ASEC Report 7월

® ASEC Report

2004. 8

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

지속적인 넷스카이 웜의 피해와 IRCBot 변형 발견…

2004년 7월에 피해신고 된 악성코드 Top 10 중 7개가 넷스카이 웜(변형포함)에 의한 것으로, 여전히 넷스카이 웜에 의한 피해신고가 가장 많았다. 넷스카이 웜에 의한 피해가 가장 많았던 것은 한국 뿐 아니라 일본, 중국도 마찬가지였다. 또한 사용자에게서 피해신고 된 악성코드의 수는 934건으로, 이는 약 1,000개의 악성코드가 국내에서 활동하고 있다는 것을 의미하며 이 수치 또한 역대 최고의 수치를 기록하고 있다.

2004년 7월에 발견된 신종(변형포함) 악성코드는 여전히 악성 IRCBot 이 가장 많았으며, 7월에 발견된 악성코드 중 주목할 만한 것으로는 WinCE 환경에서 감염활동을 하는 WinCE/Dust 가 있다. 이는 WinCE 환경에서 활동하는 바이러스가 가능하다는 것을 보여주기 위해 제작된 Concept 바이러스로, 사용자에게서 직접 피해신고가 있었던 것은 아니지만, 점점 악성코드가 제작되는 운영체계 플랫폼이 확대되고 있다는 것에 그 의미가 있다 하겠다.

7월에 마이크로소프트사에서 발표한 정기보안패치 7가지 중에는 윈도우 작업 스케쥴러 취약점(MS04-022)와 HTML 도움말 취약점(MS04-023)이 악성코드에서 이용될 가능성이 매우 높으므로, 이에 대한 패치적용 또한 매우 중요하다.

이번 호 테크니컬 컬럼에서는 자동 이메일 추출 수집기를 이용하여 수집된 메일주소로 스팸메일이 수신되는 것에 대한 대응방법과 기업의 네트워크 트래픽 과다 현상 발생시 네트워크 상의 유해 트래픽을 탐지하고 판단할수 있는 방법에 대해 알아보았다.

I. 7월 악성코드 피해 Top 10

작성자 : 차민석 연구원(jackycha@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	5488	36.2%
2	-	Win32/Netsky.worm.17424	1353	8.9%
3	-	Win32/Dumaru.worm.9234	1270	8.4%
4	-	Win32/Netsky.worm.28008	1050	6.9%
5	-	Win32/Netsky.worm.17920	1002	6.6%
6	3↑	Win32/Bagle.worm.Z	526	3.5%
7	1↑	Win32/Netsky.worm.22016	524	3.5%
8	1↓	Win32/Netsky.worm.25352	417	2.8%
9	3↓	Win32/Sasser.worm.15872	414	2.7%
10	New	Win32/Netsky.worm.16896.B	260	1.7
		기타	2836	18.7%
합 계			15,140	100

[표1] 2004년 7월 악성코드 피해 Top 10

7월 악성코드 피해 동향

바이러스, 웜, 트로이목마 등의 악성코드 피해 Top 10은 몇 달 동안 비슷한 현황을 보여 주고 있다. 여전히 Win32/Netsky.worm.29568(이하 넷스카이.29568 웜)이 가장 많은 보고 및 신고건수를 차지하고 있다. 다만 집계 방식이 사용자들이 실제 감염되지 않아도 메일 등을 통해 웜 메일을 접한 형태도 포함되므로 상대적으로 대량의 메일을 보내는 메일로 전파되는 웜에 의한 피해순위가 높을 수 밖에 없다.

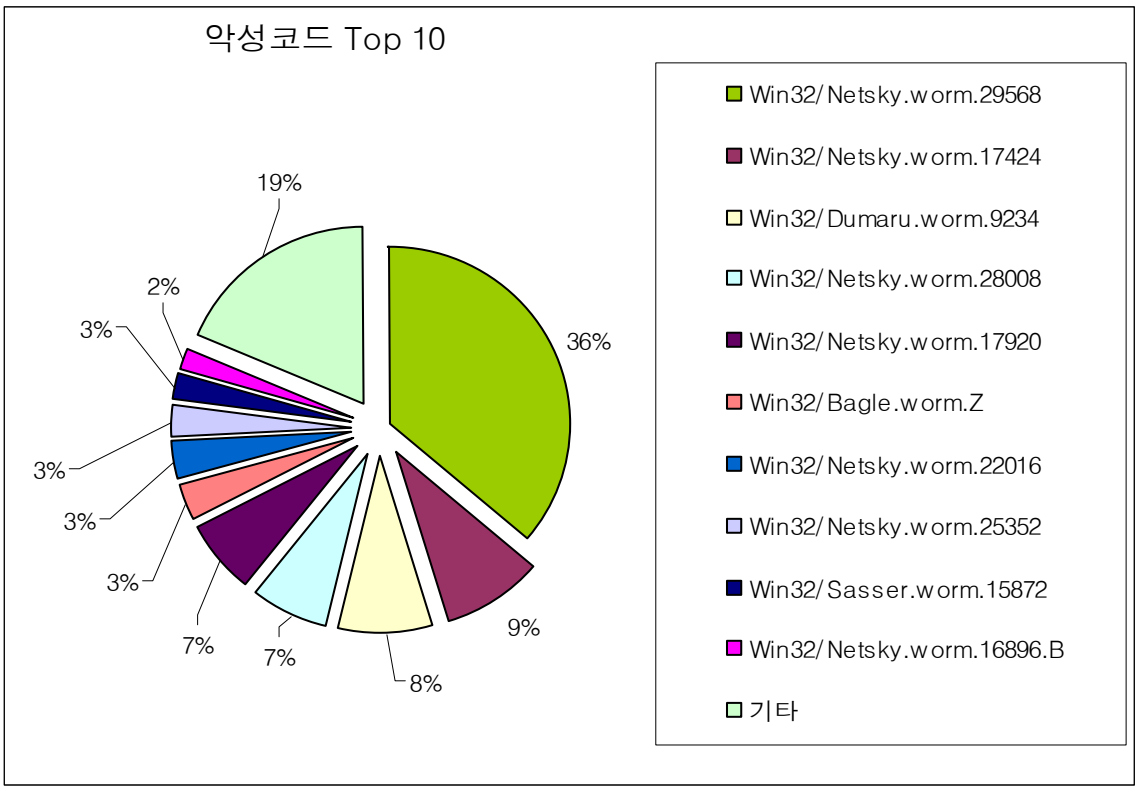
지난달에 이어 7월에도 1위를 차지만 넷스카이.29568 웜의 특징은 다음과 같다.

- 메일 및 공유폴더로 전파 (공유폴더는 P2P 응용 프로그램의 공유폴더)
- 메일로 전파시 취약점 사용 (부정확한 MIME 헤더로 인한 첨부파일 자동실행 가능)
- 다양한 확장자에서 메일주소를 수집 (A:₩ ~ Z:₩ 드라이브 내에서)
- 다양한 첨부파일명과 메일 제목, 본문 등을 가지고 있음
- 특정 악성코드의 실행을 중지

3월 중순경에 처음 발견된 이 웜은 초기 확산시 상당히 많은 시스템에 감염되었고 현재도 감염된 시스템들에서 대량의 메일을 발송하고 있는 것으로 보인다.

넷스카이 웜 제작자는 Win32/Sasser.worm.15872(이하 새서 웜)도 만들었는데, 5월 1일 발견된 이 웜은 3개월이 지난 지금까지 꾸준히 피해를 많이 입히고 있다. 즉, 한 악성코드 제작자에 의한 제작된 웜에 의한 피해가 매우 높으며, 이는 국내뿐 아니라 외국에서도 동일하다.[1]

7월의 악성코드 피해 Top10을 도표로 나타내면 [그림1]과 같다

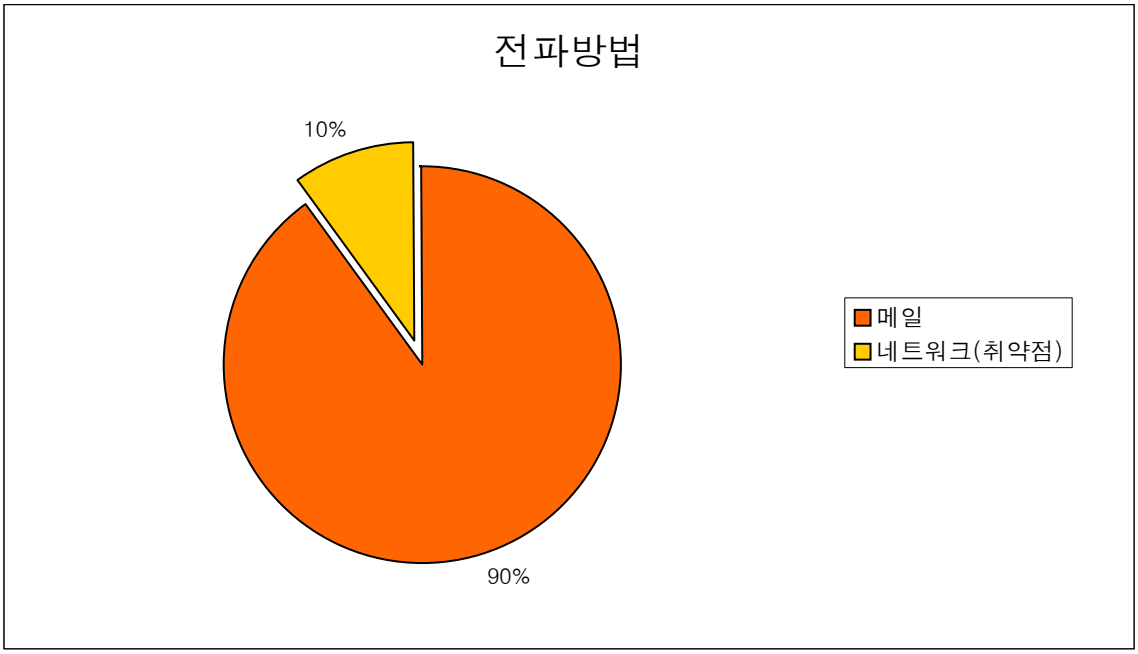


[그림1] 2004년 7월 악성코드 피해 Top 10

7월 악성코드 Top 10 전파방법별 현황

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

[1] ZDNet Korea, 상반기 바이러스 피해 70% 1명이 벌인 일
http://www.zdnet.co.kr/keyword/virus/0,39025204,39129403,00.htm 참조

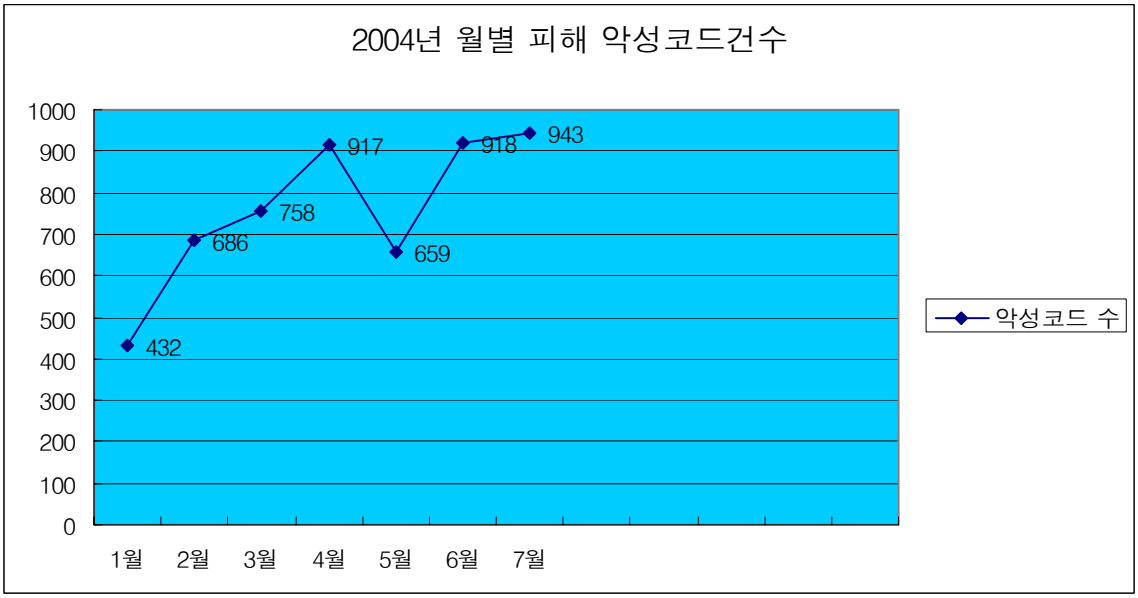


[그림2] 악성코드 Top 10의 전파방법별 현황

지난 달과 순위 변화는 거의 없어, 보안취약점을 이용해 네트워크로 전파되는 새서 웜을 제외하고는 모두 메일로 전파되는 웜들이다.

월별 피해신고 악성코드 건수 현황

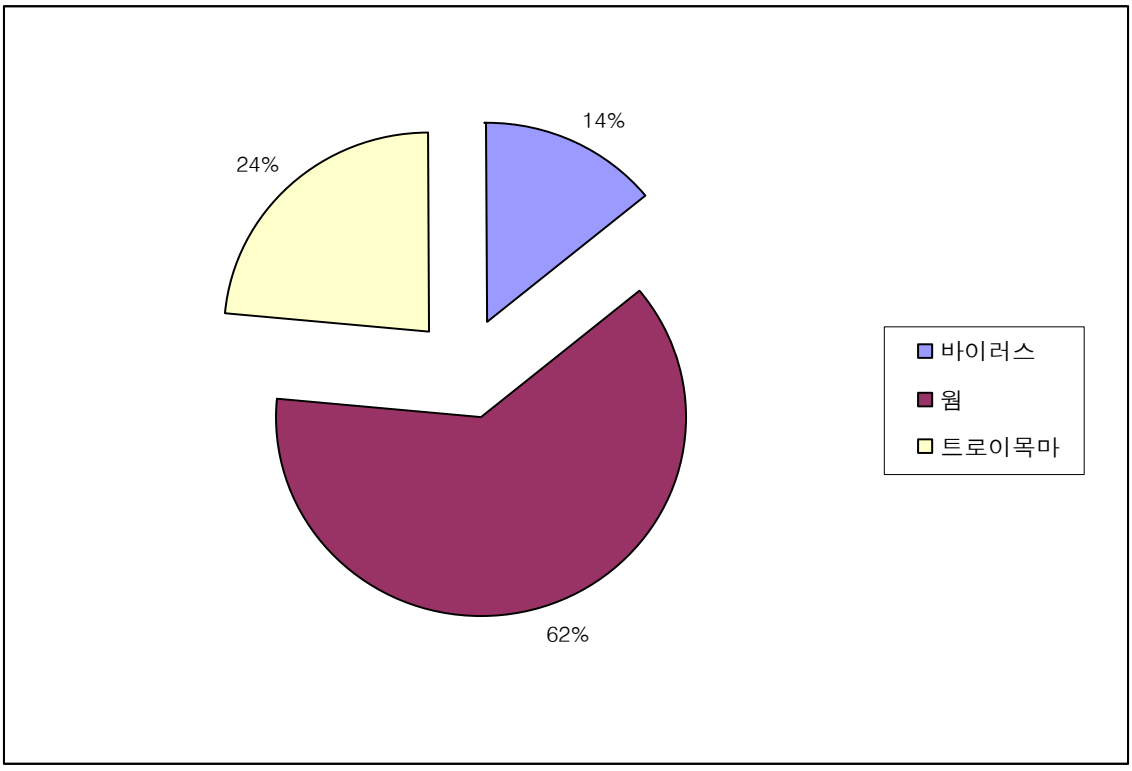
7월에 피해 신고된 악성 코드는 943개이다. 즉, 국내에 활동이 보고된 악성코드 수가 최소 1000개 정도는 된다는 것을 의미한다. 수치적으로도 2004년 최대 수치이다. 이중 대부분이 악성 IRCBot 류가 차지하고 있다. 이와 같은 결과는 상반기와 마찬가지로 7월에도 많은 종류의 악성 IRCBot이 발견되고 활동하기 있기 때문이다([그림3]참조).



[그림3] 2004년 월별 피해신고 악성코드 수

주요 악성코드 현황

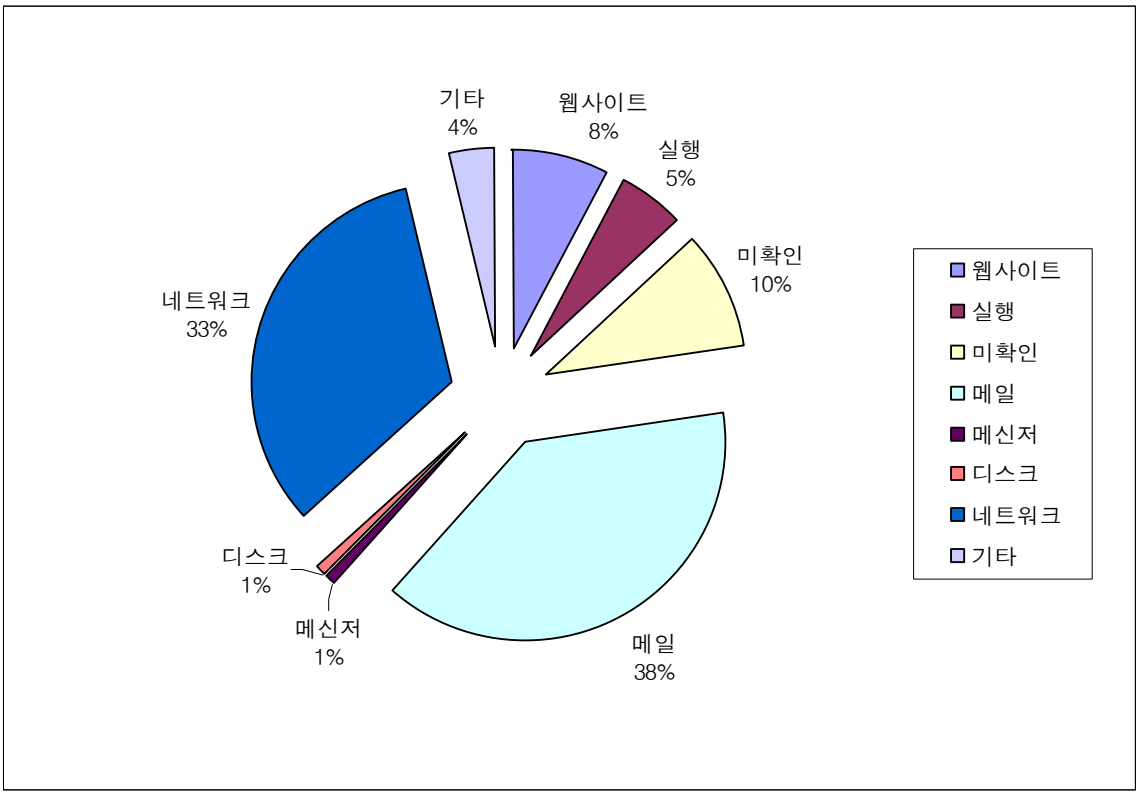
7월에 피해가 접수된 악성코드 중 3건 이상의 문의가 들어온 악성코드의 종류는 [그림4]와 같다.



[그림4] 3건 이상 피해 신고된 악성코드 종류별 현황

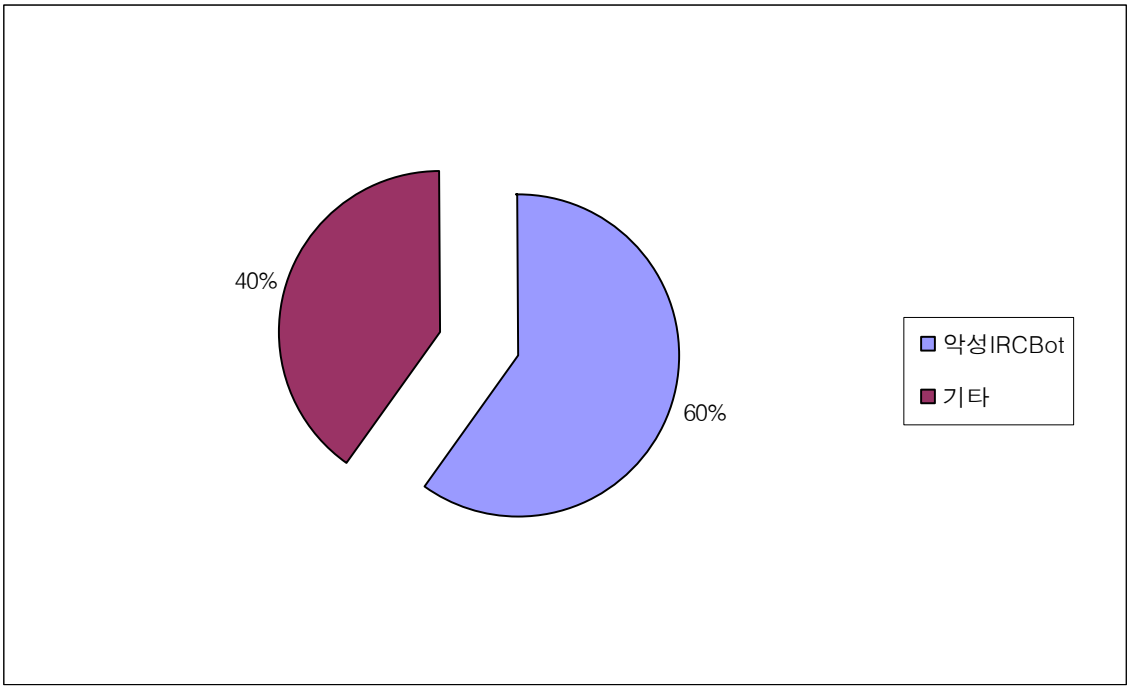
웜이 62%(71개)로 가장 많았으며 트로이목마 24%(27개), 바이러스 14%(16개)이다. 여전히 웜과 트로이목마가 대세이며 바이러스는 구형의 바이러스가 계속 활동하고 있다.

3건 이상 보고된 악성 코드의 전파 방법별 현황은 [그림5]와 같다. 메일(38%)과 네트워크(33%)를 통한 전파가 71%로 대부분을 차지하고 있다. 현재 피해를 입히고 있는 대부분의 악성코드는 메일과 네트워크로 전파됨을 알 수 있다.



[그림5] 3건 이상 보고된 악성 코드의 전파 방법별 현황

7월의 악성코드 피해 동향을 총평 해 본다면 2004년 상반기 내내 많이 등장한 악성 IRCBot류의 변형의 활동이 왕성했다. [그림6]을 보면 7월의 피해 악성 코드 종류 중 60%가 악성 IRCBot류에 의한 것임을 알 수 있다.



[그림6] 2004년 7월 총 피해 중 악성 IRCBot 현황

악성 IRCBot류는 전체적으로 피해를 주는 경우는 드물지만 특정 회사 단위로 피해를 주고 있다. 7월에는 전통적인 넷스카이 웜과 새서 웜등의 피해 속에 기업이나 학교 등을 대상으로 악성 IRCBot 류가 끊임없이 괴롭혔음을 알 수 있다.

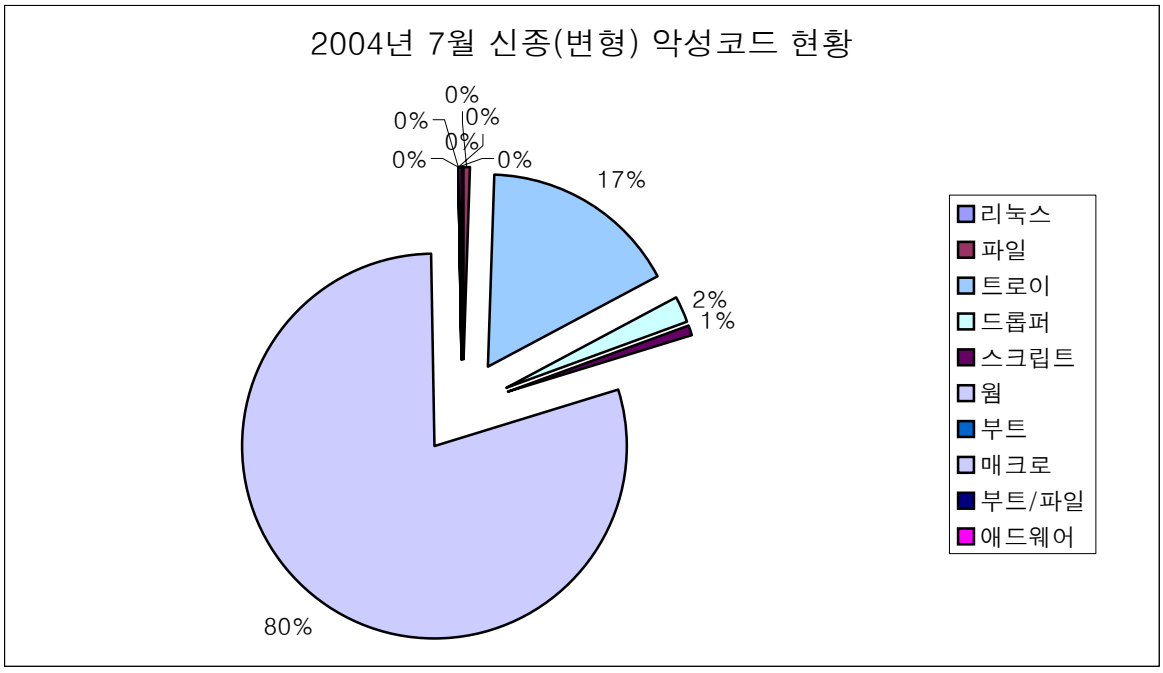
II. 7월 국내 신종 악성코드 발견 동향

작성자 : 정진성 연구원(jsjung@ahnlab.com)

7월 한달 동안 접수된 신종 (변형) 악성코드의 건수는 [표1], [그림1]과 같다.

리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	애드웨어	합계
0	2	80	10	4	379	0	0	0	1	476

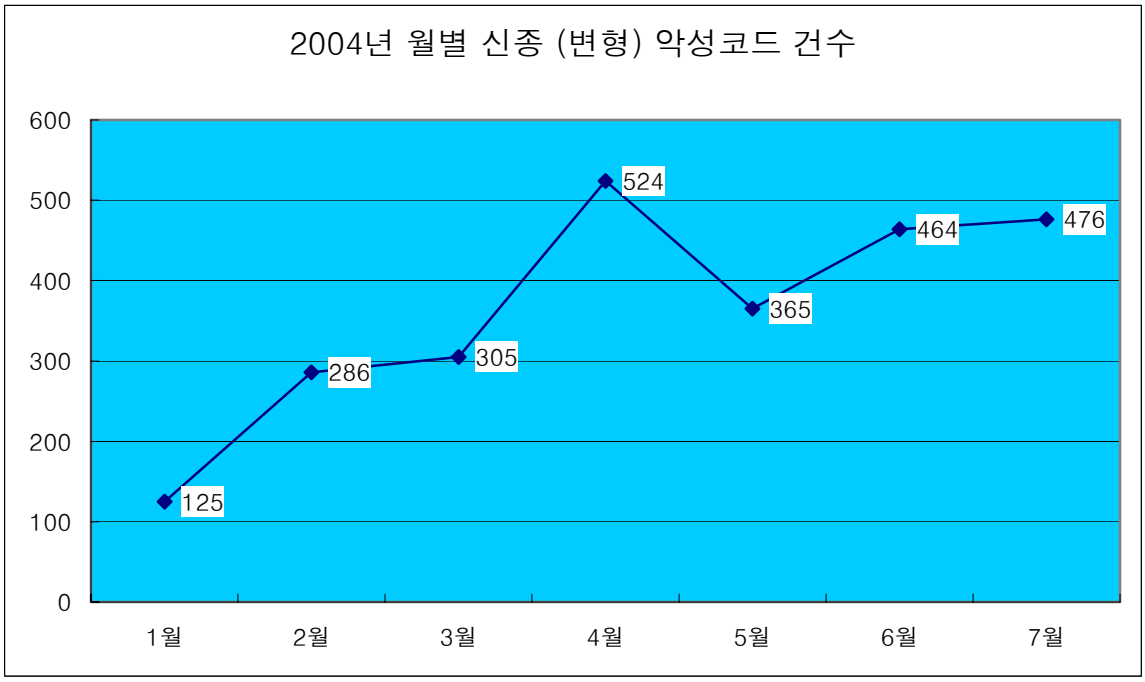
[표1] 2004년 7월 유형별 신종 (변형) 악성코드 발견현황



[그림1] 2004년 7월 신종 악성코드 발견현황

7월 신종 악성코드 동향

7월에 발견된 신종(변형 포함) 악성코드는 지난달 수치보다 10여건 증가하여, 7월은 올해 들어 두 번째로 많은 악성코드가 발견된 달로 기록되었다. 또한 이는 지난해 동월과 비교했을 때는 무려 600%이상 증가한 수치이기도 하다. 지난해 경우 발견된 대부분의 악성코드는 악성 IRCBot 트로이목마이거나 전형적인 백도어류가 대부분이었다. 이번 달은 지난달과 동일하게 악성 IRCBot 웜이 많았다. 또한 이번 달에는 Win32/LovGate.worm(이하 러브게이트 웜) 변형이 다수 발견되어 극성을 부렸다.



[그림2] 2004년 월별 신종(변형) 악성코드 발견 현황

변형이 다수 발견되었던 러브게이트 웜처럼 7월에 발견된 Mass Mailer들은 변형까지 포함하여 모두 23개가 발견, 보고되었다.

이번 달에 새로이 발견, 보고된 악성코드 중 이슈가 있었던 것은 다음과 같다.

▶ WinCE/Dust

윈도우 CE 환경에서 최초로 동작하는 바이러스이다. 컨셉 개념으로 제작되어진 이 바이러스는 일반 사용자에게 발견되지 않았고 바이러스 제작자가 안티 바이러스 업체에 보내지면서 알려지게 되었다. 이 바이러스는 윈도우 CE에서 동작되는 PE 형식의 실행파일(*.exe)을 감염시킨다. 실행하면 메시지 박스를 활성화하여 감염시키려는 의도를 보여주고 실행된 폴더 내 윈도우 CE의 PE 파일을 찾아서 파일의 뒷부분에 감염되는 후위형 형태를 가지고 있다. 이 바이러스는 윈도우 CE 환경에서만 동작되며 일반적으로 사용되는 윈도우 9x/NT/2000/XP환경에서는 윈도우 CE의 PE 파일의 머신 정보가 달라서 동작되지 않는다.

올해 들어 특정 OS의 핸드폰에서 동작하는 악성코드의 발견을 시작으로 x86 이외의 기기들에서 활동하는 악성코드가 벌써 두 번째 발견되었다. 이제 더 이상 이와 같은 기기들이 악성코드로부터 안전하지 못하다는 단편적인 모습을 보여주는 것이다. 또한 안티 바이러스 업체에서도 이미 이와 관련된 기술력을 확보했거나 또는 확보 중에 있으므로 끊임없는 연구/개발을 토대로 이와 같은 악성코드에 대응해 갈 수 있는 기술력을 갖춰야 할 것이다.

▶ Win32/Bagle.worm.AA

한 동안 제작되어지지 않았던 Win32/Bagle.worm(이하 베이글 웜)의 새로운 변형이 제작자가 웜 소스를 공개 한 채 유포하였다. 이전에도 Win32/MyDoom.worm(이하 마이둠 웜) 관련 악성코드의 소스가 공개되어 다른 변형이 제작되었었다. 이와 같이 악성메일에 소스가 첨부된 채로 발송되므로, 원래의 웜 제작자가 아닌 다른 누군가에 의해 소스를 이용한 변형이 제작될 가능성이 매우 높았으며, 우려한대로 소스를 이용한 변형들이 발견, 보고되었다. 베이글 제작자가 베이글 웜 소스를 공개한 이유에 대해서는 추적을 피하기 위한 것으로 보고 있기도 하다.

▶ Win32/LovGate.worm. 변형

작년 봄에 발견되어 현재까지도 계속적인 변형이 제작되고 있는 Win32/LovGate.worm (이하 러브게이트 웜)은 변형이 거듭되면서 제작기법도 향상되고 있다. 이번 달에는 무려 12개의 변형이 발견, 보고 되었다. 특히 이번에 발견된 변형 중 하나는 윈도우 실행파일을 감염시키는 증상이 있다. 감염형태는 정상파일을 가운데 두고 파일의 앞 부분에는 러브게이트의 트로이목마를, 정상파일의 뒤 부분에는 러브게이트 웜을 감염시키는 형태이다. 또한 러브게이트는 제작기법이 발전하면서 자신이 생성하는 트로이목마 모듈을 다른 정상 프로세스에 Injection하는 기법을 초기에 사용하였다. 하지만 올해부터 이 트로이목마를 다른 프로세스의 Thread(이하 쓰레드)로 동작하도록 하는 기법을 사용하여 진단 및 치료를 어렵게 하였다.

▶ Win-Trojan/Kobar

Kobar(이하 코바)라고 명명된 이 트로이목마는 국내 사용자로부터 안철수연구소가 처음 발견하였다. 이 트로이목마는 현재까지 2개의 변형이 발견되었다. 이 트로이목마도 자신의 쓰레드를 다른 정상 프로세스의 쓰레드로 Injection하여 동작한다. 따라서 트로이목마의 감염여부를 눈치채기 어렵다. 이 트로이목마는 특정 호스트에 연결되어 *.CGI 파일의 내용을 실행하도록 되어 있다. 분석 당시 이미 해당 호스트가 정상적으로 동작하지 않았는데 이 트로이목마는 감염된 시스템의 정보(윈도우 버전, MAC 주소, 컴퓨터 이름, IP 등)를 보내고 특정 파일을 내려 받아 실행하는 것으로 추정되었다.

▶ Win32/MyDoom.worm.M

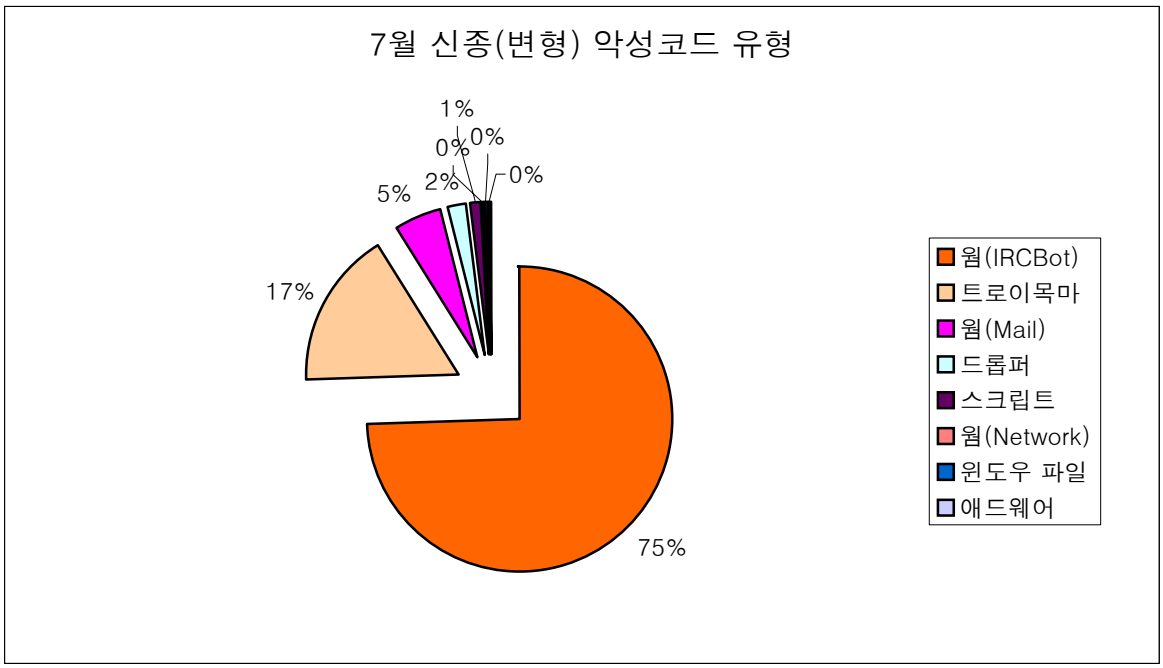
Win32/MyDoom.worm(이하 마이둠 웜) 역시 올 초부터 현재 지속적으로 변형이 제작 및 유포되고 있다. 특히 이 웜은 웜이 열어둔 포트로 다른 악성코드가 감염되는 증상도 가지고 있다. 이번 달에 발견된 M형은 지난 변형 이후 꽤 오랜 기간이 흐른 후 발견되었다. 이번에 발견된 변형의 특징은 자신을 전파시킬 목적으로 수집되는 메일주소의 수집방법을 변화하였다는 것이다. 기존의 Mass Mailer들은 단지 로컬 드라이브나 네트워크 드라이브 내에서 메일 주소를 수집한 반면, 이번 마이둠.M 웜은 수집된 메일주소에서 도메인(ex, @도메인명.com)만을 추출하여 잘 알려진 검색엔진을 통해 메일 주소를 수집하는 방법을 사용하여

이슈가 되었다. 이의 Side Effect로 검색엔진에 대한 트래픽 부하를 가져오는 결과를 가져오기도 하였다.

또한 웜이 Drop하는 트로이목마는 다른 악성코드인 Win-Trojan/Zindos(이하 진도스)를 설치하도록 유도한다. 이 진도스는 DDoS 공격 툴로써 MS사 홈페이지를 공격하도록 되어 있다. 공격방식은 www.microsoft.com에 대하여 Win32 API 인 URLDownloadToCacheFileA를 이용하여 접속을 시도한다. 이때 사용되는 캐쉬파일은 인터넷 익스플로어가 사용하는 Index.dat 파일이다. 즉, 트로이목마의 쓰레드 중 하나가 이와 같이 해당 캐쉬파일에 대하여 무한히 읽는 것을 반복함으로써 해당 사이트에 접속하는 효과를 가져오도록 한다.

유형별 신종(변형) 악성코드 현황

다음은 7월 발견된 신종 (변형) 악성코드의 유형별 현황이다.

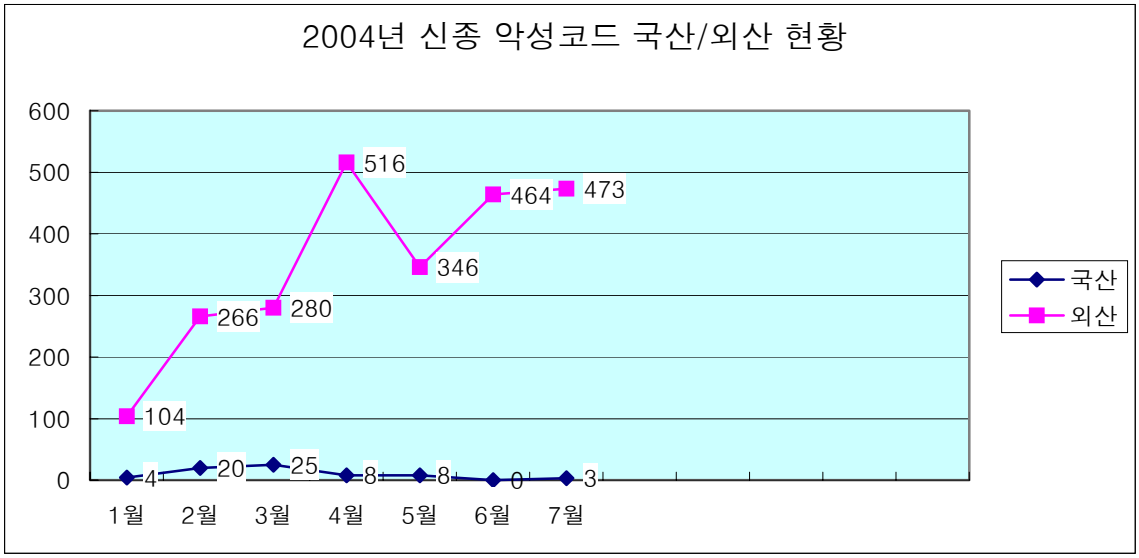


[그림 3] 7월 신종 (변형) 악성코드 유형별 현황

악성 IRCBot 류가 가장 많은 유형을 차지하고 있다. Mass Mailer 유형도 5%를 차지 하고 있다. Dropper(드롭퍼)는 주로 mIRC 클라이언트를 변형한 형태 또는 악성 IRCBot 류가 대다수를 차지하고 있다.

제작지별 신종(변형) 악성코드 현황

다음은 신종(변형) 악성코드들의 국산/외산 현황이다.



[그림4] 2004년 제작지별 신종 악성코드 현황

이번 달은 파일의 크기와 그 코드가 조금씩 동일한 진단명을 가진 국산 트로이목마가 발견되었다. 이 트로이목마는 원래는 애드웨어 이지만 사용자 동의 없이 특정 키워드 입력 시 특정한 사이트로의 접속을 막는다. 이 트로이목마는 처음 올해 4월에 발견, 보고 되었으며 이번 달 들어서 고객으로부터 다시 감염보고가 있었다.

일반적으로 위와 같은 형태나 애드웨어들은 특정 사이트 방문시 실행되는 Active X를 제대로 확인하지 않고 실행하는 경우가 많으므로 반드시 설치 전 신뢰할 수 있는 사이트에서 제공했는지 사용자가 우선 판단 후 설치하는 것이 좋다. 또한 설치 후 문제가 발생되면 대부분 제어판의 프로그램 추가/제어에서 삭제할 수 있도록 되어 있다.

애드웨어 또는 스파이웨어에 대한 진단/치료에 대한 궁금증이 높아진 요즘 반드시 이에 대한 정확한 정의와 대응 방법을 알고 있다면 대처하는데 별다른 어려움이 없다. 그러므로 신뢰할 수 있는 정보를 주는 사이트에서 관련 내용이나 진단/치료 툴을 비교해 보는 등 꼼꼼히 선택하도록 한다.

III. 7월 신규 보안취약점

작성자 : 조경원 연구원(dubhe@ahnlab.com)

매월 둘째 주 수요일에 발표하는 마이크로소프트사의 정기 보안 패치에는 MS04-018부터 MS04-024[1]까지 총 7개가 발표되었다. 이중 실제 직접적인 보안 위협이 되는 '긴급' 수준의 보안 패치는 MS04-022, MS04-023 두건이 포함되어 있다.

MS04-022 윈도우 작업 스케쥴러 취약점

작업 스케쥴러(Task Scheduler)는 윈도우 시스템에서 예약 작업을 지원하는 서비스로, 응용 프로그램의 이름을 처리하는 부분에서 취약점이 발견되었다.

취약점은 .job 확장자를 가진 작업 스케쥴러 파일 내부에 악의적으로 긴 명령을 작성하여, 해당 파일을 익스플로어를 통하여 실행(스케쥴러 등록)하거나 미리보기 등을 수행할 경우 버퍼 오버플로우 취약점이 발생하게 되는 것이다. 이 취약점은 .job 파일을 인터넷 익스플로어로 실행 시에만 약점으로 웹 등을 통해 악성 .job 파일의 설치를 유도하거나 다른 취약점과 조합되어 자동으로 설치하게 유도할 경우 외부에서의 공격이 가능하다. 이 취약점은 윈도우 2000과 XP에서만 해당된다.

취약점 발표 및 패치가 7월 14일에 발표된 지 4일 만에 특정 언어의 Windows XP 시스템에 대한 공격코드(Exploit)가 발표 되었으며 7월 31일 모든 언어의 XP 시스템에 공격이 가능한 공격코드가 현재 알려져 있다.

현재 직접적으로 공격에 악용된 사례는 알려지지 않았지만 추후 악성코드 등에서 .exe, .zip 등이 아닌 .job 확장자의 메일 첨부 형태로 발전할 가능성도 있다.

패치 설치 방법 및 자세한 Microsoft의 정보는 MS04-022 Bulletin[2]을 참조하면 된다.

MS04-023 HTML 도움말 취약점

showHelp() 취약점과 HTML 도움말에 대한 두 가지 취약점에 대한 패치이다.

showHelp() 취약점은 2003년 12월에 발견된 취약점이며 HTML 도움말을 웹상에서 지원하게 하는 메소드로, 자세한 형식은 MSDN의 정보[3]를 참조하면 된다.

이 취약점은 showHelp() 함수에서 경로를 적절히 검사하지 않아 발생하는 취약점으로, 시스템 내부에 있는 파일을 인터넷 익스플로어 상에서 실행시킬 수 있다. 시스템 내부에 실행시킬 파일이 존재하여야 하므로 직접적으로 공격자가 의도하는 공격은 힘들며, 다른 취약점 및 특수한 캐쉬 파일, 다운받아지는 응용프로그램 파일[4] 등을 악용하여 공격하는 사례가 알려져 있다.

---

[1] http://www.microsoft.com/korea/security/security_bulletins/200407_windows.asp
[2] http://www.microsoft.com/korea/technet/security/bulletin/MS04-022.asp
[3] http://msdn.microsoft.com/workshop/author/dhtml/reference/methods/showhelp.asp
[4] Winamp의 특정버전을 사용할 경우 특정확장자의 파일을 자동으로 다운로드 받을 수 있다.

악성코드 등에서 사용된 경우는 현재 알려져 있지 않다.

MS04-023에는 또 하나의 HTML 도움말 취약점에 대한 패치가 들어 있지만 마이크로소프트사가 신뢰된(외부에 발표되지 않고 직접 마이크로소프트사에게만 통보되어 취약점 보완작업이 이루어진) 정보 제공자로부터 받은 경우로 자세한 정보가 알려지지 않았다.

패치 설치 방법 및 자세한 마이크로소프트사의 정보는 MS04-023 Bulletin[1]을 참조하면 된다.

[1] http://www.microsoft.com/korea/technet/security/bulletin/MS04-023.asp

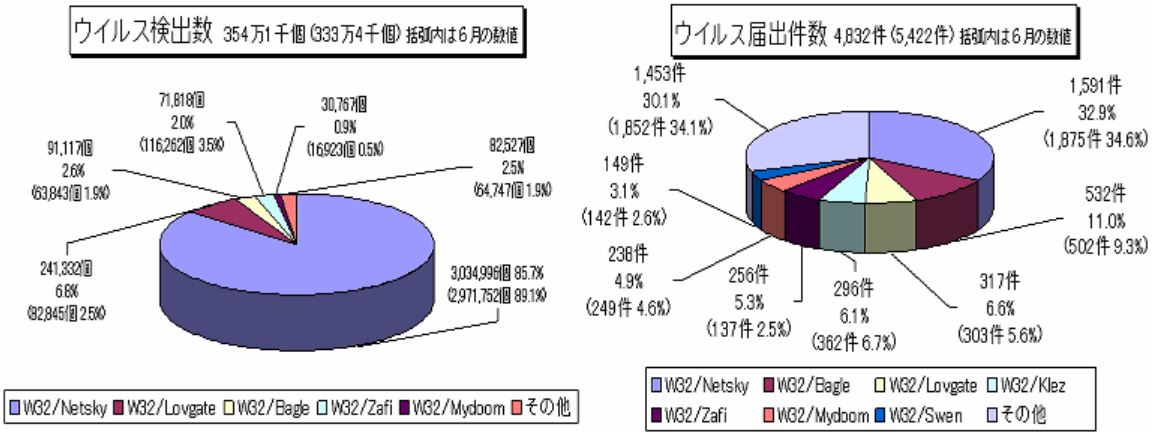
Ⅳ. 7월 일본 피해 동향

작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

넷스카이 웜은 2004년 상반기에 최초로 발견된 이후 현재까지도 활발하게 자신을 전파하려는 시도를 계속하고 있다.

아래의 [그림1]은 2004년 7월 한달 동안 일본의 IPA에 신고된 악성코드 피해 현황에 대한 통계를 그래프로 나타낸 것이다. 참고로 왼쪽의 그래프는 신고자가 신고한 악성코드의 개수의 총합이고 오른쪽의 그래프는 신고된 악성코드 중 동일한 악성코드는 하나만 카운트하여 통계를 추출한 것이다.

두 그래프에서 흥미로운 것은 사용자에게서 7월에 검출된 악성코드의 개수는 354만 건 정도이고 이 중에 넷스카이 웜이 차지하고 있는 비율은 85%에 이르는 것에 비해 피해 신고를 한 사용자의 비율은 32%에 불과함을 알 수 있다. 이는 넷스카이 웜의 전파력이 다른 웜에 비해서 강하다는 것을 보여주지만 다른 한편으로는 넷스카이 웜으로 인해 발생하는 메일 트래픽에 비해 상대적으로 감염자가 많지는 않다는 것을 반증해주기도 한다.



[그림1] 2004년 7월 악성코드 피해 현황(출처 : 일본의 IPA)

일본 유행 악성코드 유형별 발생현황

2004년 7월 일본에서 가장 유행한 악성코드는 넷스카이 웜과 Win32/Bagle.worm(이하 베이글 웜)으로 이는 전월과 크게 차이가 없다.

아래의 [표1]은 2004년 7월 IPA/ISEC에 접수된 악성코드 피해에 대한 통계자료로, 여전히 넷스카이 웜의 노출건수가 많음을 알 수 있다. 그러나 전월과 비교하였을 때 피해건수는 상대적으로 감소했는데 이는 백신 프로그램 등을 통한 치료로 감염 시스템이 점점 줄어드는 것과 활발하게 제작되어 유포되던 변형의 발견이 감소한 것 등이 주요 원인으로 생각된다.

이외에 주목할만한 점은 Win32/Zafi.worm(이하 자피 웜)의 피해 건수가 전월에 비해 크게 증가한 것이다. 자피 웜은 2004년 4월 최초로 발견된 이후 6월 중순경 새로운 변형이 발견

된 이메일 웜이다.

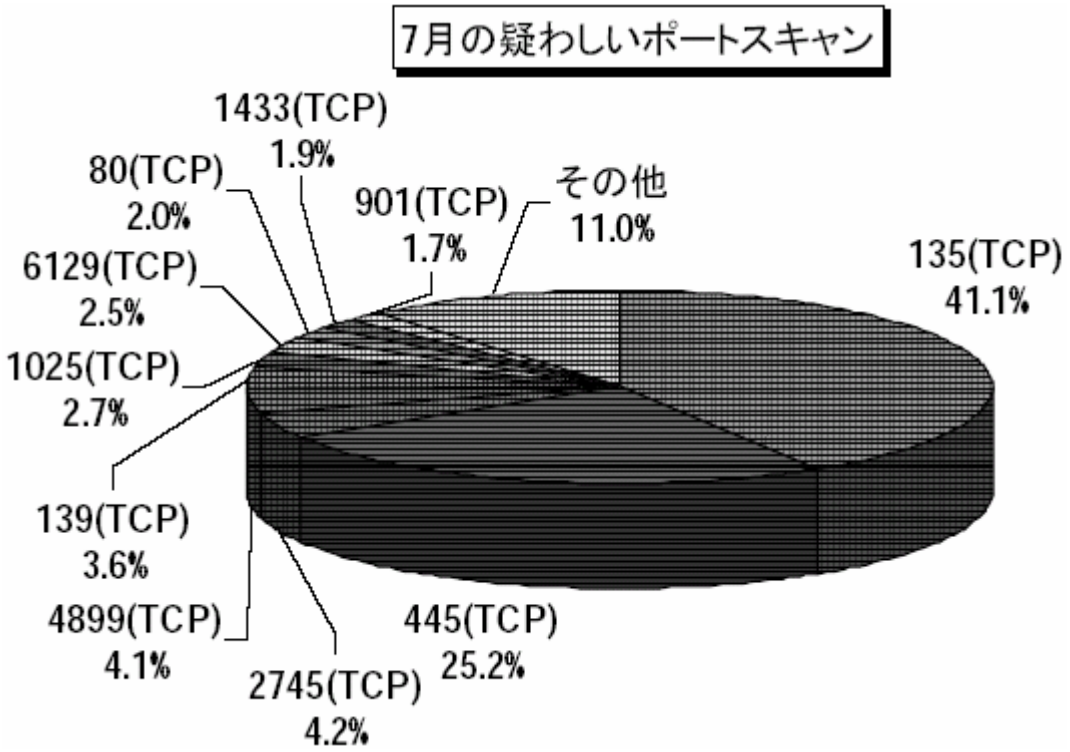
Window/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Netsky	1,591	Xm/Laroux	29	VBS/Redlof	108
W32/Bagle	532	X97M/Divi	10	Wscript/Fortnight	11
W32/LovGate	317	X97M/Tristate	8	Wscript /Kakworm	9
W32/Klez	296	W97M/Bablas	6	VBS/Loveletter	5
W32/Zafi	256	WM/Cap	2	VBS/Internal	2
W32/Mydoom	238	W97M/Concept	2	VBS/Netlog	1

[표1] 일본의 악성코드 피해 신고 현황 (출처 : IPA/ISEC)

일본 네트워크 트래픽 현황

아래의 [그림2]는 2004년 7월 일본에서 발생한 네트워크 포트 사용현황을 나타낸 것이다. 가장 많은 트래픽이 발생한 포트는 TCP 135와 TCP 445 포트이다. 두 포트는 윈도우 OS에서 인증을 위하여 사용되는 포트이지만 최근 유행하는 웜들이 윈도우 OS의 RPC 관련 취약점을 이용한 공격을 시도할 때에도 사용된다.

TCP 2745포트를 이용한 트래픽이 많은데 이는 베이글 웜에 감염된 시스템에 설치된 백도어에서 발생하는 것일 가능성이 있다.



[그림2] 일본의 네트워크 트래픽 현황

한국 KISA(정보보호진흥원)과 일본 IPA(정보처리추진기구)의 협력관계 결성

한국의 KISA와 일본의 IPA 두 기구 사이에 정보보안과 관련한 현안에 대한 협력관계가 맺어졌다. 두 기관의 주요 협력분야는 정보보호에 관한 정책과 연구조사, 취약성 분석 정보 교환, 암호기술 등 정보보호와 관련한 전반적인 내용을 포함하고 있으며 양 기관의 현안에 대한 정보교환을 통해 최근 인터넷 환경이 고도로 발전하고 있는 양국간의 정보보호 수준의 향상에 크게 기여할 것으로 기대된다.

V. 7월 중국 피해 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

2004년 7월 중국 악성코드 동향은 지난 6월부터 이어져온 네트워크로 전파되는 웜과 Mass Mailer들의 혼전 양상이 지속되고 있다. 한동안 감염보고가 줄어 들었던 악성코드가 다시 순위에 올라오는 등 네트워크로 전파되는 웜과 Mass Mailer들의 혼전 양상이 더욱더 심해지고 있는 것으로 보인다. 2004년 7월에는 어떠한 악성코드들이 발견되고 확산되고 있는지 살펴보도록 하자.

악성코드 TOP 5

순위 변화	7월	Rising	CNCVERC
*	1	Worm.Netsky	Worm_AgoBot
*	2	Worm.Lovgate	Worm_Netsky.D
NEW	3	Worm.Lentin.m	Worm_Lovgate.C
NEW	4	Backdoor.Sdbot	Worm_Bbeagle.J
NEW	5	Worm.Sobig.f	-

[표1] 2004년 7월 악성코드 TOP 5

'*' - 순위변동 없음, 'NEW' - 순위에 새로 진입, '-' - 순위 하락

[표1]은 중국 로컬 백신업체인 라이징(Rising)사와 정부연구기관인 중국국가컴퓨터바이러스대응중심(China National Computer Virus Emergency Response Center, 이하 CNCVERC)이 작성한 7월 중국 악성코드 TOP 5이다. 순위상으로는 조금씩 차이가 있지만 전반적인 흐름은 지난 6월부터 이어져 온 네트워크로 전파되는 웜과 Mass Mailer들의 혼전 양상을 그대로 보여주고 있다. 순위에 기록된 악성코드 중에는 7월에 발견된 악성코드는 없으며 기존에 발견된 악성코드들이 대부분이다. 그러나 한동안 순위에 오르지 못하고 감염보고의 수도 적었던 악성코드들이 다시 순위권으로 진입한 것이 특이한 점으로 볼 수 있다. 순위권에 재진입한 악성코드들은 [표1]에 나와 있는 것과 같이 Worm.Lentin.m(Win32/Yaha.worm – 이하 야하 웜), Backdoor.Sdbot(Win32/SdBot.worm – 이하 에스디봇 웜)과 Worm.Sobig.f(Win32/Sobig.worm – 이하 소빅 웜)을 들 수 있다. 그러나 해당 악성코드들이 순위권에 재진입을 하였으나 아래 기술할 악성코드 분포를 참고할 경우 감염보고 면에는 그렇게 높은 비율을 차지하고 있지는 않다.

신종 악성코드

[표1]의 악성코드 순위에 포함이 되지 못하였지만 라이징(Rising)사에서 보고한 감염보고가

있었던 신종 악성코드들은 다음과 같으며 해당 악성코드들의 감염보고 수치는 그렇게 높은 편은 아니다. 감염 보고된 악성코드들 대부분이 트로이목마 류이며 중국 내에서만 발견되는 QQ 트로이목마 류가 점차 증가하고 있는 것이 특이점으로 볼 수 있다.

▶ Harm.Smith

자기 자신을 지속적으로 복사하여 시스템의 자원을 모두 소비시키는 증상을 보이며 현재까지 발견된 변형으로는 Harm.Smith.b, Harm.Smith.c 가 있는 것으로 보고되었다.

▶ Trojan.PSW.QQPass

Trojan.PSW.QQPass는 중국에서만 발견되는 트로이목마로서 중국에서 많이 사용되는 QQ 메신저의 패드워드를 가로채는 기능을 가지고 있는 것으로 알려져 있다. 최근까지 보고된 바에 따르면 Trojan.PSW.QQPass의 변형은 총 13건이 알려져 있다.

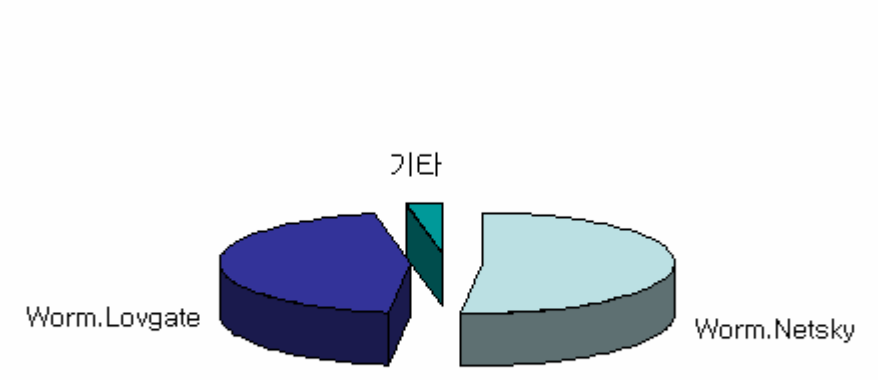
▶ Trojan.QQMSG.Boker

해당 트로이목마는 비주얼 베이직으로 제작이 되었으며 감염 시 발견되는 가장 큰 특징은 인터넷 익스플로어의 메인 페이지를 특정 웹사이트로 변경하는 기능이 있다. 그리고 QQ 메신저에 등록되어 있는 사람들에게 지속적으로 특정 문구를 전송해 특정 웹사이트로 접근을 유도하는 기능도 가지고 있는 것으로 알려져 있다. 변형은 총 33건인 것으로 보고되었다.

▶ Trojan.PSW.MSN.a

비주얼 베이직으로 제작된 트로이목마이며 MSN 메신저의 사용자명과 암호를 후킹하는 기능이 있는 것으로 보고되었다.

악성코드 분포



[표2] 2004년 7월 중국의 악성코드 분포

위 [표2]는 7월 한달 동안 조사된 중국 악성코드의 분포도이다. 위 분포도를 보게 되면 Worm.Netsky(Win32/NetSky.worm – 이하 넷스카이 웜)가 52%를 그리고 Worm.Lovgate(Win32/Lovgate.worm – 러브게이트 웜)가 45%로 전체의 97%를 차지하고 있다. 그리고 나머지 3%는 소빅 웜, 야하 웜, Harm.Smith, Trojan.PSW.QQPass, Backdoor.IRCBot(Win32/IRCBot.worm – 이하 아이알씨봇 웜), Trojan.QQMSG.Boker 등이 차지하고 있다.
이러한 대결 구도는 지난 6월부터 지속되고 있었으나 이번 7월달에 들어 메일로 전파되는 Mass Mailer들이 다시 증가현상을 보이고 있는 점이 특이하다고 볼 수 있다.

결론

지난 6월부터 이어져 오는 네트워크로 전파되는 웜 류와 메일로 전파되는 Mass Mailer류의 대립 구도가 7월에도 이어져 오고 있으며 러브게이트 웜과 넷스카이 웜의 염보고가 전체 보고의 97%를 차지할 정도로 이 두 웜의 영향력이 높아진 편이다. 그리고 이 외의 다른 특징으로는 QQ 메신저를 이용해 전파되는 QQ 트로이목마 류의 보고도 다시 증가하고 새로운 변형이 발견되는 것도 이번 7월 중국 악성코드 동향의 특이사항이 아닌가 생각된다. 당분간 러브게이트 웜과 넷스카이 웜으로 대표되는 네트워크 웜과 Mass Mailer 웜의 대립 구조는 지속될 것으로 예측된다.

VI. 테크니컬 컬럼 I – 자동 이메일 추출 수집기 대응방법

작성자 : 최동균 연구원(cdk@ahnlab.com)

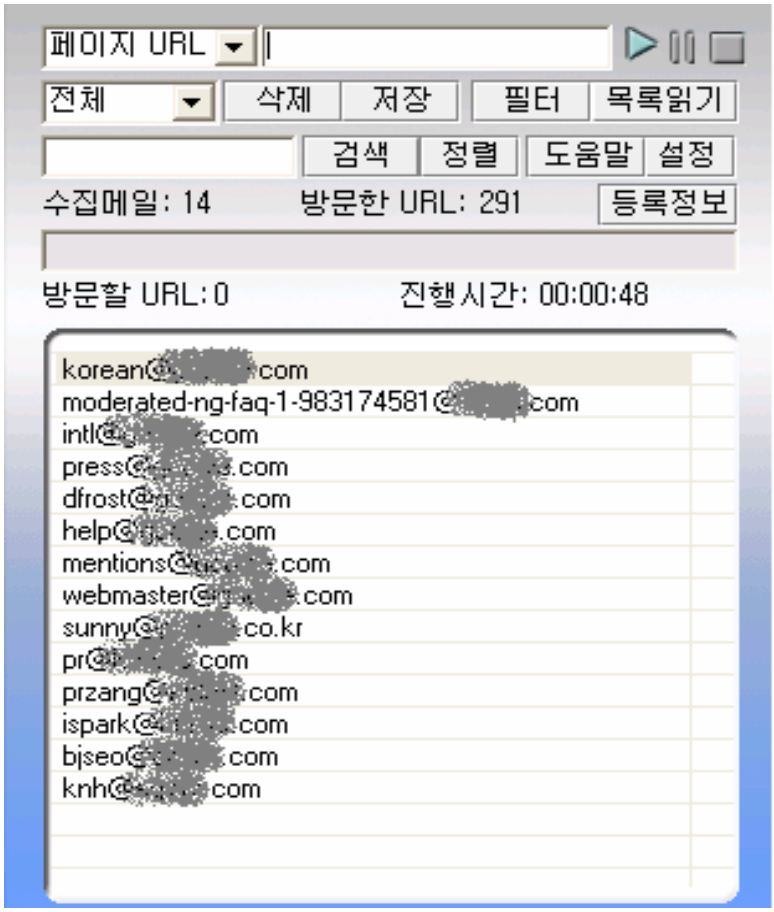
초고속 인터넷 망의 확산과 함께 빠르고 효율적인 커뮤니케이션 수단으로 이메일이 대중화 되었으며 이를 이용한 이메일 광고는 비용이 저렴하고 효과가 크다는 점에서 전자상거래 태동기에 매우 유용한 마케팅 수단이 되었다. 그러나 수신자의 의사와 무관하게 지속적이고 대량으로 전송되며, 내용 자체가 불법적이거나 선정적인 내용을 담고 있어 많은 사용자들에게 정신적 물질적 피해를 끼치고 있어 사회적으로 큰 문제를 야기하고 있다.

이와 같이 사용자가 원하지 않음에도 무차별적으로 발송되는 스팸메일은 초기 자본이 많지 않은 소규모 사업자들에게 손쉬운 마케팅 수단으로 이용되고 있으며, 단시간 내에 많은 사용자들에게 스팸메일을 발송하기 위해 이들은 이미 수집되어 있는 수백만개의 메일링리스트를 은밀히 거래하거나, 인터넷상에 공개된 이메일 주소를 자동 추출하는 '이메일 수집기'를 이용하여 사용자 이메일 계정을 확보한다.

아래는 스팸메일 발송 대상이 되는 이메일 주소 수집의 방법과 이를 효과적으로 대응할 수 있는 방법을 기술한다.

이메일주소 자동 추출기를 이용한 이메일 수집방법

스패머(Spammer)가 메일링리스트 확보를 위해 사용하는 '이메일 수집기'는 사용자가 웹페이지 요청(HTTP/80)을 하는 방법과 동일하게 웹서버에 정보를 요청하여 컨텐츠를 제공받는다. '이메일 수집기'는 제공받은 컨텐츠를 분석하여 HTML Code 내에 포함된 이메일 주소만을 추출한다. 이메일 주소를 추출하는 방법은 HTML Code 내에서 이메일을 유추할 수 있는 'mail to' 또는 '@' 등의 특정 구분자를 식별하여 이와 관련된 문자열을 이메일 주소로 인식한다.



[그림1] 이메일 수집기를 통해 수집된 이메일 계정들

자동 이메일 추출 수집기 대응방법 (E-mail Masking)

위와 같이 자동 이메일 수집기를 이용하여 수집되는 메일링리스트를 무력화하기 위한 대응 방법을 살펴보면 다음과 같다.

▶ 유효하지 않은(의미없는) 문자열 첨부

HTML Code 내에서 이메일 주소로 예상되는 '@' 또는 'mail to' 등을 식별하여 관련 문자열을 무작위로 추출하는 이메일 수집기의 특성에서 착안하여, 노출되는 이메일 주소 어두 또는 어미에 유효하지 않은(의미없는) 문자열을 함께 첨부하는 방법이다.

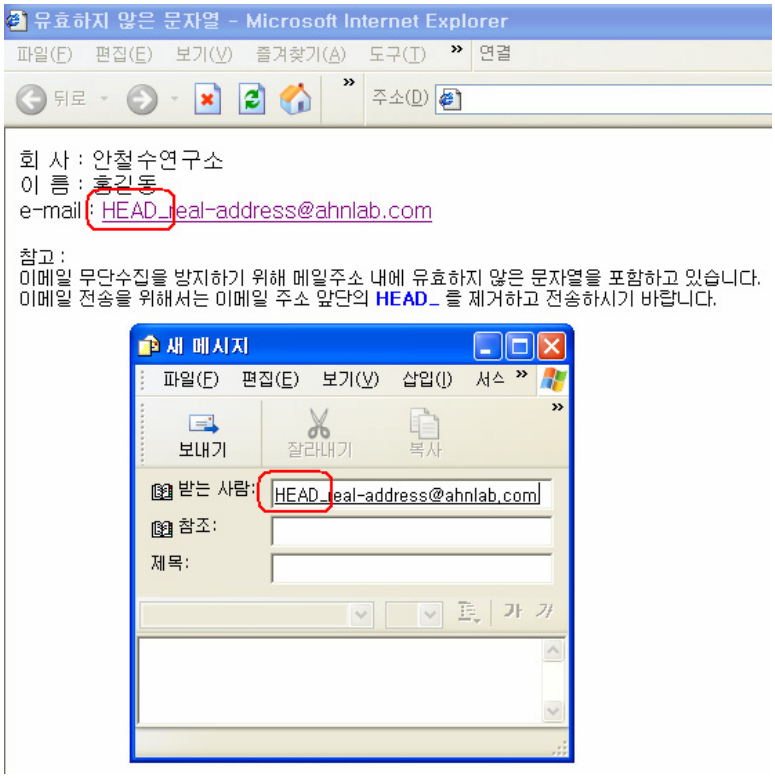
이메일 수집기는 유효하지 않은 문자열을 함께 이메일 주소로 인식하게 되므로 스팸메일 전송 실패를 유도하는 것이다. 번거로운 절차 없이 간편하게 적용할 수 있지만 이메일 수집기에서 손쉽게 대응(이메일 유효성 검사)할 수 있다는 단점도 있다. 하지만 수집한 메일주소 중 유효하지 않은 리스트는 통상 해당 메일주소를 제거(메일링리스트에서 삭제)하는 스패머의 성향을 감안한다면 특별한 기술을 필요로 하지 않는 간편한 대응방법이 될 수 있다.

변경 전:

real-address@ahnlab.com

변경 후:

HEAD_real-address@ahnlab.com



[그림2] 의미없는 문자열(HEAD_)을 포함한 웹 페이지(메일 전송 시 HEAD_ 제거 필요)

```
<html>
<head>
<title>유효하지 않은 문자열</title>
</head>
<body>
        회 사 : 안철수연구소
        이 름 : 홍길동
        e-mail : <a href="mailto:HEAD_real-address@ahnlab.com">HEAD_real-address@ahnlab.com</a>

        참고 :
        이메일 무단수집을 방지하기 위해 메일주소 내에 유효하지 않은 문자열을 포함하고 있습니다.
        이메일 전송을 위해서는 이메일 주소 앞단의 <font color=blue>HEAD_</font> 를 제거하고 전송하시기 바랍니다.
</body>
</html>
```

[그림3] 의미없는 문자열(HEAD_)을 포함한 웹 페이지의 HTML 코드

▶ Character Unicode

노출되는 이메일 주소의 알파벳 문자를 유니코드로 변환하여 수집된 메일링리스트를 무력화하는 방법이다.

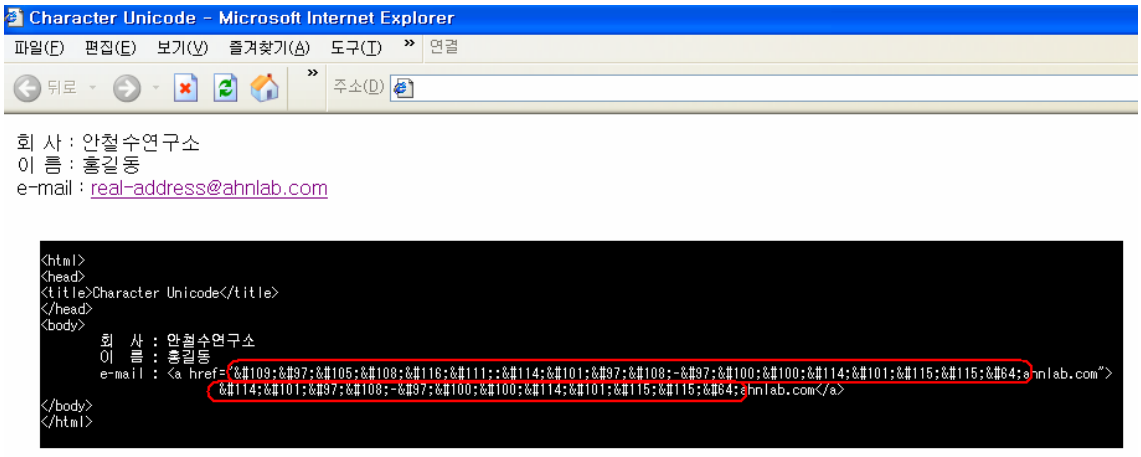
각각의 알파벳 문자를 이에 대응하는 유니코드 변환의 간단한 절차로 적용이 가능하며, 식별자로 사용하는 'mail to' 또는 '@'를 함께 유니코드로 변환한다면, 이메일 수집기로부터 더욱 자유로울 수 있다. 하지만 이를 고려한 추출 프로그램 제작이 쉽다는 단점이 있다.

변경 전:

real-address@ahnlab.com

변경 후:

real-address@ahnlab.com



[그림4] 웹페이지에 노출된 이메일 주소와 해당하는 실제 HTML 코드

▶ JavaScript

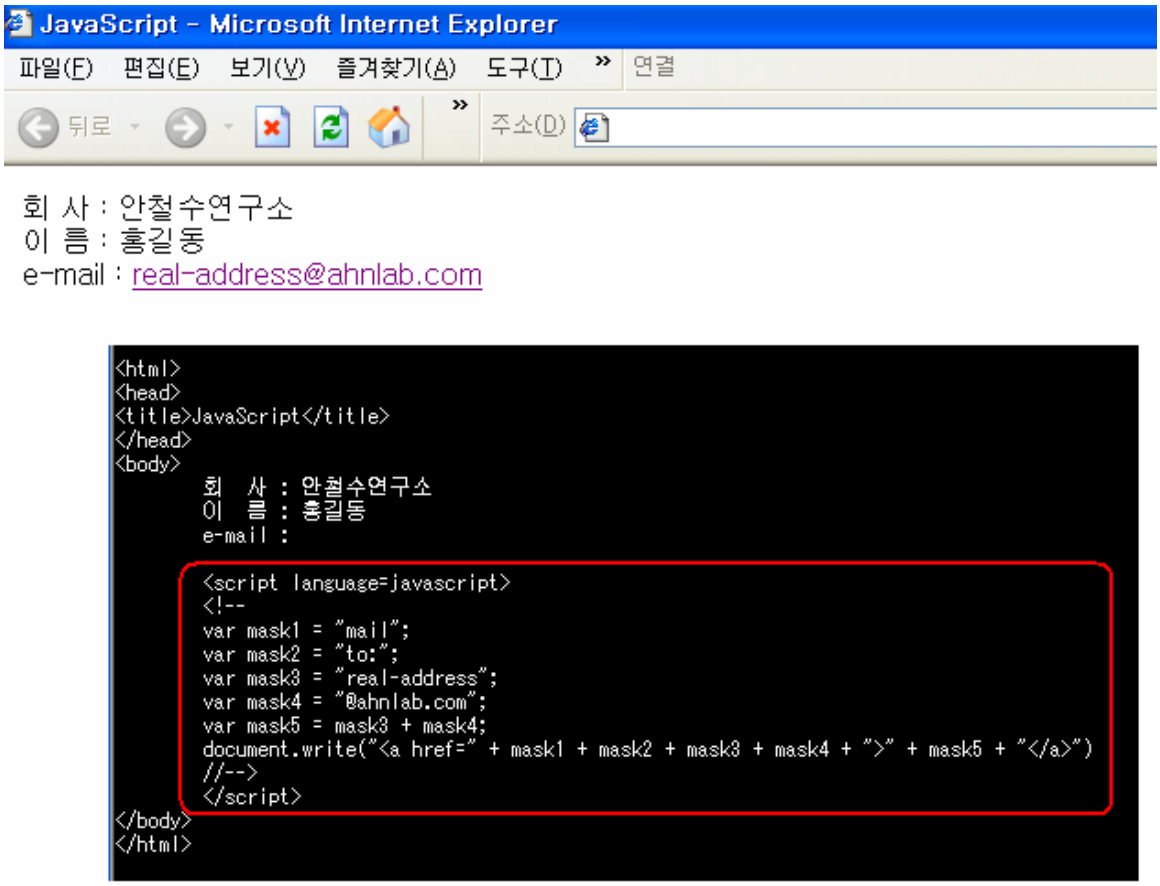
노출되는 이메일 주소의 직접 기입을 피하고 JavaScript를 이용하여 이메일 주소를 간접 적용한다. 수집된 메일링 리스트는 실존하는 이메일 주소가 아닌 JavaScript 소스가 수집된다. 적용이 간편한 반면 대응 추출 프로그램 제작 또한 용이하다는 단점이 있다.

변경 전:

real-address@ahnlab.com

변경 후:

```
<script language=javascript>
<!--
var mask1 = "mail";
var mask2 = "to:";
var mask3 = "real-address";
var mask4 = "@ahnlab.com";
var mask5 = mask3 + mask4;
document.write("<a href=" + mask1 + mask2 + mask3 + mask4 + ">" + mask5 + "</a>")
//-->
</script>
```



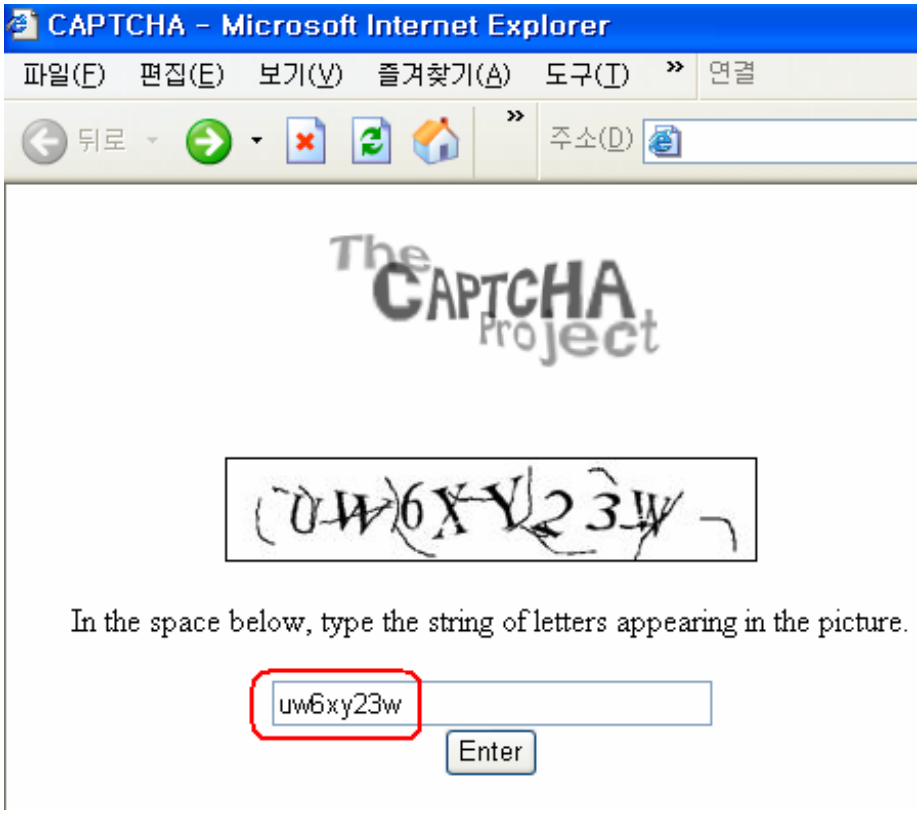
[그림5] 웹페이지에 노출된 이메일 주소와 해당하는 실제 HTML 코드 (JavaScript)

▶ Captcha(Completely Automated Public Test to tell Humans and Computers Apart) algorithm

Captcha 알고리즘[1]은 카네기-멜론 대학에서 창안 하였으며, 이를 웹사이트에 적용하여 스팸과 관련된 일련의 작업을 효과적으로 무력화시킬 수 있는 방법이다.

노출된 이메일 주소에 이벤트(메일 전송을 위한 마우스 클릭) 발생시 확인 절차를 위해 질의 창이 출력된다. 다음 단계로 넘어가기 위해서는 질의 창(OCR[2]을 방해하기 위해 노이즈 처리) 내의 형상화된 이미지 문자를 입력해야 하며, 결과 입력 시 발생된 이벤트의 주체가 사람(Humans)이라면 허용을 하고 자동 봇(Computers)이라면 거부를 한다.

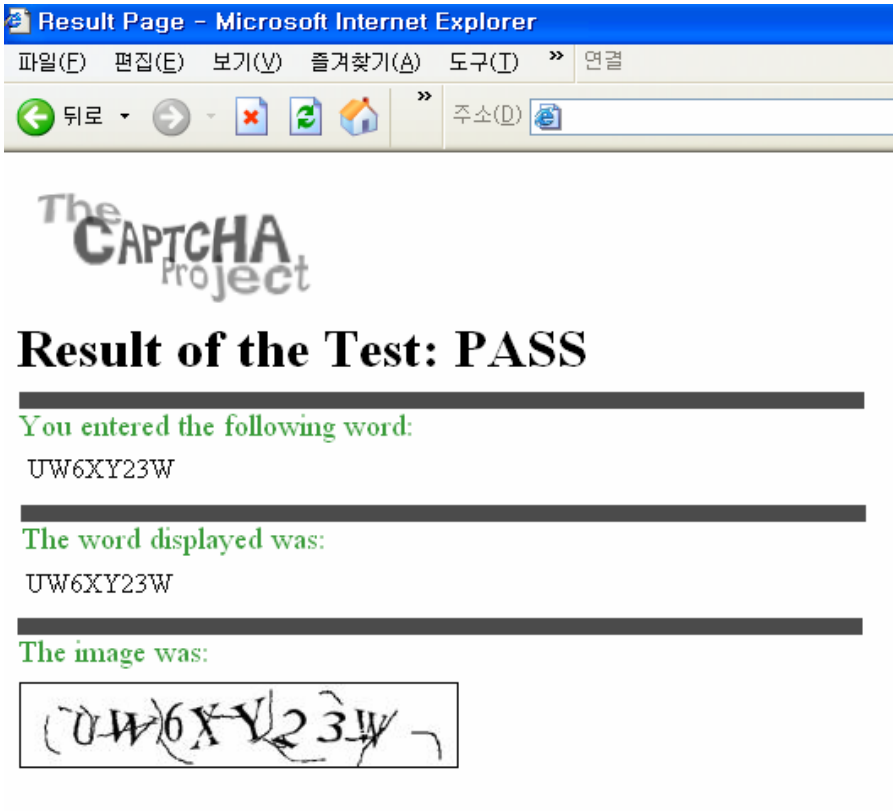
지금까지 기술된 대응 방법 중 가장 효과적으로 이메일 수집기를 무력화 시킬 수 있는 방법이지만, 구현에 있어 상대적으로 어려운 점이 있다.



[그림6] 이벤트 주체를 확인하기 위한 질의 단계와 입력 예시

[1] Captcha 참고 사이트 : http://www.captcha.net

[2] OCR (optical character recognition) : 인쇄되거나 또는 손으로 쓴 글씨들을 컴퓨터로 인식하는 장치



[그림7] 답안 입력 후 이벤트 주체가 사람으로 확인되어 허용

제품 홍보를 위한 마케팅 비용이 거의 들지 않는다는 이점을 악용하여 무차별적으로 살포되는 스팸메일을 대응하기 위해서는 위에서 언급한 이메일 수집 대응방안 중 하나를 적용하는 것보다는 여러 방안을 함께 적용하는 것이 보다 효과적인 방법이라 하겠다.

VII. 테크니컬 컬럼 II – 트래픽 분석의 시작과 준비

작성자 : 정관진 주임연구원(intexp@ahnlab.com)

넷스카이, 베이글, 아고봇. 한번쯤은 들어보았을 악성코드 이름들이다. 이러한 악성코드들은 사내 기업 네트워크 또는 보안담당자들에게 골치 아픈 존재로써, IRC봇(IRCBot)은 현재 천여 개 이상의 변종이 존재할 만큼 기업에서 감염피해 단골손님이기도 하다. 일반적으로 웜은 특성상 자기자신을 전파하기 위하여 다양한 전파 방법을 이용하는데, 네트워크라는 환경은 웜의 전파 범위를 더욱 넓혀주고 있다. 이에 따라 네트워크가 몸살을 앓고 있다 해도 과언이 아니다.
특히나 기업의 네트워크를 운영하고 있는 담당자로서는 현실적으로 직면하고 있는 문제이므로 담당자들의 고민은 더욱 많아지고 있다. 더구나 기업의 망 규모가 큰 경우에는 사용되는 PC 규모도 많기 때문에 외부로부터 악성코드에 감염될 확률은 더욱 높다. 관리의 범위가 넓어지게 되고 이에 따라 관리의 범위를 넘어나는 시스템들이 증가함에 따라 위협에 노출되는 범위가 자연스럽게 높아지는 것이다. 물론, 기업들에서도 이에 대한 방어대책으로 바이러스월, 백신 소프트웨어, 방화벽, 침입탐지시스템(IDS)까지 동원하며 2중 3중의 방어망을 펼쳐놓아도 웜에 감염되어 내부 네트워크를 마비시키는 문제들이 이어지고 있다. 이메일을 통해 받은 악성코드를 실행시키거나 인터넷 브라우저를 통한 다운로드, FTP의 다운로드 등 보안의식이 충분치 않은 환경에서는 특히 이런 문제들이 발생할 가능성이 높다. 이에 대한 근본적인 해결책은 사용자들의 보안의식이 선행되어야만 한다. 방화벽과 같은 보안 제품은 외부의 위협으로부터 위험을 최소화하기 위한 하나의 방어수단에 불과한 것이다.

하지만 분명한 것은 아직도 이 시각에도 수 많은 악성코드들은 감염대상 시스템을 찾기 위해 계속 분주히 활동하고 있고, 관리자들은 지속적으로 이러한 위협에 대응하기 위해 노력하고 있다. 최근 악성코드들의 특성상 네트워크를 이용하여 전파되는 현상이 두드러지고 이에 따라 네트워크 상의 유해 트래픽을 탐지하고 판단할 수 있는 방법을 제시하고자 한다.
앞으로 3회의 연재에 걸쳐 트래픽 분석을 위한 툴의 사용부터 악성코드에 의한 트래픽의 위협까지 살펴볼 것이다.

트래픽 분석의 준비

네트워크상에서는 수 많은 프로토콜이 이용되고 있으며, 이에 대한 프로토콜을 분석하기 위해서는 해당 프로토콜 구조를 알고 있어야 한다. 이러한 프로토콜의 구조는 RFC(Requests for Comments)에 정의되어 있고, 이것의 구조를 이해해야만 분석이 가능하게 된다. 하지만, 모든 구조를 이해하고 프로토콜을 분석하기에는 한계가 있으므로, 프로토콜 구조를 이해하기 쉽게 표현하여 분석을 도와주는 패킷 분석도구들이 많이 이용되고 있다.

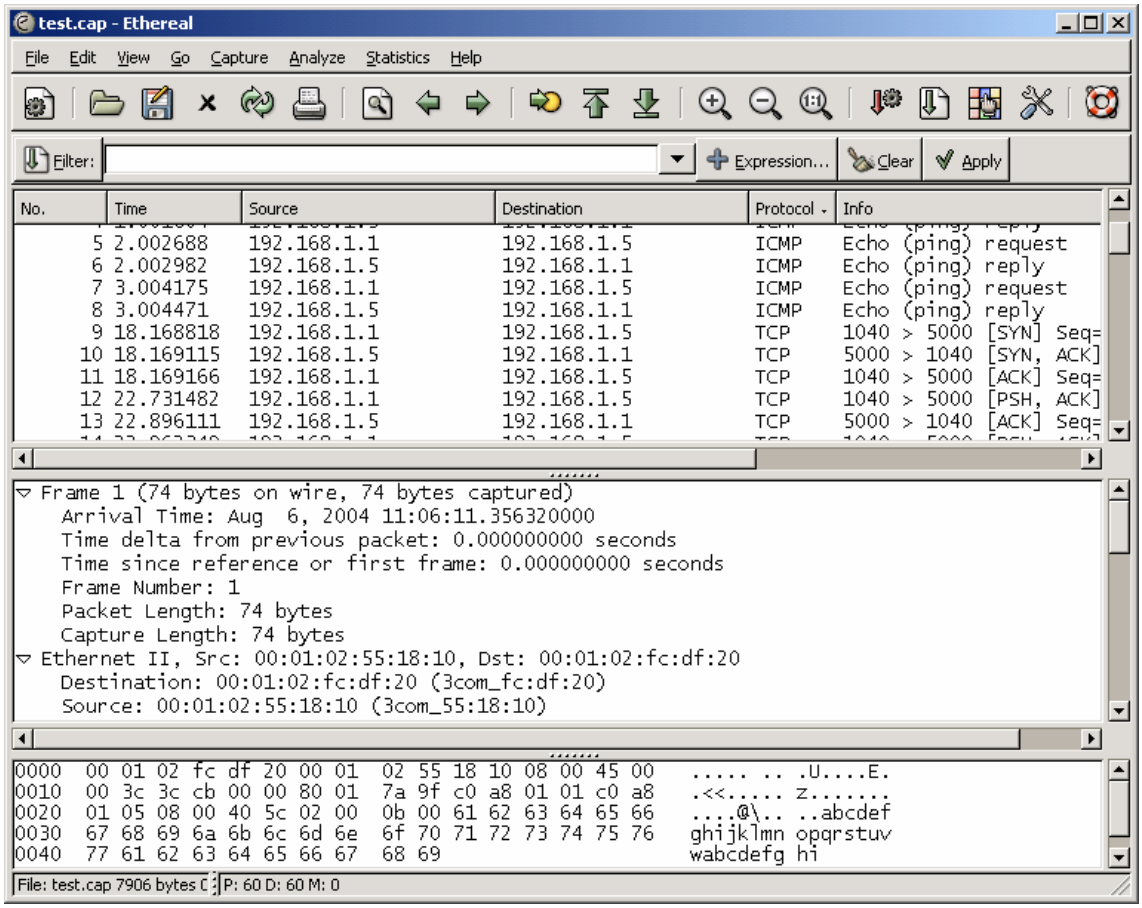
무료로 사용 가능한 것부터 시작하여 상업용에 이르기까지 수 많은 제품들이 분석도구로 활용되고 있다. 여기서는 무료로 사용가능하며 많은 인기를 누리고 있는 공개 소프트웨어인 Ethereal(이하 이더리얼)이란 프로그램을 이용하고자 한다. 이더리얼은 다음과 같은 방법을 통하여 쉽게 구할 수 있다.

- http://www.ethereal.com 또는 미러사이트에서 Korea를 선택한다.
  이 글을 작성하는 시점에 0.10.5 가 최신 버전이다.
- 한국 공식 미러사이트(http://ethereal.secuwiz.com)를 직접 방문한다.
- 윈도우에 설치하는 경우 PCAP 라이브러리의 설치가 필요하다.
  http://ethereal.secuwiz.com/distribution/win32/

이더리얼은 GUI(Graphical User Interface)기반의 네트워크 프로토콜 분석도구로 다양한 종류의 네트워크 디바이스, 프로토콜, 포맷형태를 지원하고 있다.[1] 강력한 필터 기능과 500 여개 이상의 프로토콜 지원, 출력필터를 통한 데이터 출력 정의, 칼라 룰을 이용한 분석의 용이성 등 다양한 장점들을 가지고 많은 사용자층을 확보하고 있다.

우선 이더리얼을 실행하면 [그림1]과 같은 메인 화면을 볼 수가 있다.

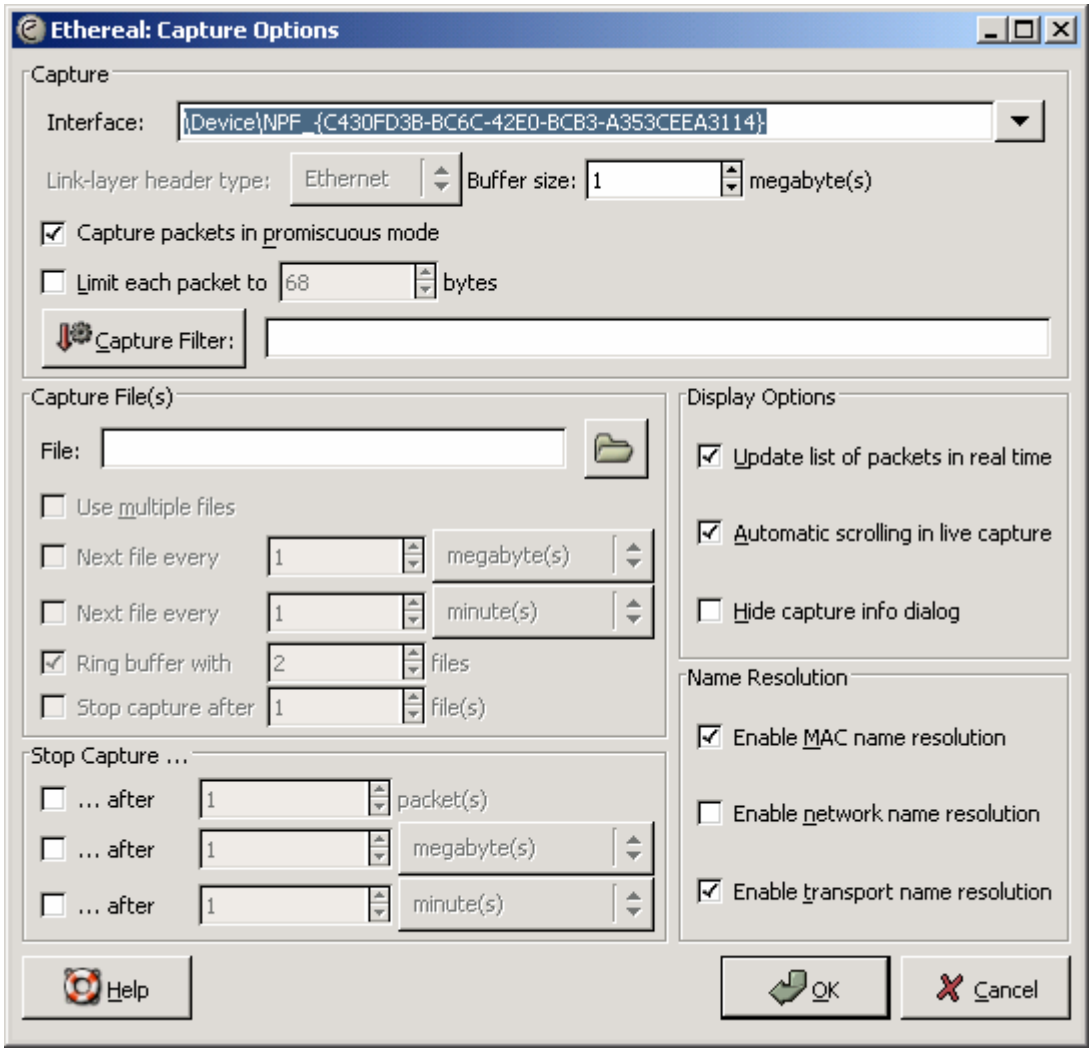
[1] 텍스트 기반의 프로그램인 Tethereal 도 지원하고 있다.



[그림1] 이더리얼의 메인 화면(기본 레이아웃)

이더리얼과 시작하는 패킷 분석의 기본

메인 화면의 구성은 크게 패킷리스트 화면, 패킷상세 화면, 패킷 바이트 화면으로 나뉘어져 있다. 물론 환경설정인 Edit->Preferences(Shift+ Ctrl+ P)를 이용하여 기본 레이아웃의 변경도 가능하다. 분석을 위한 자기만의 환경설정이 마무리되었다면, 실제 네트워크 상에서 흘러 다니는 패킷을 캡쳐 해 보도록 한다. 메인 메뉴의 Capture->Start (Ctrl+ K)를 클릭하면 [그림2]와 같이 패킷 캡쳐를 시작하기 위한 기본적인 정보를 물어온다.



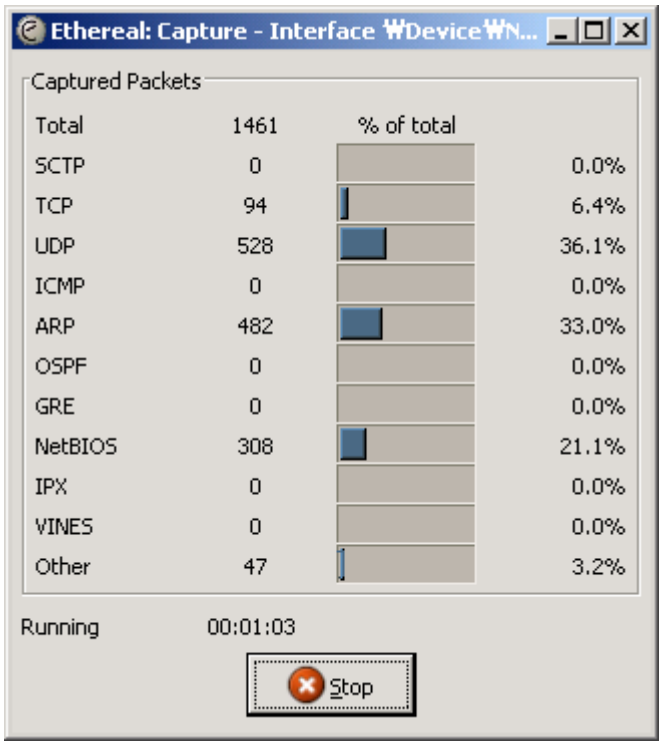
[그림2] 패킷 캡쳐 시작을 위한 옵션

- Interface
  패킷 캡쳐를 할 네트워크 인터페이스를 선택
- Capture Filter
  모든 내용을 캡쳐하는 것이 아니라 정의된 필터에 따른 패킷만 캡쳐
  e.g) port 17333 : 포트번호가 17333인 패킷을 캡쳐
- Capture File
  패킷 덤프한 내용을 저장. 캡쳐를 진행한 후에도 전체 또는 부분적인 저장도 가능
- Display Options
  - Update list of packets in real time
  실시간으로 캡쳐되는 내용을 봄
  - Automatic scrolling in live capture
  실시간으로 캡쳐되는 내용이 자동으로 스크롤

◆ Stop Capture

패킷 개수, 데이터 사이즈, 시간을 지정하여 패킷 캡쳐를 정의된 값에 따라 중지

패킷 캡쳐를 시작하기 위한 옵션들을 지정해 주고 시작하게 되면 [그림3]과 같은 캡쳐 정보를 볼 수 있다. 화면의 예시에서는 TCP(Transmission Control Protocol)의 사용보다도 UDP(User Datagram Protocol)와 ARP(Address Resolution Protocol)의 패킷이 각 30% 이상으로 전체에서 차지하는 비중이 크게 나타나고 있다.[1]

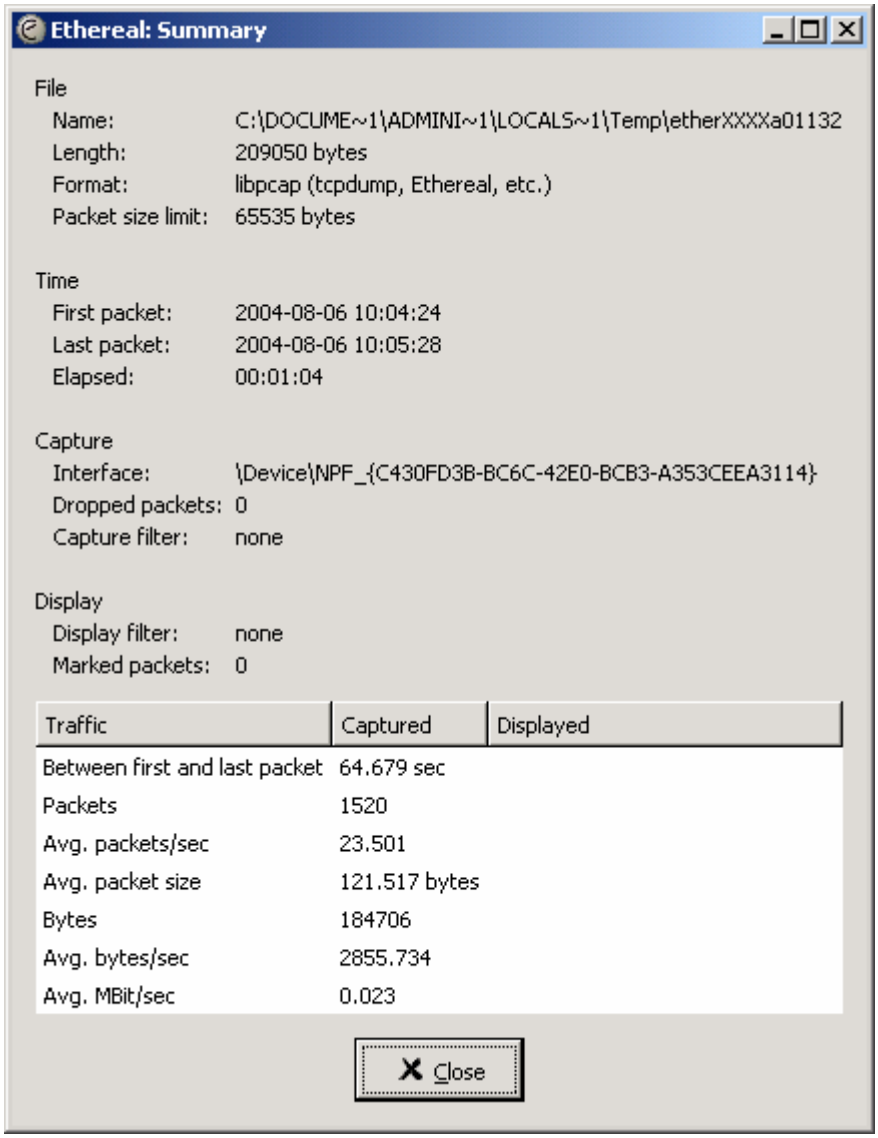


[그림3] 패킷 캡쳐 정보

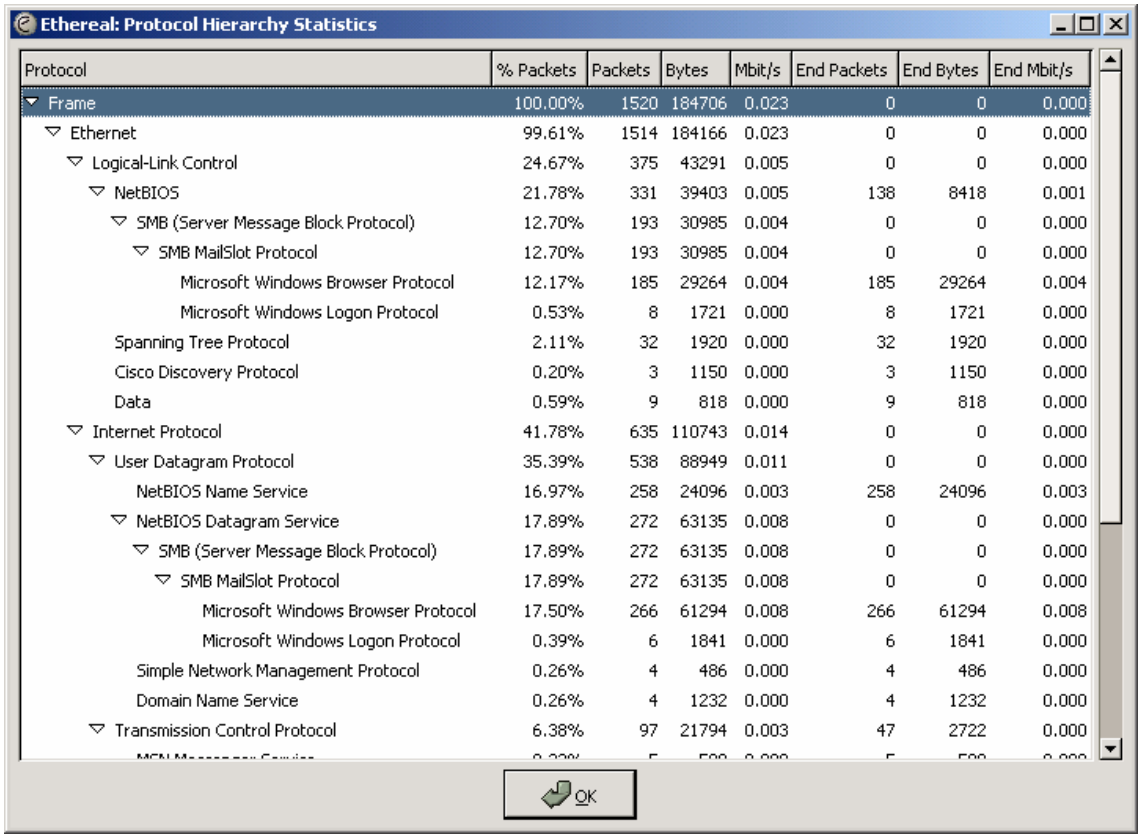
캡쳐된 데이터의 내용이 많은 경우에는 패킷을 모두 분석하는데 어려움을 겪게 된다. 하지만, 네트워크에 문제가 발생하였을 경우 빠르게 원인 분석을 하여 문제를 찾을 수 있어야 한다. 예를 들어, 웜에 의해 감염된 컴퓨터가 전체 내부 네트워크를 마비시키고 있다면 무엇보다도 감염된 시스템을 찾아내는 것이 급선무 일 것이다. 그렇다면 이런 경우에 효과적인 방법이 상세분석에 앞서 요약된 정보를 최대한 이용하는 것이다. 이더리얼의 메인 메뉴중의 하나로 'Statistics'가 바로 이러한 역할을 담당하게 되는데, 분석하는데 있어 많은 도움을 주게 되는 기능 중의 하나이다. Summary, Protocol Hierarchy, Conversations 등의 기능을 이용하게

[1] 기업의 많은 네트워크 환경이 스위치(Switch)장비를 이용하고 있어 해당 네트워크 대역의 모든 내용을 캡쳐하기 위해서는 스위치에서 제공하는 미러링포트(Mirroring Port)를 이용하면 된다.

되면 기본적인 정보를 파악하는데 있어 유용한 기능들이다. [그림4], [그림5]는 캡쳐된 요약 정보와 프로토콜 별 상태 정보를 보여주고 있다. 초당 평균 23개의 패킷 전달이 이뤄졌고, 전체적으로 보면 184,706바이트 크기이다. 전체 프로토콜 중 TCP가 6.38%, UDP 35.39%를 차지하고 있다.

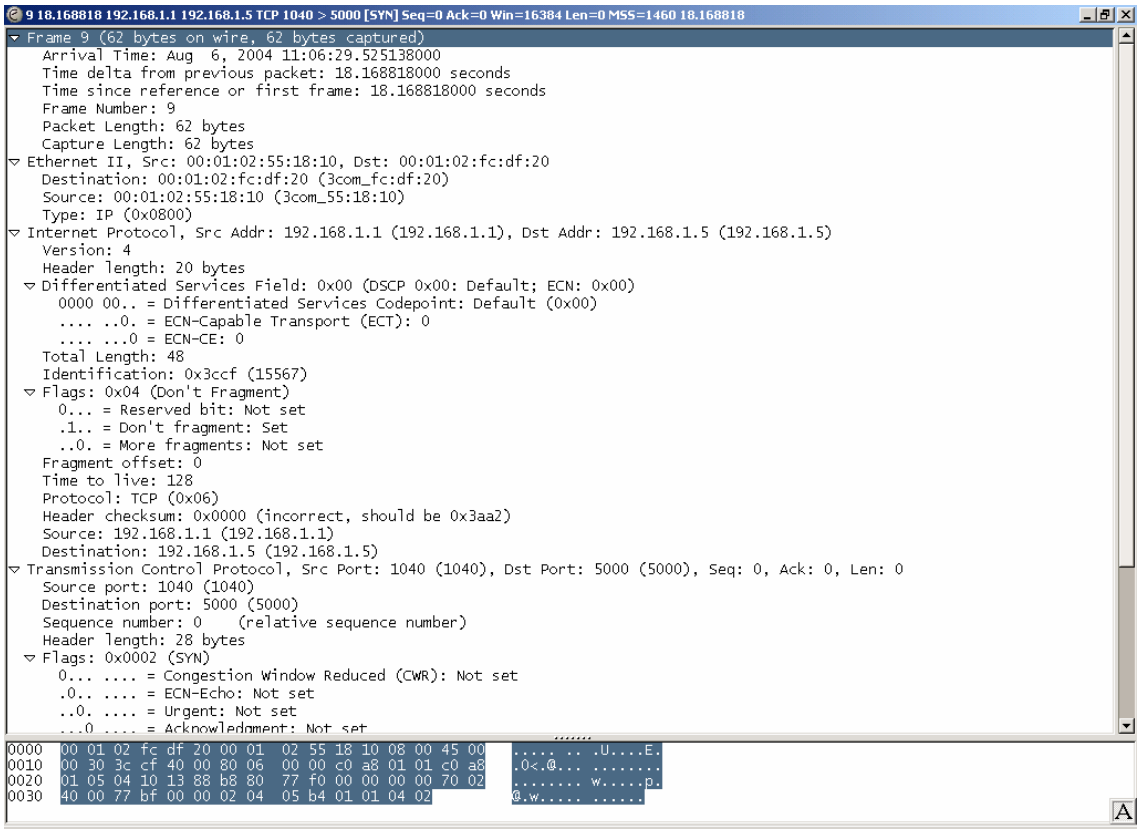


[그림4] 캡쳐 정보 요약 화면



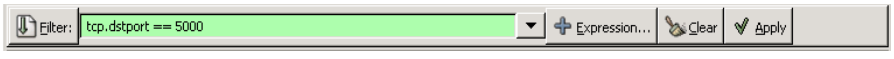
[그림 5] 프로토콜 별 요약 정보

캡쳐된 패킷의 형태를 파악하였으면 사전에 판단된 요약정보를 기준으로 각 패킷의 상세분석을 시도하게 된다. 캡쳐된 패킷에는 모든 내용들이 다 기록되기 때문에 정상적인 패킷 내용들 또한 상당히 많이 존재하게 되므로, 여러 패킷 중에서 사전에 파악한 정보를 기준으로 분석을 하게 되면 빠르게 시작할 수 있다. [그림6]은 특정 패킷의 상세 내용을 살펴본 것으로 192.168.1.1에서 192.168.1.5의 5000번 포트로 접속을 시도한 내용이다. 총 62바이트로 출발지, 목적지의 MAC 주소와 Flags, Checksum, Sequence, Port 정보 등 TCP 패킷 포맷에 따라 한눈에 쉽게 보여주고 있다. 패킷을 세부적으로 분석하기 위해서는 OSI 모델, TCP, IP 패킷 포맷 및 통신 방법에 대해서 이해하고 있어야 한다. 본 고에서는 이러한 내용을 모두 다 언급할 수는 없으므로 2회차 연재에서 프로토콜 포맷과 이더리얼의 상세 화면을 비교하여 이해를 돕고자 한다.



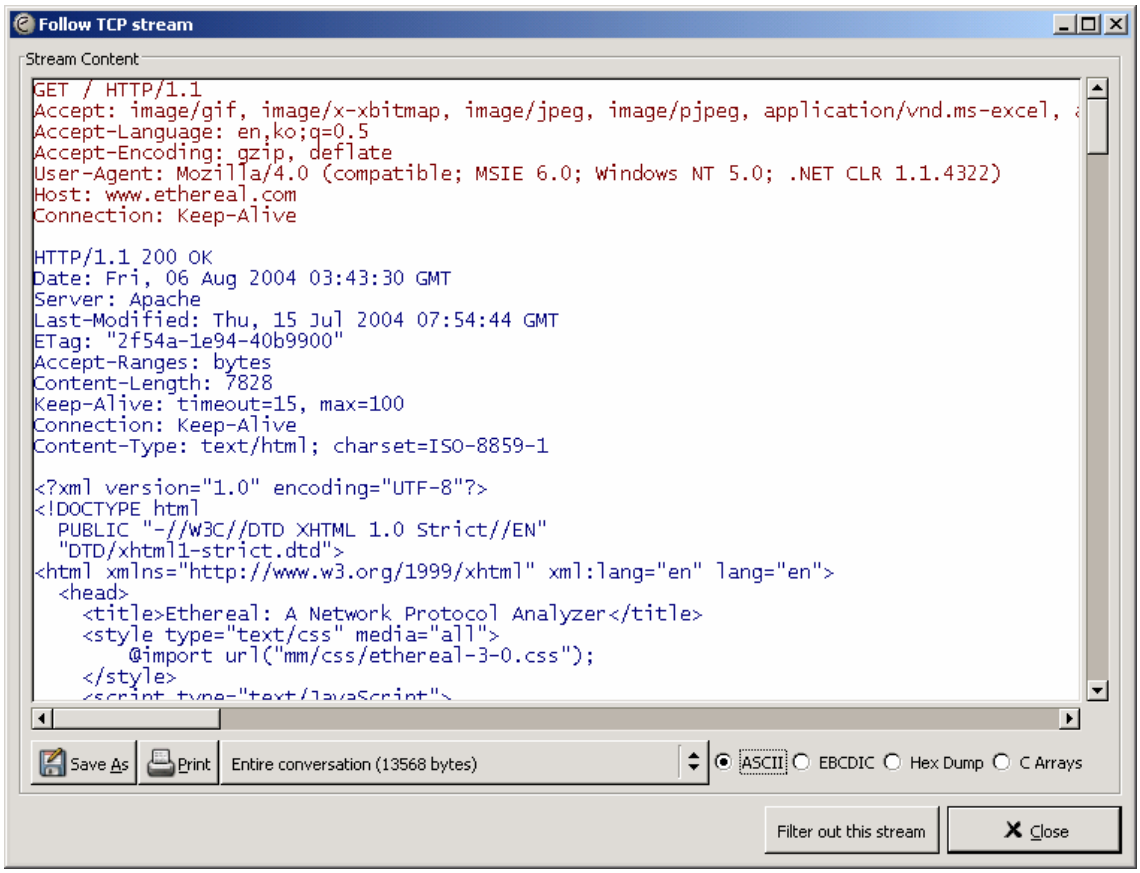
[그림6] 패킷 분석 상세화면

분석 시에 또 하나 유용하게 사용할 수 있는 기능이 필터 기능이다. 필터기능은 크게 캡쳐 시에 사용하는 캡쳐용 필터와 디스플레이 필터로 나뉜다. 디스플레이 필터는 캡쳐된 내용을 기준으로 필터를 적용하여 원하는 내용의 패킷만을 선별하여 볼 수 있기 때문에 분석시 많은 도움이 된다. [그림7]은 'tcp.dstport == 5000'이라는 필터를 적용한 화면 예시이다. 이 뜻은 TCP 프로토콜 목적지 포트번호가 5000번인 것만을 화면에 보여달라는 것이다. 규칙을 알면 바로 입력할 수도 있지만 모른다고 해서 걱정할 필요는 없다. 우측의 Expression을 누르면 마우스 클릭을 통하여 룰을 만들 수 있도록 되어 있고, 좌측의 Filter는 룰 이름을 만들어 지속적으로 사용할 수 있도록 도와준다. 또는 상세분석 화면에서 해당하는 라인의 필드에서 마우스 오른쪽을 클릭하면 필터로 바로 적용하는 룰 등의 더욱 편리한 기능들이 있다.



[그림7] Quick Display Filter

이외에 TCP 프로토콜을 이용하는 경우 'Follow TCP Stream' 기능을 이용해 보도록 하자. [그림8]과 같이 TCP 연결과정을 하나의 화면으로 나타내주어 통신상의 내용을 한눈에 보기 쉽도록 보여준다.



[그림8] Follow TCP Stream

지금까지 분석을 위한 기본도구인 이더리얼의 몇 가지 기능에 대해서 알아보았다. 이더리얼은 패킷 분석도구로써 훌륭한 프로그램이다. 필자가 여기서 언급한 기능 이외에도 분석 시에 편리하게 이용할 수 있는 다양한 기능들이 있다. 앞으로 남은 연재에서 필요 시마다 유용한 기능들을 소개하며 분석을 같이 진행하도록 하겠다.

이번 호에서 다룬 내용은 패킷 분석을 시작하기 위한 준비단계였다면 다음 호는 사용자 스스로 위협 트래픽을 탐지하고 판단하여 문제를 해결할 수 있는 방안을 알아보도록 하겠다.