ASEC Report 10월

® ASEC Report

2005. 11

안철수연구소의 시큐리티대응센터(AhnLab Security E-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.

SUMMARY

전반적인 악성코드 피해 감소, 트로이목마 발견비율 증가…

안철수연구소로 10월에 신고된 악성코드 피해 Top 10을 살펴보면 1위는 여전히 넷스카이 웜이 차지하고 있다. 그러나 Top10 순위를 차지하고 있는 악성코드 10개 중 6개는 10월에 새로이 발견된 신종(변형)이며, 그 중에서 4개는 마이톱 웜 변형이며 2개가 리니지핵 트로이 목마이다. 10월에 마이톱 웜 변형이 많이 발견되어 피해를 입힌 이유로는 마이톱 웜 소스가 공개되어 이를 이용한 변형이 많이 제작되었기 때문인 것으로 보인다. 10월 국내에서 발견된 신종(변형) 악성코드는 전체적인 발견건수는 감소하였으나, 트로이목마의 발견비율은 여전히 증가한 추세를 보이고 있다. 이는 과거의 전통적인 해킹의 형태와는 달리 최근에는 해킹을 한 후 트로이목마를 설치하여 다른 악성코드를 다운로드하거나 사용자 정보를 유출하는 형태로 변화되고 있기 때문으로 파악된다. 또한 10월에는 PSP와 닌텐도 DS용 트로이목마가 출현하여 업계의 관심을 모아지기도 하였다. 세계 악성코드 동향을 살펴보면 일본과 유럽을 중심으로한 지역은 여전히 매스메일러에 의한 피해가 많은 반면, 중국은 온라인게임 사용자의 계정과 비밀번호를 유출하는 목적의 트로이목마에 의한 피해가 많은 것으로 나타났다. 10월 발견된 신종(변형) 유해가능 프로그램의 경우는 그 발견추이는 이전과 비슷한 비율을 보이고 있으나 제작방법적인 면에서는 더욱 교묘해지고 있어 안티 스파이웨어 업체와의 숨바꼭질이 계속되고 있다. 10월에는 MS에서 총 9개의 정기 보안패치가 발표되었다 이중 3개의 보안패치가 '긴급'의 등급을 가지고 있으며, 이중에서 특히 MS05-047 취약점은 이를 이용한 웜의 출현까지 예견되고 있어 주의가 필요하다.

이달의 ASEC 컬럼에서는 인터넷을 이용한 사기 프로그램의 위험성에 대해 살펴보고, XSS를 이용한 새미 웜의 출현과 이에 대한 향후 전망을 예측해 보았다.

I. 10월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자: 조성준 주임연구원(sjcho@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	130	10.5%
2	-	Win32/Maslan.C	109	8.8%
3	New	Win32/Mytob.worm.27480	76	6.1%
4	New	Win32/Mytob.worm.41824	37	3.0%
5	New	Win32/Mytob.worm.48640.C	36	2.9%
6	New	Win32/Mytob.worm.51062	33	2.7%
7	New	Win-Trojan/LineageHack.46836.B	29	2.3%
8	New	Win-Trojan/LineageHack.330240	25	2.0%
9	↓4	Win32/Netsky.worm.31744	25	2.0%
10	↓3	Win32/Sasser.worm.15872	22	1.8%
		기타	718	57.9%
합계			1,240	

[표1] 2005년 10월 악성코드 피해 Top 10

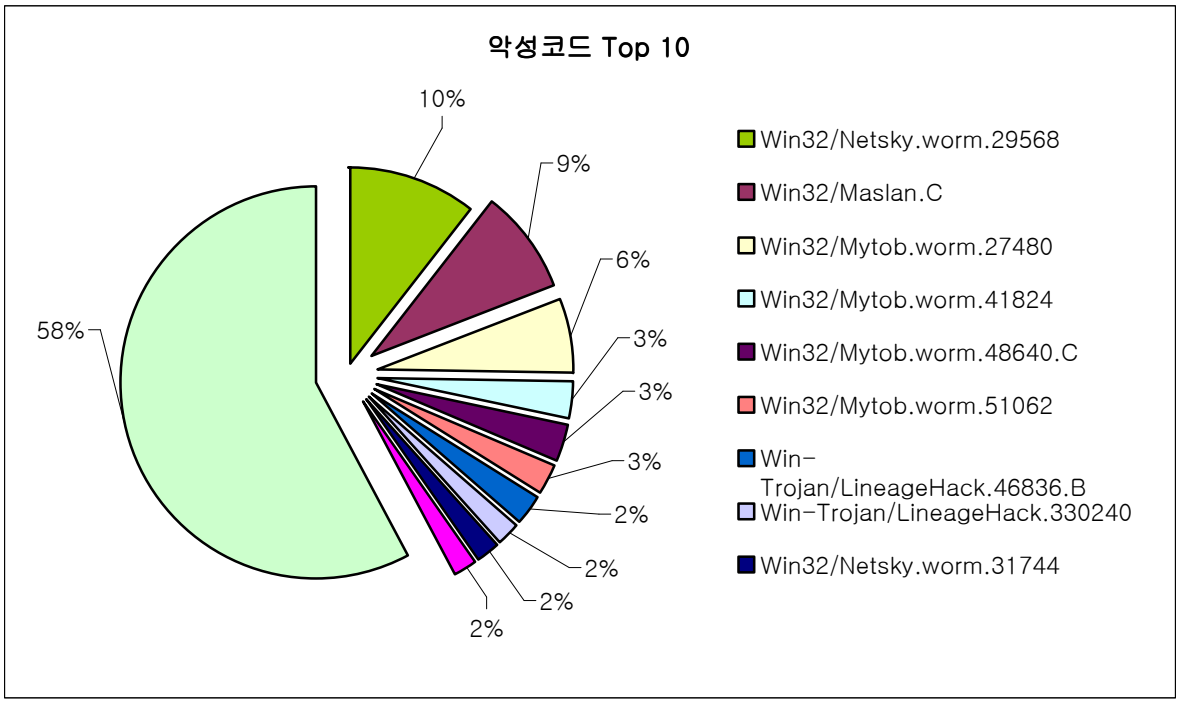
10월 악성코드 피해 동향

2005년 10월 악성코드 피해 건수는 지난달에 비해 소폭 증가한 1,240건이다.
지난달과 마찬가지로 1, 2위는 여전히 넷스카이.29568 웜(Win32/Netsky.worm.29568)과 마슬란.C(Win32/Maslan.C)가 차지하고 있으나, 10위권 내에 새로운 악성코드가 6개나 진입하는 등 지난달의 악성코드 피해 Top 10과는 다소 차이를 보이고 있다.

특히 새로 순위에 진입한 6개 중 마이톱 웜(Win32/Mytob.worm) 변형이 무려 4개를 차지하고 있는데, 그 이유는 마이톱 웜의 소스가 공개되어 이를 이용한 많은 변형이 제작되었기 때문으로 보인다. 이중에서 10월에 새로이 순위에 진입하며 3위를 차지하고 있는 마이톱.27480 웜(Win32/Mytob.worm.27480)은 일반적인 마이톱 웜과 달리 윈도우 방화벽과 인터넷 연결공유(Internet Connection Sharing, ICS)기능의 서비스를 '사용 안함'으로 변경하는 증상이 있는 것이 특이하다.

10월에는 지난 7월 많은 피해를 입혔던 리니지핵 트로이목마(Win-Trojan/LineageHack) 변형 중 2개도 새로이 순위에 진입하였다. 8, 9월 피해가 감소하였다가 다시 10월에 피해가 증가한 것은 악성코드의 버그로 인해 감염된 시스템에서 svchost.exe 파일이 런타임 에러를 일으켜 그만큼 사용자들이 감염사실을 많이 인지할 수 있었기 때문인 것으로 보인다.

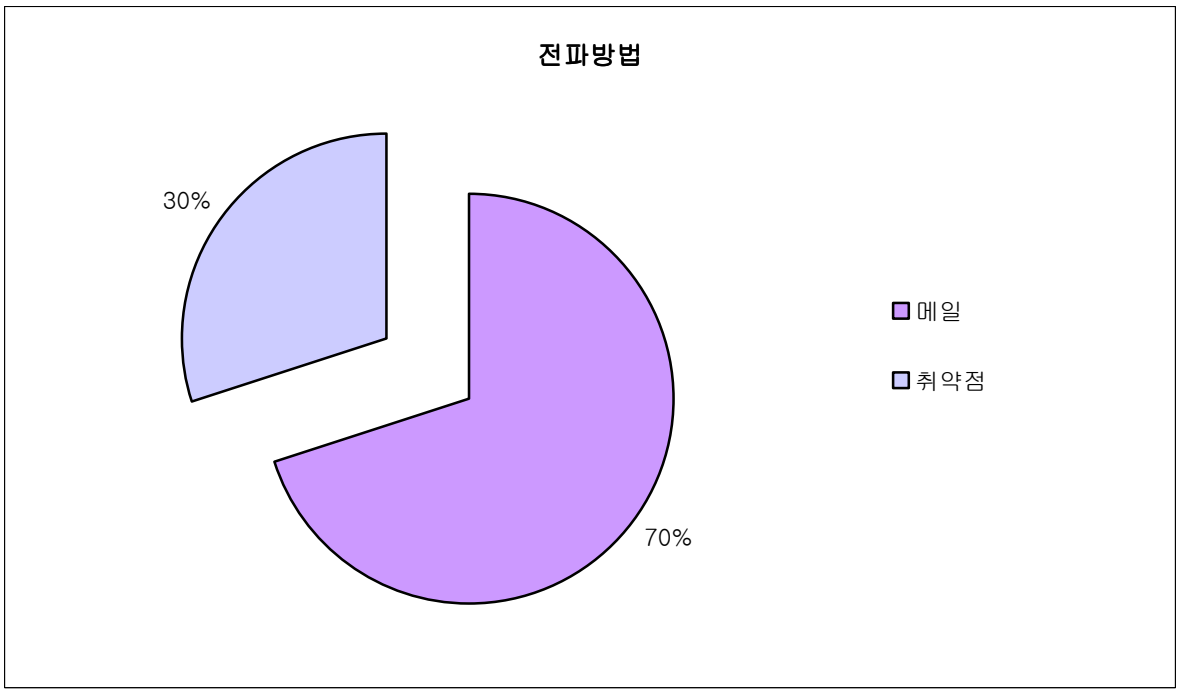
10월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.



[그림1] 2005년 10월 악성코드 피해 Top 10

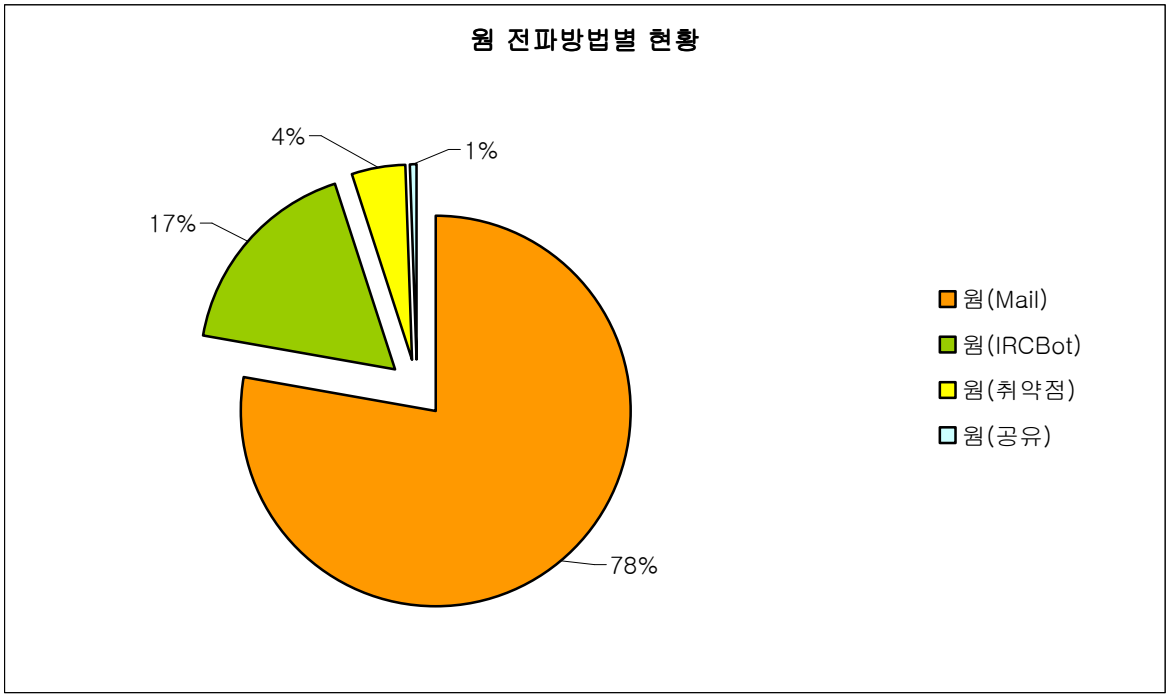
10월 악성코드 Top 10 전파방법별 현황

[표1]의 Top 10 악성코드들은 주로 어떠한 감염 경로를 가지고 있는지 [그림2]에서 확인할 수 있다.



[그림2] 악성코드 Top 10의 전파방법별 현황

[그림2]에서와 같이 피해순위 Top 10에 랭크된 악성코드의 70%가 메일을 이용하여 전파되고 있다. 이는 지난 8월부터 메일을 이용한 전파 비율이 50%에서 9월에 60%로 현재 매월 10%씩 계속 증가하고 있는 추세이며, 이와 반대로 네트워크와 운영체제 취약점을 이용한 전파 비율은 지난 8월 50%에서 9월 40%, 10월에는 30%로 매월 10%씩 계속 감소하고 있다.

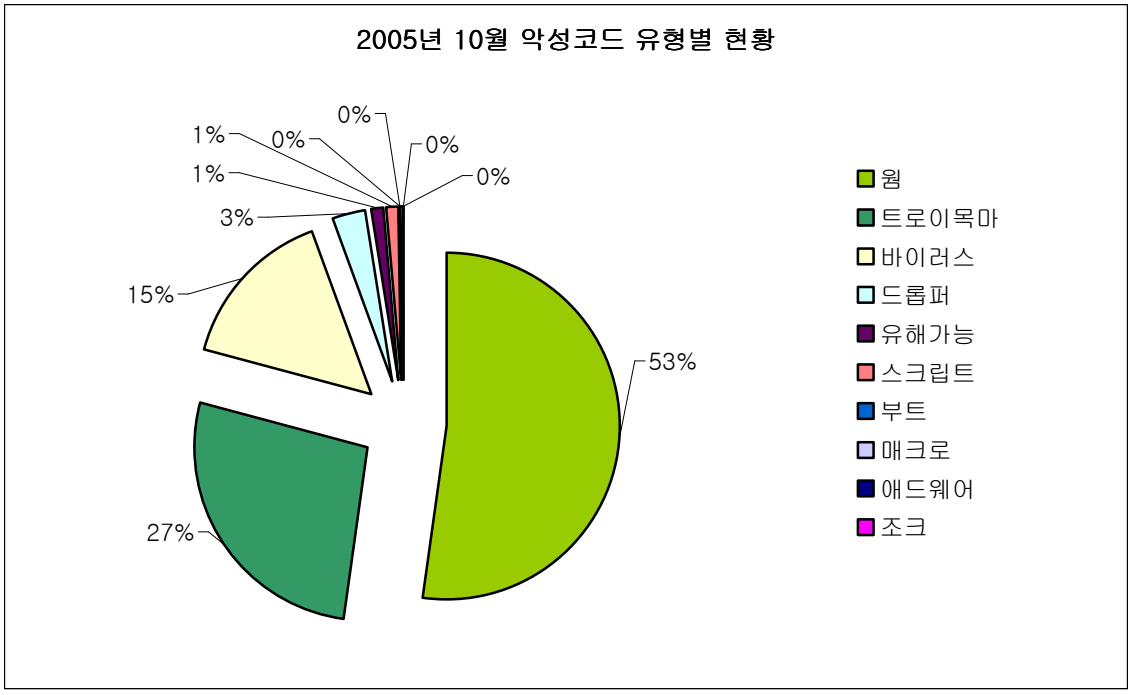


[그림3] 웜의 전파방법별 현황

[그림3]은 10월에 피해 신고된 웜의 전파방법에 대한 현황이다. 이 또한 [그림2]와 유사하게 이메일(Mail)을 이용한 웜의 전파는 전월에 비해 7% 증가하며 계속하여 증가하는 추세이다. 반면 인터넷 채팅(IRC), 취약점은 각각 9월에 비해 4%, 3% 감소하여 10월에는 각각 17%, 4%를 차지하고 있다.

피해신고 된 악성코드 유형 현황

10월에 피해신고 된 악성코드를 유형별로 분류해 보면 [그림5]와 같다.

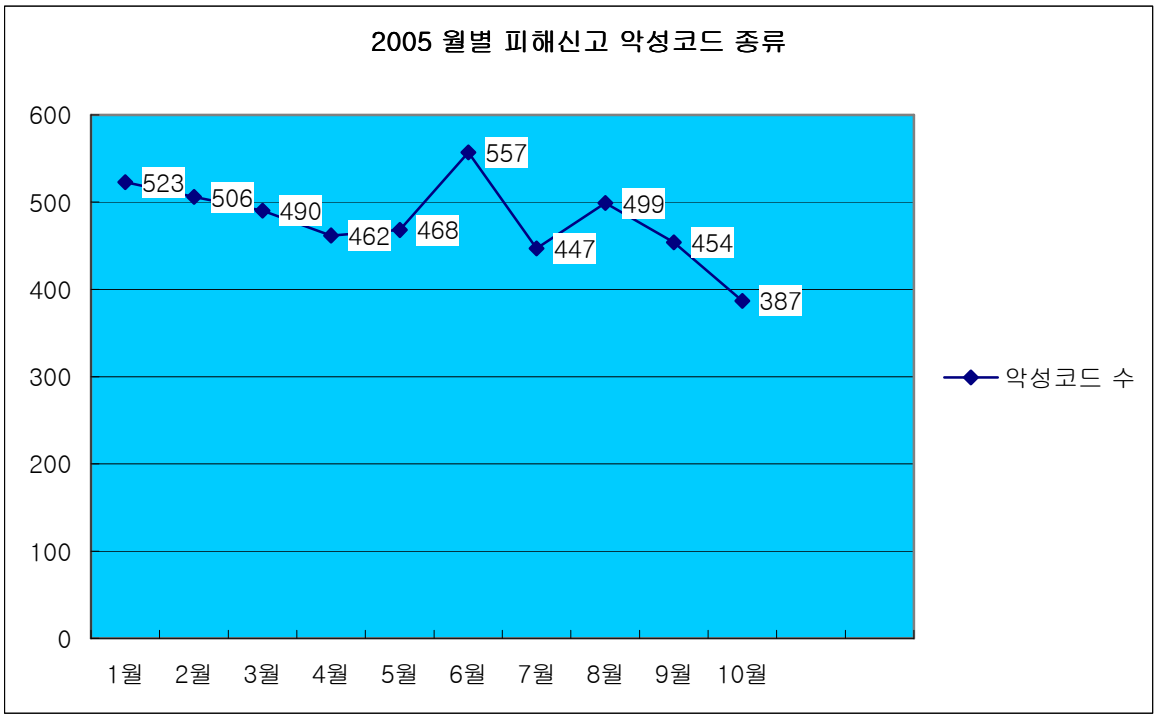


[그림5] 악성코드 유형별 현황

10월에는 9월에 비해 웜이 2% 가량 감소하여 53%를 차지한 반면, 트로이목마는 전월에 비해 2% 증가하여 27%를 차지하고 있다. 꾸준히 증가하던 바이러스 비율도 지난 9월에 비해 다소 감소한 추세이다.

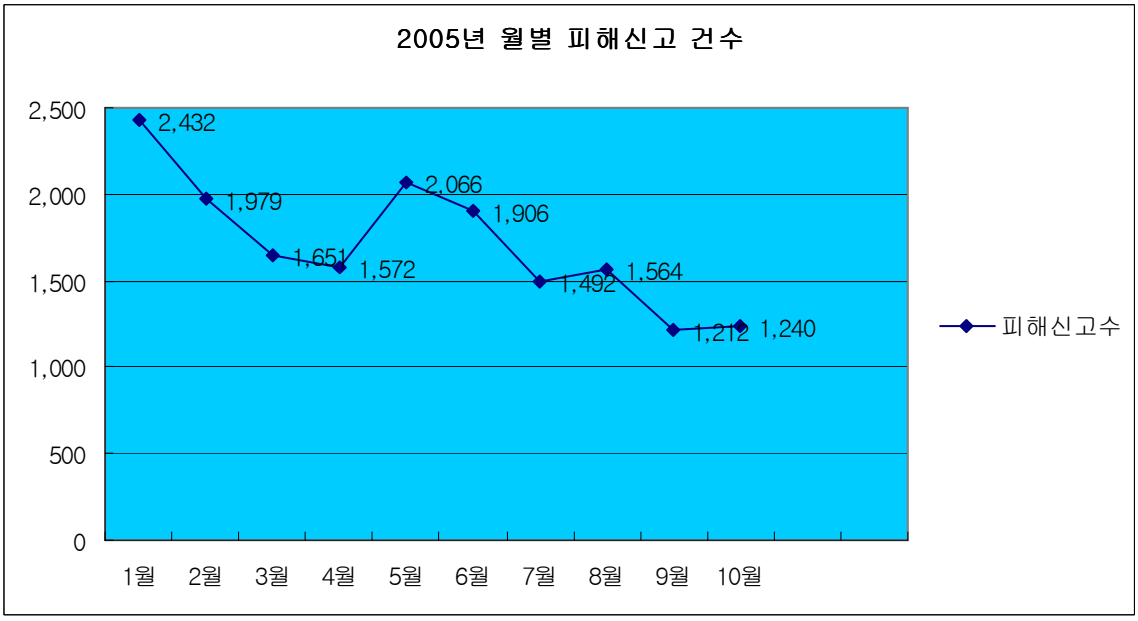
월별 피해신고 된 악성코드 종류 현황

10월에 피해 신고된 악성코드 진단명은 387개이며, 지난 9월에 비해 67건 정도 감소하였다. 올해는 리니지핵 트로이목마 변형의 피해가 많았던 6월과 8월을 제외하고는 전반적으로 피해 신고되는 악성코드의 종류가 감소하고 있는 추세이다.



[그림4] 2005년 월별 피해신고 악성코드 종류

월별 피해신고 현황



[그림5] 2005년 월별 피해신고 건수

2005년 악성코드 피해건수는 리니지핵 트로이목마 변형이 다수 발견, 피해를 입히면서 다소 증가했을 뿐 전반적으로 감소하는 추세를 보이고 있다. 이는 [그림4], [그림5]와 같이 2005

년 피해신고 된 악성코드 종류에 대한 추이와 동일한 추이를 보이고 있는 것으로, 올해는 전반적으로 악성코드에 의한 피해도 감소하고 피해를 입히는 악성코드의 종류도 감소하고 있는 것으로 보인다.

(2) 신종(변형) 악성코드 발견 동향

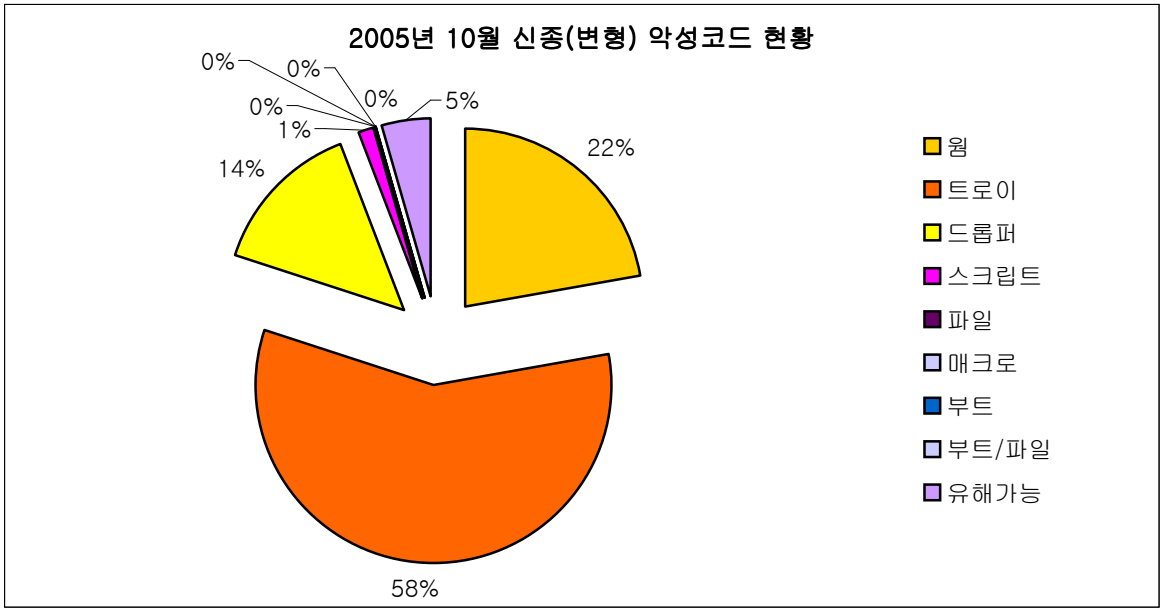
작성자: 정진성 주임연구원 (jsjung@ahnlab.com)

10월 한달 동안 접수된 신종(변형) 악성코드의 건수는 [표1]과 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
39	101	25	2	0	0	0	0	8	0	175

[표1] 2005년 10월 유형별 신종(변형) 악성코드 발견현황

10월에 접수된 신종(변형)악성코드가 차지하는 유형을 비율로 살펴보면 [그림1]과 같다. 10월에는 트로이목마가 지난달에 비해 7% 증가한 58%를 차지하고 있다..



[그림1] 2005년 10월 신종(변형) 악성코드 비율

최근 3개월 동안 국내에서 접수되는 신종(변형)악성코드의 수는 [표2]와 같이 감소추세를 보이고 있다. 이에 대한 가장 큰 원인은 지난 호에 자세히 소개한 악성 아이알씨봇 웜(Win32/IRCBot.worm)의 접수가 줄었기 때문이다.

월	웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
8월	70	123	29	2	1	1	0	0	10	0	236
9월	58	116	30	7	0	1	0	0	13	0	225
10월	39	101	25	2	0	0	0	0	8	0	175

[표2] 2005년 8월 ~ 10월 유형별 신종 (변형) 악성코드 발견현황

지난 3개월의 악성코드 발견현황을 살펴보면 전반적인 악성코드 발견수치는 감소하고 있지만, 다른 악성코드에 비해 트로이목마의 발견수치는 월등히 많은 수치를 보이고 있다. 이는 해킹을 하는 이들이 과거의 해킹 목적과는 다른 형태로 해킹을 하고 있기 때문이다. 즉, 과

거와 달리 최근에는 해킹을 한 후 트로이목마를 설치하여 다른 악성코드를 다운로드하거나 사용자 정보를 유출하도록 하는 형태가 증가한 것이다. 이로 인해 최근 발견되고 있는 트로이목마의 유형은 다음과 같은 형태를 보이고 있다.

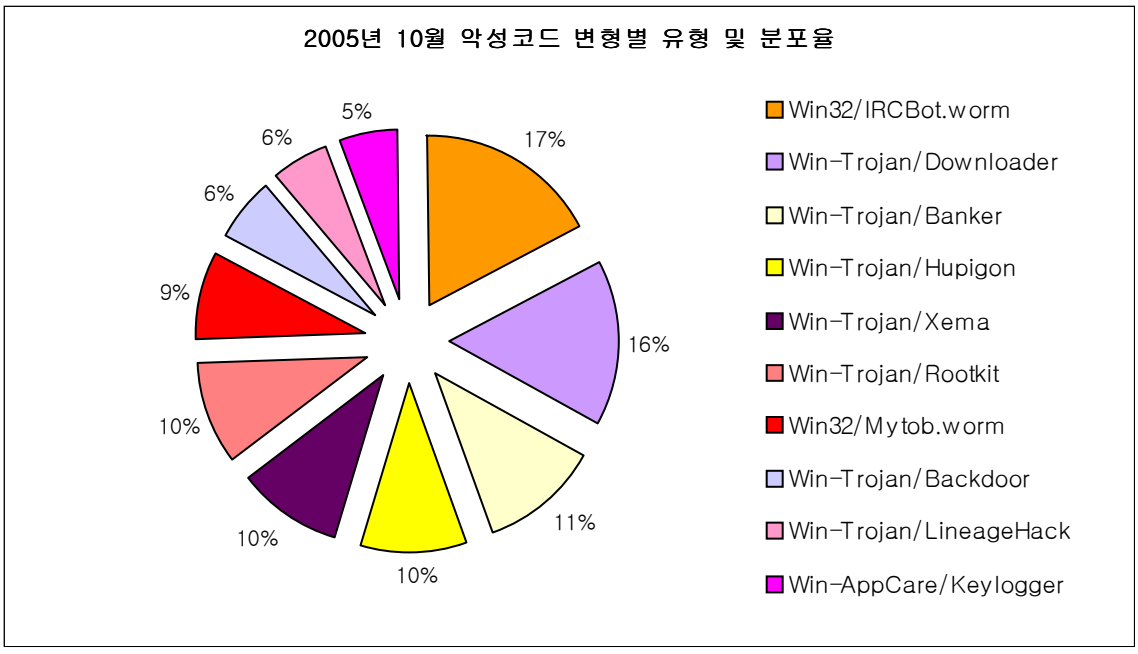
- 온라인 게임의 계정을 탈취하는 유형
- 다른 악성코드를 다운로드 하는 유형
- (은폐형) 키로깅 및 원격제어 증상을 갖는 유형

또한 이번 달에는 자신의 프로세스 및 파일, 레지스트리 등을 숨기는 은폐기법(Stealth technologies)을 사용하는 트로이목마가 다수 발견 되기도 하였으며, 다음과 같다.

- 피씨클라이언트 트로이목마(Win-Trojan/PcClient)
- 핵스도어 트로이목마(Win-Trojan/Haxdoor)
- 핵데프 트로이목마(Win-Trojan/HacDef)

이 트로이목마들은 은폐된 상태로 동작하며 주로 숨겨진 포트를 오픈하여 악의적인 목적을 가진 사용자로부터의 접속을 대기한다. 일반적으로 은폐기법을 사용하는 악성코드들은 사용자 및 안티 바이러스로부터 검색을 회피할 목적으로 주로 이용된다.

[그림2]는 10월에 V3엔진에 추가된 악성코드 중 진단명별로 가장 많은 변형을 가지고 있는 악성코드 Top 10을 보여주고 있다. 악성코드의 유형 중 가장 많은 변형을 가지고 있는 것은 트로이목마 형태였으며, 그 중에서 다른 악성코드를 다운로드하는 트로이목마 형태가 가장 많았다. 단일 악성코드명 중에서는 악성 아이알씨봇 웜에 대한 변형이 가장 많았다.

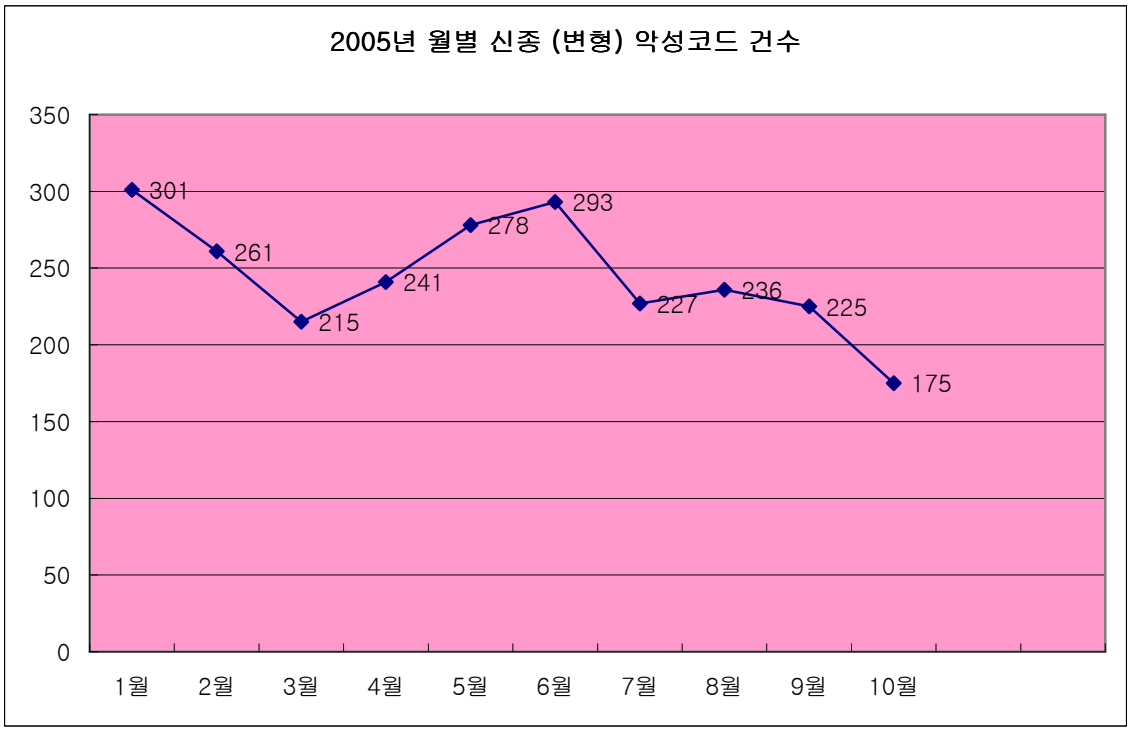


[그림2] 악성코드 변형별 유형 및 분포율

뱅커 트로이목마(Win-Trojan/Banker)는 은행 웹사이트 로그인시 사용자 계정을 훔쳐내는 증상을 가지고 있는 것으로 국내에서는 발견되지 않았지만 외국에서는 다수 발견보고가 있

었다. 후피곤 트로이목마(Win-Trojan/Hupigon)는 그레이버드 트로이목마(Win-Trojan/GrayBird)의 변형 중에 하나이며 중국에서 제작 되어졌다. 최근 들어 중국 發 해킹 때문에 이 변형이 증가하고 있는 추세이다.

[그림3]은 2005년 월별 신종(변형) 악성코드 건수를 나타낸 것이다. 6월부터 전체적으로 접수되는 악성코드의 수가 줄어들고 있다. 위에서 언급한 것처럼 전체 접수건수는 줄어들고 있지만 중국 發 해킹과 더불어 트로이목마의 피해는 이전보다 더욱 늘어나고 있는 실정이다.



[그림3] 2005년 월별 신종(변형) 악성코드 발견 현황

10월 주요 신종(변형) 악성코드

이번 달에는 휴대용 게임기에서 동작하는 악성코드 2종류가 발견되었다. 이 악성코드들은 짧은 시간차이를 두고 발견 되었으며, 두 기종 모두 개인들이 홈브루(Homebrew) 프로그램-전문 개발자(사)가 아닌 개인이 제작한 응용 프로그램-을 제작하는 것이 가능하기 때문에 트로이목마가 제작 될 수 있었던 것으로 보인다.

또한 차기 윈도우 버전인 윈도우 비스타 베타1이 베타 테스터들에게 공개 되었는데, 공개된 지 얼마 되지 않아 윈도우 비스타 베타1에 포함된 닷넷 프레임웍 2.0(.NET Framework 2.0)에서 동작하는 바이러스가 공개되었다. 이는 일반적인 형태의 겹쳐쓰기 바이러스이며 이전에도 닷넷 프레임웍 2.0을 필요로 하는 바이러스들이 보고 된 적은 있었다.

MS04-047은 MS04-039 와 같은 PnP 관련 취약점이며 10월에 보고 되었는데, 이 취약점을 이용한 악성코드가 일부 안티 바이러스 업체에 의해서 보고 되어 주목을 받았었다. 그러나 이를 분석해본 결과 이전 취약점을 이용한 것으로 밝혀져 결국은 해프닝으로 끝나기도

하였다. 이는 제로데이 공격(Zero Day Attack)에 관한 위협이 점점 커지고 있기 때문에 나타난 재미난 사건이라고 할 수 있겠다.

이슈가 되었던 이번 달의 악성코드는 다음과 같다.

► 피씨클라이언트 트로이목마(Win-Trojan/PcClient)

최근 국내에서 다수 발견 보고된 트로이목마로, 중국에서 제작된 것으로 추정되며 은폐형이다. 이 트로이목마는 자신의 파일 및 레지스트리를 숨기기 위하여 특정한 커널 함수를 후킹(Hooking)하는 방식의 은폐기법을 사용하고 있다. 정상 인터넷 인터넷 익스플로러에 자신을 인젝션(Injection)하는 형태로 동작하며 백도어 포트를 오픈 해 두고 있다. 인터넷 익스플로러에 자신을 인젝션하는 동작은 그레이버드 트로이목마(Win-Trojan/GaryBird)와 매우 유사한 형태인데, 이 경우 일부 클라이언트 방화벽들은 아웃바운드 접속을 탐지해 내지 못하기도 한다.

► 은폐형 악성코드 다소 증가

피씨클라이언트 트로이목마를 비롯하여 전형적인 은폐형 악성코드인 핵스도어 트로이목마, 핵데프 트로이목마 변형들이 다소 증가하였다. 또한 최근 몇 달 사이에 트로이목마가 급증하면서 위에 열거된 트로이목마 이외에도 은폐증상을 가지고 있는 트로이목마들의 발견, 보고가 잦아지고 있다. 은폐형 악성코드는 감염된 시스템으로부터 샘플확인 및 수집이 어려운 문제가 있으며 은폐기법을 잘 아는 안티 바이러스 전문가 혹은 전용 검사 프로그램을 이용하는 경우에만 찾아 낼 수 있다.

► 플레이스테이션 포터블(PSP)과 닌텐도(Nintendo) DS 용 트로이목마 등장

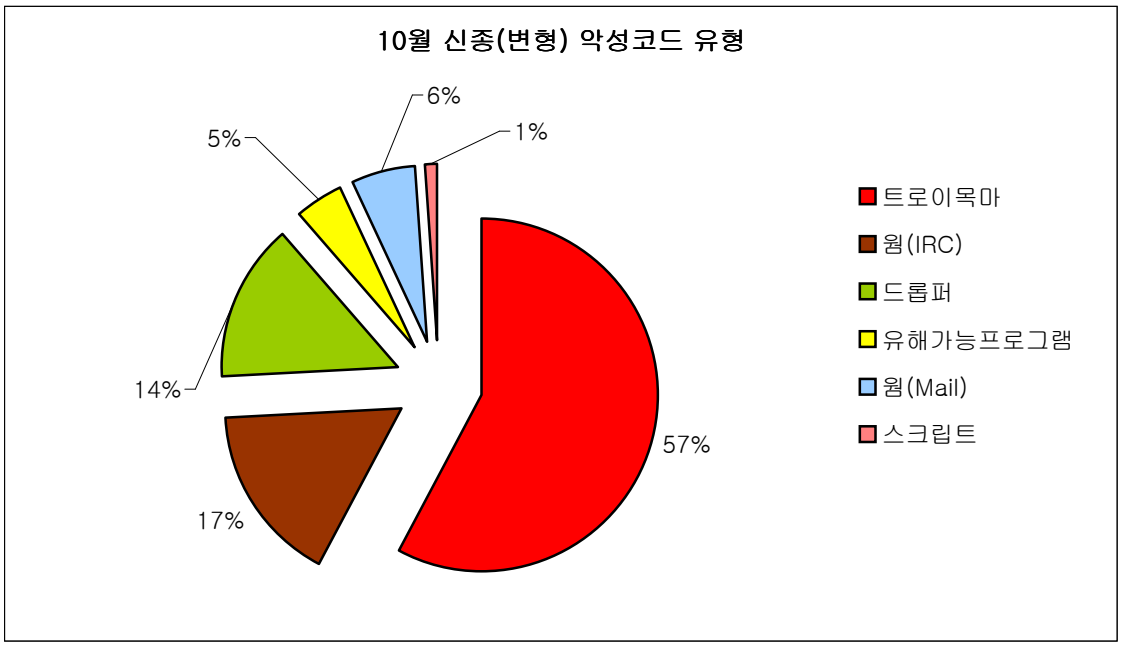
개인이 제작한 홈브루 프로그램의 동작이 게임기에서 가능한 시기부터 휴대용 게임기의 악성코드 등장은 예견되어 왔다. 일반적으로 게임기 제작사는 응용 프로그램 개발사에만 SDK(Software Development Kit)를 제공한다. 하지만 게임기와 같은 새로운 하드웨어들은 해커들의 집중적인 분석을 받게 되는 게 일반적이다. PSP 경우 일반적으로 홈브루 프로그램을 실행할 수 없지만 PSP 롬을 수정하거나 특정 버전으로 다운그레이드를 한 롬을 이용하면 실행이 가능한 방법이 공개되었다. 보고된 PSP 트로이목마도 PSP의 펌웨어를 해킹해 준다는 제목의 파일명으로 위장되어 있었다. 트로이목마가 실행되면 롬 바이오스의 특정 영역을 손상하여 이후 PSP가 부팅 할 수 없도록 만든다.

닌텐도 DS 트로이목마는 PSP 트로이목마가 발견된 지 얼마 되지 않아서 보고 되었다. IRC를 통해서 누군가 고의로 유포 하였다. 닌텐도 DS 는 ARM CPU를 사용하며 ARM CPU는 PDA와 같은 모바일 기기에 주로 사용되기 때문에 응용 프로그램 제작 및 리버스 엔지니어링 자료가 많이 소개 되어 있다. 이 트로이목마도 실행하면 게임기의 롬 바이오스를 손상하여 이후 해당 게임기의 부팅이 불가능하게 된다.

휴대용 게임기들의 악성코드 출현은 새롭지만 예상 되어 왔다. 첫 출현한 악성코드의 형태는

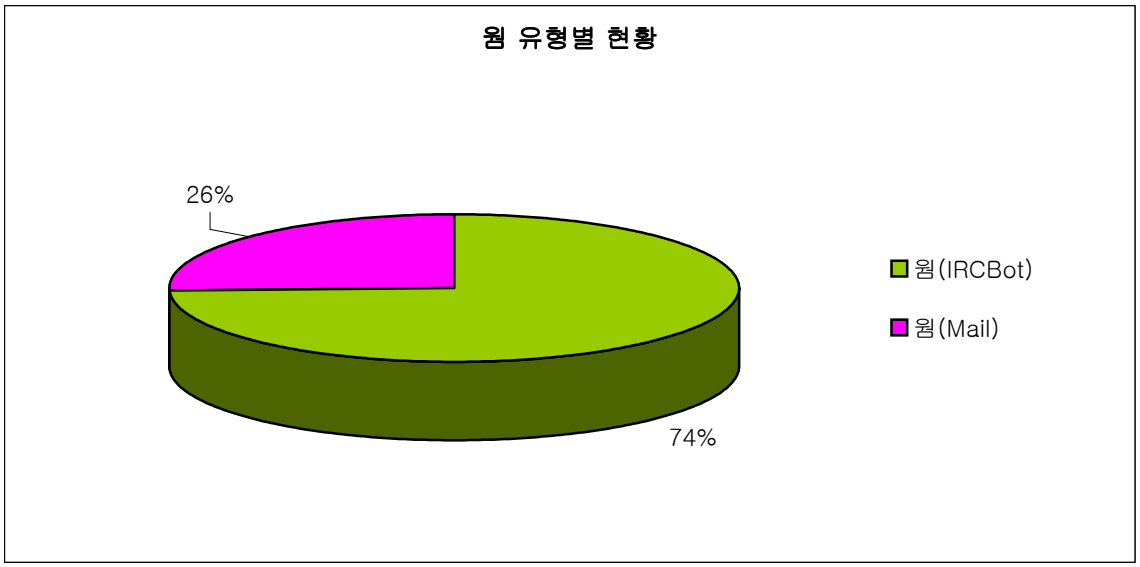
트로이목마였고 해커들이 시스템이나 파일구조를 더 파악하고 있는 중이라면 다른 유형의 악성코드 등장도 예상 해볼 수 있다.

[그림4]는 이번 달에 발견된 신종(변형) 악성코드에 대한 유형 분포이다.



[그림4] 10월 신종 (변형) 악성코드 유형별 현황

10월 신종(변형) 악성코드 유형 중 웜을 유형별로 분류해 본 결과, [그림5]와 같이 메신저나 P2P 웜은 발견되지 않고. 통상 발견되는 매스메일러(Mass Mailer)와 악성 아이알씨봇 웜들만 발견, 보고되었다.



[그림5] 10월 신종(변형) 웜 유형별 현황

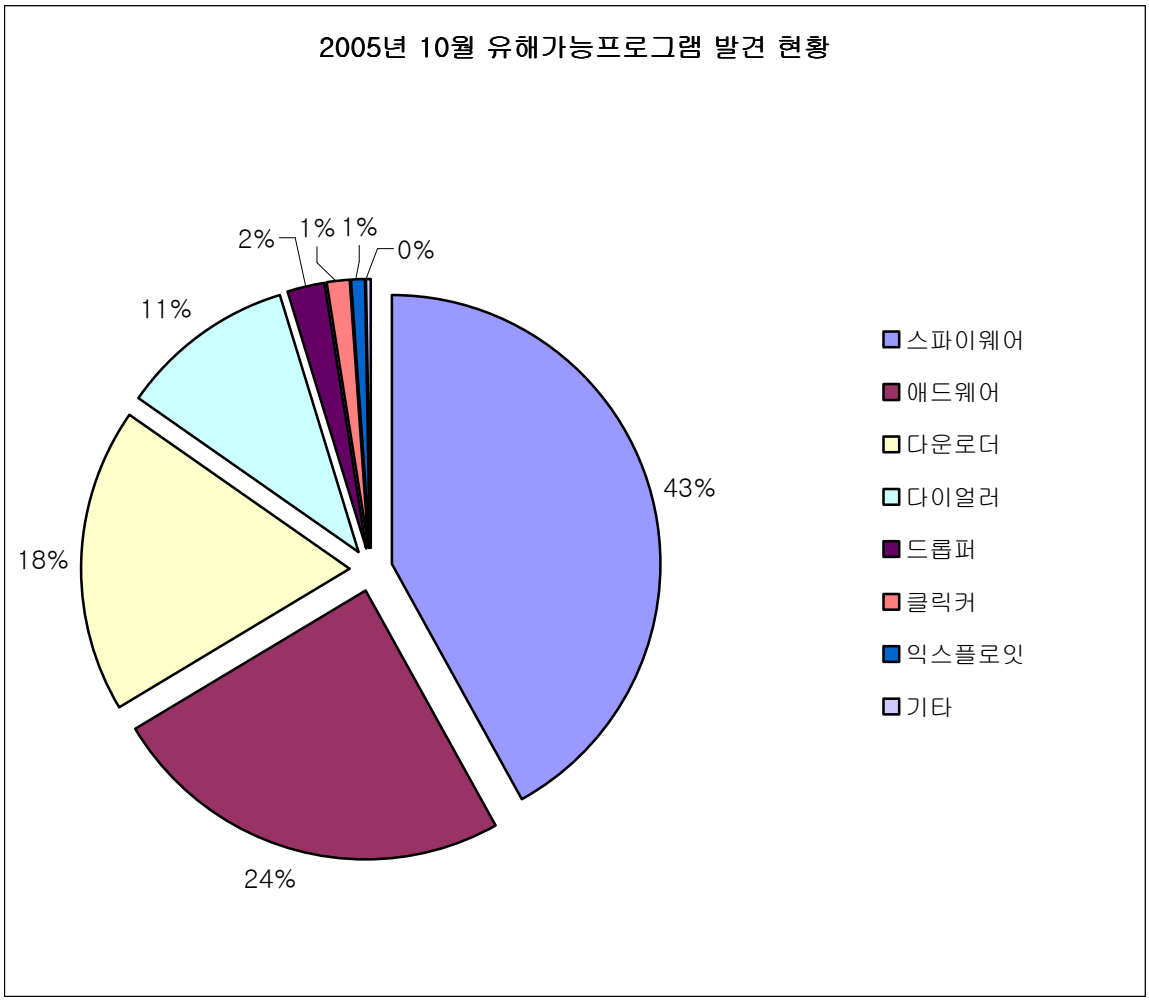
II. 10월 AhnLab 스파이웨어 동향

작성자: 박호진 주임연구원(hojinpk@ahnlab.com)

10월 한달 동안 접수된 신종(변형) 유해가능 프로그램 건수는 [표1], [그림1]과 같다. 4분기가 시작되는 10월에는 특이한 현상을 보이지 않았고 이전 분기와 비슷한 유해가능 프로그램 발견 비율을 보이고 있다.

스파이웨어	애드웨어	다운로더	다이얼러	드롭퍼	클릭커	익스플로잇	기타	합계
630	366	275	160	33	21	10	6	1501

[표1] 10월 유형별 신종(변형) 유해 가능 프로그램 발견 현황



[그림1] 2005년 10월 발견된 유해가능 프로그램 비율

아직 스파이웨어의 범주가 표준화되지 못한 상황에서 스파이웨어들이 다양한 방법으로 사용자에게 접근하고 있고, 특히 은폐형 기술인 루트킷(RootKit) 방법들이 보다 교묘해지고 있어

안티 스파이웨어 업체들간의 숨바꼭질은 여전히 계속되고 있는 상황이다.
최근에는 소니 뮤직이 자사의 CD 음반에 DRM(Digital Rights Management)기술의 일종인 불법복제를 방지하기 위한 기술로 루트킷을 사용하고 있어 구설수에 오르내리는 일이 있었다. 보안업체들은 이것이 악성코드 제작자들에 의해서 악용될 수 있다며 심각한 우려의 목소리를 내었고, 얼마 후 소니 측에서는 루트킷 드라이버(aries.sys)를 제거하는 업데이트를 시행하였다.

스팸 블로그 '스프로그'

요즘 블로그가 폭발적인 인기를 누리면서 스프로그(splog)가 기승을 부리고 있다. 스프로그는 스팸 블로그(spam blog)의 약어로 광고수익이나 블로거 자신의 다른 사이트를 홍보하기 위해 만들어진 블로그를 지칭하는 말이다.
스프로그는 특히 최근 주목받고 있는 '키워드를 나열해 검색 엔진의 상위권을 차지하는 등의 방법'으로 블로그 방문자들을 유인하는 경우가 많으며, 스크립트나 ActiveX를 이용해 프로그램 설치를 유도하는 방법으로 선량한 방문자를 괴롭히기도 한다. 스프로그가 기승을 부리면서 앞으로 피싱과 결부된 사기성 블로그도 등장할 것으로 우려된다.

서버 해킹을 통한 악성코드 유포

서버 해킹을 통해 악성코드를 유포하는 기법은 이제 전 세계적인 유행처럼 보인다. 최근의 해킹은 특정 사이트에 악의적인 스크립트를 심어 놓음으로써 다른 악성코드를 유포하도록 이루어지고 있으며, 10월 초에만 대략 1만개에 다다르는 사이트들이 이에 악용되고 있는 것으로 추정된다. 해커들은 이러한 악의적인 자바 스크립트들을 인터넷 익스플로러나 파이어폭스(Firefox)의 iFrame 취약점을 이용하거나 윈도우의 알려지거나 알려지지 않은 보안 취약점을 이용하여 심어놓고 있다.

스파이웨어에 대한 외국의 정의

지난 8월에 정보통신부에서 스파이웨어를 정의한 것에 이어 이번 달에는 ASC(Anti-Spyware Coalition)에서 스파이웨어를 정의한 최종 문서를 발표하였다. ASC는 잠재적으로 원하지 않는 기술들과 스파이웨어를 둘러싼 논쟁들 속에서 정의와 실천들에 관한 의견을 일치하는데 헌신적인 그룹이다. 이 단체는 안티 스파이웨어 업체들과 학교, 그리고 소비자 그룹들로 구성되었고, 스파이웨어와 다른 잠재적으로 불필요한 기술을 통제하는 문제에 대한 다양한 전망을 모으려 하고 있다. 이곳에서 정의하고 있는 스파이웨어와 그밖에 잠재적으로 원하지 않는 기술은 아래와 같다

스파이웨어와 그밖에 잠재적으로 원하지 않는 기술들[1]

[1] ASC(Anti-Spyware Coalition), http://www.antispywarecoalition.org

기술들은 적절한 사용자의 동의없이 전개되거나 혹은 사용자 통제를 약하게 하는 여러 가지 점에서 이행된다.

* 사용자의 경험, 개인정보 또는 시스템 보안에 영향을 미치는 물질 변화
* 컴퓨터에 설치된 프로그램들에 포함된 시스템 자원을 사용
* 개인적이거나 다른 민감한 정보를 수집, 사용, 배포

III. 10월 시큐리티 동향

작성자: 김지훈 주임연구원(smallj@ahnlab.com)

10월 발표된 보안취약점 동향과 주요 이슈들을 살펴보자

10월에 발표된 보안 취약점 동향

이번 달에는 마이크로소프트사(이하 MS)의 10월 정기 보안 패치가 총 9개 발표되었다. 이중에는 3개의 긴급 보안 공지(MS05-050, MS05-051, MS05-052)가 포함되어 있으므로 이에 대해 반드시 보안 패치를 적용하도록 한다.

특히, 플래그 앤 플레이의 취약점으로 인한 원격 코드 실행 및 로컬 권한 상승 문제점(MS05-047)은 지난 8월의 플러그 앤 플레이(Plug and Play, PnP) 서비스 취약점(MS05-039)과 유사한 것이어서 이 취약점을 이용한 웜의 출현이 조심스레 전망되고 있다. MS05-047 취약점은 윈도우 2000와 XP의 PnP 서비스 상에서 레지스트리 키 이름에 다량의 백슬래쉬(\)를 지정함으로써, 특정 함수가 호출될 때 스택 오버플로우가 존재하게 되는 것이다. 이 취약점이 발표된 이후 이를 이용한 공격코드가 계속 발견되었으므로, 반드시 패치를 적용하여야 하겠다.

2005/10/11 MS05-047 MS에서 보안취약점 권고문 공개
2005/10/21 MS05-047 첫번째 공격코드 발견
2005/10/24 MS05-047 두번째 공격코드 발견

10월의 주요 취약점 현황[1]은 다음과 같다.

위험 등급	취약점	공격코드 유/무
HIGH	플러그 앤 플레이의 취약점으로 인한 원격 코드 실행 및 로컬 권한 상승 문제점 (MS05-047)	유
HIGH	DirectShow의 취약점으로 인한 원격 코드 실행 문제점 (MS05-050)	무
HIGH	MSDTC 및 COM+의 취약점으로 인한 원격 코드 실행 문제점 (MS05-051)	무
HIGH	nternet Explorer 누적 보안 업데이트 (MS05-052)	무

[1] 취약점 현황은 ASEC 의 보안전문가들에 의해 공격코드 유/무, 악성코드 활용가능성, 취약점의 위험도등 다양한 관점에서 판단하여 선별된 것으로, 사용자들의 주의가 필요한 것임을 나타낸다. 공격코드의 존재유무는 이 리포트를 작성하는 시점에서 인터넷 상에서 접할 수 있는 기준으로 작성되었다

► 보안 패치의 중요성과 또 다른 위협

우리는 이미 수 차례의 인터넷 대란과 최근 조톱 웜(Win32/Zotob.worm)의 제로데이 공격(Zero-Day Attack)위협을 통해 보안 패치가 얼마나 중요한 것인지 실감하고 있다. 한국정보보호진흥원(KISA)의 '인터넷 침해사고 동향 및 분석 월보' 10월 자료에 따르면 보안 패치가 적용되지 않은 PC를 인터넷에 연결할 경우 평균 생존가능 시간이 약 15~ 20분에 불과하다고 한다. 그러나 이렇듯 중요한 보안 패치가 종종 시스템의 위협요소로 변질되기도 한다. 즉, 보안 패치를 적용한 후 오히려 시스템에 예기치 못한 영향을 주는 경우도 있다.

10월에 발표되었던 MS 보안 패치 2건(MS05-051과 MS05-052)에서 이런 위험요소가 발견되었으며, MS에서는 이 패치에 버그가 존재함을 공식적으로 공지하였다. MS05-051과 MS05-052 보안 패치 적용 시 야기될 수 있는 시스템 영향은 다음과 같다.

- %windir%₩registration 디렉터리의 기본 액세스 제어 목록 사용 권한을 변경한 시스템에 COM+ 및 MS DTC용 Microsoft 보안 공지 MS05-051을 설치한 후 여러 가지 문제가 발생할 수 있다. (KB 909444[1])
- Microsoft 보안 공지 MS05-052을 설치한 후 웹페이지에 포함된 ActiveX 컨트롤이 인터넷 익스플로러에 올바르게 적재되지 않을 수 있다. (KB 909738[2], KB 909889[3])

시스템의 취약한 부분을 보완하기 위한 보호 수단이 또 다른 피해를 초래했을 때, 보안 패치에 대한 고객 불안과 불신은 그 어떠한 것으로도 치유할 수 없을 것이다.
보안 패치는 시스템의 취약점을 제거하는 가장 확실하고 유일한 방법이며, 고객은 보안 패치 제공 업체에 대한 강한 신뢰를 바탕으로 보안 패치의 적용을 진행하고 있다. 보안 패치 제공 업체는 이러한 보안 패치의 중요성을 다시금 상기하고, 보안 수단이 도리어 시스템에 해를 끼치는 일이 없도록 더더욱 신중을 기해야 할 것이다.

► 웹 서비스 보안 강화를 위해 취약점 점검 서비스 활용

ASEC 리포트를 포함한 대부분의 보안 사이트에서 웹 서비스 보안에 대해 끊임없이 이슈를 제기하여 왔다. 그럼에도 불구하고 국내외 주요 포털 사이트 등의 웹서버 해킹 피해 사례가 끊임없이 접수되고 있다. 공격자들의 웹서버 해킹 목적은 금적적인 이득을 취하게 위한 것으로, 크게 두 가지로 요약해 볼 수 있다. 첫째, 악의적인 IFRAME 코드를 삽입하여 사이트 방문 고객 PC에 키로거 등의 악성코드를 자연스레 유포한 후 고객의 개인정보 빼내가는 것, 둘째, 정상적인 웹서버를 해킹해 위장 사이트를 개설한 후 피싱 경유지로 악용하는 것이다.
또한, 10월 초에는 웹서버의 취약점을 이용하는 XSS(Cross-Site Scripting) 웜이 출현하기도 하였다. MySpace 사이트의 한 사용자가 많은 친구들을 만들기 위한 방법을 생각하다 XSS를

[1] http://support.microsoft.com/kb/909444
[2] http://support.microsoft.com/kb/909738
[3] http://support.microsoft.com/kb/909889

이용한 스크립트를 만들게 되었고, 이로 인해 해당 사이트가 일시적인 서비스 장애를 겪게 되었다.

이와 같이 웹서버의 취약점을 이용한 홈페이지 변조와 악성코드 삽입, 피싱사이트 악용 등 해킹 사고 피해를 예방하기 위해서 다음과 같은 보안 대책이 필요하다.

- 홈페이지 구축의 전 단계에 충분한 보안성을 고려
- 사용자 입력 값 검증을 통해 SQL 인젝션(Injection) 취약점을 제거
- 공격에 이용될 수 있는 데이터베이스의 불필요한 확장 저장 프로시져 제거

이 밖에도, 홈페이지 보안 세미나에 참석하거나 보안 업체를 통해 홈페이지 취약점 점검 서비스를 받아보는 것도 웹서비스 보안 강화를 위한 좋은 활동이라 할 수 있을 것이다.

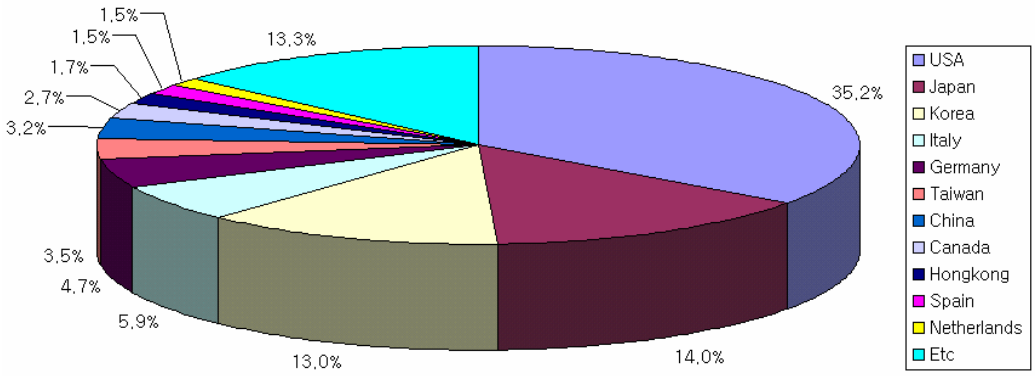
Ⅳ. 10월 세계 악성코드 동향

10월 세계 악성코드 동향은 일본과 유럽을 중심으로 메일로 전파되는 매스메일러의 강세가 여전히 지속되고 있는 반면 중국에서는 개인 정보 유출을 시도하는 트로이목마기 기승을 부리고 있는 것으로 분석되었다. 이러한 중국의 트로이목마는 온라인 게임의 사용자 계정과 비밀번호를 외부로 유출하는 것이 주목적이며, 인접한 국가들인 한국, 대만 및 일본에 까지 그 영향이 확대되고 있어 그에 따른 피해들이 우려되고 있다.
그리고 휴대용 게임기인 PSP와 닌텐도에서 실행되는 악성코드도 발견이 되어 악성코드의 영향력이 모바일 장비를 넘어 휴대용 게임기에 까지 영향을 미치는 것으로 나타나 그에 따른 파급도 커질 것으로 보여진다.

(1) 일본의 악성코드 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

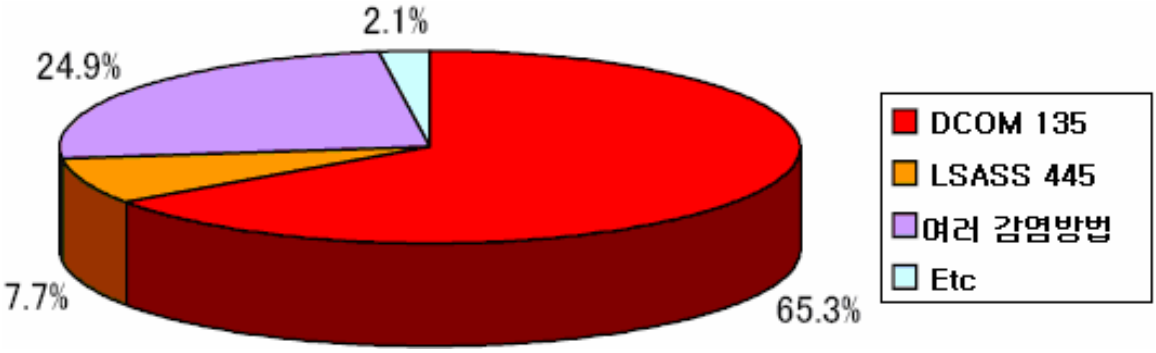
일본 경찰청(www.cyberpolice.go.jp)에서 2005년 상반기에 파악한 봇넷(Botnet) 현황을 발표했다. 봇넷이란 원격제어 기능을 가진 악성코드를 무작위적으로 배포한 후 감염된 시스템에서 배포자가 명령한 작업을 수행할 수 있도록 구성한 서버/클라이언트 방식의 네트워크를 말하며, 주로 서비스 거부(DoS) 공격, 스팸메일 발송, 개인정보 획득과 같은 악의적인 동작을 위해 사용된다. [그림1]은 일본 경찰청의 자료 중 봇넷 서버를 운영하고 있는 IP 주소의 국가별 비율을 도표로 나타낸 것이다. 대부분의 서버가 미국과 일본, 한국에 위치하고 있는 점이 이채롭다.



[그림1] 국가별 봇넷 서버 현황(출처: 일본 경찰청)

발표 자료에서 파악된 봇넷 서버의 도메인은 모두 143개이고 이들 도메인에서 사용하고 있는 IP주소는 664개였다. 이중 일본으로 밝혀진 IP주소는 93개로 14%를 점유하고 있다.

[그림2]는 감염을 위해 주로 사용되는 취약점에 대한 정보이다. 윈도우 시스템의 DCOM 취약점을 이용한 공격이 대부분을 이루고 있다.

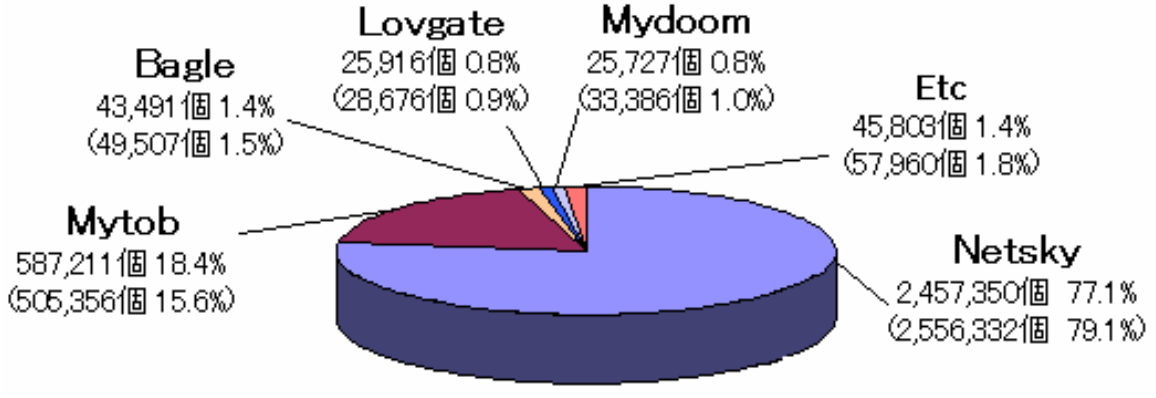


[그림2] 감염을 위한 공격 취약점 정보(출처: 일본 경찰청)

OS의 취약점을 악용하여 자동으로 감염 대상을 검색하는 형태의 봇넷 특성상 빠른 시간 동안 많은 시스템을 에이전트로 사용할 수 있고 이는 단기간에 여러 시스템을 장악하여 효과적인 공격을 시도할 수 있는 위험성을 가지고 있음을 나타내는 것이므로 항상 잠재적인 위협을 가지고 있다고 볼 수 있다. 백신 프로그램을 사용한다고 하더라도 적절히 탐지하지 못할 가능성을 배제할 수 없기 때문에 OS의 패치나 방화벽과 같은 네트워크 단계에서 감염을 방지해줄 수 있는 보안프로그램의 사용의 필요성이 요구된다.

일본 유행 악성코드 유형별 발생현황

2005년 10월 일본에서 가장 많이 확산된 악성코드는 넷스카이 웜(V3 진단명 Win32/Netsky.worm)이다. [그림3]은 일본의 IPA(www.ipa.go.jp)에서 발표한 악성코드 통계 자료 중 10월에 발생한 악성코드의 종류별 검출 통계를 나타낸 것이다. [그림3]에서 알 수 있는 것처럼 가장 많이 유포된 악성코드는 넷스카이 웜으로, 전체 검출 악성코드의 77%를 차지하고 있는 것을 볼 수 있다.



[그림3] 악성코드 검출 통계(출처: IPA)

10월 데이터에서 주목할 점은 전체 발생량은 변화가 없으나 실제 감염 등 피해가 보고된 건수가 전월에 비해 현저하게 감소한 것이다. [그림3]에서 보는 것처럼 10월 한달 동안 전체 악성코드 검출 건수는 약 319만 건으로 전월과 비교해서 크게 차이가 없다. 그러나 [표1]의

데이터는 전반적으로 매스메일러에 의한 감염 피해는 전월에 비해 약 13% 정도 감소했음을 알 수 있다.

윈도우/도스 바이러스	금월피해 전월피해	매크로 바이러스	금월피해 전월피해	스크립트 바이러스	금월피해 전월피해
Win32/Netsky	902 1,057	Xm/Laroux	11 9	VBS/Redlof	60 58
Win32/Mytob	484 634	W97M/X97M/ P97M/Tristate	4 1	VBS/Loveletter	9 9
Win32/Mydoom	299 379	WM/Cap	3 2	Wscript/Fortnight	5 0
Win32/Bagle	287 328	W97M/Lexar	1	VBS/Soraci	3 6
Win32/Lovgate	231 242	X97M/Divi	1 3	VBS/Terrosist	1 0
Win32/Klez	184 210	X97M/Pink	1 0	Wscript/Kakworm	1 7

[표1] 악성코드 피해 신고 현황

악성코드의 감염 경로별 통계

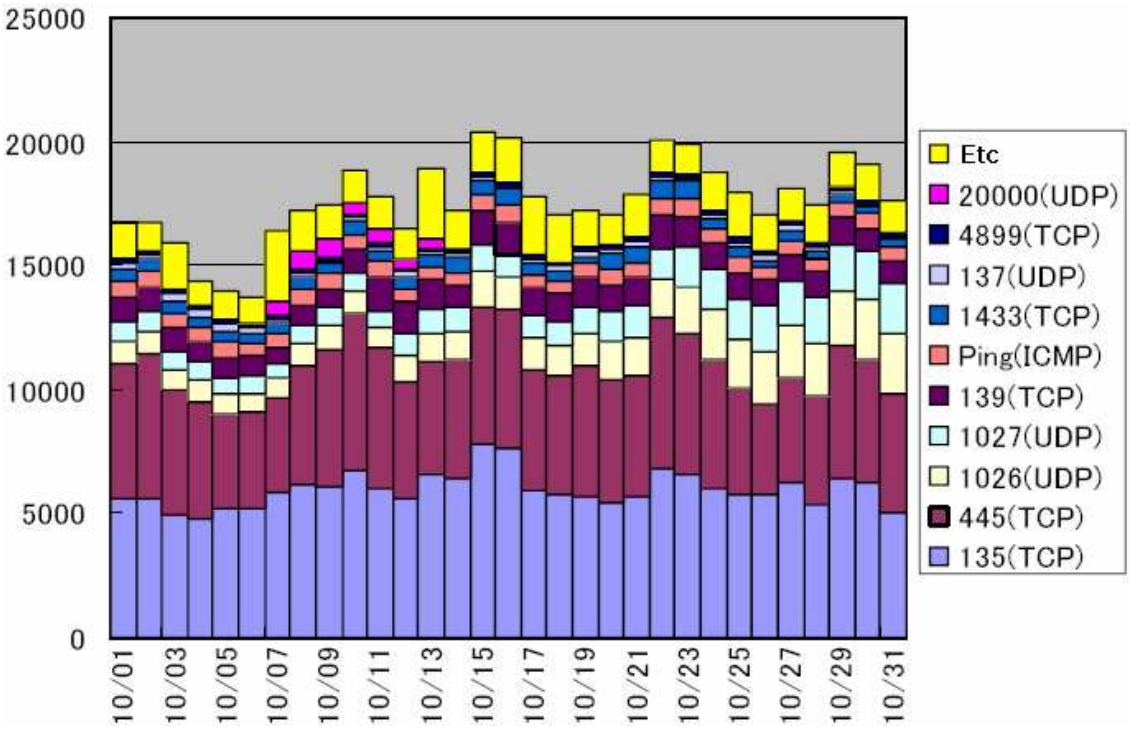
[표2]는 악성코드의 감염 경로 별 통계를 나타낸 것이다. 악성코드의 감염 경로로 많이 사용되는 매체는 메일이고 이는 전월과 차이가 없었다. 10월 통계에서 주목할 점은 네트워크를 이용한 악성코드가 점점 늘어나고 있다는 점이다. [표2]에서 보는 것처럼 전월에 비해 네트워크를 통한 감염 피해는 30여건이 증가했고 이는 취약점을 이용하여 전파되는 웜의 영향으로 생각된다.

감염경로	피해 건수					
	2005년 10월		2005년 9월		2004년 10월	
메일	3,386	94.2%	4,524	95.8%	4,586	98.5%
외부의 모체	7	0.2%	0	0.0%	1	0.0%
다운로드	1	0.0%	0	0.0%	6	0.1%
네트워크	224	5.5%	187	4.0%	51	1.1%
기타	3	0.1%	12	0.3%	10	0.2%

[표2] 악성코드 감염 경로 통계

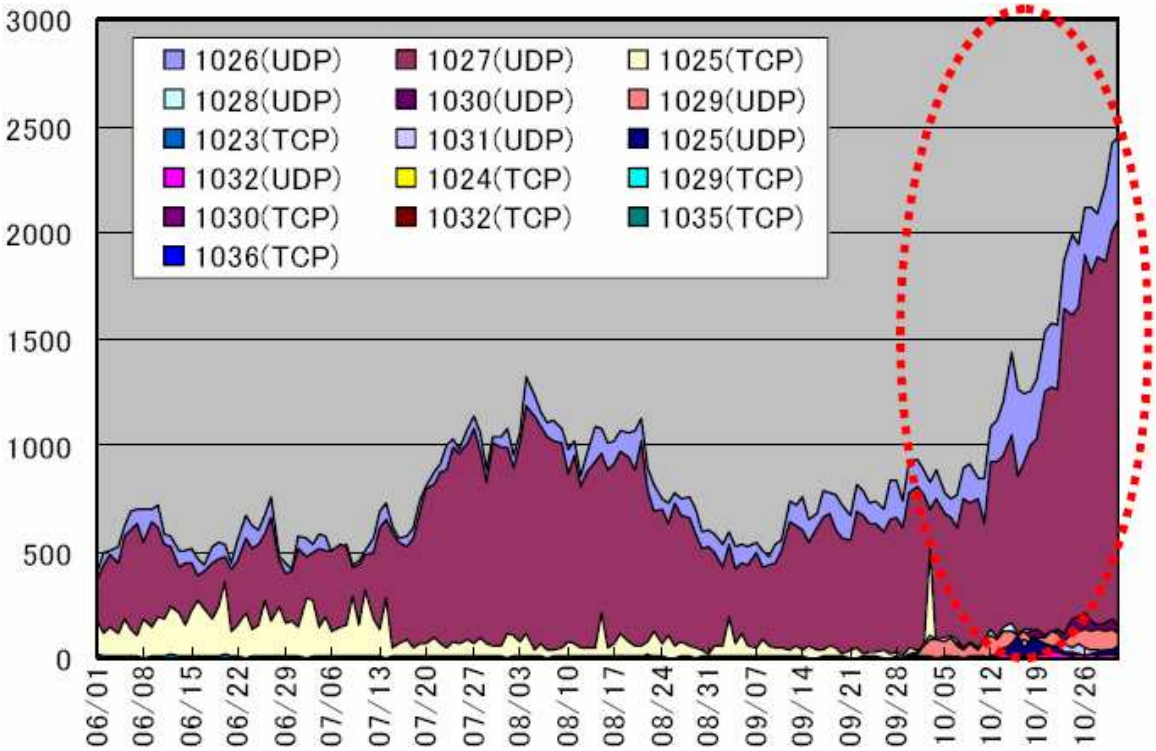
일본 네트워크 트래픽 현황

[그림4]는 10월 일본에서 발생한 네트워크 트래픽에 대한 통계이다. TCP 135 포트와 TCP 445 포트를 이용한 트래픽의 양이 매우 많은 것을 볼 수 있는데 이는 전월과 비교해서 크게 차이가 없다.



[그림4] 네트워크 포트별 트래픽 발생 통계(출처: 일본 IPA)

10월의 네트워크 트래픽 통계에서 특이한 점은 10월 들어 중국을 진원지로 하는 UDP 1026 포트와 UDP 1027 포트의 트래픽이 급증한 것이다. 두 포트는 윈도우 운영체제의 메신저 서비스에서 사용되는 포트로써 메신저 서비스를 이용하여 공격 대상 시스템에 팝업 메시지를 띄우는 경우가 발생하고 있다. 동일한 진원지 IP 주소에서 여러 대상으로 패킷을 전송하는 경우가 발생하는 것을 관측한 경우가 있는 점 등으로 미루어 불특정 다수를 향한 공격의 일종으로 생각된다.



[그림5] UDP 1026/1027 포트 트래픽 현황(출처: 일본 IPA)

(2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

10월 1일은 중국의 국경일로, 일주일간의 연휴를 즐기게 된다. 이러한 연휴 기간 동안에도 중국내의 악성코드 동향은 트로이목마를 중심으로 지속적인 증가를 보여 왔던 그레이버드 트로이목마(V3 진단명, Win-Trojan/GrayBird 또는 Win-Trojan/Hupigon)의 위협이 이번 10월에도 이어지고 있다. 이러한 그레이버드 트로이목마의 위협은 중국뿐 아니라 한국 역시 감염 피해가 증가하고 있는 것으로 분석되고 있다. 그러나 이에 반해 악성 아이알씨봇으로(IRCBot)으로 대변되는 웜들은 순위권내에서 찾아보기 힘들 정도로 대부분 급격한 감소 추세를 보이고 있다.

중국의 악성코드 TOP 5

순위 변화	순위	Rising
-	1	Backdoor.Gpigeon
-	2	Trojan.PSW.LMir
↑1	3	Trojan.PSW.QQRobber
↓1	4	Backdoor.Rbot
New	5	Trojan.PSW.QQPass

[표1] 2005년 10월 라이징(Rising) 악성코드 TOP 5

순위 변화	순위	JiangMin
-	1	Backdoor/SdBot.atp.Rootkit
New	2	TrojanDownloader.Agent.ry
New	3	Win32/Parite.a
New	4	Trojan/Script.Seeker
↓1	5	Trojan/QQMsg.Zigui.b

[표2] 2005년 10월 강민(JiangMin) 악성코드 TOP 5

[표1]과 [표2]는 중국 로컬 백신 업체인 라이징(Rising)과 강민(JiangMin)의 10월 악성코드 TOP 5이다. 이 중 [표1] 라이징의 악성코드 TOP 5를 먼저 살펴보도록 하자. 지난 9월에 이어 그레이버드 트로이목마와 엘미르핵 트로이목마(V3 진단명, Win-Trojan/LmirHack)가 1위와 2위를 그대로 유지하고 있다. 그러나 두 트로이목마는 순위 변화만 없을 뿐 전체 악성코드 분포에서는 지속적인 증가를 보이고 있는 것으로 분석되고 있다. 3위는 지난 9월 4위에서 한 계단 상승한 QQ롭 트로이목마(V3 진단명, Win-Trojan/QQRob)가 차지하고 있다. QQ롭은 중국에서 개발한 QQ 메신저에서 사용자가 입력하는 키보드 입력 값을 가로채는데 사

용되고 있는 트로이목마이다. 4위는 한 계단 순위 하락을 보인 악성 아이알씨봇 웜(V3 진단명, Win32/IRCBot.worm)이 차지하고 있다. 악성 아이알씨봇 웜은 지난 여름을 기점으로 점차적으로 감염신고가 하락하고 있는 것으로 보이며 이와 더불어 메일로 전파되는 매스메일러의 감염신고도 역시 동반 하락하고 있는 것으로 분석되고 있다. 5위는 이번 10월에 순위권 내에 새롭게 진입한 QQ패스 트로이목마(V3 진단명, Win-Trojan/QQPass)가 차지하고 있다. QQ패스 트로이목마 역시 QQ 메신저를 이용하여 사용자의 아이디와 암호를 외부로 유출하는 특징을 가지고 있는 트로이목마이다.

[표2] 강민의 악성코드 TOP 5에서는 전월에 이어 악성 아이알씨봇 웜이 1위를 차지하고 있지만 분포 면에서는 라이징 순위와 유사하게 하락세를 보이고 있는 것으로 분석되어 11월에는 급격한 하락세를 그릴 것으로 예상 된다. 2위에서 4위까지는 이번 10월 새로 순위권에 포함된 악성코드들이 자리잡고 있다. 2위는 다른 악성코드 또는 애드웨어들을 다량으로 다운로드하는 다운로더인 에이전트 트로이목마(V3 진단명, Win-Trojan/Downloader 또는 Win-Trojan/Agent), 3위는 기존에 알려진 패리티 바이러스(V3 진단명, Win32/Parite)가 차지하고 있으며 4위는 스크립트 형태인 Trojan/Script.Seeker가 차지하고 있다. 그리고 Trojan/QQMsg.Zigui.b는 한 계단 하락하여 5위를 차지하고 있다.

주간 악성코드 순위

순위	1주	2주	3주	4주
1	-	Backdoor.Gpigeon	Backdoor.Gpigeon	Backdoor.Gpigeon
2	-	Trojan.PSW.LMir	Trojan.PSW.LMir	Trojan.PSW.LMir
3	-	Backdoor.Rbot	Worm.IRC	Trojan.PSW.QQRobber
4	-	Trojan.PSW.QQRobber	Trojan.PSW.QQPass	Backdoor.Rbot
5	-	Trojan.DL.Small	Trojan.PSW.QQRobber	Worm.QQ.TopFox

[표3] 2005년 10월 라이징(Rising) 주간 악성코드 순위

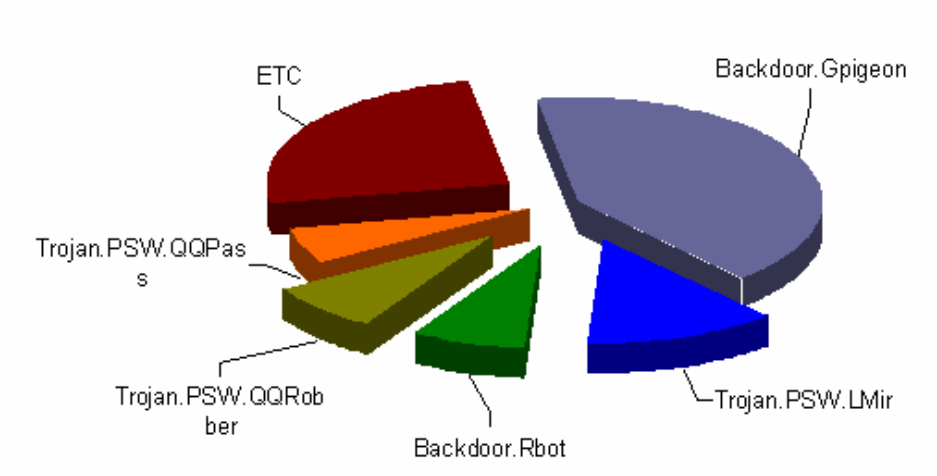
순위	1주	2주	3주	4주
1	-	Backdoor/SdBot.atp.Rootkit	TrojanDropper.Agent.vb	Backdoor/Huigezi.mv
2	-	TrojanDownloader.Agent.ry	Backdoor/SdBot.atp.Rootkit	TrojanDropper.Agent.vb

3	-	Win32/FunLove.4070	TrojanDownloader.Agent.ry	Backdoor/SdBot.atp.Rootkit
4	-	Win32/Parite.a	Win32/Parite.a	Trojan/Script.Seeker
5	-	Trojan/QQMsg.Zigui.b	Exploit.HHCtrl.Jiaozhu	Trojan/WebImport

[표4] 2005년 10월 강민(JiangMin) 주간 악성코드 순위

[표3]과 [표4]는 라이징과 강민의 주간 악성코드 순위 도표이다. 라이징의 주간 악성코드 순위는 악성코드 TOP 5에서 설명한 바와 같이 1위와 2위에는 그레이버드 트로이목마와 엘미르핵 트로이목마가 순위 변화 없이 3주 동안의 순위를 유지하고 있다. 그리고 QQ룹 트로이목마 역시 주간 순위에서도 지속적인 감염 신고가 증가하고 있는 것을 볼 수 있다. 그러나 이에 반해 악성 아이알씨봇 웜은 3주차에서 순위 밖으로 밀려나는 등 감염신고의 감소가 진행되고 있는 것으로 분석된다. 강민의 주간 악성코드 순위에서도 역시 아이알씨봇 웜은 서서히 감소하고 있는 것으로 분석되며 이와는 대조적으로 라이징의 통계와 유사하게 그레이버드 트로이목마는 4주차에서 1위를 차지하며 급격한 감염 신고 증가가 있었던 것으로 분석된다.

악성코드 분포

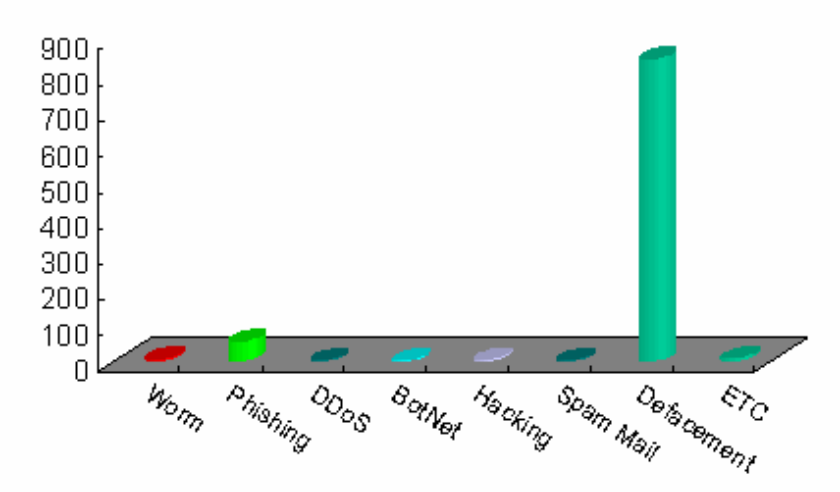


[그림1] 2005년 10월 중국의 악성코드 분포(출처:라이징)

이번 10월 악성코드 분포 역시 그레이버드 트로이목마와 엘미르핵 트로이목마의 증가를 첫 번째로 꼽을 수 있다. 그레이버드 트로이목마는 지난 9월 36%에서 41%로 5%가 증가하였으며 엘미르핵 트로이목마는 12%에서 13%로 1% 증가한 것으로 분석되었다. 그러나 악성 아이알씨 봇 웜은 9.7%에서 7.5%로 2.2%가 감소한 것으로 분석되어 11월 분포에서도 감소 현상은 지속될 것으로 예상된다. 기타에 포함되어 순위 권에 집계되지 못한 다양한 형태의

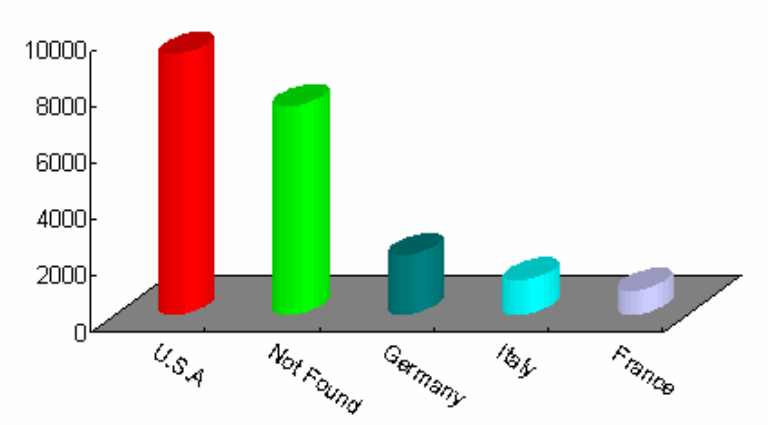
군소 트로이목마 류가 금년 들어 처음으로 악성코드 분포에서 감소하고 있는 것으로 분석되었다. 지난 9월 기타에 포함된 트로이목마 류들은 전체 27.7%에서 25.4%로 2.3%가 감소하였다. 이는 그레이버드 트로이목마와 엘미르핵 트로이목마의 증가와 함께 QQ 메신저를 이용한 트로이목마의 증가 추세로 인한 것으로 분석되고 있다. 그러나 11월에는 악성 아이알씨 봇 웜의 감소로 인해 기타에 포함된 트로이목마 류가 다시 증가할 것인지는 현재로서는 정확하게 파악하기 힘들다.

중국내 보안 사고 현황



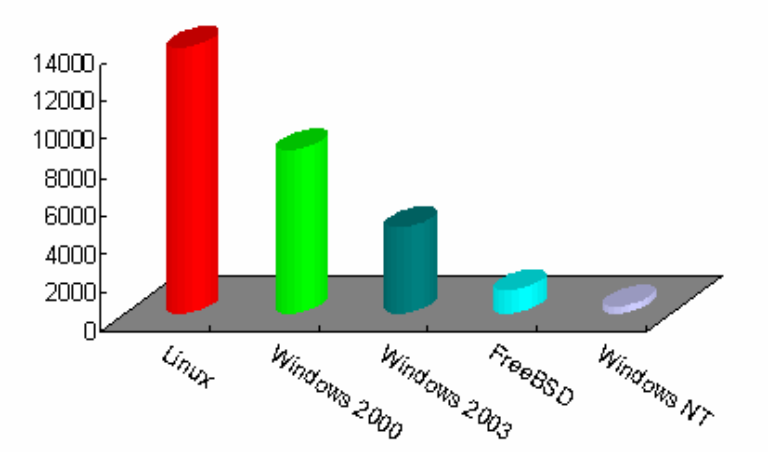
[그림2] 2005년 10월 중국의 보안사고 분포(출처: CNCERT/CC)

10월 중국 CNCERT/CC가 조사한 중국 내 보안사고는 [그림2]와 같이 홈페이지 변조사고가 가장 많은 수치를 기록하고 있다. 홈페이지 변조사고는 지난 9월 511건에서 845건으로 크게 증가한 반면 다른 보안사고들은 전반적으로 큰 변화 없이 현상 유지를 하고 있는 것으로 분석되었다.



[그림3] 2005년 10월 중국 내 해킹 원격지 국가(출처: CNCERT/CC)

[그림3]은 중국 CNCERT/CC가 집계한 중국으로 시도한 해킹의 원격지를 국가별로 분류한 것이다. 미국으로부터 시도된 해킹 시도는 지난 9월 7,955건에서 9,255건으로 약 1,300건 가량 증가한 것으로 분석하고 있으며 원격지의 국가를 탐지하지 못한 건도 7,424건으로 지난 달 5,204건에서 2,200건 가량 증가한 것으로 분석하고 있다. 그 외에는 독일, 이탈리아 그리고 프랑스 순으로 이어지고 있다.



[그림4] 2005년 10월 중국 내 해킹 대상 시스템(출처: CNCERT/CC)

[그림4]는 중국 CNCERT/CC에서 집계한 중국 내 해킹 대상이 된 시스템을 운영체제 별로 분류한 것이다. 리눅스 시스템이 가장 많은 해킹의 대상이 되고 있음을 알 수 있으나 지난 9월 14,874건에서 이번 달에는 13,932건으로 900건 가량 감소하였다. 반면 윈도우 2000은 리눅스 시스템보다 건수가 많지는 않지만 9월 5,263건에서 10월 8,588건으로 약 3,300건 가량 오히려 증가한 것으로 나타났다. 이는 최근 들어 윈도우 2000 운영체제에 대한 취약점 보고가 많아지며 이에 대한 공격코드의 공개로 인해 윈도우 운영체제에 대한 공격이 많아졌기 때문인 것으로 보인다.

(3) 세계의 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

2005년 10월도 영국의 소포스 통계[1]와 독일의 아비라 통계[2] 에 다르면 넷스카이 웜 변형이 부동의 1위를 차지하고 마이톱 웜(V3 진단명, Win32/Mytob.worm) 변형들이 순위에 올라와 있다. 아비라 통계에는 손상된 넷스카이 웜 변형이 2위에 올려져 있다. 보통 손상된 악성코드는 실행되지 않아 진단에서 제외되지만 대량의 메일로 전파되는 웜의 경우 메일과 손상된 파일 자체가 스팸으로 간주되어 진단에 추가하는 경우가 있다. 아비라는 독일에서 제작된 것으로 추정되는 소버 웜 변형에 대해서도 잠깐 언급되었는데 소버 웜 변형의 경우 메일 제목이 영어와 독일어로 작성되어 있으며 한글 윈도우 등 특정 국가 윈도우에서 오동작하므로 아시아 지역까지 확산되지는 못했다.

러시아의 캐스퍼스키랩의 통계[3]는 서유럽 회사들과 달리 마이톱 웜 변형이 1위를 차지하고 있으며 마이둠 웜을 수정한 것으로 보이는 Email-Worm.Win32.Doombot 변형 2개가 높은 순위로 새롭게 진입했다. 이외 한국에서도 감염 보고된 중국판 마이톱 웜 변형인 팬봇[4]도 순위에 올라와 있다.

중국 해커들에 의한 온라인 게임의 사용자 계정과 비밀번호 유출 시도가 인근 국가로 계속 확대되고 있다. 중국에서 서비스 중인 온라인 게임의 비밀번호를 외부로 유출하는 프로그램이 최근에는 한국, 일본 및 대만의 게임들로 확대되고 있다. 이는 사이버머니나 게임 아이템들이 현금 거래가 가능함으로 인해 나타나는 부작용으로 보고 있다.

대부분의 안티 바이러스 업체들의 동향에서 넷스카이 웜과 마이톱 웜처럼 메일로 전파되는 웜이 상위에 존재하며 이들 악성코드 중 상당수는 악성 아이알씨봇 기능이 있거나 마이둠 웜, 마이톱 웜과 같이 공개된 소스를 바탕으로 새로운 기능이 추가된 변형이다. 향후에도 이들 변형은 계속 등장할 것으로 보인다. 이외 휴대용 게임기인 PSP와 닌텐도 DS(Nintendo DS)용 악성코드가 발견되어 휴대용 게임기도 악성코드의 공격을 받을 수 있음이 증명되었다. 다만, 현재 등장한 악성코드는 불법복제를 통해서만 감염되므로 정품 사용자는 감염될 가능성이 낮다.

[1] http://www.sophos.com/pressoffice/news/articles/2005/11/pr_uk_toptenoct05.html
[2] http://www.avira.com/en/news/october_virus_top_10.html
[3] http://www.viruslist.com/en/analysis?pubid=173190935
[4] http://info.ahnlab.com/smart2u/virus_detail_2806.html

V. 이달의 ASEC 컬럼

(1) 인터넷을 이용한 신종 사기 프로그램

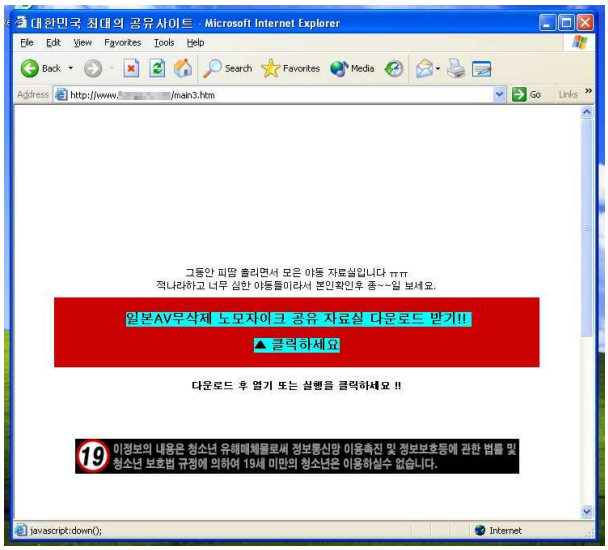
작성자: 김정석 주임연구원(js_kim@ahnlab.com)

피싱이나 홈페이지 변조를 통한 트로이목마, 백도어 등의 설치와 개인정보 유출 등의 범죄 행위는 널리 알려져 있으며 사회문제가 되기도 했다. 악성코드와 해킹을 이용한 범죄 행위 이외에도 최근에는 인터넷 사용자들의 심리를 이용하는 사기 행위가 늘고 있다. 이에 이번 컬럼에서는 인터넷에서 거래되는 재화나 용역을 그 대상으로 하지 않고, 윈도우용 응용프로그램을 일종의 사기에 이용하는 사례를 살펴보자.

음란 동영상 공유 프로그램

2005년 10월 경남 지방경찰청의 사기 인터넷 성인 사이트에 대한 적발 보도가 있었다. 이 사건은 인터넷 성인물 서비스 제공자가 선전하는 것과는 달리 영상물 등급 위원회의 심의를 받은 평범한 컨텐츠를 제공하였으며, 약 백만 명의 사용자가 허위광고에 넘어가 일정액의 회원가입비를 지불하였으며 전체적인 피해액은 약 400억이나 되었다. 이 사건은 성인 사이트 이용자 개개인으로 볼 때 손해를 입은 금액이 비교적 적은 금액이고, 인터넷 성인 사이트 이용자들이 신고를 꺼려한다는 점을 이용한 사기로 볼 수 있다.

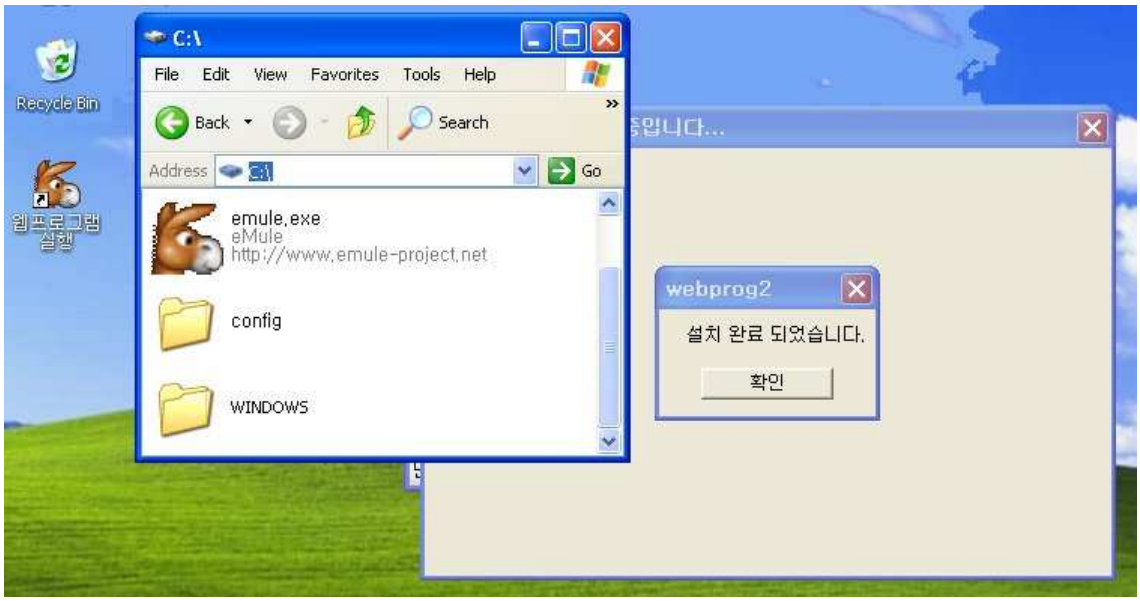
또한 10월에는 합법적으로 운영되는 성인사이트로 위장하여 가짜 성인 동영상 검색 프로그램을 이용해 이용료 결제를 요구하는 프로그램도 발견되었다. 이 웹사이트는 인터넷 검색사이트의 '공유' 키워드를 이용한 검색결과, 제휴 사이트의 팝업 광고를 통한 웹 페이지 노출 등의 방법으로 [그림1]과 같이 사용자의 방문과 일명 '웹프로그램'의 설치를 유도한다.



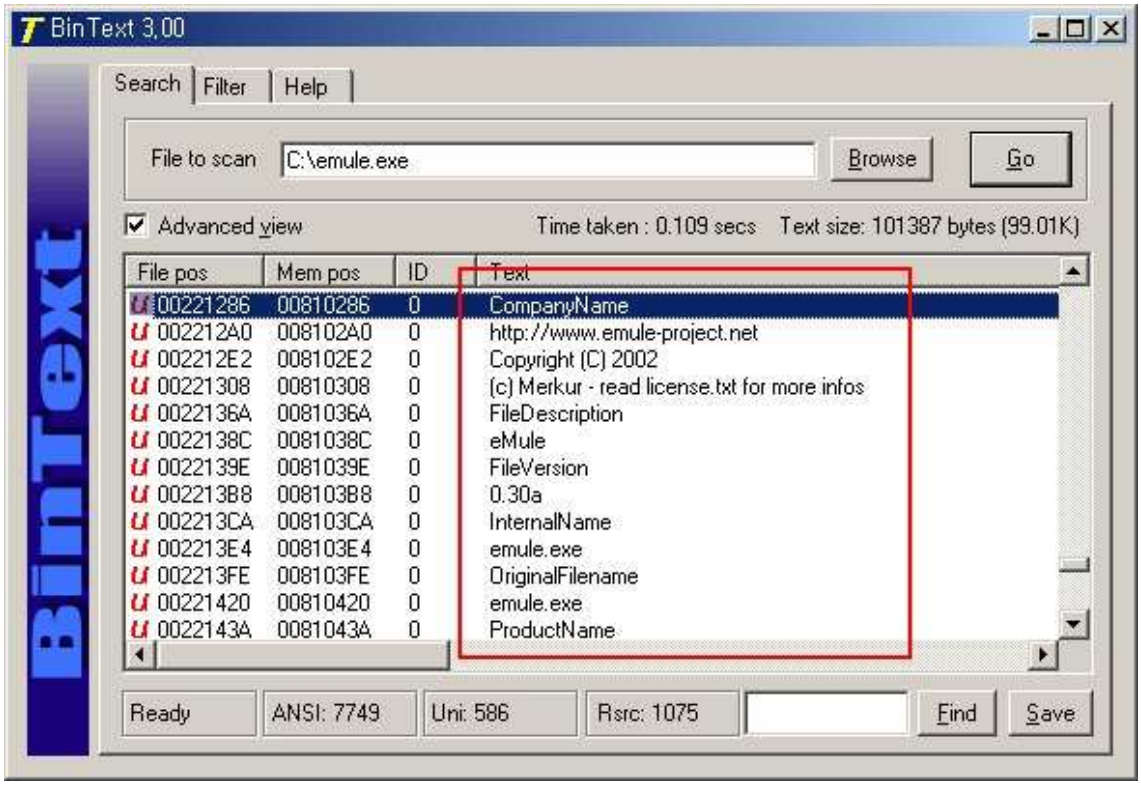
[그림1] 제휴 사이트 팝업 또는 인터넷 검색사이트를 통한 웹 페이지 방문

이 웹 페이지에서 다운로드할 수 있는 '웹프로그램'은 RAR 자동 압축 추출기(RAR Self

Extractor)로 제작되어 더블클릭으로 간단히 설치할 수 있다. 설치되는 '웹프로그램'은 [그림 2]에서 보는 것과 같이 P2P 파일 공유 프로그램으로 널리 알려져 있는 이뮬(eMule)과 동일하다. 이 프로그램은 실제로 소스코드가 공개된 이뮬을 변형하여 제작된 것으며, 이는 [그림 3]과 같이 파일의 등록정보와 내부 문자열 추출 만으로도 사실을 확인할 수 있다.

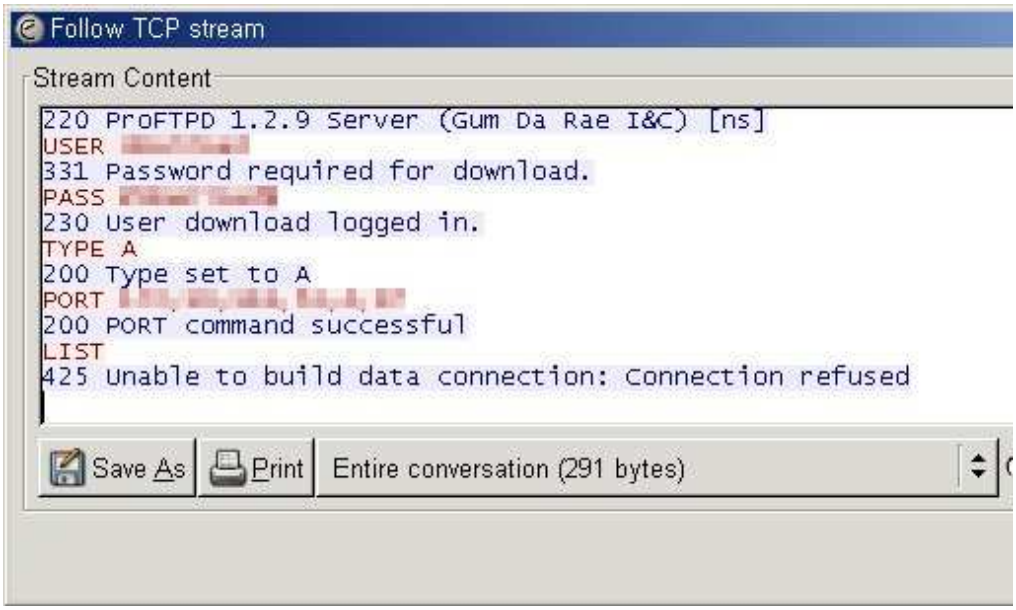


[그림2] 이뮬(eMule)을 변형하여 제작된 '웹프로그램'



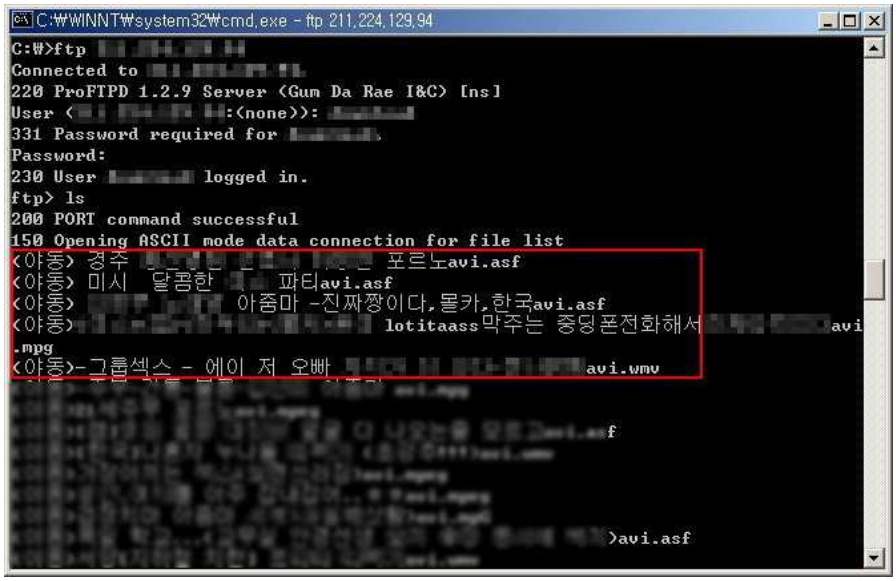
[그림3] 내부 문자열 확인

이 프로그램을 실행하면 프로그램의 시작과 함께 동영상 검색이 시작된다. 동영상 파일검색은 이뮬의 P2P 파일공유 검색기능과는 무관한, 미리 지정된 FTP 서버에 접속하여 업로드된 파일의 목록을 보여주게 된다. FTP 서버에 업로드 된 파일만을 다운로드 대상으로 제한하기 때문에 어떠한 검색어를 사용해도 동일한 검색 결과만 나타나게 된다. [그림4]는 FTP 서버로의 접속과정을 TCP 패킷 캡쳐 프로그램을 이용하여 분석한 결과이다. FTP서버 접속과정에서 모자이크로 처리된 유저아이디와 암호를 확인할 수 있다.

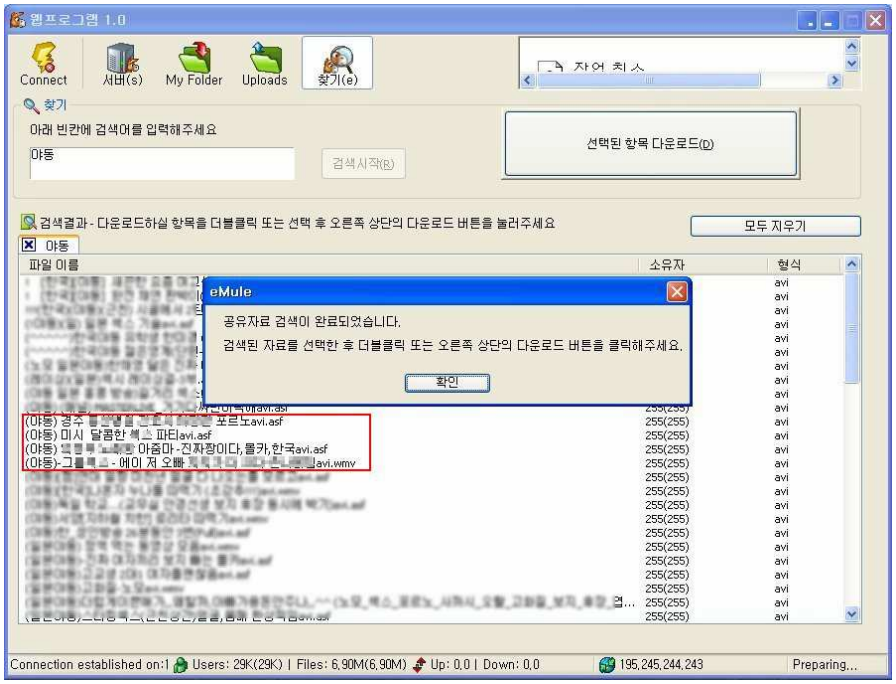


[그림4] '웹프로그램'이 미리 지정된 FTP 서버에 로그인 하고 파일의 리스트를 얻어온다.

[그림5]와 [그림6]에서 이 프로그램을 이용하여 검색된 동영상 리스트와 수동으로 FTP서버에 접속하여 얻어오는 파일의 리스트가 동일한 것을 확인할 수 있다.

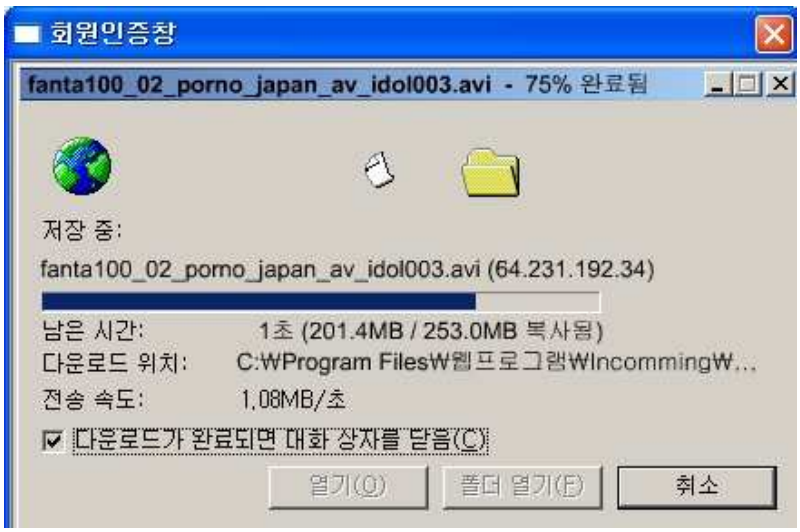


[그림5] 수동으로 접속하여 확인한 FTP서버의 파일리스트



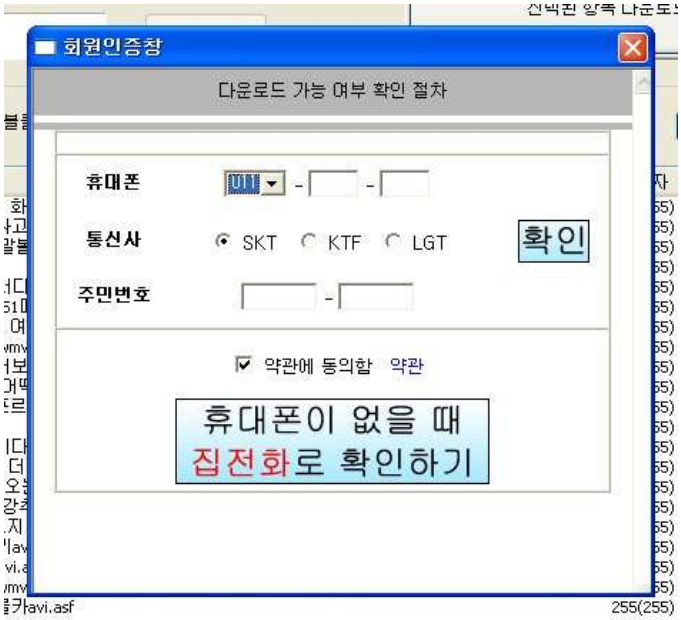
[그림6] '웹프로그램'을 이용하여 얻은 동영상 검색결과

'웹프로그램'의 동영상 검색 후 다운로드를 시도하면 다음 그림과 같이 플래시 애니메이션으로 제작된 허위 다운로드 진행 표시기를 노출한다.



[그림7] 플래시 애니메이션으로 제작된 허위 다운로드 진행 표시기

파일을 다운로드 하기 위해서는 회원가입이 필요하며, 이 때 '쿠폰', '이벤트 당첨' 등의 사용자를 현혹하는 문구가 포함된 메시지를 출력한다. 회원가입의 마지막 과정에서 휴대전화 소액결제를 요구하고, 가입비가 결제되지만 계약사항에 대한 설명은 어디에도 존재하지 않는다.



[그림8] 휴대전화 소액결제 요구

회원 가입 후 '웹프로그램'에서 검색된 동영상에 대한 다운로드가 가능하지만, 다운로드는 네트워크나 FTP 서버의 상태에 따라 수분에서 수 십분의 시간이 소요된다. 다운로드 과정에서 '웹프로그램'은 동작이 중지된 것처럼 보이며, 다운로드 하는 파일들은 국내에서 허용되지 않는 음란 동영상 일색이다.

[그림9] 음란동영상

'웹프로그램' 사용 중에 원하지 않는 팝업 광고가 노출되는 것을 확인할 수 있는데 팝업 광고의 내용 또한 성인 동영상 검색이 가능한 '파일공유' 프로그램에 대한 내용이다. 규모나 형태를 미루어 짐작할 때 여러 연계 사이트가 존재하는 것으로 예상된다. 실제로 인터넷 검색 사이트를 이용한 검색과정에서 찾을 수 있는 또 하나의 프로그램은 위에 설명한 '웹프로그램'의 구(舊)버전으로 짐작되는 '공유프로그램'을 발견할 수 있었다.
'공유프로그램'은 '웹프로그램'보다 사용자 인터페이스의 질이 떨어지며 '웹프로그램'이 다운로드 진행 표시기를 플래시 애니메이션을 이용하는 대신 공유프로그램은 윈도우 애니메이션 컨트롤을 이용하여 표시한다. 나머지 회원가입요구, FTP서버를 이용한 동영상 검색 결과 노출과 다운로드 과정은 모두 동일하다.

배포 웹사이트	프로그램이름	비고
0**a.com	공유프로그램	'웹프로그램'의 구(舊)버전으로 짐작. 조잡한 사용자 인터페이스.
Kong***.com	웹프로그램	'웹프로그램' 보다 향상된 사용자 인터페이스 제공. Kong***.com 의 메인(index)페이지에서는 '웹프로그램'이 아닌 정상 이뮬 프로그램의 다운로드 제공.

[표1] 다른 웹사이트에서 배포하는 유사 프로그램의 비교

각 프로그램의 배포 사이트 Whois 검색 결과 동일 인물이 소유한 웹 사이트로, 이 프로그램들이 동일한 제작사가 서비스하는 프로그램으로 판단된다. 또 한가지 재미있는 것은 같은 회사에서 제작한 동일한 프로그램인 것으로 추정되는 이 두 프로그램이 서로 호환되지 않아 각 프로그램 별로 별도의 회원가입과 결제를 해야 한다는 것이다. 제작사는 현재 두 개의 프로그램이 별개의 프로그램이라는 주장을 하고 있다.

결과적으로 이 프로그램은 국내에서 허용되지 않는 음란 동영상을 배포하고, 기능에 제한적인 프로그램으로 사용자를 속여 결제를 유도하는 사기 프로그램인 것이다.

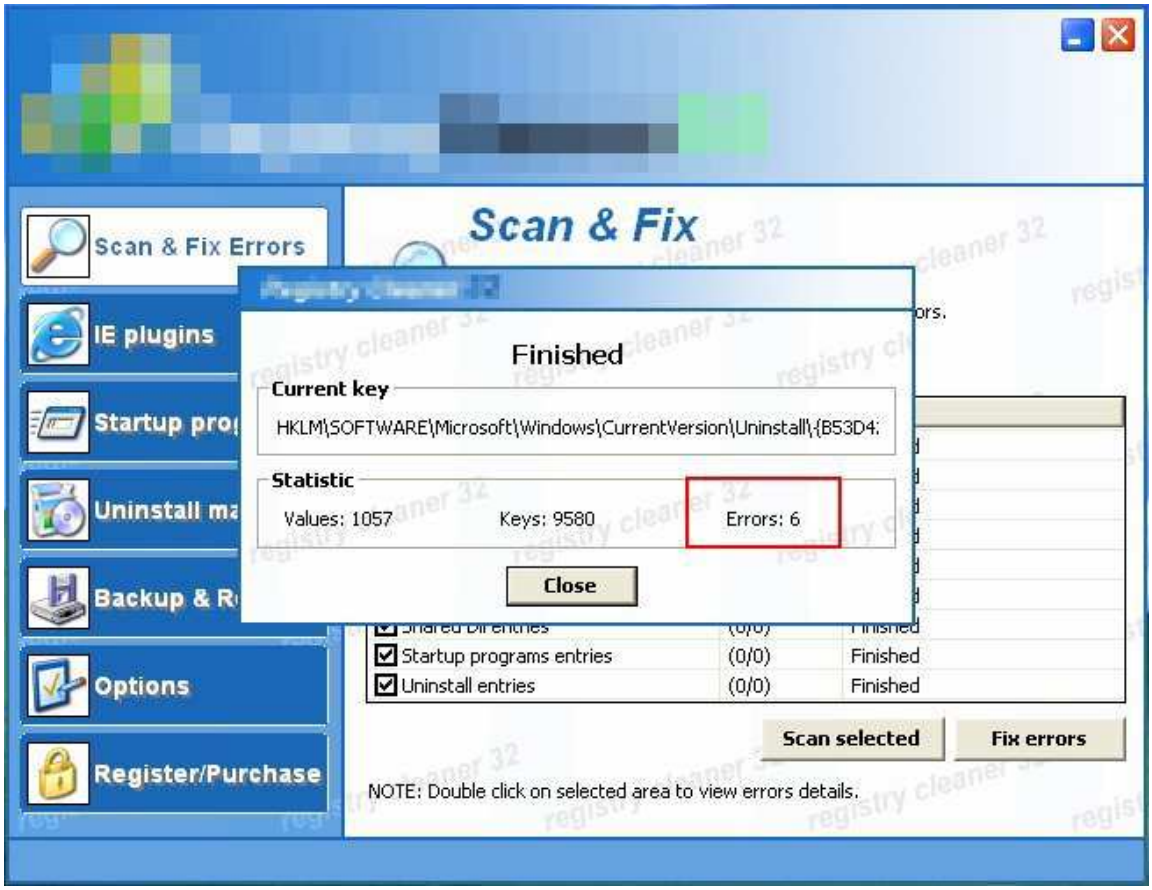
다단계 판매 방식을 이용하는 프로그램의 배포

스파이웨어나 애드웨어 같은 유해가능 프로그램에 대한 위협이 증가하면서 사용자의 불안심리를 이용한 사기 프로그램의 등장과 피해도 더 이상 어제 오늘의 이야기는 아니다. 일부 안티 스파이웨어 프로그램 제작사 또는 보안관련 사이트에서 이런 종류의 가짜 안티 스파이웨어 프로그램을 Rogue 또는 Suspected 프로그램[1]으로 분류하여 리스트를 공개하기도 하였다.

최근에는 이러한 Rogue / Suspected 프로그램에 다단계 판매 방식을 결합한 프로그램이 발견되었다. 문제의 프로그램은 레지스트리 오류 검사 프로그램으로 이하 '레지스트리유틸리티'라 지칭한다. 레지스트리유틸리티가 검출하는 레지스트리 오류에는 시작프로그램, 언인스톨 정보 등의 일반적이고 심각하지 않은 오류도 포함한다.

다음 그림은 OS만 설치한 깨끗한 시스템(Clean System)에서의 레지스트리유틸리티의 레지스트리 오류 검사 결과이다. 방금 OS를 설치한 정상 시스템에서도 6개의 오류를 검출한 것을 확인할 수 있다.

[1] "Rogue/Suspect" 안티 스파이웨어 프로그램이란 기능이 의심스럽고 사기성이 짙은 프로그램이다. 허위 검사결과 또는 과장된 검사결과를 보여주는 것이 보통이며, 발견된 스파이웨어 제거 시 이용료를 요구한다.(참고: http://www.spywarewarrior.com/rogue_anti-spyware.htm)



[그림10] OS만 설치된 깨끗한 시스템에서의 레지스트리 오류 검출

발견된 레지스트리 오류를 복구하기 위해서는 다른 Rogue / Suspected 프로그램과 마찬가지로 이용료를 지불해야 한다.

문제는 대부분의 시스템에서 레지스트리 오류가 발견된다는 사실을 이용하여 다단계 방식으로 회원 모집을 하고 있으며, 프로그램 판매 방식을 취하고 있는 것이다. [그림11]은 제작사 홈페이지의 회원가입 안내문이다. 95% 이상의 시스템에서 레지스트리 오류가 발견되고 있으며, 회원 프로그램에 동참하는 경우 손 쉽게 돈을 벌 수 있다는 점을 안내하고 있다.

[그림11] 레지스트리유틸리티 제작사의 회원 가입 안내

레지스트리유틸리티의 회원 프로그램에 동참하게 되면 별도의 계정과 하이퍼링크를 제공한다. 회원들은 이 하이퍼링크를 인터넷 게시판 또는 스팸 메일 등을 통하여 홍보하게 되며, 사용자가 이 하이퍼링크를 통하여 프로그램을 사용하고 이용료를 결제하는 경우에 수익금의 일부를 받게 된다. [그림12]는 인터넷 검색 사이트에서 검색한 레지스트리유틸리티 관련 링크이다.

[그림12] 인터넷 검색 사이트에서 검색한 레지스트리유틸리티 관련 링크

위 두 가지 프로그램의 사례를 종합하여 볼 때 인터넷을 이용한 사기 프로그램들은 대부분 스팸 메일이나 인터넷게시판 등을 이용하여 현혹되기 쉬운 문구로 허위 과장 광고를 하고, 웹 사이트를 방문하는 사용자에게 프로그램 설치와 사용료를 요구한다. 이러한 허위 과장 광고는 실제 프로그램과는 관련이 없으며 사용자의 심리를 자극하는 문구를 사용하는 것이 보통이다. 실제 스파이웨어 등의 유해 가능 프로그램에 대한 피해를 경험한 사용자는 허위 검사 결과에 대한 불안 심리가 작용하여 이용료를 결제하고 사용하는 경우도 많은 것으로 추정된다.

사용자는 무분별한 팝업광고, 스팸 메일 등으로 과장광고를 하는 프로그램에 대해 경계할 필요가 있으며, 되도록이면 신뢰하는 제작사가 제공하는 프로그램만 이용하는 것이 좋다.

(2) XSS를 이용한 웜의 출현, 또 다른 위협의 예고

작성자: 정관진 주임연구원(intexp@ahnlab.com)

최근 국내의 유명 웹 사이트에서 잇따라 악성코드가 발견되는 사례가 보고되었다. 과거의 악성코드는 사용자의 직접적인 행동을 필요로 했는데, 이제는 웹 사이트를 방문하는 것 자체만으로도 악성코드에 감염되어 개인 정보가 외부에 유출될 수 있는 환경에 놓여있는 것이다. 이것은 이전의 수동적인 측면에서 네트워크 환경자체가 변화하며 악성코드 자체도 새로운 변화의 트랜드를 겪고 있기 때문이다. 개인과 기업 모두 이러한 변화에 따라 안티 바이러스(Anti-Virus) 프로그램 또는 방화벽 프로그램의 사용 그리고 기업체에서는 중앙에서 네트워크를 통제하는 형태로 점점 보안성이 증대되고 있다. 이러한 이유로 악성코드는 여러 가지 제약에 부딪치면서 자기 스스로를 전파하기 위한 다양한 방법들이 모색되었고 최근 해킹 기법으로도 많이 이용되고 있는 웹 애플리케이션(Web Application)의 활용이 관찰되고 있다. 이런 공격방법 중 대표적인 것은 XSS와 SQL 인젝션(Injection) 기법을 이용하는 것이다. 이번 컬럼에서는 XSS를 이용한 자가복제 개념의 웜 출현과 이에 따른 향후 전망을 예측해 보고자 한다.

XSS란 무엇인가?

XSS는 Cross Site Scripting의 약자이다. 고정된 HTML을 자유롭게 쓰게 해주는 CSS(Cascading Style Sheets)와 혼동되어 사용될 수 있기 때문에 'XSS' 라고 많이 불리고 있다. XSS는 웹 애플리케이션에서 입력되는 데이터를 적절하게 검사하지 않아 클라이언트의 스크립트나 HTML 태그의 사용이 가능하게 되는데, 이것은 의도적으로 악의적인 형태의 공격으로까지 이어질 수 있다. XSS에 노출되어 있는 것을 확인하는 것은 [그림1]과 같이 HTML의 입력 폼 또는 URL 상에 스크립트를 입력하여 간단히 테스트 해 볼 수 있다. 최근에는 이렇게 스크립트를 직접적으로 사용하지 못하도록 프로그램에서 필터링을 하고 있지만, 16진수로 표현하거나 특수 문자열 등을 사용하여 침입탐지시스템(IDS:Intrusion Detection System) 등에서 탐지하지 못하도록 우회하는 방법들도 사용되고 있다.

입력 폼에 <script>alert("hello")</script> , <script>alert(document.cookie)</script> 사용 또는
http://www.domain.com/user.php?op=userinfo&uname=<script>alert(document.cookie);</script> 와 같이 URL 직접 입력

[그림1] XSS에 노출된 것을 확인하는 스크립트

XSS 의 보안적 위협증대

XSS는 많은 웹 애플리케이션에 그 문제가 존재하고 있으며, 버퍼 오버플로우(Buffer Overflow)와 같이 직접적으로 시스템의 권한을 획득하는 것은 아니지만 간접적 또는 다양한 형태로 악용될 우려가 높다. 공격자는 HTML, JavaScript, VBScript, ActiveX 또는 Flash를

이용하여 취약한 웹 애플리케이션을 통한 사용자 정보의 수집, 사용자 계정의 탈취, 정보의 변경, 쿠키 정보 획득/변조, 부정확한 정보제공 등 악용 가능한 범위가 넓다. 이것은 Cross Site Scripting 이라는 이름에서도 알 수 있듯이 다양한 플랫폼에 걸쳐 사용이 가능하기 때문이다. 악성코드의 관점에서 보면 운영체제와 응용 프로그램 등 실행상에 여러 제약들이 있지만 XSS는 이런 제약범위가 더욱 좁아져 환경적 영향을 덜 받게 된다.

또한, XSS는 금융사기 기법으로 많이 소개되고 있는 피싱(Phishing)에서도 사용되고 있으며, 홈페이지에 특정 태그를 삽입하는 악성코드 설치 사례 그리고 최근에 XSS를 이용한 웜으로까지 확장되어 이에 대한 보안적 위협이 증대될 가능성이 높다.

MySpace 사이트의 사례를 통해 본 XSS 웜

앞서 언급한 XSS의 위협을 실질적으로 보여주었던 사례가 올 10월 4일 보고되었는데 이것은 XSS를 이용한 첫 웜-새미(Samy)라는 이름으로 불린다-의 사례로 기록되고 있다. 사건의 개요는 이렇다. MySpace 사이트의 한 사용자가 많은 친구들을 만들기 위한 방법을 생각하다 XSS를 이용한 스크립트를 만들게 되었고, 이 스크립트는 백만명이 넘는 사람들이 본인의 의지와는 상관없이 친구 추가 등록 요청을 제작자에게 하게 된 것이다. 이로 인하여 해당 사이트는 일시적인 서비스 장애를 겪게 되어 XSS 웜을 통해 서비스거부공격(DoS:Denial of Service) 가능성을 보여주었다.

MySpace 사이트는 기본적으로 스크립트의 사용을 허용하고 있지 않았지만, 제작자는 CSS(Cascading Style Sheet)태그 안에서 자바스크립트 사용이 가능함을 확인하고 스크립트를 사용자 프로파일(User's Profile) 안에 삽입해 놓았던 것이다. 즉, 이것은 누군가 프로파일 페이지에 접속하게 되면 자동적으로 친구 등록 요청을 하게 된다. 예를 들어, 만약 5명의 사람들이 처음 제작자의 사용자 프로파일 페이지를 방문하게 되면 자동적으로 해당 스크립트가 방문한 사람들의 프로파일에도 추가되고 그 페이지를 또 다른 5명의 사람들이 방문하면 결국 25 명의 친구가 생기는 것과 같은 원리이다. 다단계와 같은 개념의 이 수치는 몇 시간 안에 급격하게 증가하게 되었고 제작자도 전혀 예상하지 못한 [표1]과 같은 현상이 발생하였다.

일시	친구 수	친구등록 요청자	경과시간	비고
10월04일 12:34 PM	73	0		
10월04일 01:30 AM	73	1	1시간	
10월04일 08:35 AM	74	221	8시간	
10월04일 09:30 AM	74	480	9시간	
10월04일 10:30 AM	518	561	10시간	
10월04일 01:30 PM	2503	6,373	13시간	

10월04일 06:20 PM	2503	17,084	18시간	3초 후 918,268 이후 다시 3초 후 919,664. 몇분 후 1,005,831 명까지 도달

[표1] 새미 웜의 시간대별 친구등록 추가 현황

[그림2] 실제 그 당시의 화면 일부 (친구요청자가 919,664명에 이른다)

제작자는 의도하지 않았지만 24시간 이내라는 짧은 시간에 백만명의 사람들이 친구 요청을 하게 되었고 일약 유명세를 타게 되었다. 이미 해당 사이트는 문제를 제거하여 더 이상 스크립트가 동작하지 않지만 이 사건은 XSS를 이용한 악성코드 전파 가능성을 보여주었기 때문에 많은 언론에서도 언급되었다.

XSS의 위험성 인지되어야 ...

지속적인 인터넷의 보급과 확산은 '보안' 이라는 것이 얼마나 더욱 중요해 져야 하는지 말해주고 있다. 인터넷의 기술발전에 따라 악성코드 또한 기술적 변화가 나타나고 있고 공격의 방법이 변화하고 있다. Cross Site Scripting은 현재의 트랜드를 반영하며 증가하고 있는 것으로 만약 지금과 같이 웹이 대중화 되지 않았다면 나타나지 않았거나 크게 사용되지 않았을 것이다.

이런 위험성에 XSS를 방지하기 위하여 클라이언트 측면에서는 브라우저에서 Java-Script의 사용을 중지할 수 있지만, 현실적으로 이것은 대안이 되지 못한다. 그렇다면 서비스를 제공하는 측면인 즉, 애플리케이션에서 입력되는 데이터에 대해서 충분한 검증 절차가 필요하게 된다. 따라서, 아직까지 현존하는 많은 웹 응용프로그램들이 이러한 XSS에 노출되어 있는 만큼 위험성을 인지하고 개발 당시에 보안성 검토가 이뤄지는 등의 노력이 필요할 것이다. 분명한 것은 웹이 대중화 되어 있는 만큼 웹 애플리케이션을 통한 보안 문제는 앞으로도 계속 증가될 것이 자명하다는 것이다.