# ASEC Report 11월

® ASEC Report

2007. 12



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

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

# I. ASEC 월간 통계

## (1) 11월 악성코드 통계

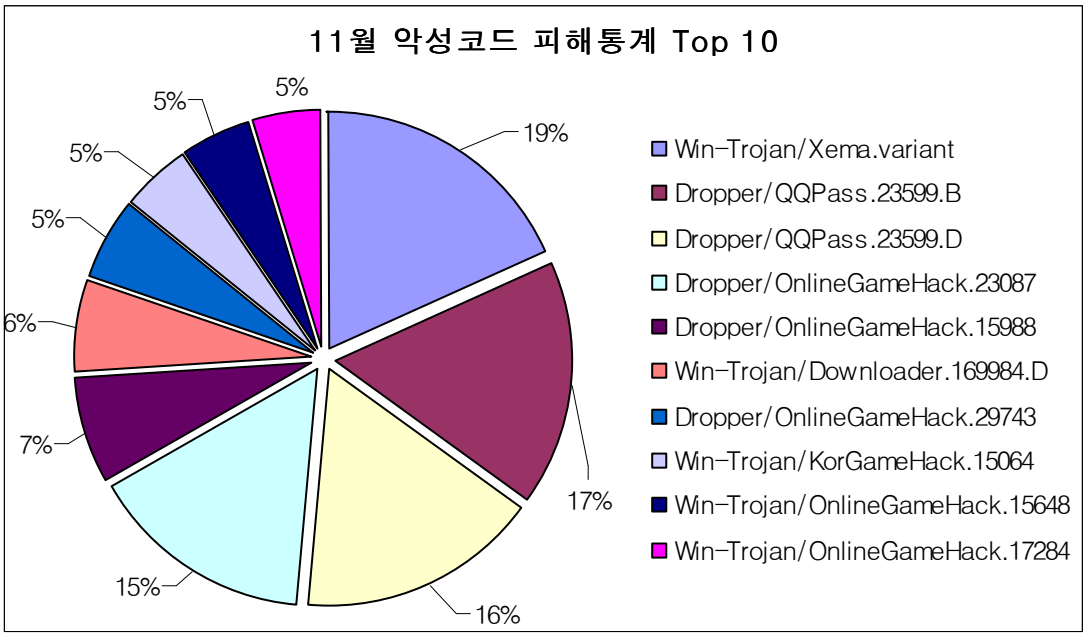
| 순위 | | 악성코드명 | 건수 | % |
|---|---|---|---|---|
| 1 | ↑3 | Win-Trojan/Xema.variant | 326 | 18.3% |
| 2 | new | Dropper/QQPass.23599.B | 298 | 16.7% |
| 3 | new | Dropper/QQPass.23599.D | 293 | 16.4% |
| 4 | new | Dropper/OnlineGameHack.23087 | 272 | 15.2% |
| 5 | new | Dropper/OnlineGameHack.15988 | 130 | 7.3% |
| 6 | new | Win-Trojan/Downloader.169984.D | 116 | 6.5% |
| 7 | new | Dropper/OnlineGameHack.29743 | 95 | 5.3% |
| 8 | new | Win-Trojan/KorGameHack.15064 | 88 | 4.9% |
| 9 | new | Win-Trojan/OnlineGameHack.15648 | 84 | 4.7% |
| 10 | new | Win-Trojan/OnlineGameHack.17284 | 83 | 4.6% |
| 합계 | | | 1,785 | 100.0% |

[표 1-1] 2007년 11월 악성코드 피해 Top 10

11월 악성코드 피해 Top 10에 랭크 된 피해건수는 1785건으로 11월 한달 총 피해건수(6454건)의 약 27%를 차지하였으며 지난 10월에 비해 약 24%가 증가하였다.

[표 1-1]에서 보듯이 11월 악성코드 피해 Top 10의 전체적인 악성코드 형태별 동향은 지난 10월에 비해 크게 달라지지 않았지만 세부적으로 약간의 변화가 있었다. 우선 지난 10월에 피해건수가 140건으로 3단계 하락하여 4위에 랭크 되었던 Win-Trojan/Xema.variant의 경우, 지난 10월에 비해 57%(186건)가 증가한 326건의 피해사례가 접수되면서 11월 악성코드 피해 Top 10의 1위에 재 등극하였다.

또한 10월의 악성코드 피해 Top 10에는 게임 핵 관련 Dropper 2종만이 각각 7, 10위에 랭크 되었으나 11월에는 Dropper 3종이 악성코드 피해 Top 10에 새롭게 진입하였다. 특히 중국에서 많이 애용되는 QQ Messenger 사용자의 계정정보 유출을 시도하는 것으로 보이는 Dropper/QQPass계열 2종이 각각 2, 3위로 전체 악성코드 피해 Top 10의 37.1%를 차지하고 있다는 것이 눈에 띈다.

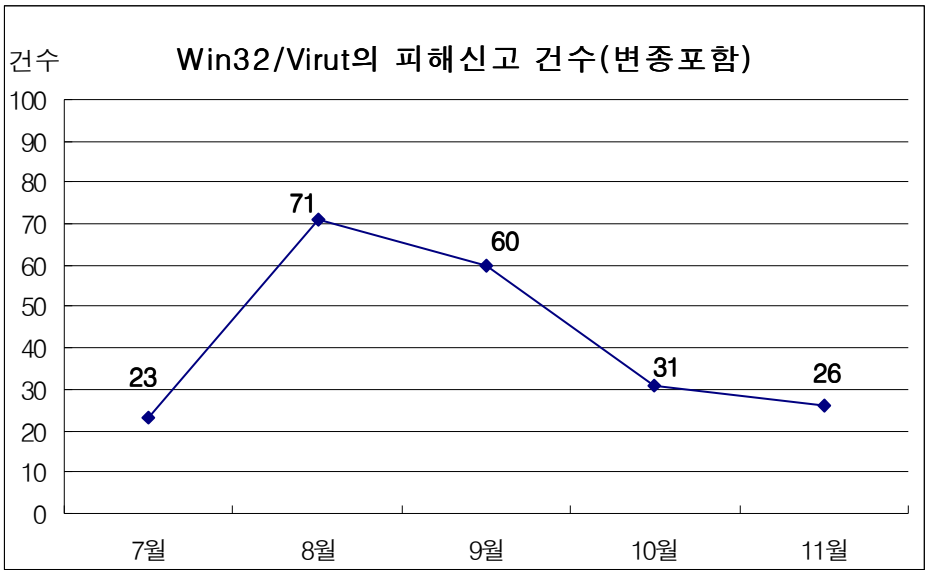



[그림 1-1] 2007년 11월 악성코드 피해 Top 10

10월 악성코드 Top 10의 10위에 랭크 되어 있던 Win32/Autorun.worm계열의 변종도 11월에는 Top 10 순위 권 밖으로 밀려났다.

### 11월 악성코드 피해 Top 10의 유형별 현황

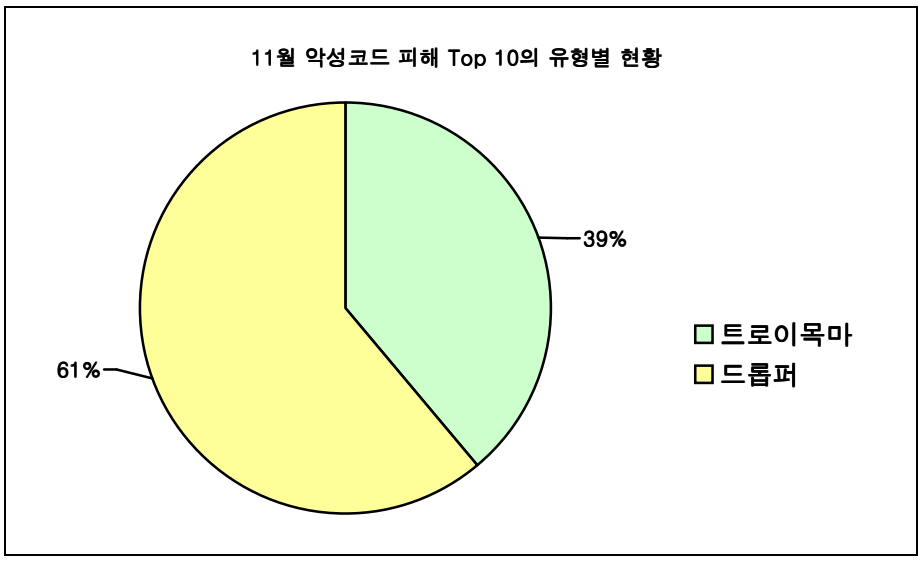
10월에 31건의 피해신고가 접수되면서 18위에 랭크 됐던 Win32/Virut은 11월에는 단지 5건이 감소했지만 11월 전체 피해신고 접수순위에서 큰 폭으로 하락하여 31위에 랭크 되었다 그 이유는 11월 악성코드 피해신고 상위 1 ~ 30위까지 살펴보면 지난 10월 과 동일하게 13위 랭크 된 Win32/IRCBot.worm.variant를 제외한 대부분이 모두 게임 핵 관련 트로이목마이거나 드롭퍼 및 다운로더가 차지했기 때문인 것으로 보인다.




[그림 1-2] Win32/Virut 피해신고 건수

지난 7월부터 11월까지 Win32/Virut 및 그 변종을 포함한 피해신고 건수에 대한 통계는 [그림 1-2]와 같다. 보통 바이러스는 감염조건의 특수성 때문에 라이프 사이클이 다른 악성코드에 비해 짧다는 특징이 있지만 2006년 6월경에 최초 발견된 Win32/Virut를 비롯하여 이후에 발견된 그 변종들은 IRC채널접속 및 복잡한 감염기법 등을 사용하여 완벽한 치료를 어렵게 하는 특징을 갖고 있어 현재도 감염피해 건수가 꾸준히 보고되고 있다.

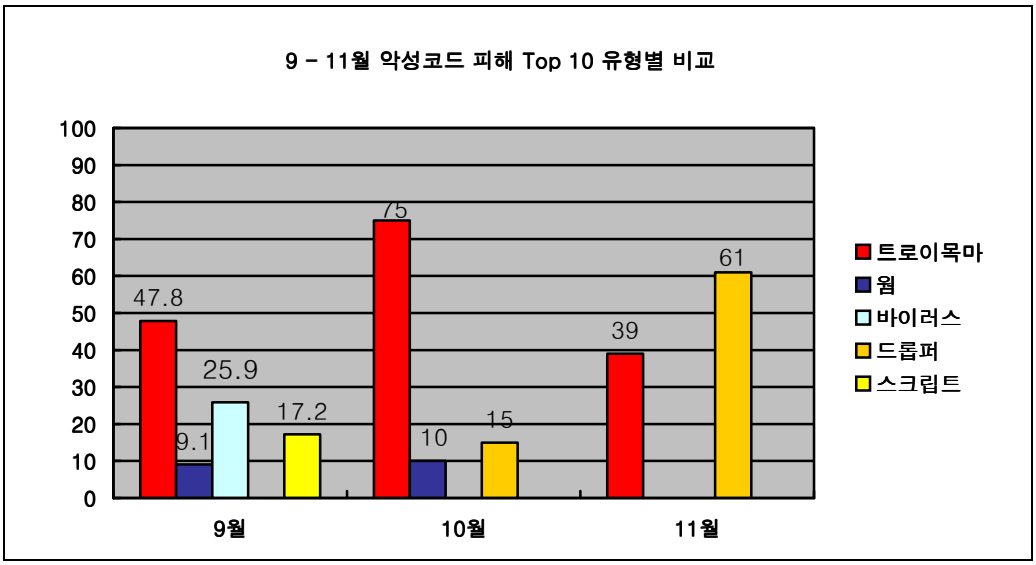
### 11월 악성코드 피해 Top 10의 유형별 현황




[그림 1-3] 11월 악성코드 피해 Top 10의 유형별 현황

[표 1-1]에 열거된 11월 악성코드 피해 Top 10을 유형별로 분류해 보면 예상대로 11월 역시 금전적인 이득을 노린 드롭퍼와 트로이목마 유형의 악성코드들이 가장 많은 피해를 발생시켰음을 [그림 1-3]을 통해서 알 수가 있다. 앞에서도 언급했지만 11월 악성코드 피해 Top 10의 전체적인 분위기는 전월과 유사하나 다만 악성코드 형태별 점유율은 크게 달라졌다.

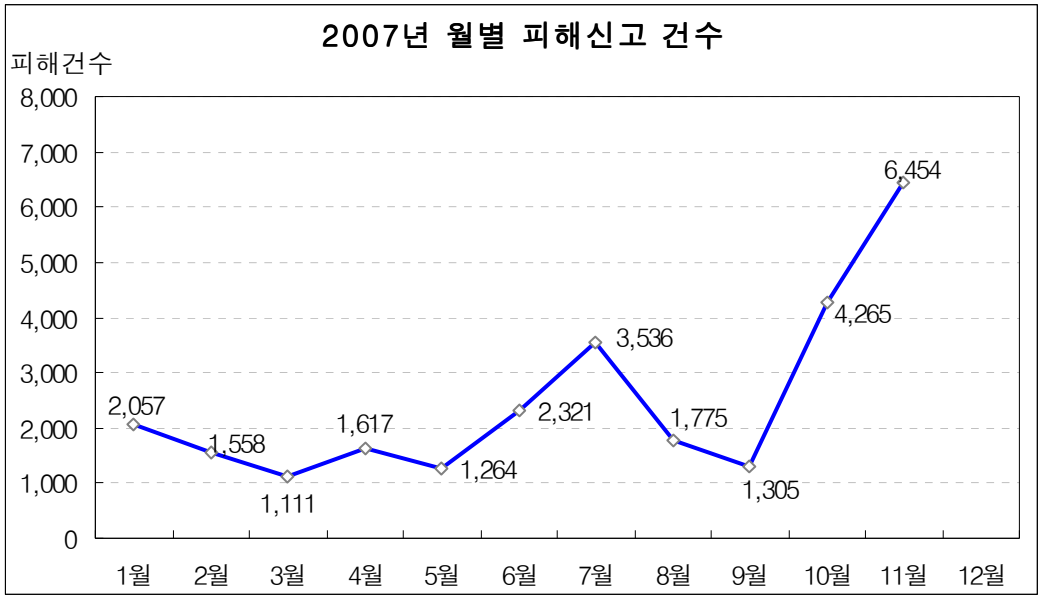
최근 3개월 악성코드 피해 Top 10에 랭크 되었던 악성코드들의 형태별 점유율을 비교해 보면 [그림1- 4]와 같다.




[그림 1-4] 최근 3개월간 악성코드 피해 Top 10 유형별 비교

[그림 1-4]를 통해서 9월의 경우를 살펴보면 수치상에서는 큰 차이가 있으나 웜 -> 스크립트 -> 바이러스 -> 트로이목마 순으로 악성코드 유형에서 대체적으로 골고루 분포해 있다. 하지만 10월의 경우 전월 대비 트로이목마는 27.2%, 웜은 극히 미비하지만 0.9%증가하였으며 드롭퍼가 15% 점유하면서 바이러스가 Top 10 순위권 밖으로 밀려남으로써 일부 악성코드로 피해신고 점유율이 편향되기 시작하였음을 알 수 있다. 그리고 11월에는 트로이목마가 36%로 감소, 반면에 드롭퍼가 46%로 증가하면서 유형면에서 나머지 악성코드들은 Top 10 순위권 밖으로 밀려났고, 이로 인해 일부 악성코드 유형에서 나타났던 피해신고 점유율 편향 현상은 더욱 심화되었다.

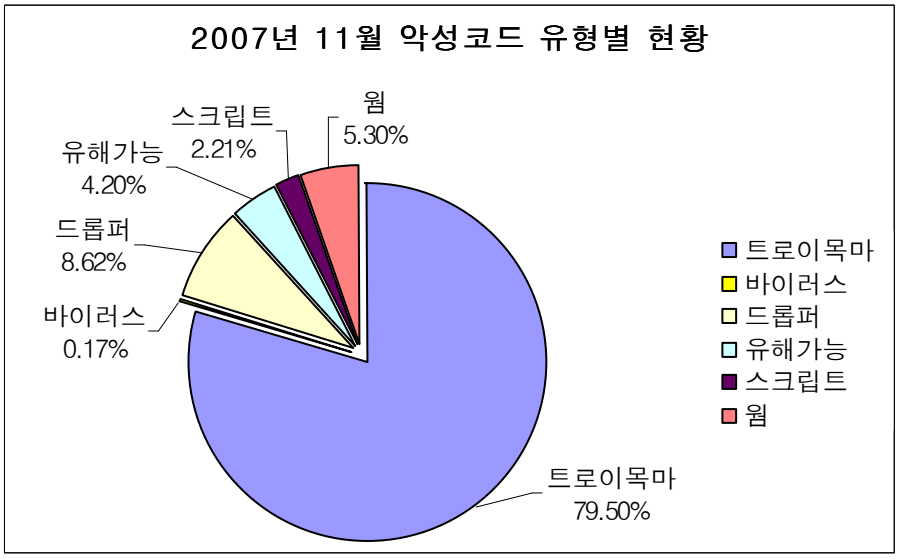
### 2007년 월별 피해신고 건수




[그림 1-5] 2007년 월별 피해신고 건수

[그림 1-5]는 2007년 11월까지 월별 피해신고 건수를 나타낸 차트로 9월까지는 월별 피해신고 건수가 4,000이하로 밑돌다가 10월에는 4,265건, 11월에는 10월보다 약 34%(2,189건) 상승한 6,454건의 피해신고가 접수되었는데 증가원인을 살펴보면 지난 10월과 마찬가지로 다운로더나 드롭퍼에 의해서 생성되는 신종 또는 변종 악성코드가 다수 발견되었기 때문이며, 특히 중국의 국경절 연휴가 끝나는 시점에서 다수의 악성코드, 주로 온라인 게임 사용자 계정 탈취와 관련된 악성코드가 집중적으로 접수된 것도 하나의 요인으로 파악된다.

### 피해 신고된 악성코드 유형현황




[그림 1-6] 11월 피해 신고된 악성코드의 유형별 현황

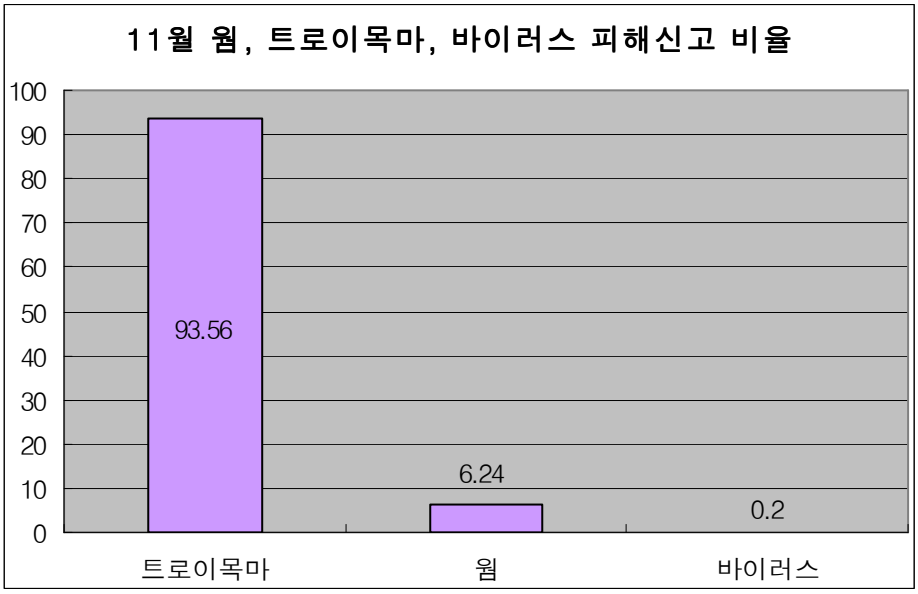
[표1-1]과 [그림 1-4]에서 살펴 보았듯이 11월 악성코드 피해신고 Top 10에서 유형별 점유율이 트로이목마 -> 드롭퍼 순으로 편향되어 알 수 있었으나, [그림 1-6]을 보면 11월 전체 악성코드 유형별 현황에는 그리 큰 변화는 주지 못했으며 전월과 마찬가지로 유사한 형태의 분포를 보이고 있다.

| | 9 월 | 10 월 | 11 월 |
|---|---|---|---|
| **트로이목마** | 782(74.76%) | 831(75.55%) | 1439(79.5%) |
| **바이러스** | 4(0.38%) | 2(0.18%) | 3(0.17%) |
| **드롭퍼** | 128(12.24%) | 142(12.9%) | 156(8.62%) |
| **유해가능** | 17(1.63%) | 28(2.55%) | 76(4.2%) |
| **스크립트** | 33(3.15%) | 22(2%) | 40(2.21%) |
| **웜** | 82(7.84%) | 75(6.82%) | 96(5.3%) |
| **통 계** | 1046(100%) | 1100(100%) | 1810(100%) |

[표 1-2] 최근 3개월 악성코드 유형별 현황

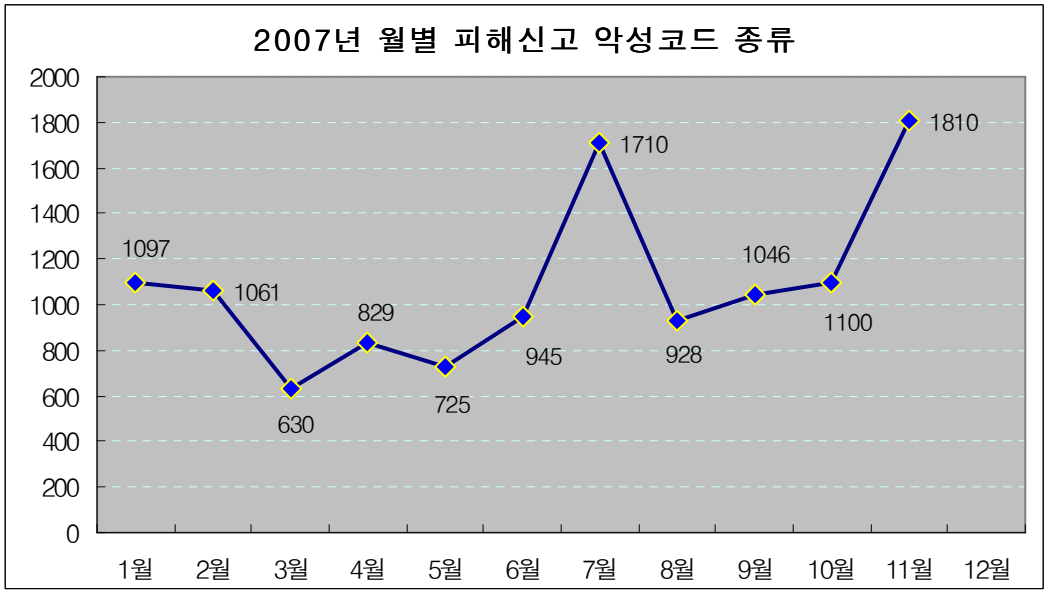
[표 1-2]를 보면 트로이 목마와 유해가능은 3개월 동안 꾸준히 상승했으며 드롭퍼의 경우는 해당 월의 유형별 건수는 꾸준히 상승했지만 점유율에서는 오히려 감소하였다. 그 원인은 트로이목마의 지속적인 상승세와 유해가능에서 전월 대비 63% 상승하면서 드롭퍼의 전체 점유율은 하락한 것으로 보인다. 이중 주요 악성코드 유형인 트로이목마, 바이러스 웜에 대한 피해신고 비율을 계산해 보면 [그림 1-7]과 같다.

최근 3개월 간의 주요 악성코드 유형의 피해신고 비율을 비교해 보면 큰 폭으로 상승하거나 하락하는 경우는 없었으며 그 폭이 미비할 정도의 상승 또는 하락만이 재 반복되고 있다. 웜의 경우 트로이목마에 비하면 그 영향이 극히 미비하나 금전적인 이득을 취하기 위해 다양한 경로를 통해서 불특정 다수에게 스팸메일을 발송하는데 여전히 이용되고 있다.




[그림 1-7] 2007년 11월 웜, 트로이목마, 바이러스 피해신고 비율

**월별 피해 신고된 악성코드 종류 현황**




[그림 1-8] 2007년 월별 피해 신고 악성코드 종류

[그림 1-8]은 바이러스 신고센터로 접수된 변종 및 신종 악성코드에 대한 현황을 나타내며, 8월 이후로 다시 증가추세를 보이고 있으며 11월의 경우 전월 대비 약 39% 상승하였다.

**국내 신종(변형) 악성코드 발견 피해 통계**

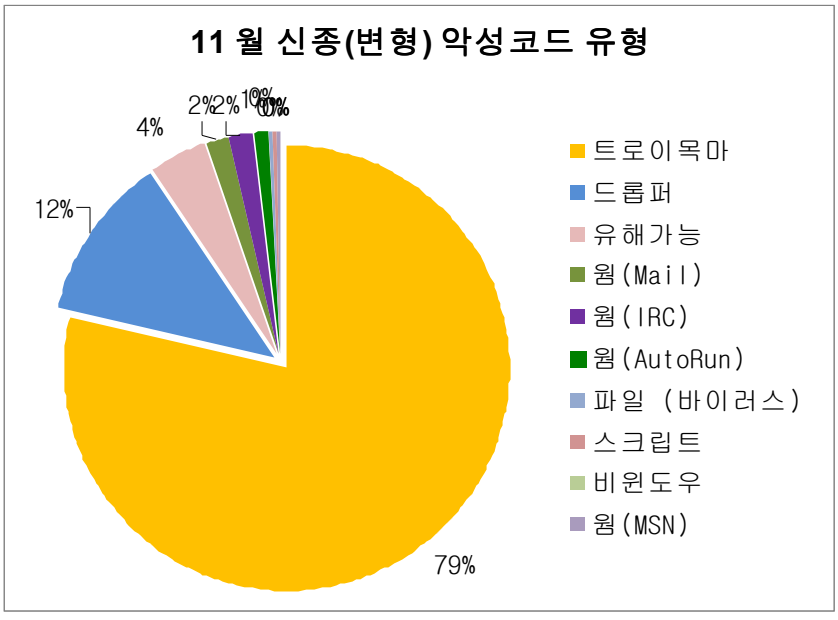
11월 한달 동안 접수된 신종 (변형) 악성코드의 건수 및 유형은 [표 1-3], [그림 1-9]와 같다.

| | 웜 | 트로이 | 드롭퍼 | 스크립트 | 파일 | 매크로 | 부트 | 부트/파일 | 유해가능 | 비윈도우 | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **9 월** | 32 | 418 | 78 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 531 |
| **10 월** | 23 | 269 | 55 | 1 | 2 | 0 | 0 | 0 | 5 | 0 | 355 |
| **11 월** | 24 | 406 | 62 | 1 | 1 | 0 | 0 | 0 | 22 | 1 | 517 |

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

악성코드는 전월 대비 46% 증가한 것으로 보이나 이는 지난달에 밝힌 바 있듯이 지난달 경우 10월 1일부터 10월 25일까지만 통계 데이터를 산출 한 것에 근거한다. 따라서 굳이 지난달과 비교하지 않아도 11월 국내 접수된 신종 및 변형 악성코드의 전체적인 수는 크게 달라 지지 않았다. 다만 유해 가능 프로그램이 소폭 증가하였는데 일부 상용 키로거와 원격제어 관련 파일이 주로 차지 한다.

다음은 이번 달 악성코드 유형을 상세히 분류 하였다.




[그림 1-9] 2007년 11월 신종 및 변형 악성코드 유형

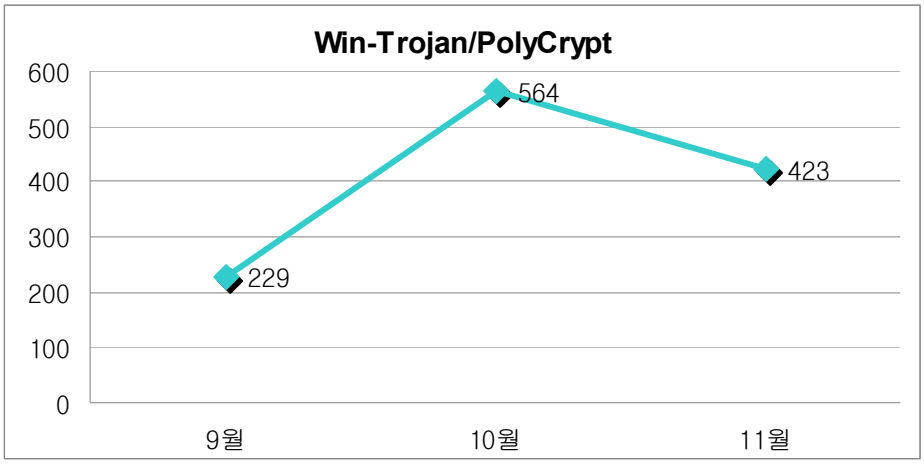
악성코드는 점점 그 기능이 복잡하고 다양해지고 있다. 따라서 위와 같은 분류도 점점 그 의미를 잃어가고 있는 실정이다. 가령 악의적인 호스트로부터 파일을 다운로드 하는 증상을 갖

는 악성코드가 파일도 감염 시키고 자신의 복사본을 자동으로 실행하기 위해서 Autorun.inf 파일도 생성한다면 이 악성코드는 어떤 유형에 속해야 하는가는 실로 쉽게 결정하기 어려운 문제이다. 혹자는 제일 먼저 나타는 증상을, 어떤이는 악성코드의 가장 주된 목적 (또는 증상)으로 악성코드를 분류 하곤 한다. 따라서 이러한 이유 때문에 분석가들마다 악성코드 명명법중 접두어에 해당 하는 부분이 달라지기도 한다. 악성코드의 다양한 증상은 어제 오늘의 일은 아니지만 최근 들어 악성코드를 분류하기 더욱 애매해지고 있다.

이번 달에는 500여종의 악성코드가 발견 되었다. 위에서 언급 한 바와 같이 유해가능 프로그램이 소폭 증가 하였고, 지난달에 보이지 않았던 MSN 웜 그리고 비윈도우 악성코드도 1개가 발견 되었다. MSN 으로 전파 되는 웜은 일종의 악성 IRCBot 웜과 더 가깝다. 이것은 근래에 발견 되는 MSN 웜의 특징이다. 메신저로의 전파는 IRC 채널의 Master에 의해서 역시 제어가 가능하다.

비윈도우 악성코드는 Linux 환경에서 동작하는 백도어인 Kaiten이 발견, 보고 되었다. 특정 IRC 서버로 접속하여 명령을 수행 받아 DoS 공격을 수행할 수 있도록 되어 있다.

다음은 Win-Trojan/PolyCrypt 라고 불리우는 악성코드의 3개월간의 통계이다. 이 악성코드는 국내에서 지난 3개월 동안 단 1건만 보고 되었으나 국외의 타 백신업체에서는 많은 변형으로 각사의 엔진에서는 대량 추가된 샘플중에 하나이다. 이 악성코드의 진단명에서 알 수 있듯이 다형성 Cryptor 또는 다중 실행압축등으로 의해서 자신의 코드를 매번 변형한 특징을 갖는다. 따라서 일부 안티 바이러스 업체는 Cryptor된 형태를 바로 진단 하기도 한다.




[그림 1-10] 2007년 최근 3개월 Win-Trojan/Polycrypt 현황

이 트로이목마의 실체는 Win-Trojan/Hupigon인데 압축을 해제한 경우, V3도 이를 Generic하게 진단 할 수 있다. Hupigon 트로이목마는 대표적인 중국산 악성코드로서 제작자의 홈페이지에서 이 프로그램을 원격 제어 목적으로 배포 하고 있지만 이를 다운로드 받은 사용자

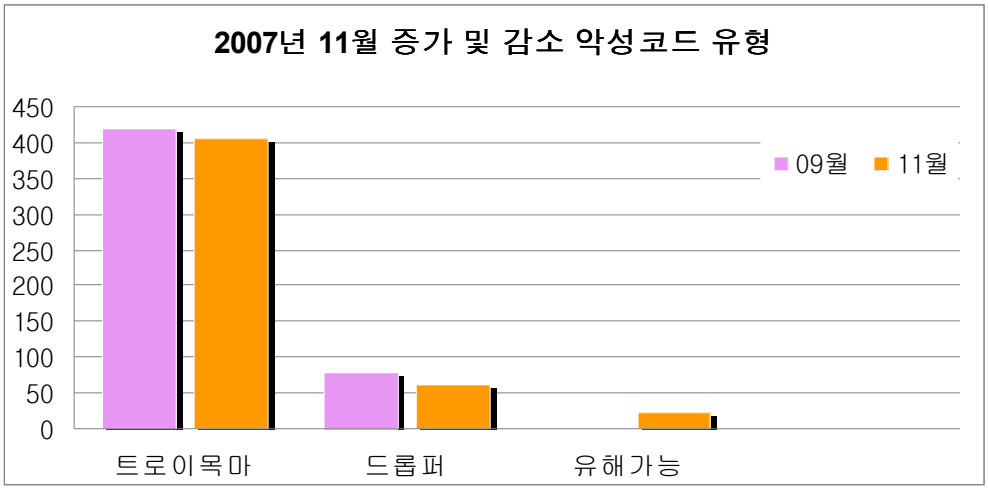
들은 악의적인 목적에 활용한다. Hupigon 트로이목마가 올해 들어서 발견, 보고가 줄어든 이유를 대략 추정해보면 이와 같이 Cryptor로 파일을 변형하여 안티 바이러스를 우회한 형태가 많았기 때문으로 추정해 본다.

이번 달은 1종의 바이러스가 보고 되었는데 다음과 같다.

- Win32/Sbill

이 바이러스는 간단한 전위형 바이러스로서 감염시킬 파일 앞에 자신을 위치 시키며 감염된 파일은 20,377바이트 증가한다. 바이러스 자체가 실행압축된 형태이고 전위형이므로 EntryPointRVA 값이 항상 일정하여 쉽게 바이러스 유무를 진단 할 수 있다.

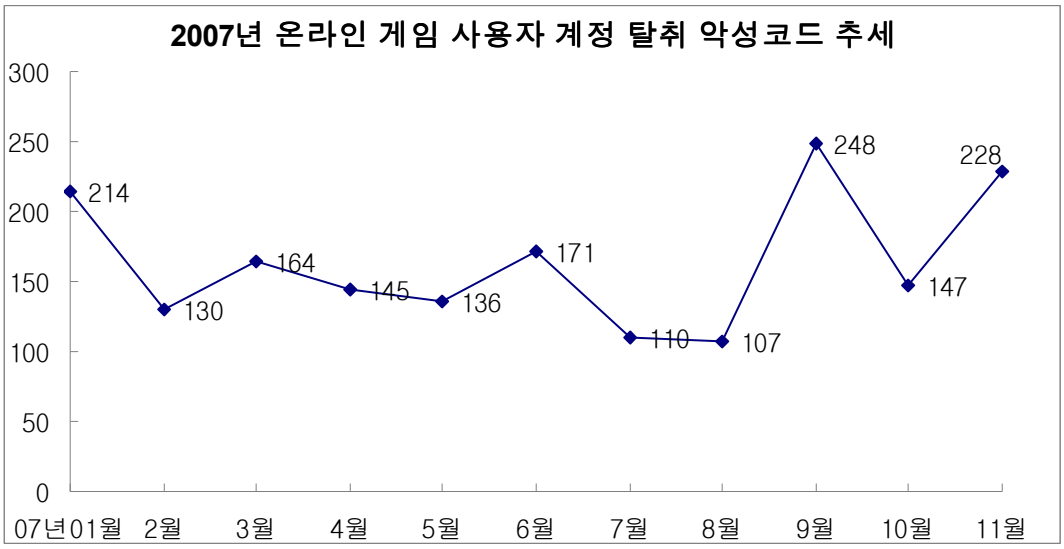
다음은 11 월에 증가 및 감소한 주요 악성코드 유형에 대한 현황이다.




[그림 1-11] 2007년 11월 감소 및 증가 악성코드 유형

위에서 언급 했듯이 지난달은 통계기준 기간이 변경 되어 10월과 11월 두 기간을 위와 같이 비교 하는 것이 다수 무리 일 수도 있어 9월/11월을 비교하였다. 3가지 유형이 근소한 차이를 보이고 있으며, 특히 드롭퍼는 다른 악성코드 보다는 온라인 게임 계정을 탈취하는 트로이목마를 Drop 하는 형태가 주를 이루고 이는 전체적으로 온라인 게임 계정을 훔쳐내는 악성코드에 통계에도 영향을 준다.

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



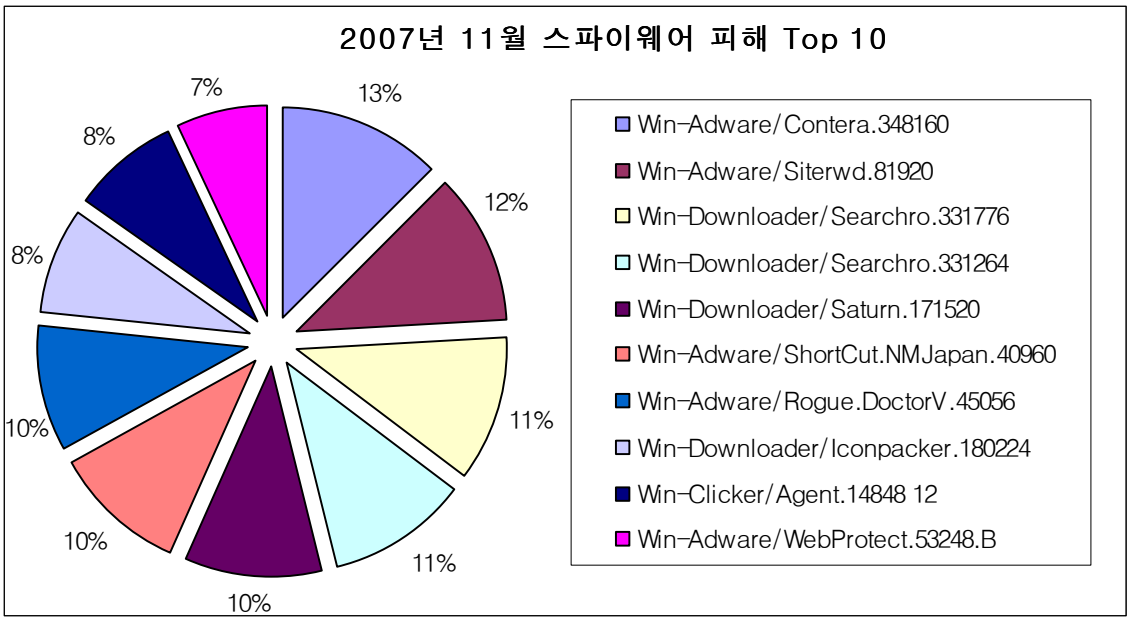

[그림 1-12] 온라인 게임 사용자 계정 탈취 트로이목마 현황[1]

전월 대비하여 비교하는 것은 의미가 없음을 위에서 밝혔다. 9월과 비교해서는 소폭 감소한 수치 이다. 국산 온라인 게임과 외산 온라인 게임과의 비중은 외산에 무려 145% 넘는 비중을 차지하고 있다.

### (2) 11월 스파이웨어 통계

| 순위 | | 스파이웨어 명 | 건수 | 비율 |
|---|---|---|---|---|
| 1 | New | Win-Adware/Contera.348160 | 18 | 13% |
| 2 | New | Win-Adware/Siterwd.81920 | 17 | 12% |
| 3 | New | Win-Downloader/Searchro.331776 | 16 | 11% |
| 4 | New | Win-Downloader/Searchro.331264 | 16 | 11% |
| 5 | New | Win-Downloader/Saturn.171520 | 15 | 10% |
| 6 | New | Win-Adware/ShortCut.NMJapan.40960 | 15 | 10% |
| 7 | New | Win-Adware/Rogue.DoctorV.45056 | 14 | 10% |
| 8 | New | Win-Downloader/Iconpacker.180224 | 12 | 8% |
| 9 | New | Win-Clicker/Agent.14848 | 12 | 8% |
| 10 | New | Win-Adware/WebProtect.53248.B | 10 | 7% |
| 합계 | | | 145 | 100% |

[표 1-4] 2007년 11월 스파이웨어 피해 Top 10




[그림 1-13] 2007년 11월 스파이웨어 피해 Top 10

2007년 11월 전체 스파이웨어 피해신고 건수는 총 1535건으로 지난 10월의 999건에서 약 54% 증가하였으며, 지난 9월의 592건과 비교하면 약 260% 나 증가한 수치를 보였다. 이렇게 11월에 스파이웨어 피해 신고가 급증한 원인은 국내에서 제작 배포되는 스파이웨어의 피해가 크게 늘었기 때문이다. 지난 호에 이미 언급한 바와 같이 국내 제작 스파이웨어의 배포 방법은 기존의 ActiveX 컨트롤을 이용한 배포에서 다운로더를 이용한 번들 설치로 변화하였

으며, 변화의 시작은 대략 2007년 하반기부터인 것으로 추정된다. 제작자는 번들 설치를 통한 설치 배당금을 목적으로 다운로더를 만들게 되는데, 안티-바이러스, 안티-스파이웨어 프로그램과 같은 보안 프로그램의 탐지를 피하기 위하여 코드와 형태가 조금씩 변경된 변형을 다수 만들어 배포하고 있으며, 이들 다운로더로 인해 스파이웨어 피해 신고가 크게 증가한 것으로 추정된다.

이런 변화는 스파이웨어 피해 Top10 순위에 고스란히 반영되어 있는데, 10월 스파이웨어 피해 Top 10의 모두를 온라인게임 계정 유출 스파이웨어가 차지하고 있는 반면, 11월에는 국내에서 제작된 애드웨어 및 다운로더가 피해신고 Top 10의 대부분을 차지하고 있다. 스파이웨어 피해 Top10 순위에서는 밀려났으나 온라인게임 계정 유출 스파이웨어의 피해 신고는 지난달과 비슷한 수치를 기록하고 있는 점이 주목할 만하다.

2007년 11월 유형별 스파이웨어 피해 현황은 [표 1-5]와 같다.

| | 스파이웨어류 | 애드웨어 | 드롭퍼 | 다운로더 | 다이얼러 | 클리커 | 익스플로잇 | AppCare | Joke | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 9월 | 291 | 119 | 35 | 132 | 8 | 7 | 0 | 0 | 0 | 592 |
| 10월 | 632 | 131 | 38 | 180 | 7 | 11 | 0 | 0 | 0 | 999 |
| 11월 | 480 | 354 | 147 | 525 | 3 | 25 | 1 | 0 | 0 | 1535 |

[표 1-5] 2007년 11월 유형별 스파이웨어 피해 건수

11월 유형별 스파이웨어 피해 통계에서도 위에서 언급한 국내제작 스파이웨어의 증가로 애드웨어, 드롭퍼, 다운로더의 피해 신고가 크게 증가한 수치를 보이고 있다. 번들 설치를 위한 다운로더는 인스톨러 형태의 애드웨어 드롭퍼를 사용자 동의 없이 다운로드하고 실행하며, 결국 리워드(쇼핑몰 현금적립 프로그램), 툴바, 허위 안티-스파이웨어와 같은 원하지 않는 프로그램을 설치하게 된다.

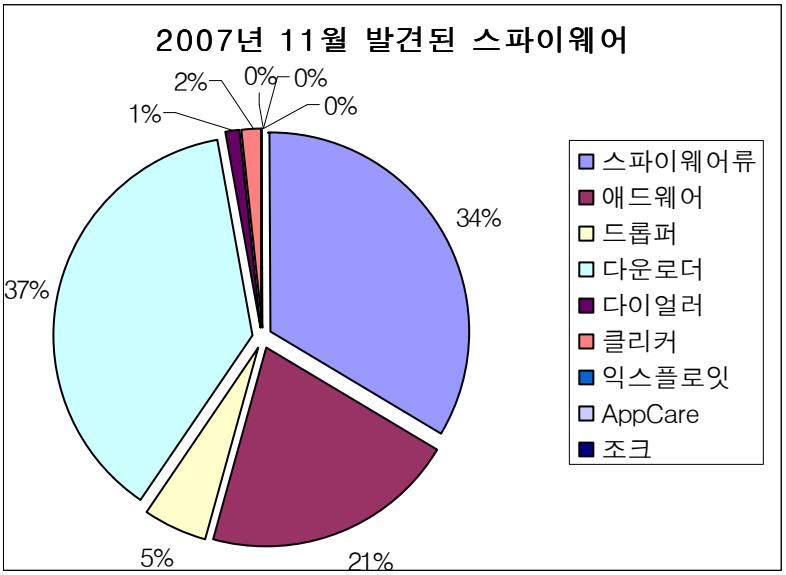
사용자의 중요 기밀 정보를 유출하는 목적으로 만들어진 스파이웨어류의 경우 그 자체만으로도 보안에 직접적인 위협이 될 수 있는 반면, 단순 광고 목적으로 만들어진 애드웨어나 보안 프로그램으로 위장하는 허위 안티-스파이웨어의 경우 보안에 직접적인 위협을 가하는 경우는 드물기 때문에 관리에 소홀하기 쉽다. 그러나 이들 애드웨어의 다운로드 과정에서 네트워크 트래픽 증가, 애드웨어 자체 프로그램 오류로 인한 시스템다운 또는 성능저하는 잠재적으로 가용성(Availability)에 위협이 될 수 있으며, 바이러스와 같은 악성코드의 감염 매개체로 사용될 수 있기 때문에 시스템 무결성(Integrity)에도 영향을 줄 수 있다.

### 11월 스파이웨어 발견 현황

11월 한달 동안 접수된 신종(변형) 스파이웨어 발견 건수는 [표 1-6], [그림 1-14]와 같다.

| | 스파이웨어류 | 애드웨어 | 드롭퍼 | 다운로더 | 다이얼러 | 클리커 | 익스플로잇 | AppCare | Joke | 합계 |
|---|---|---|---|---|---|---|---|---|---|---|
| 9월 | 91 | 37 | 12 | 40 | 6 | 6 | 0 | 0 | 0 | 192 |
| 10월 | 98 | 42 | 14 | 51 | 5 | 6 | 0 | 0 | 0 | 216 |
| 11월 | 99 | 61 | 15 | 112 | 3 | 5 | 0 | 0 | 0 | 295 |

[표 1-6] 2007년 11월 유형별 신종(변형) 스파이웨어 발견 현황

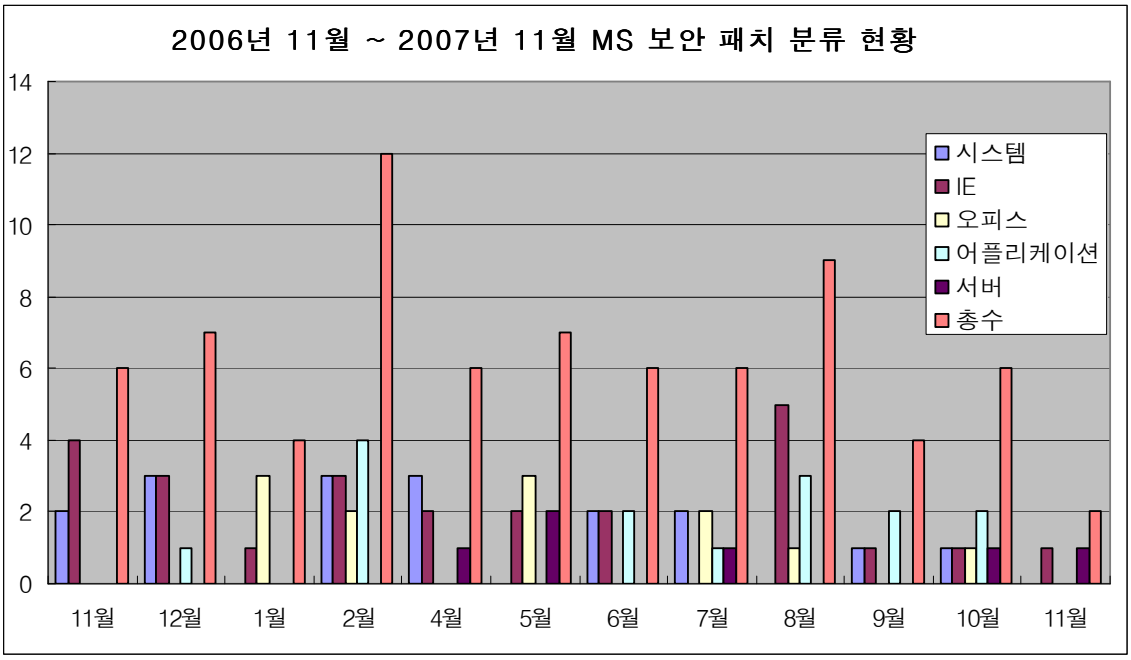



[그림 1-14] 2007년 11월 발견된 스파이웨어 프로그램 비율

[표 1-6]과 [그림 1-14]는 2007년 11월 발견된 신종 및 변형 스파이웨어 통계를 보여준다. 애드웨어 및 다운로더의 신종 및 변형 발견 건수가 다소 증가하였으며, 다른 카테고리의 스파이웨어는 지난 10월과 비슷한 수치를 보이고 있다.

### (3) 11월 시큐리티 통계

2007년 11월에는 이전 달과 비해 마이크로소프트사에서 2개의 보안 업데이트를 발표하고, 발표된 업데이트는 긴급(Critical) 1개, 중요 1개로, 10월의 총 6건에 비해서, 줄어들었다. 이 중에서 PDF 웜 전파에 사용되고, 인터넷 익스플로러 공격에 사용될 수 있는 MS07-061 에 대한 패치가 포함되었으며, 윈도우 DNS 서버 관련 패치인 MS07-062 가 포함된 것이 특징이라고 할 수 있다.

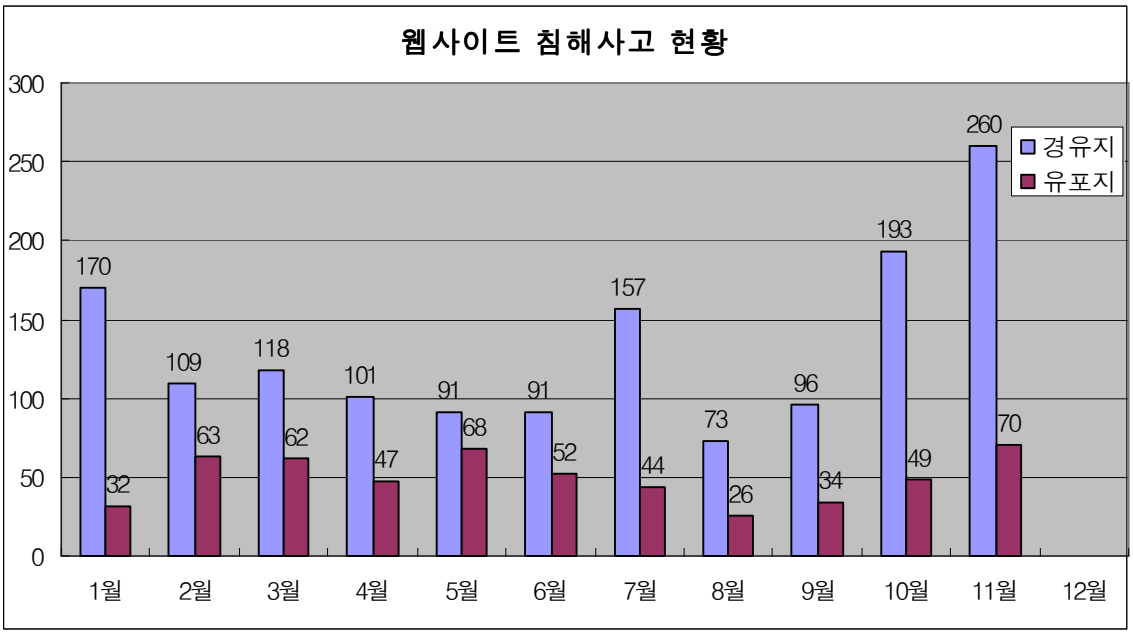



[그림 1-15] 2006년 11월 ~ 2007년 11월 공격대상 기준 MS 보안 패치 현황

[그림 1-15]을 보면, 전반적으로 2007년에 들어와서, 어플리케이션 취약점들(IE, 오피스, 기타 어플리케이션) 취약점들이 증가 추세에 있는데 반해, 서버 관련 취약점들은 현저하게 줄어든 것을 알 수 있다. 그러나, 11월달에 발표된 DNS 의 취약점으로 인한 스푸핑 허용 문제점(941672) 는 윈도우로 운영하고 있는 DNS 서버가 스푸핑(Spoofing)되어, 악의적인 웹 사이트로 변경되는 공격에 이용될 수도 있기 때문에, 주의가 필요하다.

9월에 발표된 마이크로소프트 오피스 2003 서비스팩 3 가 출시된 이후에 오피스 관련 취약점 또한 줄어든 것을 알 수 있으나, 11월달에 마이크로소프트 Access (.mdb)파일의 공격코드가 발표되어 주의가 필요하다. 오피스 취약점들은 악성코드가 포함 되어져 메일이나 웹을 통해 공격하기 때문에, 신뢰하지 않는 사용자에게서 오피스 파일이 메일로 오는 경우에는 특히 주의가 필요하다. 또한, 오피스에 대한 보안패치는 반드시 오피스 홈페이지에서 보안 업데이트를 적용해야만, 클라이언트 시스템의 보안성을 강화할 수 있다.

**2007년 11월 웹 침해사고 현황**




[그림 1-16] 악성코드 배포를 위해 침해된 사이트 수/ 배포지 수

2007년 7월의 웹 사이트 침해지/배포지 수는 260/70으로 2007년 10월과 비교하여 침해지 수가 증가하였다. 이는 2007년 10월에 예측한 경향과 일치하는 것으로 탐색 사이트수가 약 3배가량 증가한 결과이다.

탐색 사이트 수와 침해지 사이의 관계를 알아보기 위해 2007년 11월 탐색사이트와 침해사이트의 비율을 계산하면 0.287%로 탐색사이트 수가 증가하기 전인 2007년 10월 이전인 0.279%와 비교하여 거의 변화가 없다. 이것은 침해 당한 사이트의 비율이 일정하다는 것을 보여준다. 탐색 사이트의 수가 더 증가되더라도 이와 같은 비율은 변함이 없을 것이라고 예상된다.

악성 코드 배포를 위해 사용된 취약점 종류의 비율은 이전과 마찬가지로 MS07-017 ANI 취약점의 비율이 27%로 큰 비중을 차지한다. 침해사고를 확인한 웹 사이트의 관리자들은 사이트의 사후 관리에 신경을 써야 하고 일반 PC 사용자들은 운영체제의 패치를 항상 적용하고 Anti-Virus 제품을 설치한 후 인터넷을 사용하는 것이 안전하다.

# II. ASEC Monthly Trend & Issue

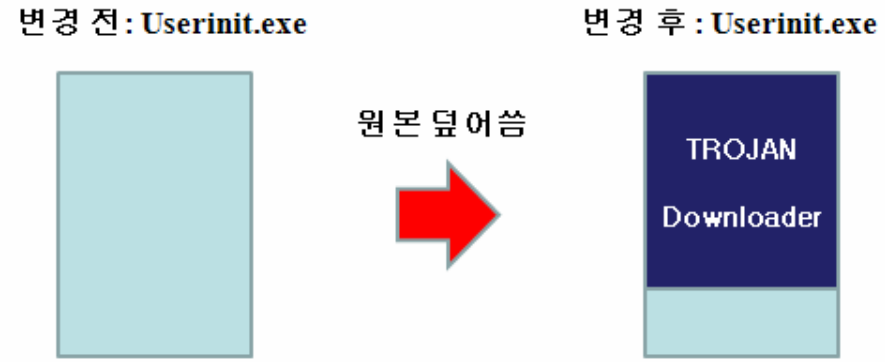
## (1) 악성코드 – 파일의 디스크 위치 정보를 계산하여 감염 시키는 악성코드

이번 달은 파일의 디스크 위치 정보를 계산하여 특정 파일을 감염 시키는 악성코드, 정품 하드웨어에 감염되어 판매된 상품과 해당 악성코드에 대해서 알아보고 미 법무부를 사칭하는 이메일을 보내는 악성코드, 루머로 끝난 사이버 성전과 사용된 도구 등 이번 달 국,내외적으로 이슈가 되는 악성코드에 대해서 알아본다.

### 파일의 물리 디스크 위치 정보를 계산하여 감염 시키는 악성코드

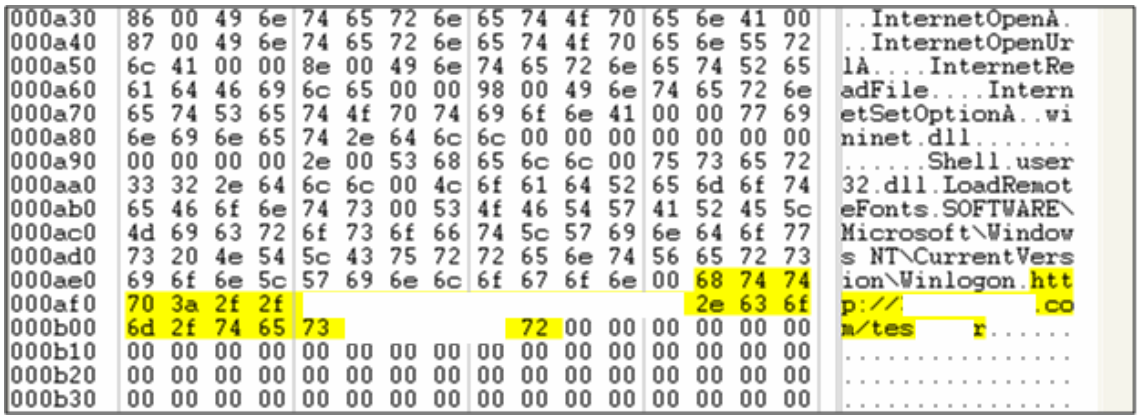
Dropper/Agent.49152.O (EXE), Win-Trojan/Agent.6768 (SYS) 두개의 악성코드 중 드라이버 파일인 Win-Trojan/Agent.6768이 먼저 발견 되었고 드라이버를 드랍하는 *.exe 의 Dropper/Agent.49152.O 는 최근에 발견 되었다. 이 두 개의 악성코드는 약 2달간의 차이를 두고 발견 되었다.

악성코드는 윈도우의 정상 시스템 파일인 Userinit.exe 파일의 물리적 위치정보를 계산하여 파일의 시작부터 0x1000 만큼 악의적인 코드로 덮어쓴다.




[그림 2-1] 악성코드에 변경된 Userinit.exe 전, 후 모습

덮어쓰는 코드는 Win-Trojan/Agent.6768 에 암호화 되어 담겨져 있다. 이렇게 악의적인 코드로 덮어쓴 Userinit.exe는 재부팅시 실행 되어 특정 호스트로부터 20개의 악성코드를 다운로드 받는다.



```
000a30  86 00 49 6e 74 65 72 6e 65 74 4f 70 65 6e 41 00  ..InternetOpenA.
000a40  87 00 49 6e 74 65 72 6e 65 74 4f 70 65 6e 55 72  ..InternetOpenUr
000a50  6c 41 00 00 8e 00 49 6e 74 65 72 6e 65 74 52 65  lA....InternetRe
000a60  61 64 46 69 6c 65 00 00 98 00 49 6e 74 65 72 6e  adFile....Intern
000a70  65 74 53 65 74 4f 70 74 69 6f 6e 41 00 00 77 69  etSetOptionA..wi
000a80  6e 69 6e 65 74 2e 64 6c 6c 00 00 00 00 00 00 00  ninet.dll.......
000a90  00 00 00 00 2e 00 53 68 65 6c 6c 00 75 73 65 72  ......Shell.user
000aa0  33 32 2e 64 6c 6c 00 4c 6f 61 64 52 65 6d 6f 74  32.dll.LoadRemot
000ab0  65 46 6f 6e 74 73 00 53 4f 46 54 57 41 52 45 5c  eFonts.SOFTWARE\
000ac0  4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77  Microsoft\Window
000ad0  73 20 4e 54 5c 43 75 72 72 65 6e 74 56 65 72 73  s NT\CurrentVers
000ae0  69 6f 6e 5c 57 69 6e 6c 6f 67 6f 6e 00 68 74 74  ion\Winlogon.htt
000af0  70 3a 2f 2f                          2e 63 6f  p://        .co
000b00  6d 2f 74 65 73                 72 00 00 00 00  m/tes     r.....
000b10  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000b20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000b30  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

[그림 2-2] 악성코드가 다운로드 하는 URL

이 악성코드의 목적은 윈도우 파일 보호를 우회하면서 시스템 파일을 수정하여 대량의 악성코드를 다운로드 받는데 있다.

**정품 하드웨어에 감염된 악성코드**

세계 최대의 하드디스크 제조사인 시게이트에서 출시한 외장형 저장장치(Maxtor Basics Personal Storage 3200)에 바이러스가 검출되어 외신을 통해서 국내에 보도 되었다.

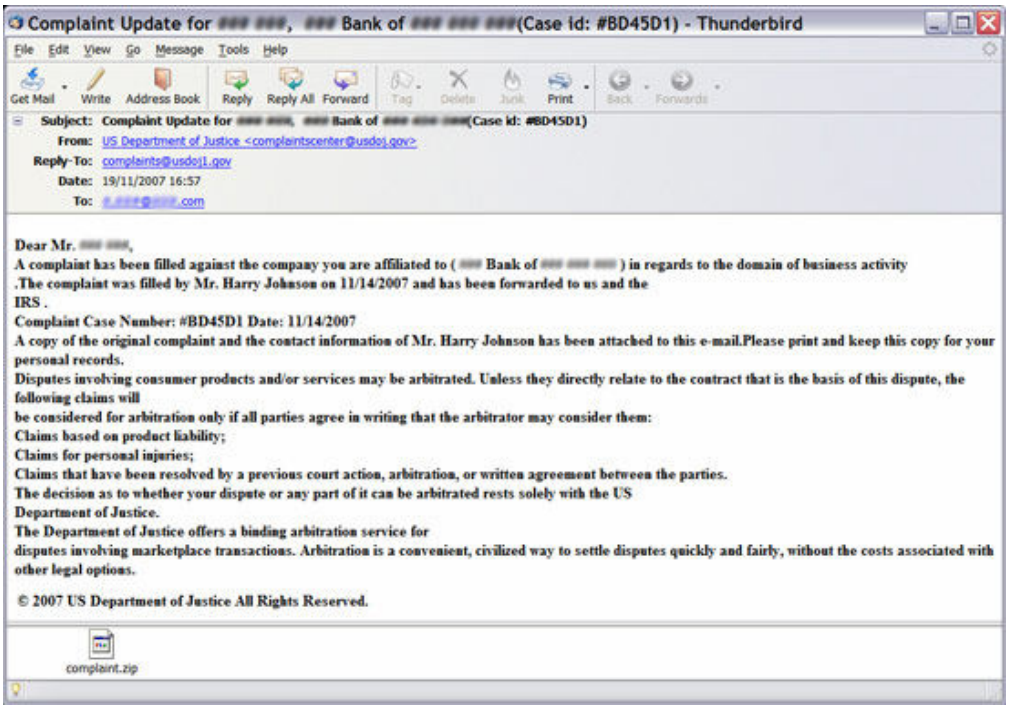

[그림 2-3] Maxtor Basics Personal Storge 3200

문제의 외장형 저장장치는 NTFS 규격으로 포맷까지 한 상태에서 제품을 판매하기 때문에 이 과정에서 바이러스에 감염되었을 가능성이 있는 것으로 제기되고 있다. 근래의 악성코드 중 일부는 각 드라이브에 루트에 자신의 복사본과 Autorun.inf 를 생성하여 이동식 디스크 또는 네트워크 드라이브도 감염 대상에 포함 시키고 있다. 따라서 포맷을 하고 난 후에 해당

악성코드에 감염될 확률이 높다. 문제의 악성코드는 Dropper/OnlineGameHack.21042 이며 실행 후 특정 DLL 파일을 생성하고 Explorer.exe 프로세스에 자신을 인젝션 한다. 이 DLL 파일은 Win-Trojan/OnLineGameHack.12338로 진단 된다. 악성코드는 특정 온라인 게임의 사용자 계정을 훔쳐내도록 되어 있으며 V3는 2007년 6월 23일자 엔진에 추가 되었다.

**미 법무부를 사칭한 악성코드**

미 법무부의 고소장으로 위장된 메일이 미국내 특정인들에게 배달 되었다. 그 모습은 다음과 같다. 메일에는 Complaint.zip 파일이 포함 되어 있었으며 이는 악성코드이다.




[그림 2-4] 악성코드가 첨부된 메일 화면 (제공 – MessageLabs)

실행하면 특정 파일을 C: 드라이브 루트에 생성하고 인터넷 익스플로러가 실행 될 때마다 자신이 실행 되도록 해두었다. 악성코드는 mstask.exe 란 작은 파일을 역시 C: 드라이브 루트에 생성해두는데 이는 다운로더 증상을 갖는 트로이목마이다.

근래 들어 악성코드의 감염 대상은 불특정 다수가 아닌 특정인 또는 단체 또는 국가로 타켓팅 되고 있다. 이는 노출을 최소화 하면서 악성코드의 생존기간 및 훔쳐낸 정보를 통한 이익 실현을 극대화 하려고 보인다.

**루머로 끝나버린 사이버 성전 (聖戰 – 지하드) 과 이용된 악성코드**

이슬람의 과격 단체인 알카에다 가 11월 중 특정일을 선택하여 사이버 성전을 벌일 것이라는 외신이 있었다. 여기에 사용되는 도구 역시 공개 되었는데 다음과 같다.

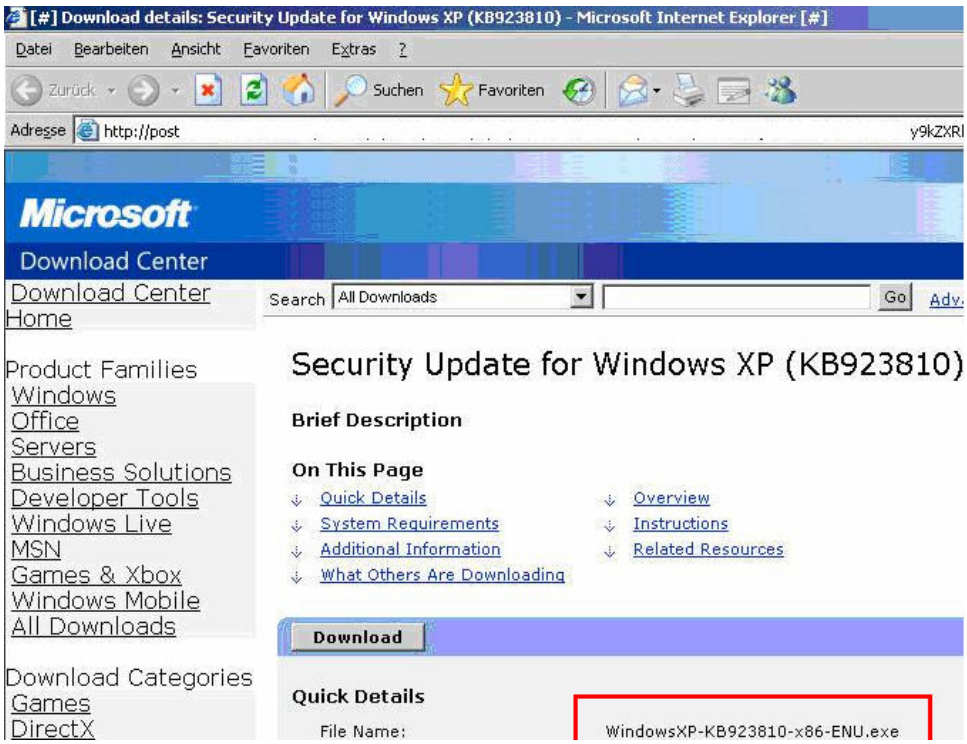

[그림 2-5] 사이버 성전에 사용된 도구 (출처 – McAfee)

이 도구는 특정 호스트에 대하여 분산 서비스 거부 공격을 할 수 있도록 되어 있다. 일부 보안 전문가들은 이 도구가 아주 기본적인 형태이고 쉽게 분석 될 수 있다고 한다. 필자 역시 프로그램을 간단히 분석해 보았는데 하드코딩 URL 이 그대로 노출 되었으며 또한 분석을 지연 시키거나 방해하기 위한 어떠한 노력도 되어 있지 않았다. 따라서 일부 보안 전문가들

은 이것이 과연 테러리스트들이 사용하는 툴인지 의심이 될 정도라고 하는 이들도 있다. 왜냐하면 악성코드 제작자들은 자신이 제작한 악성코드가 빠른 시간 내 노출 되는 것을 상당히 꺼려하기 때문이다.

### MS 보안 업데이트 관련 사이트를 위장한 악성코드

Dropper/Agent.1057651 이라고 알려진 이 악성코드는 위조된 MS 의 보안 업데이트 사이트로부터 다운로드 되었다. 먼저 스팸머는 윈도우의 특정 보안 업데이트를 받을 것을 권고하는 조작된 내용의 메일을 보냈다. 그리고 메일 하단에 특정 호스트로 연결 되는 URL을 알려주고 사용자로부터 방문을 유도하였다. 다음과 같다.




[그림 2-6] Dropper/Agent..1057651를 다운로드 받도록 조작된 사이트 (출처 – CA)

사용자 개입이 필요한 유형의 스팸 메일 형태지만 사용자가 'Download' 버튼을 누르면 악성코드 다운로드가 활성화되며 이를 보안 업데이트 인 줄 알고 실행하면 악성코드에 감염 된다. 악성코드는 백도어 증상을 갖으며 특정 포트를 오픈 하여 외부로부터 접속을 대기하는 상태로 만들어 둔다.

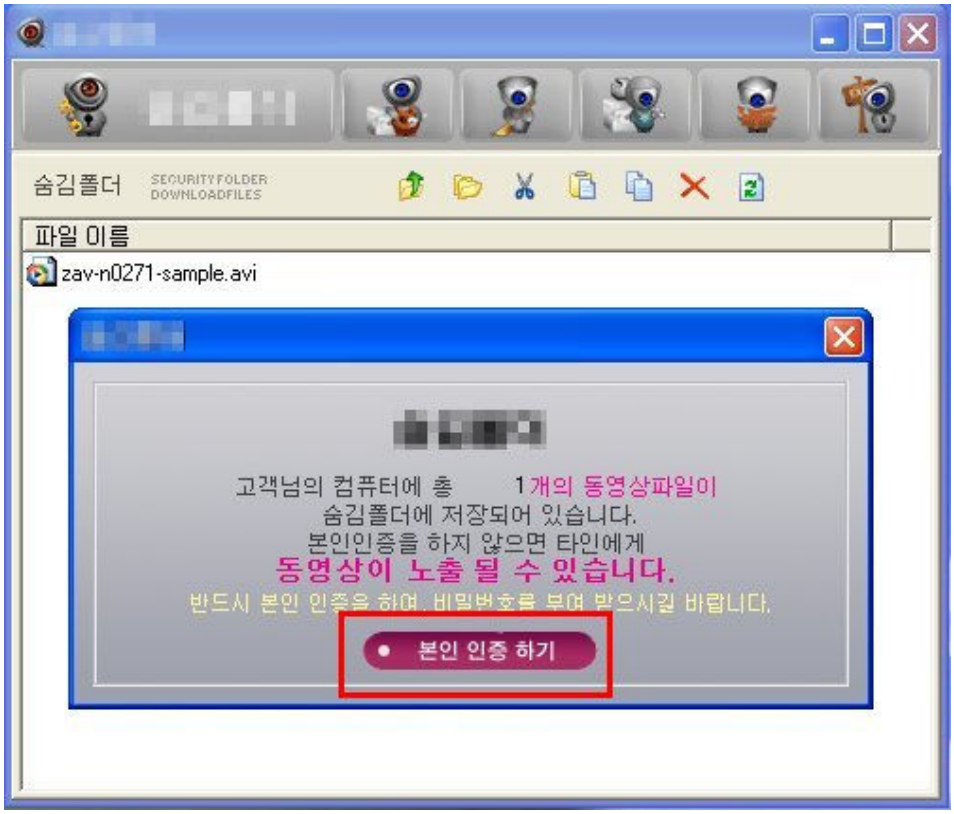
위에서도 언급했지만 악성코드의 전파는 특정 대상을 타켓으로 감염을 유도하는 형태로 공격하는 스팸 메일 형태가 단연코 눈에 띈다. 진짜처럼 보여지는 가짜 웹 사이트 그리고 호기심을 자극할 만한 문구와 첨부파일은 예전부터 보안에 가장 취약한 인간의 호기심을 자극한 사회공학 기법을 악용하고 있다.

### (2) 스파이웨어 - 새로운 형태의 랜섬웨어(Ransomware)

최근 동영상 플레이어로 사용자를 속여 설치되었던 UCCCPlay에 의해서 랜섬웨어가 설치되었다. 적절한 사용자 동의 절차 없이 사용자 PC에 설치되어 설치된 PC의 동영상 파일들을 한 곳의 폴더에 수집한 후 그 폴더를 루트킷(RootKit) 기능으로 일반 사용자들에게는 접근할 수 없도록 하였고 동영상을 보기 위해서는 결제를 해야 하는 랜섬웨어가 출현하였다.

랜섬웨어(Ransomware)란 ransom과 ware의 합성어로 사용자의 컴퓨터에 데이터를 암호화하여 데이터의 내용을 확인하기 위해서 비밀번호를 요구하는데 그 비밀번호를 얻기 위해서 일정 금액을 요구하는 형태의 악성코드를 가리키는 말이다. 2005년 5월에 발견되어 일명 MayAlert 으로 알려진 랜섬웨어에 의해 넓게 인식되는 계기가 되었다고 한다.

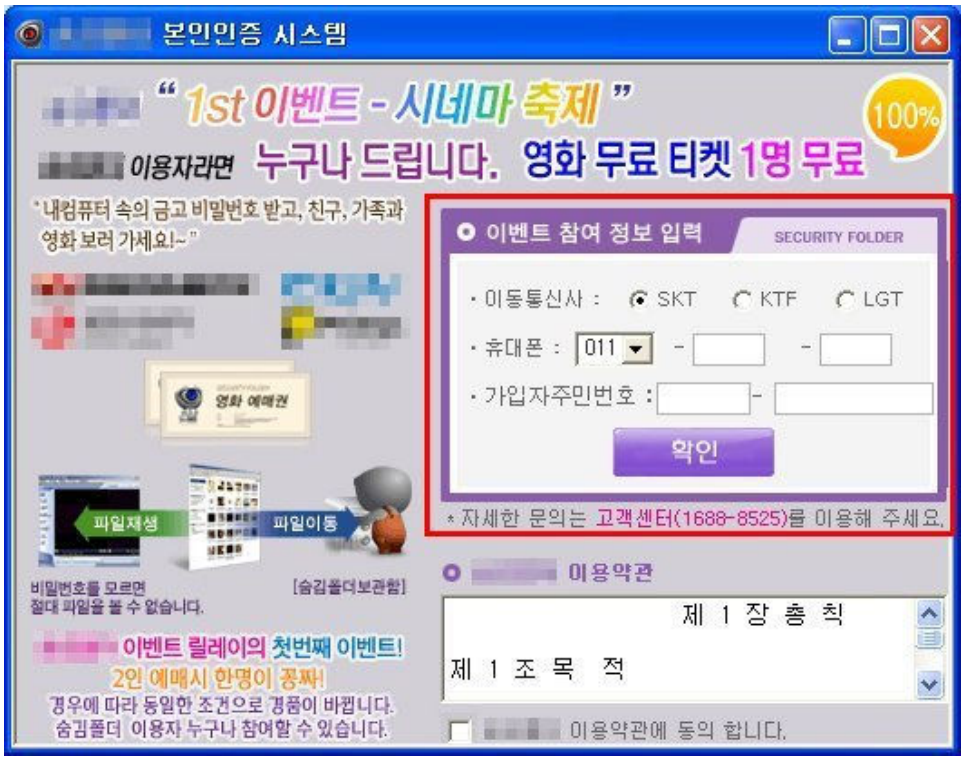
이렇게 설치된 랜섬웨어는 설치된 컴퓨터에 모든 동영상 파일 및 국내 대표적인 P2P 프로그램의 다운로드 경로의 파일들을 검색하고 루트킷 기법으로 숨겨진 폴더에 복사 후 원본은 삭제한다. 해당 폴더는 루트킷에 의해 접근이 불가능 하고 랜섬웨어 프로그램에 의해서만 접근이 가능하다. 동영상을 보기 위해서 랜섬웨어를 실행하면 아래와 같이 본인 인증을 받아야 한다는 메시지를 출력한다.




[그림 2-7] 자신의 동영상을 보기 위해 본인 인증을 요구하는 화면

하지만 실제로 랜섬웨어가 출력한 화면에서 “본인 인증 하기” 버튼을 클릭하면 결제를 위해

아래 그림과 같은 화면으로 이동한다. 한편 사용자 약관을 매우 작은 크기로 표시하고 있어 일반적으로 사용자 동의를 받기 위한 적절한 방법이라고는 생각할 수 없을 것이다.




[그림 2-8] 자신의 동영상을 보기 위해 결재를 요구하는 화면

Win-Spyware/MyComGo.6209 으로 진단되는 루트킷 드라이버는 KeServiceDescriptor Table 에 존재하는 ZwQueryDirectoryFile 함수와 ZwQuerySystemInformation 함수를 아래 역분석(Reverse Engineering)된 코드와 같이 후킹(Hooking) 하고 있다.

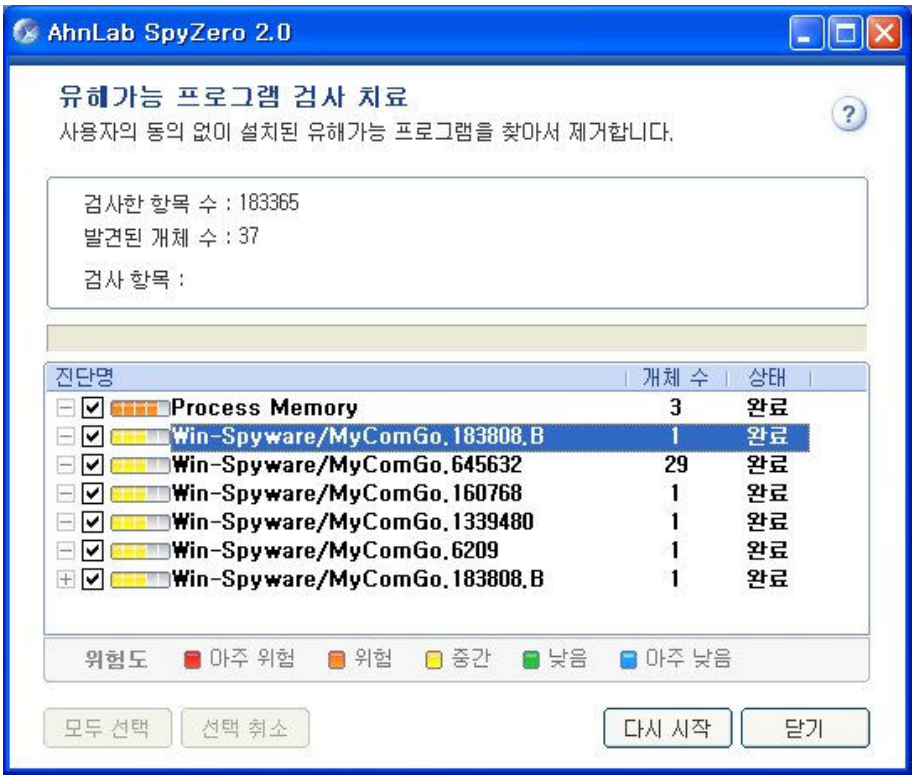
```
mov     edx, ds:ZwQueryDirectoryFile                ; 함수의 위치를 얻는다.
mov     eax, [edx+1]                                ; 함수위치 다음 1바이트의 값, 즉 서
                                                    비스 번호로 KeServiceDescriptorTabele 의 인덱스번호를
                                                    기억한다.
mov     ecx, ds:KeServiceDescriptorTable
mov     edx, [ecx]
mov     dword ptr [edx+eax*4], offset MyZwDir       ; 4바이트인 함수주소 목록에서 위에서
                                                    구한 인덱스 만큼에 위치한 ZwQueryDirectoryFile 함수를
                                                    MyZwDir 함수로 변경한다.
mov     eax, ds:ZwQuerySystemInformation
mov     ecx, [eax+1]
mov     edx, ds:KeServiceDescriptorTable
mov     eax, [edx]
mov     dword ptr [eax+ecx*4], offset MyZwSysInfo
```

위의 코드로 인해 ZwQueryDirectoryFile 함수와 ZwQuerySystemInformation 함수는 각각

Win-Spyware/MyComGo.6209 가 정의한 MyZwDir 함수와 MyZwSysInfo 함수로 윈도우 시스템 함수의 기능을 변경한다. 변경된 함수에서는 윈도우 파일시스템이 넘겨준 파일 및 폴더명이 "_systemcom.go"로 시작하는지 비교 후 일치할 경우 윈도우 시스템에게 반환하지 않음으로써 은폐동작을 수행한다.

```
push    ODh                     ; pszObjName 의 문자열 길이
push    offset g_szObjName      ; "_systemcom.go"
lea     ecx, [ebp+pszObjName]   ; 시스템이 넘겨준 비교할 문자열
push    ecx                     ; char *
call    strncmp
add     esp, 0Ch                ; strncmp 함수의 파라미터 개수 * 4바이트
test    eax, eax                ; strncmp 결과값 검사
jnz     short loc_101520        ; "_systemcom.go"와 같지 않을 경우 Skip
```

랜섬웨어에 의해 숨겨진 파일들을 얻기 위해서는 스파이제로를 실행하여 아래 그림과 같이 Win-Spyware/MyComGo 로 진단되는 항목들을 치료 하고 시스템을 재부팅하면 %SystemDrive%₩_systemcom.go 폴더가 보이는 것을 확인할 수 있다.




[그림 2-9] 랜섬웨어 설치 후 스파이제로 진단/치료 결과 화면

**'N'으로 시작하는 파일 은폐하는 루트킷**

루트킷을 사용하여 스파이웨어를 제작하는 것이 최근 트렌드이다. 2005년 소니(Sony)사에서

루트킷을 배포하여 이슈가 된 적이 있었으나, 그 후로 국내 샘플 중 한 달에 두 건 이상의 루트킷이 많은 사용자들에게 피해를 입히는 것을 발견되는 것은 처음 있는 일이다. 루트킷 관련 자료 및 개발 방법들을 인터넷에서 쉽게 구할 수 있어 루트킷을 사용하는 스파이웨어가 지속적으로 발견될 것으로 쉽게 예상할 수 있을 것이다.

11월 21일 기업 고객을 시작으로 바탕화면에 바로 가기가 실행되지 않는 다는 이슈가 접수되기 시작했다. 분석 결과 밝혀진 원인은 Win-Spyware/RootKit.Ntspl.4068으로 진단되는 루트킷에 의해서 "N"으로 시작하는 파일들이 은폐되어 정상 프로그램 중에서도 "N"으로 시작하는 파일들이 정상적으로 수행되지 않았던 것이다.

Win-Spyware/RootKit.Ntspl.4068 으로 진단되는 시스템 드라이버는 위에서 살펴본 랜섬웨어의 루트킷과 동일한 방법으로 NtQueryDirectoryFile 과 NtQuerySystemInformation 함수를 후킹하는 방법을 사용하고 있다. Win-Spyware/RootKit.Ntspl.4068은 Win-Spyware/Ntspl.704512으로 진단되는 ntspl.exe 파일을 은폐하려는 목적으로 제작되었고, ntspl.exe 는 윈도우 서비스로 등록되어 지정된 웹 페이지에서 다운로드 목록을 받은 후 이에 기록된 다운로드 경로의 파일들을 다운로드 하는 동작을 한다.

**다운로더 경로에 "별 이름" 또는 국가명을 사용하는 스파이웨어 증가**

11월 초부터 특정 도메인(http://5566****9900.com) 앞에 "별 이름"을 사용한 URL을 이용하는 스파이웨어 샘플 접수가 증가되었다. 한편 비슷한 시기에 증가를 보인 스파이웨어 중 http://aabb****eeff.com 도메인을 사용하는 스파이웨어들이 증가하였는데, 이 도메인 앞에는 국가명을 사용한 URL를 조합하여 사용되었고, 특히 이 두 개의 도메인 등록정보를 검색한 결과 동일한 사람에 의해 등록된 것으로 밝혀졌다.

특히 이런 종류의 샘플들은 동일한 실행압축 툴을 사용하여 실행압축 되어있었는데, 그 실행압축 툴의 기능으로써 파일 및 레지스트리 등의 시스템 모니터링 툴을 실행하지 못하도록 하여 분석을 방해하고 있었다.

스파이제로에서는 "별 이름"을 사용하는 스파이웨어의 진단명에는 "별 이름"을, 국가이름을 사용하는 스파이웨어에는 국가이름을 축약하여 진단명으로 사용하였다. 각각 예를 들어 금성(Venus) 이름을 사용하는 스파이웨어에게는 Win-Downloader/Venus.241664, 불가리아(Bulgaria) 이름을 사용하는 스파이웨어에게는 Win-Downloader/Bul.241664 로 진단명을 결정하였다.

### Win-Spyware/Crypter 변형 증가

오래 전 크립터 (Win-Spyware/Crypter)가 발견된 이후 스파이제로뿐만 아니라 다른 안티 스파이웨어 업체에서도 Virtumonde 등의 진단명으로 지속적으로 진단 추가해왔다. 크립터는 진단을 회피하고자 BHO로 설치되는 이름을 변경하거나 외부에 노출된 함수명을 변경하는 등 다양한 변형을 만들어낸 스파이웨어이다. 그러나 최근 상당히 많은 변화를 가진 샘플이 접수되고 있는 상황이다.

이전 크립터의 특징으로, 윈도우 로그온 시 메시지를 윈도우로부터 전달 받을 수 있도록 특정 레지스트리에 등록되는 형태와는 대조적으로 최근에 접수된 크립터는 윈도우 시작 프로그램으로 등록되고 실행되면 익스플로러(exeplorer.exe) 프로세스에 인젝션(Injection)되어 동작한다. 또한 이전 크립터와 실행파일 압축알고리즘이 상당 부분 달라졌고 동적 로드 파일의 외부 노출 함수가 외부로 노출되지 않고 있다는 점이 특징이다. 반면 서버와 주고 받는 모든 데이터는 암호화하고 서버에서 받은 명령에 의해 파일을 다운로드 하거나 팝업 광고를 띄우는 등 의 증상은 이전과 동일하다.

### (3) 시큐리티 -- Mac OS X 보안 위협 증가

마이크로소프트 사에서 이번 2007년 11월에 발표한 보안 업데이트는 총 2개로 긴급(Critical)과 중요에 해당하는 업데이트였다. 매월 발표되는 보안 패치의 개수와 비교하면 이번 달은 비교적 적은 보안 업데이트가 이뤄졌다. 특히 이번 취약점들은 관련 공격코드 형태가 공개되어 있어 더욱 주의가 요구되는 만큼 마이크로소프트에서 제공하는 보안업데이트 기능을 통하여 최신의 보안 패치를 유지할 것을 권고한다.

적은 수의 보안패치 때문인지 이번 달은 특별한 보안적 이슈가 많이 발생하지 않았던 날로 평가할 수 있으며, 다음은 악의적인 공격에 이용될 수 있는 원격 코드 실행 취약점과 살펴볼 만한 주요 취약점들에 대한 목록이다.

| 위험등급 | 취약점 | PoC |
|---|---|---|
| 긴급 | 윈도우 URI 핸드링 원격 코드 실행 취약점 (MS07-061) | 유 |
| 중요 | 마이크로소프트 DNS Spoofing (MS07-062) | 유 |
| 중요 | Apple QuickTime 7.2/7.3 RTSP 코드 실행 취약점 | 유 |

#### IE의 URI Handling 취약점과 PDF 제로데이 공격코드

최근 발표된 MS07-061 의 URI Handling 취약점은 다른 종류의 파일을 처리할 때 다른 응용프로그램을 수행할 수 있는 기능을 제공하는 부분에서 취약점이 발생하였다. 윈도우 쉘은 운영체제 내에서 특정 파일을 어떤 응용프로그램이 처리하게 될지를 결정하는데, 이것은 우리가 이미지 파일을 클릭했을 때 적절한 응용프로그램이 수행되어 보여지는 것을 생각해 보면 쉽게 이해해 볼 수 있다. URI 핸들러는 “mailto”, “news”, “nntp”, “snews”, “telnet” 등이 있으며 사용자가 위와 같은 URI를 클릭할 경우 적절한 프로그램이 수행되게 된다. 바로 이 URI 에서 사용자 입력을 제대로 체크하지 않아 취약점이 존재하여 윈도우 ShellExecute 핸들러에 조작된 URI 를 넘길 수가 있다. URI 핸들러 상에 “%” 캐릭터가 존재하는 경우 ShellExecute()는 시스템에 등록된 응용프로그램을 수행하지 않고 CreateProcess() 를 호출하여 지정된 프로그램을 수행시킬 수 있게 된다. 예를 들어 다음과 같은 명령어를 브라우저에서 전달하면 임의의 명령어가 실행가능 하게 된다.

예1) mailto:test%../../../../windows/system32/calc.exe".cmd
예2) nntp:../../../../../Windows/system32/telnet.exe" "test.com 80%.bat

이 취약점은 위와 같이 조작된 웹 페이지에 방문하거나, 또는 악의적 정보를 담고 있는 PDF 파일을 오픈하였을 경우 수행이 가능하게 된다. 이번 취약점과 관련하여 인터넷 상에서 많이 언급되었던 것이 바로 “PDF Zero day” 이다. 최근에 언급되고 있는 이 취약점이 결국

MS07-061 의 취약점을 이용한 부분이기 때문에 직접적으로 PDF 의 취약점으로 보기에는 어렵다. PDF 의 경우 AcroJS 의 스크립트를 사용하고 있는데 다음과 같은 코드를 통해서 Alert 창을 띄울 수 있게 된다.

<</S /JavaScript /JS ({app.alert₩("TEST"₩)})>>

즉, PDF 파일내에 URI를 이용한 방법의 공격코드를 삽입해 놓고 사용자가 웹에 올려진 PDF 파일을 보는 경우 공격코드가 수행될 수 있게 된다.

이번 취약점은 사용은 어렵지 않은 만큼 패치가 되어 있지 않은 경우 바로 패치를 적용하여 악의적 공격으로부터 시스템을 보호할 것을 권고한다.

**윈도우 환경만 위험한 게 아니다.**

10월달에 Mac OS X 레퍼드(Leopard) 출시된 이후에, Mac OS X은 사용자를 점차 늘려나가고 있는 중인데, 11월14일 수요일 애플 컴퓨터사에서는 Mac OS X 및 관련 응용프로그램의 취약점 41 개 패치를 발표 소식이 있었다. 이번 취약점에는 Mac OS X 에서 임의의 코드를 실행할 수 있거나 시스템 또는 프로그램을 비 정상 종료 시킬 수 있는 것들이 포함되어 있다.

이외 윈도우 XP SP2 와 윈도우 비스타에서 애플 퀵타임 소프트웨어의 패치되지 않은 공격코드도 공개되어 많은 위험성을 노출시켰다. 이번 취약점은 퀵타임 7.2 와 7.3 그리고 이전 버전 또한 영향을 받는 것으로 알려져 있는데 RTSP(Real Time Streaming Protocol)을 처리하는 부분에 취약점이 존재한다. 이 취약점을 이용해 조작된 웹 사이트 또는 악의적으로 첨부된 메일의 첨부파일을 오픈할 경우 공격자는 악성코드를 컴퓨터에 설치하는 등의 악의적 행동을 수행할 수 있다. 이번 RTSP 취약점을 이용한 공격코드가 이미 여러 개 인터넷 상에 공개되어 있는 만큼 더욱 주의가 요구되고 있다.

또 Mac OS X 시스템을 대상으로 하는 트로이목마 프로그램도 확산되어 있다는 보고도 있었다.  물론 이번 트로이목마가 맥 시스템에서 나타난 첫 악성코드 사례는 아니지만 지속적으로 Mac 에서도 악의적 형태가 계속 나타나고 있다는 점이 주목할 만한 것이다.

사용자가 있다는 것은 결국 악의적으로 이용될 수 있는 가능성이 존재하는 만큼 새로운 위협 출현에 더욱 주의를 기울여야 할 것이다.

**모질라 파이어폭스와 취약점**

가장 많은 사용자층을 확보하고 있는 인터넷 익스플로러 브라저의 사용자층을 조금씩 넓혀나가고 있는 브라우저가 파이어폭스 이다. 오픈 소스로 개발되고 있으며 점차 그 세력을 넓혀가고 있는 브라우저 중에 하나이다. 보통의 악성코드와 취약점은 일반적으로 잘 알려진 소프트웨어를 대상으로 많이 하고 있는데, 이는 많은 사용자층을 확보하고 있기 때문에 공격의 효과를 크게 볼 수 있기 때문이다. 파이어폭스 또한 점차 취약점의 보고도 많이 나타나고 있고 이를 악용한 공격코드도 증가추세에 있는 실정이다.

최근에도 발표된 취약점 JAR 프로토콜의 XSS 취약점을 이용하여 사용자의 로그인 정보를 획득하거나 임의의 컨텐츠를 업로할 수 있는 것이 취약점이 발표되었다.

이렇듯 현재 파이어폭스2에서 2007년에 공식적으로 발표된 보안권고문(Mozilla Foundation Security Advisory)은 39개에 이르며 2006년에 발표된 것까지 포함하면 파이어폭스 2에서만 약 50여개의 이르는 취약점이 공식적으로 존재하는 것이다.

취약점을 찾는 사람과 이러한 취약점을 방어하기 위해 끊임없이 이어지는 전쟁은 과연 언제까지 이뤄질 것인가? 아마도 컴퓨터와 소프트웨어가 존재하는 한 끊이지 않을 것이다.

[참고]
모질라의 시큐리티 정보는 다음의 블로그를 통해서 많이 얻을 수가 있다.
http://blog.mozilla.com/security