ASEC Report 10월

® ASEC Report

2007. 11

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]

(1) 10월 악성코드 통계

순위		악성코드명	건수	%
1	new	Win-Trojan/KorGameHack.17920.BR	272	20.3%
2	new	Win-Trojan/KorGameHack.26624.AI	267	19.9%
3	new	Win-Trojan/KorGameHack.14848.FO	195	14.5%
4	↓3	Win-Trojan/Xema.variant	140	10.4%
5	new	Win-Trojan/OnlineGameHack.15360.I	120	8.9%
6	new	Win-Trojan/KorGameHack.19456.BM	113	8.4%
7	new	Dropper/OnlinegameHack.18944	70	5.2%
8	new	Win32/QQPass.worm.26667	60	4.5%
9	new	Win32/Autorun.worm.31244	55	4.1%
10	new	Dropper/OnlineGameHack.18432.J	51	3.8%
합계			1,343	100.0%

[표 1-1] 2007년 10월 악성코드 피해 Top 10

► 월 악성코드 피해 동향

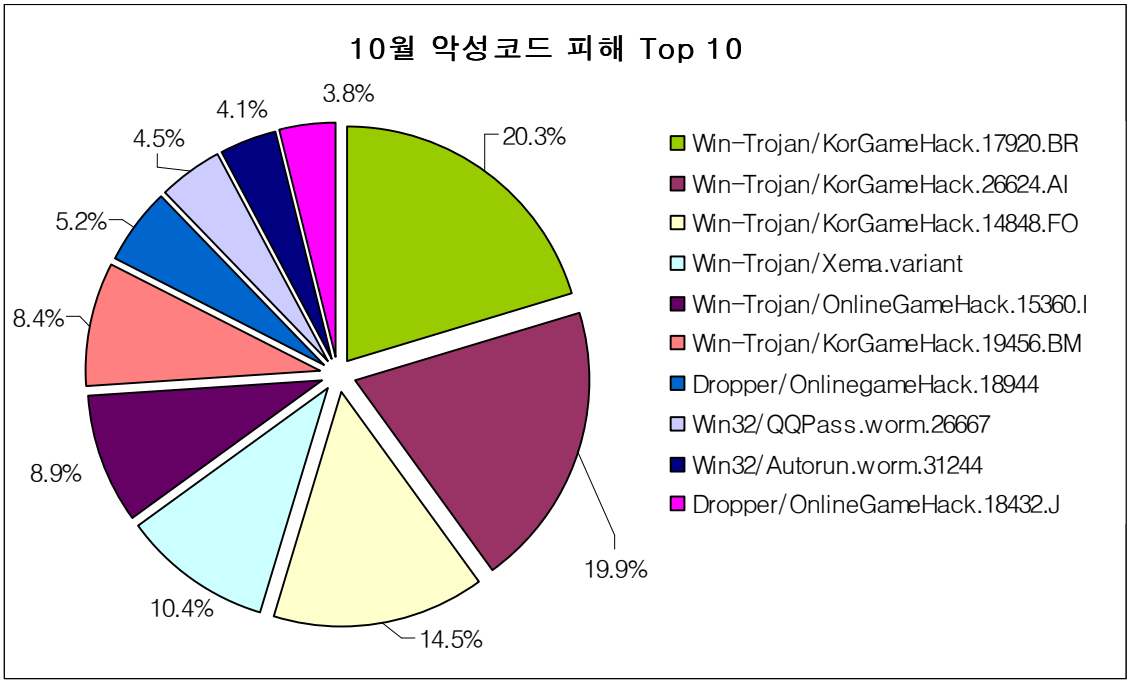
전월 악성코드 피해 Top10과 비교했을 때 10월의 악성코드 피해 Top10에는 많은 변화가 있었다. 금전적인 목적을 위해서 사용자의 게임계정 정보를 유출하려는 게임 핵 류의 트로이목마 5종과 이와 관련된 드롭퍼 2종이 10월 악성코드 피해 Top10에 새롭게 진입하였고 지난 8, 9월 2달 동안 꾸준하게 피해 Top10의 1위를 고수해 온 Win-Trojan/Xema.variant는 3계단 하락한 4위를 내려 앉았으며, 그 밖에 2, 3위에 랭크 되어있던 Win32/Virut과 Win32/IRCBot.worm.variant 등도 각각 16, 12위로 하락하였다. 또한 전월 악성코드 피해 Top10에서 각각 4, 5, 8위에 랭크 되었던 스크립트 형 악성코드인 VBS/Autorun, VBS/Solow, TextImage/Autorun 등도 10월 악성코드 피해 Top 10의 순위권 밖으로 밀려났다.

10월 악성코드 피해 Top10에 랭크 되어있는 악성코드는 주로 게임 핵 류의 트로이목마로 바이러스, IRCBot, 악성스크립트, 다운로더 등이 분포해 있던 전월에 비해 다양성은 다소 떨어지지만 금전적인 목적을 위해서 특정대상을 공격하는 정보유출 형 악성코드들의 변종 및 신종이 꾸준하게 양산되고 있음을 알 수가 있다.

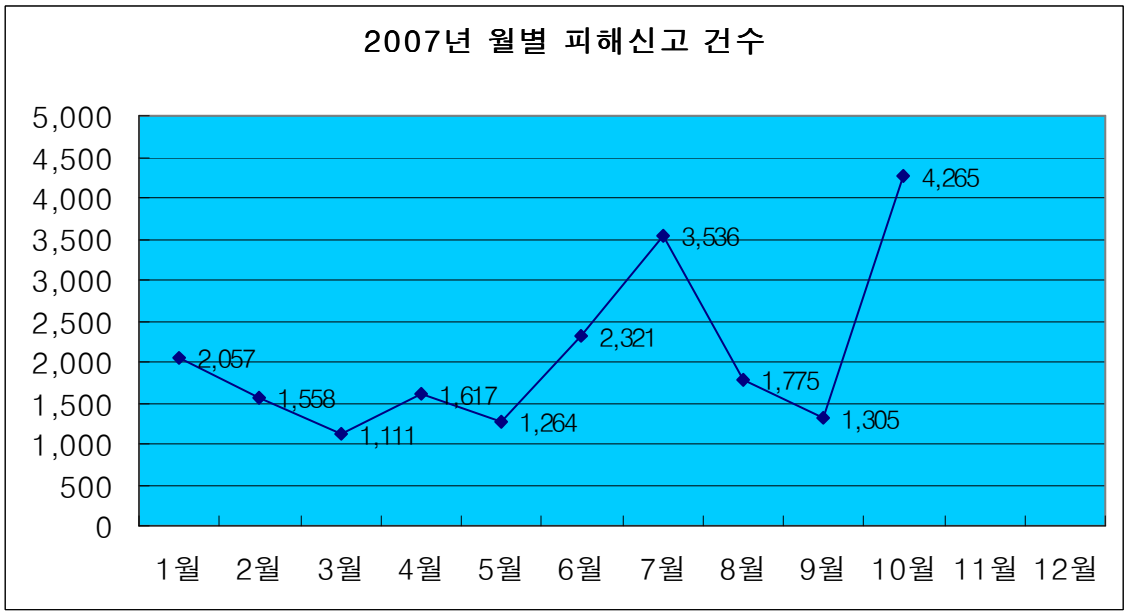
[1] 2007년 11월부터는 악성코드 통계산출 기준날짜가 전월 25일부터 익월 26일로 변경 되었다. 특히 10월은 부득히 10월1일부터 25일까지를 기준으로 통계 기간이 조정되었다

이처럼 금전적인 목적을 위한 정보유출 형의 트로이목마 류는 앞으로도 계속 악성코드 피해 Top 10에 랭크될 것으로 보이므로 사용자들은 이런 트로이목마 류를 포함한 다양한 악성코드로부터 감염을 예방하고 피해를 최소화하기 위해서는 자신이 사용하는 운영체제 및 백신 프로그램에 대한 꾸준한 업데이트와 관리가 필요하다.

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



[그림 1-1] 2007년 10월 악성코드 피해 Top 10



[그림 1-2] 2007년 월별 피해 신고건수

[그림 1-2]에서 월별 피해 신고 건수는 7월의 피해 신고건수 3,536건을 제외한 9월까지의 월별 피해 신고건수는 2,500건을 넘지 않았으나, 10월에 4,265건으로 전월 1,305건에 비해 200% 이상 피해건수가 증가하였다. 이는 기존에 감염된 악성코드(주로 다운로더)가 백신의 탐지를 회피하기 위해서 새로운 신종 및 변종을 다수 다운로드 하여 사용자의 시스템에 설치하기 때문인 것으로 판단된다.

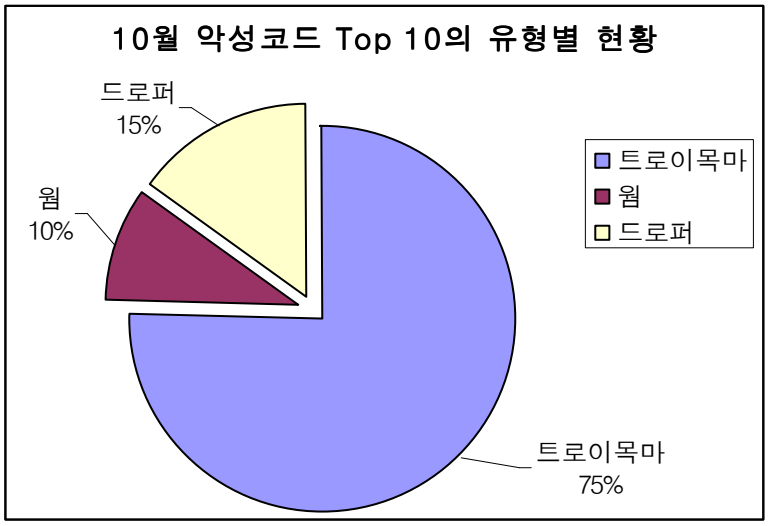
순위	진단명	건수
1	Win-Trojan/KorGameHack.17920.BR	272
2	Win-Trojan/KorGameHack.26624.AI	267
3	Win-Trojan/KorGameHack.14848.FO	195
4	Win-Trojan/Xema.variant	140
5	Win-Trojan/OnlineGameHack.15360.I	120
6	Win-Trojan/KorGameHack.19456.BM	113
7	Dropper/OnlinegameHack.18944	70
8	Win32/QQPass.worm.26667	60
9	Win32/Autorun.worm.31244	55
10	Dropper/OnlineGameHack.18432.J	51
11	Win-Trojan/OnlineGameHack.17408.B	47
12	Win32/IRCBot.worm.variant	45
13	Dropper/OnLineGameHack.17408.B	41
14	Win-Trojan/OnlineGameHack.17920.E	34
15	Dropper/OnLineGameHack.17408.C	32
16	Win32/Virut	31
17	Win-Trojan/OnlineGameHack.24576.L	31
18	Dropper/OnLineGameHack.17920.B	28
19	Win-Trojan/KorGameHack.16896.CI	28
20	Dropper/OnlineGameHack.16896.B	26

[표 1-2] 2007년 10월 악성코드 피해 Top 20

[표 1-2]에서 보면 Top 20에 드롭퍼가 6종이 랭크 되어있고 전체 Top 20의 14%를 차지하였음을 알 수 있는데, 이는 5종의 정보유출 형 트로이목마가 Top 10([표 1-1참고)의 상위권에 랭크될 수 있었던 하나의 요인으로 파악되며 Top 20에 랭크 된 정보유출 형 트로이목마들 중의 일부는 파일 다운로드 하는 기능을 가진 경우도 있었다.

► **10월 악성코드 피해 Top 10의 유형별 현황**

[표 1-1]의 악성코드 피해 Top 10에 랭크 되어있는 악성코드를 유형별로 살펴보면 아래 [그림 1-3]과 같다.

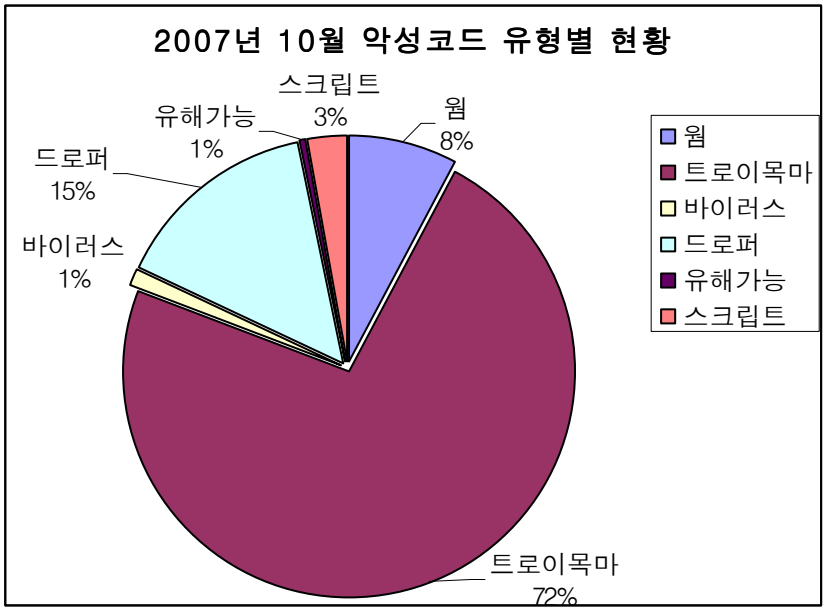


[그림 1-3]2007년 10월 악성코드 Top 10 유형별 현황

10월에도 마찬가지로 금전적인 이득을 노린 정보유출 형 악성코드들이 가장 많은 피해를 발생시켰으며 전월(48%)대비 36% 증가하였다. 10월 경우 Mydoom 및 Mytob 등 다양한 웜이 발견되긴 하였으나 피해신고건수가 미비하였고 Win32/QQPass.worm.26667는 60건, Win32/Autorun.worm.31244 55건의 피해신고가 접수되면서 각각8, 9위에 랭크 되었고 이로 인해 전월 대비(9%) 1%정도 상승하였고, 스크립트(17%)와 바이러스(26%)는 2007년 10월 악성코드 피해 Top 10 순위권 밖으로 밀려났기 때문에 [그림 1-3]에는 포함되지 못 했으며 그 자리를 드로퍼(15%)가 대신하였다.

► **피해신고 된 악성코드 유형현황**

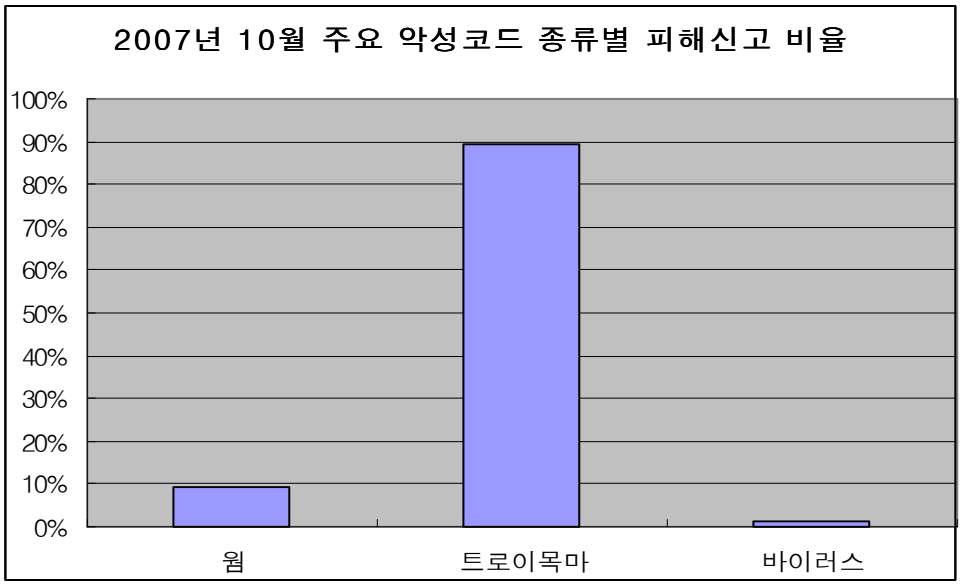
2007년 10월에 피해신고 된 악성코드의 유형별 현황은 아래 [그림 1-4]와 같다.



[그림 1-4] 2007년 10월에 피해 신고된 악성코드의 유형별 현황

[그림 1-4]를 살펴보면, 전월과 마찬가지로 트로이목마 계열이 72%로 가장 많이 차지하고 있으며 2위 드로퍼 15%, 3위 웜 8% 그리고 스크립트 3%, 유해가능 1%, 바이러스 0.18%순이다. 트로이 목마의 경우 전월(74.8%)에 비해 소폭 하락하였으나 지난 몇 개월에 이어 10월에도 마찬가지로 전체 피해 건수에서 부동의 1위를 차지하였다. 그 원인은 정보유출 형 트로이목마를 제작 및 유포함으로써 막대한 금전적인 이득을 취하고 있고, 이를 위하여 다수의 신/변종 트로이목마가 제작 및 유포되고 있기 때문인 것으로 판단된다.

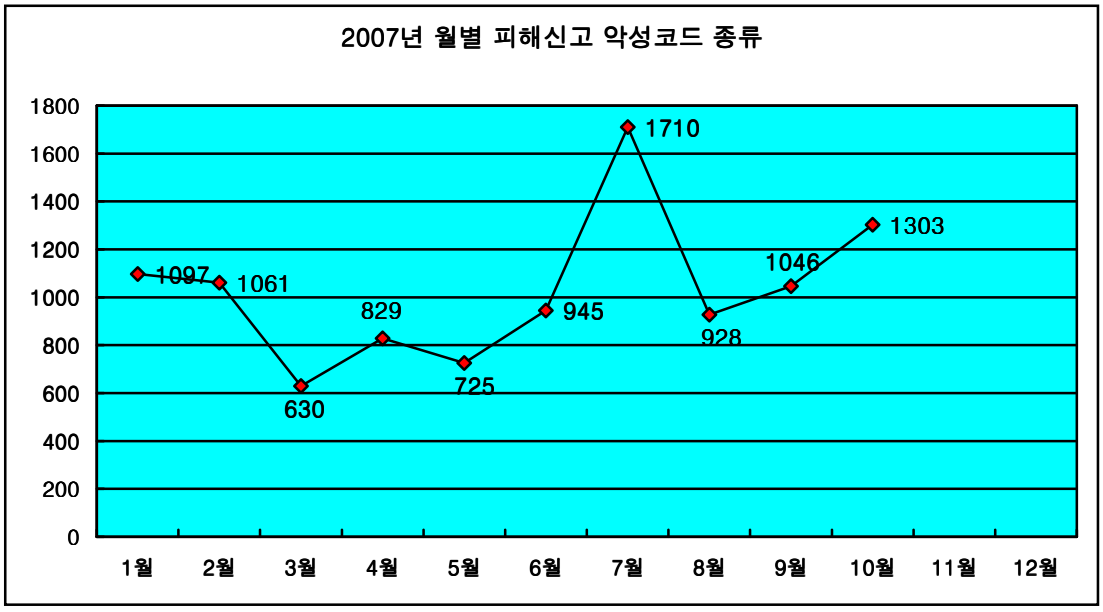
주요 악성코드 유형의 피해신고 분포를 보면 [그림 1-5]와 같다.



[그림 1-5] 2007년 웜, 트로이목마, 바이러스의 피해신고 비율

[그림 1-5]에서 보면 전월 대비 웜과 트로이목마는 다소 하락하였으나 바이러스의 경우는 약 1%정도로 다소 상승하였으며 [그림 1-5]에서 바이러스가 차지하는 비율은 극히 미비하지만 Win32/Virut와 그 변형들의 감염피해가 발생했을 경우 완전한 치료가 다소 어렵다는 특징이 있다.

► **월별 피해신고 된 악성코드 종류 현황**



[

그림 1-6] 2007년 월별 피해신고 악성코드 종류

[그림 1-6]은 국내에서 발견된 변종 및 신종 악성코드의 현황을 나타내며, 8월 이후로 다시 증가추세를 보이고 있다. 또한 10월의 경우 PDF의 취약점을 이용한 악성코드**(PDF/Exploit-Downloader)**가 스팸메일의 첨부파일로 확산되기도 하였다.

국내 신종(변형) 악성코드 발견 피해 통계

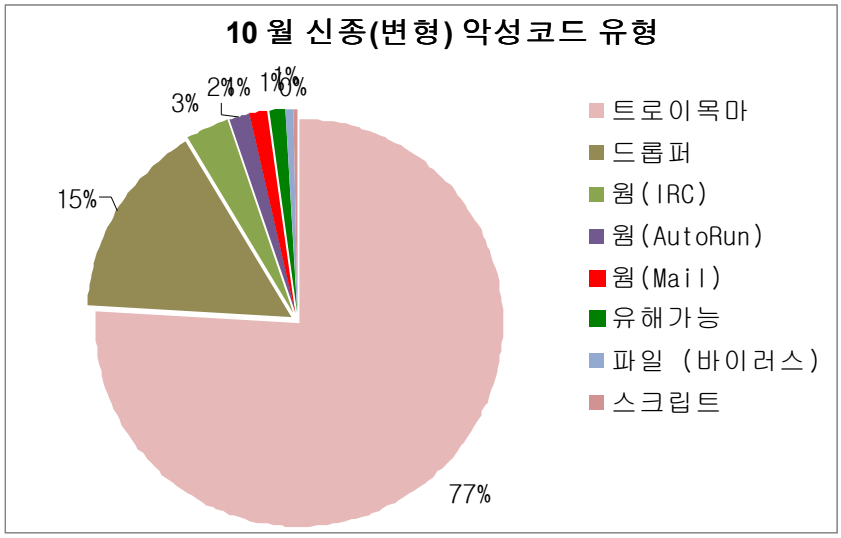
10월 한달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 1-3], [그림1-7]과 같다.

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
8 월	54	327	72	1	6	0	0	0	10	1	471
9 월	32	418	78	1	1	0	0	0	1	1	531
10 월	23	269	55	1	2	0	0	0	5	0	355

[표 1-3] 2007년 최근 3개월간 유형별 신종 (변형) 악성코드 발견현황

지난 2월 ASEC 리포트에서 밝혔듯이 중국의 명절은 국내 악성코드 유입에 큰 영향을 주고 있다. 지난 2월의 경우 춘절로 인하여 악성코드 수가 감소 하였고 10월은 중추절의 이유로 악성코드의 수가 감소하였던 것으로 보인다. 물론 위에서 밝힌 대로 통계기간이 다소 짧아서 전월과 비교 될 수도 있겠지만 5일정도의 기간을 제외하여도 10월은 전월보다 악성코드는 33% 감소하였다. 트로이목마의 비율만 본다면 36% 감소하였다. 이로서 다시금 국내 중국산 악성코드 유입이 많음을 다시 실감 할 수가 있었다.

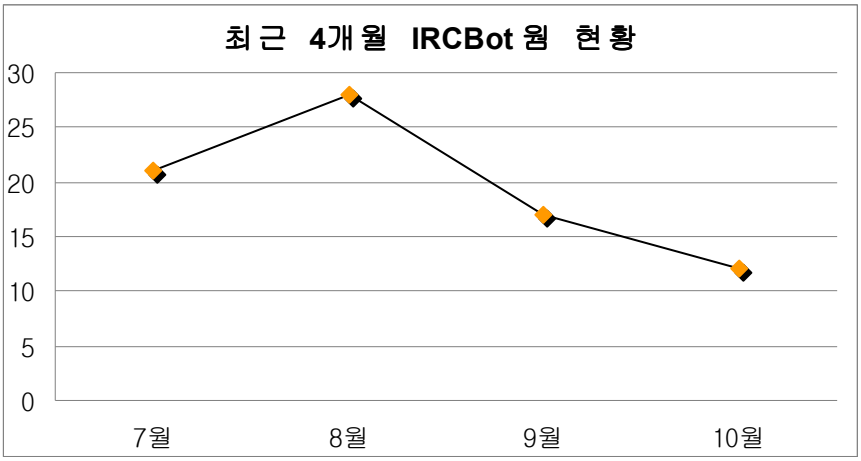
다음은 이번 달 악성코드 유형을 상세히 분류 하였다.



[그림 1-7] 2007년 10월 신종 및 변형 악성코드 유형

트로이목마이 유형은 역시 온라인 게임 계정을 탈취하는 게임핵류가 가장 많다. Autorun.inf 를 생성하여 자신을 자동실행하는 악성코드가 상당수 존재하며 이전 ASEC 리포트에서도 언급한 바와 같이 중국산 악성코드 대부분이 이 증상을 가지고 있다. 위 통계에서는 자신의 복사본과 Autorun.inf 를 생성하는 경우만 반영한 것이다.

최근 IRCBot 웜은 접수 건수가 감소하고 있다. 전체 악성코드의 3% 밖에 지나지 않는다. IRCBot 웜이 많았던 2004년, 2005년 상황과는 현재는 비교 되지 않는다.



[그림 1-8] 2007년 최근 4개월 악성 IRCBot 웜 현황

위 현황에서는 최근 2개월간 하락하고 있으며 그 이유는 뚜렷하지 않다. 다만 악성코드의 BotNet은 근래들어 굳이 악성 IRCBot 웜을 이용하지 않아도 얼마든지 은밀하게 동작하는 Win32/Zhelatin.worm이나 Win-Trojan/Runtime과 같은 은닉채널을 이용하는 악성코드가 강세를 보이므로 이런 이유도 그 원인으로 추정 해 볼 수가 있다.

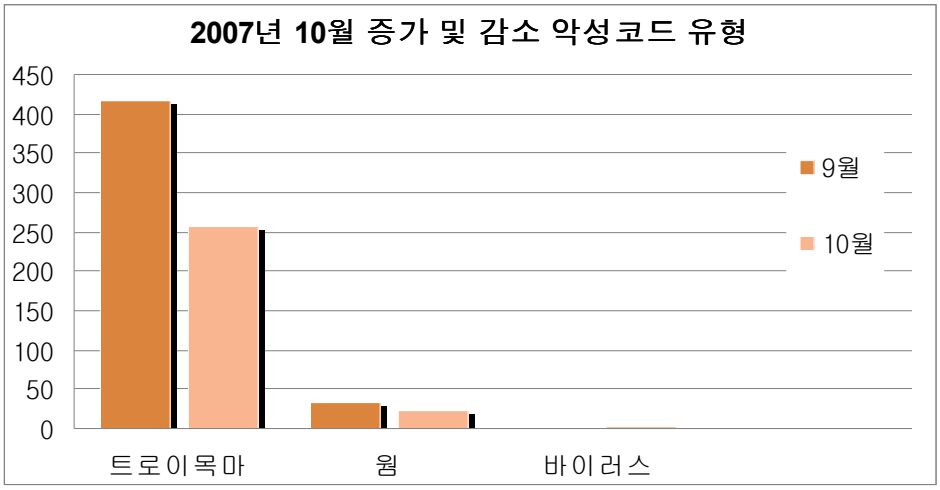
이번 달은 2종의 바이러스가 보고 되었는데 다음과 같다.

- Win32/Hala
- Win32/Jlok 변형

Win32/Hala 는 프로그램의 시작 실행 시점에 return 코드를 삽입하여 바이러스 섹션으로 점프하도록 되어 있다. 따라서 감염된 파일은 *.DL5 라는 섹션이 추가 되어 있다. MZ Header에 4 바이트의 특정값을 채워 자신이 감염 되었음 마킹하여 중복감염 되지 않도록 한다. 이 바이러스는 마지막 섹션 헤더 추가시 Bound Improt Table 정보가 있어도 덮어 쓰기 때문에 감염된 파일은 치료를 하기 전까지는 실행 되지 않는다. 따라서 치료시 Bound Improt Table Directory 정보 (RVA, Size) 를 0 으로 세팅해주면 실행이 가능해진다.

Win32/Jolk 는 이전에 알려진 형태의 변형이다. 특이하게 워드 문서 파일인 *.DOC 확장자를 감염 대상으로 한다. 감염된 DOC 파일은 원본의 앞 0x400 바이트가 암호화 되어 바이러스 파일이 앞에 붙은 형태로 동일명의 *.exe 파일로 변경된다. 감염된 *.DOC 파일을 실행하면 원본의 *.DOC 가 만들어져 워드문서는 정상적으로 오픈된다.

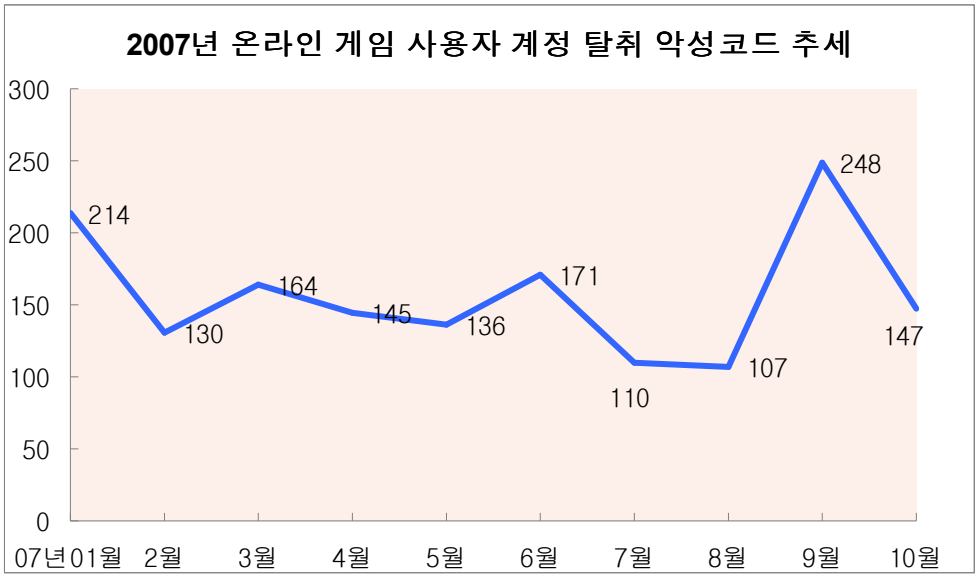
다음은 10 월에 증가 및 감소한 주요 악성코드 유형에 대한 현황이다.



[그림 1-9] 2007년 10월 감소 및 증가 악성코드 유형

위에서 밝혔듯이 통계기간과 중국의 국경절의 영향으로 추정되어 악성코드 수는 전월 대비 감소 하였다. 위 [그림 1-9]에는 없지만 유해가능 프로그램의 경우 전원대비 소폭 증가 하였다. 여기에는 다양한 형태가 있는데, 프로세스를 숨겨주는 형태, FTP 데몬, IE BHO에 등록되어 광고를 보여주는 형태가 있었다.

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



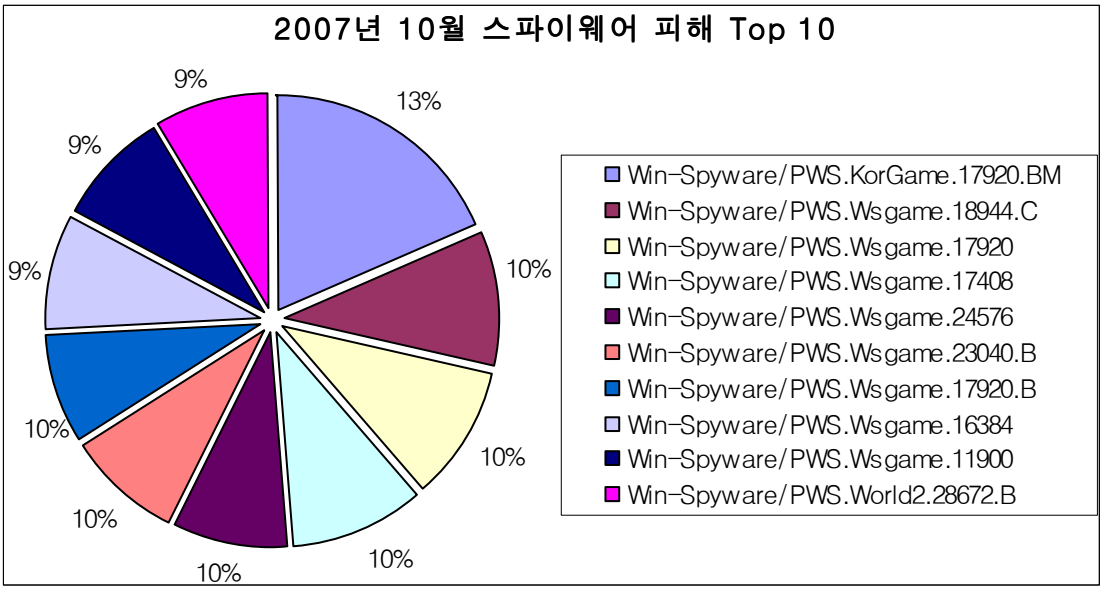
[그림 1-10] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

전월과 달리 41%감소 하였으나 감소 추정 원인은 위에서 밝힌 바와 같다. Win-Trojan/KorGameHack과 Win-Trojan/OnLineGameHack을 비교하면 Win-Trojan/OnLineGameHack 의 비율이 30% 정도 높은 편이다. 이들의 차이는 주로 국내 온라인 게임과 국외 (대부분 중국 및 대만) 온라인 게임 계정을 탈취하는 형태로 나눌 수 있다. 그러나 진단명을 이렇게 분류 하였지만 이 부분은 오차가 있을 수도 있다.

(2) 10월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Spyware/PWS.KorGame.17920.BM	13	13%
2	New	Win-Spyware/PWS.Wsgame.18944.C	7	10%
3	New	Win-Spyware/PWS.Wsgame.17920	7	10%
4	New	Win-Spyware/PWS.Wsgame.17408	7	10%
5	New	Win-Spyware/PWS.Wsgame.24576	6	10%
6	New	Win-Spyware/PWS.Wsgame.23040.B	6	10%
7	New	Win-Spyware/PWS.Wsgame.17920.B	6	10%
8	New	Win-Spyware/PWS.Wsgame.16384	6	9%
9	New	Win-Spyware/PWS.Wsgame.11900	6	9%
10	New	Win-Spyware/PWS.World2.28672.B	6	9%
합계			70	100%

[표 1-4] 2007년 10월 스파이웨어 피해 Top 10



[그림 1-11] 2007년 10월 스파이웨어 피해 Top 10

2007년 10월 전체 스파이웨어 피해신고 건수는 총 999건으로 지난 9월의 592 건에서 약 400건 가량 크게 증가하였다. 10월 스파이웨어 피해 신고가 증가한 원인은 다수의 온라인게임 계정 유출 목적의 스파이웨어가 많이 배포되었기 때문인 것으로 분석된다. 피해신고 건수 999건 중 455건이 온라인게임 계정 유출을 시도하는 패스워드스틸러(PWS) 계열의 스파이웨어로 전체 피해 신고의 약 45%를 차지하고 있으며, 9월의 약 140건 보다 약 100건 증가하였다. 이를 반영하여 스파이웨어 피해 통계의 Top10을 모두 온라인게임 계정 유출 스파이

웨어가 차지하고 있는데, 이 중에서도 스파이웨어 피해 Top10의 대부분을 차지하고 있는 스파이웨어 더블유에스게임(Win-Spyware/Wsgame)은 중국에서 제작된 온라인게임 계정 유출을 목적으로 제작되었으며, 2006년 말부터 배포되기 시작하였다.

2007년 10월 유형별 스파이웨어 피해 현황은 [표 1-5]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
8월	197	105	43	156	12	6	0	0	0	519
9월	291	119	35	132	8	7	0	0	0	592
10월	632	131	38	180	7	11	0	0	0	999

[표 1-5] 2007년 10월 유형별 스파이웨어 피해 건수

2007년 10월 전체 스파이웨어 피해신고 건수는 온라인게임 계정 유출 스파이웨어의 증가로 스파이웨어류의 피해신고가 크게 증가한 반면 애드웨어나 다운로더 같은 다른 분류의 스파이웨어의 피해 신고 건수는 대체로 9월에 비해 소폭 증가하거나 비슷한 수준임을 알 수 있다. 피해 신고가 접수된 애드웨어의 경우 대부분이 국내에서 제작된 프로그램이었으며, 이들 애드웨어를 다시 형태별로 분석해 본 결과 리워드(쇼핑몰 현금적립 프로그램), 툴바, 허위 안티-스파이웨어가 대부분을 차지하고 있었다.

최근에 발견되는 애드웨어는 툴바나 BHO와 같은 브라우저 확장을 이용한 키워드 간접광고, 리워드 서비스가 대부분을 차지하고 있으며, 직접적으로 팝업 광고를 노출하는 형태의 애드웨어는 감소하고 있는 추세이다. 애드웨어의 배포 방법으로 과거에는 불특정 웹 사이트에서 ActiveX 컨트롤을 이용하여 배포하였으나 최근에는 ActiveX 컨트롤을 이용하는 대신 다운로더를 이용하거나 다른 프로그램의 번들로 설치되는 방식으로 배포하고 있다. 번들 설치는 애드웨어가 설치되면 자사 또는 제휴사의 또 다른 애드웨어를 사용자 동의 없이 설치하는 방식으로 ActiveX 컨트롤을 이용하여 배포하는 방식보다 배포지 추적이 어렵다. [표 1-5]의 다운로더 건수의 경우 피해 신고 접수 180건 중 대부분이 국내제작 애드웨어와 관련이 있었으며 애드웨어 피해 신고 증가의 원인으로 파악된다.

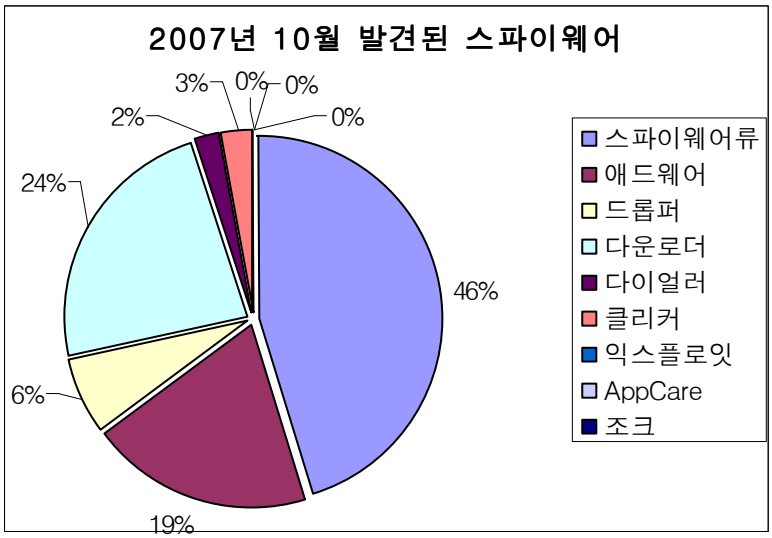
► 10월 스파이웨어 발견 현황

10월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-6], [그림 1-12]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
8월	64	31	6	52	4	2	0	0	0	159

9월	91	37	12	40	6	6	0	0	0	192
10월	98	42	14	51	5	6	0	0	0	216

[표3] 2007년 10월 유형별 신종(변형) 스파이웨어 발견 현황

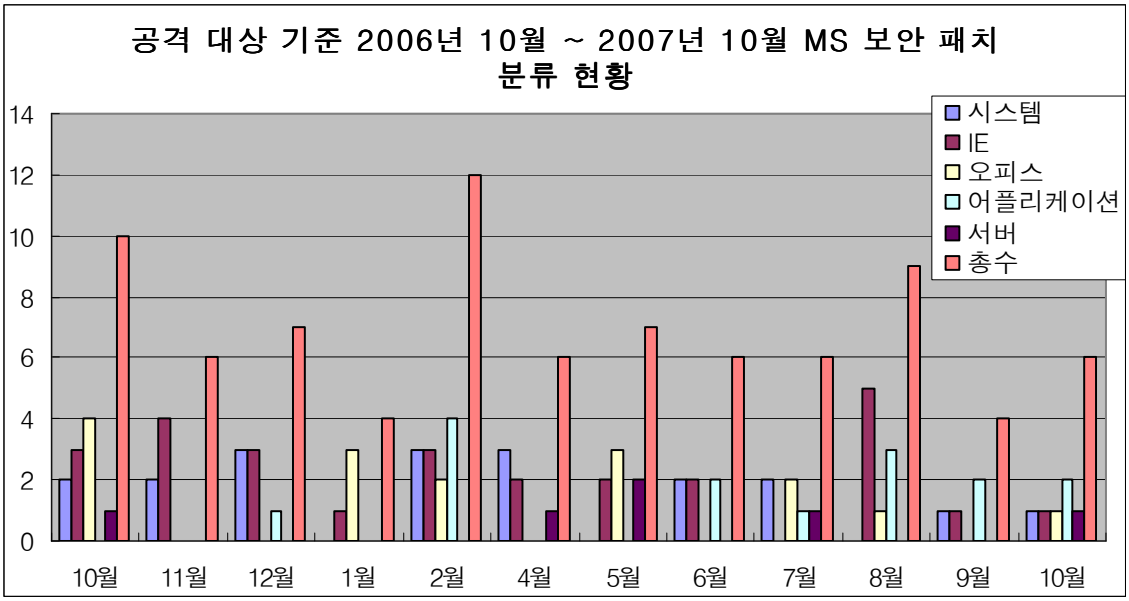


[그림 1-12] 2007년 10월 발견된 스파이웨어 프로그램 비율

[표 1-6]과 [그림 1-12]는 2007년 10월 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 지난 9월에 비하여 스파이웨어 피해신고는 크게 증가한 반면 신종 및 변형 발견 건수는 각 유형별로 소폭 증가하는데 그쳤다.

(3) 10월 시큐리티 통계

2007년 10월에는 마이크로소프트사에서 총 6개의 보안 업데이트를 발표하였으며, 발표된 업데이트는 긴급(Critical) 4개, 중요 2개로, 9월의 총 4건과 비교하여 50% 증가하였다. 이 중에서 인터넷 익스플로러 공격에 사용될 수 있는 MS07-057 에 대한 패치가 포함되었으며, 마이크로소프트 오피스(MS Office) 관련 패치인 MS07-060 Kodak 이미지 뷰어 원격 코드 실행 취약점인 MS07-055 가 포함된 것이 특징이라고 할 수 있다.



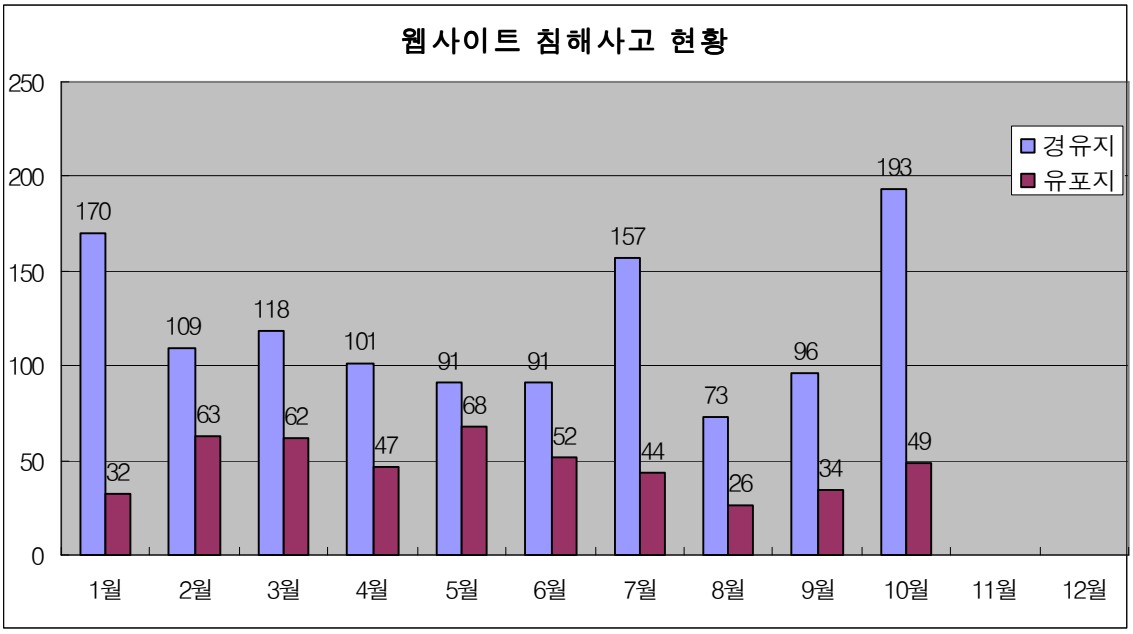
[그림 1-13] 2006년 10월 ~ 2007년 10월 공격대상 기준 MS 보안 패치 현황

[그림 1-13]을 보면, 전반적으로 2007년에 들어와서, 어플리케이션 취약점들(IE, 오피스, 기타 어플리케이션) 취약점들이 증가 추세에 있는데, 10월달에 다시 오피스 취약점인 Microsoft Word 의 취약점으로 인한 원격 코드 실행 문제점인 MS07-060이 발표되었다.

오피스 취약점은 꾸준히 발견되는 추세이긴 하지만, 대부분 MS Office 2007 버전에는 영향을 주지 않고 있다. 또한 9월에 발표된 마이크로소프트 오피스 2003 서비스팩 3 에도 영향을 주지 않고 있다.

이러한 오피스 취약점들은 악성코드가 포함되어 메일이나 웹을 통해 공격하기 때문에, 주의가 필요하다. 기업 관리자들은 MS Office 2003 SP3나 MS Office 2007 의 사용을 고려해 볼 수 있다. 또한, 오피스에 대한 보안패치는 반드시 오피스 홈페이지에서 보안 업데이트를 적용해야만, 클라이언트 시스템의 보안성을 강화할 수 있다.

► 2007년 10월 웹 침해사고 현황



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

2007년 10월의 웹 사이트 침해지/배포지 수는 193/49로 2007년 9월과 비교하여 침해지수가 크게 증가하였지만 배포지의 수는 변화가 거의 없다. 침해지의 수가 크게 증가한 이유는 10월 중 웹 침해사고 현황 조사를 위해 탐색한 사이트의 수가 3배정도 증가하였기 때문이다. 따라서 2007년 11월에는 기존 달보다 침해지의 수가 더욱 증가할 것으로 예상된다. 그럼에도 불구하고 최종 배포지의 수가 전과 비교하여 큰 차이가 없는 것은 여전히 국내의 많은 웹 사이트 침해사고의 대부분이 소수의 공격자에 의한 것으로 추정할 수 있다. 2007년 11월에는 탐색한 사이트수의 증가와 침해지 수 증가의 관계에 대한 자세한 분석도 가능할 것이다.

악성 코드 배포를 위해 사용된 취약점 종류의 비율은 이전과 마찬가지로 MS07-017 취약점의 비율이 33%로 상위를 차지했다. 침해사고를 확인한 웹 사이트의 관리자들은 사후처리에 신경을 써야하고 일반 PC 사용자들은 운영체제의 패치를 항상 적용하고 Anti-Virus 제품을 설치한후 인터넷을 사용하는 것이 안전하다.

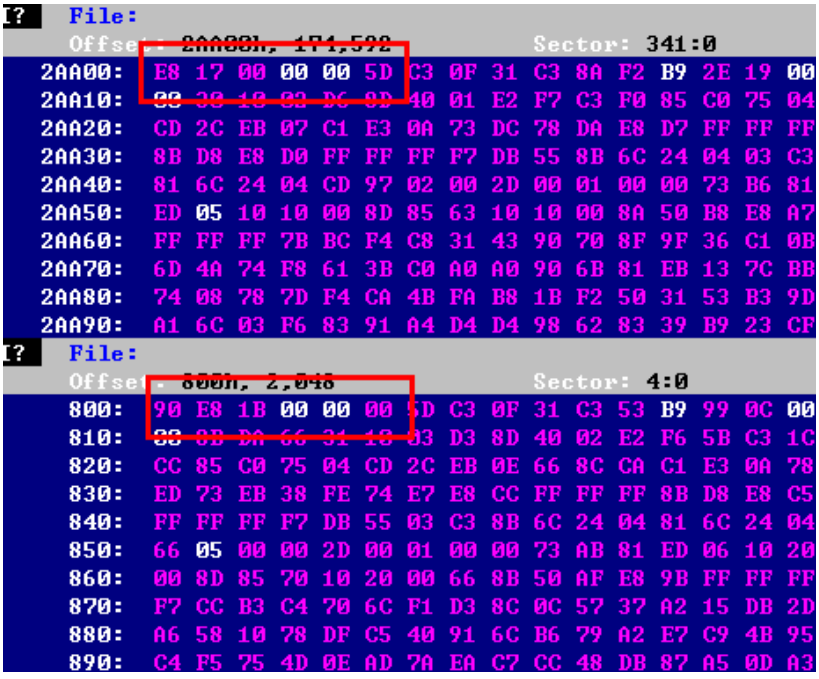
II. ASEC Monthly Trend & Issue

(1) 악성코드 – PDF 의 잘못된 URI 처리와 관련 악성코드 등장

10월은 악성코드 수치도 전월 대비 감소 하였고 비교적 조용한 한달 이였다. 지난달 Win32/virut 변형이 발견 된 이후로 Virut 바이러스 원형 또는 B 형에 대한 간단한 변형이 국내에서 여러 건 신고가 접수 되었다. 그리고 Win32/Zhelatine.worm 이라고 알려진 악성코드 변형이 자신의 파일명을 변경한 내용과 MP3 파일을 스팸으로 보낸 사건 그리고 PDF 파일 취약점을 이용하여 특정 악성코드를 다운로드 실행하는 이슈에 대해여 정리해 보도록 하겠다.

► Win32/Virut 바이러스 변형

러시아에 호스트를 두고 있는 특정 URL 에서 계속적으로 Win32/Virut 바이러스 원형에 대한 변형을 만들고 배포하고 있음이 밝혀졌다. 특히 일부 안티 바이러스의 진단 및 치료를 회피 하려고 바이러스의 시작 주소의 옵코드를 E8 또는 90을 사용하고 있음이 알 수가 있었다.



[그림 2-1] Win32/Virut 변형 시작주소 비교

특히 V3가 진단/치료를 추가하면 바로 변형을 배포하는 행위를 서슴지 않았다. 또한 변형에 따라 바이러스 몸체를 암호화 한 것과 하지 않는 것으로 나누기도 하여 진단을 회피하려는 모습이 역력하였다. 다행이라면 Win32/Virut 바이러스 원형이므로 진단/치료가 복잡한 B, C

이 아니어서 감염시 치료 성공율 또는 진단/치료 엔진 제작의 난이도가 그리 높지는 않았다.

► MP3로 전달 되는 스팸 메일

최근 스팸메일의 형태는 매우 독특하다. 엑셀 문서 파일 (*.xls) 에 이어서 어도브아크로벳 문서 (*.PDF)로 된 스팸이 보고 되었다. 이것은 안티 스팸 제품을 우회 하려는 의도가 다분하다. 이번 달에는 *.MP3 파일 형태의 스팸이 발견 되었다. 이것은 특정 회사에 대한 주식 광고를 하여 주가를 부풀리도록 의도 하고 있다. MP3 는 다음과 같은 내용을 담고 있다.

> "Hello, this is an investor alert
>
> Exit Only Incorporated has announced it is ready to launch its new text4cars.com website, already a huge success in Canada, we are expecting amazing results in the USA.
>
> Go read the news and sit on EXTO. That symbol again is EXTO. Thank you."

[그림 2-2] MP3 스팸내용

MP3 파일 특성상 음질이 좋으면 파일 크기가 늘어나기 때문에 이것을 스팸으로 보내기에는 적당하지 않다. 따라서 해당 파일은 다음과 같은 제원을 가지고 있다.

General

Duration	0:26.074 (287471 samples)
Sample Rate	11025 Hz
Channels	1
Bitrate	16 kbps
Codec	MP3
Codec Profile	MP3 CBR
Encoding	lossy

Other

<MP3_STEREO_MODE>	mono

[그림 2-3] MP3 스팸 제원

따라서 해당 파일을 실제로 재생해보면 매우 소리가 작고 음질이 나쁘다. 따라서 이러한 형태의 스팸은 앞으로 더 발생 될지 귀추가 주목된다. 그러나 더 많은 내용을 담고 음질을 향상 하면 메일 크기는 커지므로 안티 스팸 제품의 필터링은 피하기 어려울 것으로 본다.

► 변화하는 Win32/Zhelatein.worm

Win32/Zhelatin.worm 변형은 본 글을 작성하는 현재도 변형이 발견되어 엔진에 추가 되고

있는 실정이다. 10월에 발견 되기 시작한 Zhelatin 웜 변형은 이전과 다르게 자신이 생성하는 파일명을 변경하였다. 피해가 국,내외적으로 크게 발생하고 있어 파일명이 변경된 것까지도 이슈가 될 만하다. 이전에 사용한 파일명은 Spooldr.sys 로 국,내외 유명 포털에서 검색하면 관련 글을 상당수 볼 수 있다. 이번에 새롭게 변경된 파일명은 다음과 같다.

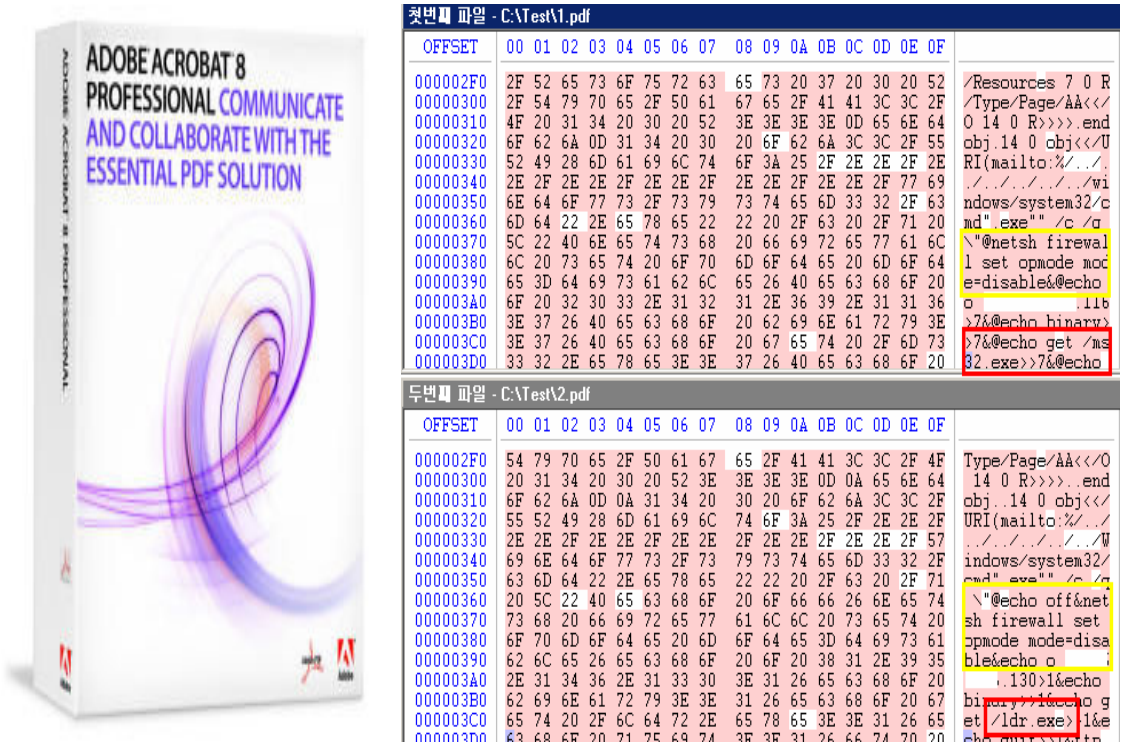
[그림 2-4] Win32/Zhelatin.worm 의 복사본 파일명

Noskrnl.exe 이외에도 Noskrnl.sys, Noskrnl.config 파일을 만들고 드라이버 파일인 Noskrnl.sys 가 특정 커널 함수를 후킹하여 Noskrnl이란 문자열이 들어간 파일을 은폐하도록 해둔다. 이전과 다른 것은 파일명만이 아니라 우선 자신이 생성한 Noskrnl.sys를 실행하기 위하여 기존 변형은 TCPIP.SYS를 패치한다. 즉, Noskrnl.sys를 예로 든다면 정상적인 방법의 드라이버 로드는 이것을 서비스로 등록하여 실행하는 반면에 기존 Zhelatin 웜은 TCPIP.SYS에 작은 쉘코드를 삽입하여 로컬에 존재하는 Zhelatin 웜을 실행하도록 해둔다. 이러한 형태는 Win-Trojan/Patched 라고 진단 된다. 그러나 이번 변형은 정상적인 방법으로 레지스트리에 자신을 등록하여 드라이버를 실행하도록 해두었고, 어떠한 시스템 파일도 변경하지 않는다. Explorer.exe 와 같은 정상 윈도우 파일에 악의적인 쓰레드를 생성하는 증상도 발생하지 않는다. 다만 드라이버는 은폐증상 이외에 특정 보안 프로그램을 무력화 시키는 증상은 여전하다. 이번 달에 발견된 변형은 이것이 어떤 의미를 가지는지는 명확하지는 않지만 제작자는 어떤 의도를 가지고 점점 변화 또는 진화 하고 있음을 틀림없다.

► PDF 문서 파일의 잘못된 URI 를 이용한 악성코드 실행

PDF 취약점이라고 알려졌으나, 실제로는 인터넷 익스플로러 7에서 악용될 수 있는, 이 취약점은 PDF 문서 내에 존재하는 mailto 태그를 처리하는 루틴에서 % 값을 인터넷 익스플로러 7의 ShellExecute() 함수에서 제대로 처리하지 못하는 URL 핸들링 버그이다. 취약한 PDF 문서의 대상은 어도비 아크로뱃 및 리더 8.1 또는 이전 버전들로서, 문서를 작성하는 현재 해당 응용 프로그램 제작사로부터 패치가 공개 되었다.

다음은 취약점을 이용한 악성코드 샘플의 일부와 응용 프로그램 팩키지 모습이다.



[그림 2-5] 취약한 PDF 문서 파일 일부

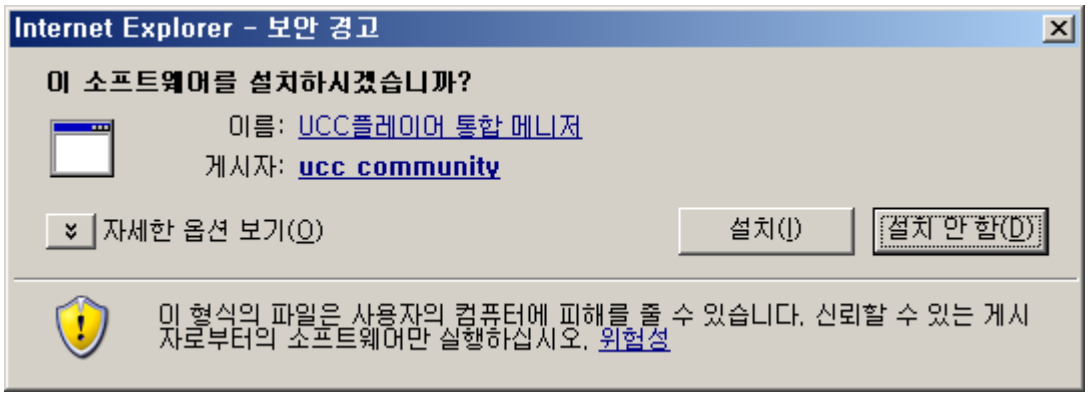
먼저 취약한 문서를 실행한 경우 netsh 명령을 이용하여 윈도우 방화벽에 특정 호스트에 대한 접속 경고를 disable하고, 해당 호스트로부터 파일을 다운로드 하여 실행한다. 이것은 또 다른 악성코드를 시스템에 설치한다. 취약한 문서 파일의 크기는 3K 이내로 작으며 사용자가 메일에 첨부된 상태에서 쉽게 클릭하여 볼 수 있어서 잠재적인 위험이 크다고 할 수 있다. 따라서 메일에 첨부된 PDF 파일의 경우 아는 사람에게 전달 받았다고 해서 바로 실행하지 말고 반드시 안티 바이러스 프로그램을 이용하여 검사 해보는 것이 바람직하겠다. 또한 응용 프로그램 제작사가 공개한 패치를 반드시 설치할 것을 권장한다.

(2) 스파이웨어 – 스파이웨어의 오작동으로 인한 피해

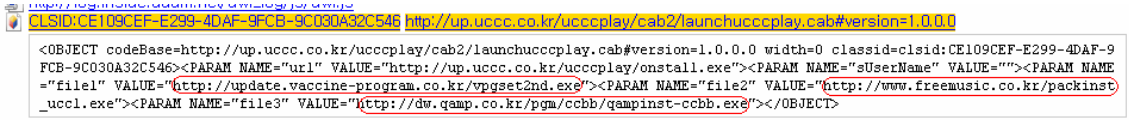
어느 날 바탕화면에 있는 아이콘이 모두 똑같이 표시되거나, 갑자기 컴퓨터가 부팅되지 않는다면 컴퓨터 사용자는 당황할 수 밖에 없을 것이다. 스파이웨어는 컴퓨터의 속도를 느리게 하고 사용자가 원하지 않는 광고를 출력하는 드러난 문제점과 함께 사용자 모르게 컴퓨터를 손상시킬 수 있는 잠재적인 문제를 내포하고 있다. 스파이웨어에 의해 손상된 컴퓨터를 원상태로 복구하는 데는 많은 시간이 소요될 수 있으며 그 과정에서 중요한 데이터를 손실할 수도 있다.

지난 10월 18일 바탕화면 아이콘 확장자가 lnk로 변경되어있고, 모든 실행 가능한 파일이 열리지 않는다는 문의가 안철수연구소로 다수 접수되어 증상을 확인한 결과 Win-Adware/UcccPlayer 업데이트 파일이 동작하는 과정에 레지스트리 정보를 삭제/수정하면서 문제가 발생된 것이 확인되었다.

Win-Adware/UcccPlayer는 동영상 낚시글을 통해 특정 웹사이트로 유인 후 큰 화면의 동영상을 감상하기 위해서 UCC플레이어 통합 매니저 설치를 유도하는 전형적인 스파이웨어의 배포방법을 통해 사용자의 PC에 설치가 되었다. 동영상 실행을 위해 통합 매니저를 설치한 사용자의 PC에는 동영상 실행과 관계없는 허위 백신프로그램, 큐앰프, 윈사이드바, 캐시플러스 등의 프로그램이 사용자 동의를 받지 않은 채 함께 설치된다. (UCCC Player는 지난 4월 동영상 1회 클릭당 1원이라는 새로운 수익방식으로 스파이웨어를 통한 새로운 수익구조를 제시하여 많은 스파이웨어 배포자를 양산한 것으로 보인다.)



[그림 2-6] UCCC player 통합메니저



[그림 2-7] UCCC Player ActiveX CodeBase

[그림 2-7]에서와 같이 ActiveX의 CodeBase를 통해 설치되는 목록 조절이 가능하며, 이렇

게 설치된 스파이웨어의 종류는 서버 설정에 따라 계속해서 바뀔 수 있으며 뚜렷한 증상이 없는 한 설치 사실을 사용자가 인지하기 어렵다.

Win-Adware/UcccPlayer외에도 스파이웨어로 인한 컴퓨터 오류 문제는 꾸준히 보고되고 있다. 5월 7일에는 Win-Downloader/Adod.49238로 진단되는 프로그램이 오류가 있는 BHO파일을 설치해 IE가 실행되지 못하게 하였으며, 같은 달 Win-Adware/IEDoumi의 경우 윈도우에서 방문된 웹사이트 목록을 저장하는 레지스트리(HKCU₩Software₩Microsoft₩Internet Explorer₩TypedURLs)를 이용해 키워드 광고 수단으로 이용하면서 PC 부팅속도가 늦어지게 하는 등 스파이웨어로 인한 많은 문제들이 꾸준히 보고되고 있다.

지난 10월 한달 간 국내에서 제작되고 배포된 프로그램 중 정통부 스파이웨어 사례집과 안철수연구소 스파이웨어 진단규정을 위반하는 것으로 확인된 프로그램은 44종이었으며 이들 프로그램이 번들로 설치하는 목록까지 포함한다면 50종이 넘는다. 매월 이렇게 확인된 수십 종의 국산 신/변종 스파이웨어를 끊임없이 진단추가 하고 있으나, 더 많은 신/변종 스파이웨어들이 생겨나고 있다. 또, 포털사이트 게시판에는 새로운 변형이나 신종 스파이웨어에 의한 컴퓨터 오류를 해결하는 방법을 묻는 글들이 줄어들지 않고 있다.

다양한 필요에 의해 제작되는 소프트웨어는 개발 단계에서 다양한 테스트를 통해 예상할 수 있는 대부분의 버그를 수정하고 안정성이 보장된 상태에서 배포되어야 한다. 이렇게 배포되는 프로그램 조차도 실제 환경에서는 예상치 못한 오류가 발생하는 경우가 있을 수 있다. 응용프로그램의 문제점과는 그 관점이 조금 다를 수 있으나 마이크로소프트 같은 대형소프트웨어 업체에서 제작한 운영체제인 Windows에서도 매월 문제점이 발견되고 있으며 이에 대한 크고 작은 패치들을 나오고 있는 실정이다. 그러나, 우후죽순으로 생겨나는 스파이웨어 제작자들과 보안업체간의 쫓고 쫓기는 관계 속에서 스파이웨어 제작자들은 빠른 시간에 프로그램을 제작해 배포하기 때문에 프로그램 설치 및 동작 시 나타날 수 있는 심각한 오류들에 대비해 필요한 테스트를 거칠 시간적 여유가 충분하지 않을 수 있다. 이런 스파이웨어들은 보안업체의 모니터링과 진단 추가 속에서도 알려지지 않은 루트를 통해 계속 배포되고 있으며 컴퓨터 사용자는 이러한 위협에 항상 노출되어 있는 것이다.

넘쳐나는 스파이웨어 속에서 컴퓨터 사용자를 보호하기 위해서는 스파이웨어를 모니터링하고 끊임없이 진단 추가하는 업체의 노력, 불확실한 프로그램을 설치하지 않는 개인사용자의 노력뿐만 아니라 사용자의 동의 없이는 프로그램이 설치될 수 없도록 하는 엄격한 법규 제정이 무엇보다도 필요할 것이다.

(3) 시큐리티 - MS07-058 RPC의 취약점으로 인한 서비스 거부 문제점

마이크로소프트사가 발표한 2007년 10월 보안 업데이트는 총 6건으로 각각 긴급 4건, 중요 2건의 보안수준을 갖는다. 이달에 발표된 보안 업데이트에는 코드 실행이 가능한 다수의 취약점들과 서비스 거부 공격을 통해서 시스템 자체를 공격하는 취약점이 포함되어 있다.

위험등급	취약점	PoC
긴급	Kodak 이미지 뷰어의 취약점으로 인한 원격 코드 실행 문제점 (MS07-055)	유
긴급	Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(MS07-060)	무
긴급	Internet Explorer 누적 업데이트 (MS07-057)	무
중요	RPC의 취약점으로 인한 서비스 거부 문제점 (MS07-058)	유

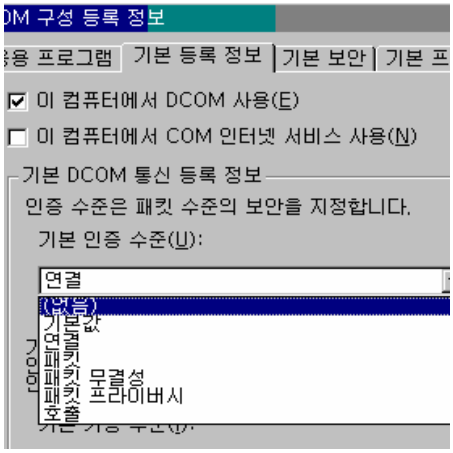
지속적으로 시스템 자체에 대한 취약점 보다는 애플리케이션 또는 애플리케이션에서 사용되는 파일을 통한 공격이 많이 보고되고 있다. 그러나, 이 중 시스템 자체를 공격하는 RPC의 취약점은 DoS(서비스 거부 공격)만 가능하지만, 해당 시스템의 재부팅을 유발할 수 있기 때문에 사용자들의 주의를 요한다. 언제나 그렇듯이 보안 업데이트는 사용자 시스템을 보호하는 가장 기초적이며 최선의 방어책이 되므로, 해당 취약점에 영향을 받는 사용자들은 즉시 업데이트를 적용하여야 한다.

이 달에 보고된 주요 취약점들(MS RPC 서비스 거부 취약점, MS URL 핸들링 취약점, GOM 플레이어 취약점 등) 및 보안 이슈(DDoS 공격)에 대해서 좀 더 살펴보도록 하자.

► MS RPC 서비스 거부 취약점(MS07-058)

애플리케이션을 대상으로 하는 많은 취약점들이 발표되고 있는 요즈음, 오랜만에 시스템 서비스를 공격하는 취약점이 발표되었다. 해당 취약점은 RPCSS 서비스가 NTLM 인증 메시지를 처리하는 과정에서 발생하는 Integer Underflow로서 서비스 거부 공격에 악용될 수 있다.

RPC 호출을 수행하려면 모든 분산 응용 프로그램의 클라이언트와 서버 간에는 바인딩(Binding)이 우선적으로 성립하고, 요청에 대한 인증을 수행한다. MS는 다음과 같이 여러 인증 수준을 제공하며, 클라이언트 인증을 위한 프로토콜로 NTLM(NT Lan Manager)을 지원한다.



*기본값(0x00: RPC_C_AUTHN_LEVEL_DEFAULT)

*없음(0x01: RPC_C_AUTHN_LEVEL_NONE)

*연결(0x02: RPC_C_AUTHN_LEVEL_CONNECT)

***호출 (0x03: RPC_C_AUTHN_LEVEL_CALL)**

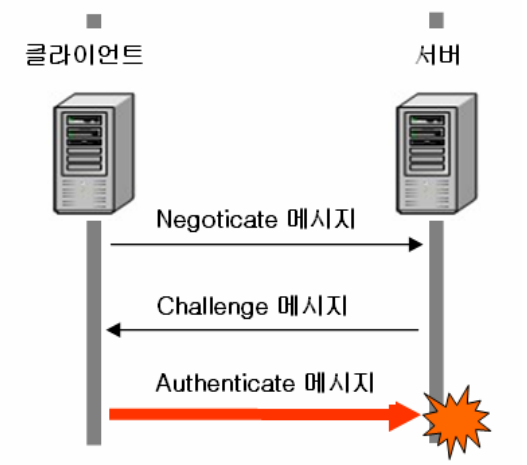
***패킷 (0x04: RPC_C_AUTHN_LEVEL_PKT)**

*패킷무결성(0x05:RPC_C_AUTHN_LEVEL_PKT_INTEGRITY)

*패킷프라이버시(0x06:RPC_C_AUTHN_LEVEL_PKT_PRIVACY)

[그림 2-8] DCOM 구성 등록 정보

NTLM을 사용한 인증절차는 서버와 클라이언트 사이에서 다음 3개의 메시지를 교환하는 Challenge-Response 구조를 갖는다. 해당 취약점은 서버의 RPCSS 서비스가 Authenticate 메시지를 처리하는 과정에서 발생한다.



[그림 2-9] NTLM 인증 메시지 교환

Authenticate 메시지는 인증을 원하는 클라이언트의 도메인명(DomainName), 사용자명(UserName) 등을 내부 구조체인 SECURITY_BUFFER 버퍼에 담아서 전달하게 된다.

```
SECURITY_BUFFER
  + short(Length): 바이트 단위의 버퍼 길이
  + short(Allocated Space): 바이트 단위의 할당된 버퍼 공간(length와 동일)
  + long(Offset) : 바이트 단위의 Offset 값. NTLM message의 처음으로부터의 거리
```

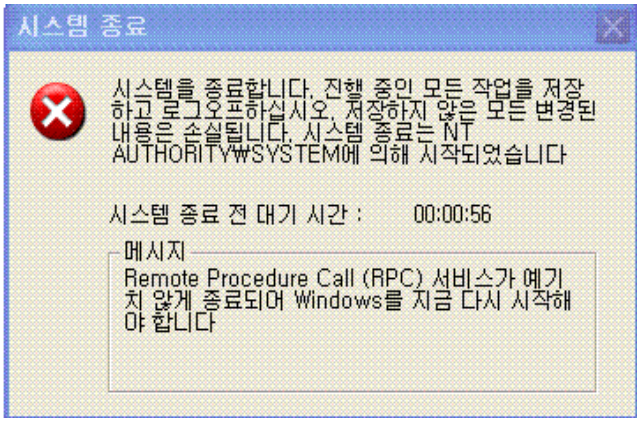
이 때, 보안 인증 레벨로서 “호출/패킷(AUTH LEVEL)“이 선택되고 사용자 길이(Length of UserName) 정보가 “ 0 “ 으로 설정된 NTLM Authenticate 메시지를 받는 경우,

RPCRT4!OSF_SCONNECTION::SendFragment 함수 내에서 두 번의 Integer Underflow가 발생하고 잘못된 메모리 번지를 덮어쓰는 오류가 발생하게 된다.

```
.text:77D9DCFF                  mov     eax, [ebp+14h]
.text:77D9DD02                  add     eax, 0FFFFFFF8h
.text:77D9DD83                  movzx   ecx, word ptr [esi+0Ah]
.text:77D9DD87                  mov     edx, [ebp-38h]
.text:77D9DD8A                  sub     ecx, edx
.text:77DBB275                  shr     ecx, 2
.text:77DBB278                  xor     eax, eax
.text:77DBB27A                  repe stosd
```

[그림 2-10] Integer underflow 발생

공격 NTLM RPC 메시지를 받은 대상(target) 시스템은 다음과 같이 RPCSS 서비스가 크래쉬(Crash) 되면서 시스템을 재부팅한다.



[그림 2-11] RPCSS 서비스가 크래쉬(Crash)

해당 취약점 공격은 별도의 사용자 인증을 필요로 하지 않기 때문에 조작된 공격 패킷을 전달하는 것만으로 쉽게 시스템 서비스 거부 공격을 성공할 수 있다.

► GOM 플레이어 원격 코드 실행 취약점

GOM 플레이어는 국내에서 가장 대중적으로 애용되고 있는 멀티미디어 플레이어이다. 이번 GOM 플레이어에서 발견된 취약점은 GOM 웹 컨트롤러(GomWeb3.dll)의 OpenURL() 메쏘드의 첫번째 인자인 sURL에서 버퍼의 크키를 체크 하지 않아서, 발생하는 스택 기반의 버퍼 오버플로우이다. 해당 취약점은 웹을 통해서 악용될 수 있으며 인터넷 익스플로러가 크래쉬(Crash) 되거나 공격자가 원하는 코드를 실행할 수 있다.

해당 ActiveX 컨트롤러의 정보는 다음과 같다.

GomManager Class

InprocServer32 : C:₩Program Files₩GRETECH₩GomPlayer₩GomWeb3.dll

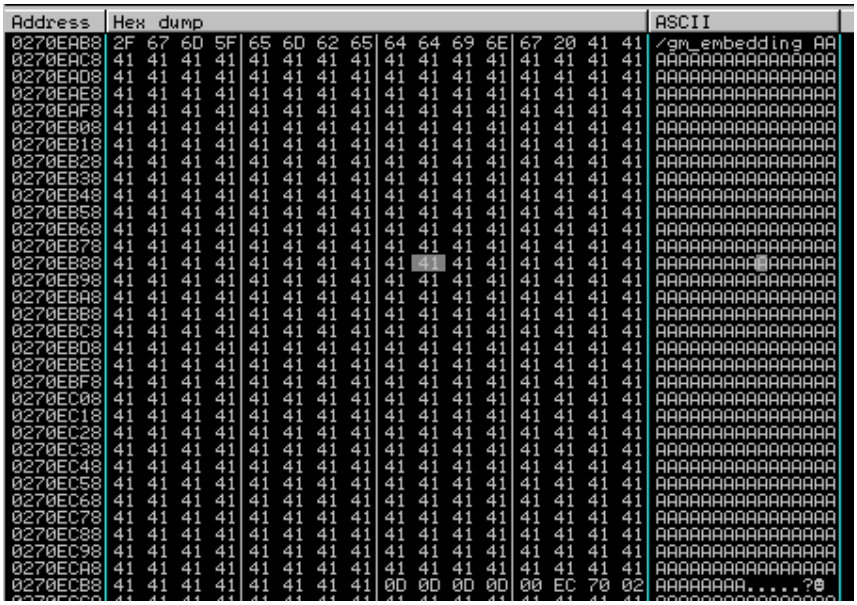
ProgID : GomWebCtrl.GomManager.1

CLSID : {DC07C721-79E0-4BD4-A89F-C90871946A31}

OpenURL() 메쏘드가 호출되면 메쏘드에 넘겨진 URL 문자열은 **"/gm_embedding "** 문자열과 재조합된다. 이를 처리하기 위해서 함수 내에서 아래와 같이 로컬 스택에 0x208(520) 바이트 공간을 확보한다. 차례로 확보된 로컬 스택에 kernel32.lstrcatA 함수를 호출하여 "gm_embedding "과 전달된 URL을 복사하게 된다.

[그림 2-12] 곰플레이어 취약점 발생

그러나, 이때 사용자 입력으로 전달된 URL의 길이가 "gm_embedding "(14)문자열을 제외하고 506 바이트 이상인 경우, 함수 내에서는 길이에 대한 유효성 검사를 전혀 수행하지 않기 때문에 본래의 로컬 스택 공간(520)을 초과하여 덮어쓰는 버퍼 오버플로우가 발생한다.



[그림 2-13] 곰플레이어 취약점의 오버플로우 발생 상태

이 과정에서 본래의 함수 RET 번지(Return Address)가 Overwrite되며, 만약 공격자가 원하는 코드 번지로 점프하도록 적절하게 제 RET 번지를 조작한다면 다음의 리턴 코드를 수행하는 과정에서 공격자의 코드가 실행된다.

[그림 2-14] 곰플레이어 취약점의 RET 번지의 조작

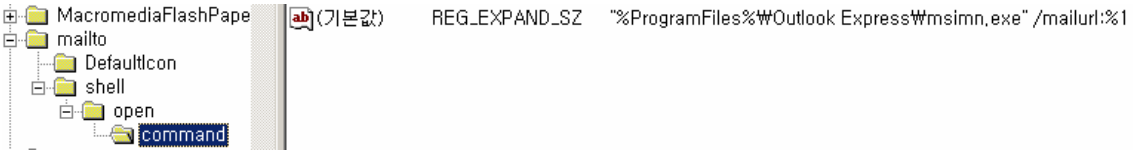
GOM 플레이어는 이미 코드 실행이 가능한 공격코드가 공개되었으며, 국내에 많은 사용자들이 존재하기 때문에 공격 확산의 가능성이 매우 높다. 따라서, 제품 업데이트 기능을 통해서 벤더가 제공하는 가장 최신 버전(2.1.8.3680)으로 반드시 업그레이드하여 사용하도록 한다.

[그림 2-15] 취약점이 해소된 곰플레이어 등록 정보

► MS URL 핸들링 취약점

지난 10월 초 마이크로소프트사는 Windows Server 2003과 Windows XP 상의 인터넷 익스플로러 7 버전에 대한 보안 권고문(Security Advisory 943521)[1]을 발표하였다. 해당 권고문은 다수의 사람들에게는 "PDF 제로데이 취약점"으로 더 많이 알려진 URL 핸들링 코드 실행 취약점에 대한 권고사항을 담고 있다.

Windows Shell은 "http","ftp", "mailto" 와 같은 URL 프로토콜 핸들러(Handler)를 사전에 등록하고, 사용자가 링크를 클릭할 때 해당 애플리케이션을 통해 자동으로 수행되도록 지원한다.



그러나, % 문자를 포함하는 URI의 경우 등록된 애플리케이션을 실행하지 않고, URI를 경로로 삼아 새로운 프로세스를 실행한다. 따라서, 다음과 같이 임의의 명령을 포함하는 URI를 웹 페이지에 삽입한다면, 이를 클릭하는 사용자들은 시스템에서 자연스럽게 계산기 프로그램을 수행하게 된다.

```
mailto:test%../../../../windows/system32/calc.exe".cmd
```

해당 취약점은 Adobe Acrobat Reader(PDF) 뿐만 아니라 Firefox, Outlook Express와 같이 스크립트를 수행할 수 있는 많은 다른 애플리케이션을 통해서도 이용될 수 있으며, 이미 공격에 응용된 PDF 파일 형태의 다운로더 악성코드가 신고 접수되었다. 좀 더 상세한 내용은 컬럼을 통해서 알아보자.

► DDoS 공격을 통한 서비스 거부 공격

"OO시까지 OO원을 입금하라. 그렇지 않으면..." 마치 영화 속 유괴범의 금품 요구 대사 같지만 이제 이러한 돈을 목적으로 하는 범죄는 비단 현실만의 얘기가 아닌 온라인 상에서도 자행되고 있다. 9월 말 아이템 베이, 아이템 매니아, 아이템 플포와 같은 온라인 게임 아이템 거래 사이트가 동시에 접속 불능이 되는 사태가 일어났다. 해당사들은 접속 과다로 인한 통신장애라고 사유를 급히 밝혔지만, 실상 그 뒤에 돈을 요구하는 UDP Flooding DDoS 공격으로 인한 장애였던 것으로 밝혀졌다.

[1] http://www.microsoft.com/technet/security/advisory/943521.mspx

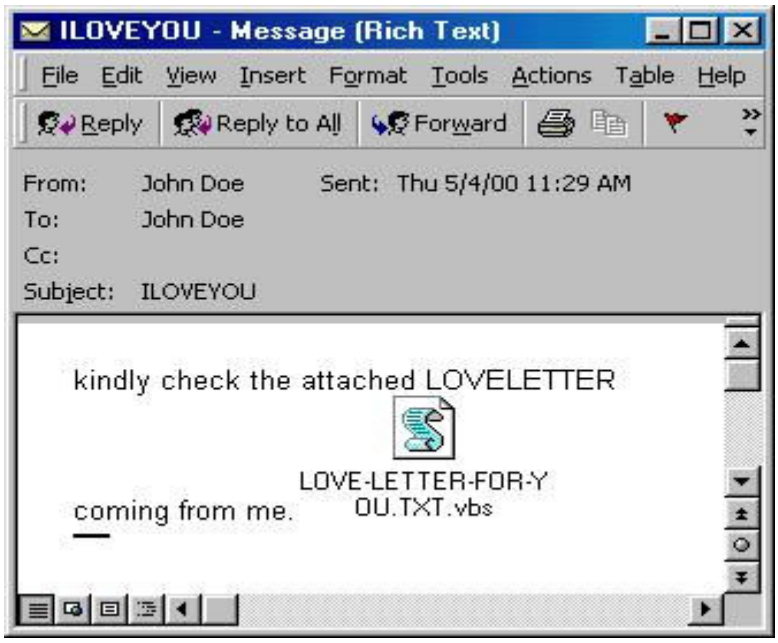
UDP Flooding은 다양한 DoS(Denial of Service) 공격의 일종으로 대량의 UDP 패킷을 이용하여 대상 호스트의 네트워크 자원을 소모함으로써 정상적인 서비스를 중단시키는 공격을 말한다. DDoS 공격은 일부 취약한 호스트를 해킹하여 '좀비' 시스템으로 만들고, 이를 통해서 대량의 트래픽을 발생시킨다. 이번 공격에서도 최대 17G 정도의 엄청난 양의 트래픽이 발생되었고, 일반적인 장비로는 이를 막아낸다는 것이 불가능하다. 이번 사건뿐만 아니라 DDoS 공격은 성인, 도박, 화상 채팅 사이트 등 음성적인 서비스를 제공하는 업체를 대상으로 빈번하게 자행되고 있으나, 신고를 통해 사건을 조치하기 보다는 원하는 요구를 그대로 들어주고 있는 실정이다. 현재 DDoS 공격 패킷은 정상적인 트래픽 패킷과 구별하는 것이 쉽지 않지만 대응책으로는 Source Tracking, Packer Per Rate 설정, Syn Cookie/Proxy, Load Balancing, QoS 등의 방법을 이용하여, 어느정도 방어가 가능하다. 그러나, 이러한 경우에도, 트래픽이 엄청날 경우 해당 ISP 와 더불어서 조치를 취하는 것이 효과적인 방법이다. 따라서, 이미 발생한 공격을 막는 것도 중요하지만 자신의 시스템이 DDoS 공격을 위한 '좀비' 시스템으로 이용되지 않도록 각별히 주의를 기울여야 할 것이다.

III. ASEC 컬럼

(1) 추억의 악성코드 - 러브레터

러브레터(Love Letter)

연애편지는 생각만해도 설레는 단어이다. 그런데, 이 달콤한 말이 악성코드 역사에도 한 획을 그었다. 한국시간으로 2000년 5월 4일 오후부터 'I love you'라는 제목의 메일이 메일함에 쌓이기 시작했다. 많은 사용자들은 '당신을 사랑합니다'에 호기심을 느끼고 메일을 열어보고 첨부된 LOVE-LETTER-FOR-YOU.TXT.vbs 파일을 별생각 없이 클릭했다.



[그림 3-1] 러브레터 바이러스 메일 (출처: http://www.f-secure.com/v-descs/love.shtml)

첨부 파일의 정체는 러브레터 바이러스(VBS/Love_Letter virus, 일명 러브, 러브버그)[1]로 필리핀의 오넬 드 구즈만(Onel de Guzman)에 의해 제작되었으며 메일을 통해 삽시간에 전 세계로 퍼졌고 다양한 변종이 양산되었다. 러브레터의 성공적 확산에 이후 VB 스크립트로 작성된 수많은 유사 웜이 발견되었다.

[1] http://kr.ahnlab.com/info/smart2u/virus_detail_708.html

[그림 3-2] 러브레터 바이러스를 제작한 오넬 드 구즈만

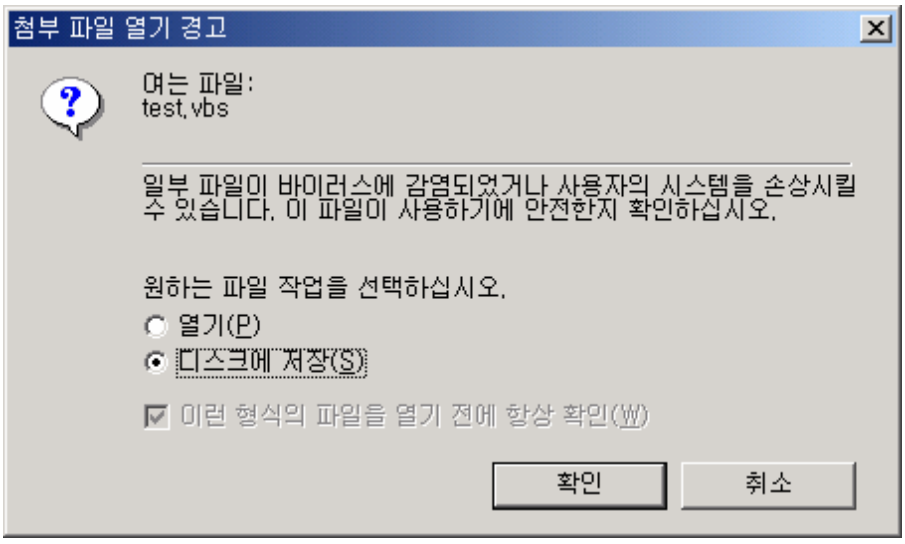
러브레터 바이러스의 교훈은 크게 다음과 같다.

- 첫째, 사용자에 대한 교육 필요: 1999년부터 본격적으로 메일로 전파되는 악성코드가 유행하면서 사용자에게 플로피 디스크나 인터넷에서 다운로드 받는 파일 뿐 아니라 메일에 첨부된 실행 파일도 주의해야 함이 강조되었지만 악성코드가 등장한지 20여 년이 지났어도 컴퓨터 사용에 익숙하지 않거나 보안에 관심 없는 사용자에게는 어려운 일이다.
- 둘째, 메일 서버 제품의 필요성: 컴퓨터를 잘 모르고 보안에 관심 없는 사용자가 많으므로 사용자 교육에는 한계가 있다. 메일로 퍼지는 악성코드는 메일 서버를 통해 전달되므로 메일 서버에 보안 프로그램이 설치되어 있으면 내부 사용자뿐 아니라 외부로 악성코드가 퍼지는걸 예방할 수 있어 메일 서버용 제품의 중요성이 강조되었다.
- 셋째, 업체간 협력 체계 강화: 2000년 4월 메일로 전파되는 악성코드가 증가하면서 안티 바이러스 업체간 샘플 공유 목적으로 와일드리스트(WildList Organization)는 영국 소포스(Sophos)사 지원으로 REVS(Rapid Exchange of Virus Samples) 시스템이 구축되었는데 러브레터 바이러스는 업체간 협력의 필요성을 더욱 느끼게 했으며 이후 미국 맥아피(McAfee)사 주도의 AVED(AntiVirus Emergency Discussion Network, http://www.aved.net/)가 만들어지면서 긴급 샘플의 공유와 정보 교류가 이뤄진다. 이들 시스템을 통해 긴급을 요하는 샘플에 대한 업체간 협력이 있었지만 2005년 이후 악성코드의 급격한 증가, 악성샘플 활동의 단기화 및 지역화로 성격이 바뀌고 유명 안티 바이러스 업체끼리 긴급 샘플 공유 체계가 강화되면서 AVED 활동은 많이 축소되었다.
- 넷째, 서비스로의 안티 바이러스 업계: 1999년 3월 발생한 멜리사 바이러스(W97M/Melissa virus)로 안티 바이러스 시장은 제품 중심에서 서비스의 중요성이 서서히 대두되었다. 하지만, 러브레터가 발생할 때 한국시간은 2000년 5월 4일 늦은 오후였고 같은 시간 유럽과 대부분의 미국 업무 시간이 종료되었을 때였다. 미국 시간으로 밤 사이 사용자들의 메일 함에는 이미 러브레터 웜이 쌓여있었고 아침에

컴퓨터를 켜고 메일을 확인하면서 감염되기 시작했다. 감염된 사용자와 언론을 통해 알게 된 많은 사용자들이 안티 바이러스 업체의 홈페이지 접속과 전화 문의가 집중되면서 홈페이지 접속에 원활하기 않았고 전화 통화도 불통되었다. 게다가 많은 사용자들의 시그니처 업데이트 시도로 평소보다 업데이트 시간도 오래 걸렸으며 이마저도 아직 러브레터 바이러스를 진단하지 못하는 경우도 있었다. 빠른 악성코드 진단/치료와 정보 제공뿐 아니라 사용자 부하에도 이겨내야 하는 안티 바이러스 업계는 서비스 면에서 완패였고 서비스 강화 방안을 마련하게 되었다.

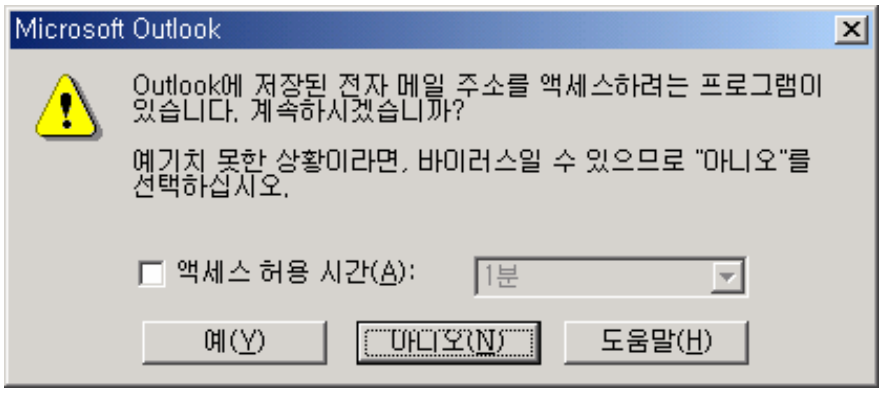
- 다섯째, 보안을 생각한 프로그램 설계: 멜리사 바이러스(W97M/Melissa virus), 러브레터 바이러스가 유행하면서 사람들은 보안을 생각하지 않고 제품을 만든 마이크로소프트사에 비난의 화살을 돌렸다. 이에 마이크로소프트사는 아웃룩에 실행파일과 스크립트 파일을 첨부시키지 못하고 스크립트로 아웃룩을 통한 메일 발송을 제한하는 오피스 보안 패치를 배포했다.[1]

공개된 보안 패치는 아웃룩으로 도착한 메일에 첨부된 파일의 확장자가 실행 파일(EXE, VBS 등)인 경우, 외부프로그램에서 아웃룩 주소록 검색, 아웃룩을 통한 메일 발송 할 때 등의 수상한 상황에 사용자에게 경고 창을 띄우게 했다.

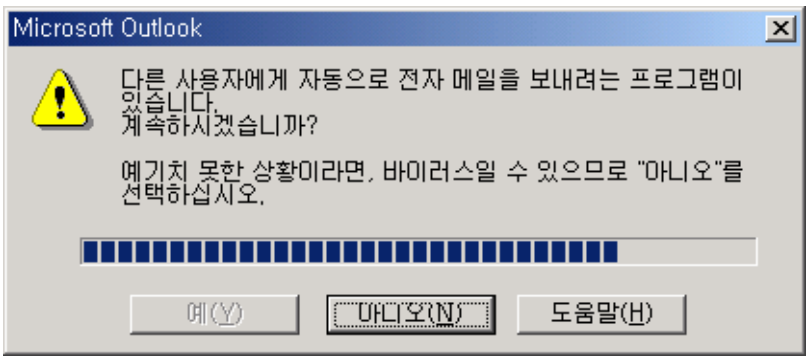


[그림 3-3] VBS 파일을 열었을 때 발생하는 경고

[1] http://office.microsoft.com/ko-kr/outlook/HA010550011042.aspx



[그림 3-4] 아웃룩 주소록 접근하는 경우 발생하는 경고



[그림 3-5] 아웃룩으로 메일 발송을 시도할 경우 발생하는 경고

2001년 중반 이후 VBS 등의 확장자는 아웃룩으로 메일 발송을 제한하는 새로운 오피스 제품의 보급으로 VB 스크립트를 이용한 웜이나 바이러스는 감소하고 대신 초기에 써캠 웜(Win32/Sircam.worm), 님다 웜(Win32/Nimda.worm)와 같은 윈도우 실행 파일 웜이 다시 증가하게 되었다.

러브레터 바이러스는 안티 바이러스 업계에는 제품에서 서비스로의 변화와 마이크로소프트사에는 보안에 대한 생각을 다시 하게 하였다. 2000년 5월 러브레터 바이러스가 발생한지 7년이 훌쩍 지났지만 악성코드는 여전히 우리는 괴롭히고 있다. 악성코드를 실행하기 위해 아이러브유로 유혹하는 메일이 아니라 보안 패치에 조금이라고 소홀하면 인터넷에 연결해서 컴퓨터를 켜두는 것 만으로 인터넷 웹 서핑을 하는 것만으로 감염되는 시대가 온 것이다.

(2) MS07-055 Kodak 이미지 뷰어 원격코드 실행 취약점

► 취약점 개요

마이크로소프트 10월 보안 패치에서 어플리케이션 취약점 중에 MS07-055 Kodak 이미지 뷰어에 대한 보안 패치가 있었다. 코닥 이미지 뷰어에서 이용하는 oieng400.dll에서 특수하게 조작된 TIF/TIFF 이미지를 처리하는 방식에 Memory Corruption이 발생하여, 원격 코드 실행 취약점이 존재한다. Kodak 이미지 뷰어는 Windows 2000에서는 기본 뷰어로 설정되어 있고, Explorer 에서 TIF/TIFF 파일을 열게 되면 Kodak 이미지 뷰어가 실행된다. 그러나, 3rd Party 이미지 관련 프로그램을 설치하였을 경우에는 Kodak 이미지 뷰어가 자동으로 실행되지는 않는다.

MS07-055 Kodak 이미지 뷰어 취약점을 이용한 공격자는Internet Explorer를 통해 이 취약점을 악용하도록 조작된 웹 사이트를 호스팅한 다음 사용자가 이 웹 사이트를 보도록 유도하거나, 메일 또는 메신저를 이용하여 해당 파일을 전송하는 방식으로 공격을 시도 할 수 있다. 단 두 경우 모두 사용자의 개입이 필요하다.

영향을 받는 OS 플랫폼은 아래와 같다.

- Microsoft Windows 2000 서비스 팩 4
- Windows XP 서비스 팩 2
- Windows Server 2003 서비스 팩 1 및 Window Server 2003 서비스팩2

이중에서, 문제가 되는 것은 Windows 2000이지만, Windows 2000 에서 XP 또는 2003 서버로 업그레이드 한 경우에도 문제가 발생할 수 있다.

► TIF/TIFF 파일

Tagged Image File Format(TIFF)은 이미지 저장을 위해서 사용되는 포맷으로, 포토그래프와 라인 아트를 포함한다. 현재는 해당 파일의 소유권은 Adobe 에서 가지고 있다.

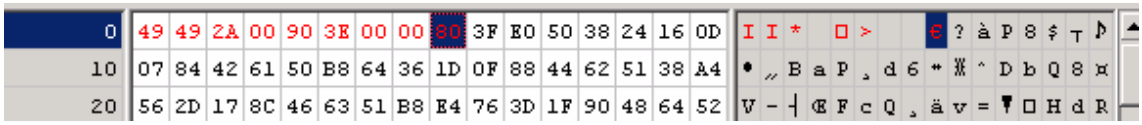
TIFF는 스캐닝 이미지를 포함하여 응용프로그램 간에 래스터 이미지를 주고받는 보편적인 형식이다. TIFF 파일은 대개 파일이름 확장자에 ".tiff" 또는 ".tif"가 붙어있으므로, 쉽게 구분할 수 있다. TIFF 형식은 1986년에 Aldus Corporation(지금은 '어도비 소프트웨어'로 이름이 바뀌었다)이 의장을 맡고 있는 산업계의 한 위원회에 의해 개발되었다. 마이크로소프트나 휴렛패커드도 이 형식을 개발하는데 공헌한 회사들이다. 가장 보편적인 그래픽 이미지 형식 중의 하나로서, TIFF 파일은 탁상출판, 팩스, 3차원 응용프로그램 및 의료 이미지 업무 등에 널리 사용된다.(terms.co.kr)

TIFF 파일들은 그레이스케일, 컬러 팔레트 또는 RGB 컬러 등의 몇 가지 등급으로 나뉘며, JPEG이나 LZW 또는 CCITT 그룹4 표준 등의 압축파일들을 포함할 수 있다.

► TIF/TIFF 파일 포맷의 이해

TIFF 파일의 최대 크기값은 2^32 bytes 만큼 가질 수 있는데, 먼저 헤더는 아래와 같다.

헤더 8bytes

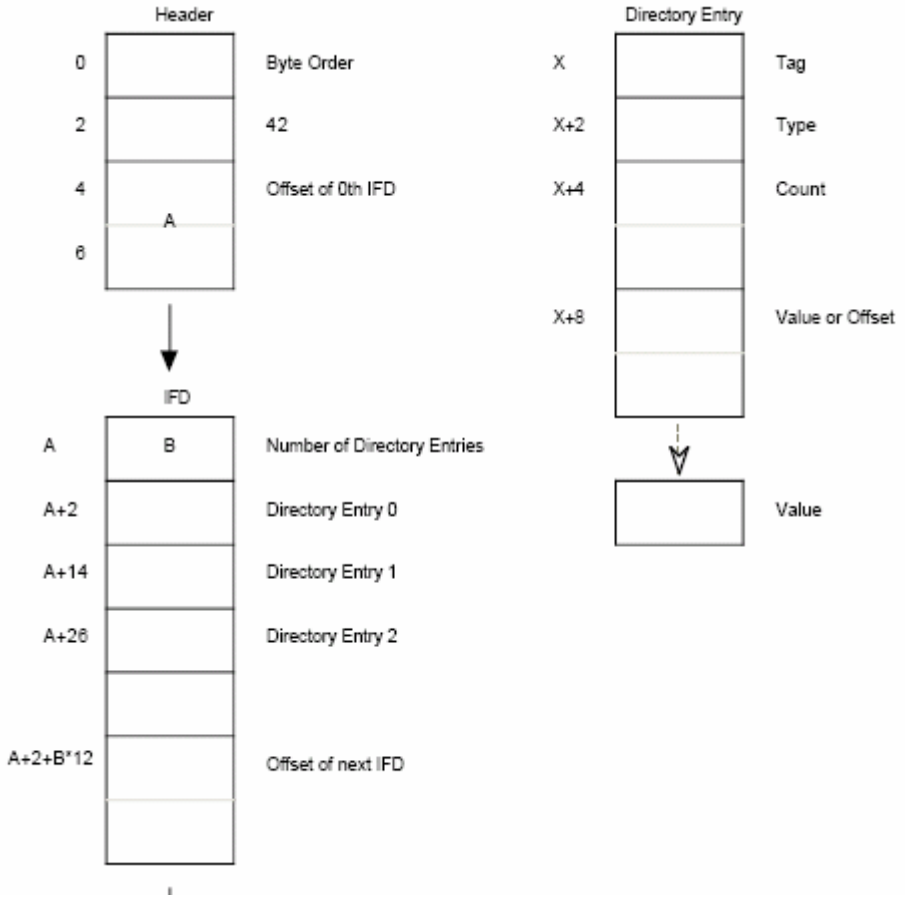


0-1(시그너쳐 바이트): II (4949H) little Endian

MM(4D4DH) Big Endian

2-3 추가적인 TIFF Identify 인식 시그너쳐 바이트에 의존(2A)

4-7 처음 Image File Directory(IFD)의 오프셋



[그림 3-6] TIFF 기본 구조

► Image File Directory(IFD) 의 이해

IFD 는 TIFF 파일 내부의 이미지의 정보를 가지고 있는 데이터 구조이다. TIFF 파일내부에 이미지의 수만큼 IFD 를 가질 수 있으며, IFD 는 2byte(16bit)의 디렉토리 엔트리의 수와 연관되어 있다. TIFF 파일에는 최소한 한 개의 IFD가 포함되어야 하며, 각각의 IFD는 최소한 한 개의 Entry를 가지고 있어야 한다.

IFD Entry

12bytes 로 구성되어져 있다.

0-1 : Tag identifies 필드

2-3 : 필드 타입

4-7: 해당 타입의 데이터 카운트

8-11: Value Offset

예) Compression Tag 의 IFD Entry

Tag identifies: 0103

File Type: 0003 (SHORT)

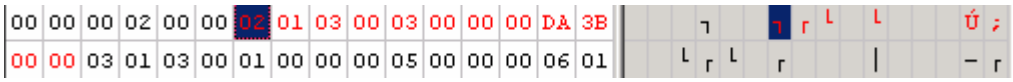
Data Count: 00000001

Value Offset: 00000005

일반적으로 IFD Entry들은 아래와 같은 것들이 존재한다.

0x0100	ImageWidth	3 =SHORT
0x0101	ImageLength	3 =SHORT
0x0102	BitsPerSample	3 =SHORT
0x0103	Compression	3 =SHORT
0x0106	PhotometricInterpretation	3 =SHORT
0x0111	StripOffsets	4 =LONG
0x0115	SamplesPerPixel	3 =SHORT
0x0116	RowsPerStrip	3 =SHORT
0x0117	StripByteCounts	4 =LONG
0x011a	XResolution	5 =RATIONAL
0x011b	YResolution	5 =RATIONAL
0x0128	ResolutionUnit	3 =SHORT

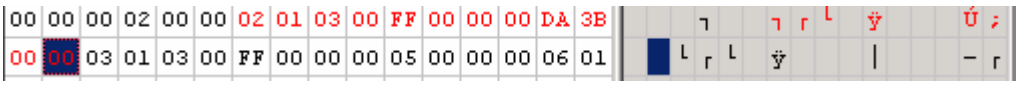
MS07-055 Kodak Image Viewer 에서 문제가 되는 것은 IFD Entry의 태그중에 0x0102 BitsPerSample이다. 아래는 정상적인 TIFF 파일의 BitsPerSample 태그이다.



BitsPerSample Tag는 컴포넌트의 해당 비트수를 나타내는 태그이며, BitsPerSample Tag의 구조는 아래와 같다.

IFD	Image
Code	258 (hex 0x0102)
Name	BitsPerSample
Type	SHORT
Count	N = SamplesPerPixel
Default	1

MS07-055 Kodak Image Viewer 원격 코드 실행 취약점에서 문제가 되는 것은 TIFF 파일의 BitsPerSample Tag의 데이터 카운트 값(4-7bytes)이다.



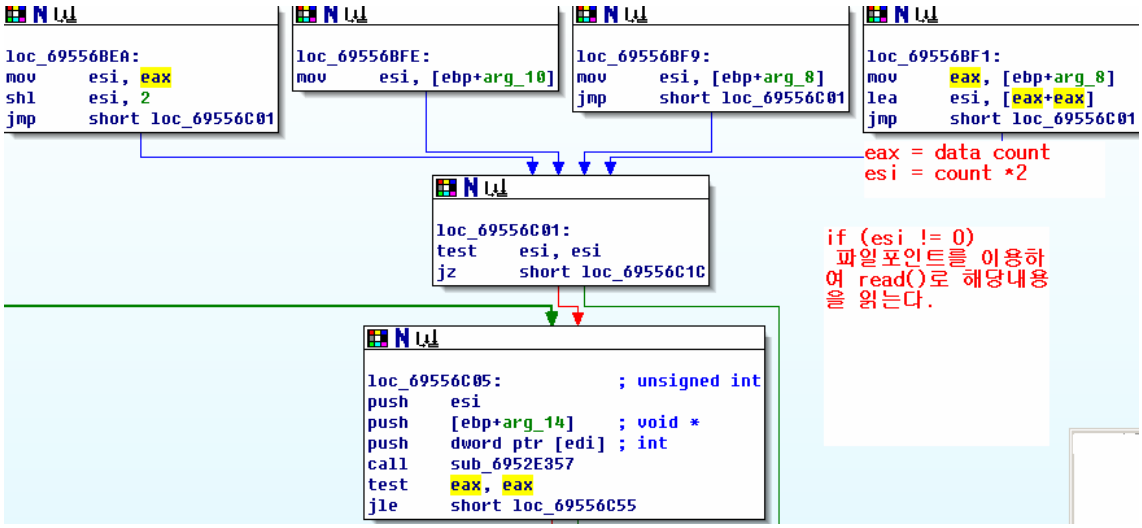
[그림 3-7] BitsPerSample Tag의 데이터 카운트 값이 FF로 조작된 그림

Kodak Image Viewer 에서 조작된 TIFF 파일이 로딩되면 아래와 같은 Exception 이 발생하게 된다.

```
(3ec.2a8): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00ae0000 ebx=00003bda ecx=00000000 edx=002c1f90 esi=69569b8c edi=69569ae8
eip=695530fc esp=000ae2b0 ebp=000ae2f0 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00010246
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:
OIENG400!OiOpAbortOperation+0x92c:
695530fc 394808          cmp     dword ptr [eax+8],ecx ds:0023:00ae0008=??????
0:000> ~kb
ChildEBP RetAddr  Args to Child
WARNING: Stack unwind information not available. Following frames may be wrong
000ae2f0 011b0000 00e80000 00ae0000 00ae0000 OIENG400!OiOpAbortOperation+0x92c
000ae2f4 00e80000 00ae0000 00ae0000 00ae0000 0x11b0000
000ae2f8 00ae0000 00ae0000 00ae0000 00b90000 0xe80000
000ae2fc 00ae0000 00ae0000 00b90000 00ba0000 0xae0000
000ae3fc 69559ea6 00000000 00000005 000e50b0 0xae0000
000ae648 69559a94 000d8960 00000001 000f05d8 OIENG400!wgfsopen+0x230
000ae674 695207c4 0001016e 00000001 00000001 OIENG400!wgfsgeti+0x56
000ae6dc 69521069 00000000 0001016e 000af260 OIENG400!IMGFileDeletePagesND+0xc
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:
000ae6fc 646bbbbd 00000000 0001016e 000af260 OIENG400!IMGFileGetInfo+0x2a
000af2b4 646b8202 000e04dc 002cc3d8 00000000 ImgAdmin!CPagePropSheet::`default
000af308 646bb0c6 070b0058 000af58c 0000000c ImgAdmin!CPagePropSheet::`default
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:
000af588 76fea629 00000000 00730084 76fe94fc ImgAdmin!CPagePropSheet::`default
000af614 76fe9b83 646b2b24 000af5a8 00000000 MFC42u!Ordinal6089+0x54
000af6a4 76fea2b8 00000001 00000071 7700cb28 MFC42u!Ordinal4024+0x3b3
000af740 76fea5b7 00000071 00000001 00000000 MFC42u!Ordinal4031+0x1b8
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:
000af760 0102abfc 002c7bb0 00000071 00000001 MFC42u!Ordinal4028+0x1e
000af7dc 010205f7 000af800 00001000 070c0460 kodakimg!CPagePropSheet::`default
000af814 76fad2b5 01005460 00000111 000af854 kodakimg!CPagePropSheet::`default
```

► **정적 분석**

oieng400.dll 에는 TIFF 파일의 내용을 읽는 부분이 존재하는데, 문제가 되는 코드는 아래의 코드이다. 기본적으로 IFD Entry 의 데이터 카운트는 eax 레지스터에 저장되면, 이것은 다시 esi 에 2배로 저장되어, _read() 으로 해당 파일에 내용을 버퍼크기만큼 읽게 된다. 이 과정에서 크키에 해당하는 length 길이값(esi = data count)을 체크하지 않아서, Memory Corruption이 발생하게 된다.



[그림 3-8] oieng400.dll에서 Memory Corruption 발생

_read() function

Int _read(int handle, void *buf, unsigned len);

Handle : 해당 파일 포인트

Buf : 읽을 데이터 버퍼

Len : 버퍼 크기

```
; int __stdcall sub_6952E357(int,void *,unsigned int)
sub_6952E357 proc near

arg_0= dword ptr  4
arg_4= dword ptr  8
arg_8= dword ptr  0Ch

push    [esp+arg_0]
call    sub_6952E021
push    [esp+arg_8]     ; unsigned int
push    [esp+4+arg_4]   ; void *
push    dword ptr [eax] ; int
call    ds:_read
add     esp, 0Ch
retn    0Ch
sub_6952E357 endp
```

이것을 가상코드로 생각해보면 다음과 같다.

```
…
Eax = IFD Entry data count
Esi = eax * 2
If (esi !=0)
_read([edi], [ebp+arg_14], esi)
```

► 동적 코드 분석

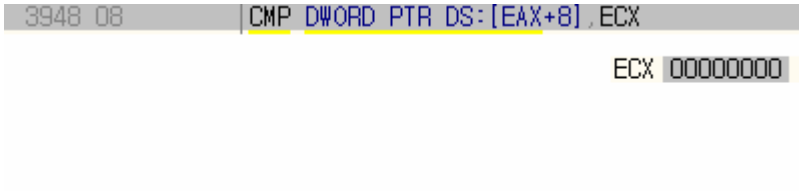
아래 그림을 보면, IFD Entry의 Data Count 필드부분이 EAX 에 저장되는 것을 알 수가 있다. 또한 해당 코드는 ESI에 두배의 값으로 저장된다. 또한 EAX 에 저장된 00000061 값은 조작되어 있는 것을 볼 수 있다.

```
8D3400      LEA ESI,DWORD PTR DS:[EAX+EAX]
EB 08       JMP SHORT 01ENG400.69556C01
8B75 10     MOV ESI,DWORD PTR SS:[EBP+10]
EB 03       JMP SHORT 01ENG400.69556C01
8B75 18     MOV ESI,DWORD PTR SS:[EBP+18]
85F6        TEST ESI,ESI
74 17       JE SHORT 01ENG400.69556C1C
56          PUSH ESI
FF75 1C     PUSH DWORD PTR SS:[EBP+1C]
FF37        PUSH DWORD PTR DS:[EDI]
E8 4777FDFF CALL 01ENG400.6952E357
```

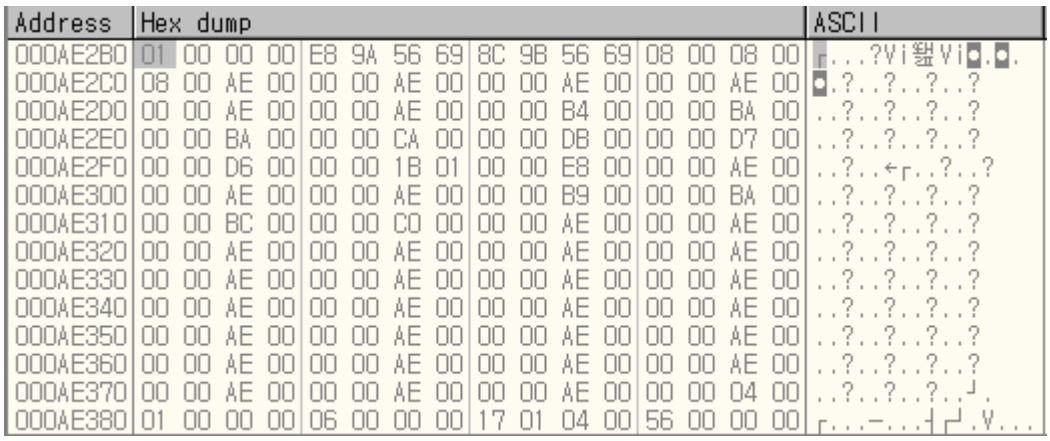
[그림 3-9] IFD Entry Data Count 계산

[그림 3-10] 비정상적인 EAX 값

조작된 EAX 값으로 인하여, ECX 값이 00000000 이 됨으로 Memory Corruption 이 발생하게 된다.



이 후 비정상적인 값들도 인하여, 스택의 상태는 아래와 같다.



► **결론**

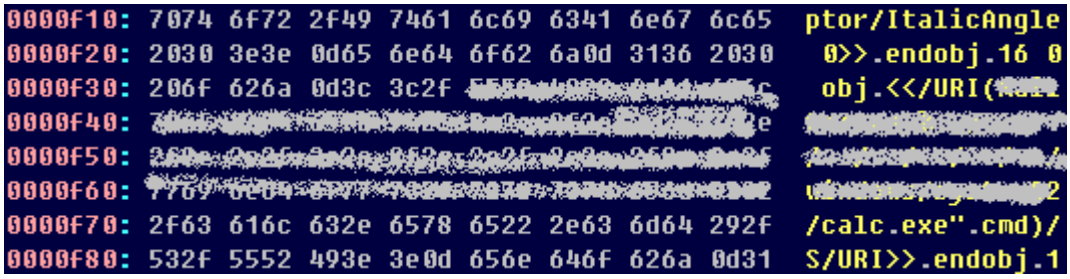
MS07-055 Kodak 이미지 뷰어 취약점은 조작된 TIF/TIFF 파일을 읽는 과정에서 문제가 생기는 것으로, 이러한 파일을 이용한 취약점은 오피스 취약점과 유사하다고 할 수 있다.

사용자는 출처가 불분명한 TIF/TIFF 파일을 다운로드하거나, 메일로 온 경우에는 열지 말아야 한다. 또한 이 취약점을 예방하기 위해서는 보안 패치가 필수이며, 더불어서 Anti-Virus 제품이나, 개인 방화벽 등을 이용할 수도 있다.

(3) 마이크로소프트 Internet Explorer 7 URL 핸들링 취약점

2007년 10월, 마이크로소프트 Internet Explorer 7의 URI 처리관련 메커니즘의 취약점을 이용한 PDF 파일이 공개되었다. PC 사용자가 해당 스크립트가 삽입된 PDF 파일을 Acrobat Reader를 사용하여 열면, 공격자가 삽입한 스크립트 코드가 실행되어 사용자의 권한으로 임의의 코드가 실행된다.

이 PDF 파일을 이용한 코드 실행은 Adobe사의 제품에만 가능하며 또 다른 PDF 관련 프로그램인 Foxit software사의 foxit reader에서는 불가능하다. 현재 Adobe사는 이 문제점을 해결한 패치를 발표한 상태이다. [그림 3-11]은 스크립트가 삽입된 PDF 파일의 바이너리 데이터를 나타낸 것이다. 해당 스크립트가 텍스트 형태로 삽입되어 있는 것을 관찰 할 수 있다.



[그림 3-11] 공격 코드가 삽입된 PDF 파일의 일부

► 취약점 개요

사용자가 Windows 운영체제의 탐색기(explorer)에서 그림 파일을 더블 클릭하면 그 그림파일을 보거나 편집할 수 있도록 해당 그림 파일 형식과 연결된 프로그램이 실행된다. 이것은 Windows 운영체제가 제공하는 기능으로, Windows운영체제는 파일 형식뿐 아니라 “mailto”와 같은 URI와 관련된 링크를 처리할 수 있는 URI 처리 기능을 제공한다. 예를 들어, “mailto:”같은 링크를 사용자가 더블 클릭하면 windows운영체제는 해당 링크를 사용하여 Internet Explorer를 실행하거나, 등록된 이메일 클라이언트를 실행한다. 이 때 해당 링크에 특수하게 조작된 문자가 삽입이 되면 windows 운영체제는 해당 링크와 관련된 연결 프로그램을 찾는데 실패하고 사용자가 선택한 링크를 사용하여 새로운 프로세스를 생성한다. 만약 링크가 사용자 PC내에 있는 프로그램의 위치를 나타낸다면 해당 프로그램이 실행된다.

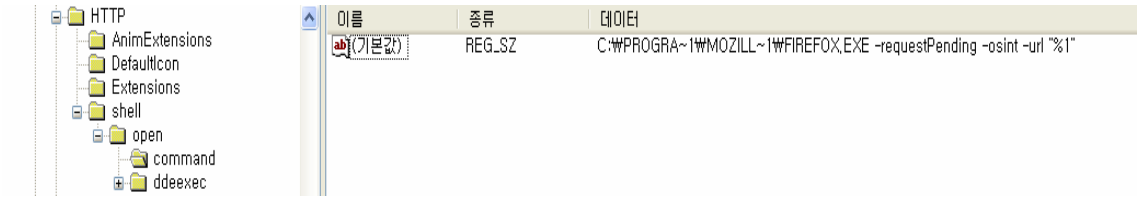
► 취약점 분석

해당 취약점은 Windows 운영체제의 ShellExcute 함수에 존재한다. ShellExcute 함수는 shell32.dll 파일이 제공하는 함수로 특정한 URI을 처리할 때, Windows 운영체제는 ShellExecute 함수를 호출하여 해당 URI를 처리한다 ShellExcute함수는 운영체제가 넘겨준

URI 문자열을 분석(parsing)하여 프로토콜과 확장자를 추출하여 처리한다. ShellExecute함수가 해당 URI를 처리하는 과정은 아래와 같다.

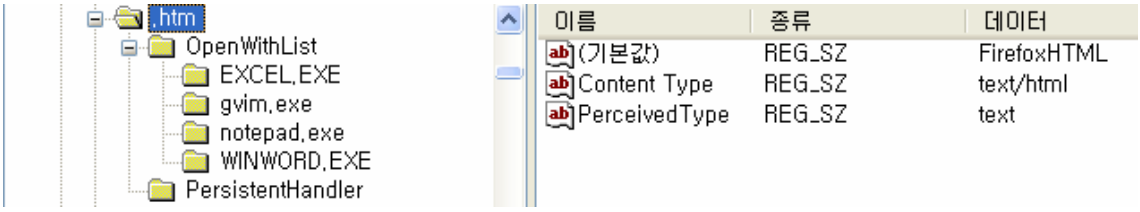
1. URI 문자열에서 프로토콜과 파일 확장자를 추출한다.
2. 추출한 프로토콜이나 확장자와 관련된 프로그램을 레지스트리에서 살펴 보고 추출한 프로그램이나 파일확장자와 관련된 프로그램을 실행한다.

만약 URI가 "http://www.ahnlab.com" 과 같은 문자열일 경우 ShellExecute함수는 해당 URI를 "http://" 와 "www.ahnlab.com" 문자열로 분해한다. 프로토콜이 "http://"이므로 ShellExecute 함수는 HKEY_CLASSES_ROOT₩http₩shell₩open"레지스트리를 조사한 후 연결 프로그램을 실행한다. [그림 3-12]는 어떤 PC의 레지스트리의 내용중 "http"와 관련된 내용을 표시한 것이다. "HKEY_CLASSES_ROOT₩http₩shell₩open" 에 연결 프로그램으로 firefox.exe가 등록되어 있으며 관련 firefox.exe의 위치 및 "%1"과 같은 인자도 표시되어 있다.

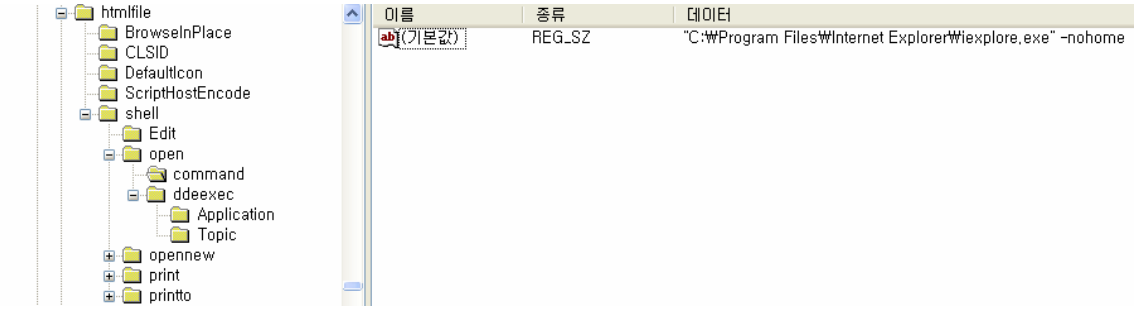


[그림 3-12] HKEY_CLASSES_ROOT₩http₩shell₩open 레지스트리

마찬가지로 URI 가 "abc.htm" 같은 문자열일 경우 ShellExecute 함수는 해당 URI 문자열을 "abc"와 ".htm"으로 분리 한 후, ".htm"을 파일의 확장자로 간주하여 레지스트리 HKEY_CLASSES_ROOT₩.htm의 내용을 살펴보고 해당 레지스트리의 내용을 참조하여 HKEY_CLASSES_ROOT₩htmlfile₩shell₩open 레지스트리에 기록된 연결 프로그램을 실행한다. [그림 3-134]와 [그림 3-14]는 각각 HKEY_CLASSES_ROOT₩.htm 레지스트리와 HKEY_CLASSES_ROOT₩htmlfile₩shell₩open를 나타낸 것이다.



[그림 3-13]. HKEY_CLASSES_ROOT₩.htm 레지스트리



[그림 3-14]. HKEY_CLASSES_ROOT₩htmlfile₩shell₩open 레지스트리

일반적으로, Windows 운영체제가 처리할 수 있는 URI의 프로토콜 종류는 “mailto”, ”news”, ”nntp”, ”snews”, ”telnet”, ”http”등이 있으며 “www”와 “ftp”같은 문자열도 HTTP 프로토콜과 FTP 프로토콜과 연결하여 처리한다.

앞서의 과정을 요약하면, 먼저 ShellExecute 함수는 URI 문자열을 프로토콜과 파일 확장자로 나눈 후 프로토콜이나 파일 확장자에 맞는 프로그램을 실행한다. ShellExecute 함수는 먼저 URI 문자열에서 해당 프로토콜 문자열이 존재하는지 확인한 후, 프로토콜에 해당하는 문자열이 존재하지 않으면 해당 URI 문자열을 파일이름으로 해석하여 파일 확장자와 관련된 프로그램을 실행한다.

따라서 만약 “%”등과 같은 문자가 삽입된 URI가 ShellExecute 함수로 넘겨질 경우 Shell Exucte 함수는 URI 문자열을 파일이름으로 해석하여 확장자와 관련된 프로그램을 실행한다. “blahblah%/calc.exe”.cmd”와 같은 조작된 URI를 ShellExecute함수가 처리하는 과정은 아래와 같다.

1. 조작된 URI 에서 프로토콜을 확인한다. URI 에는 “blahblah%” 와 같은 문자열이 포함되어 있으므로 ShellExecute 함수는 해당 URI 문자열에서 프로토콜 이름을 얻어내는데 실패한다.
2. ShellExecute 함수는 URI 문자열을 파일이름으로 간주하여 파일 확장자를 추출한다. URI 문자열의 끝에는 .cmd 가 존재하므로 ShellExecute 함수는 파일 확장자를 .cmd 로 간주한다.
3. HKEY_CLASSES_ROOT₩.cmd 레지스트리를 읽는다
4. CLASSES_ROOT₩cmdfile₩shell₩open₩command 레지스트리를 읽는다. 이 때 아규먼트 치환에 사용되는 문자열을 “%1” %* 이다. [그림 5]
5. “%1”을 URI 로 치환한다. 따라서 최종 아규먼트는 “blahblah%/calc.exe” .cmd” ; %*가 된다.
6. 치환된 문자열을 파라미터로 사용하여 CreateProcess 함수를 호출한다.
7. calc.exe(계산기 프로그램)이 실행된다.

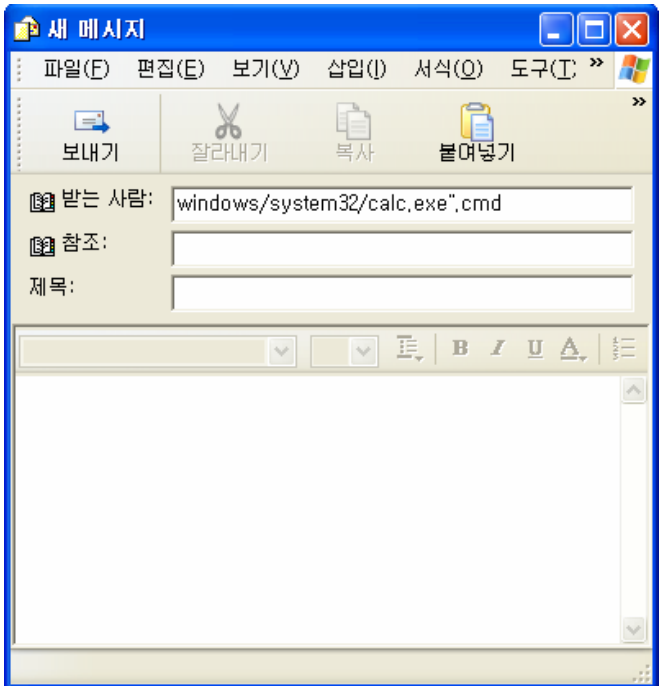
CreateProcess함수는 프로세스를 실행할 때 사용하는 함수로, 함수 원형은 아래와 같다.

```
BOOL WINAPI CreateProcess(
__in LPCTSTR lpApplicationName,
__in_out LPTSTR lpCommandLine,
__in LPSECURITY_ATTRIBUTES lpProcessAttributes,
__in LPSECURITY_ATTRIBUTES lpThreadAttributes,
__in BOOL bInheritHandles,
__in DWORD dwCreationFlags,
__in LPVOID lpEnvironment,
__in LPCTSTR lpCurrentDirectory,
__in LPSTARTUPINFO lpStartupInfo,
__out LPPROCESS_INFORMATION lpProcessInformation
);
```

위의 6번 과정에서 치환된 문자열은 CreateProcess 함수의 두 번째 인자인 lpCommandLine 에 대입되고 CreateProcess 함수는 “blahblah%/calc.exe”와 같은 문자열 중 “blahblah%”와 같은 무시하므로 남은 부분인 calc.exe가 실행된다.

해당 취약점은 새로운 URI 처리기를 사용하는Internet Explorer(IE) 7이 설치된 (http://blogs.msdn.com/ie/archive/2005/08/15/452006.aspx 참조) 시스템에서만 영향을 미치며, IE 6가 설치된 시스템에서는 “blahblah%”와 같은 문자열을 올바른 프로토콜로 해석하므로 영향을 주지 않는다.

[그림 3-15]는 공격 코드가 삽입된 PDF 파일을 IE 6가 설치된 시스템에서 열었을 때의 모습이다. IE 6가 설치된 시스템에서는 조작된 URI문자열의 프로토콜을 올바르게 해석하여 메일 클라이언트 프로그램인 아웃룩 익스프레스가 실행되어 공격코드가 올바르게 동작하지 않는다. 메일주소에 실행 타겟 프로그램인 계산기의 파일이름 calc.exe를 관찰할 수 있으며 그 결과 URI가 조작되었음을 추론할 수 있다.



[그림 3-15] IE 6가 설치된 시스템에서 공격코드가 실행된 모습

► **결론**

이번 취약점에 이용된 PDF 파일은 가장 널리 사용되고 있으며, 이 취약점을 이용한 악성코드 또한 존재함으로 주의가 필요하다. Acrobat 사의 제품을 사용하는 사용자는 해당 제품의 패치를 반드시 해야 하며 출처가 불분명한 PDF 파일은 다운로드하거나 열지 말아야 한다.

이 취약점은 PDF 파일 형식의 문제가 아니라 운영체제의 문제이므로, 글을 작성하는 시점에는 마이크로소프트의 패치가 나오지 않았으나, 패치가 발표되면, 반드시 적용해야 한다. 또한 공격코드가 실행되는 최악의 경우에 대비하기 위해서 Anti-Virus 제품을 반드시 설치 하도록 한다.