ASEC Report 11월

® ASEC Report

2005. 12

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

악성코드 피해신고와 신종(변형)발견 소폭 증가 …

11월은 지난달에 비해 악성코드 피해거수와 신종(변형) 악성코드 발견건수가 소폭 증가하였다. 악성코드 피해 Top 10을 살펴보면 11월에 발견된 소버 웜 변형, 베이글 웜 변형, 마이톱 원 변형이 발견과 동시에 10위권 내에 진입함으로써, 그 피해가 많았음을 보여주고 있다. 이렇듯 매스메일러 웜의 출현이 잦아지면서 악성코드 피해 Top 10에 랭크된 악성코드 중 70%는 메일을 통해 전파되는 것이 차지하고 있어, 취약점을 이용해 전파되는 악성코드보다 메일을 이용해 전파되는 악성코드에 의한 피해가 많았음을 보여준다. 11월에 발견된 신종(변형) 악성코드도 지난달과 마찬가지로 트로이목마가 강세를 보였다. 그 중 그레이버드 변형과 후피곤 변형이 눈에 띄게 증가하였다. 세계적으로는 소버 웜 변형으로 인한 피해가 많았는데, 이 웜은 안철수연구소의 11월 악성코드 피해 Top 10에서도 3위를 차지하고 있어 한국 뿐 아니라 여러 나라에서 피해가 많았던 것으로 보인다. 특히 이 웜은 기존까지는 한국어를 비롯한 특정 OS 에서는 동작하지 않아 아시아 지역에서는 확산도가 낮았으나, 11월에 발견된 변형은 한국, 일본 등 아시아 지역에서도 많은 피해 보고가 있었다. 그러나 중국은 다른 아시아 지역과는 달리 소버 웜 변형에 대한 피해는 적었고, 오히려 트로이목마에 의한 피해가 많았던 것으로 보고되었다. 11월에 발견된 스파이웨어는 10월보다 적은 수가 발견되었다. 그러나 연말이 다가오면서 금적전 이득을 보기 위해 다량으로 스파이웨어가 배포되는 현상을 보이고 있어 주의가 필요하다. 11월에는 이렇다 할 보안사고가 보고되지 않았다. 또한 MS사에서 매달 발표하는 보안패치도 1건만 발표되었다. 하지만 이를 이용한 악성코드도 이미 발견된 만큼 주의가 필요하겠다. 이번 ASEC 컬럼에서는 국제적인 보안 컨퍼런스 중 하나인 AVAR 2005 컨퍼런스에서 발표된 주제들과 이모저모에 대해 살펴 보았다.

I. 11월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자: 이재호 연구원(explod@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	163	12.1%
2	-	Win32/Maslan.C	103	7.7%
3	new	Win32/Sober.worm.55390	94	7.0%
4	new	Win32/Mytob.worm.41824	40	3.0%
5	↑2	Win32/Parite	33	2.5%
6	-	Win32/Mytob.worm.48766.C	23	1.7%
7	↓2	Win32/Tenga.3666	22	1.6%
8	new	Win32/Bagle.worm.AM	20	1.5%
9	↓6	Win32/Sasser.worm.15872	19	1.4%
10	new	Win32/Mytob.worm.51062	19	1.4%
		기타	807	60.1%
합계			1,343	

[표1] 2005년 11월 악성코드 피해 Top 10

11월 악성코드 피해 동향

11월 악성코드 피해건수는 10월에 비해 소폭 증가한 1,343건이다.

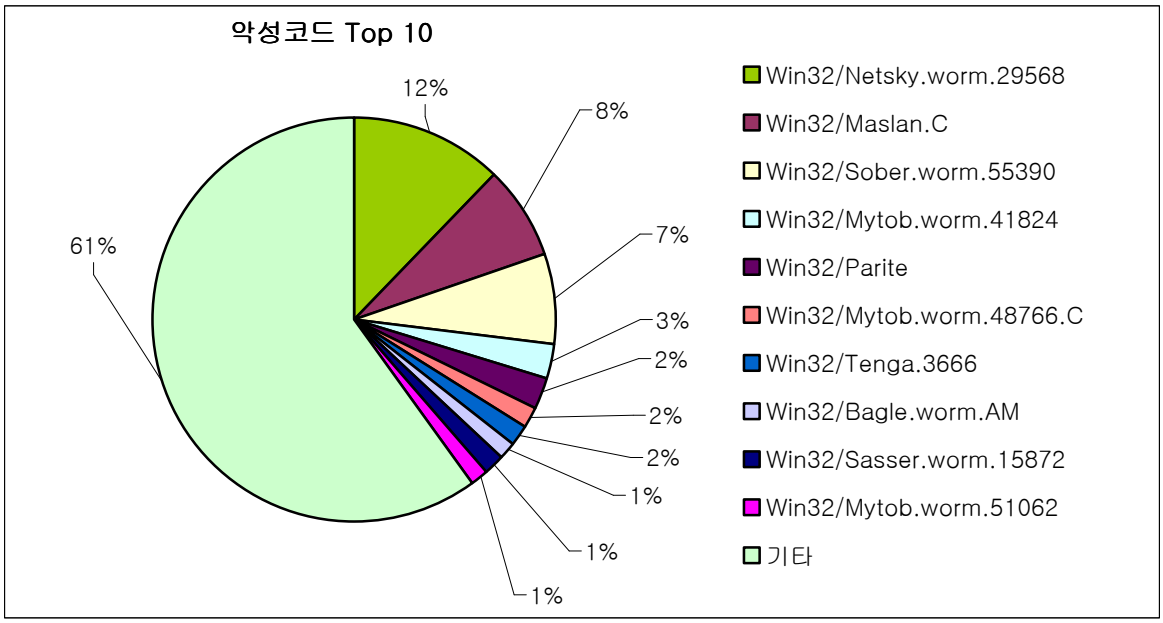
지난 7월부터 11월까지 넷스카이.29568 웜(Win32/Netsky.worm.29568)과 마슬란.C (Win32/Maslan.C)가 여전히 악성코드 피해 Top10의 1, 2위를 차지하고 있다. 그 외 11월에 발견된 소버, 베이글, 마이톱 웜 변형이 10위권 내에 새로이 진입하였다.

11월에 발견된 소버.55390 웜(Win32/Sober.worm.55390)은 발견됨과 동시에 많은 피해를 입혀 11월 악성코드 피해순위 3위를 차지하였다. 이 웜은 실행되면 에러메시지를 띄워 정상적으로 실행되지 못한 것처럼 위장하지만 실제로는 정상 실행되고, 감염된 시스템에서 메일 주소를 수집하여 일정시간이 지나면 웜이 첨부된 메일을 발송한다. 또한 MS사의 악성코드 제거 유틸리티를 종료시킨 후 “No Viruses, Trojans or Spyware found!”라는 메시지를 출력하여 마치 유틸리티가 정상적으로 종료된 것처럼 위장한다. 이로 인해 감염사실을 사용자들이 미처 인지하지 못하여, 다른 웜들에 비해 단시간에 빠르게 전파될 수 있었던 것으로 보인다.

11월 피해동향 중 또 하나는 특정 사이트 방문 시 다른 특정 URL 에서 악성코드를 다운로드하여 실행되는 형태로 인한 피해가 많았다는 것이다. 이 특정 사이트는 해킹 등을 통해 해

당 악성코드를 다운로드하여 실행하는 스크립트가 인젝션(injection)된 것으로 보인다.

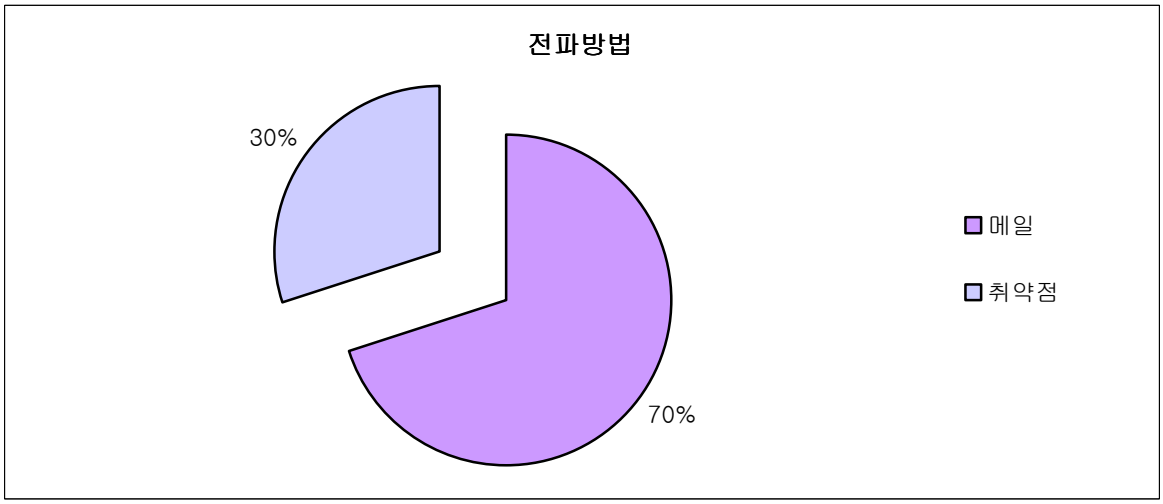
11월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.



[그림1] 2005년 11월 악성코드 피해 Top 10

11월 악성코드 Top 10 전파방법별 현황

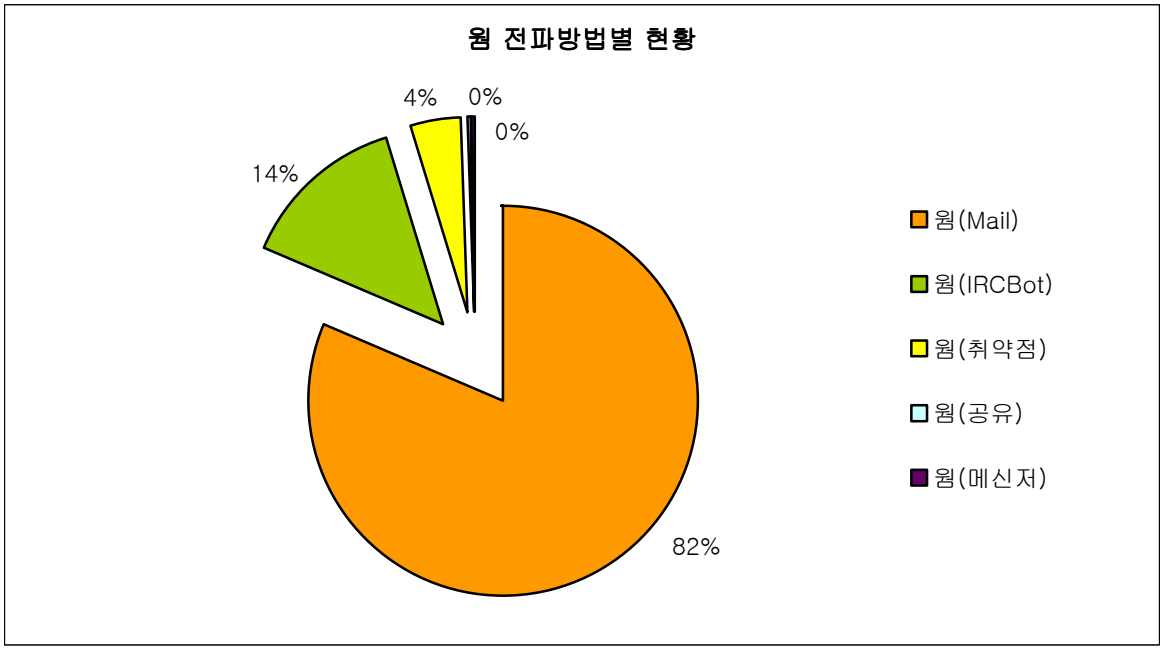
[표1]의 Top 10 악성코드들은 주로 어떠한 감염 경로를 가지고 있는지 [그림2]에서 확인할 수 있다.



[그림2] 2005년 11월 악성코드 Top 10의 전파 방법별 현황

매스메일러인 마이톱 웜은 감소 추세를 보이고 있으나, 또 다른 매스메일러인 소버 웜과 베이글 웜 변형이 새로이 출현하면서 지난달과 마찬가지로 Top 10에 랭크 된 악성코드의

70%가 메일을 이용하여 전파되고 있는 것으로 나타났으며, 나머지 30%의 악성코드는 취약점을 이용해 전파되는 것은 나타났다.



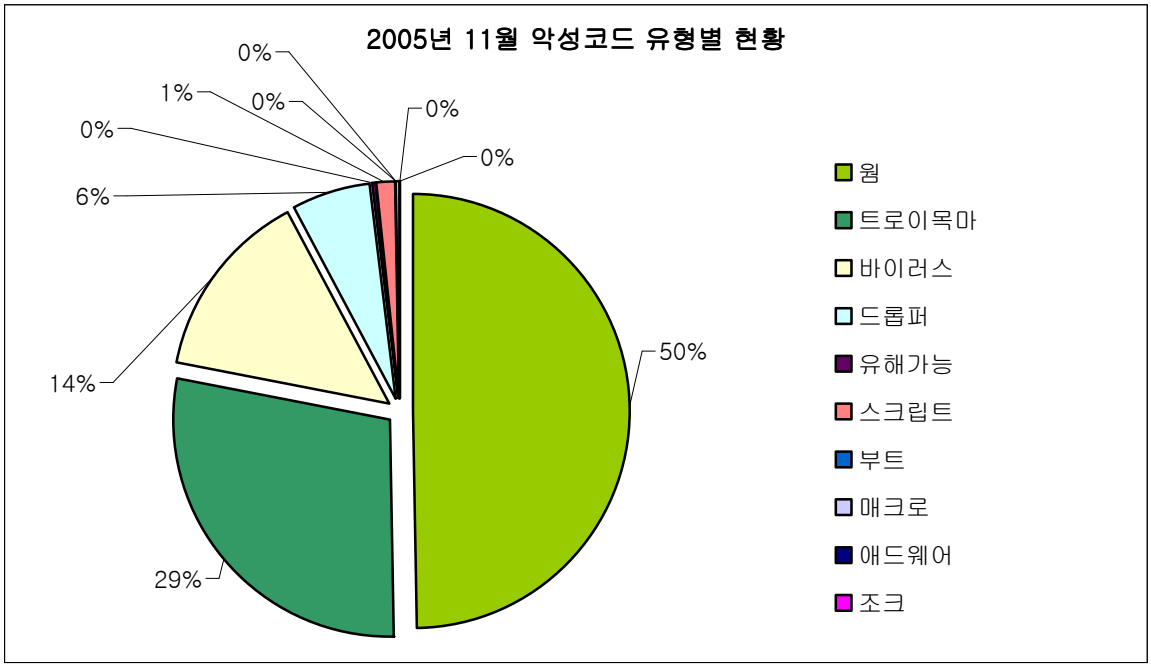
[그림3] 2005년 11월 웜의 전파방법별 현황

[그림3]은 11월에 피해 신고된 웜의 전파방법에 대한 현황이다. 이메일을 통해 전파되는 웜은 7월 기준으로 매달 10%씩 증가하여 42%에서 82%까지 증가한반면, 악성 아이알씨봇(IRCBot) 웜은 꾸준히 감소되어 52%에서 14%까지 감소하였다. 올 하반기 들어 이메일로 전파되는 베이글 웜, 소버 웜 변형이 여러 건 발견되어 피해를 입힌 것이 그 원인이다.

피해신고 된 악성코드 유형 현황

11월에는 10월에 비해 웜이 3% 가량 감소하여 50%를 차지한 반면, 트로이목마, 드롭퍼는 전월에 비해 3%씩 증가하여 트로이목마 29%, 드롭퍼 6%를 차지하고 있다. 꾸준히 증가하던 바이러스 비율도 지난 9월을 기점으로 1%씩 감소하여 14%로 감소 추세이다.

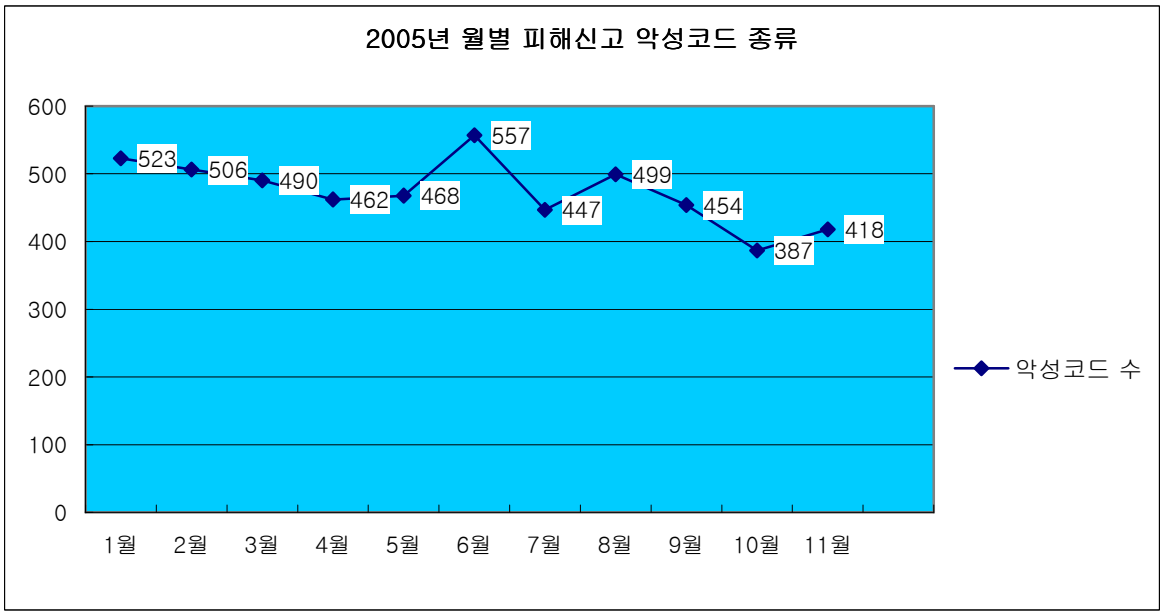
악성코드 유형별 현황은 [그림4]와 같다.



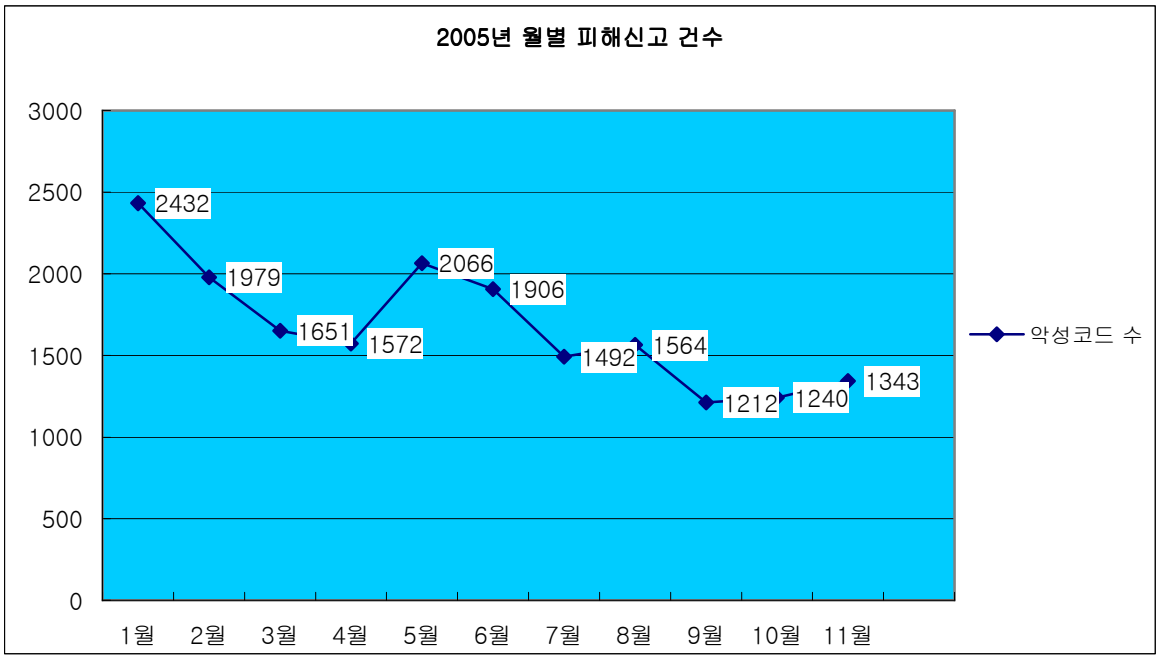
[그림4] 2005년 11월 피해 신고된 악성코드 유형별 현황

월별 피해신고 된 악성코드 종류 현황

11월에 피해 신고된 악성코드 진단명은 418개이며, 지난 10월에 비해 31개 증가하였다. 앞서 얘기했듯이 웜이 3%가량 감소한 반면, 트로이목마와 드롭퍼는 각각 3% 가량 증가하였다. 이것은 리니지핵(Win-Trojan/LineageHack), 드롭퍼(Dropper), 다운로더(Donwloader), 스크립트와 같은 일부 트로이목마 및 드롭퍼의 증가가 주요 원인이다.



[그림5] 2005년 월별 피해신고 악성코드 종류



[그림6] 2005년 월별 피해신고 건수

2005 년도 악성코드 피해건수는 전반적으로 감소추세를 보이다 9월부터 주춤하며 다시 소폭의 증가추세를 보이고 있다.

11월에 많은 변형이 발견되었던 매스메일러 웜 변형과 트로이목마 변형은 앞으로도 한동안은 점진적으로 증가할 것으로 보인다.

(2) 신종(변형) 악성코드 발견 동향

작성자: 정진성 주임연구원 (jsjung@ahnlab.com)

11월 한달 동안 접수된 신종(변형) 악성코드 건수는 [표1], [그림1]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
40	136	30	3	0	0	0	0	3	0	212

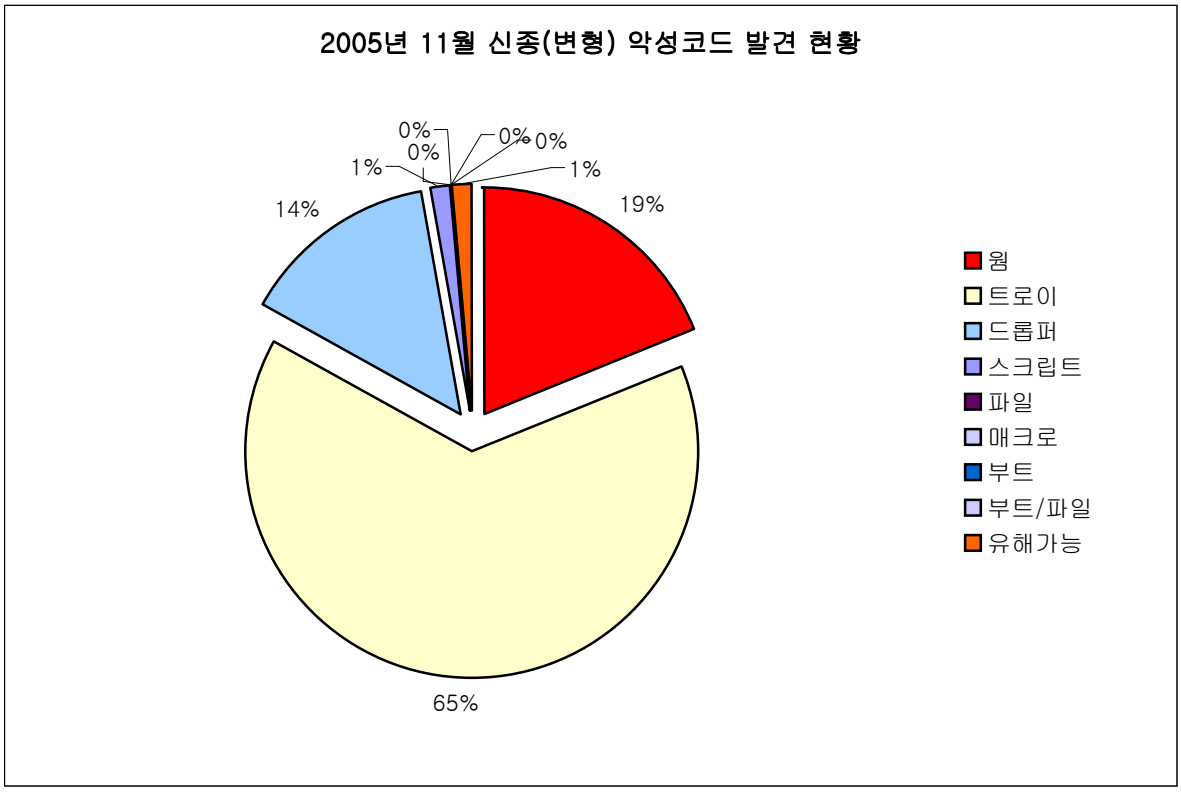
[표1] 2005년 11월 유형별 신종 (변형) 악성코드 발견현황

접수된 악성코드 건수가 지난달에 비해 소폭 증가하였다. 특히 트로이목마가 여전히 강세로 보이고 있어 다수의 트로이목마 변형들이 보고 되었다. 이중에서도 중국에서 제작된 것으로 알려진 다음의 트로이목마 변형들이 눈이 띄게 증가하였다.

- 그레이버드 트로이목마(Win-Trojan/GrayBird)
- 후피곤 트로이목마(Win-Trojan/Hupigon)

이 트로이목마들은 거의 동일한 형태로, 제작자는 웹 페이지에 계속적인 변형을 업로드 해 두고 있다. 해당 사이트에서는 이를 다운로드하여 사용하는 사용자에게 모든 책임을 전가하도록 하는 등 이를 공개한 자신은 악성코드를 유포한 것이 아니라고도 항변하고 있다. 이와 같이 주장하는 이유 중 하나는 제작자 자신이 이 트로이목마에 감염된 것으로 확인될 때 이를 삭제 할 수 있는 방법을 자세히 소개하고 있기 때문이다. 즉, 이를 이용하여 올바른 목적으로 사용하지 않는 사람들에게 책임을 짓도록 하고 있다. 중국에서는 관련법이 어떤지 알 수 없으나 별다른 제재가 없이 오랜 동안 사이트를 운영하고 있으며 이러한 악성코드를 제작, 업로드 하거나 또는 해킹 방법을 자세히 소개한 사이트가 상당수에 이르는 것으로 추정된다.
또한 해당 트로이목마들은 이를 다운로드하는 악의적인 목적을 가진 사람들에 의해 여러 가지 실행압축 툴을 조합하여 바이너리 코드가 완전히 다른 변형들이 계속적으로 만들어지기도 한다. 이 트로이목마들이 11월에 엔진에 추가된 악성코드 중 어느 정도의 비율을 차지하는지는 악성코드 유형별 변형 분포율에서 소개하도록 하겠다.

[그림1]은 11월 신종(변형)악성코드의 비율을 나타낸 것으로, 트로이목마가 차지하는 비율이 점점 높아지고 있다.



[그림1] 2005년 11월 신종(변형) 악성코드 현황

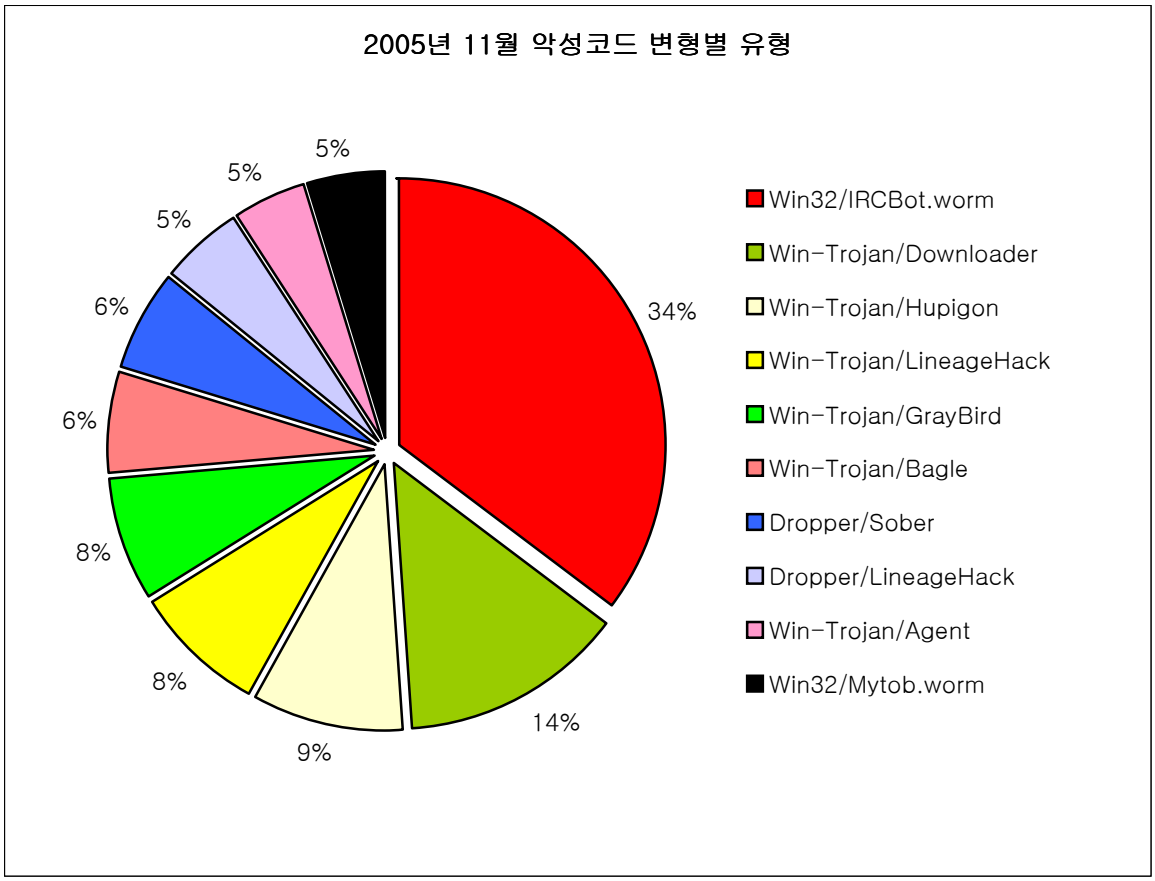
이번 달에 발견, 보고된 트로이목마 중 특이할 만 한 것은 다음과 같다.

- 코게임핵 트로이목마(Win-Trojan/KorGameHack)
- 그레이버드 트로이목마(Win-Trojan/GrayBird)
- 후피곤 트로이목마(Win-Trojan/Hupigon)

코게임핵 트로이목마는 국내 다수의 온라인 게임 사이트의 사용자 계정을 훔쳐내는 악성코드이다. 최근에는 온라인 게임의 아이템을 거래하는 사이트의 사용자 계정도 훔쳐내는 증상이 추가되었다. 이외에도 다음과 같은 트로이목마가 국내에서 제작되었다.

- 스팸에이전트 트로이목마(Win-Trojan/SpamAgent)
- 스팸메일러 트로이목마(Win-Trojan/SpamMailer)

이 트로이목마들은 국내 유명 포털 사이트의 메일 서버를 이용하여 스팸 메일을 발송하는 증상을 가지고 있으며 주로 포털 사이트의 커뮤니티게시판에서 Active X를 이용하여 설치된다. 이러한 유형의 스팸 메일러나 에이전트 류는 이전에도 있었던 형태이나 꽤 오랜만에 다시 발견, 보고된 사례라 할 수 있다.

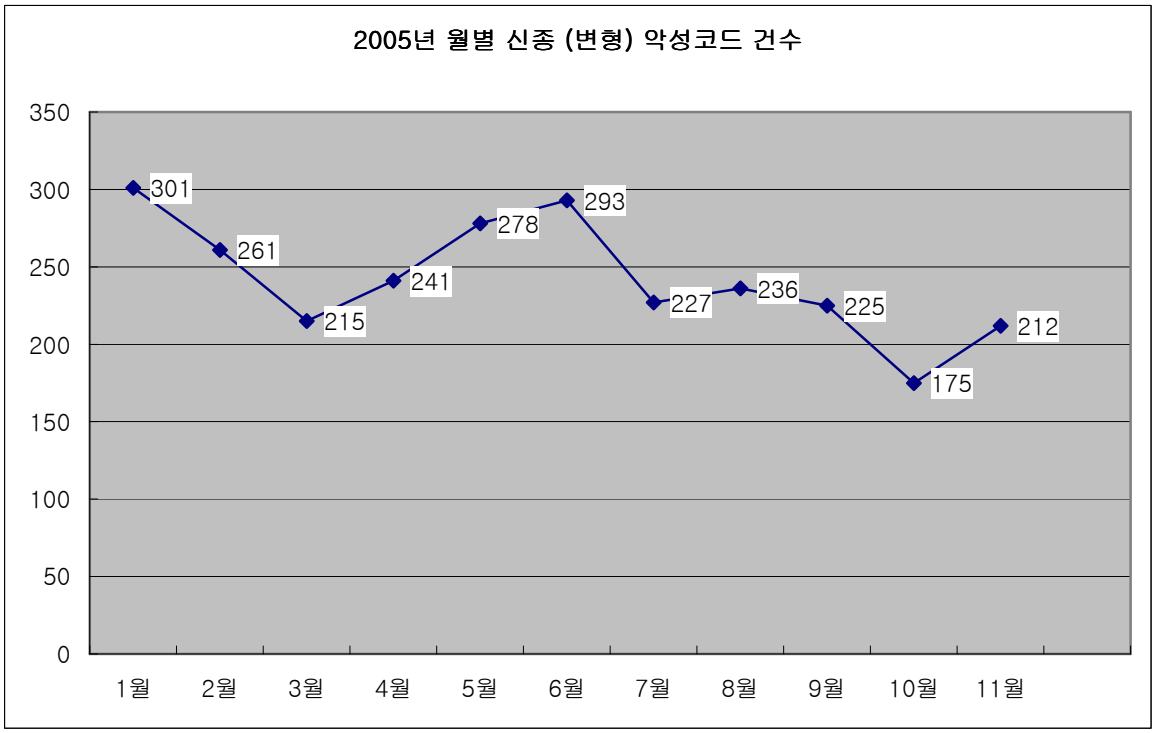


[그림2] 악성코드 변형별 유형 및 분포율

[그림2]는 11월 엔진에 반영된 악성코드 중 가장 많은 변형들을 가진 Top 10만을 집계 해 본 것이다. 지난달과 마찬가지로 아이알씨봇 웜(Win32/IRCBot.worm)이 가장 많은 분포를 차지하고 있다. 또한 위에서 언급한 것처럼 후피곤 트로이목마, 그레이버드 트로이목마 변형들에 대한 분포도 많은 부분을 차지하고 있으며, 특히 이번 달에 다수 발견, 보고된 Dropper/Sober도 눈에 띈다.

[그림3]은 월별 신종(변형) 악성코드 건수를 나타낸 것이다. 지난달은 200건 미만의 적은 수의 악성코드가 접수되었었으나, 이번 달은 다시 신종(변형)의 악성코드 접수가 소폭 상승하였다. 전체적인 상승의 원인은 다음과 같은 악성코드의 발견, 보고가 증가했기 때문이다.

- 그레이버드 트로이목마(Win-Trojan/GrayBird)
- 후피곤 트로이목마(Win-Trojan/Hupigon)
- 코게임핵 트로이목마(Dropper/KorGameHack)
- 소버 드롭퍼(Dropper/Sober)



[그림3]2005년 월별 신종(변형) 악성코드 발견 현황

11월 주요 신종(변형) 악성코드 정리

이번 달의 최대 이슈는 소니 BMG(Sony BMG)의 DRM (Digital Rights Management) 관련 루트킷(Rootkit) 사건으로, 불법복제를 방지하려고 만들어 둔 프로그램이 은폐형 악성코드가 이용하는 은폐기법을 이용하여 자신을 숨겨두어 문제가 된 것이다. 또 다른 이슈로는 소버웜(Win32/Sober.worm) 변형과 자신을 끊임없이 확장, 유지하고 있는 베이글 트로이목마(Win-Trojan/Bagle)변형이 다수 보고된 것이다. 끝으로 심비안 OS(Symbian OS) 관련 악성코드들의 피해증상이 주로 모바일 폰 기기 자체나 모바일 폰 내 특정 응용 프로그램을 손상하는 형태로 발전하고 있는 것 또한 이슈가 되었다.

이슈가 되었던 이번 달의 악성코드 및 주요사건은 다음과 같다.

► 소니 BMG의 DRM 관련 루트킷 사건

소니 BMG는 불법복제를 방지하기 위해 자사의 몇 가지 음악 CD에 DRM 관련 프로그램을 함께 담아 두었다. 문제는 이 DRM 프로그램이 자신이 실행중인 것을 숨기기 위하여 커널모드 루트킷이 사용하는 기법-Native API를 후킹하여 자신의 프로세스, 파일, 레지스트리, 네트워크 등을 숨기는 것-을 그대로 사용하고 있다는 것이다. 응용 프로그램이 자신의 존재를 숨기는 것은 매우 부절한 방법이다. 가장 큰 문제는 이 음악 CD를 구입한 소비자 조차 해당 프로그램이 자신의 시스템에서 수행되고 있다는 것을 모르도록 숨기고 있다. 또한 은폐되는 파일이나 정보 등을 다른 악성코드가 역이용하여 자신의 존재를 쉽게 숨길 수도 있다. 브레

프리봇 트로이목마(Win-Trojan/Breplibot)라고 명명된 악성코드가 그 좋은 예이다. 소니 DRM 루트킷 사건이 알려지지 얼마 되지 않은 시점에서 해당 DRM 프로그램이 사용하는 파일명으로 위장한 악성코드가 발견되었기 때문이다.
지금은 소니가 해당 DRM 프로그램이 더 이상 은폐기법을 사용하지 않도록 업데이트 하였지만 필자가 원고를 준비하는 12월초에도 이 악성코드의 변형이 보고 되고 있다.
소니 BMG는 불법복제를 막기 위하여 DRM 프로그램을 사용하고 또한 이 프로그램을 보호하기 위해서 은폐기법을 사용한 것으로 보이지만 악성코드가 이용하는 기법을 그대로 사용하는 것은 분명 문제가 있다. 자신이 만든 프로그램을 보호하기 위해 은폐기법을 사용하기 보다는 컴파일 된 바이너리를 보호하는 툴을 사용하는 것이 바람직하며 보안을 위해 악성코드가 이용하는 기법들을 사용하는 일이 더 이상 발생해서는 안 될 것이다.

► 소버 웜(Win32/Sober.worm) 확산

소버 웜은 2003년 10월 중순경 처음 발견, 보고된 이메일 웜이다. 아마도 가장 오랜 기간 변형이 계속적으로 발견되고 있는 이메일 웜이 아닌가 싶다. 이번에 발견된 소버 웜(Win32/Sober.worm.55390)은 메일에는 드롭퍼(Dropper)를 첨부하여 발송하였고 해당 드롭퍼를 실행하면 여기서 생성된 파일이 로컬 드라이브에서 메일주소를 수집하여 역시 드롭퍼 형태의 자신을 첨부하여 메일을 보내게 된다. 소버 웜의 특징 중 하나는 웜 내부에 하드코딩된 NTP(Network Time Protocol, TCP/37) 서버 리스트와 통신하고 특정일에 어떤 조건을 실행한다는 것이다. NTP 서버를 이용하면 감염된 시스템이 어느 지역에 있어도 동일한 날짜와 시간에 특정 조건을 수행 할 수 있다는데 그 의미가 있다. 이번 소버 웜 변형의 경우 2006년 1월 5일 특정 호스트로부터 자신의 변형으로 추정되는 파일을 다운로드 받도록 되었다.

또한 이번 달에 발견된 소버 웜 변형의 특징 중 하나는 네트워크를 마비시킬 정도의 대량 메일을 발송하였다는 것이다. 이로 인해 국내 모 업체는 잠시 네트워크가 중단된 사례까지 있었다. 이는 이 웜이 윈도우 XP SP2의 TCPIP.SYS 파일을 패치하여 윈도우가 TCP 동시연결을 제한하는 것을 무력화시키는 증상이 있는데, 이로 인해 나타나는 현상으로 추정된다. 즉, 윈도우 XP SP2는 악성코드에 감염되어도 네트워크 트래픽을 유발시키지 못하도록 한번에 아웃바운드 되는 TCP 커넥션에 대한 동시연결 수를 10개로 제한하고 있으나, 소버 웜은 TCPIP.SYS 파일을 패치하여 이를 50개로 증가시켜 자신을 전파하는 TCP/25 커넥션을 충분히 확보 할 수 있도록 한다. 따라서 이로 인해 동일 세그먼트 내 네트워크에 감염된 시스템이 많다면 네트워크 마비 등의 문제가 충분히 발생할 수 있는 것이다. 이와 같은 패치 방법은 오래 전부터 외국의 한 해커로부터 알려졌으며 이를 그대로 소버 웜이 사용하고 있다. 또한 소버 웜은 윈도우 업데이트 시 설치되는 '악성 소프트웨어 제거 도구'도 실행하지 못하도록 무력화하는 등 자신의 생존을 위해 더욱 더 악의적인 증상을 수행한다.

► 베이글 제국(Empire of Bagle)

지난 10월에 개최된 Virus Bulletin 2005 Conference에서는 “Solving the Bagle jigsaw”란 주제로 CA 연구원들의 발표가 있었다.[1] 이 발표에서는 웜, 바이러스 그리고 트로이목마 등 다양한 형태로 존재해 온 베이글 웜을 대략 10가지로 분류하고 있다. 이를 국내에 유입된 것과 그렇지 않은 것으로 다시 분류해 보면 다음과 같다.

종류	유형	국내 발견시기	비고
베이글(Bagle)	Expansion[2]	최초발견 ~ 2005년 중반	매스메일러
미트글라이더(Mitglieder)	Exploitation [3] Survival[4]	2004년 중반 ~2005년	프록시 서버와 스팸 릴레이 담당 백도어 포트 오픈, 보안 및 백신 프로그램 무력화
인터글라이더(nterglieder)	Survival		
글라이더(Glieder)	Exploitation, Survival	2005년 2월 ~현재	특정 URL 에서 베이글 다운로더나 인터글라이더 파일 다운로드 보안 및 백신 프로그램 무력화
매니백(Manibag)	Expansion	2005년초	
웹호스트(Web hosts)	Exploitation Expansion Survival	미발견	
헤프티글라이더 (Heftyglieder)	Exploitation	미발견	
폼글라이더(Formflider)	Exploitation	미발견	
하백(Harbag)	Exploitation Expansion	미발견	
팬티백(Fantibag)	Survival	미발견	

악성 아이알씨봇에 감염된 시스템들이 공격자에 의해서 거대 네트워크로 연결된 형태를 봇넷(BotNet)이라고 부른다. 이것처럼 베이글도 그 제작자로부터 거대한 네트워크를 형성하고 있어 제작자가 필요하다면 언제든지 감염된 시스템을 이용하여 어떤 이익을 취득하거나 확

[1] VB 2005., ‘Solving the bagle jigsaw’ http://www.virusbtn.com/conference/vb2005/abstracts/HamishODea_ScottMolenkampTechThurs0900.xml

[2] Expansion: 베이글에 감염된 시스템을 확대시키는 목적을 수행하기 위한 베이글 변형

[3] Exploitation: 감염된 시스템을 이용하여 프록시 서버나 스팸 릴레이 등의 기능을 수행하는 베이글 변형

[4] Survival: 베이글 자신의 생존을 유지시키는 목적을 수행하기 위한 베이글 변형

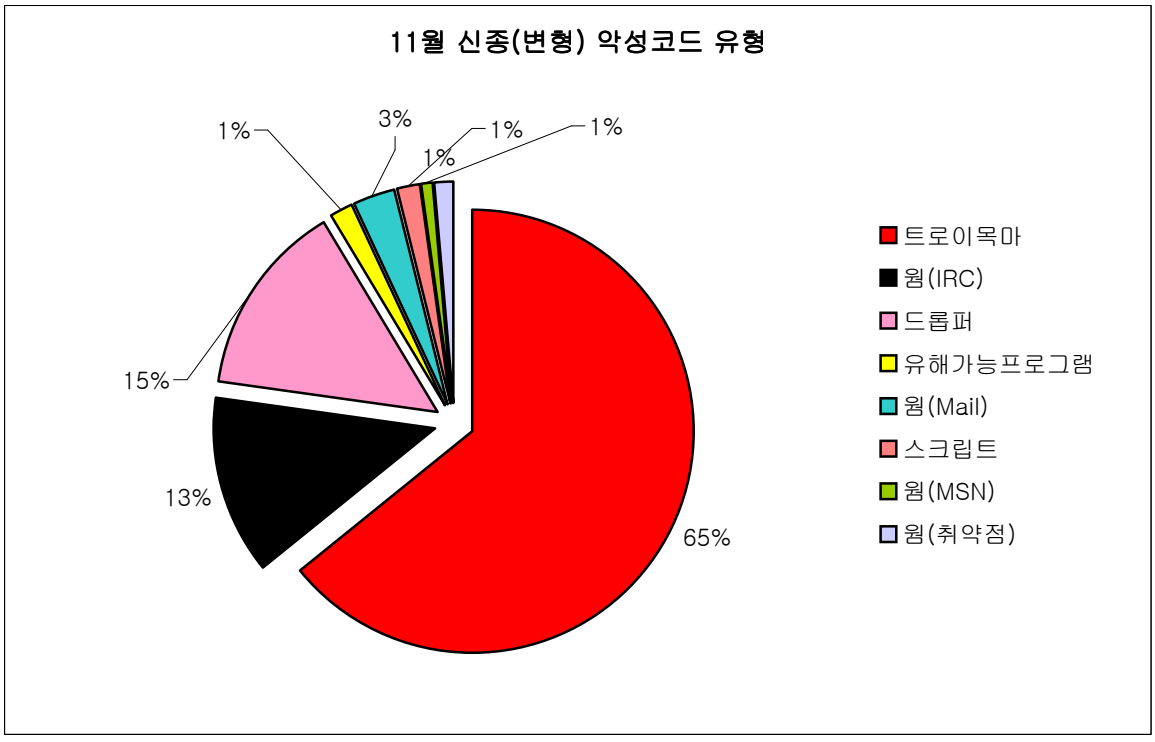
장, 혹은 필요시 자신을 소멸 시킬 수 있도록 베이글 전파와 생존이 자동화 및 시스템화되어 있다. 앞으로도 베이글의 거대 네트워크는 좀처럼 타의에 의해서 무력화되거나 소멸되지 않을 것으로 예상된다.

► 심비안(Symbian) OS을 노리는 모바일 악성코드 피해

11월 한달 동안 여러 종류의 모바일 악성코드가 발견, 보고 되었다. 최근에 발견되는 악성코드들은 모두 심비안 OS 자체를 손상하거나 해당 기기의 응용 프로그램을 공격하는 형태가 증가하고 있다. 여기서 심비안 OS 자체 손상은 OS 자체의 중요한 파일을 악성코드로 대체하거나 또는 손상된 시스템 파일을 드롭(Drop)함으로써 이후 기기를 재부팅하면 손상된 파일로 인해 기기가 올바르게 부팅되지 못하도록 하는 것을 말한다. 응용 프로그램의 공격 역시 해당 프로그램의 메뉴를 숨기거나 자신으로 대체함으로써 해당 응용 프로그램이 올바른 동작을 하지 못하도록 방해하는 것을 말한다.

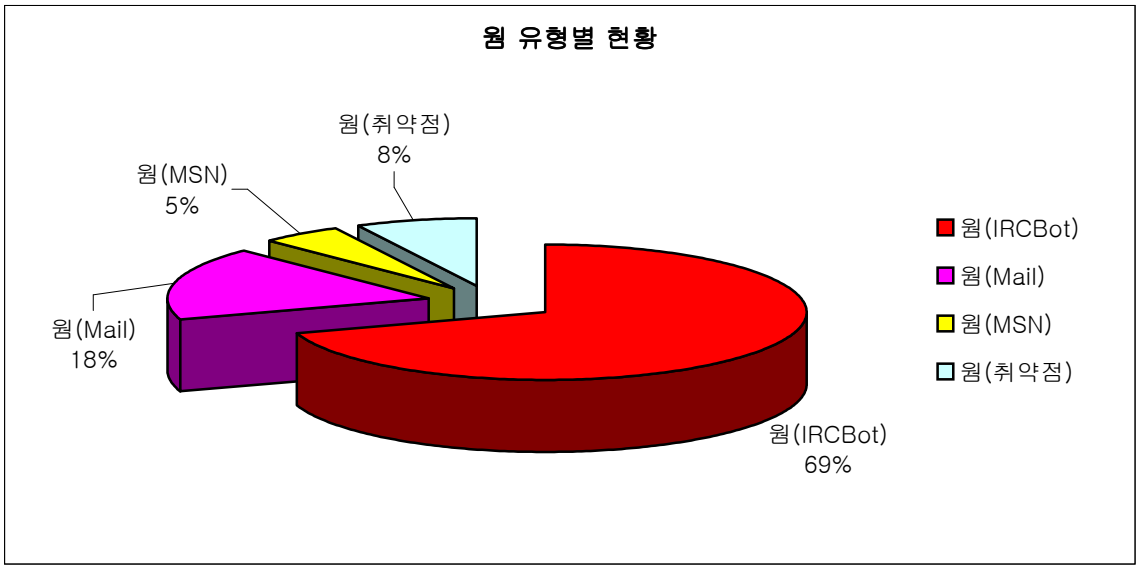
모바일 기기에서 이런 피해증상은 일반 사용자들이 복구하기 어려운 문제점을 갖고 있다. 심지어 시스템을 초기화하거나 시스템 파일을 복구하기 위하여 A/S 센터를 방문해야 할 수도 있기 때문이다. 모바일 기기 특성상 계속 켜져 있어야 하고 데이터를 저장하거나 일정관리 또는 전화를 받아야 한다. 악성코드의 이러한 피해증상으로 단지 기기를 수리하는 물리적인 피해액 이상의 피해가 발생 할 수 있다는 점에서 이와 같은 증상의 악성코드가 널리 확산되었을 경우 심각한 문제를 초래할 수도 있다.

다음은 이번 달에 발견된 신종(변형) 악성코드 유형에 대한 분포이다.



[그림5] 11월 신종(변형) 악성코드 유형별 현황

이번 달은 다양한 웜 유형들이 보고되었다. 특히 알려진 SQL 서버의 취약점을 노리는 웜이 보고 되었다. 또한 국내에 중국 발 해킹이 잦아지면서 공격툴은 이미 자동화되었다. 그렇다면 이제는 능동적으로 취약한 시스템을 찾아 대상 시스템에 악의적인 일을 수행하는 웜의 제작이 가능할 수도 있다고 일부에서는 생각한다. 하지만 우려와 달리 중국 발 해킹은 자신을 전파하려는 목적보다는 2대 이상의 대상 시스템을 해킹하고 이를 관리하며 다른 악성코드를 업로드 해두는 등의 작업이 필요하다. 즉, 관리라는 측면이 들어가므로 능동적으로 자신을 전파하여 해킹하는 문제는-기술적으로는 어렵지 않겠지만-관리의 어려움 등으로 인하여 아직 출현, 보고되지는 않았다.



[그림6] 11월 신종 및 변형 웜 유형별 현황

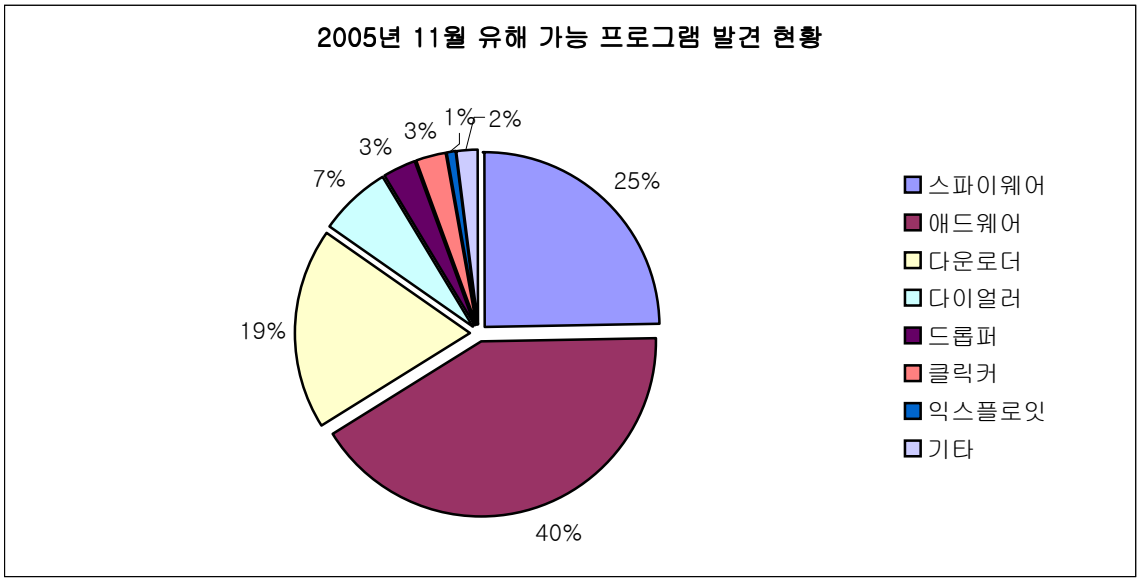
II. 11월 AhnLab 스파이웨어 동향

작성자: 장혜윤 연구원(planet@ahnlab.com)

11월 한달 동안 접수된 신종(변형) 유해 가능 프로그램 건수는 [표1], [그림1]과 같다. 11월에는 특이한 현상을 보이지 않았고, 이전 10월보다는 적은 유해 가능 프로그램 발견 비율을 보이고 있다.

스파이웨어	애드웨어	다운로더	다이얼러	드롭퍼	클릭커	익스플로잇	기타	합계
153	257	116	41	19	17	6	12	611

[표1] 11월 유형별 신종(변형) 유해 가능 프로그램 발견 현황



[그림1] 2005년 11월 발견된 유해 가능 프로그램 비율

11월은 올 다른 달에 비해 대량으로 스파이웨어를 배포하고 있다. 그 원인으로는 여러가지가 있겠지만, 결정적인 이유는 연말이 다가오면서 돈벌이를 하려는 것으로 추측된다.
스파이웨어는 사람들이 의심하지 않고 클릭하거나 다운로드하는 의심스러운 인터넷 광고나 다운로드 프로그램을 통해 대부분 전파되며, 전파된 스파이웨어는 사용자에게 팝업 광고를 보여주거나 특정 사이트로 이동을 시키게 된다. 팝업 광고 클릭 및 특정 사이트 이동 시마다 스파이웨어 제작사들에게 돈을 주기 때문이다.

국내 포털사이트 및 카페에 접속하게 되면 최소 4개의 ActiveX 방식을 통해 설치되는 프로그램을 확인할 수 있다. 대부분이 안티 스파이웨어 제품들이다. 업체마다 아르바이트를 고용해서 웹에 ActiveX를 게시하고 배포하고 있다. 이렇게 게시된 AcitveX에는 게시한 아르바이트에 대한 정보를 갖고 있어, 설치될 때마다 일정 금액을 주기 때문이다.

III. 11월 시큐리티 동향

작성자: 정관진 주임연구원(intexp@ahnlab.com)

1년 12달 중 벌써 많은 시간이 흘러 2005년의 마지막에 이르렀다. 이번 11월 달에는 큰 보안적 사고가 보고되지 않았으며 MS의 보안업데이트도 1건만이 발표되었다. 이번에 발표된 보안업데이트 중 MS05-053은 그래픽 렌더링 엔진과 관련한 취약점으로 이를 이용한 악성코드도 발견되었다. 보고된 것은 특정 코드를 실행시키는 것이 아닌 서비스거부공격(DoS:Denial of Service) 수준으로, 위험성은 낮은 편이다. 그리고 MS05-051을 이용하는 공격코드가 공개되어 향후 이를 이용한 악성코드의 등장도 우려되지만 영향을 받는 운영체제를 고려하면 제한적이 될 것으로 예측된다. 이외에 인터넷 익스플로러에서 새로운 신규 취약점이 보고되었으나 MS의 공식적인 패치가 발표되지 않은 상태이며, 윈도우 플랫폼 이외에 오라클 데이터베이스와 PHP XML-RPC 취약점을 이용하여 전파되는 웜의 사례를 통하여 향후 악성코드의 플랫폼 향방에 대해서 조명해 보고자 한다.

11월의 주요 취약점 현황[1]

위험등급	취약점	공격코드 유/무
HIGH	그래픽 렌더링 엔진 취약점(MS05-053)	유
MID	윈도우 RPC 메모리 할당 서비스거부공격	유
HIGH	인터넷 익스플로러 "Window()" 원격코드 실행 취약점	유
HIGH	윈도우 DTC(Distributed Transaction Coordinator) 원격코드 실행 취약점(MS05-051) – 10월에 발표된 취약점으로 11월에 공격코드 공개됨	유

► 악성코드의 플랫폼은 어디까지인가?

현재 악성코드의 주요 활동무대가 되고 있는 플랫폼은 윈도우 환경체제이다. 윈도우 플랫폼이 주 무대가 될 수 있었던 것은 가장 대중적으로 사용되고 있기 때문이다. 악성코드 제작자 입장에서도 유닉스 시스템과 같이 제한적으로 사용되는 플랫폼 보다는 윈도우 플랫폼이 훨씬 매력적일 것이다. 이것은 악성코드를 많은 사용자에게 전파시킬 수 있고 피해를 더욱 크게 입힐 수 있는 간단한 답이 있기 때문이다.

하지만, 악성코드가 존재하는 영역은 다양하고도 넓게 확장될 것이다. 이미 모바일(Mobile) 환경이 증가하면서 모바일 악성코드가 나타나고 있고, 다양한 플랫폼에서 호환만 될 수 있다면 급속한 증가가 이뤄지리라 예측된다.

[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

최근에는 오라클 데이터베이스를 통해 전파되는 웜의 가능성을 보여준 사례도 보고되었다. 이것은 PL/SQL로 제작된 개념증명의 공격코드로 로컬 서브넷(Local Subnet)네트워크를 스캐닝하고 TNS를 통해 접속한다. 이후 기본 사용자이름과 패스워드를 이용하여 다른 데이터베이스에 접속 후 성공할 경우 'X' 라는 테이블을 생성하게 된다. 이 자체가 위험성을 내포하고 있지는 않았지만 데이터베이스로까지 위협대상이 넓어질 수 있음을 보여준 경우이다.

물론, 직접적으로 데이터베이스의 문제점을 이용한 것은 아니다. 디폴트 사용자이름과 패스워드를 사용하지 않고 리스너의 기본포트인 1521을 사용하지 않았다면 영향을 받지 않았기 때문이다. 이외 PHP XML-RPC 취약점을 이용하여 전파되는 루퍼 웜(Linux/Lupper)도 보고되었다. POST 형식으로 XML-RPC를 사용하는 PHP 파일에 특정 명령어를 삽입하는 방법을 이용하고 있다. 비단 최근에 발생한 사례가 아니더라도 과거에 다양한 플랫폼에 대한 사례가 보고 되었기 때문에 인터넷에 연결되어 있는 네트워크 환경이라면 언제든 위협에 노출될 수 있다는 사실에 주목해야 할 것이다.
새로운 플랫폼의 등장과 다양한 응용프로그램들의 증대가 악성코드의 생명력을 더욱 확장시켜 줄지는 알 수 없지만 분명한 것은 대중화가 된다는 사실이 표적의 대상이 될 수 있다는 사실을 기억해야 할 것이다.

► 취약점 공개 정책 – 찬반 양론

'새로운 취약점을 발견하였을 경우 이것을 공개하는 것이 타당한가?' 라는 질문에 명확한 답을 내리기는 쉽지 않다. 찬반 양론에 놓여있는 이 질문에는 다양한 관점이 존재하기 때문이다. 취약점을 공개적으로 발표하는 경우 패치가 제공되지 않은 시점에서는 외부의 위협에 노출되어 위험에 직면할 가능성이 높아진다. 공격자 입장에서는 이러한 정보가 또 다른 공격을 야기하는데 큰 도움이 되지만 실제 실 사용자입장에서는 달갑지 않은 것이 사실이다. 그렇다면 취약점 정보를 공개하지 않는다면 어떨까? 해당 취약점은 계속 공격에 노출된 형태로 놓여있게 되고 만약 악의적인 공격자에 의해 발견되게 되면 실질적인 공격위협에 놓여질 수 있다. 현재 취약점 공개 정책은 모두 다 다르지만 공통적으로 다음과 같은 프로세스에 의해 처리된다.

- 발견된 취약점을 해당 업체에 통보
- 취약점 공개시점 논의 (취약점 공개시기에 대한 적절한 사유가 있어야 하며 이러한 것에는 패치 개발 시간, 적용, 테스트등의 다양한 요소들이 있다)
- 업체의 취약점 패치 발표 또는 해결책 제시
- 취약점 공개

고객의 피해를 최소화하기 위하여 해당 업체와 의견조율 후 취약점 공개일정을 정하게 되는 것이 일반적인 관례이다. 즉, 취약점을 공개하더라도 취약점에 대한 문제해결 방법이 제공된 후 공개하는 정책이다.

이와 달리 최근에 컴퓨터 테러리즘(Computer Terrorism)[1]에서는 개념증명코드(PoC: Proof of Concept)와 함께 취약점 권고문을 발표하였다. 이 취약점은 인터넷 익스플로러에서 자바스크립트 Window() 기능을 이용하여 원격에서 코드가 실행 가능한 것으로 마이크로소프트사(이하 MS)에서 패치가 제공되지 않은 경우여서 논란의 여지가 일고 있다. MS사는 이미 이 취약점에 대해서 인지하고 있었고 조사를 진행 중 이라고 밝혔으나, 패치 발표 이후에 취약점을 공개하는 업계의 관습을 깬 행위라고 비난하였다.[2] 이 취약점은 이미 2005년 5월에 발표된 것이었으나 그 당시에는 DoS 수준으로만 알려져 있었다

일단 패치 발표전에 취약점이 공개되어 인터넷 익스플로러를 사용하는 사용자는 주의가 필요하게 되었고 이번 취약점의 공개로 인하여 해당 취약점에 대한 패치 제공 속도가 더욱 빨라질 것은 자명한 일이다.

취약점 공개에 따른 찬반 양론은 앞으로도 계속 뜨거운 감자로 남을 것이다.

[1] Computer Terrorism: http://www.computerterrorism.com
[2] 취약점의 위험성에 따라 조만간 패치가 발표될 예정이다.

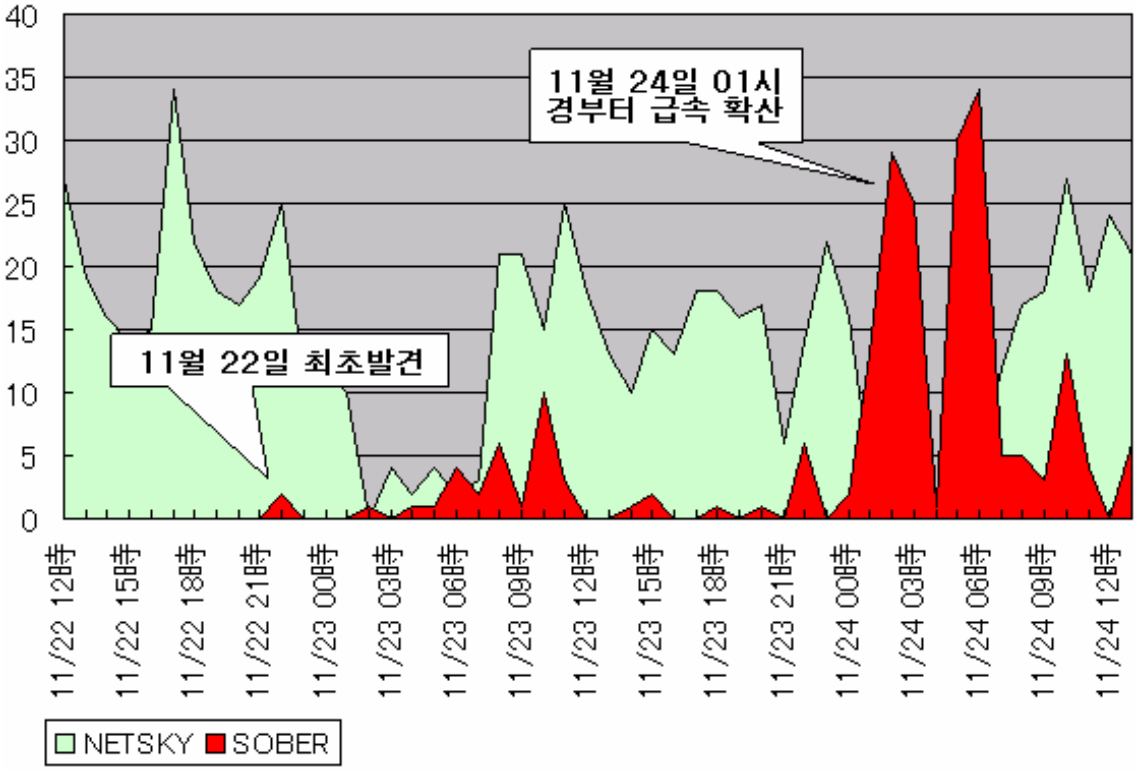
IV. 11월 세계 악성코드 동향

2005년 11월 세계 악성코드 동향에서 가장 큰 이슈가 되었던 사건은 소버 웜 변형이 급속하게 확산된 것이다. 최근 발견된 소버 웜 변형은 11월 22일 최초로 발견된 이후 매우 많은 피해 사례가 보고되었다. 기존의 소버 웜의 경우 일부 언어의 윈도우 OS에서 웜이 실제로 동작하지 않았기 때문에 아시아 국가에서의 확산도가 매우 낮았으나 이번에 발견된 소버 웜 변형의 경우 한국과 일본 등 아시아 지역에서도 매우 많은 피해가 보고되고 있다. 그러나 중국의 경우 아시아 지역의 다른 나라들에 비해 상대적으로 소버 웜에 의한 피해가 적은 것으로 보이고 여전히 트로이목마에 의한 피해가 많은 상태이다.

(1) 일본의 악성코드 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

2005년 11월 발생한 일본의 악성코드 동향에서 가장 큰 이슈는 11월 말부터 소버 웜(Win32/Sober.worm)이 급속히 확산된 것이다. 아래의 [그림1]은 일본의 IPA(www.ipa.go.jp)에서 발표한 소버 웜의 확산도에 대한 탐지 통계이다.



[그림1] 소버 웜 탐지 통계(출처: 일본 IPA)

11월 24일을 기점으로 소버 웜의 탐지 건수가 급격하게 급격히 늘어난 것을 볼 수 있다. [그림1]에서는 소버 웜의 확산도를 넷스카이 웜과 비교해서 보여주고 있는데 넷스카이 웜과

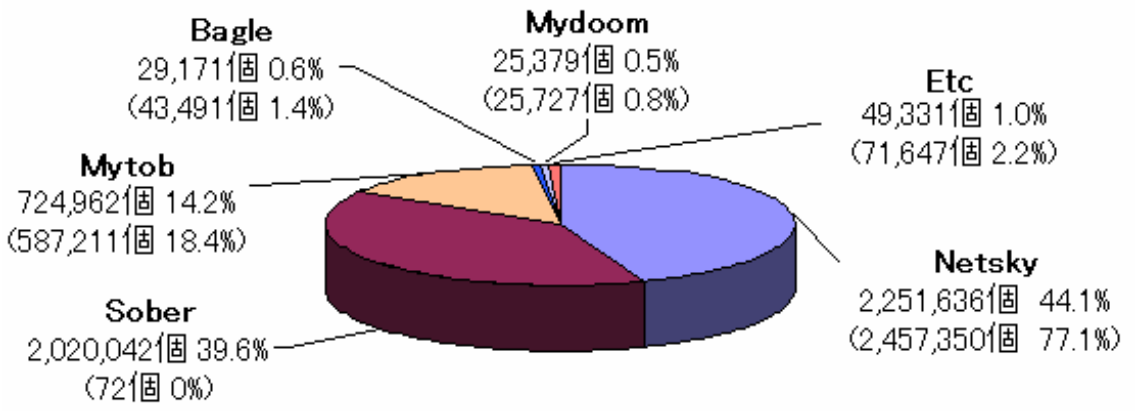
같이 지속적으로 전파되지는 않았지만 짧은 기간 동안 넷스카이 웜과 비슷한 정도로 확산되는 것을 알 수 있다. 소버 웜의 경우 여러 변형이 많은 넷스카이 웜에 비해 상대적으로 변형이 많지 않은 것을 고려했을 때 최근 확산된 소버 변형의 감염 시 피해의 정도를 짐작할 수 있게 해준다. 일본 Cert(www.jpcert.or.jp)에서도 소버 웜의 감염 피해에 대한 주의를 당부하는 권고문을 발표했다[1].

일본의 악성코드 동향

11월 일본에서 가장 많이 확산된 악성코드는 넷스카이 웜(Win32/Netsky.worm)이다.

[그림2]는 일본의 IPA에서 발표한 악성코드 통계 중 11월에 발생한 악성코드의 탐지 건수를 그래프로 나타낸 것으로써 넷스카이 웜이 전체 탐지된 악성코드의 44%를 차지하고 있는 것을 볼 수 있다.

한가지 특이할 만한 사항은 소버 웜의 탐지 건수가 40%에 달하는 점이다. 전월 소버 웜에 대한 탐지 건수가 72건인 것과 비교했을 때 탐지 건수가 급격하게 증가한 것을 알 수 있다.



[그림2] 악성코드 검출 통계(출처: 일본 IPA)

아래의 [표1]은 악성코드 별 감염피해 신고현황을 나타낸 것이다. 소버 웜의 경우 신고 건수가 133건으로 도표에 나타나지는 않았지만 11월 말 새로운 변형이 발생하여 확산되기 시작한 점을 고려해 보았을 때 단기간 동안 매우 많은 사용자가 감염 피해를 당했음을 짐작할 수 있다.

[1] http://www.jpcert.or.jp/at/2005/at050011.txt

Window/Dos Virus	금월피해	Macro Virus	금월피해	Script Virus	금월피해
	전월피해		전월피해		전월피해
Win32/Netsky	907	Xm/Laroux	10	VBS/Redlof	54
	902		11		60
Win32/Mytob	529	XF/Sic	5	VBS/Soraci	6
	484				3
Win32/Bagle	296	X97M/Divi	3	Wscript/	6
	287		1	Fortnight	5
Win32/Mydoom	243	W97M/Bablas	2	VBS/Loveletter	5
	299				9
Win32/Lovgate	189	W97M/Lexer	1	VBS/Gedza	2
	231				
Win32/Klez	168	X97M/Makrer	1	VBS/Freelink	1
	184				

[표1] 악성코드 피해 신고 현황

악성코드의 감염 경로별 통계

[표2]는 악성코드의 감염 경로 별 통계로써 메일을 통한 감염 피해가 가장 많은 것을 알 수 있다. 또한 전월에 비해 네트워크를 이용하여 전파되는 악성코드의 감염 건수가 상대적으로 감소한 것을 알 수 있다.

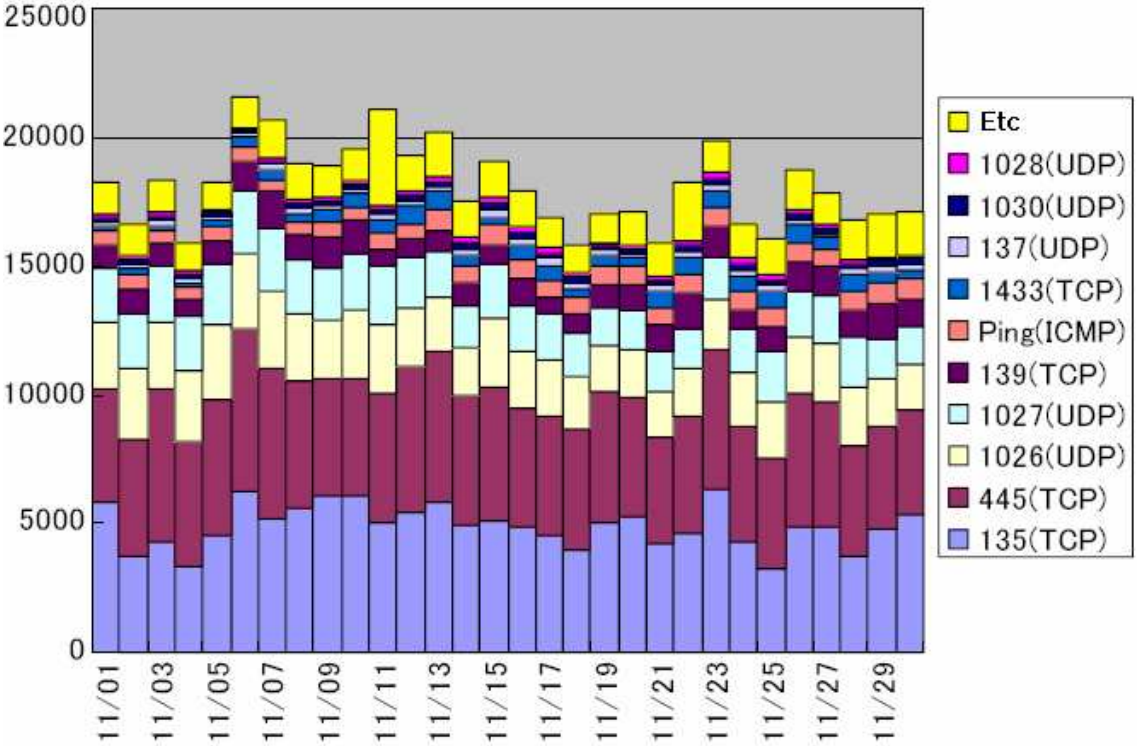
감염경로	피해 건수					
	2005년 11월		2005년 10월		2004년 11월	
메일	3,643	95.5%	3,386	94.2%	5,229	98.5%
외부의 모체	2	0.1%	7	0.2%	3	0.1%
다운로드	1	0.0%	1	0.0%	5	0.1%
네트워크	166	4.4%	224	5.5%	62	1.2%
기타	4	0.1%	3	0.1%	9	0.2%

[표2] 악성코드 감염 경로 통계

일본 네트워크 트래픽 현황

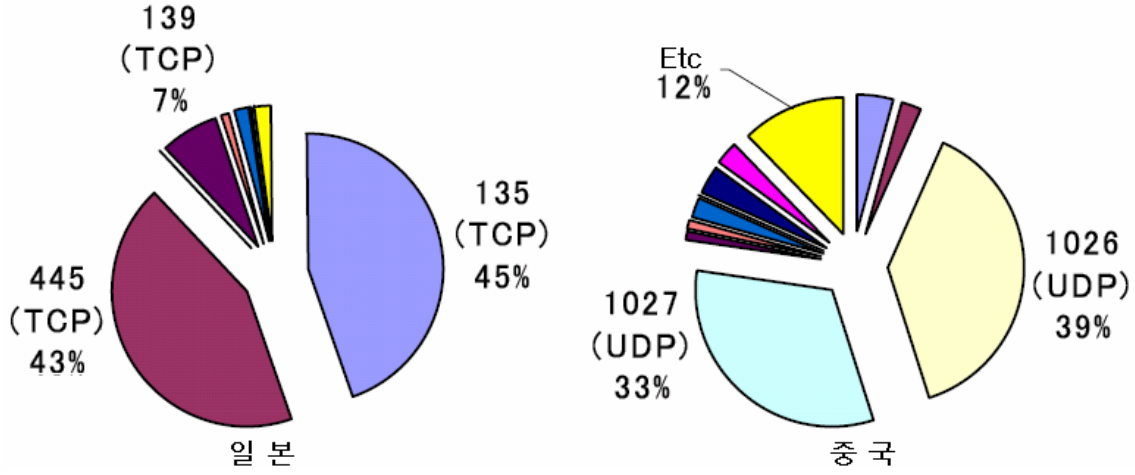
[그림3]은 2005년 11월 발생한 일본의 네트워크 트래픽 현황을 나타낸 것이다. TCP 135 포트와 TCP 445 포트를 이용한 네트워크 트래픽이 매우 많은 것을 볼 수 있다. 해당 포트들은 윈도우 OS에서 기본으로 사용되는 포트들이지만 아이알씨봇과 같은 웜들이 자신을 전파하기 위한 공격 경로로 사용하기도 한다.

[그림3]에서 특이할 점은 UDP 1026 포트와 1027 포트의 트래픽이 현저하게 늘어난 것이다.

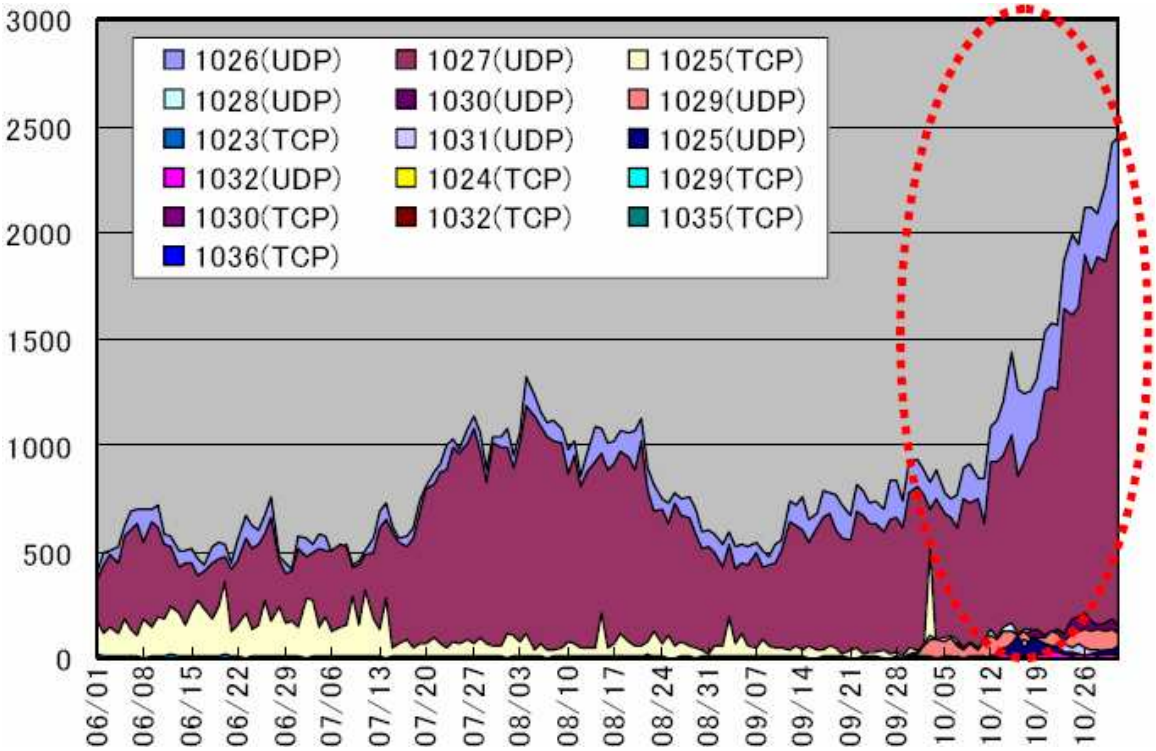


[그림3]일본의 네트워크 트래픽 현황(출처: 일본 IPA)

[그림4]는 일본을 목적지로 하는 포트들에 대한 통계 중 일본과 중국의 IP에 대한 사용 포트들에 대한 통계를 나타낸 것이다. 그림에서 볼 수 있는 것처럼 중국을 발신지로 하는 IP들에서 UDP 1026 포트와 UDP 1027 포트를 이용한 트래픽이 매우 많은 것을 알 수 있는데 이러한 현상이 발생한 원인은 윈도우 OS에 내장된 메신저 서비스를 이용한 광고성 메시지를 전송하는 것으로 파악되고 있다.



[그림4] 일본과 중국의 사용 포트 비교



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

(2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

이번 11월 중국 악성코드 동향은 여전히 트로이목마의 감염 비율이 높게 점유되고 있다. 하지만 그 세부적인 내역을 10월과 비교해 보면 새로운 트로이목마 변형들 다수가 순위권에 진입한 것을 알 수 있다. 그러나 그레이버드 트로이목마(V3 진단명, Win-Trojan/GrayBird 또는 Win-Trojan/Hupigon)는 여전히 가장 높은 감염 비율을 보이고 있었다. 새로운 트로이목마들은 다운로더, 스타트페이지 류와 같은 전통적인 트로이목마의 형태가 아니라 최근에 들어서야 알려진 트로이목마가 대부분 차지하고 있는 것으로 미루어 트로이목마 형태 내부에서도 변화가 이루어지고 있는 것으로 추정되고 있다.

악성코드 TOP 5

순위 변화	순위	Rising
-	1	Backdoor.Gpigeon
New	2	Backdoor.Agent
↓ 1	3	Trojan.PSW.LMir
New	4	TrojanDownloader.Small
New	5	Trojan.StartPage

[표1] 2005년 11월 Rising 악성코드 TOP 5

'-' - 순위변동 없음, 'New' - 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

순위 변화	순위	JiangMin
New	1	TrojanDownloader.Agent.th
↓ 1	2	Backdoor/SdBot.atp.Rootkit
New	3	TrojanDownloader.Agent.te
New	4	Backdoor/Huigezi.nc
↓ 1	5	Trojan/Script.Seeker

[표2] 2005년 11월 JiangMin 악성코드 TOP 5

'-' - 순위변동 없음, 'New' - 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

[표1]과 [표2]는 중국 로컬 백신 업체인 라이징(Rising)과 강민(JiangMin)의 11월 악성코드 TOP 5이다. 이 중 [표1] 라이징의 악성코드 TOP 5를 먼저 살펴보도록 하자. 라이징의 경우 1위를 차지한 그레이버드 트로이목마와 엘미르핵 트로이목마(V3 진단명, Win-Trojan/LmirHack)만 순위권에 이름을 올리고 있으며 나머지는 모두 이번 11월에 들어서 새로이 순위권에 진입한 트로이목마들이다. 1위는 여전히 그레이버드 트로이목마가 차지하고

있는데 이는 제작자의 금전적인 이해관계로 인해 제작자가 꾸준히 새로운 변형들을 제작 및 유포하고 있기 때문으로 알려져 있다. 특정 온라인 게임의 사용자 계정과 암호를 외부로 유출하는 엘미르핵 트로이목마는 지난 달 2위에서 3위로 한 계단 하락하였다. 이번 달 새로이 순위권에 진입한 트로이목마는 에이전트 트로이목마(V3 진단명, Win-Trojan/Agent)와 다운로더 트로이목마(V3 진단명, Win-Trojan/Downloader) 그리고 스타트페이지 트로이목마(V3 진단명, Win-Trojan/StartPage)가 있다. 에이전트 트로이목마와 다운로더 트로이목마는 기존 동향에서 기타 악성코드에 포함되어 그 감염 건이 많지는 않았으나 일정한 수치를 유지하고 있었다. 그러나 이번 11월에 들어서는 순위권에 진입 할 정도로 크게 증가한 것으로 분석되었다. 특히 스타트페이지 트로이목마는 작년부터 꾸준히 등장하고 있었으나 금년 10월을 기점으로 하여 지속적으로 수치가 증가하고 있었다.

[표2]는 강민의 악성코드 TOP 5이며 강민의 순위 역시 라이징과 유사하게 기존 트로이목마들의 순위는 하락하고 새로운 트로이목마들이 대거 순위권에 포함되어 있다. 그리고 기존 악성코드 중에서는 에스디봇 웜(V3 진단명, Win32/IRCBot.worm)과 Trojan/Script.Seeker만이 순위에 포함되어 있으나 모두 1계단 순위 하락을 보여주고 있다. 특히 그레이버드 트로이목마[1]가 강민의 악성코드 TOP 5에서 4위를 차지하고 있는 점으로 미루어 그레이버드 트로이목마가 한국 뿐 아니라 중국 내에서도 큰 위협인 것으로 보인다.

주간 악성코드 순위

순위	1주	2주	3주	4주
1	Backdoor.Gpigeon	Backdoor.Gpigeon	Backdoor.Gpigeon	Backdoor.Gpigeon
2	Trojan.PSW.QQRobber	Backdoor.Agent	Backdoor.Agent	Backdoor.Agent
3	Backdoor.Rbot	Trojan.PSW.LMir	Trojan.PSW.LMir	Trojan.PSW.LMir
4	Worm.Mail.Bagle	TrojanDownloader.Small	TrojanDownloader.Small	TrojanDownloader.Small
5	Trojan.PSW.LMir	Trojan.StartPage	Trojan.StartPage	Adware.Clicker.YNYW

[표3] 2005년 11월 라이징 주간 악성코드 순위

[1] 라이징 진단명은 Backdoor.Gpigeon로 강민의 진단명은 Backdoor/Huigezi.nc로 진단명이 다르나 동일한 그레이버드 트로이목마이다.

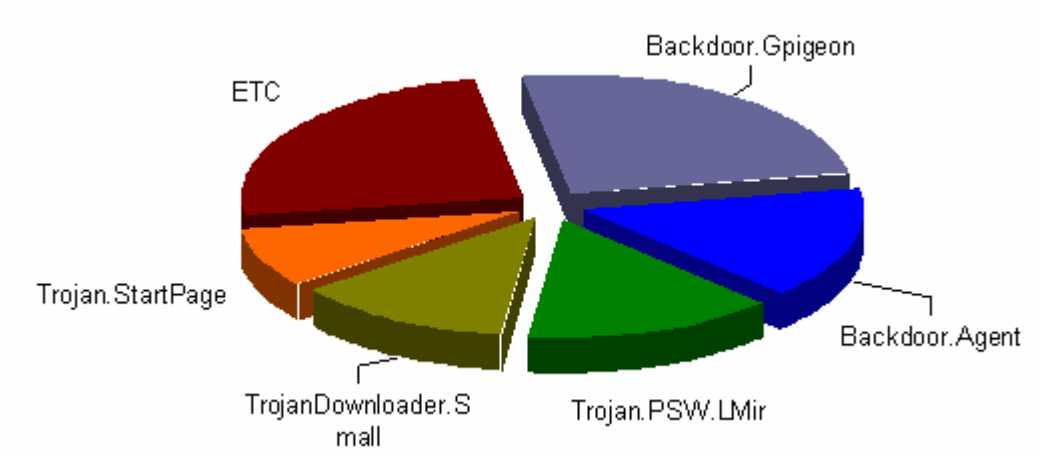
순위	1주	2주	3주	4주
1	Exploit.Applet.ActiveXComponent	Adware/Hmtool	TrojanDownloader.Agent.th	TrojanDownloader.Agent.th
2	Trojan/PSW.LMir.ant.Dll	TrojanDownloader.Agent.th	Adware/Hmtool	Adware/Hmtool
3	TrojanDownloader.Dyfuca.dp	Backdoor/SdBot.atp.Rootkit	Backdoor/SdBot.atp.Rootkit	Backdoor/SdBot.atp.Rootkit
4	TrojanDropper.Agent.uw	TrojanDownloader.Agent.te	Backdoor/Huigezi.nc	Backdoor/Huigezi.nc
5	Adware/ClearSearch.a	Backdoor/Huigezi.nc	TrojanDownloader.Agent.te	Exploit.MhtRedir

[표4] 2005년 11월 강민 주간 악성코드 순위

[표3]과 [표4]는 라이징과 강민의 주간 악성코드 순위 도표이다. 라이징의 경우에는 그레이버드 트로이목마는 4주 동안 순위 변화 없이 1위를 지키고 있었으며 에이전트 트로이목마는 11월 2주차에 급격히 증가하여 2위를 기록한 후 순위 변동이 없었다. 그러나 엘미르핵 트로이목마는 1주차에서 5위로 떨어졌으나 다시 3위로 순위 상승을 보였으며 다운로더 트로이목마 역시 2주차에서 4위를 기록한 후 순위 변동 없이 11월을 마감하였다. 특이한 점은 4주차에서 5위로 애드웨어인 Adware.Clicker.YNYW가 랭크 된 점이다. 자세한 통계에 반영되지 않았던 애드웨어가 같이 포함된 점으로 미루어 중국내에서도 애드웨어 형태의 감염 신고가 많은 것으로 추정된다. 다음 12월 통계에는 애드웨어의 통계가 어떠한 추세를 보일지 지켜볼 필요가 있다.

강민의 통계에서 그레이버드는 2주차에 이르러서야 5위를 기록하였으나 시간이 흐를수록 감염 신고가 증가한 것으로 분석된다. 그리고 다운로더 트로이목마의 순위는 다양한 변형들이 순위에 고르게 기록되며 새로운 트렌드의 변화를 유도하고 있는 것으로 추정된다.

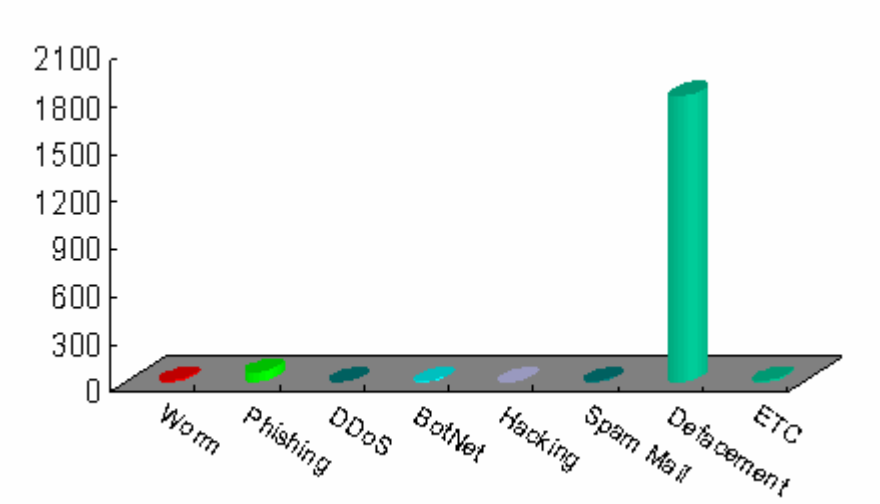
악성코드 분포



[그림1] 2005년 11월 라이징의 악성코드 분포

이번 11월 악성코드 분포에서는 지난 10월 41%를 차지하고 있던 그레이버드 트로이목마가 25%로 16%가량 감소한 것으로 분석되었다. 악성코드 TOP 5에서는 1위를 차지하고 있지만 한 달 동안의 전체 악성코드 분포에서는 오히려 감소한 형태를 나타내고 있어 다음 12월에 그 증감 여부를 지켜볼 필요가 있다. 그리고 지난 달 13%를 차지했던 엘미르핵 트로이목마는 악성코드 TOP 5에서는 4위로 떨어졌으나 분포 면에서는 1.4% 증가한 14.4%를 차지하고 있다. 그 외 새로이 순위권에 진입한 에이전트 트로이목마는 15.4%를 그리고 다운로더 트로이목마는 12.3%를 차지하고 있다.

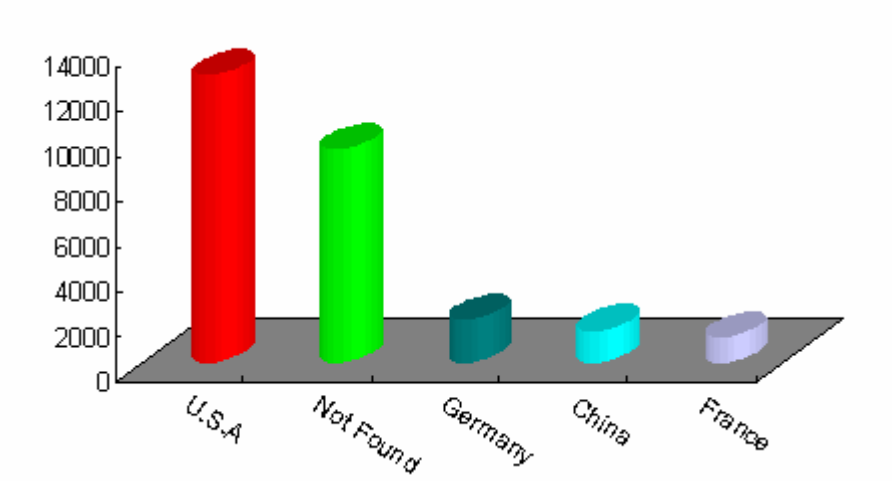
보안 사고



[그림2] 2005년 11월 CNCERT/CC의 보안사고 분포

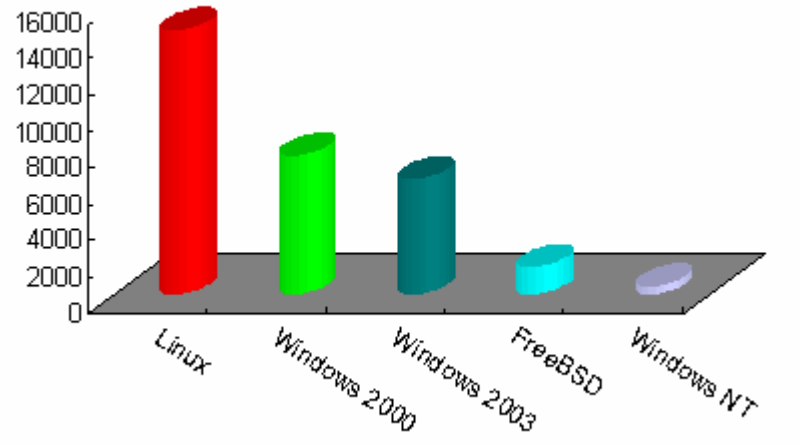
11월 중국 CNCERT/CC가 조사한 중국 내 보안사고는 [그림2]에서와 같이 홈페이지 변조사고가 가장 많은 수치를 기록하고 있다. 홈페이지 변조사고는 10월 845건에서 이번 11월 1803건으로 1000건 넘게 증가한 것으로 분석되고 있다. 이는 9월 511건과 비교하여 2달

사이 3배가 넘게 증가한 것으로 분석되고 있다. 그 외의 보안 사고는 커다란 변화 없이 기존과 유사한 수치를 기록하고 있다.



[그림3] 2005년 11월 CNCERT/CC의 중국 내 해킹 원격지 국가

[그림3]은 중국 CNCERT/CC가 집계한 중국으로 시도한 해킹의 원격지를 국가별로 분류한 것이다. 이번 11월 특이점은 지난 달 4위를 차지하였던 이탈리아가 순위권에서 빠지고 4위는 1,413건을 기록한 중국 내부가 차지하고 있다. 미국으로부터의 해킹 시도도 지난 달 9,255건에서 12,781건으로 3,000건 가량으로 크게 증가한 것으로 분석하고 있다. 이와 함께 해킹 시도지가 어디인지 구체적인 정보를 획득하지 못한 곳도 7,424건에서 9,524건으로 2,000건 가량 증가하여 전반적으로 해킹의 시도가 증가한 것으로 분석하고 있다.



[그림4] 2005년 11월 CNCERT/CC의 중국 내 해킹 대상 시스템

[그림4]은 중국 CNCERT/CC에서 집계한 중국 내 해킹 대상이 된 시스템의 운영체제별로 분류한 것이다. 리눅스 시스템이 가장 많은 해킹 대상 시스템이 되었으며 10월 소폭 감소가 있었으나 이번 11월에는 13,932건에서 14,553건으로 600건 가량 증가하였다. 리눅스 시스

템에 대한 공격이 증가한 반면 윈도우 2000 시스템에 대한 공격은 8,588건에서 7,665건으로 900건 가량이 감소하였다. 그리고 이와 함께 윈도우 2003 시스템 역시 소폭 감소한 것으로 분석되었다.

(3) 세계의 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

2004년 한해는 넷스카이 웜, 마이둠 웜, 베이글 웜의 3파전이었다면 2005년은 초반 넷스카이 웜의 독주에서 후반 다양한 마이톱 변형의 도전이 있었으며 몇몇 지역 보고에서는 넷스카이 웜의 기세를 꺾었다.

영국 소포스사의 11월 악성코드 동향[1]은 새로 등장한 소버 웜 변형이 등장과 동시에 전체 악성코드의 42.9%를 차지해 1위에 올랐으며 나머지 악성코드는 한 단계식 순위에서 밀렸다. 소버 웜 변형은 독일에서 제작된 것으로 추정되며 영어와 독일어의 메일 제목과 본문으로 전파된다. 또한 한글 윈도우 등 특정 윈도우에서는 오동작 해 아시아 지역에서는 피해가 적은 편이었다. 하지만, 11월 등장한 다수의 소버 웜 변형은 한글 윈도우에서도 실행되어 한국에서도 많은 보고가 있었다. 소버 웜의 확산은 FBI 혹은 CIA에서 보낸 것처럼 위장해 많은 사람들이 메일의 첨부 파일을 실행한 것으로 추정된다. 한가지 흥미로운 것은 소버 웜 변형 발생 전 독일 경찰에서 소버 웜 변형이 등장할 것을 미리 경고한 것이다. 정확하게 어떤 경로로 경찰에서 정보를 입수했는지 알 수 없지만 악성코드 제작자에 대한 수사가 있는 게 아닌가 하는 전망도 해본다.

러시아 캐스퍼스키 연구소의 11월 통계[2]에 의하면 마이톱 웜 변형이 1위를 차지하고 있으며 소버 웜은 13위에 그치고 있다. 다른 회사 통계에는 없는 둠봇(Doombot)과 러브게이트(LovGate) 변형이 2위와 5위를 차지하고 있다.

독일 아비라의 11월 보고[3]를 보면 대부분 독일에서 만들어진 넷스카이 웜과 소버 웜이 순위를 차지하고 있다. 아비라는 피싱에 대한 통계도 내고 있는데 이베이(Ebay)와 페이팔(PayPal)에 대한 피싱이 가장 많았다.

2005년도 이제 한달 정도 남은 시점에서 큰 변화가 없다면 마이톱 변형이 올해 최악의 악성코드로 기억될 것으로 보인다.

[1] http://www.sophos.com/pressoffice/news/articles/2005/11/toptennov05.html
[2] http://www.viruslist.com/en/analysis?pubid=175014602
[3] http://www.avira.com/en/news/november_virus_top_10.html

V. 이달의 ASEC 컬럼 - AVAR 2005 컨퍼런스를 다녀와서..

작성자: 장영준 연구원(zhang95@ahnlab.com)

국제적인 보안 컨퍼런스 중 하나로 인정받고 있는 AVAR(Association of Anti-virus Asia Reseachers, 아시아안티바이러스협회)는 지난 98년 6월 한국의 안철수(안철수연구소 이사회) 의장, 일본의 세이지 무라카미(JCSR-Jpan Computer Security Research Center) 회장 등이 아시아 지역 안티 바이러스 분야 협력 증진을 위해 창립한 비영리 조직이다. 매년 아시아 각국을 순회하며 컨퍼런스를 개최하고 있으며, 이번 AVAR 컨퍼런스는 8회째로 바이러스 블러틴(Virus Bulletin) 컨퍼런스 등에 이어 세계적인 보안 컨퍼런스로 평가받고 있다.

이번 AVAR 2005 컨퍼런스는 작년 일본에 이어 올해는 11월 17일과 18일 양일간 중국 천진에서 개최되었다. 그리고 중국의 보안 전문가들 뿐 아니라 전세계의 보안 전문가들이 대거 참여하여 높은 관심을 보였었다.

[그림1] AVAR 2005는 중국 천진에서 11월 17일, 18일 양일간 개최되었다.

이번 AVAR 2005 컨퍼런스는 보안 제품 또는 보안 사고와 관련한 새로운 기술적 내용들을 다루기 보다는 현재 전세계 각국에서 발생하고 있는 보안사고와 관련하여 전반적인 동향 및 추이 변화에 대한 내용을 다룸으로써 향후 발생할 수 있는 새로운 보안 사고들에 대해서 많은 의견들이 발표되었다.

이번 컨퍼런스에서 안철수연구소는 황규범 선임연구원과 정덕영 주임연구원이 둘째 날인 18일 오후에 한국의 모바일 환경에 존재하는 취약점과 이를 노리는 위협을 소개하고, 예상되는 공격과 방어 방법을 설명하였다. 이번 발표에서는 멀티미디어 데이터 이용이 증가함에 따라 용량이 큰 데이터를 전송할 때 많은 사용자가 경제적인 이유로 무선 환경이 아닌 PC를 경유해 전송하는 것이 일반적이다. 또한 핸드폰 사용자들은 자신만의 데이터를 업로드하기 위해

다양한 툴을 사용하는데, 이러한 툴을 잘못 사용할 경우 핸드폰의 시스템 파일이 삭제돼 서비스가 불가능해지거나 핸드폰에 너무 많은 데이터를 넣어 오작동하는 경우가 발생하고 있는 것을 데모 동영상과 함께 보여주었었다.

안철수연구소의 모바일 보안 관련 논문 외에도 악성코드 관련한 논문들이 많이 발표가 되었으나 이 중에서도 다음의 논문들이 컨퍼런스 참가자들의 높은 관심을 끌었었다.

AVAR 2005 컨퍼런스 첫째날

첫째날인 17일에는 중국의 많은 언론 기자들이 참여하여 중국 내에서 AVAR 2005에 대한 높은 관심을 증명하였으며 다음 논문들이 많은 관심을 받았었다.

마이크로소프트(Microsoft) 레드몬드 본사에서 보안 제품 개발을 담당하고 있는 제이슨 그람(Jason Garms)이 발표한 'An Accurate Understanding Of On-Going Malware Prevalence'가 돋보였다. 새로운 악성코드의 확산이 발견되고 이를 진단 및 치료할 수 있는 새로운 엔진이 배포되었다고 하여 기존에 발견된 악성코드들이 네트워크 내에서 완전히 사라지지 않았음을 마이크로소프트 특유의 자세한 데이터와 통계를 통해서 보여주었다. 이 통계는 마이크로소프트가 윈도우 업데이트(Windows Update)를 통해서 개인 및 기업의 윈도우 운영체제 사용자들에게 무료로 배포하고 있는 악성코드 제거 도구의 통계에 기반한 것이었다. 이는 윈도우 운영체제 사용자들이 해당 악성코드 제거 도구를 이용하여 시스템을 치료한 정보를 마이크로소프트로 전송하여 이를 종합하여 나타낸 수치였다. 제이슨의 논문을 통해서 기존의 새로운 악성코드에 대한 대응도 중요하지만 기존에 확산되어 있는 악성코드의 진단 및 치료 역시 이에 못지 않게 중요하다는 것을 잘 보여주고 있었다.

그리고 노드32(NOD32)라는 백신 제품을 개발하고 있는 슬로바키아 업체인 이셋(ESET)에서 보여준 스렛센스 닷넷(ThreatSense.NET) 또한 흥미로웠다. 스렛센스 닷넷(ThreatSense.NET)은 알려지지 않은 악성코드를 휴리스틱 진단을 통해 새로운 악성코드를 수집하는 것에 주 목적을 두고 있었다. 노드32(NOD32) 제품에 하나의 새로운 기능으로 제공되고 있는 이 스레드씬 닷넷은 해당 백신 제품이 설치된 개인 또는 기업 사용자들의 시스템에서 기존에 알려지지 않은 새로운 악성코드가 탐지 되는 경우, 이셋(ESET) 본사로 악성코드 감염에 대한 통계 정보를 수집하여 전송하는 기능과 새로운 악성코드 발견 시 해당 악성코드를 수집하여 전송하는 기능을 포함하고 있다. 이렇게 개인 또는 기업 사용자들의 시스템을 통해서 수집된 악성코드 감염 정보를 통하여 이셋(ESET)에서는 새로운 악성코드를 조기에 탐지하는 조기 탐지 시스템(Early Warning System)으로 활용하고 있다. 이러한 노드32(NOD32) 제품을 통하여 수집된 정보는 곧 전세계적으로 확산되고 있는 악성코드의 그 발견지와 경로를 추적하는데 사용되고 있다. 특히 새로운 악성코드가 발견되었을 때 수치상의 그래프 뿐 만이 아니라 세계 지도 상에 실시간으로 수집 통계를 동심원으로 표시하며 확산 상황을 실시간으로 보여준 동영상은 특히나 인상적이었다.

헝가리에 위치한 백신 업체인 바이러스버스터(VirusBuster)는 네트워크로 전파되는 웜의 수집과 관련하여 웜 트랩(Worm Trap)이라는 흥미로운 논문을 발표하였다. 기존에 허니팟(HoneyPot) 또는 허니넷(HoneyNet)으로 알려져 있는 시스템을 구축하여 새로운 악성코드 수집 임무를 수행하며 급격한 증가를 보이는 새로운 악성 코드 수집의 통로로 활용되고 있다고 한다. 이 새로운 악성코드 수집 시스템이 모니터링 하는 사항들은 포트, 이메일, 네트워크 트래픽, IRC, P2P, 유즈넷 등 다양한 경로를 모두 모니터링하고 있어 새로운 감염 경로와 감염 기법을 보이는 새로운 악성코드를 조기에 탐지하고 수집할 수 있도록 하고 있다.

이제는 너무나도 유명해져 버린 러시아 캐스퍼스키 랩의 유진 캐스퍼스키는 현재의 악성코드는 기존의 악성코드와 달리 공격 대상을 무작위로 지정하는 것이 아니라 1,000대 정도만 공격하여 해당 시스템들을 완벽하게 장악한다는 악성코드의 새로운 변화에 대하여 발표하였다. 해당 논문은 현재의 악성코드, 그 중에서도 악성 아이알씨봇의 공격형태에 대해서 너무나도 정확하게 표현하고 있었다. 단순하게 수치상으로 1,000대이지만 이 1,000의 시스템이 하나의 봇넷(BotNet)을 형성하고 이를 다시 확장하여 1,000대의 시스템으로 늘어나게 되면 결국 소규모 봇넷들이 다시 대형 봇넷을 이루게 되고, 시스템 장악에 대해서 이것만큼 효과적인 방법이 없다고 보고 있었다. 이와 함께 금전적인 이해 관계를 배경으로 하여 전 세계적인 확산이 아니라 특정 지역 또는 특정 국가에 한정된 국지적으로만 관찰 가능한 스파이웨어와 트로이목마 들을 새로운 보안 위협의 트렌드로 보고 있었다

이로써 컨퍼런스의 첫째날이 마무리되고 AVAR 협회 측에서 주최한 저녁 만찬이 준비 되어 있었다. 저녁 만찬에는 AVAR 2005 컨퍼런스 개최에 많은 도움을 주었던 업체들에 감사패를 수행하는 등 다채로운 저녁 행사들이 준비되었다. 저녁 만찬에는 중국이라는 국가적 특색을 살린 중국 전통 음악단이 등장하여 중국 전통악기를 통한 음악들을 들려주어 중국적인 특색을 느낄 수가 있었다.

[그림2] AVAR 저녁 만찬에서 중국 전통음악을 들을 수 있었다.

AVAR 2005 컨퍼런스 둘째날

둘째날인 18일에는 첫째날 보다 인원이 많이 줄었으나 보안 업체 관계자들 대부분이 참석하였다. 중국 대학생 등 보안 분야에 관심이 많은 학생들도 눈에 띄어 중국 내에서 정보 보안이라는 분야의 관심도를 간접적으로나마 느낄 수 있었다. 둘째 날에는 다음의 논문들이 많은 관심을 끌었었다.

시만텍 스렛 리포트(Threat Report)의 편집장은 악성코드와 스파이웨어의 차이와 새로운 위협들에 대하여 다루었다. 특히 스파이웨어 제작사와의 충돌에 대해 언급하였는데 한국에서 발생하는 스파이웨어 업체와 비슷한 문제를 가지고 있었다. 하지만 시만텍의 입장은 근본적으로 시만텍 제품을 사용하는 개인 및 기업 고객들의 요구사항으로 대응이 필요하다는 것을 강조하고 있었다. 이와 함께 개인 및 기업 고객들로부터 접수되는 스파이웨어에 대한 처리 프로세스에 대해서도 언급하였는데 위험도 평가에서 성능, 프라이버시, 삭제, 은폐 등 스파이웨어가 가지고 있는 위협적인 요소들을 다양한 기준으로 분류하여 진단 및 치료 엔진에 반영하고 있었다. 시장 전망에 대하여서는 안티 바이러스 업체가 안티 스파이웨어 업체를 추월하고 있으며 안티 스파이웨어 업체들이 안티 바이러스 엔진을 탑재하거나 안티 바이러스 업체로 인수 합병될 것이라고 조심스러운 예측을 내놓았었다. 또, 안티 스파이웨어 제품에 대한 표준화된 평가 지표가 확립된다면 전문성이 떨어지는 개인 리뷰자들이 사라지고 안티 스

파이웨어 제품과 관련한 신뢰할만한 인증이 등장하게 될 것이라고 전망하고 있었다.

중국 반대편에 위치한 시만텍 아일랜드 보안센터에서 날아온 캔디드 우드셋의 온라인 뱅킹과 관련된 논문은 매우 일목요연하고 쉽게 잘 정리되어 있었다. 논문의 결론은 온라인 뱅킹 시에는 하드웨어 방식의 PKI가 안전하며 이러한 방식을 독일에서는 6년째 벌써 사용하고 있다고 한다. 그리고 피싱과 같은 보안 사고 발생 당시 보안 업체의 대응도 중요하지만 보안 사고 발생 이전에 무형의 또는 유형의 고객들의 자산을 이로부터 보호해주는 것 또한 중요하다는 것을 강조한 논문이었다.

이번 AVAR 컨퍼런스의 마지막 시간으로 보안 전문가들의 열띤 패널 토론이 이어졌었다. 패널 토론에서 포티넷의 기욤(Guillaume)은 루트킷(RootKit)의 미래에 대해 이야기하다 골든 해커 디펜더의 안티 바이러스 엔진 감지 기능과 관련하여 맥아피의 드미트리와 논쟁했었다. 특히 해커 디펜더에 안티 바이러스 제품의 엔진에 대한 탐지 기능이 추가가 되면 이에 대해서 백신 업체에서는 어떻게 대처할 것이냐라는 날카로운 질문을 하였었다.

[그림3] AVAR 멤버들이 취재 중인 기자들을 위해 포즈를 취하고 있다.

이번 AVAR 2005 컨퍼런스는 악성코드와 관련한 기술적인 변화 등에 대해 높은 기술적인 분석 논문은 발표되지 않았었다. 하지만 악성코드의 변화 추이 그리고 스파이웨어의 위협과

같은 새로운 보안 위협에 대한 논문들이 발표되어 시대적인 변화와 악성코드의 추이 변화에 대해 다룬 논문들이 많았다. 이러한 논문들을 통해 안철수연구소를 포함한 전세계 모든 보안 업체들이 이러한 변화의 조류에 뒤쳐지 않기 위해 많은 노력을 기울이고 있으며 더욱더 안전한 컴퓨팅 환경을 만들기 위해서 많은 노력을 기울이고 있는 모습들을 엿 볼 수 있었다. 내년 AVAR 2006은 뉴질랜드에서 개최 될 예정이며 내년 역시 새로운 악성코드의 추이 변화와 기술적인 변화를 따르는 뛰어난 논문들이 많이 발표되기를 기대해본다.