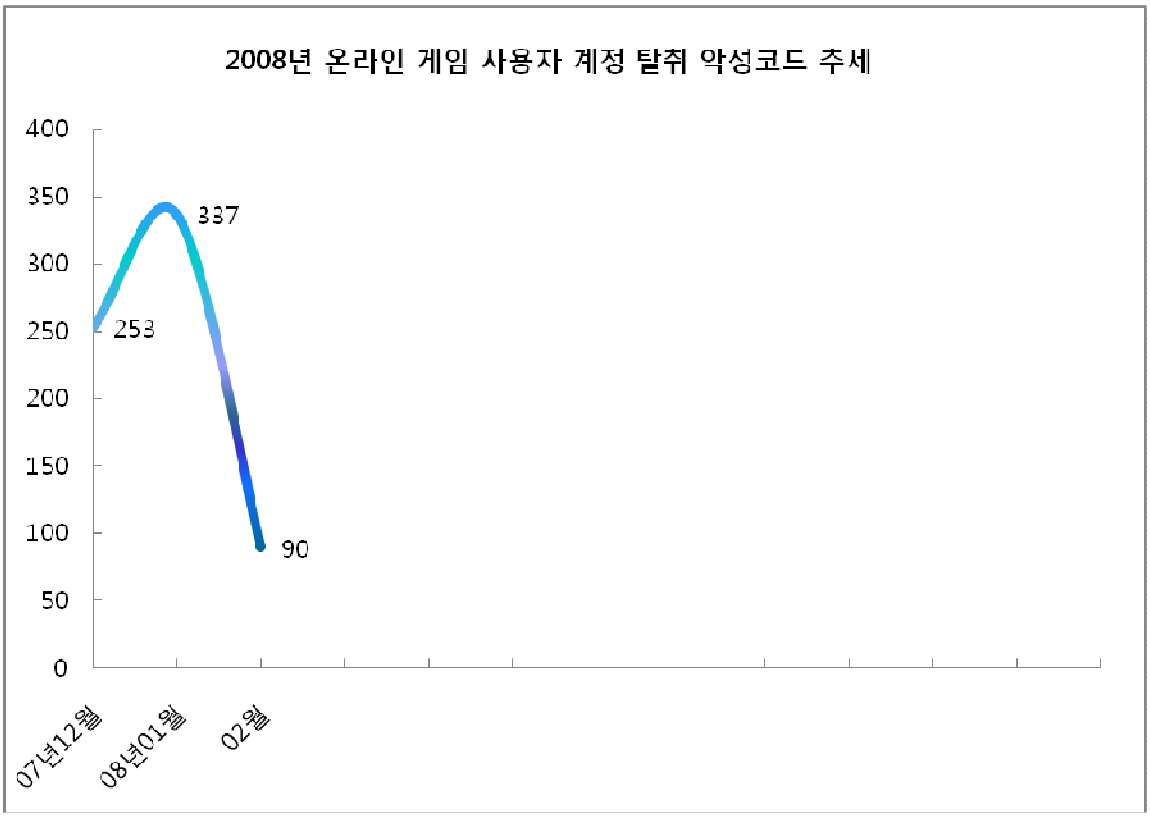
다음은 2 월에 증가 및 감소한 주요 악성코드 유형에 대한 현황이다.



[그림 1-9] 2008년 02월 감소 및 증가 악성코드 유형

이번 달 악성코드 감소의 원인 이외에도 특이할 만 한 점이 몇 가지 있다. 먼저 Win-Trojan/Hupigon (이하 휘피곤 트로이목마) 이라고 불리어지는 중국산 악성코드가 다시 모습을 보이고 있다. 일전에 본 지면을 통해서 소개한 Win-Trojan/PolyCrypt 악성코드는 휘피곤 트로이목마에 각종 실행 압축 프로그램으로 진단을 피하도록 한 것을 대표적으로 일컫는다. 또한 2월에 있었던 발렌타인데이와 미국 대통령선거 후보자 관련 투표에 관한 내용을 위장하고 스팸 메일 형태로 유포된 Dropper/Srizbi 관련 스팸 메일러 트로이목마의 재등장도 관심 있게 지켜보아야 할 것이다.

다음은 트로이목마 및 드롭퍼의 전체 비중에서 상당한 비율을 차지 하는 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 추세를 살펴보았다.



[그림 1-10] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

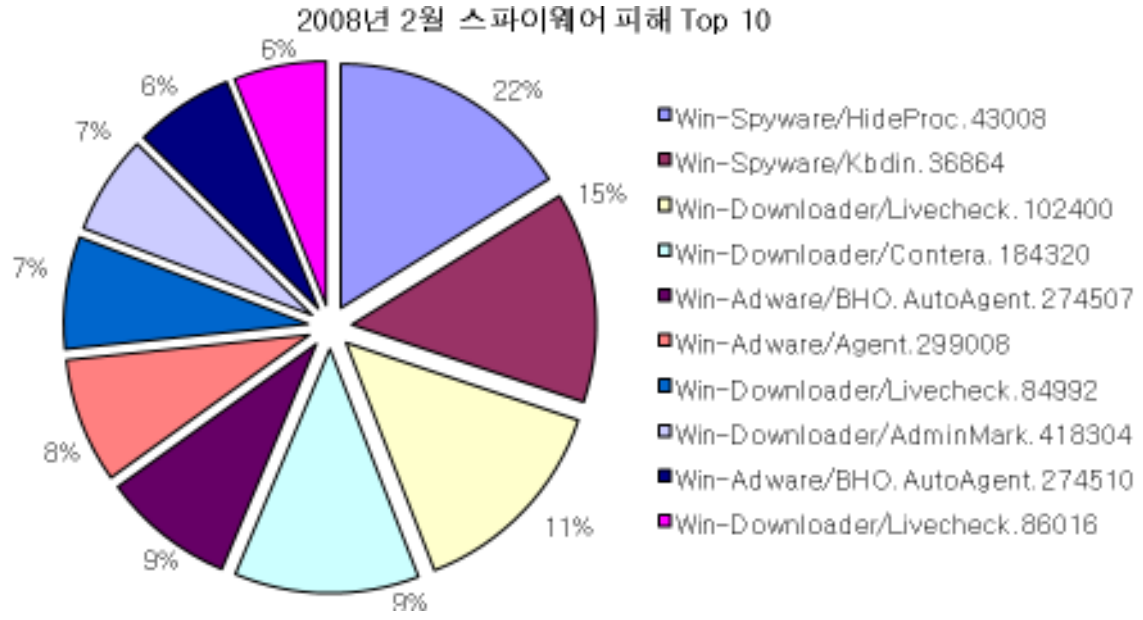
온라인 게임의 사용자 계정 정보 등을 탈취 하는 트로이목마는 지난 1월 까지는 분명히 상승추세에 있었으나, 2월을 기점으로 대폭 하락 하였다. 그러나 3월에는 중국쪽 영향을 받아 다시 증가추세로 돌아 갈 것이다.(작년 동월의 경우 3월에는 2월 대비 11% 증가 하였다) 이런 류의 트로이목마나 드롭퍼와 관련하여 최근에는 다시 국내 온라인 게임을 노리는 형태가 종종 발견되고 있다. 다시 국산 온라인 게임으로 악성코드의 타겟이 변경된 것인지는 좀 더 추이를 지켜봐야 할 것으로 보인다.

그 외에는 기존에 알려진 유형과 크게 다르게 않다.

(2) 2월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	↑6	Win-Spyware/HideProc.43008	37	22%
2	New	Win-Spyware/Kbdin.36864	32	15%
3	New	Win-Downloader/Livecheck.102400	32	11%
4	↓3	Win-Downloader/Contera.184320	28	9%
5	New	Win-Adware/BHO.AutoAgent.274507	20	9%
6	-	Win-Adware/Agent.299008	19	8%
7	↓4	Win-Downloader/Livecheck.84992	17	7%
8	↑1	Win-Downloader/AdminMark.418304	15	7%
9	New	Win-Adware/BHO.AutoAgent.274510	15	6%
10	New	Win-Downloader/Livecheck.86016	14	6%
합계			229	100%

[표 1-3] 2008년 2월 스파이웨어 피해 Top 10



[그림 1-11] 2008년 2월 스파이웨어 피해 Top 10

2008년 2월 스파이웨어 피해신고 건수는 총 1061건으로 지난 달에 비하여 약 1000건 가량 큰 폭으로 감소하였다. 전년도와 비교하여 보면, 매년 2월은 설 명절의 영향을 받아 피해 신고가 감소하는 경향을 보이고 있다. 이 시기에는 국내뿐만 아니라 중국 악성코드에 의한 피해도 크게 감소하는데, 이런 시기적인 특징은 올해에도 스파이웨어 피해 통계에 잘 반영되어 있다.

전체 피해 건수는 감소한 가운데 스파이웨어 피해 상위 Top10의 스파이웨어 중 상당 수가 지난 1월에 이어 많은 피해를 입혔다. 2월에 가장 많은 피해를 입힌 스파이웨어 하이드프록(Win-Spyware/HideProc.43008)은 델파이로 제작된 프로세스 숨김 기능의 DLL 파일이다. 이 스파이웨어가 많은 피해를 입힌 원인은 국내에서 제작된 여러 스파이웨어가 실행중인 프로세스 목록에서 자신의 프로세스를 은폐하기 위한 목적으로 하이드프록을 사용했기 때문인 것으로 추정된다. 이 외에도 다운로더 라이브체크(Win-Downloader/LiveCheck), 다운로더 어드민마크(Win-Downloader/AdminMark) 등의 국내에서 제작된 스파이웨어가 지난 1월에 이어 많은 피해를 입혔다.

2008년 2월 유형별 스파이웨어 피해 현황은 [표 1-4]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
12월	325	446	164	461	4	8	4	0	1	1413
08'1월	268	556	117	1134	4	4	0	0	0	2083
08'2월	264	281	139	358	3	12	2	1	1	1061

[표 1-4] 2008년 2월 유형별 스파이웨어 피해 건수

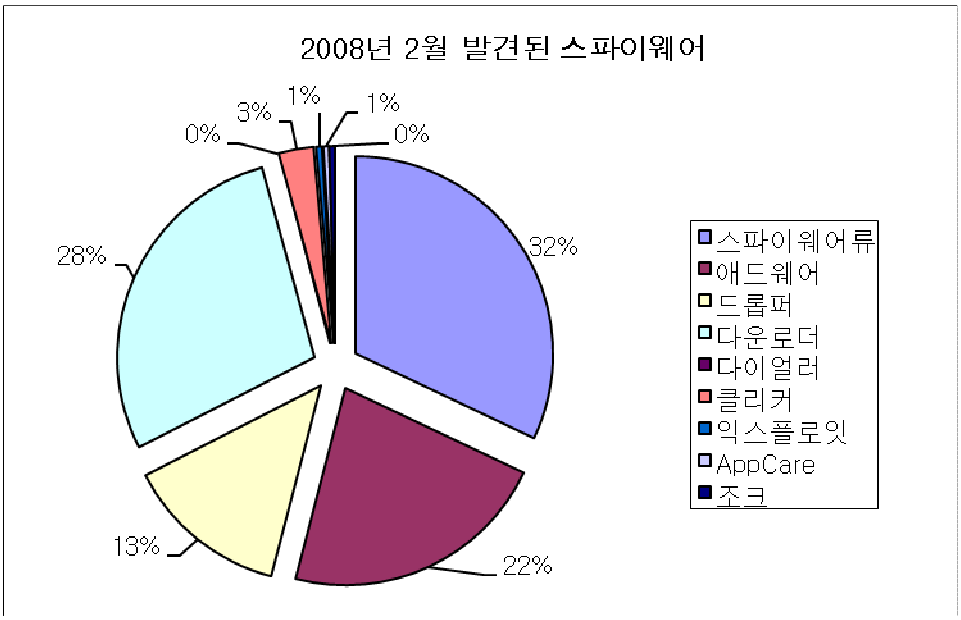
2008년 2월 유형별 스파이웨어 피해 통계를 살펴보면 다운로더와 애드웨어 피해 신고 감소가 두드러진다. 1월 리포트에도 언급한 바와 같이 다운로더는 애드웨어, 스파이웨어 피해의 직접적인 원인이 될 수 있는데, 다운로더 피해의 감소가 애드웨어 피해 감소의 원인이 된 것으로 생각된다.

2월 스파이웨어 발견 현황

2월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-5], [그림 1-12]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
12월	86	32	22	48	1	3	1	0	1	194
08'1월	20	50	24	80	0	1	0	0	0	175
08'1월	67	46	28	59	0	6	1	1	1	209

[표 1-5] 2008년 2월 유형별 신종(변형) 스파이웨어 발견 현황



[그림 1-12] 2008년 2월 발견된 스파이웨어 프로그램 비율

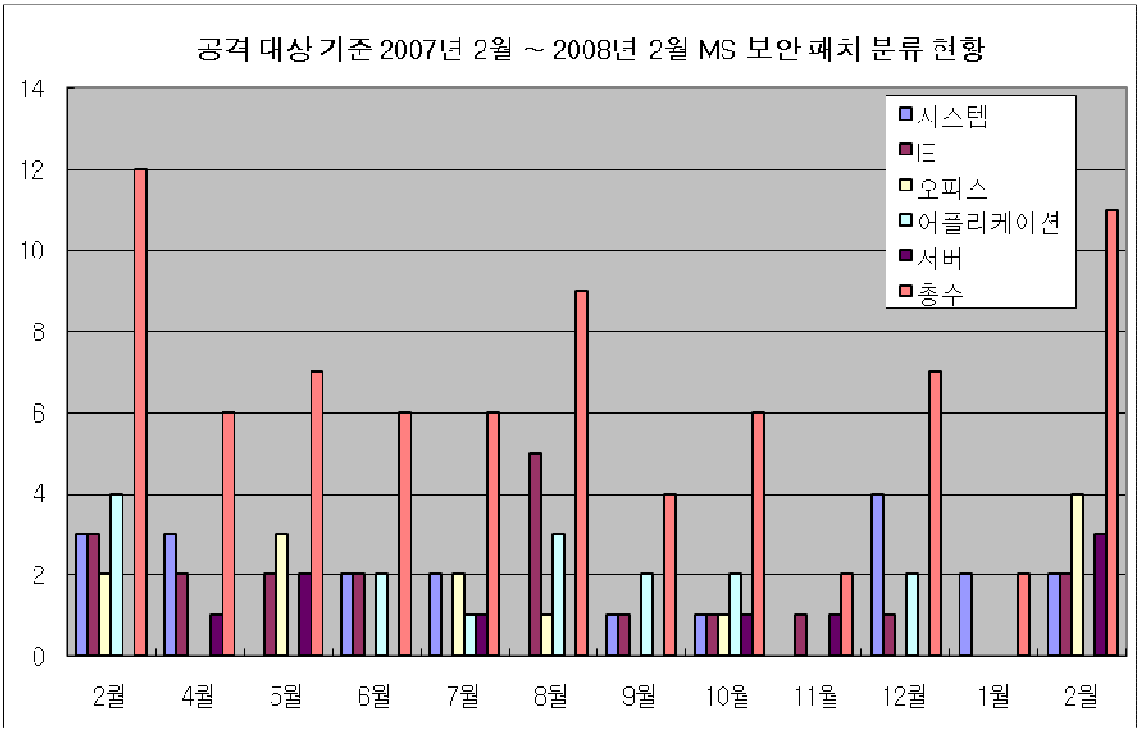
스파이웨어 신종 발견 건수가 지난 1월에 비해 다소 증가하였는데, 이는 가짜 코덱프로그램에 의해 설치되는 스파이웨어 Zlob(Win-Spyware/Zlob) 변형이 다수 발견되었기 때문이다. 스파이웨어 Zlob은 동영상을 보기 위한 코덱프로그램으로 위장하고 있으나, 이 프로그램을 설치하면 코덱 대신 클리커, 툴바 등 다수의 스파이웨어가 설치된다.

스파이웨어의 증가를 제외하면 신종 및 변형 발견 건수는 지난 달과 비슷한 수치를 보이고 있다.

(3) 2월 시큐리티 통계

2008년 2월에 마이크로소프트사에서는 11개의 보안 업데이트를 발표하였다. 발표된 업데이트는 긴급(Critical) 6개, 중요 5개로, 1월의 총 2건에 비해서, 대폭 늘어났다.

이 중에서 특히 웹 서버로 많이 사용하고 있는 IIS(Internet Information Server)에 대한 공격에 이용될 수 있는 MS08-005, MS08-006이 포함된 것이 특징이라 할 수 있다. 또한 지난 1월과 유사한 윈도우 커널의 TCP/IP Stack을 원격에서 공격할 수 있는 MS08-004가 포함되어 있다. 커널 내부 드라이버에 관련된 취약점인 경우에 일반적으로 로컬 권한 상승으로 이어지나, TCP/IP 처럼 네트워크 스택 관련 드라이버들은 원격 공격에 이용이 될 수 있기 때문에 주의가 필요하다.



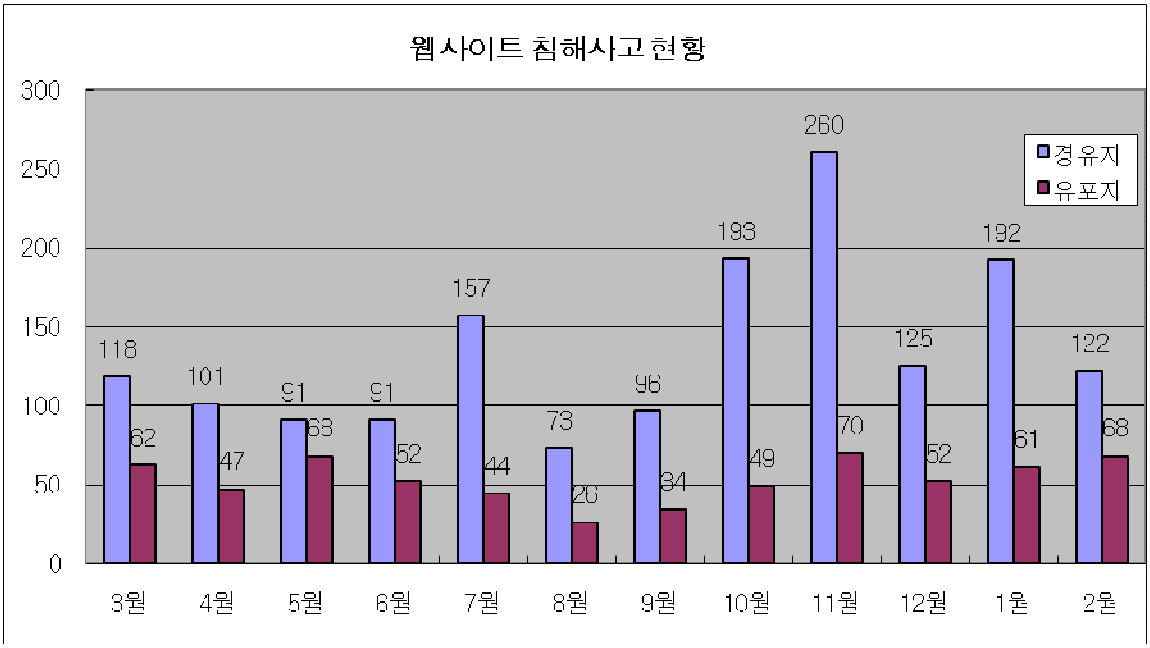
[그림 1-13] 지난 1년간 공격대상 기준 MS 보안 패치 현황

[그림 1-13]을 보면, 2008년 1월에 발표된 MS 보안패치는 모두 시스템 관련 취약점이었으나, 2월에 들어와서, 서버 및 오피스 관련 취약점이 증가한 것을 파악할 수가 있다.

2월달에도 역시 오피스 취약점 공격에 관련된 패치가 4건 포함되어 있는데, 오피스 취약점은 악성코드가 포함되어 메일이나 웹을 통해 공격하기 때문에, 신뢰하지 않는 사용자에게서 오피스 파일이 메일로 오는 경우에는 특히 주의가 필요하다. 오피스 사용자들은 오피스 2003 서비스팩3 또는 오피스 2007의 사용하는 것이 좋으며, 오피스에 대한 보안패치는 반드시 오피스 홈페이지에서 보안 업데이트를 적용해야만, 클라이언트 시스템의 보안성을 강화

할 수 있다.

2008년 2월 웹 침해사고 현황



[그림 1-14] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2월의 웹 사이트 경유지/유포지 수는 122/63으로 2007년 12월의 192/63과 비교하여 경유지 수가 감소하였다 비록 침해지수는 감소하였지만 유포지 수는 오히려 증가하였다. 경유지 수는 줄었지만 실제 공격 위험은 예전과 같거나 조금 증가하였다고 볼 수 있다.

2월 결과 역시 1월과 마찬가지로 악성 코드 배포를 위해 중국 벤더에서 배포하는 ActiveX 콘트롤의 취약점 공격 코드가 삽입된 페이지가 발견되었다. 일반적으로 중국 벤더에서 배포하는 ActiveX를 국내 사용자들이 사용하지 않는 것을 감안하면 그 효과는 아직 작지만 공격 대상이 전통적인 마이크로소프트사의 제품에서 ActiveX등 서드파티 제품으로 옮겨가고 있다는 것을 의미한다고 할 수 있다. 취약점 개수가 한정적인 마이크로소프트 제품과는 달리 서드파티 제품의 수는 무수히 많고 이에 대한 취약점 역시 엄청나게 많기 때문에 서드파티 제품의 취약점을 공격하는 경향은 지속될 것이다.

이와 같은 방식의 악성 코드 배포는 운영체제나 서드파티 제품의 취약점을 이용하여 배포되기 때문에 일반 PC 사용자들은 운영체제뿐 아니라 서드파티 제품의 보안 상태를 항상 확인하고 제품 상태를 항상 최신으로 유지하여야 한다. 또한 AV 제품을 설치하여 자신의 PC를 보호하여야 한다. 그리고 침해사고를 확인한 웹 사이트의 관리자들은 사이트의 사후 관리에 신경을 써 그 영향을 최소화 해야 한다.

II. ASEC Monthly Trend & Issue

(1) 악성코드 – Win32/Diskgen 바이러스와 유명인 사칭 메일

지속적으로 이슈가 되고 있는 Win32/Zhelatin.worm(이하 젤라틴 웜)의 활동은 2월달에도 핫이슈였다. 그리고 이와 유사한 커널 기반의 스팸 메일인 Srizbi의 활동도 발견되었다. 무엇보다도 국내에서는 Win32/Diskgen 이라고 알려진 바이러스의 활동이 여러 차례 보고 되었는데, 재작년 피해가 극심했던 Win32/Viking 바이러스와 같은 형태로 폭발적 증가를 하지 않을까 우려 되고 있다.

► 디지털 액자에서 발견된 악성코드

미국에서 판매된 디지털 액자에서 악성코드가 검출 되었다는 보도가 있었다. 해당 디지털 액자는 PC와 USB를 이용하여 데이터를 주고 받는다. 지금까지 이동형 저장 장치에 악성코드가 발견된 사례는 처음이 아니다. MP3 플레이어, 네비게이션, 이동식 하드 드라이브, USB 메모리 스틱 등에 이어 디지털 액자에서도 악성코드가 발견되었다. 이러한 이동형 저장 장치에서 악성코드가 발견되는 것은 충분히 예상 가능하였던 것이다.

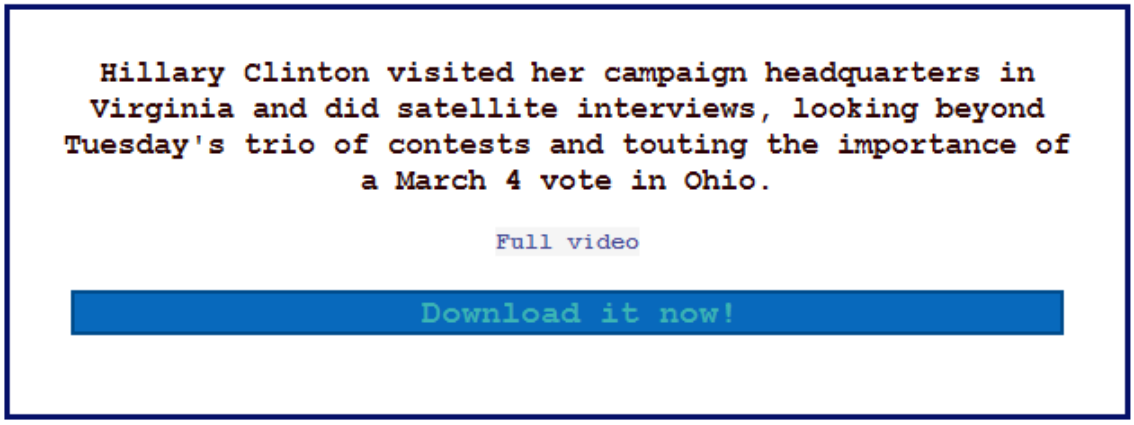
[그림 2-1] Bestbuy 에서 판매된 insignia 사 제품 추정 이미지 (출처 - http://www.techgadgets.in)

이와 같은 제품에는 내부에 그림 파일을 저장하기 위한 스토리지 공간이 있을 것이고 테스트 등을 위해서 PC와 연결 되어야만 했을 것으로 보인다. 따라서 보통 이러한 장치에서 악성코드가 발견되는 것은 보통 테스트 단계 또는 기 구성된 폴더구조와 데이터 등을 PC 에서 그대로 가져와 복사하는 과정 중에 PC가 악성코드에 감염되어 있을 경우 악성코드가 함께 복사된 것으로 보인다. 일각에서는 이동식 저장장치를 노리는 악성코드가 많아지면서 이러한

장치에서 품질 테스트 중 악성코드에 감염된 제품을 걸러 낼 수 있도록 안티 바이러스 검사 기준을 마련 해야 한다는 이야기도 나오고 있다.

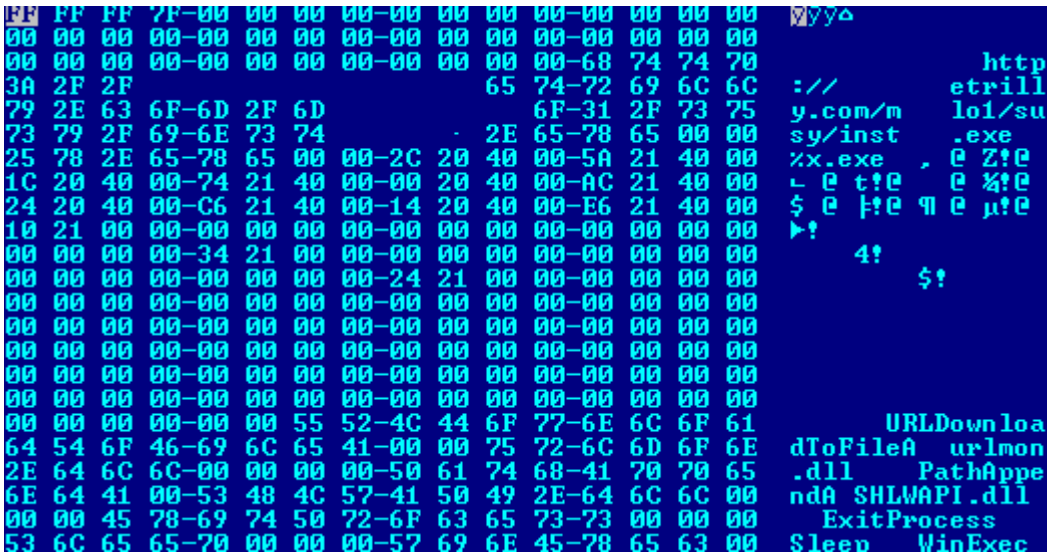
► 유명인 사칭 메일과 Dropper/Srizbi 의 관계

유명인을 사칭 하는 형태의 메일로 악성코드를 전파 하는 것은 매우 고전적인 방법 중에 하나이다. 이번 달에는 페리스 힐튼, 힐러리 클린턴의 동영상을 다운 받을 수 있다는 스팸 메일에 대해서 약간의 분석을 하였다. 악성코드는 아래의 스팸 메일에 링크를 걸어 작은 크기의 다운로더를 다운로드 하도록 유도 한다.



[그림 2-2] Dropper/Srizbi 관련 메일 내용

이것은 2K 가 넘지 않은 매우 작은 파일로 FSG 로 실행압축 되어 있다. 내부에는 특정 호스트로부터 파일을 다운로드 받아 실행 하도록 되어 있다.

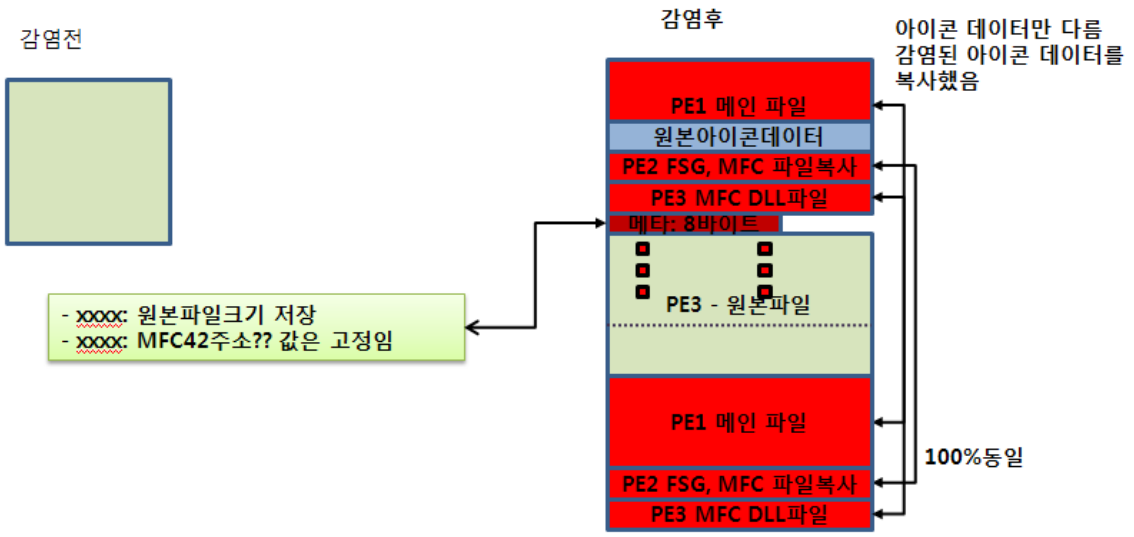


[그림 2-3] Dropper/Srizbi 관련 다운로더 트로이목마

해당 다운로드는 Srizbi 라고 알려진 은폐형 스팸 메일러를 다운로드 하여 실행 한다. Srizbi 는 작년초에도 '풀 커널 스팸메일러'라고 일부 언론에도 알려진바 있으며 이번에 발견된 형태는 그 변형이라고 할 수 있다.

► 피해가 증가하고 있는 Win32/Diskgen 바이러스 변형

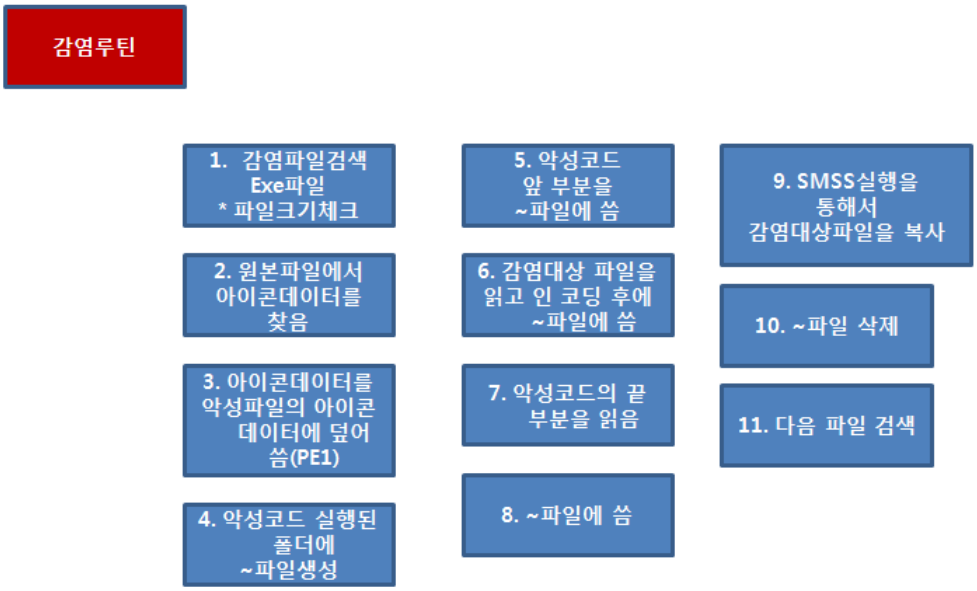
Win32/Diskgen 바이러스의 이력은 1년 전으로 거슬러 올라간다. 이 악성코드는 Diskgen 이라는 웜으로 먼저 알려지기 시작하였으며, 당시에 일부 외산 안티 바이러스 업체는 이를 웜으로 진단하여 감염된 파일을 삭제하기도 하였다. 그러나, 작년 11월에 두번째 변형이 발견된 이후 지금까지 15종의 변형이 보고되었다. 이 바이러스는 다음 그림과 같이 원본 실행 파일을 바이러스 내부에 감싼 형태를 보이고 있다.



[그림 2-4] Win32/Diskgen 감염 전, 후 모습

변형마다 조금씩 다른데 초기에는 VB 로 작성 되었고 최근 발견되는 변형은 MFC로 제작되어 있다. 또한 악성코드 자체도 각기 다르게 실행압축된 형태로 보고되고 있다.

감염특징으로는 자신의 악성코드 보다 큰 PE 파일만 감염 되고 원본이 악성코드 안에 끼어들기 형태로 감염 된다. 원본 파일은 특정 크기단위로 한 바이트 암호화 해두었다. 변형에 따라 감염조건이 다르나 보통 윈도우 폴더와 프로그램 파일 폴더 내 실행 파일을 감염 시킨다. 전체적인 감염 루틴은 다음과 같다.



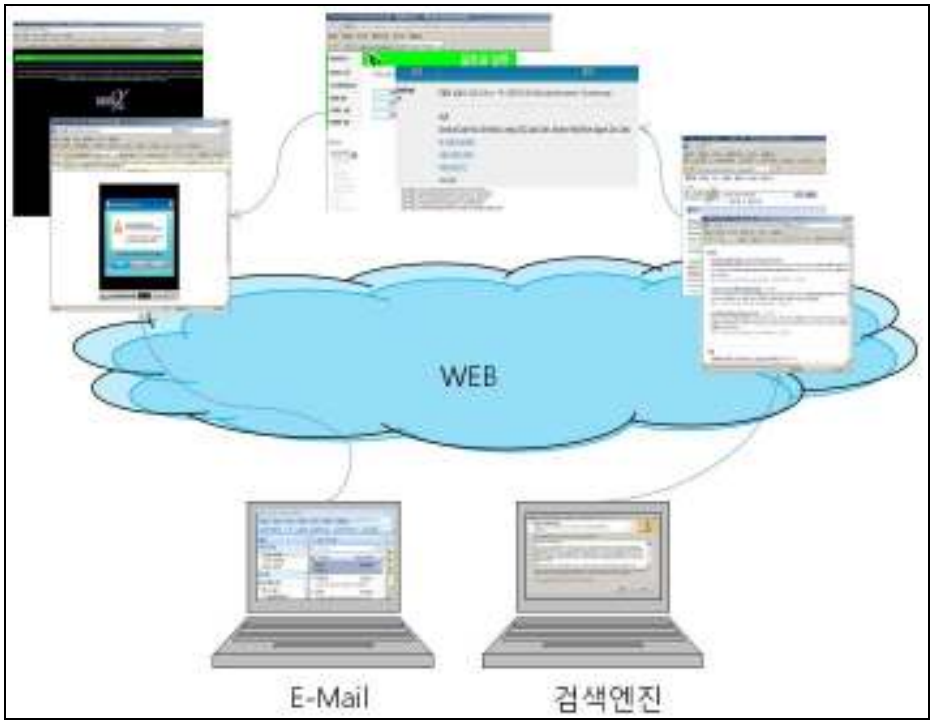
[그림 2-5] Win32/Diskgen 감염루틴

감염 후 증상으로는 특정 안티 바이러스 프로그램을 종료하는 증상, 특정 폴더에 대한 권한 변경, IE를 백그라운드로 실행하여 특정 호스트 접속, pagefile.pif 과 Autorun.inf를 각 드라이브마다 생성하여 악성코드 원본을 자동실행 하도록 유도한다. 또한 htm, html, asp, spx, php, jsp 파일을 발견할 경우 랜덤으로 수를 생성해서 조건에 맞으면 특정 호스트가 명시된 URL을 삽입한다. 또한 안전모드 관련 레지스트리 키 값을 삭제하여 안전모드로 부팅을 방해하며 숨김 속성 변경 등 실행 후 다양한 악의적인 증상을 가지고 있다

특히 악성코드에서 드랍되는 DLL 파일은 (가장 마지막으로 보고된 변형에서 생성되는 파일 (dnsq.dll)) 실행중인 프로세스와 실행하려고 하는 프로세스에 모두 인젝션 된다. 그런데 후킹 방식이 메시지 훅 방법을 사용하여 메시지 처리 과정을 증가하게 되어 훅 된 타켓 프로세스 가 비정상적으로 종료 되는 등 시스템이 매우 불안정하게 되는 현상을 발생시킨다.

(2) 스파이웨어 - 코덱을 가장한 스파이웨어 즐롭(Win-Spyware/Zlob)

2006년 6월 국내에서 처음 신고된 스파이웨어 즐롭(Win-Spyware/Zlob)은 1년 6개월이 지난 지금도 계속해서 국내 감염이 신고되고 있다. 즐롭은 정상적인 코덱[1]을 가장해서 사용자의 PC에 설치되어 사용자의 데이터를 외부로 유출시키거나 허위백신을 설치하고 광고를 노출시키는 스파이웨어이다.



[그림 2-6] 즐롭의 감염경로

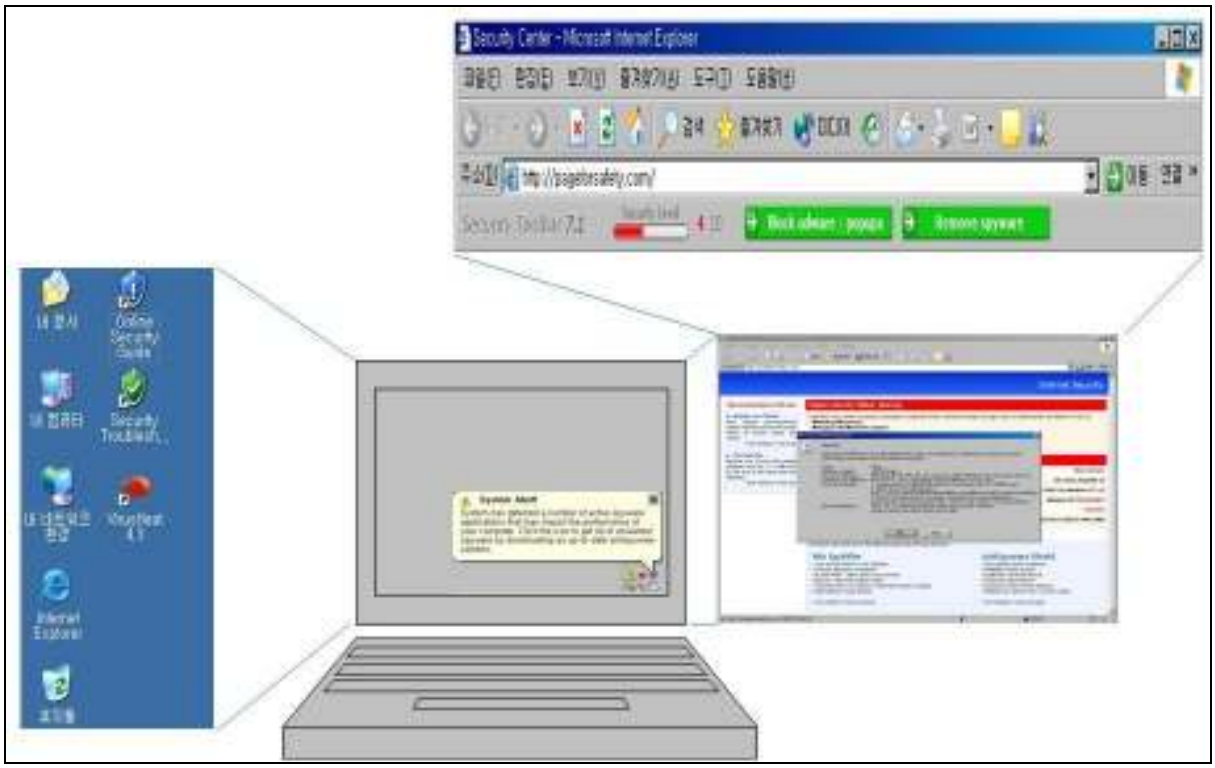
배포자는 먼저 정상적으로 보이는 몇 개의 배포사이트를 준비한 후 무작위로 메일을 발송하거나, 로봇[2]을 이용해 여러 게시판에 배포사이트로 유인하는 내용의 글을 등록한다. [그림 2-6]의 우측경로에서는 검색엔진을 통해 배포 사이트로 접근하는 경우로 코덱이 필요한 PC 사용자가 웹에서 관련 검색을 하는 경우 로봇에 의해 많은 웹사이트에 등록된 허위 배포사이트로 유인하는 배포물이 손쉽게 검색된다. 검색된 국내외의 사이트를 통해 코덱 배포 사이트로 유인된 사용자는 동영상 재생에 필요한 프로그램을 설치하기 위해 해당 사이트에서 배포하는 프로그램을 설치하면 감염이 이루어진다.

[그림 2-6]의 좌측경로는 E-mail을 통해서 배포가 되는 과정으로 PC사용자를 유행하는 동

[1] 코덱은 코더(coder)와 디코더(decoder)의 합성어로, 음성이나 비디오 데이터를 컴퓨터가 처리할 수 있게 디지털로 바꿔 주고, 그 데이터를 컴퓨터 사용자가 알 수 있게 모니터에 본래대로 재생시켜 주기도 하는 소프트웨어를 말한다.

[2] 인터넷상에서 자동화된 일을 수행하는 소프트웨어를 의미하며 Internet bots, web robots, WWW robots, bots등으로 불린다

영상 유포등의 내용이 담긴 메일을 읽은 후 첨부된 사이트로 접속해 동영상을 보기 위해 코덱을 설치하면 감염이 이루어 진다.



[그림 2-7] Zlob 감염 증상

일반적으로 Zlob에 감염되면 시작페이지가 변경되고, 툴바가 설치된다. 또한 계속해서 사용자의 PC가 바이러스에 감염되었음을 알리며 허위 백신 프로그램의 설치를 유도한다. 이러한 허위 백신 프로그램을 설치하게 되면 허위 진단 결과를 표시하며 치료를 위해 결재를 요구하는데 이 때 결재를 하게 되면 PC사용자의 신용카드 번호가 유출된다.

인터넷의 발전과 함께 국내 또는 해외에서 인기 있는 영화나 드라마 같은 동영상 컨텐츠들의 이용이 활발해 지고 있다. 동영상 컨텐츠는 다양한 코덱을 이용하여 압축되어 있으며, 재생하기 위해서는 적절한 코덱이 필요하다. 최근의 많은 동영상 재생 프로그램들이 자동으로 필요한 코덱을 검색하고 사용자의 PC에 설치하는 기능이 있지만 지속적으로 국내에서 감염이 신고되는 것으로 미루어 코덱을 가장한 즐롭의 배포방법은 여전히 효과가 있는 것으로 판단된다.

Win-Spyware/HideProc.43008 진단 증가

지난 1월 진단 추가된 Win-Spyware/HideProc.43008는 Memory mapped file io를 사용해 프로세스 목록에서 숨길 프로세스를 공유하며, 공유된 프로세스를 작업관리자(taskmgr.exe)

의 메모리를 패치하고, NtQuerySystemInformation, Heap32ListFirst, Heap32ListNext, Heap32First, Heap32Next, Process32First, Process32Next, Process32FirstW, Process32NextW, Thread32First, Thread32Next, Module32First, Module32Next, Module32FirstW, Module32NextW 등을 후킹해 프로세스의 존재 사실을 은폐시키는 기능을 한다.

이 프로그램은 허위백신과 같은 의심스러운 프로그램에서 자신의 실행을 감추기 위한 목적으로 사용되고 있는데, Win-Spyware/HideProc.43008의 진단 및 문의건수가 증가하게 된 것은 많은 허위백신들이 동일한 엔진 모듈을 이용하면서 UI만 조금 바꾸는 방법으로 새로운 백신인 것처럼 배포하기 때문으로 판단된다.

스파이제로에서 허위 백신과 같은 유해가능한 프로그램을 진단하기 위해서는 배포지 확인 등 스파이웨어 진단 정책에 위반하는 사항들을 모두 분석해야 하기 때문에 진단 추가가 늦어질 수 있다. 따라서 Win-Spyware/HideProc.43008이 계속해서 진단되는 경우 불필요한 프로그램이 설치되어있을 가능성이 높기 때문에 자신이 설치하지 않은 프로그램이 PC에 설치되었는지에 대한 확인이 필요하며, 스스로 확인이 어려울 경우 백신업체에 문의해서 확인해야 한다.