ASEC Report 3월

® ASEC Report

2007. 3

안철수연구소의 시큐리티대응센터(AhnLab Security Emergency response Center)는 악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스와 보안 전문가들로 구성되어 있는 조직이다.

이 리포트는 ㈜안철수연구소의 ASEC에서 국내 인터넷 보안과 고객에게 보다 다양한 정보를 제공하기 위하여 바이러스와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

I. ASEC Monthly 통계

(1) 3월 악성코드 통계

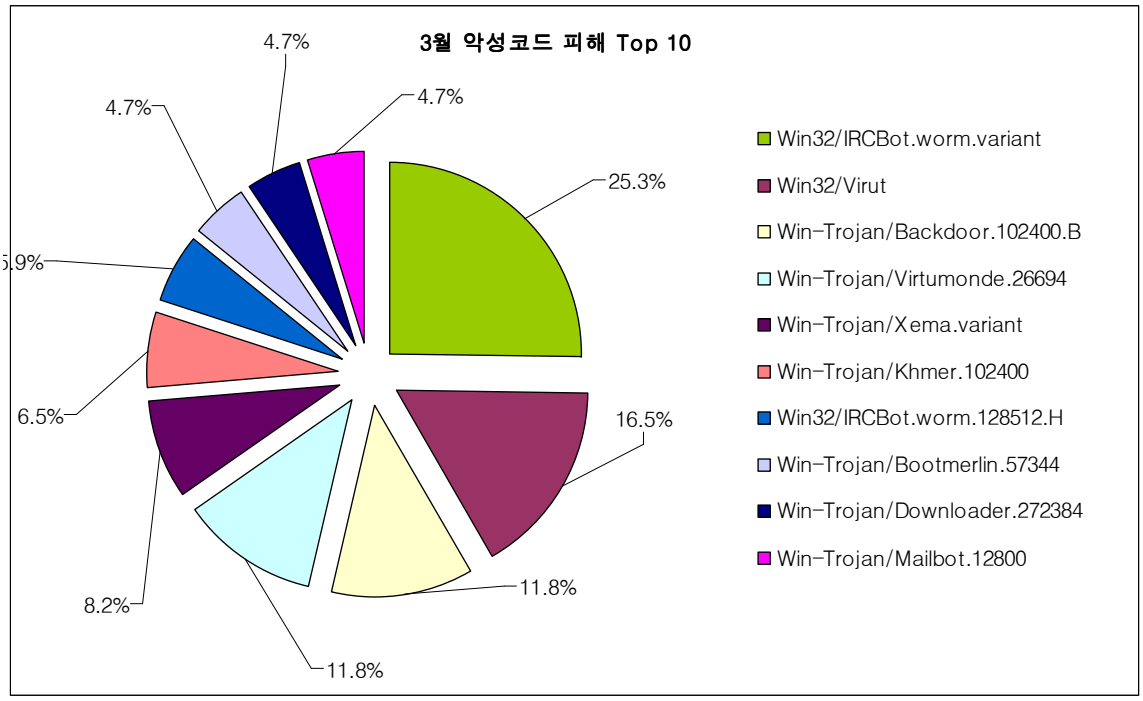
순위		악성코드명	건수	%
1	↑2	Win32/IRCBot.worm.variant	43	25.3%
2	↑1	Win32/Virut	28	16.5%
3	new	Win-Trojan/Backdoor.102400.B	20	11.8%
3	new	Win-Trojan/Virtumonde.26694	20	11.8%
5	↓3	Win-Trojan/Xema.variant	14	8.2%
6	new	Win-Trojan/Khmer.102400	11	6.5%
7	new	Win32/IRCBot.worm.128512.H	10	5.9%
8	new	Win-Trojan/Bootmerlin.57344	8	4.7%
8	new	Win-Trojan/Downloader.272384	8	4.7%
8	new	Win-Trojan/Mailbot.12800	8	4.7%
합계			170	100.0%

[표 1-1] 2007년 3월 악성코드 피해 Top 10

월 악성코드 피해 동향

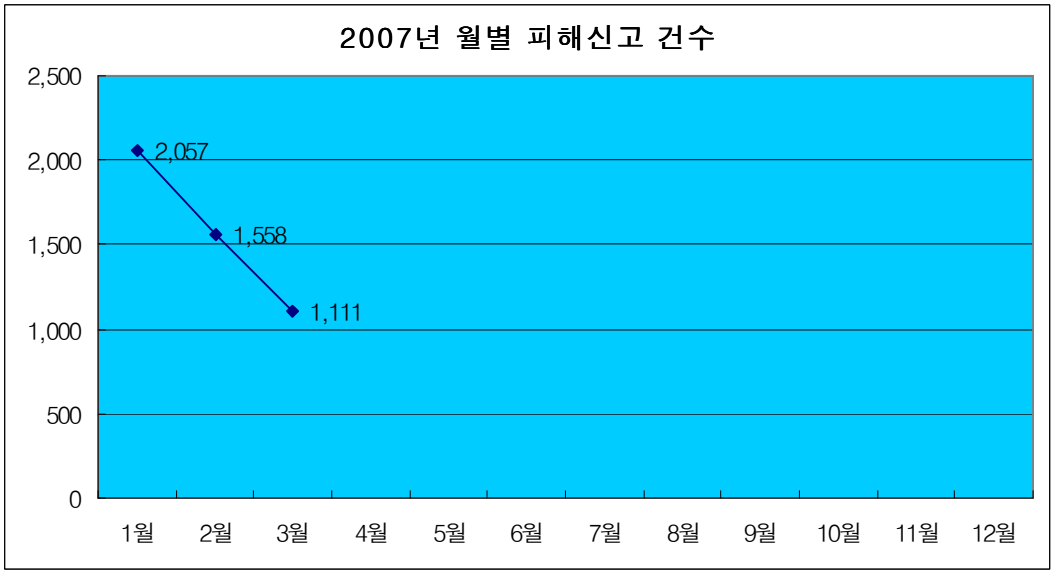
2007 년 3 월 악성코드 Top10 에는 전월에 3 위였던 아이알씨봇(Win32/IRCBot.worm.variant)이 1 위에 올랐으며, 전월의 1 위였던 바이럿(Win32/Virut)은 2 위로 순위가 한 계단 하락하였다. 1~2 월과 큰 차이 없이 트로이목마류가 Top10 중 7 종을 차지하고 있으며, 이를 통하여 악성코드의 대세가 트로이목마류임을 다시 한번 확인할 수 있다. 전월의 2 위였던 Win-Trojan/Xema.variant 가 3 계단 하락하여 5 위에 랭크되었으며, 다른 순위들은 새로운 트로이목마류가 Top10 에 진입하였다. 이는 중국에서 개발된 자동 트로이목마 제작 툴을 이용하여 트로이목마류의 악성코드가 지속적으로 제작/유포되고 있는 것이 원인으로 유추된다. 이러한 위협으로부터 대비할 수 있는 방법으로 사용자들은 주기적인 백신엔진 업데이트를 통하여 다양한 악성코드로부터 보호를 받아야 하며, 백신엔진 업데이트를 소홀히 할 경우 신종 트로이목마에 사용자 시스템이 언제든 무방비로 노출될 수 있음을 인지하여야 한다.

3월의 악성코드 피해 Top 10을 도표로 나타내면 [그림 1-1]과 같다.



[그림 1-1] 2007년 3월 악성코드 피해 Top 10

[그림 1-2]에서와 같이 1월부터 월별 피해신고 건수는 꾸준히 감소하고 있음을 알 수 있다. 이는 광범위하게 확산되는 웜(메스메일러, 봇)보다는 인터넷 사이트, 게시판으로 전파되는 트로이목마 위주로 확산됨으로써, 특정사이트만을 방문하는 사용자 위주로 전파됨으로써 피해 건수가 감수되는 것으로 보인다.

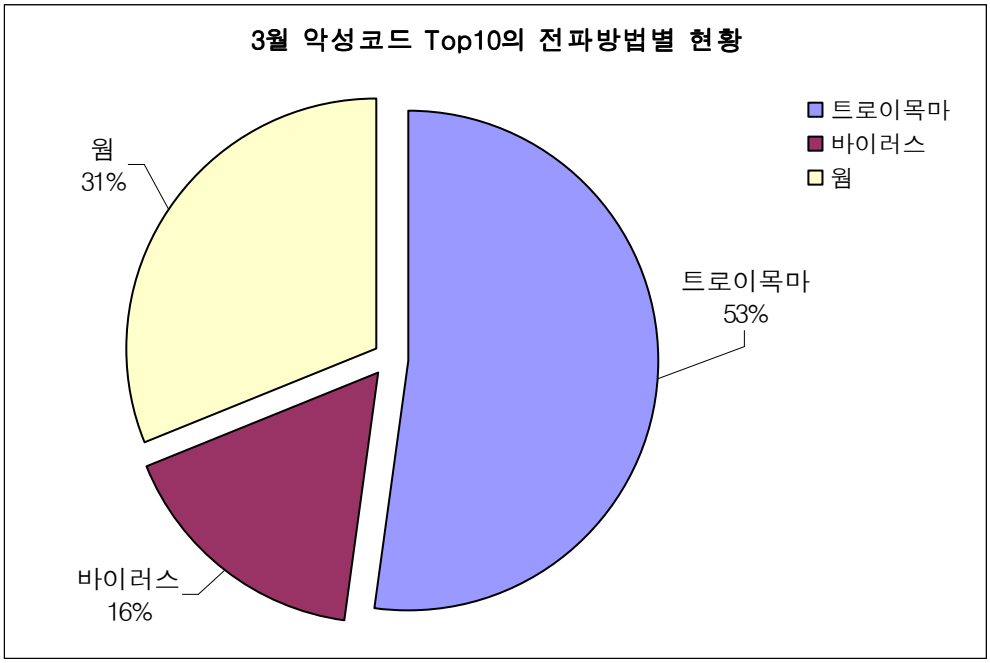


[그림 1-2] 2007년 월별 피해신고 건수 악성코드 피해 Top 10

}

3월 악성코드 Top 10 전파방법 별 현황

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

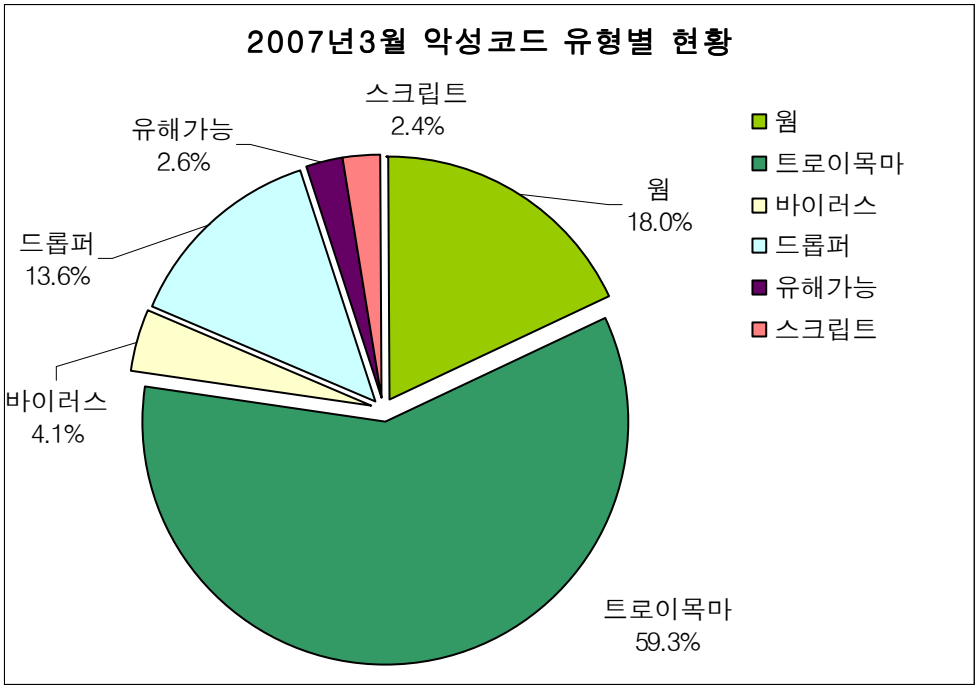


[그림 1-3] 2007년 2월 악성코드 Top 10의 전파방법별 현황

3월에도 변함없이 트로이목마류가 가장 많은 피해를 발생시켰으며, 점유률은 53%로 전월(40%)에 비해 증가하였으며, 웜에 의한 피해는 전월(26%)에 비해 소폭 증가하였고, 바이러스는 바이럿(Win32/Virut)의 순위하락으로 점유율이 하락하였다. 그러나, 3월말에 바이럿의 새로운 변종이 2개가 발견되어 이로 인한 피해가 접수되고 있어 바이러스에 의한 피해가 줄어들고 있다고 볼 수는 없다.

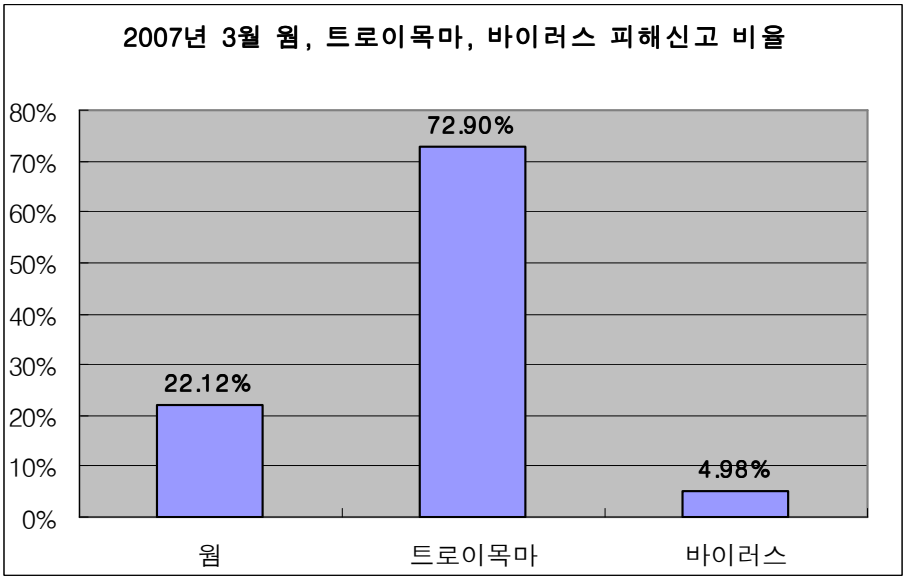
피해신고 된 악성코드 유형 현황

2006년 3월에 피해신고 된 악성코드의 유형별 현황은 [그림 1-4]와 같다.



[그림 1-4] 2007년 3월 피해 신고된 악성코드 유형별 현황

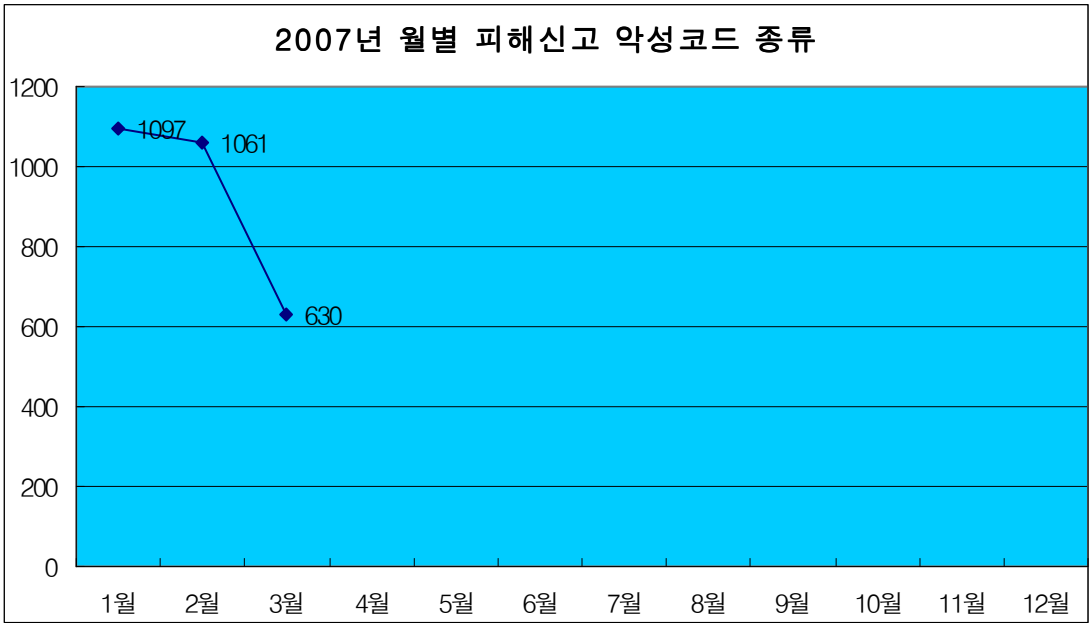
전체 피해 신고에서의 악성코드 유형을 확인해보면, Top10의 악성코드 유형과 유사한 양상을 띄고 있다. 트로이목마, 바이러스, 웜 등이 주요 악성코드 유형인 것으로 확인되었으며, 이중 주요 악성코드 유형인 트로이목마, 바이러스, 웜에 대한 피해신고 비율을 따져보면 [그림 1-5]와 같다.



[그림 1-5] 2007년 3월 웜, 트로이목마 피해신고 비율

월별 피해신고 된 악성코드 종류 현황

[그림 1-6]에서와 같이 피해신고 악성코드 종류는 전월에 비하여 40%가까이 감소된 것을 확인할 수 있다. 이는 피해를 일으키는 악성코드가 다수의 종류가 아닌, 파괴력이 높은 특정 악성코드들 위주로 전파되는 것이 그 원인으로 보인다.



[그림 1-6] 2007년 월별 피해신고 악성코드 종류 개수

국내 신종(변형) 악성코드 발견 피해 통계

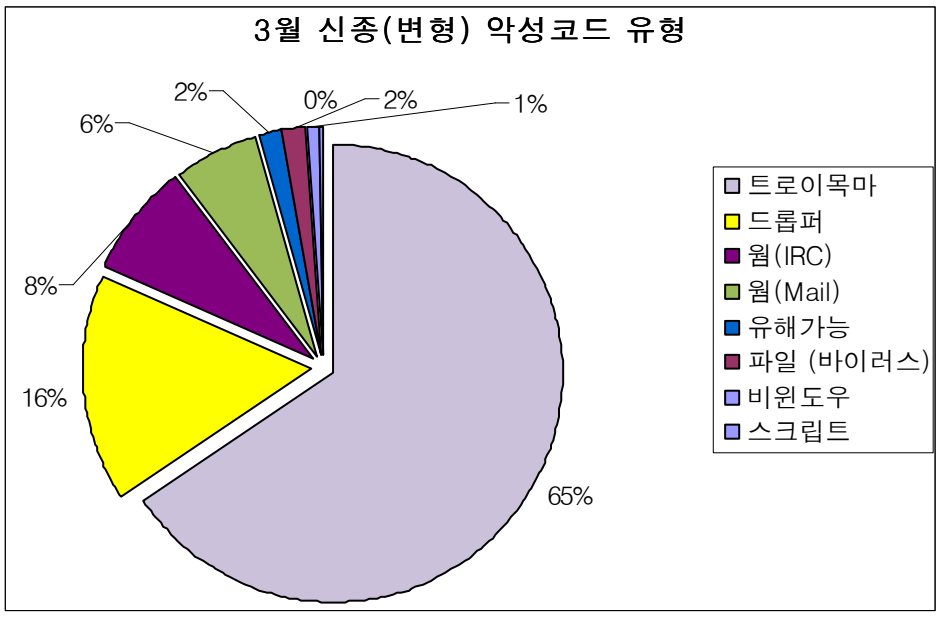
3월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표 1-2], [그림 1-7]과 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
67	323	79	2	9	0	0	0	8	4	492

[표 1-2] 2007년 3월 유형별 신종 (변형) 악성코드 발견현황

이번 달은 전월 대비 악성코드는 16% 증가 하였다. 이는 지난달에 추정한 바와 같이 중국산 악성코드의 국내 유입이 늘어나면서부터 나타나는 증상이라 할 수 있다. 즉, 중국 명절기간(춘절)에 악성코드 제작 및 유입이 줄어들고, 3월부터 다시 증가한 것으로 볼 수 있다.

증가된 악성코드도 역시 중국산 트로이목마와 드롭퍼가 제일 큰 비중을 차지하며 전월 대비 11% 증가 하였다. 특히 온라인 게임의 사용자 계정을 훔쳐내는 악성코드는 26%나 증가 하였다. 이전 리포트에서도 언급한 바와 같이 국내 유입되는 중국산 그리고 실행 파일을 감염시키는 바이러스와 유해가능 프로그램들도 소폭 증가 하였다.



[그림 1-7] 3월 신종(변형) 악성코드 유형

전월과 비교해서 증가한 또 다른 악성코드로는 Win32/IRCBot.worm (이하 아이알씨 봇 웜)으로, 39% 증가한 이 악성코드는 일부 안티 바이러스 솔루션에서 실행압축을 해제할 수 없는 실행압축 프로그램을 사용한 형태가 다수 발견되었다. 그 외에는 다른 아이알씨 봇 웜과 큰 차이가 발견되지 않았다. Win32/Zhelatin.worm (이하 젤라틴 웜)이라고도 불리는

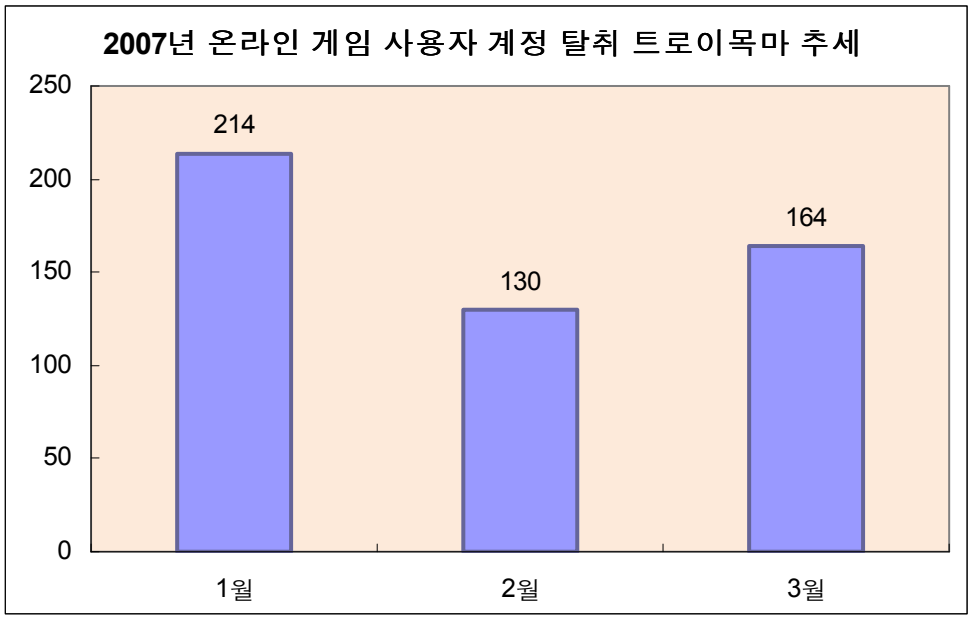
Win32/Mixor.worm (이하 믹쏘 웜)의 변형도 이메일 웜으로 사용자의 피해를 입혔다. 마지막으로 트로이목마 중 팝업 광고 창을 노출 하는 Win-Trojan/Virtumonde(이하 버추몬드 트로이목마)도 작지만 증가 추이를 보이는데, 이는 이번 달에 보고된 Win32/Virut.C, D 형에 의해서 설치 되고 있었다.

최근에 중국에서 제작된 국내 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마들은 다음과 같은 특이한 점이 발견되고 있다.

- 일부 안티 바이러스 솔루션의 진단 시 경고 창을 꺼버리거나 윈도우의 볼륨설정을 제로화 시킴
- 일부 온라인 게임에 적용된 키보드 보안 솔루션을 우회 하는 증상

위와 같은 증상은 작년 하반기부터 나타나기 시작하여 최근 발견되는 변형들에서 자주 보이는 증상들이다. 이를 통하여 안티 바이러스 솔루션에서 진단되더라도 고객이 인지하지 못하게 하고, 안티 바이러스 솔루션에 대한 생존력을 극대화하려는 시도인 것으로 보인다.

[그림 1-8]은 중국 발 웹 해킹의 주목적이기도 하며, 많은 변형이 발견, 보고되고 있는 온라인 게임의 사용자 계정을 탈취하는 악성코드에 대한 2007년도 월 발견 건수에 대한 그래프이다.

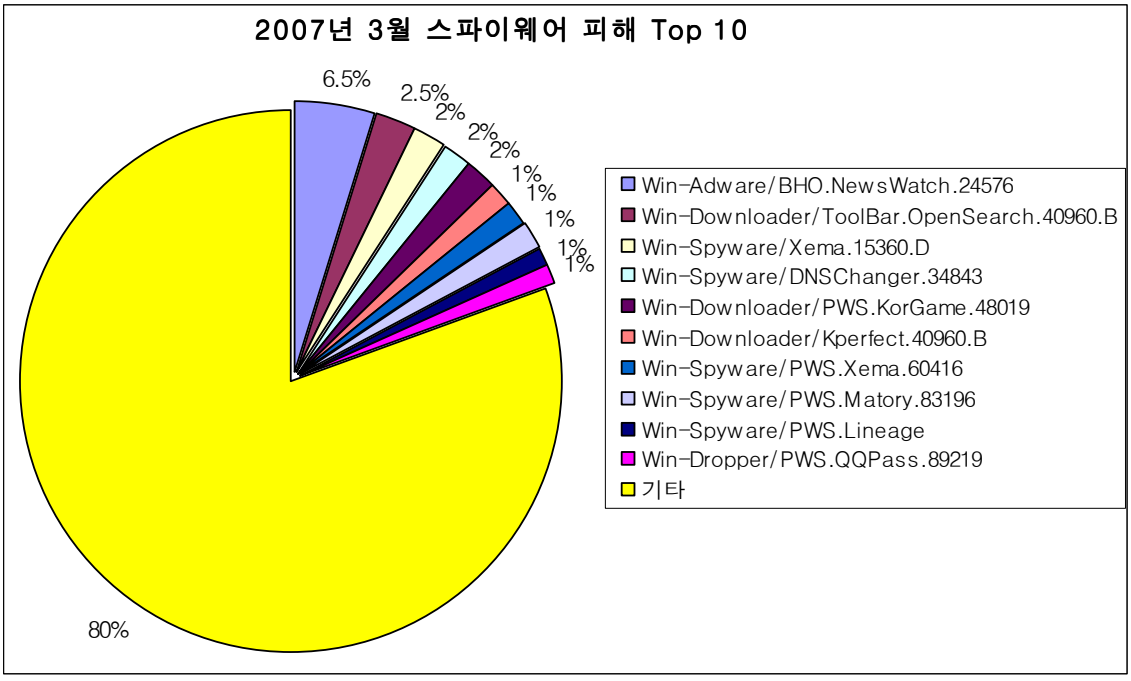


[그림 1-8] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

(2) 3월 스파이웨어 피해 통계

순위		스파이웨어 명	건수	비율
1	New	Win-Adware/BHO.NewsWatch.24576	16	6.5%
2	New	Win-Downloader/ToolBar.OpenSearch.40960.B	8	2.5%
3	New	Win-Spyware/Xema.15360.D	7	2%
4	New	Win-Spyware/DNSChanger.34843	6	2%
4	New	Win-Downloader/PWS.KorGame.48019	6	2%
5	New	Win-Downloader/Kperfect.40960.B	5	1%
5	New	Win-Spyware/PWS.Xema.60416	5	1%
5	New	Win-Spyware/PWS.Matory.83196	5	1%
9	New	Win-Spyware/PWS.Lineage	4	1%
9	New	Win-Dropper/PWS.QQPass.89219	4	1%
		기타	272	80.0%
합계			338	100%

[표 1-3] 2007년 3월 스파이웨어 피해 Top 10



[그림 1-9] 2007년 3월 스파이웨어 피해 Top 10

2007년 2월에 비하여 온라인게임 계정 유출 스파이웨어에 의한 피해가 다소 증가하긴 했지만 1월만큼의 큰 피해는 나타나지 않았다. 피해신고 top 10의 5개 항목이 사용자 계정 유출 목적의 패스워드 스틸러 계열의 스파이웨어며, 3월에 발견된 스파이웨어 마토리(Win-

Spyware/Matory)의 경우에는 웜 기능이 포함된 것도 있어 피해 증가가 예상된다.

피해신고 1위를 차지한 애드웨어 뉴스워치(Win-Adware/BHO.NewsWatch.24576)는 사용자 동의없이 설치되어 IE 검색 결과를 변경하는 애드웨어이다. 중국에서 제작된 것으로 분석되었으며 다운로더 또는 드랍퍼에 의해 설치되는 것으로 추정된다. 국내 애드웨어에 의한 피해도 눈에 띄는데 피해신고 top 10의 2위를 차지한 애드웨어 오픈서치(Win-Adware/ToolBar.OpenSearch.40960.B)는 허위 안티-스파이웨어 프로그램에 의해 사용자 동의 없이 설치되는 애드웨어이다.

2007년 3월에는 총 338건의 스파이웨어 피해 신고가 접수되었으며, 1월의 445건에 비하여 약 25% 감소하였다. 유형별 피해 현황은 [표 1-4]와 같다.

스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
123	100	25	69	1	14	6	0	0	338

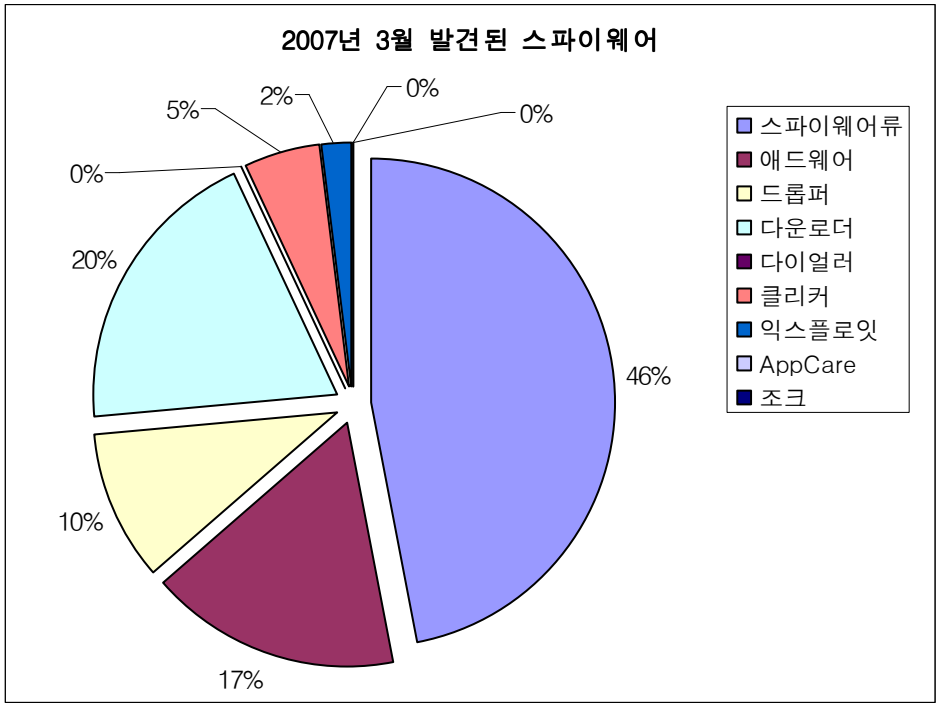
[표 1-4] 2007년 3월 유형별 스파이웨어 피해 건수

3월 스파이웨어 발견 현황

3월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-4], [그림 1-10]과 같다.

스파이웨어류	애드웨어	드롭퍼	다운로더	다이얼러	클리커	익스플로잇	AppCare	Joke	합계
48	17	10	20	0	5	2	0	0	102

[표 1-4] 2007년 3월 유형별 신종(변형) 스파이웨어 발견 현황



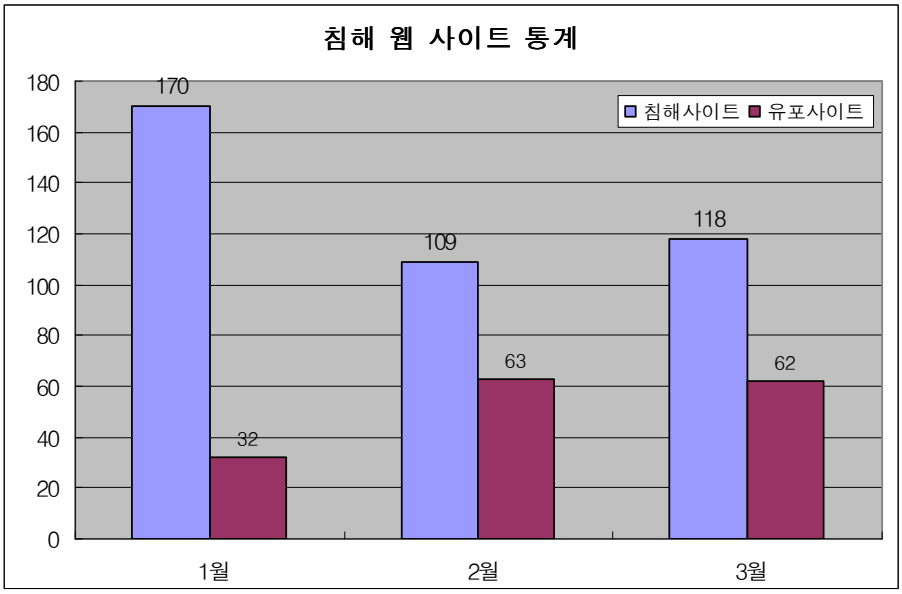
[그림 1-10] 2007년 3월 발견된 스파이웨어 프로그램 비율

2월에 비하여 약 35% 감소한 102건의 신종 및 변형 스파이웨어가 접수되었으며, 새로 발견된 스파이웨어류의 수가 72건에서 48건으로 크게 감소하였다. 스파이웨어류의 감소와 이와 관련된 다운로더의 감소가 전체 신종 및 변형 스파이웨어 발견 건수에 영향을 미친 것으로 분석된다.

(3) 3월 시큐리티 통계

2007년 3월에는 마이크로소프트사의 정기 보안 업데이트가 발표되지 않았으며 3월 31일 Animated Cursor Handling 취약점에 대한 비 정기 정기 업데이트를 4월 3일 발표하였다. 2007년 2월 패치이후 발견된 취약점을 이용한 공격이 매우 "제한적인" 상황에서만 가능하기 때문에 MS사는 정기 보안 업데이트를 발표하지 않은 것으로 보인다

2007년 1/4분기 웹 침해사고 현황



[그림 1-11] 침해 웹사이트 개수

► 침해/유포사이트 수의 변화

2007년 3월의 침해/유포 사이트의 수는 118/62로 2007년 1월에 비해 30% 감소하였다. 하지만 2007년 2월과 비교하였을 때는 큰 차이가 없으며 오히려 침해사이트의 수가 소폭 상승하였다. 이는 웹사이트의 관리 상태가 이전과 큰 차이가 없이 방치되고 있는 사이트가 여전히 존재하고 있다는 것을 의미한다.

► Animated Cursor Handling 취약점을 이용한 악성 코드 배포

침해사고가 일어난 일부 사이트에 Animated Cursor Handling 취약점을 이용한 웹페이지가 발견되었다. 이 취약점을 이용한 코드는 많은 플랫폼에서 실행 가능하기 때문에 앞으로 많은 침해 웹페이지에 해당 취약점을 이용한 코드가 삽입될 것으로 예상된다. 아래 그림은 해당 취약점을 이용한 악성 코드 배포 사례이다.

```
w2k = ((a.indexOf('windows nt 5.0')!=-1) || (a.indexOf('windows 2000')!=-1));
wxp = ((a.indexOf('windows nt 5.1')!=-1) || (a.indexOf('windows xp')!=-1));
w2k3 = ((a.indexOf('windows nt 5.2')!=-1) || (a.indexOf('windows 2003')!=-1));
if(wxp)jpDiv.innerHTML = "<div style=\"cursor: url(
if(w2k)jpDiv.innerHTML = "<div style=\"cursor: url(
```

이런 악성코드의 공격에 의한 피해를 최소한으로 하기 위해서는 해당 패치를 반드시 해야 한다.

II. ASEC Monthly Trend & Issue

(1) 악성코드 - ANI 관련 취약점과 Win32/Virut 바이러스 변형 출현

윈도우 애니메이션 커서 처리의 취약점을 이용한 악성코드가 쏟아져 나왔다. 특히 취약점이 있는 파일을 제작해주는 도구도 존재하는 것으로 알려졌다. 해당 취약점은, 중국의 악성코드 제작자들이 국내의 보안의 취약한 웹 사이트를 해킹 후 악성코드를 유포하는데 이용하였던, 기존의 MS06-014 취약점을 대체하고 있는 것으로 보인다. 또한 작년 한해 큰 피해를 주었던 Win32/Virut 바이러스의 변형이 보고되었고 원형보다 진단, 치료하기가 어렵게 되어있다.

► 윈도우 애니메이션 커서 관련 취약점

윈도우의 애니메이션 커서 및 아이콘 파일 형태에 취약점이 존재하였으며, 보안패치가 공개되기 전에 취약점 공격코드가 공개된 Zero-Day 공격이라 할 수가 있다. 이 취약점은 User32.DLL에서 사용하는 이미지로드 관련 함수가 이미지의 헤더 값을 제대로 핸들링 하지 못하기 때문에 발생하였다. 이 취약점 공격코드가 알려지자마자 기존 국내 웹 사이트를 해킹 후 악성코드를 다운로드 및 자동 실행하도록 하는 MS06-014 취약점을 대체하려는 듯이 해킹된 많은 사이트에서 해당 취약점을 사용한 파일이 업로드 되어 있음을 확인 할 수 있었다. MS에서 MS07-017 긴급 보안패치를 배포하였으나, 대부분 사용자들이나 불법 윈도우를 사용하는 사용자들이 보안 패치에 무관심하거나 받지 못하기 때문에 해당 취약점은 MS06-014을 대체할 수도 있고, 그 피해는 증가 될 것으로 예상된다.

► Win32/Virut 바이러스의 변형 출현

작년 한 해 큰 피해를 주었던 Win32/Virut (이하 바이럿 바이러스) 바이러스의 변형이 발견, 보고되었다. 백신의 개발을 지연시킬 목적으로 이전 원형과는 달리 분석 및 진단, 치료를 쉽게하지 못하도록 제작되었다. 이들 변형은 Win32/Virut.C와 D형으로 명명 되었다. 특히 C형은 시작 실행시점 불명확화 기법(Entry-Point Obscuring=EPO)을 사용하고, 다형성 디크립터를 가지고 있는 등 원형과 매우 다르게 제작 되었다. 또한 Winlogon.exe에 감염 쓰레드를 생성하고 파일 및 프로세스 관련 함수를 후킹하여 파일을 감염시키는 형태는 원형과 동일하여 메모리 치료를 선행하지 않으면 재감염되므로 주의를 요구한다.

또한 이번 변형은 실행 후 접속하는 IRC 서버로부터 다른 악성코드를 다운로드하는 다운로더를 설치하거나 은폐형 백도어를 설치하기도 한다. 특히 이 은폐형 백도어는 다운로드 되는 시점에 바이럿 바이러스에 감염되기 때문에 은폐된 상태에서는 진단, 치료가 되지 않으므로 반드시 은폐를 무력화 한 후 바이럿 바이러스를 치료 후 백도어도 제거해야만 한다.

안철수연구소는 바이럿 전용백신을 통하여 메모리 진단, 치료와 은폐를 무력화하는 전용백신을 무상으로 공개하여 홈페이지를 통해서 다운로드 및 진단, 치료 할 수 있도록 해두었다.

► 봇넷을 이용하는 메신저 웜

Win-Trojan/ShadoBot 이라고 (이하 쉐도봇) 명명된 악성코드는 자신의 드롭퍼를 메신저를 이용하여 전파한다. 그리고 특정 IRC 서버에 연결되어 마스터의 명령에 따라 자신을 MSN 메신저로 전파한다. 이전에 알려진 Kelvir (이하 캘비르 웜) 또는 Bropia (브로피아 웜) 웜의 경우에 아이알씨 봇 웜을 별도로 내부에 가지고 있어 이를 Drop 한 후 실행하는 형태라면 쉐도봇 트로이목마는 자신이 직접 봇넷에 연결되어 명령을 받고 악의적인 증상을 수행한다는 점에서 차이가 있다.

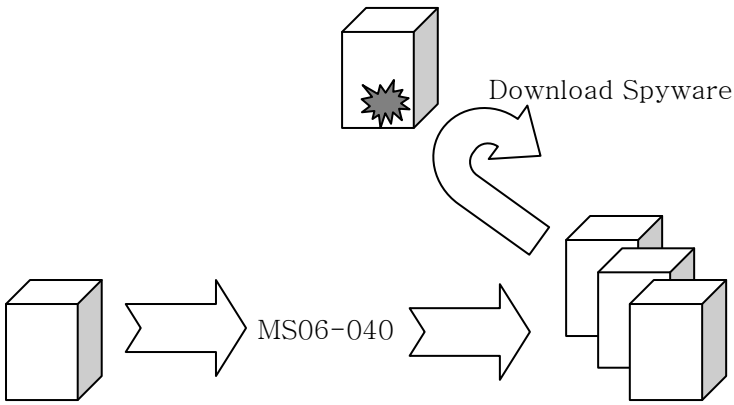
► 윈도우 정상 파일을 패치하여 동작하는 악성코드

일반적으로 트로이목마는 삭제하는 것으로 쉽게 치료될 수 있다. 그러나, Win-Trojan/Patched.B라고(이하 패치드 비 트로이목마) 명명된 악성코드는 윈도우의 Windows NT Logon Application 인 Winlogon.exe에 작은 코드를 삽입해둔다. 이 코드는 해당 파일이 시작될 때 특정 분기로 점프하여 익스포트된 외부 모듈를 실행하도록 하며, 해당 모듈은 백도어나 트로이목마의 악성코드로 파악되나 어떤 파일인지는 확인되지 못했다. 또한 해당 파일을 패치하면서 원래 코드를 파일의 어느 부분에도 남겨두지 않았기 때문에 치료에 있어서 더 신중을 기 할 수 밖에 없었다. 이처럼 윈도우의 중요한 파일을 패치하여 악성코드를 실행하도록 해두는 경우가 종종 있는데, 이 경우 패치한 정상코드를 남겨두었는지 아니면 존재하지 않는지에 대해서 치료에 큰 차이가 있다. V3는 접수된 Winlogon.exe 에 대한 버전만 치료하기로 결정하고 엔진에 진단, 치료함수를 제작하여 반영 하였다.

(2) 스파이웨어 동향 : 복합 공격의 증가

스파이웨어를 포함한 악성코드의 진화는 시간이 갈수록 더욱 지능적으로 변화되고 악성코드 보안 업체와의 줄다리기는 지금도 끊임없이 계속되고 있다. 스파이웨어들이 자신을 은폐할 목적으로 루트킷(RootKit)을 사용하고 있으며, 최근에는 자신을 전파할 목적으로 웜(Worm)의 기능이 추가되는 경향이 있다.

온라인 게임계정 유출목적의 스파이웨어가 윈도우 취약점을 공격하여, 이를 이용하여 확산을 시도하는 웜 기능이 추가된 악성코드가 발견되어 주의가 요망된다. 웜을 이용하여 다른 악성코드를 다운로드 하거나 스팸메일을 발송하는 사례는 다수 발견되었으나, 사용자의 중요 정보를 유출하기 위한 스파이웨어가 자체적으로 다른 시스템으로 확산, 감염시키기 위한 목적으로 웜 기능을 추가한 것은 복합 공격이 증가할 것이라는 예상을 반영하는 사실로 생각할 수 있다.



[그림 2-1] Win-Downloader/PWS.KorGame.48019 의 공격 개요

[그림 2-1]은 MS06-040[1] 취약점을 이용하여 원격 PC의 실행권한을 얻어 특정서버에서 파일을 다운로드하고 다운로드 받은 파일을 실행하는 흐름을 그림으로 표현한 것이다. 온라인 게임계정 유출을 목적으로 하는 스파이웨어를 설치하고 실행하는 다운로더 코게임(Win-Downloader/PWS.KorGame.48019)은 IE 취약점을 이용하여 중국발 해킹에 의해 변조된 웹사이트를 통하여 사용자 시스템에 감염되는데 여기서 그치지 않고 다른 시스템으로 확산하기 위하여 MS06-040 취약점 공격코드를 이용하는 웜의 특징을 가지고 있다. 이전에는 IE 취약점 패치가 적용되지 않은 사용자가 공격코드가 포함된 웹 페이지를 방문하여야만 감염되었지만, 웜 기능이 추가 되면서 더욱 능동적인 확산을 노리고 있다. 목적은 다른 온라인게임 계정 유출 스파이웨어와 마찬가지로 중요 사용자 정보의 획득이며, 이를 통한 금전적인 이익을 노리고 있다.

MS06-040 취약점은 윈도우 시스템에서 RPC 지원과 네트워크를 통한 파일 인쇄 및 명명

[1] http://www.microsoft.com/korea/technet/security/bulletin/MS06-040.mspx

된 파이프 공유를 제공하는 윈도우 기본 서비스인 서버 서비스(srvsvc.dll)에서 RCP Call 요청시 특정 서비스에서 버퍼를 올바르게 체크하지 않아 버퍼 오버플러우 취약점이 존재한다. 공격자는 이 취약점을 이용하여 시스템의 관리자 권한을 획득할 수 있다.

[그림 2-2] MS06-040 취약점 코드

[그림 2-2]는 다운로더 코게임의 MS06-040 취약점을 이용한 쉘코드(Shell-Code) 부분을 바이너리 덤프한 화면으로, 오른쪽 부분의 ASCII 문자열을 살펴보면 쉘코드 중간에 쓰레기 값이 들어 있어 기계적으로 쉽게 찾아내거나 판단할 수 없도록 하였는데, 이는 안티 바이러스 또는 안티 스파이웨어 제품들이 문자열 패턴 진단법을 사용하는 경우 진단을 회피하기 위한 방법을 사용한 것이고, 쉘코드를 호출하는 페이로드(PayLoad)는 암호화하는 등 다양한 기법이 사용되었다.

복합공격의 증가와 함께 검증되지 않은 프로그램에 의하여 바이러스나 트로이목마와 같은 악성코드에 감염되는 사례가 증가하고 있다. 특히 스파이웨어의 경우 그 자체가 위협적이기도 하지만 바이러스에 감염된 채로 배포되는 경우 예상치 못한 시스템 감염을 일으킬 수 있으므로 주의가 필요하다. 허위 안티-스파이웨어 프로그램인 닥터제로(Win-Adware/Rogue.DrZero [1])의 경우 인터넷 게시판이나 블로그 등의 불특정 웹사이트에서 ActiveX 형태로 사용자 동의없이 설치되고 실행된다. 허위 안티-스파이웨어 프로그램은 무료 악성코드 치료, 컴퓨터 최적화 등의 문구를 ActiveX 보안 경고창에 삽입하고 설치를 유도하는 것이 일반적이며, 일반 사용자의 경우 무심코 설치하는 것이 일반적이다. 문제는 닥터제로의 구성요소가 이미 바이럿(Win32.Virut [2])에 감염되어 배포되었기 때문에 다른 정상 실행파일까지 바이럿에 감염되는 피해를 입을 수 있다. 2007년 2월에 발견된 스파이웨어 네마리(Win-Spyware/Nemari)의 경우에도 ActiveX로 설치되는 스파이웨어이며, 바이럿에 감염된 상태로 배포되었다. 스파이웨어나 애드웨어뿐만 아니라 신뢰할 수 없는 프로그램으로 인하여 바이러스와 같은 악성코드에 감염될 위협은 항상 존재하며 이에 대한 각별한 주의가 요망된다.

► Anti-Spyware Coalition이 Best Practices, Conflicts Resolution 문서 완성

ASC가 몇 달 동안 교정 작업을 거쳐 'Best Practices'와 'Conflict Resolution' 문서를 발표하였다. ASC는 스파이웨어와 다른 원치 않는 기술들에 대해서 토론하여 정의와 적합한 행동

[1] http://kr.ahnlab.com/info/smart2u/virus_detail_7459.html
[2] http://kr.ahnlab.com/info/smart2u/virus_detail_7447.html

들에 대해 의견을 일치해가데 목적을 가지는 그룹으로 안철수연구소는 2006년 6월부터 가입되어 있으며, 해당 문서는 http://antispywarecoalition.org/documents/에서 다운로드 받을 수 있다.

'Best Practices'는 안티-스파이웨어 업체가 응용프로그램이 사용하는 기술과 행동이 사용자가 원치않는 것인지를 평가하기 위한 지침과 고려할 사항들을 제공하고 있으며 이는 ASC의 'Definitions'와 'Risk Model' 문서에 기초하고 있다. 'Conflict Resolution'는 안티-스파이웨어 제품간에 충돌이 발생할 경우 해결할 수 있는 절차와 개발자간의 대화 방법을 제시한다. 이는 안티-스파이웨어 제품간에 충돌을 경험하게 될 고객들에게도 투명성을 제공하는 것이다.

(3) 시큐리티 - Animated Cursor Handling 취약점

MS사는 2007년 3월 정기 보안 패치를 발표하지 않았다. 이는 2007년 2월 패치이후 발견된 취약점이 매우 "제한적인" 상황에서만 이용가능 하는 등, 취약점의 위험도가 그리 높지 않기 때문에 정기 보안 패치를 발표할 필요가 없다는 MS사의 자체적인 판단으로 보인다. 하지만 2007년 3월 말에 위험등급이 매우 위험인 Animated Cursor Handling에 관한 취약점이 발표되어 4월 초에 MS사는 긴급 패치(MS07-017)를 발표하게 되었다. 따라서 모든 윈도우 운영체제의 사용자는 해당 취약점의 패치를 반드시 해야 피해를 예방할 수 있다. 기존 취약점이 특정 응용 프로그램에 존재하기 때문에 해당 제품을 사용하지 않는 사용자에게 영향을 주지 못한데 반해, 이 번 취약점은 운영체제의 시스템 파일에 존재하는 것으로 이 파일을 사용하는 모든 응용프로그램에 영향을 줄 수 있는 매우 심각한 것이다.

MS사의 공식발표(http://blogs.technet.com/msrc/archive/2007/03/30/update-on-

http://blogs.technet.com/msrc/archive/2007/03/30/update-on-

http://blogs.technet.com/msrc/archive/2007/03/30/update-on-microsoft-security-advisory-935423.aspx)에 의하면 MS사는 해당 취약점을 2006년 12월에 처음 보고 받은 것으로 보인다. 하지만 이 취약점이 미칠 수 있는 큰 영향에도 불구하고 3개월이 넘게 별 다른 패치를 발표하지 않고 처음으로 이 취약점을 이용한 악성코드를 접하고서야 대응을 한 MS사의 느린 대응은 매우 아쉬운 점이라 하겠다. MS사는 이번 취약점에 관한 권고문(http://www.microsoft.com/technet/security/advisory/935423.mspxhttp://www.microsoft.com/technet/security/advisory/935423.mspx)을 발표하였다.

이번 패치와 관련된 눈길을 끄는 사실은 이번 취약점이 발견된 코드가 2년 전에 발견된 취약점(MS05-002)과 동일한 부분에서 발견되었다는 것이다. 이 사실은 결과적으로 MS사의 예전 패치가 잘못되었다는 것을 보여주며, MS사의 패치가 근본적인 문제를 해결하지 않고 해당 취약점만을 보완하는 "땜질"식이라는 일부 의혹을 확인시켜주는 예라고 하겠다. 이 번 취약점을 이용하는 악성 코드의 예처럼 이미 발표된 MS 패치의 잘못된 논리를 이용하는 악성 코드는 얼마든지 출현가능하고 볼 수 있기 때문에 과거 발표된 MS사의 패치의 안전성을 점검하는 작업이 필요하다고 할 수 있다.

MS05-002는 힙 오버플러우인 반면에, MS07-017은 사용자가 조작된 Animated Cursor 파일을 특정 어플리케이션에 로드할 경우 취약점이 존재하는 곳에서 버퍼 오버플로우가 발생하며 그 결과로 공격자는 임의의 코드를 사용자의 시스템에서 실행할 수 있다. 취약점이 존재하는 곳은 User32.dll의 LoadAniIcon 함수로 이 함수의 역할은 Animated Cursor 파일의 헤더를 파싱하고 해당 데이터를 처리하는 것이며 이 함수는 Animated File 을 로드할 때 실행된다. [그림 2-3]은 LoadAniIcon 함수가 각 헤더를 판별하고 해당 헤더를 처리하기 위해 분기하는 코드를 나타낸다.

```
text:77D33FA5                mov     eax, [ebp+var_28]
text:77D33FA8                cmp     eax, 20716573h  ; 해당 헤더의 이름이 "seq " 인가?
text:77D33FAD                jz      loc_77D3412F
text:77D33FB3                cmp     eax, 5453494Ch  ; 해당 헤더의 이름이 "LIST" 인가?
text:77D33FB8                jz      loc_77D34089
text:77D33FBE                cmp     eax, 65746172h  ; 해당 헤더의 이름이 "rate" 인가?
text:77D33FC3                jz      loc_77D3406F
text:77D33FC9                cmp     eax, 68696E61h  ; 해당 헤더의 이름이 "anih" 인가?
text:77D33FCE                jnz     loc_77D340B3
```

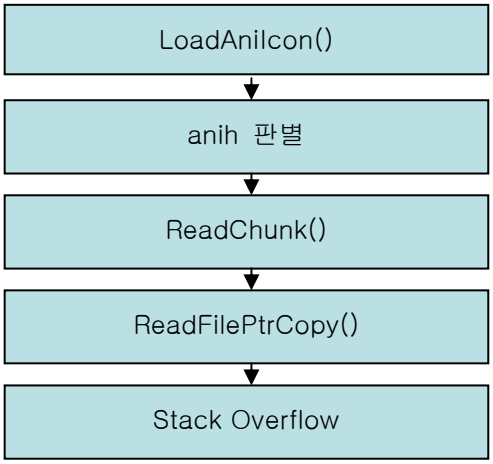
[그림 2-3]. User32.dll LoadAniIcon함수에서 처리할 각 헤더를 판별하는 부분

Animated File은 일련의 헤더로 구성되어 있고, 이번 취약점은 anih 헤더를 처리하는 부분에서 발생한다. anih 헤더의 구조는 [표 2-1]과 같다

Name	Size (bytes)	Description
Size	4	헤더의 크기 (항상 36임)
HeaderSize	4	Size 필드와 동일함
NumFrames	4	애니메이션 파일의 프레임 수
NumSteps	4	애니메이션 파일의 스텝수
Width	4	가로 픽셀 크기
Height	4	세로 픽셀 크기
BitCount	4	Colordepth의 수
NumPlanes	4	Plane의 수 (1로 고정)
DisplayRate	4	디스플레이 주파수
Flags	4	데이터의 종류를 나타내는 flag

[표 2-1] anih 헤더 구조

[표 2-1]에서 알 수 있듯이 anih 헤더의 크기는 36(=0x24)로 고정되어 있다. 만약 이 헤더의 크기가 36이 아니면 잘못된 헤더로 인식하고 Animated Cursor 파일의 로딩을 중단해야 한다. 하지만 LoadAniIcon 함수에는 anih 크기가 잘못되었을 경우의 처리가 존재하지 않고 Animated Cursor File에서 정의된 anih 헤더의 크기만큼의 데이터를 스택에 복사한다. 따라서 anih의 크기가 36보다 크게 설정된 경우 36보다 큰 데이터를 스택에 복사하게 되고 결과적으로 스택 오버플로우가 발생하게 된다. [그림 2-4]와 [그림 2-5]는 LoadAniIcon에서 anih 헤더를 처리하는 일련의 과정과 버퍼 오버플로우가 일어나는 코드를 나타낸 것이다.



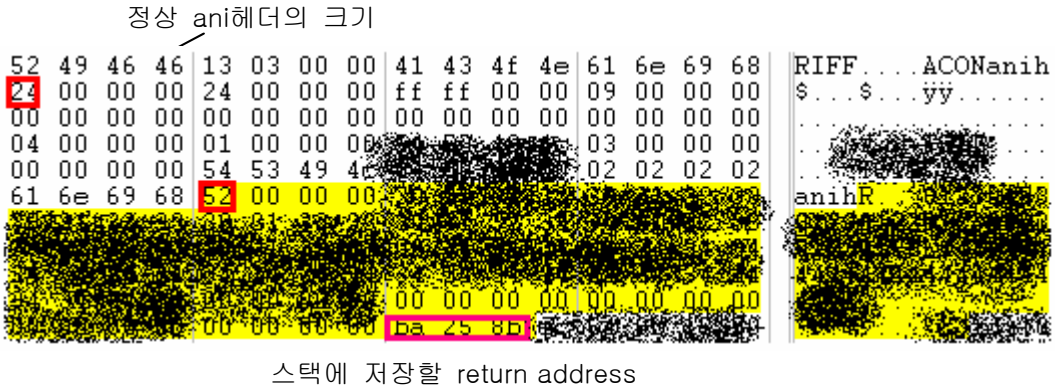
[그림 2-4] 스택 오버플로우가 발생하는 일련의 과정

```
.text:77D33A7E                mov     ecx, edx        ; edx 레지스터: anih의 크기
.text:77D33A7E                                        ; edx 레지스터의 값을 ecx 레지스터에 복사
.text:77D33A80                mov     ebx, ecx
.text:77D33A82                shr     ecx, 2
.text:77D33A85                rep movsd               ; 메모리 복사가 일어나는 코드
.text:77D33A85                                        ; ecx의 값만큼 메모리 복사를 반복
.text:77D33A87                mov     ecx, ebx
.text:77D33A89                and     ecx, 3
.text:77D33A8C                rep movsb
```

[그림 2-5] 오버플로우가 발생하는 코드

[그림 2-5]에서 rep movsd 인스트럭션에 의해 복사되는 메모리의 목적 주소는 스택 주소이므로 복사할 데이터의 크기(=anih 헤더의 크기)가 비정상적인 값인 경우 스택 오버플로우가 발생한다. 만약 공격자가 이 값을 쉘코드의 주소등으로 정교하게 조작한다면 공격자는 임의의 코드를 사용자의 시스템에서 실행할 수 있다. 일반적으로 스택 버퍼 오버플로우 취약점을 이용하는 악성 코드는 쉘코드의 주소를 스택에 저장하지만 이번에 발견된 악성 코드는 user32.dll의 특정 루틴의 주소를 스택에 저장하고 그 값을 올바른 위치에 저장하기 위해 오버플로우되는 크기를 정확히 계산하여 Animated File에 집어넣는 등 정교함을 보여주었다 [그림 2-6]. 이 것은 특정 플랫폼에서 user32.dll의 메모리 주소가 항상 일정하다는 것을 이용한 공격기법으로, 해당 플랫폼에서만 동작하는 등의 제약이 있지만 악성 코드가 점점 지능

적으로 진화한다는 것을 보여주는 예이다.



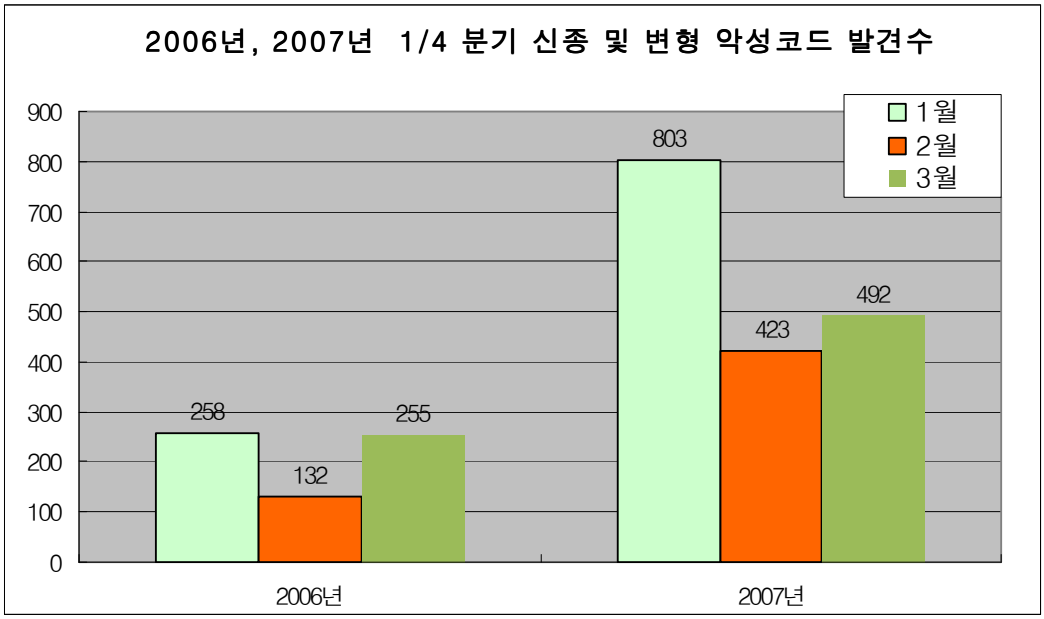
[그림 2-6]. 조작된 animated cursor 파일 덤프

이 번 취약점은 IE나 오피스 같은 특정 제품의 취약점이 아니라 운영체제의 시스템 파일에서 발견된 것으로 animated cursor를 이용하는 모든 윈도우즈 응용프로그램에 영향을 줄 수 있는 매우 심각한 취약점이라고 할 수 있다. 따라서 사용자는 해당 취약점의 패치를 반드시 해야하며, Anit-Virus 프로그램 및 개인 방화벽을 사용하여 악성코드에 의한 피해를 최소한으로 줄여야 한다.

III. 2007년 1분기 동향

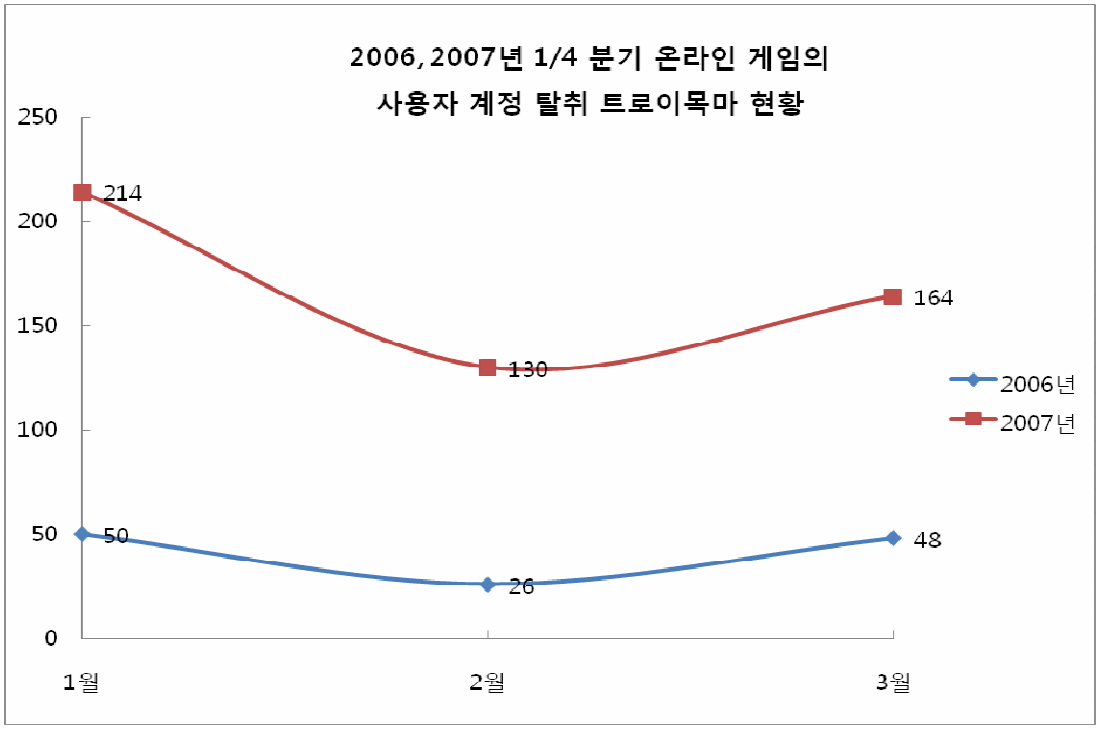
(1) 2007년 1분기 악성코드 동향

전년동기와 올해 동기의 악성코드의 전체적인 흐름은 대략적으로 비슷하다. 중국발 웹 해킹은 계속적으로 이루어지고 있으며 이에 따른 중국산 트로이목마의 유입은 악성코드 유형 중 가장 많은 수를 차지 한다. 작년 동기와 큰 차이점이라면 악성코드가 숫적으로 166% 이상 증가한 것이다. 또한 악성코드의 형태가 트로이목마에서 실행 파일을 감염시키는 바이러스가 증가하고 있고, 이는 작년 동기에는 없었던 현상으로 작년 3/4분기부터 폭발적으로 증가하고 있는 중국산 파일 바이러스의 변형에 기인한 것이다.



[그림 3-1] 06, 07년 1/4 분기 신종 및 변형 악성코드 발견 수

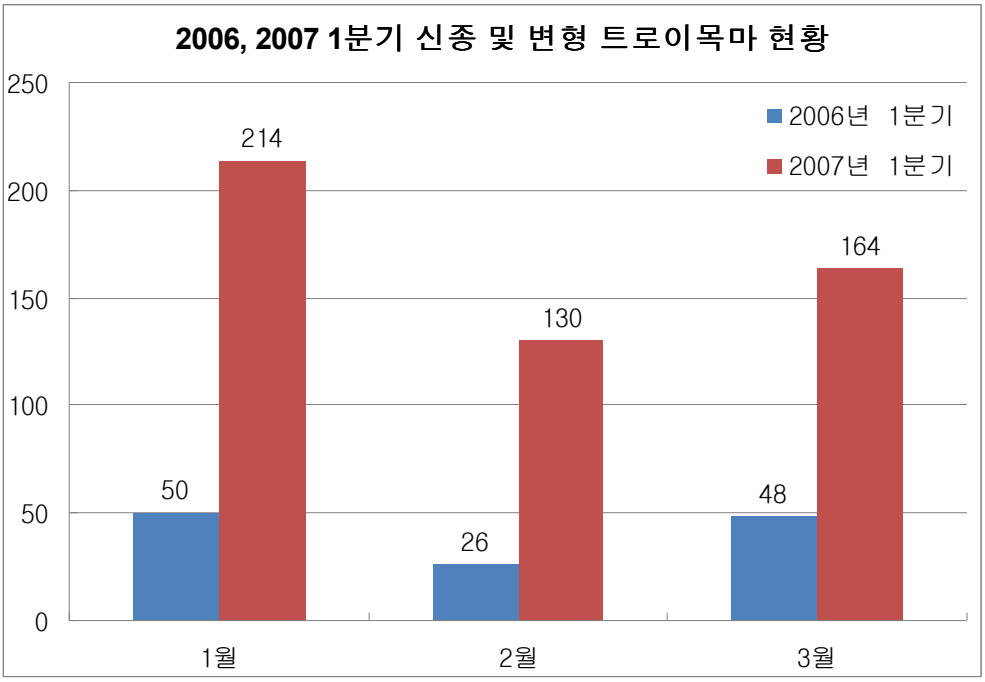
이중에서도 주로 증가 추세를 보이고 있는 중국산 트로이목마 중 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마를 작년 동기와 비교해 보면 [그림 3-2]와 같다.



[그림 3-2] 06, 07년 1/4 분기 온라인 게임의 사용자 계정 탈취 트로이목마 현황

위 그림에도 알 수 있듯이 악성코드의 수는 작년 동기와 비교하여 크게 증가하였으며, 증가 원인으로는 새로운 게임이 나오면서 이를 대상으로 하는 트로이목마의 출현과 기존 온라인 게임의 보안 솔루션이 강화되면서 보안이 비교적 허술한 게임에 대하여 집중적으로 악성코드의 제작이 증가한 것으로 추정된다.

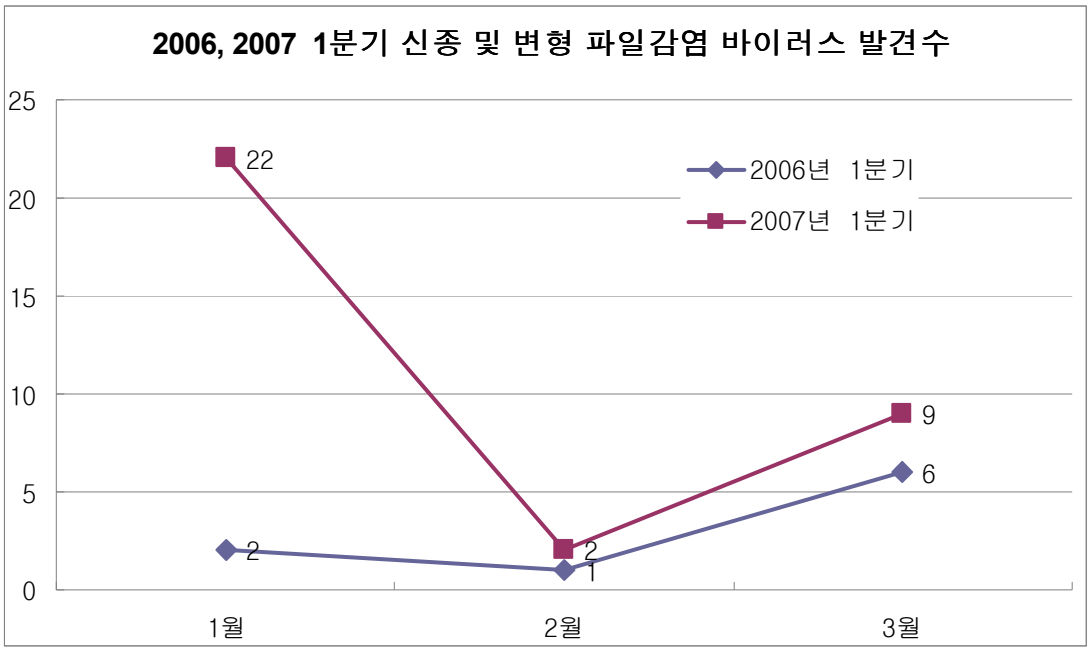
다음 [그림 3-3]은 작년 1분기와 올해 1분기에 발견된 신종 및 트로이목마의 개수를 비교한 것이다.



[그림 3-3] 06, 07년 1분기 신종 및 변형 트로이목마 현황

전체 악성코드의 70% 이상을 차지하는 유형답게 작년 동기와 비교하여 급증한 것을 확인할 수 있다. 국내의 경우 이중 상당수가 위에서 언급한 중국산 트로이목마가 차지하고 있다.

다음 [그림 3-4]는 윈도우 실행 파일을 감염시키는 파일 바이러스에 대하여 전년 동기와 비교한 자료로서 바이러스의 폭발적인 증가 흐름은 지속될 것으로 보인다.



[그림 3-4] 06, 07년 1분기 신종 및 변형 파일 바이러스 발견 수

내부 네트워크 내 파일을 손쉽게 감염 시키기 위해서는 바이러스가 효과적이라는 것은 잘 알려진 사실이다. 특히 중국산 바이러스인 Win32/Viking과 Win32/Dellboy (이하 바이킹, 델보이 바이러스)는 작년 후반기부터 많은 변형이 발견 보고 되었다. 특히 올해 1/4 분기에는 델보이 바이러스의 변형이 특히 더 많이 보고되었으며, 제작자는 금전적인 이득을 목적으로 소스를 판매하기도 하였다. 해당 바이러스의 제작자가 검거된 것이 중국쪽 언론에서 이슈화 되기도 하였다.

다음은 1/4 분기에 이슈 되었던 악성코드들이다.
- 새해인사와 국제적인 이슈를 가장한 - Win32/Stration.worm & Win32/Glowa.worm
- 급격히 변형이 증가한 - Win32/Dellboy
- 리얼 머니를 노렸던 - Win-Trojan/Banki
- 완벽한 은폐형 스팸 메일러 - Win-Trojan/Rustock
- 국내에 많은 감염이 있었던 중국산 트로이목마
- Win32/DellBoy 바이러스 제작자 검거

이중에서 국내에서 피해문의가 많았던 악성코드에 대해서 지난 ASEC 리포트내 글을 인용하여 크게 3가지로 정리하여 알아보기로 하겠다.

► 실행파일 감염 바이러스 증가

올해의 시작도 어김없이 중국산 바이러스가 국내에 큰 피해를 주고 있다. 판다 바이러스라고 일반인들에게 알려진 Win32/Dellboy (델보이) 바이러스 변형은 1/4 분기에 약 25종의 변형이 발견되었다. 또한 작년에 큰 감염보고를 보였던 Win32/Virut 바이러스의 변형인 C, D 형이 출현 하였다. 이전 버전보다 진단/치료가 복잡해졌으며 이는 백신 개발의 지연을 의도 한 것으로 보인다. 또한 바이러스는 감염 후 특정 IRC 서버로 접속하여 팝업광고를 노출하는 애드웨어를 다수 설치 한다. 이는 해당 광고를 통한 금전적인 이익을 노리는 검은 세력과 바이러스 제작자 또는 이들이 바이러스 제작 후 유포하는 등 검은 결탁이 되어 있다고 추정해 볼 수가 있다.

► 악성코드의 자기 보호 기능 고도화

악성코드가 자신의 생존시간을 더 유지 하기 위해서 안티 바이러스의 프로세스를 종료하거나 파일을 삭제하는 건 일반화 되었다. 이제 악성코드는 지능적으로 안티 바이러스나 보안 제품을 우회하여 자신이 진단 되어도 bypass 한다. Win-Trojan/Rustock (이하 러스톡 트로이목마) 이라고 알려진 은폐형 스팸 메일러는 잘 알려진 안티 루트킷 제품이 메모리에 로드되는 순간 이를 탐지하여 은폐 진단을 우회 한다.

다른 사례로 온라인 게임 계정을 탈취하는 일부 중국산 트로이목마는 특정 안티 바이러스의

진단 경고 화면 및 음향을 꺼버리는 등 지능적으로 안티 바이러스를 우회 한다. 또한 이들의 변형중 일부는 사용자 계정을 보호하도록 하는 키보드 보안 솔루션을 무력화 하는등 자신을 보안 제품의 진단으로부터 우회하거나 이를 무력화 시키는 지능적인 악성코드의 출현이 잦았다.

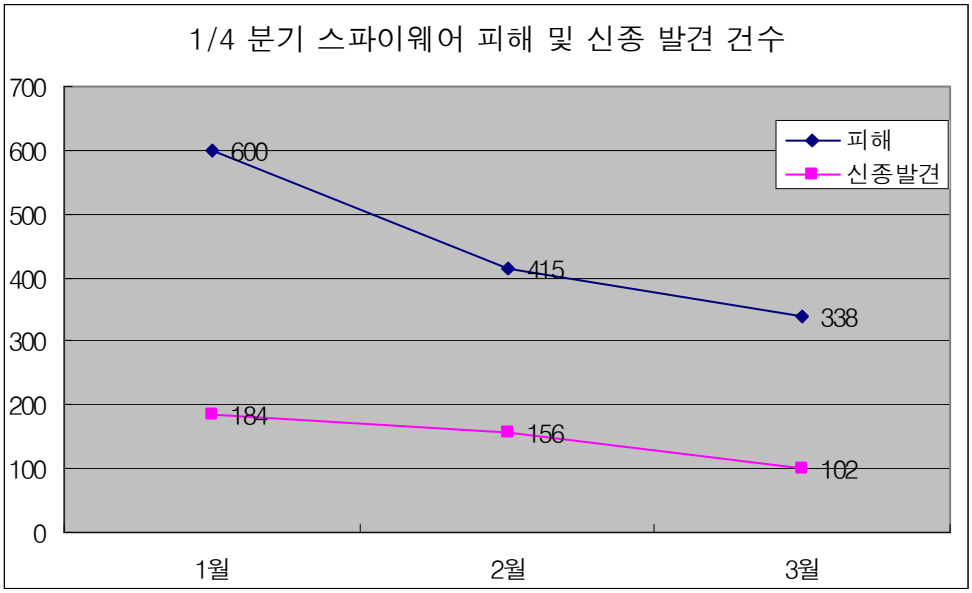
► 리얼 머니를 노렸던 Win-Trojan/Banki

그 동안의 중국산 악성코드의 상당수는 국내 온라인 게임의 타켓으로 사용자 계정을 훔쳐내어 온라인 게임의 사이버 머니 또는 아이템을 훔쳐내는 등 피해를 주었다. 그러나 Win-Trojan/Banki (이하 뱅키 트로이목마) 라고 알려진 이 트로이목마는 국내 유명 은행의 인터넷 뱅킹 접속 사이트를 가장하고 사용자의 공인 인증서도 유출한다. 사실 공인 인증서는 단순히 복사만 하면 다른 곳에서도 사용 할 수 있기 때문에 악성코드에서 이를 쉽게 이용 할 수 있어 문제가 커질 뻔 하였다.

1/4 분기의 전체적인 신종 및 변형의 악성코드에 대한 동향은 새로운 컨셉의 악성코드의 등장 보다는 그 동안 익히 알려졌던 보안위협이 전년 동기에 비하여 큰 폭으로 증가한 것이 큰 특징이다. 트로이목마와 바이러스의 수는 급증하였으며 이는 더 많은 사용자 정보의 유출과 내부 네트워크를 효과적으로 감염시키기 위한 수단으로 활용되었다. 또한 지능적으로 보안 제품을 우회하도록 하는 기법들과 비록 오래 전부터 알려진 유형이라 하더라도 이는 점차 고급기법을 사용하는 형태도 고도화 되었다는 것이다.

위에서 언급되지는 않았지만, 스트레이션 웜과 젤라틴 웜으로 명명된 해당 악성코드들은 변형이 꾸준히 증가 하고 있으며, 안티 바이러스의 에뮬레이터 기능을 우회하도록 에뮬레이터가 인식 할 수 없는 코드를 삽입하기도 하고, 자신의 쓰레드를 정상적인 윈도우 서비스 프로세스 등에 인젝션하고, ndis을 조작하여 자신의 외부와 통신을 우회하도록 하는 등 우리가 모르는 사이에 감염된 시스템이 에이전트나 스팸 메일러 등으로 사용될 수 있도록 만들어 버리는 은밀하고 지능적이며 악의적인 악성코드의 수가 증가 하고 있다는 점에서 전년 동기와 물량적으로 늘어난 차이점 이외에 하나의 특징이 될 수가 있을 것이다.

(2) 2007년 1분기 스파이웨어 동향



[그림 3-5] 2007년 1/4분기 스파이웨어 피해 및 신종발견 건수

[그림 3-5]는 2007년 1/4분기 스파이웨어 피해 및 신종발견 건수를 나타내는 그래프이다. 1월에서 3월로 갈수록 피해 및 신종 및 변형 스파이웨어 발견 건수가 감소하고 있다. 1월에 피해 접수 최고조에 달했던 온라인게임 계정 유출 스파이웨어가 2월, 3월에 들어 감소세를 보이고 있으며, 신종 발견 건수도 감소세를 보이고 있기 때문이다.

1/4분기 스파이웨어의 특징은 다음과 같이 요약할 수 있다.

► 은폐형 스파이웨어, 애드웨어의 증가

루트킷(Rootkit)을 사용하는 국내제작 은폐형 애드웨어가 증가하고 있다. 2006년 한 해 발견된 은폐형 애드웨어는 총 3건 이었으나, 2007년에는 1/4분기에만 벌써 2건이 발견되었다. 이들 애드웨어는 불특정 웹 사이트에서 ActiveX로 설치되며, 파일 및 레지스트리, 프로세스 목록을 숨기기 위하여 루트킷 드라이버를 사용한다. 허위 안티-스파이웨어 프로그램인 씨씨(Win-Adware/Rogue.CC)의 경우 프로세스 및 설치 폴더를 은폐하기 위한 루트킷 드라이버를 설치하는데 제거 방법을 제공하지 않아 감염 피해가 다수 접수되었다. 악성코드뿐만 아니라 스파이웨어도 사용자에 의한 삭제를 회피하고 안티-스파이웨어 프로그램과 같은 보안 프로그램의 탐지를 피하기 위한 목적으로 루트킷 드라이버를 사용하는 사례가 늘어날 것으로 예상된다.

► LSP를 이용한 국내 온라인 게임 계정 스틸러의 출현[1]

국내 온라인 게임을 대상으로 LSP를 사용하여 인터넷으로 송수신 되는 데이터 내용을 가로채 계정을 외부로 유출하는 스파이웨어가 다수 발견되었다. 이들 스파이웨어는 LSP로 등록된 파일만 제거할 경우 정상적으로 인터넷을 사용할 수 없게 되어 다수의 사용자에게 큰 피해를 입혔다. 각종 보안 프로그램으로부터 보호되는 데이터를 유출하기 위해 스파이웨어가 사용하는 방법도 더욱 지능화 될 것으로 예상된다.

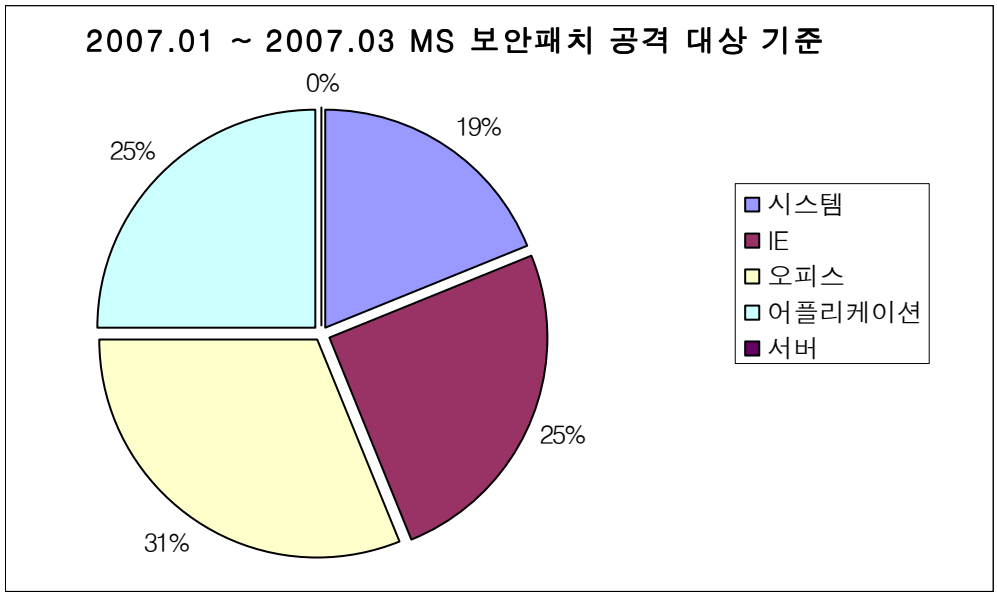
► 전파력이 있는 스파이웨어의 등장

웜이나 바이러스가 기능을 보완하기 위한 목적으로 다운로더를 이용하여 다른 악성코드를 설치하거나 트로미목마를 이용하여 스팸메일을 발송하는 사례는 널리 알려져 있다. 3월 발견된 다운로더 코게임(Win-Spyware/PWS.KorGame.48019)은 기존의 스파이웨어 다운로드 기능에 윈도우 취약점을 공격하고 자신을 전파하는 웜의 기능도 가지고 있다. 스파이웨어는 확산 기능을 가지지 않는 것이 일반적으로 알려진 사실이나, 이번에 발견된 온라인 게임 계정 유출 목적의 스파이웨어는 능동적으로 확산하기 위해 웜의 기능도 가지고 있는 것이 특징이다. 스파이웨어+웜, 애드웨어+바이러스와 같은 복합기능의 악성코드가 증가할 것으로 예상된다.

[1] ASEC Monthly Report 2월호 참조

(3) 2007년 1분기 시큐리티 동향

2007년 1/4 분기까지의 정기 보안 업데이트 내용을 분석하면 발표된 패치는 [그림 3-6]과 같이 총 16건 (1월 4건, 2월 12건)이며 이중 긴급이 9건 (1월 3건, 2월 6건)이다.



[그림 3-6] MS 보안 패치 공격 대상 종류별

2006년 4사분기에는 마이크로소프트 윈도우 관련 어플리케이션 취약점이 총 15건 이었으나 2007년 1사분기에는 총 13건이 발표 되었다. 이것은 전년(2006) 1사분기 기준 어플리케이션 취약점 5건보다는 증가하였다.

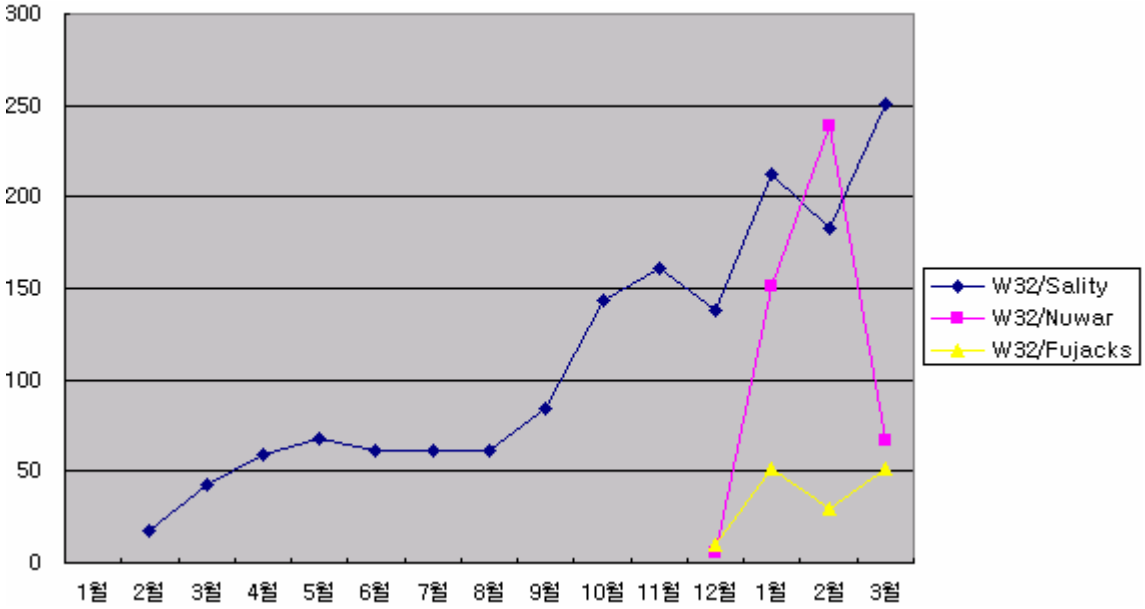
어플리케이션 취약점은 인터넷 익스플로러, 마이크로소프트 오피스 및 기타 어플리케이션 취약점이 있으며, 웹사이트 해킹 후 악성코드 배포 또는 악성코드가 포함된 오피스/아래 한글 파일등을 메일로 보내는 방식으로 공격이 이루어 지고 있다. 또한 국내 인터넷 사이트에서 많이 사용되는 ActiveX 취약점도 늘어나는 추세이다.

이러한 어플리케이션 취약점 공격에 방지하기 위해서는 신뢰되지 않은 사이트 접속 및 오피스/아래 한글 파일이 메일로 첨부해서 오는 경우에 주의가 필요하며, 보안 패치를 반드시 해야한다. 아울러 Anti-Virus 제품 및 개인 방화벽 제품 또한 필요하다.

(4) 2007년 1분기 일본 악성코드 동향

2007년 1분기 일본의 악성코드 동향에서 이슈가 된 사항은 이메일 웜인 누워 웜(Win32/Nuwar, Win32/Zhelatin)의 감염 피해가 대량으로 보고된 것과 살리티(Win32/Sality)와 델보이(W32/Fujacks, Win32/Dellboy)와 같은 파일 바이러스의 감염 피해가 지속적으로 확산되고 있는 것이다.

아래의 [그림 3-7]은 2007년 1분기에 이슈가 된 악성코드들에 대한 2006년 1월부터의 피해 현황을 그래프로 나타낸 것이다.

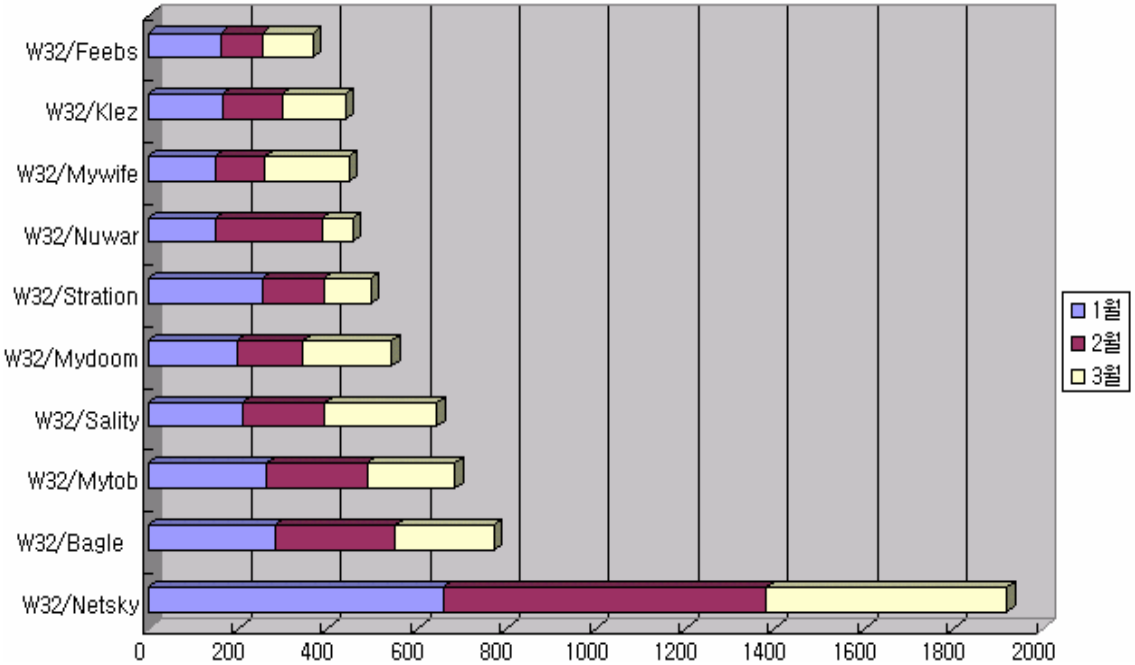


[그림 3-7] 1분기 주요 악성코드 피해 현황 (자료출처 : IPA)

2006년 2월 최초로 발생한 살리티의 피해가 9월 이후 점점 증가하고 있는 것을 알 수 있다. 누워 웜은 은폐기능을 가지고 루트킷(rootkit)을 설치하는 이메일 웜으로써 2006년 12월에 일본에서 처음 발생한 이후 현재까지도 여러 변형된 형태가 보고되고 있다.
최근 많은 피해를 주고 있는 살리티나 델보이와 같은 파일 바이러스들은 대부분 실행파일의 일부에 바이러스 코드를 삽입하는 형태로 감염이 된다. 그러나 이러한 바이러스들은 이전에 발견된 파일 바이러스들처럼 단순하게 실행파일에 바이러스코드를 삽입시키고 자가복제 하는 것을 목적으로 하는 것이 아니라 감염된 특정 사이트에서 파일을 다운로드하여 설치함으로써 개인 정보 유출과 같은 추가적인 피해를 야기한다는 점에서 차이가 있다.
개인 정보의 불법적인 획득 시도는 위에 언급한 바이러스뿐 아니라 최근 유행하는 여러 유형의 악성코드들에서 공통적으로 나타나는 현상으로 그 대상 또한 초기에는 온라인 게임의 사이버머니를 취득하기 위한 것이었으나 현재는 은행과 같은 직접적인 금전 피해가 가능한 기관에까지 확대되고 있으므로 주의가 필요하다.

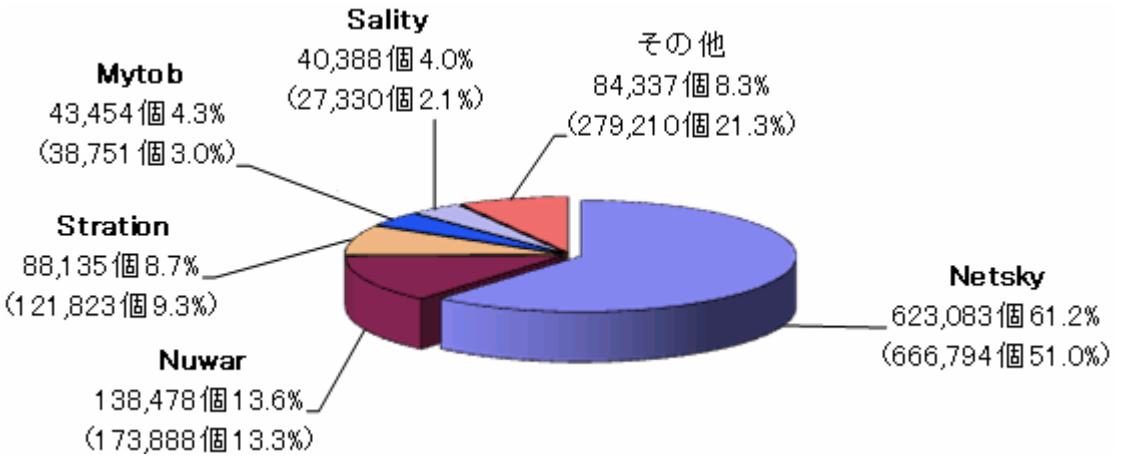
► **악성코드 피해 동향**

2007년 1분기에 일본에서 가장 많은 감염 피해를 입힌 악성코드는 넷스카이 웜(Win32/Netsky)이다. 넷스카이 웜 이외에도 베이글 웜(Win32.Bagle)이나 마이탑 웜(Win32.Mytob)과 같은 메스메일러들에 의한 피해가 많이 발생하고 있고 이러한 점은 이전과 크게 달라진 점이 없다.



[그림 3-8] 2007년 1분기 악성코드 감염 신고 통계 (자료출처 : IPA)

[그림 3-8]의 그래프에서 주목할 점은 2006년 12월 최초로 발견된 누워 웜이 1월과 2월 많은 감염 피해를 기록했으나 3월이 되면서 점점 사라지고 있는 것이다. 감염 피해가 증가한 원인은 다량의 메일을 전송하는 특성으로 인한 가능성이 높다. [그림 3-9]는 2007년 1월에 발생한 악성코드 탐지 현황에 대한 통계로써 누워 웜의 탐지수가 매우 높은 것을 볼 수 있으나, 3월 통계에는 반영되지 않을 정도의 수준으로 급속하게 감소했다.

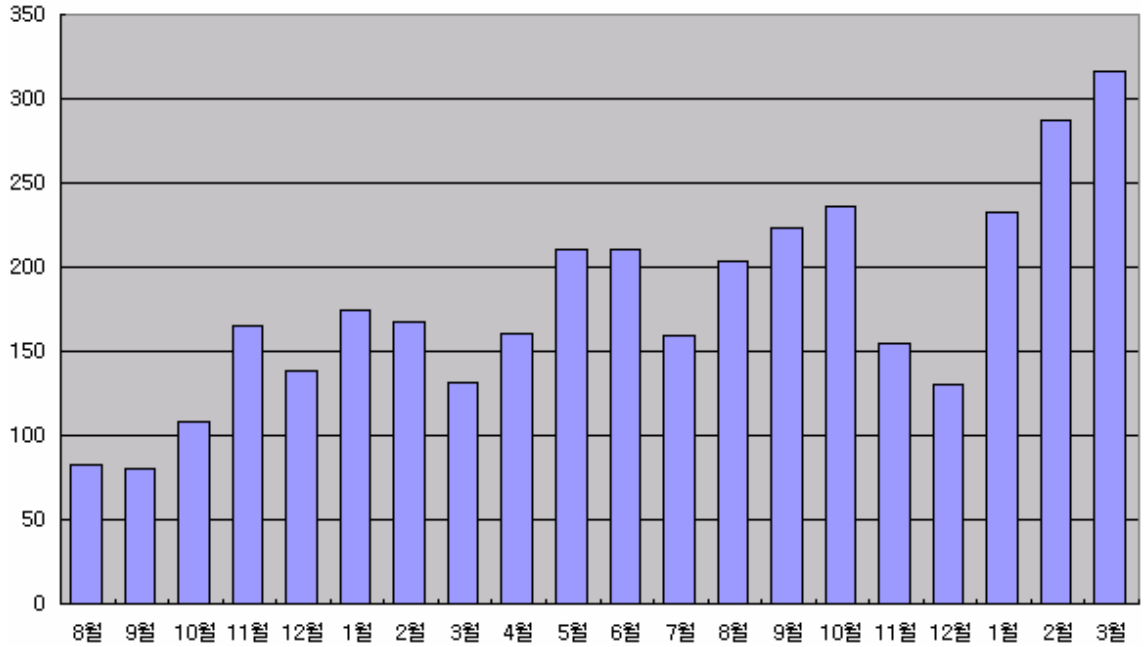


[그림 3-9] 2007년 1월 악성코드 탐지 현황 (자료출처: IPA)

► 온라인상의 불법 청구로 인한 피해 증가

일본의 경우 온라인 상의 불법 청구행위가 사회 문제화가 되기 전부터 비슷한 방법으로 엽서나 전화와 같은 매체를 이용하여 사용자를 속여 금전을 요구하는 행위가 빈번하게 발생하였었다. 온라인을 이용한 불법 청구행위의 경우 2006년부터 이슈가 된 이후 현재까지도 그 피해가 점점 증가하고 있는 추세이다. 주로 이용되는 방법이 사용자가 실제로 사용하지 않은 컨텐츠에 대하여 사용료를 지불하도록 하는 점은 최근 한국에서 발생하고 있는 전화 등을 이용한 사기 행위와 크게 다르지 않다.

아래의 [그림 3-10]은 IPA에서 집계한 월별 불법청구 피해 접수 통계이다. 2005년 이후 피해 건수가 점점 늘어나고 있는 것을 알 수 있고 이후로도 다양한 방법을 이용한 사기 행위로 인한 피해는 점점 늘어날 것으로 생각된다.



[그림 3-10] 불법 가공청구로 인한 피해 통계 (자료출처 : IPA)

(5) 2007년 1분기 중국 악성코드 동향

2006년부터 한국 악성코드 동향은 파일을 감염시키는 바이러스의 부활과 함께 중국발 웹 해킹을 통한 중국산 트로이목마의 유포로 새로운 악성코드 동향을 형성하고 있었다. 이러한 악성코드 대부분이 중국에서 제작된 것으로 추정되나 중국 현지에서는 한국과는 다른 악성코드 동향을 보였었다. 이러한 중국만의 독특한 악성코드 동향은 2007년 1분기에서도 비슷한 양상을 보이고 있다.

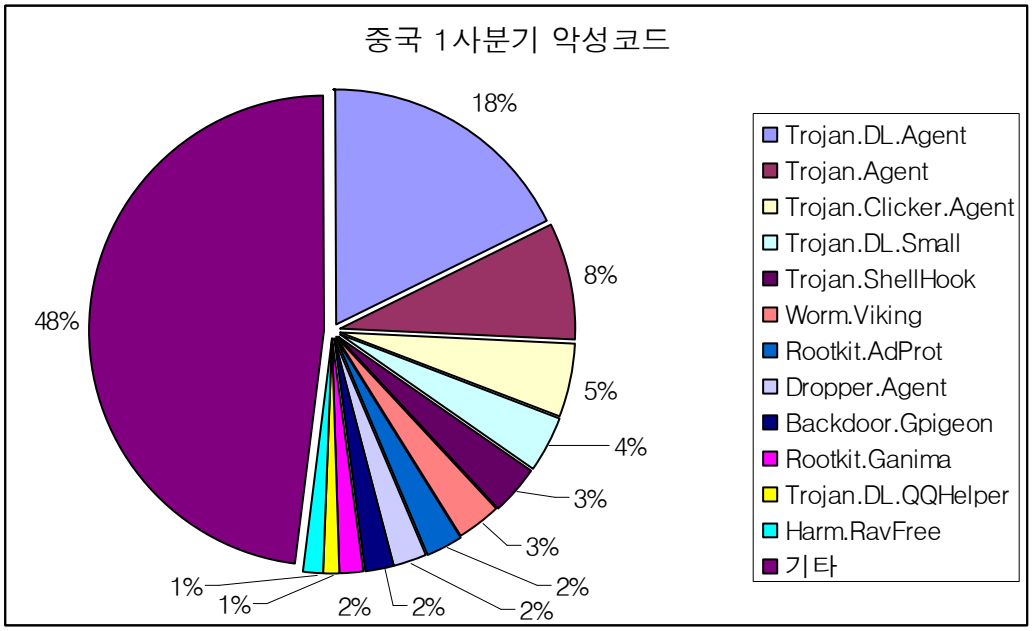
► 악성코드 TOP 10

순위	Rising
1	Trojan.DL.Agent
2	Trojan.Agent
3	Trojan.Clicker.Agent
4	Trojan.DL.Small
5	Trojan.ShellHook
6	Worm.Viking
7	Rootkit.AdProt
8	Dropper.Agent
9	Backdoor.Gpigeon
10	Rootkit.Ganima

[표 3-1] 2007년 1/4 분기 중국 라이징(Rising) 악성코드 TOP 10

[표 3-1]은 2007년 1분기 중국 악성코드 동향으로 중국 쪽에서도 악성코드 중에서 트로이목마류의 강세를 확인할 수 있다. 악성코드 TOP 10 중에서 6위를 차지한 바이킹(Win32/Viking) 바이러스를 제외한 나머지 9건 모두 트로이목마 류의 악성코드가 차지하고 있다. 그리고 특이한 점은 은폐기능으로 인해 일반 사용자들이 쉽게 발견하기 어려운 루트킷 류의 악성코드인 Rootkit.AdProt와 Rootkit.Ganima 2건이 악성코드 TOP 10에 포함되어 있다.

악성코드 TOP 10의 1위에는 2006년 말에 이어 Trojan.DL.Agent(V3 진단명 – Win-Trojan/Agent)가 강세를 보이고 있으며 2월말을 기점으로 감염 문의가 증가 추세를 보이고 있는 Trojan.ShellHook가 5위를 차지하고 있다. 그리고 2005년부터 꾸준히 발견되었던 전형적인 리버스 커넥션 형태의 백도어인 Backdoor.Gpigeon(V3 진단명 – Win-Trojan/Graybird 또는 Win-Trojan/Hupigon) 역시 9위를 차지하면서 꾸준히 감염 신고가 이어지고 있다.

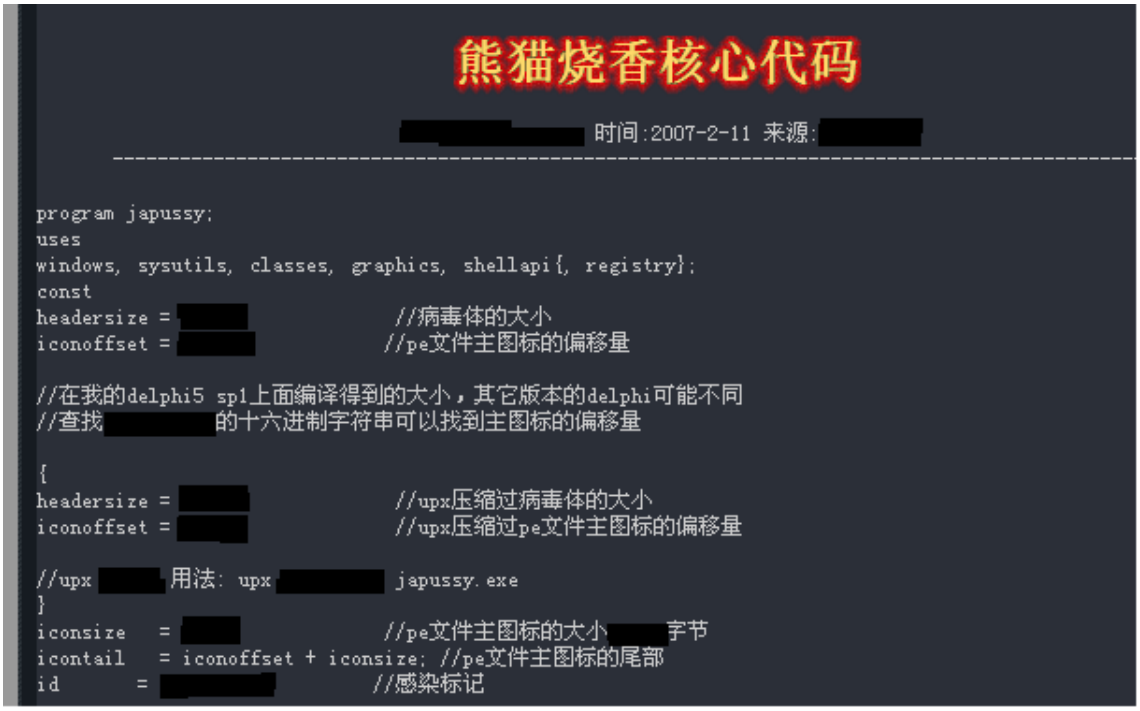


[그림 3-11] 중국 악성코드 TOP 10과 분포

[그림 3-11]은 2007년 1분기 악성코드 TOP 10을 악성코드 비율에 따른 분포로 나타낸 것이다. 악성코드 TOP 10에 포함된 악성코드가 전체 악성코드에서 52%를 차지하고 있으며, 이는 악성코드 TOP 10에 포함된 악성코드에 의해 발생하는 중국 현지 감염 피해가 많다는 것을 의미한다.

► 델보이(Win32/Dellboy) 바이러스 제작자 검거

2007년 2월 12일경 중국 신화사를 통해서 흥미로운 기사가 입수되었다. 그것은 2006년 한 해 동안 많은 피해를 일으킨 델보이(Win32/Dellboy) 바이러스의 제작자가 중국 현지에서 검거되었다는 기사였다. 신화사의 기사에 따르면 중국 우한(WuHan)시에 사는 25세 제작자를 포함하여 총 8명을 중국 공안부에서 체포하였다고 한다. 이들은 델보이 바이러스 및 기타 중국 로컬 인스턴트 메신저 프로그램인 QQ 관련 트로이목마 다수를 제작하고 그 소스코드를 판매한 혐의를 받고 있다고 한다. 이들은 소스 코드 판매를 통해 총 한화 1400만원의 수입을 챙긴 것으로 드러났으며, 얼마나 많은 사람들이 해당 바이러스의 소스코드를 구매하였는지를 입증할 수 있었다.



[그림 3-12] 중국 언더그라운드 웹 사이트에 공개된 델보이(Win32/Dellboy) 코드]

델보이 바이러스 제작자의 검거를 즈음하여 중국 언더그라운드 웹 사이트에서는 유출된 델보이 바이러스의 델파이 소스코드가 공개되었으며 많은 사람들이 해당 바이러스의 소스코드를 보고 가져 간 것으로 보여진다. 이러한 소스코드 유출은 다른 델보이 바이러스 변형의 제작으로 이어질 가능성이 있어 큰 우려가 된다.

(6) 2007년 1분기 세계 악성코드 동향

2007년 1사분기 세계 악성코드 동향은 '여전한 구형 메스메일러 웜과로 지역별 트로이목마' 로 정리 할 수 있다.

영국의 소포스(Sophos) 통계에 따르면 [1] 넷스카이(Netsky), 마이톱(Mytob), 자피 (Zafi), 샐리티(Sality), 마이둠(Mydoom), 베이글(Bagle), 나이젬(Nyxem) 등의 메일로 전파되는 웜들이 순위에 있다. 이들은 모두 발견된지 몇 년이 지난 웜들이다. 2월 통계에서 1위를 차지한 악성코드는 소포스 진단명으로 Mal/HckPk-C로 무려 50.3%를 차지하고 있다. V3에서는 젤라틴 웜(Win32/Zhelatin.worm 변형)으로 진단되며, 2006년 말부터 다수의 변형이 발견되었으며 유사 변형을 소포스에서는 Mal/HckPk-C 로 진단했기 때문으로 순위가 높아진 것으로 보인다. 3월에는 Mal/HckPk-C는 순위에서 사라지고 넷스카이 웜이 1위를 차지한다. 10위에 랭크된 Troj/DwnLdr-GFX는 다른 악성코드를 사용자 모르게 다운로드해 설치하는 다운로더로 스팸 메일로 뿌려졌을 가능성이 높다.

러시아의 카스퍼스키랩(Kaserspky Lab)의 순위도 소포스와 크게 다르지 않다. 다만 3월[2] 1위는 피싱 메일인 Trojan-Spy.HTML.Bankfraud.ra 로 2007년 2월 27일부터 대량으로 발송 된 것으로 보인다. 악성코드 제작자들의 금전적 목적은 점차 강화되어 주로 남미 지역에서 성행하던 온라인 뱅킹 정보 탈취는 점차 세계 각지 유행하기 시작한 것으로 보인다. 메일로 전파되어 순위가 비정상적으로 올라간 악성코드나 피싱에 비해 실제 온라인 백신으로 검사한 검사 순위는 상당히 다르다.

카스퍼스키랩의 온라인 검색 결과에 따르면 2007년 2월 1위는 Mydoom 변형이었고 3월의 1위는 자체 전파 기능이 없는 Padodor 백도어 변형이었다. 7위에 오른 AutoIt 웜 변형은 파이썬으로 작성된 스크립트를 실행 파일로 변환한 형태로 한국에서도 가끔 보고되었다.

순위를 보면 한국과 달리 게임 계정 탈취 프로그램 등은 찾기 어렵다. 온라인 게임의 유행과 온라인 게임 아이템의 현금화가 한국 등 일부 아시아 국가에서 가능하기 때문인 것으로 판단된다. 하지만, 비 아시아 권을 대상으로 2월 슈퍼 볼이 열리는 시점에 슈퍼 볼 관련 웹사이트가 해킹되어 트로이목마가 심어진 사건이 발생[3]하였고, 이를 통하여 온라인 게임인 월드 오브 워크래프트 게임의 로그인 정보와 비밀번호를 빼가는 트로이목마가 설치되었다. 알려진 수법과 트로이목마 형태 등을 보면 중국에서 제작된 것 추정된다. 기존에 중국 악성코드 제작자들은 주로 한국, 중국, 일본의 웹사이트를 해킹해 해당 지역에서 유행하는 온라인

[1] http://www.sophos.com/pressoffice/news/articles/2007/03/toptenfeb07.html, http://www.sophos.com/pressoffice/news/articles/2007/04/toptenmar07.html
[2] http://www.viruslist.com/en/analysis?pubid=204791930
[3] http://www.sophos.com/pressoffice/news/articles/2007/02/superbowl.html

게임 정보를 탈취하는 트로이목마를 뿌렸는데 이례적으로 아시아를 벗어난 지역을 목표로 했으며 게임 종류로 유럽, 미국에서도 인기있는 월드 오브 워크래프트를 목표 했다.

2007년에 발견되는 악성코드 역시 2006년과 같이 유사 변형 대량 발견과 지역화의 고착이다. 2007년에는 매달 거의 1-2만개의 신종 악성코드가 등장하는 것으로 추정되며 특히 한국에서 발견되는 대부분의 악성코드가 중국에서 작성된 것으로 현재 중국에서 제작되는 악성코드는 매달 9천 개 이상으로 추정된다.

IV. ASEC 컬럼

(1) ASEC이 돌아본 추억의 악성코드: 미켈란젤로 바이러스 신드롬

1992년 3월초 세계 언론을 통해 미켈란젤로 바이러스(Michelangelo virus)[1]에 대한 경고가 대대적으로 이뤄졌다.

미켈란젤로 바이러스는 1991년 4월 처음 발견되었으며 우리나라에도 같은 시기에 발견되었다. 감염된 플로피 디스크로 부팅해야 감염되는 부트 바이러스로 윈도우 95 이상의 환경에서는 제대로 활동하지 못하며 최근 출시되는 시스템에서는 미장착 되어 있는 플로피 디스크를 통해 전파되므로 지금은 보기 힘든 과거의 바이러스이다. 이 바이러스는 매년 3월 6일에 하드디스크를 파괴하는 증상이 있으며 첫 활동일인 1992년 3월 6일에 피해가 우려되어 경고가 이뤄졌다.

이미 13일의 금요일에 실행되는 파일을 삭제하는 예루살렘 바이러스(Jerusalem virus)의 첫 활동일인 1987년 11월 13일이나 매년 10월 13일부터 하드 디스크를 포맷하는 데이터범죄 바이러스(Datacrime virus)의 첫 활동일인 1989년 10월 13일에 대한 경고가 지역 언론을 통해 이뤄졌지만 미켈란젤로 바이러스처럼 세계적으로 크게 보도된 건 처음 이었다. 당시에도 발견된 지 1년이 지난 바이러스이므로 백신 프로그램만 잘 사용해도 예방 및 진단/치료가 가능했지만 컴퓨터를 잘 모르는 사람에게는 큰 공포를 줬다. 많은 사람들이 3월 6일이 되면 저절로 바이러스에 감염되어 하드 디스크가 파괴 되는 걸로 오해해 시스템 날짜를 바꾸거나 컴퓨터를 아예 사용하지 않는 일도 발생했다. 하지만, 특정일을 바꾸는 것만으로는 이미 거의 모든 날이 당시 등장한 바이러스들의 활동일이라서 현명한 방법은 아니었다.

언론을 통해 대대적으로 경고된 미켈란젤로 바이러스 특수로 상당수 백신업체가 엄청난 매출 신장을 올렸다고 한다. 이에는 언론과 함께 백신 업체의 위험성 과장도 한 몫 했다. 바이러스 블레틴(Virus Bulletin)[2]에 따르면 당시 미국의 한 백신업체는 최소 500만 대의 컴퓨터가 이 바이러스에 감염되어 있다고 밝혔지만 실제 피해는 1만 대 정도로 추정된다고 한다. 미켈란젤로 바이러스 신드롬으로 백신업체는 엄청난 매출 신장을 기록했지만 백신 업계 내부에서 사람들에게 공포심을 줄 수 있는 과장된 내용은 자제하자는 업계 룰이 성립된 시기였다.

미켈란젤로 바이러스 신드롬은 긍정적인 측면에서 컴퓨터 바이러스를 잘 모르던 일반인들도 언론을 통해 컴퓨터 바이러스에 대해 알게 되었고 미켈란젤로 바이러스 활동일을 계기로 많

[1] http://kr.ahnlab.com/info/smart2u/virus_detail_136.html
[2] http://www.virusbtn.com

은 사람들이 백신 프로그램으로 자신의 시스템을 검사해 보게 되었다는 점이다. 하지만, 언론을 통한 자극적인 내용은 사람들에게 컴퓨터 바이러스에 대한 필요 이상의 공포심을 주게 되었으며 사용자들의 보안을 책임지고 안심시켜야 할 보안업체에서 상업적 이익을 위해 공포심을 배가 시킬 수 있다는 부정적 측면이 존재한다. 다행히 보안 업계의 자정 노력으로 이후 불필요한 언론 경고를 하는 업체는 비판의 대상이 되고 있는데, 1999년 말 컴퓨터가 2000년을 인식하지 못해 혼란이 발생할 수 있다며 Y2K 문제가 한창 일 때 실체가 모호한 Y2K 바이러스 소동으로 또 한차례 백신 업체들 사이에 불필요한 경고 논쟁이 발생하였다.

(2) 커널 스팸 메일러 Rustock

2005년 이후 악성코드의 커다란 변화는 커널모드 루트킷(Rootkit)의 사용이 빈번해지고 있다는 것이다. 뿐만 아니라 2006년부터는 그 기법이 매우 정교해지고 고급화되어 안티바이러스 업체나 분석가로 하여금 상당한 시간과 노력을 투자하게 만들고 있다. 2006년 VB(Virus Bulletin) 9월호 'ROOTKIT ANALYSIS' 기사에는 최근의 진보된 루트킷 하나를 다루고 있어 흥미를 주었는데, 바로 'Rustock'이라 불리는 커널 스팸메일러 였다.

1. Rustock 이란?

커널스팸메일러인 Rustock은 생성된 커널드라이버에서 제작자가 붙인 이름(Rustock rootkit v 1.2)과 프로젝트명 (Z:\NewProjects\spambot\new\driver\objfre\i386\driver.pdb)을 찾을 수 있다. 러시아인으로 보이는 제작자는 커널 루트킷 커뮤니티에서 활동하며 다양한 기법을 연구, 발전시켜 2005년 12월 초기버전을 제작하고 2006년 7월까지 4차례 버전업데이트를 하면서 배포한 것으로 보인다.

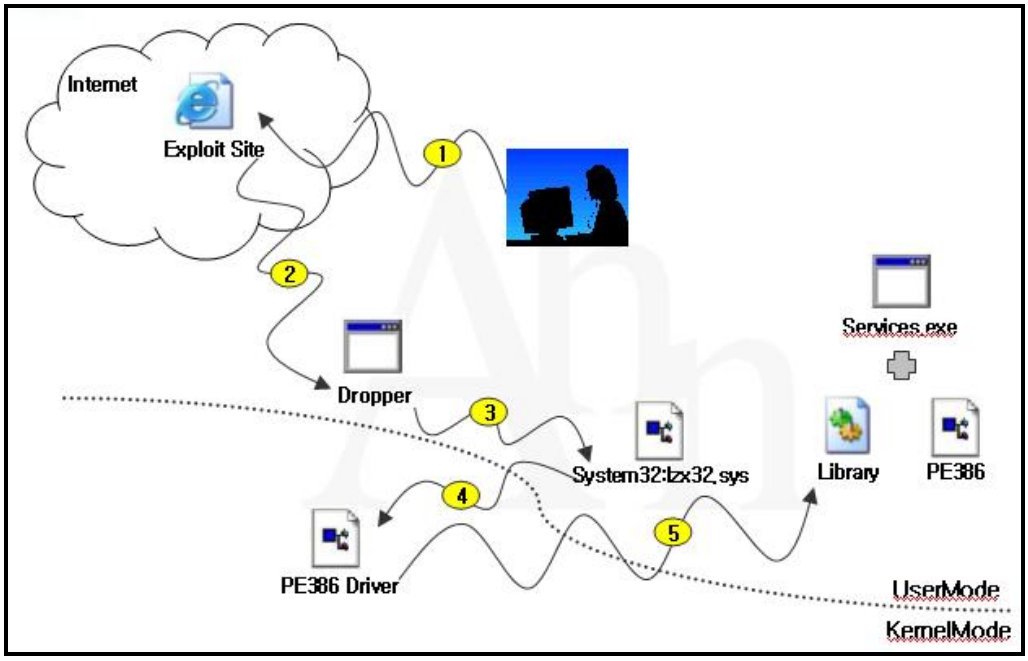
Rustock은 윈도우 커널모드 루트킷과 유저모드 라이브러리로 구성되며 사용자 몰래 동적으로 생성한 스팸메일을 발송하고, 외부로부터 명령을 받아들일 수 있도록 통신포트를 오픈한다. 자체 프로세스가 존재하지 않으며 윈도우 네트워크 시스템 모듈을 변조하기 때문에 모니터링 도구나 스캔도구를 통하여 검출되지 않는다. 뿐만 아니라 그 자체가 파일로 존재하지 않도록 NTFS ADS(Alternate Data Streams)에 기록하여 안티바이러스의 파일 감지를 피하도록 하였다.

2. 감염 방법

기본적인 감염방법은 아래 [그림 4-1]과 같을 것으로 추정된다.

① 사용자가 해킹된 웹사이트에 접속한다.
② 보안취약점을 통하여 사용자 PC에 드랍퍼(Dropper)가 다운로드 된다.
③ 드랍퍼(Dropper)가 실행되고 Rustock을 NTFS ADS에 생성한다.
④ 서비스 등록 및 실행이 되어 커널모드 루트킷이 동작한다.
⑤ Services.exe에 라이브러리(A.DLL)을 인젝션(Injection)시킨다.
⑥ 스팸메일 발송 및 외부접속 대기한다.

커널의 루트킷은 파일, 레지스트리, 오브젝트, 네트워크 등을 은닉시키는 진보된 기술을 사용하며, Services.exe에 인젝션되어진 라이브러리는 스팸발송과 백도어로서의 기능을 수행한다.



[그림 4-1] Rustock 감염 경로

3. 진보된 기술 및 기법

1) 다형성(Polymorphic) / 실행압축

다운로드된 드랍퍼(Dropper)뿐만 아니라 NTFS ADS(Alternate Data Streams)에 기록된 %WINDIR%\System32:lzx32.sys는 다형성으로 실행압축 되어있다. 이 다형성의 기본 골격은 잘게 쪼개진 루틴들로 이루어져 있으며 PUSH / RET 방식으로 호출되며, 이러한 방식을 스파게티(Spaghetti) 알고리즘이라 한다.

지금까지의 커널모드 악성코드(Rootkit)는 단순히 유저모드의 악성코드 프로세스나 레지스트리를 은닉하기 위해 사용되었으며, 실행압축과는 거리가 먼것으로 생각되어져 왔다. 이는 실행압축 해제에 필요한 Kernel32.dll의 Export 함수인 LoadLibrary(), GetProcAddress()등의 함수를 사용할 수 없다는 것이 문제였기 때문이다. 그러나 Rustock은 커널모드의 ntoskrnl.exe의 Export 함수인 ExAllocatePool(), ExFreePool(), ZwQuerySystemInformation(), _stricmp()의 함수포인터를 구하여 압축해제에 사용하였다.

[그림 4-2]는 커널모드에서 Ntoskrnl.exe의 로드이미지 주소를 얻기위해 사용된 방법이다. 드라이버 로딩의 주체는 System 프로세스(ProcessID 4)이며 FS:[--][1]은 System 프로세스의 NonPagePool Inherited Usage 주소 즉, IDT(Interrupt Descriptor Table)를 가리킨다.

[1] 오용을 막기 위해 정확한 표기는 생략한다.

IDT에는 인터럽트 서비스 포인터가 존재하며, 그 포인터는 Ntoskrnl.exe의 코드영역을 가르키고 있어 Ntoskrnl.exe의 로드이미지를 얻을 수 있다.

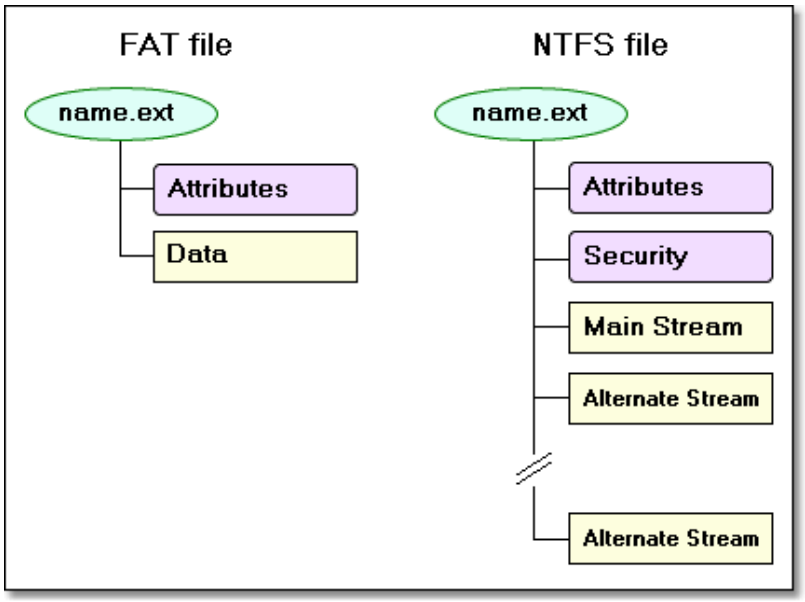
```
< Kernelmode ntoskrnl.exe >

60              PUSHAD
E800000000      CALL    XXXXXA90
5D              POP     EBP
83ED06          SUB     EBP,06
64A138000000    MOV     EAX,FS:[[redacted]]
8B4004          MOV     EAX,[EAX+04]
30C0            XOR     AL,AL
2D00010000      SUB     EAX,00000100
6681384D5A      CMP     WORD PTR [EAX],5A4D
75F4            JNZ     XXXXXA9F
0FB7583C        MOVZX   EBX,WORD PTR [EAX+3C]
813C1850450000  CMP     DWORD PTR [EBX+EAX],00004550
75E7            JNZ     XXXXXA9F
```

[그림 4-2] 커널모드에서 Ntoskrnl.exe의 로드이미지 주소 획득

2) NTFS ADS(Alternate Data Stream)

NTFS 파일 시스템의 중요한 특징은 파일과 폴더에 대해서 보안과 스트림(Stream) 적용을 추가하여 FAT 파일 시스템보다 효율적이고 안정적인 구조를 설계한 데에 있다.



[그림4-3] FAT와 NTFS 비교

Rustock에서는 시스템폴더의 ADS(Alternate Data Stream) 영역에 파일(%WINDIR%\System32:lzx32.sys)을 생성하고 SCM(Service Control Manager)으로 하여금 서비스 등록

과 실행을 하도록 하고 있다. 그리고, 안티디텍션(Anti-Detection)방법으로 FileObject의 AccessState를 변경하여 ADS 접근을 제한하고, IoCallDriver API를 후킹(Hook)하여 System32:lzx32.sys에 대한 접근(IRP_MJ_CREATE, IRP_MJ_DIRECTORY_CONTROL)의 IRP 요청에 대해서 거짓정보를 리턴(STATUS_OBJECT_NAME_NOT_FOUND)함으로서 자신을 은닉시킨다.

3) System Service Call Hook

유저모드(UserMode)의 Ntdll.dll, User32.dll, Gdi32.dll[1]은 커널모드(KernelMode) 시스템 서비스를 요청할 때, 다음과 같은 두 가지 방법을 사용한다.

① INT 0x2E (Interrupt 0x2E) - Windows NT, 2000
② SYSENTER (IA32_SYSENTER_EIP Register) - Windows XP 이상

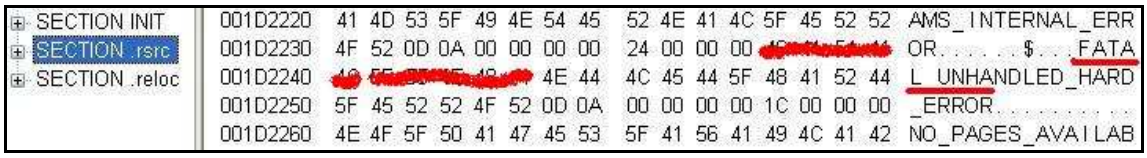
[그림 4-4]는 Intel CPU에서의 MSR(Model Specific Registers) 레지스터를 소프트아이스에서 불러온 이미지이다. SYSENTER 서비스에 대한 CS:IP 주소가 존재하는 MSR 레지스터의 0x174(IA32_SYSENTER_CS)와 0x176(IA32_SYSENTER_EIP)에 대한 포인터를 Ntoskrnl.exe의 .rsrc Section의 특정위치(FATAL_UNHANDLED_HARD_DRROR)로 후킹(Hook)하고 문자열(FATAL) 5바이트는 JMP XXXXXXXX (E9XXXXXXXX)로 대체된다.

IDT(Interrupt Descriptor Table)의 0x2E Entry는 NT_SYSTEM_SERVICE_NT로 정의된 시스템 서비스 진입점 포인터가 존재한다. 바로 INT 0x2E로 불리는데 이에 대한 포인터를 역시 Ntoskrnl.exe의 .rsrc Section의 특정위치(FATAL_UNHANDLED_HARD_DRROR)로 후킹(Hook)하고 문자열(_UNHA) 5바이트는 JMP XXXXXXXX (E9XXXXXXXX)로 대체된다.

[그림 4-4] 소프트아이스에서 MSR 레지스터

[그림 4-5]는 Ntoskrnl.exe의 .rsrc Section 내에서 후킹된 INT 0x2E와 SYSENTER가 가리키는 주소로 이곳은 다시 루트킷에 의해 JMP 코드로 덮어 씌워진다.

[1] 유저모드와 커널모드 사이의 다리역할을 하는 서브시스템(Subsystem)



[그림 4-5] Ntoskrnl.exe의 .rsrc Section

후킹설치가 끝나고 나면 루트킷 드라이버는 Ntoskrnl.exe의 코드영역에서 참조되는 모든 SYSENTER 참조포인터를 후킹된 주소로 교체하는 작업을 한다. 이와 같이 INT 0x2E와 SYSENTER를 후킹한 이유는 특정 서비스 함수에 대한 후킹이 목적이다. 하지만 Rustock은 정작 각각의 서비스 함수에 대한 후킹을 하였던 기존의 루트킷의 방법인 SSDT(System Service Dispatch Table)의 서비스 함수 후킹을 사용하지 않는다. 이유는 많은 루트킷 디텍션(Detection)툴들이 시스템의 SSDT(System Service Dispatch Table)의 포인터들을 검사하여 루트킷의 존재를 검사하기 때문이다. Rustock은 실제로 자신이 후킹하고자하는 서비스 함수는 정해져 있기 때문에 INT 0x2E와 SYSENTER를 후킹하고 복제본의 SSDT에서 자신이 목적으로 하는 서비스 함수일 경우에만 특정주소로 분기하게 만들었다.

다음은 복제된 SSDT에 후킹 서비스 주소를 등록하는 서비스 함수들이다.

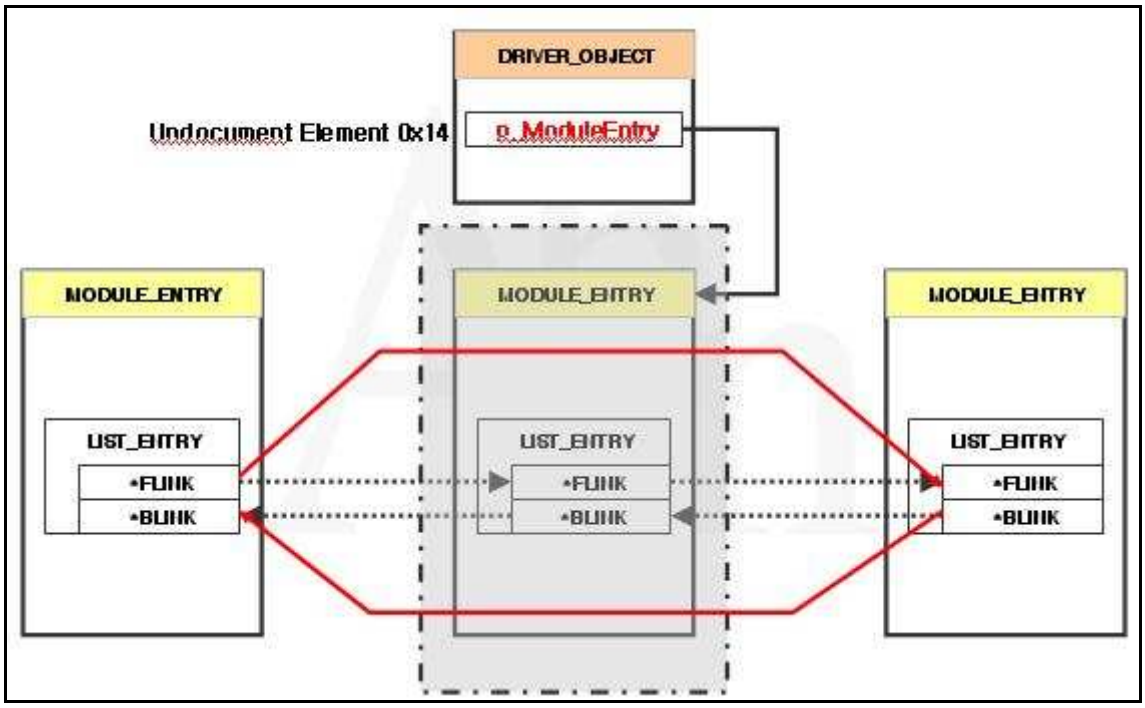
A. ZwOpenKey, ZwEnumerateKey, ZwQueryKey, ZwCreateKey
B. ZwSaveKey, ZwDeviceIoControlFile
C. ZwQuerySystemInformation
D. ZwTerminateProcess

IofCallDriver는 서비스 함수가 아니어서 Ntoskrnl.exe의 EAT(Export Address Table)에서 직접 후킹 등록한다.

4) DKOM

커널메모리에서 유지, 관리하는 모든 오브젝트(Object)는 이중연결리스트(Double Linked List)인 원형큐(Circular Queue)로 구성되어있는데, DKOM(Direct Kernel Object Manipulation) 기법은 이 연결리스트의 연결고리를 끊어 특정 오브젝트를 은닉하도록 하는 방법이다.

[그림 4-6]은 특정 커널 드라이버 오브젝트에 대한 은닉그림이으로 DKOM 방식은 메모리 보호, 대상 오브젝트 포인터획득, 오브젝트 구조의 이해 등 많은 관련지식을 필요로 한다.



[그림 4-6] 커널 드라이버 오브젝트 은닉

Rustock은 DKOM 방식을 사용하여 다양한 커널 오브젝트를 변경하는데 그 중에서 서비스 오브젝트는 SCM(Service Control Manager)인 Services.exe 프로세스가 관리하는 서비스 오브젝트 전역변수를 메모리에서 찾아내 링크를 따라가며 자신의 서비스 오브젝트명(PE386)을 찾아 관련 링크를 해제시키는 방법을 사용하였다.

[그림 4-7] DKOM 방식으로 services.exe 변경

5) Asynchronous Procedure Call

Rustock은 커널 루트킷(Rootkit)과 시스템 프로세스인 Services.exe에 인젝션된 라이브러리로 구성된다는 것은 이미 서두부분에서 언급하였다. 문제는 인젝션된 라이브러리는 어디로부터 나와서 어떻게 Services.exe의 가상메모리에 로드되어지며 어떻게 구동되느냐? 하는 것이다.

Windows는 유저모드 애플리케이션과 커널모드 드라이버간의 데이터 교환을 위해 DeviceIoControl이라는 API 함수를 사용한다. 드라이버는 DeviceIoControl에 대한 리턴버퍼를 통해서 유저모드 애플리케이션에 데이터를 전송할 수 있다. 또는 이벤트(Event)를 사용한 메모리매핑(MemoryMapping)을 이용할 수도 있다. 하지만 이 방법들로는 드라이버가 유저모드의 특정 프로세스공간에 라이브러리를 로드시키고 함수를 호출하는 것이 불가능하다.

다음의 함수는 Ntoskrnl.exe에서 Export하는 Undocument API 함수이다. 인자값은 EPROCESS 포인터이며 해당 프로세스로의 Context Switch가 동반된다. 즉, 현재 프로세스의 가상메모리 번지지정을 담당하는 CR3 레지스터가 EPROCESS가 가리키는 가상메모리 번지로 변경된다는 것이다. 그러므로 Services.exe의 가상메모리 공간에 메모리를 할당 받을 수 있게 된다. Rustock 드라이버는 시스템폴더 ADS(System32:lzx32.sys)의 마지막 부분을 읽어 들이고 복호화 과정을 거친 뒤, Services.exe의 할당된 메모리 공간에 복호화된 라이브러리 데이터를 옮겨 심는다. 즉, 실행파일(PE파일)에 대한 메모리 적재를 수행하는 시스템 로더(Loader)의 역할을 Rustock은 내부적으로 가지고 있다.

```
NTSTATUS KeAttachProcess(PEB *);
```

다음의 함수들은 Services.exe에 적재시킨 라이브러리의 함수를 호출할 수 있는 방법을 제공하는 API들이다. 굵게 표시된 부분은 실제 라이브러리의 특정함수 포인터와 파라미터 인자값들이다. Services.exe의 메모리 영역에 복사된 라이브러리는 시스템의 IRQL Level이 APC가 되었을 때에 호출된다.

```
VOID KeInitializeAPC (   struct _KAPC              *APC,
                         PKTHREAD                  thread,
                         PKKERNEL_ROUTINE          ker_routine,
                         PKRUNDOWN_ROUTINE         rd_routine,
                         PKNORMAL_ROUTINE          nor_routine,
                         Unsigned char             mode,
                         Void                      *context );

VOID KeInsertQueueApc( struct _KAPC               *APC,
                         Void                      *SysArg1,
                         Void                      *SysArg2,
                         Unsigned char             arg4 );
```

Services.exe에 인젝션(Injection)된 라이브러리 함수 rd_routine가 호출되면 초기화 과정을

거친 뒤, 스팸메일 발송과 백도어로서의 역할을 시작하게 될 것이다. (악용될 소지가 있어 상세한 기법은 소개하지 않는다.)

```
VOID rd_routine( ULONG *context, ULONG *SysArg1, ULONG *SysArg2 );
```

6) Network System Patch

윈도우 NT의 네트워크 구조의 뼈대를 이루는 것이 NDIS(Nerwork Driver Interface Specification)라고 하는 커널 네트워크 라이브러리로서 마이크로소프트와 3Com사가 공동 개발하여 네트워크 하드웨어개발의 공통 인터페이스를 제공하도록 제작되었다. 윈도우 네트워크 시스템은 바로 NDIS.SYS 드라이버 라이브러리의 익스포트함수(Export Function)를 이용하여 통신하게 된다.

Rustock은 스팸메일 발송과 외부접속에 따른 네트워크 통신을 은닉하기 위해서 윈도우 네트워크 시스템의 드라이버 파일(WanArp.sys, Tcpip.sys)을 패치(Patch)한다. Tcpip.sys와 WanArp.sys 모듈 내부의 .text 섹션(Section)에서 다음과 같은 바이너리 OP 코드를 찾아 변경한다.

① Tcpip.sys 코드영역 (FF 70 04 FF 50 30 => E8 XX XX XX XX 90)

② WanArp.sys 코드영역 (FF 75 14 50 FF 50 54 => E8 XX XX XX XX 90 90)

패치된 바이너리 코드는 네트워크 접속(Connection)이 이루어지는 곳으로 판단되며, 후에 스팸메일 발송과 외부접속에 따른 데이터 위/변조를 위한 함수코드로 디투어패치(Detour Patch) 된다.

[그림 4-8] Tcpip.sys에 대한 Detour Patch

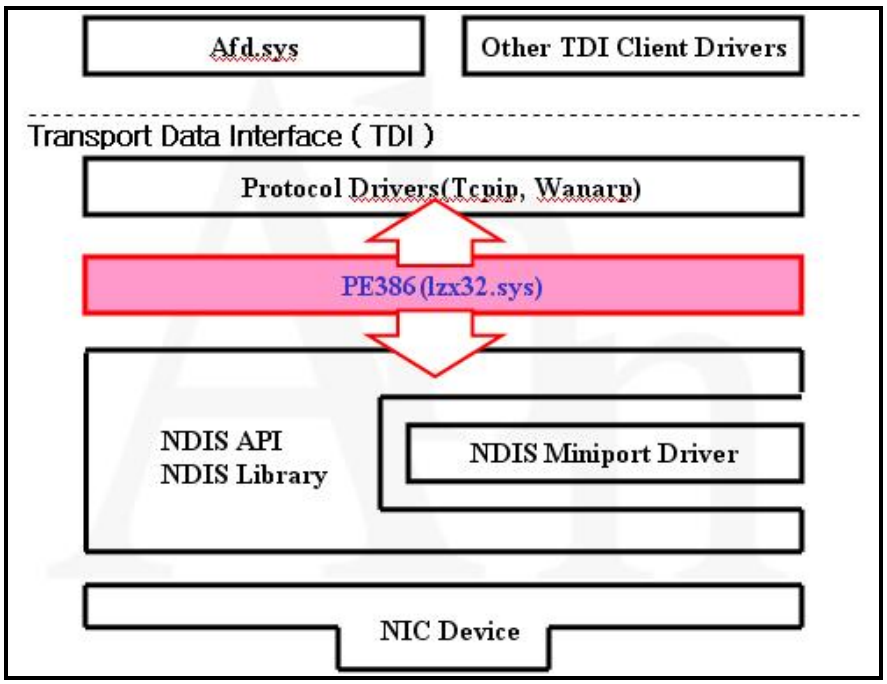
Tcpip.sys 프로토콜 드라이버에 대해서는 다음의 함수에 대해서 IMPORT Address Table에 대한 변경으로 IAT 후킹을 더하였다.

① NdisCloseAdapter

② NdisOpenAdapter

[그림 4-9]는 윈도우의 네트워크 시스템에 대해서 형상화한 것이다. Rustock은 Tcpip, WanArp 프로토콜 드라이버의 NDIS_PROTOCOL_CHARACTERISTICS 구조체를 변경하여 네트워크 통신 콜백(CallBack) 함수에 대한 후킹을 시도한다.

Rustock 루트킷 드라이버(PE386)는 TDI(Transport Data Interface) 이하 프로토콜(Protocol) 드라이버 단에서 네트워크 패킷(NDIS_Packet)에 대한 Send/Receive 핸들러를 통하여 Services.exe에 인젝션(Injection)시킨 라이브러리(A.DLL)의 스팸메일, 백도어(Backdoor) 통신을 방화벽(Firewall), 모니터링(Monitoring)으로부터 우회하도록 하였다.



[그림 4-9] 윈도우의 네트워크 시스템

7) 스팸메일

스팸메일을 발송하고 외부연결을 위한 백도어 포트를 오픈하는 것은 모두 시스템 프로세스인 Services.exe에 인젝션된 라이브러리(A.DLL)에서 담당한다. 스팸메일을 생성하고 발송하는 순서는 다음과 같다.

① 다음의 확장자를 가진 파일에서 전송대상 메일주소를 추출한다.
(wab,tbb,tbi,doc,xls,txt,csv,htm,html,xml,adb,asa,asc,asm,asp,cgi,con,csp,dbx,dlt,dwt,edm,hta,htc,inc,jsp,jst,lbi,php,rdf,rss,sht,ssi,stm,vbp,vbs,wml,xht,xsd,xst)

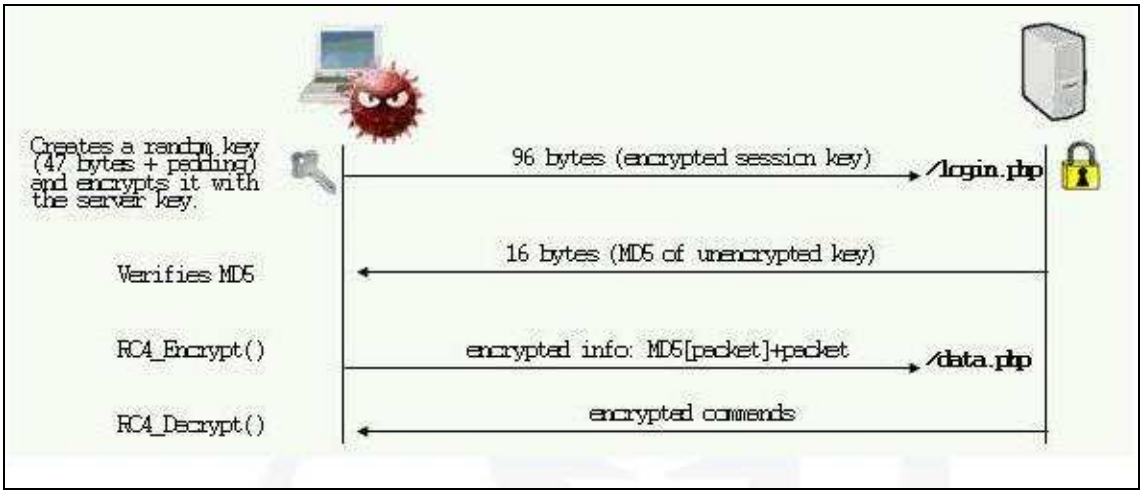
② 추출된 메일주소 중에서 다음의 문자열이 포함된 주소는 제외시키는 것으로 판단된다.
(admin,info,support,soft,webmaster,help,web,postmaster,root,bugs,rating,site,contact,privacy,service,abuse,register,sales,cisco,gnu.org,bsd.it,debian,linux,Berkeley,google,fido,ibm.com,Microsoft.com,php.net,.mil,.gov,borland.com,sun.com,xinul.com,virus,kaspersky,sophos,ripe.,iana.,drweb,secure,avp.,.arpa)

③ 다음의 단어들에 대한 Google 검색을 통해서 메일본문을 동적으로 생성한다.
(download,free,stuff,forum,politic,soft,crack,news,love,leave,games,enter,book,music,sport,console,editor)

④ SMTP(mx1.mail.yahoo.com) 서버에 스팸메일을 전송한다.

8) 백도어(Backdoor)

외부연결 포트 오픈 역시 시스템 프로세스인 Services.exe에 인젝션된 라이브러리(A.DLL)에서 이루어진다. 외부연결에 따른 모니터링 및 감지를 피하기 위해 라이브러리에서는 자체 암호화를 사용하는 것으로 보인다. 다음의 [그림 4-10]은 시만텍 자료에서 추출한 백도어 공격 세션연결 통신에 대한 그림이다. 감염된 시스템에 접속하기 위해 암호화된 키로 구성된 HTTP 세션 연결을 시도한다. 인증이 성공되면 RC4 암호화 데이터로 통신을 유지하는 것으로 보인다.



[그림 4-10] 백도어 공격 세션 연결 통신

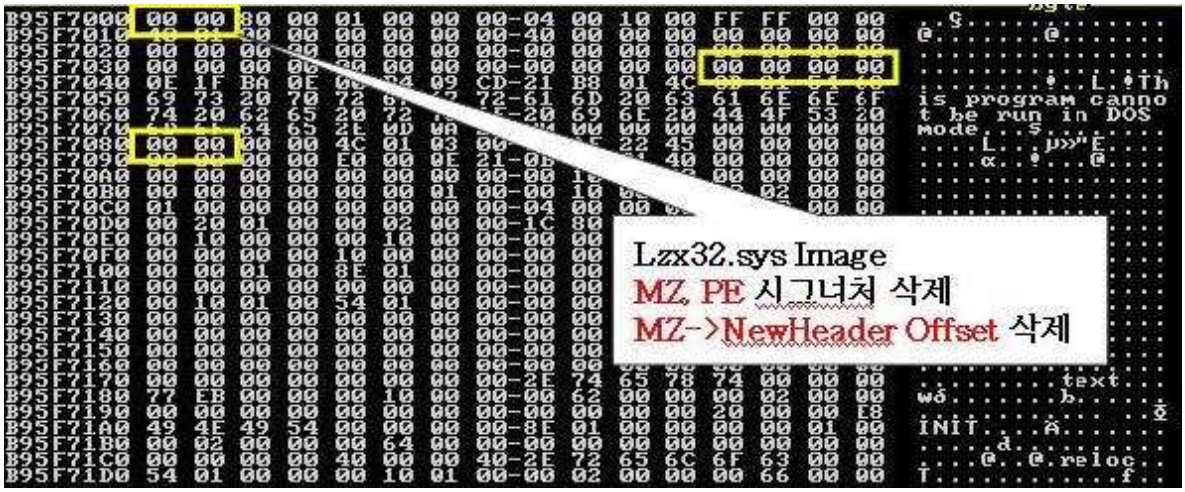
9) 그 밖의 기법들

지금까지 열거한 기법들은 상세분석 당시에 이제까지 다른 악성코드에서 보지 못하였거나 특이한 기법들에 대해서 분석한 내용을 기술한 것이다. Rustock에서는 이외에도 많은 안티디버깅, 안티디텍션, 정보은닉 등의 방법이 사용되었으며 몇 가지를 열거하면 다음과 같다.

① 새로 메모리에 로드되는 모듈에 대한 검사를 통해 디텍션툴을 감지 (Rootkitrevealer, BlackLight, PKDetector, gmer, endoscope, DarkSpy, Anti-Rootkit)
② Kaspersky 커널 방화벽 모듈 무력화 (klif.sys)
③ 안티디텍션(Anti-Detection)을 위해 로드된 자체 모듈(lzx32.sys, A.DLL)에 대한 MZ, PE, NewHeader Offset에 대한 삭제. [그림 4-11] 참조.
④ 안티디버깅을 위한 VM-ware, Virtual PC, Softice 감지 (vmscsi.sys, vmx_fb.dll, vmmouse.sys, vmx_svga.sys, siwvid.sys, siwsym.sys, ntice.sys)

⑤ 안티디텍션을 위한 레지스트리 백업 및 복구

- ZwSaveKey, ZwDeviceIoControlFile에 대한 서비스호출 시, 레지스트리키 “HKLM\SYSTEM\CurrentControlSet\Services\PE386” 를 삭제/백업 한 후, 리턴 될 때 다시 복구하는 방법으로 은닉



[그림 4-11] 안티디텍션을 위한 자체 모듈에 대한 MZ, PE, NewHeader Offset 삭제

4. 결론

이제까지 Rustock.B라 불리는 커널스팸메일러에 대해서 분석한 결과를 설명하였다. 현재 V3 엔진에는 안정화 문제가 남아있어 적용되지 않았으나, 웹페이지에서 다운로드 가능한 전용백신에는 진단, 치료가 적용되어 있다. 완벽하고 안정적인 진단/치료를 위해서는 아직 더 많은 시간과 노력이 필요할 것으로 보인다. Rustock은 자체 중복감염을 이벤트 오브젝트(Event Object)를 통해서 하기 때문에 사용자들은 이를 이용하여 감염여부를 알 수 있을 것으로 보인다.

Ex> HANDLE OpenEvent(DWORD *dwDesiredAccess*, // access flag
BOOL *bInheritHandle*, // inherit flag
LPCTSTR *lpName* // {DC5E72A0-6D41-47e4-C56D-024587F4523B});

(위의 함수를 사용하여 Rustock이 사용하는 GUID 이벤트 핸들을 획득한다면 시스템에 벌써 감염되어 있는 경우이다.)

국내에는 현재 얼마나 많은 시스템이 감염되어 있는지 보고된 바가 없다. 기업의 경우 게이트웨이나 라우터를 통해서 과다한 SMTP 트래픽이 발생하는 것이 모니터링 된다면 특정 시스템이 감염된 것을 의심해볼 필요가 있고, 개인 PC 사용자라면 웹에서 다운로드 가능한 전용백신으로 체크해 보는 것이 필요하다.