ASEC Report 8월

® ASEC Report

2004. 9

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 피해 다소 감소, 다운로더 변형 발견 증가…

IRCBot 웜 변형 출현의 감소와 휴가시즌으로 인한 사용자 감소로 인해 8월은 악성코드로 인한 피해가 지난달에 비해 다소 감소하는 추세를 보였다. 그러나 감소한 피해신고 추세속에서도 피해신고 Top 10 중 7개가 넷스카이 웜 변형에 의한 것일만큼 Mass Mailer 에 의한 피해는 여전하였으며, 이는 일본과 중국도 마찬가지의 경향을 보였다. 8월에는 새로이 발견된 신종(변형 포함)이 전반적으로 감소하는 추세를 보이는 가운데, 트로이목마류 특히 다운로더(Downloader)가 다소 증가하는 특징을 보였다.

8월에는 1개의 MS 취약점에 대한 패치와 윈도우 XP 서비스팩 2가 발표되었다. 특히 윈도우 XP 서비스팩 2는 보안정책이 강화된 것이어어서 주목을 받았다.

이번호에서는 개인정보 유출과 광고창 팝업, 인터넷 익스플로러 초기페이지 고정 등의 증상으로 많은 사용자들에게 피해 아닌 피해를 입히고 있는 스파이웨어의 위험성과 과장, 그리고 비정상적인 유해트래픽의 탐지와 판단을 하기 위한 방법에 대해 테크니컬 컬럼에서 살펴보았다.

I. 8월 악성코드 피해 Top 10

작성자 : 최동균 연구원(cdk@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	1,367	18.8%
2	-	Win32/Netsky.worm.17424	719	9.9%
3	-	Win32/Dumaru.worm.9234	626	8.6%
4	-	Win32/Netsky.worm.28008	621	8.5%
5	-	Win32/Netsky.worm.17920	467	6.4%
6	-	Win32/Bagle.worm.Z	351	4.8%
7	-	Win32/Netsky.worm.22016	326	4.5%
8	2↑	Win32/Netsky.worm.16896.B	207	2.8%
9	1↑	Win32/Sasser.worm.15872	190	2.6%
10	2↓	Win32/Netsky.worm.25352	156	2.1%
		기 타	2,254	30.9%
합 계			7,284	100%

[표1] 2004년 8월 악성코드 피해 Top 10

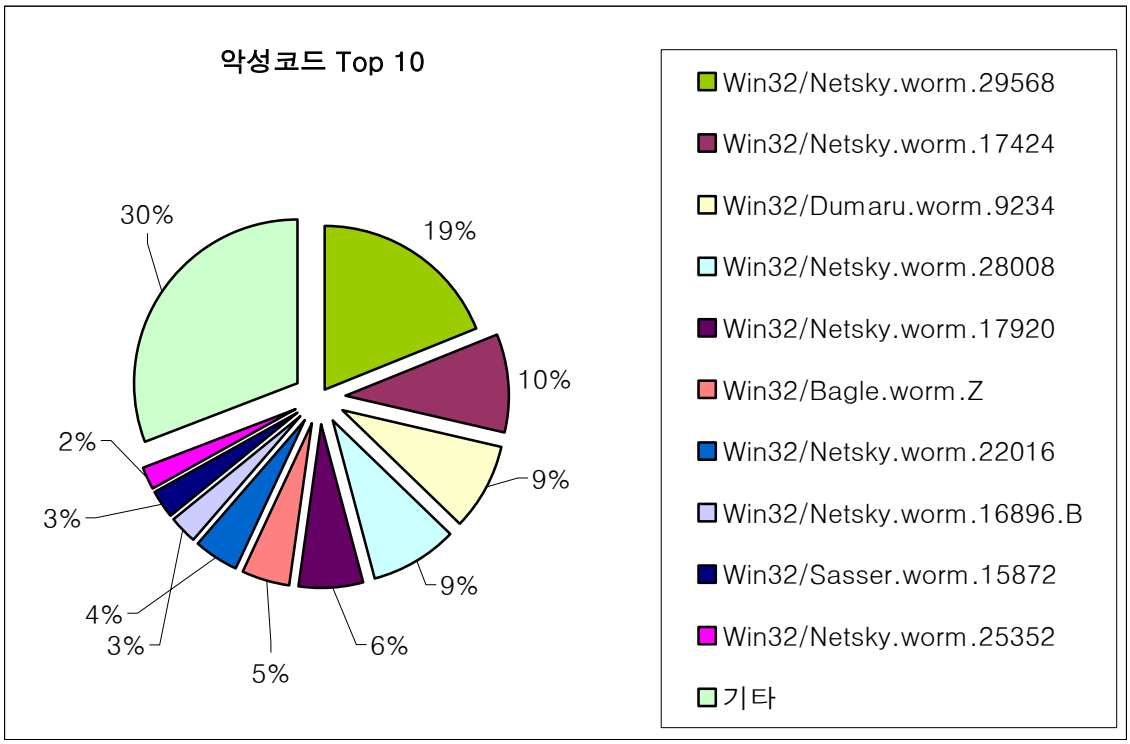
8월 악성코드 피해동향

8월 악성코드 피해동향은 지난 달에 많은 감염 피해를 가져다 준 Win32/Netsky.worm.29568(이하 넷스카이.29568 웜)의 피해감소로 인해 전반적인 감염 피해수치가 낮아졌다. 하지만 이번 달 역시 감염 피해 비중은 메일을 이용하여 전파되는 Mass Mailer에 의한 것이 많았다. 이와 같은 결과를 반영하듯 8월 악성코드 피해 Top 10 중 9건이 메일을 감염 전파 경로로 사용하였으며, 그 중 Win32/Netsky.worm(이하 넷스카이 웜)의 변형은 Top 10 리스트에서 7건을 차지하고 있다. 3월경 최초 발견된 넷스카이 웜은 현재까지 40여종 이상의 수많은 변종이 발견 보고 되었으며, 이러한 수치는 과거 사용자들의 시스템에 많은 피해를 입힌 Win32/Yaha.worm(이하 야하 웜)과 유사한 수치라 하겠다.

또한 월별 악성코드 Top 10에서 윈도우 보안 취약점(MS04-011) [1] 을 악용한 Win32/Sasser.worm(새서 웜)이 순위내에 지속적으로 포함되는 것으로 보아 윈도우 보안 취약점에 노출되어 있는 사용자 시스템이 여전히 상당수 존재함을 알수 있다.

8월의 악성코드 Top 10을 도표로 나타내면 [그림1]과 같다.

[1] http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

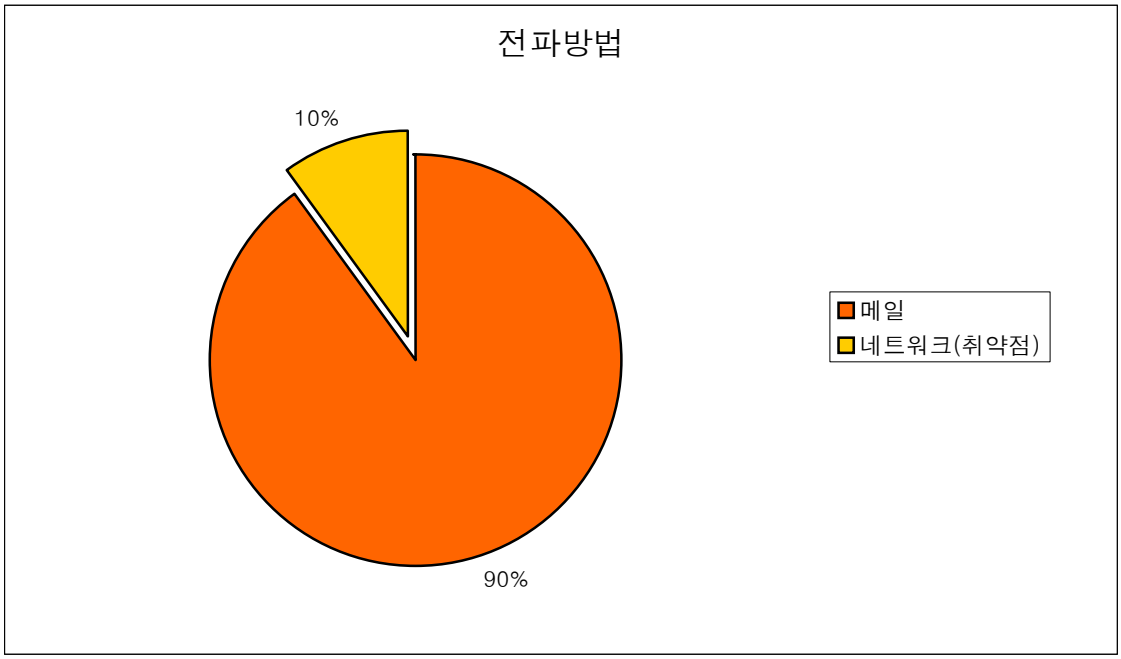


[그림1] 2004년 8월 악성코드 Top 10

과거의 Mass Mailer는 감염 메일의 시간당 전송 단위 량이 무차별적으로 발송되어 시스템 자원소모 및 네트워크 트래픽을 발생하는 특징이 있었으나, 최근의 Mass Mailer는 특정 시간대에 한정된 감염 메일을 발송하는 유형이 많아 사용자 및 네트워크 관리자가 해당 시스템이 감염된 사실을 알아 차릴 수 없는 특징이 있다.

8월 악성코드 Top 10 의 전파방법 유형별 현황

[표1]의 악성코드 Top 10은 주로 어떠한 감염 경로를 가지고 있는지 [그림2]에서 확인해 보기로 한다.

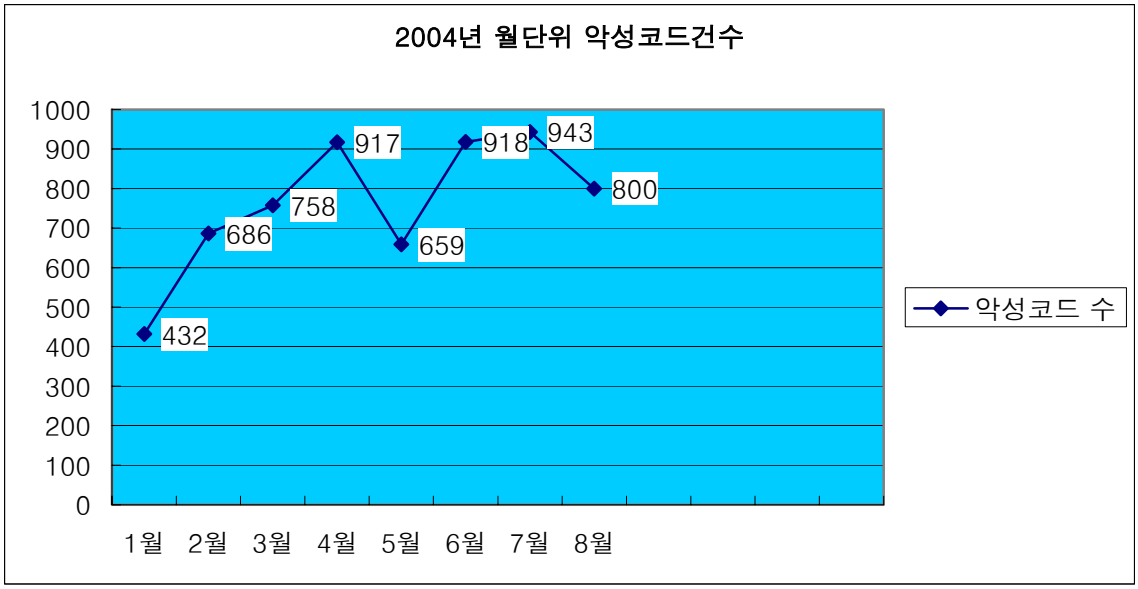


[그림2] 악성코드 Top 10 의 전파방법 및 유형별 현황

위에서 언급한 것처럼 악성코드가 이용하는 전파방법의 대다수가 이메일을 이용하였으며, 이는 지난달과 비슷한 동향으로써 구종 및 신종의 Mass Mailer에 의한 피해가 여전히 수위를 차지하고 있음을 보여주고 있다.

월별 피해신고 악성코드 수 현황

8월에 피해 신고된 악성 코드는 역대 최고 피해신고 수치를 기록한 7월에 비해 상대적으로 감소한 것을 알 수 있다.

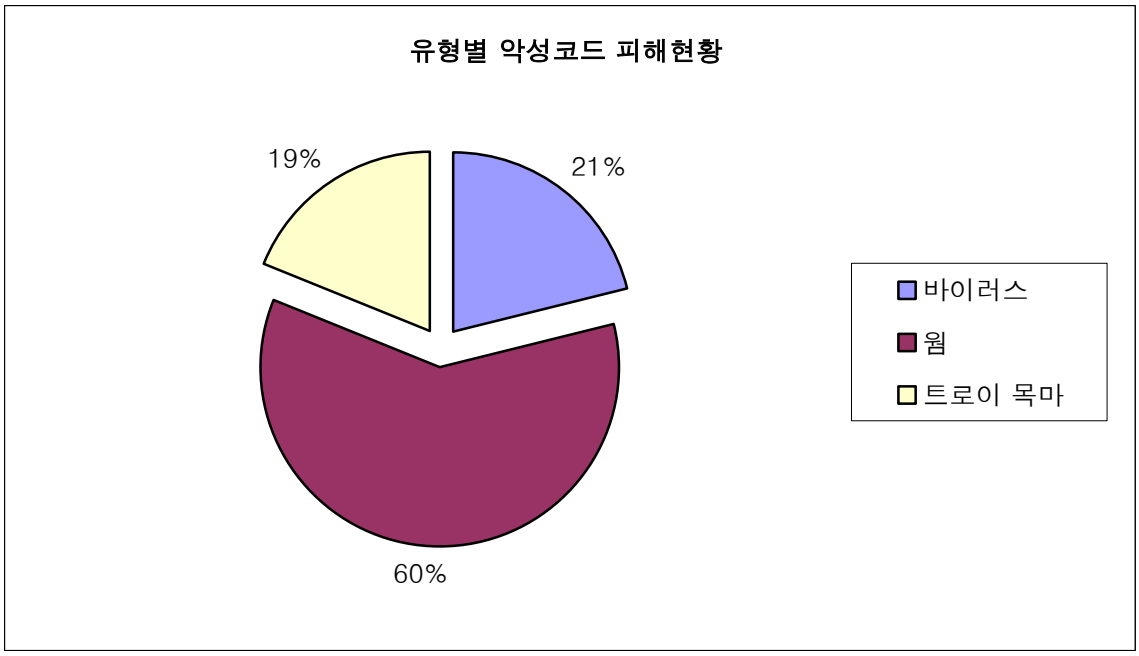


[그림3] 2004년 월별 피해신고 악성코드 수

8월의 피해신고 악성코드 수가 감소한 것은 지난 달 피해신고 접수건과 비교하였을 때 Win32/IRCBot.worm 변형의 출현이 상대적으로 감소하였으며, 더불어 8월 휴가철 특성에 기인하여 감소한 것으로 추정된다.

유형별 악성코드 피해 현황

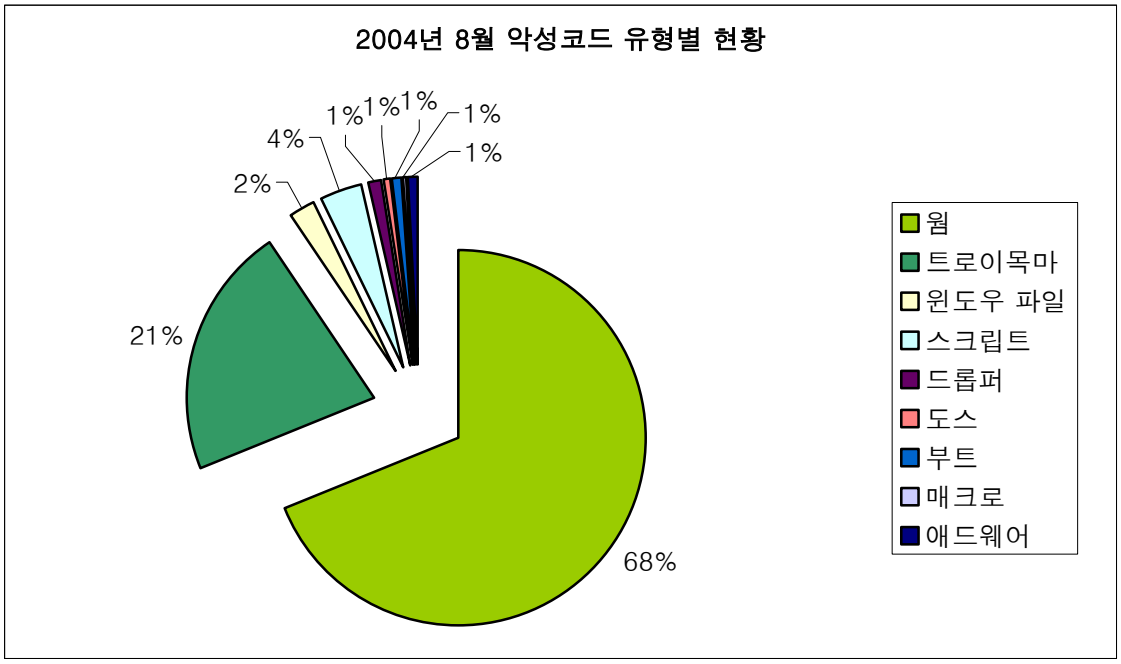
8월에 피해 신고된 악성코드 중 피해신고가 3건 이상 접수된 악성코드를 유형별로 분류하면 [그림4]와 같다.



[그림4] 2004년 8월 악성코드 유형별 현황 (피해신고 3건 이상)

8월 악성코드 유형 중 웜이 대다수를 차지하였으며, 바이러스 유형은 과거 발견된 구종의 바이러스가 계속 활동하고 있다.

8월 중 안철수연구소를 통해 피해신고 접수된 악성코드 유형을 [그림5]에서 확인할 수 있다.



[그림5] 2004년 8월 악성코드 유형별 현황

8월의 악성코드 피해 동향은 유기적으로 구축된 네트워크 인프라를 감염 전파경로로 택한 Mass Mailer 및 IRCBot 류의 활동이 왕성했다. 이는 최초 감염부터 확산까지의 소요 시간이 최단시간 내에 이루어진다는 특징에 기인한 결과라 할 수 있다.

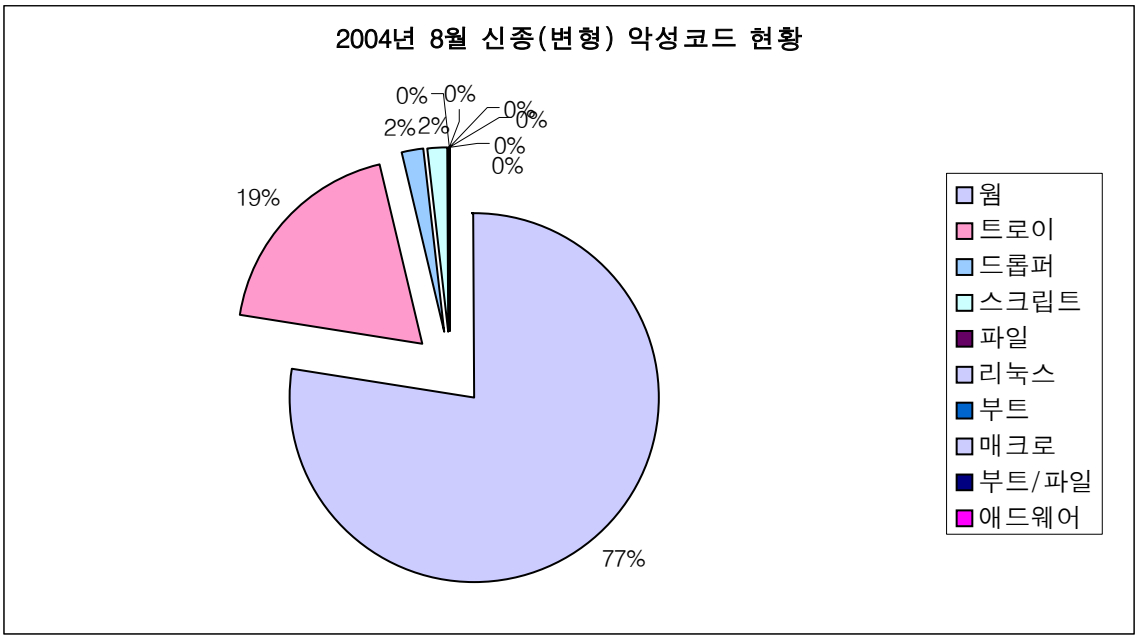
II. 8월 국내 신종 악성코드 발견 동향

작성자 : 정진성 연구원(jsjung@ahnlab.com)

8월 한달 동안 접수된 신종(변형) 악성코드의 건수는 [표1], [그림1]과 같다.

웜	트로이	드롭퍼	스크립트	파일	리눅스	부트	매크로	부트/파일	애드웨어	합계
358	87	9	8	0	0	0	0	0	0	462

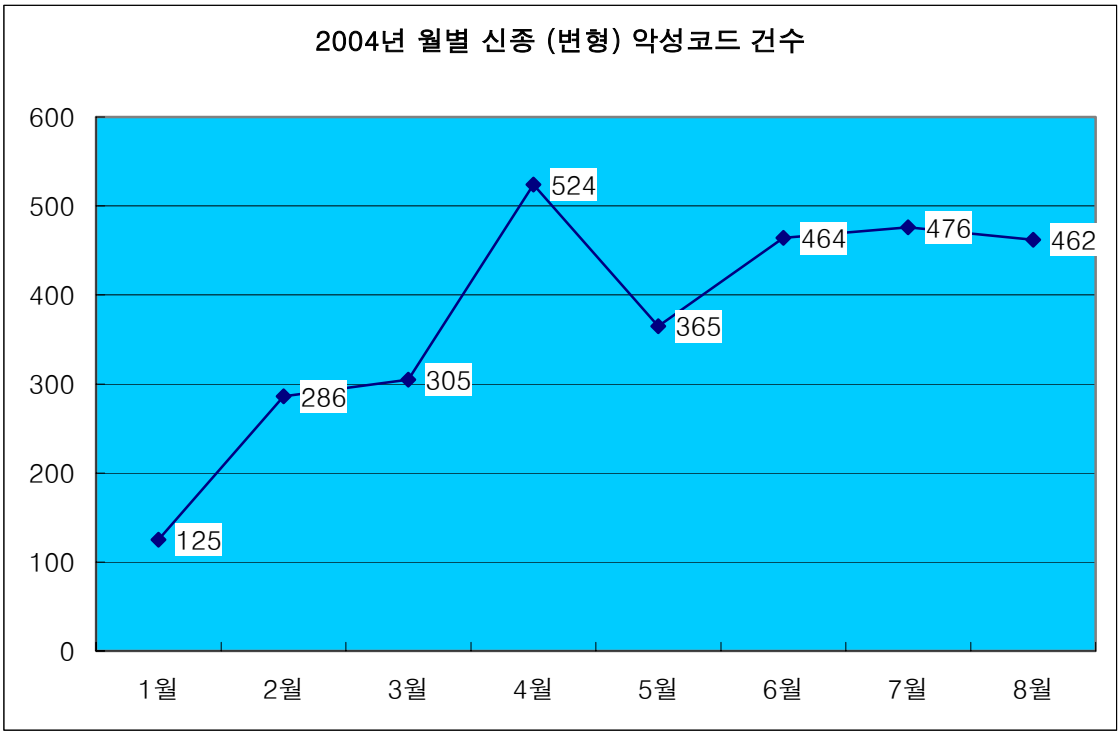
[표1] 2004년 8월 유형별 신종 (변형) 악성코드 발견현황



[그림1] 2004년 8월 신종 악성코드 발견현황

8월 신종 악성코드 동향

8월에 발견된 신종(변형) 악성코드는 462건으로 7월과 비교하여 10여건 정도 낮은 수치이지만, 악성 IRCBot 웜은 여전히 많은 발견건수를 보이고 있고, 트로이목마류가 지난달과 비교하여 조금 증가하였다. 트로이목마 중에서는 다운로더라고(Downloader) 불리우는 유형이 증가하였다. 또한 드롭퍼(Dropper)류는 지난달과 비슷한 발견건수를 보였다. 메일로 전파되는 웜은 Win32/Bagle.worm(이하 베이글 웜), Win32/MyDoom.worm(이하 마이둠 웜) Win32/LovGate.worm(이하 러브게이트 웜) 변형들이 발견, 보고 되었다. 베이글 웜 변형의 경우 웜 자신이 아닌 트로이목마를 첨부하여 전파하는 형태가 발견되었다.



[그림2] 2004년 월별 신종(변형) 악성코드 발견 현황

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

▶ Win-Trojan/Bagle.14848, Win-Trojan/Bagle.12800

이 트로이목마는 베이글 웜 변형이 메일에 첨부한 형태로 유포되었다. 즉, 메일에 웜 자신이 첨부된 형태가 아니라 웜을 다운로드 받을 수 있는 트로이목마를 메일에 첨부한 형태로, 웜이 업로드된 호스트가 폐쇄되어 이 트로이목마가 확산되는 것을 쉽게 차단할 수 있었다.

이 트로이목마는 자신을 Explorer.exe의 한 쓰레드(Thread)로 동작하도록 한다. 이렇게 되면 트로이목마가 하는 모든 동작은 Explorer.exe에 의한 것으로 표시되기 때문에 사용자들이 눈치채기가 어렵다. 트로이목마는 수십개에 이르는 호스트들 중 하나에서 웜을 다운로드 받아서 실행한다. 이러한 동작은 최초 실행 후 10시간 그리고 변형은 6시간마다 반복된다. 알려진 보안관련 응용 프로그램의 프로세스를 강제 종료하는 증상도 있으며, 최근에 발견된 변형인 Win-Trojan/Bagle.12800은 윈도우 XP(SP2)의 방화벽 기능을 Off하는 증상도 있었다. MS가 윈도우 XP SP2의 방화벽 기능을 향상시킴에 따라 이를 무력화 또는 우회하려는 악성코드의 공격이 증가할 것으로 예상된다.

▶ Win-Trojan/Agent.57344

이 트로이목마는 국내에서는 8월에 많은 발견 보고가 있었다. 하지만 그 이전부터 확산된 것으로 추정된다. 이 트로이목마의 감염경로는 인터넷 익스플로러의 취약점을 이용한 것으로

추정된다. 즉, 사용자가 악의적인 웹사이트에 방문하면 보안패치가 되어 있지 않은 인터넷 익스플로러는 트로이목마의 모듈을 로컬 드라이브에 다운로드 하고 다음번 부팅시마다 자동 실행되도록 레지스트리에 자신을 추가하는 형태로 감염되는 것으로 보인다.
이 트로이목마는 무려 60개가 넘는 API를 후킹하고 있으며 후킹된 API가 일부 응용 프로그램에서 사용중이라면 충돌하는 현상이 발생한다. 그리고 USER32.DLL 모듈을 사용하는 응용 프로그램이 실행될 때 마다 해당 프로세스에 자신의 모듈을 삽입(Injection)하는 형태이다.
이 트로이목마는 다음과 같은 증상이 있다.

- 특정 응용 프로그램의 실행을 방해 (프로세스 뷰어 관련 툴등..)
- 특정 디버거 실행 및 파일들을 감지 및 트로이목마 은폐기능 동작하지 않음
- 윈도우 특정 로컬 드라이브에 경로 획득
- 일반적인 시스템 정보를 획득
- 트로이목마 모듈을 Lock 하여 삭제되지 않음
- 트로이목마는 다수의 API 를 후킹하여 위와 같은 동작을 수행한다.

또한 치료하는데 있어서 다소 번거로운 형태로, 치료를 위해서는 재부팅이 반드시 필요하다.

▶ Win-Trojan/Downloader.xxxxx

Win-Trojan/Downloader.(이하 다운로더)는 매우 일반적인 진단명으로 특정 호스트에 업로드된 악의적인 증상이 있는 파일을 다운로드하는 형태를 일컫는다. 8월에는 6종의 다운로더가 발견되었다. 대부분 애드웨어를 다운로드하는 형태로 알려졌다.

▶ T-Virus Hoax

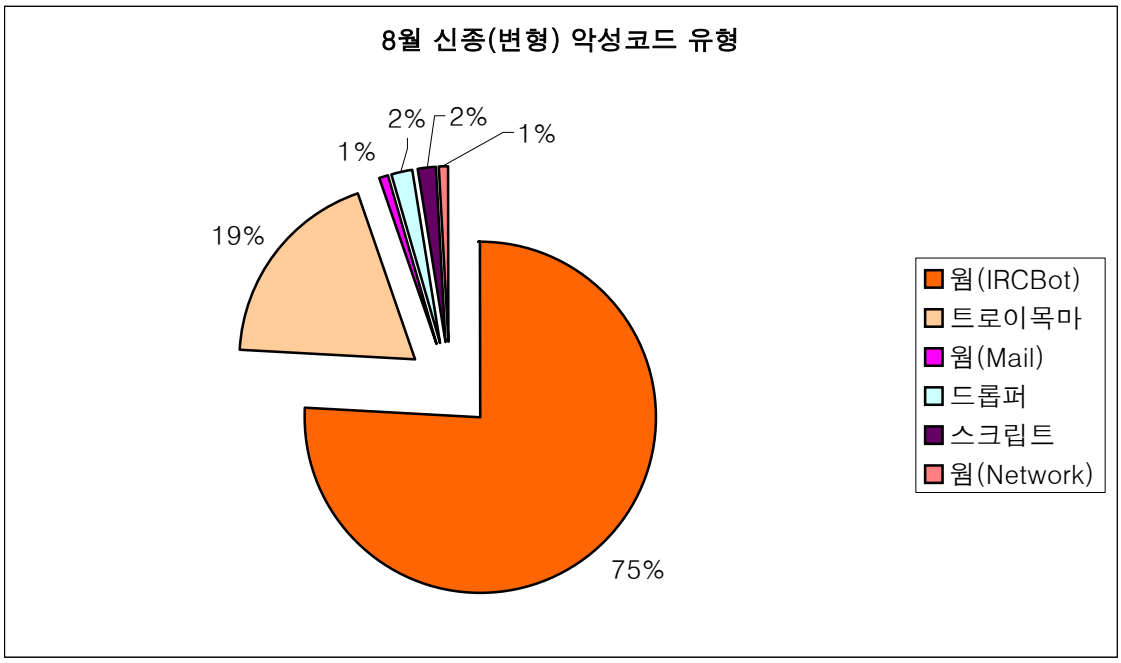
휴대폰 및 PDA와 같은 모바일기기에 대한 보안위협이 커지고 있는 요즘, 영국에서 특정 게임에 대한 홍보를 목적으로 한 단문문자메시지 서비스가 실제 휴대폰의 악성코드로 오인되는 해프닝이 있었다. 홈페이지내에서 사람들끼리 휴대폰을 이용하여 보낸 단문문자메시지 내용이 마치 휴대폰에 악성코드가 감염된 것처럼 오인하는 소동이 있었던 것이다. 모바일 기기에 대한 보안위협이 커지고 있는 시점에서 나온 Hoax(가짜 바이러스)라서 외신을 통해 언론에 보도가 되었다.

▶ Win32/MyDoom.worm.27136

마이둠 웜 변형으로 메일전파 기능 이외에 특정 호스트에서 트로이목마를 다운로드 받아오는 기능이 있다. 다운받아진 트로이목마는 메일 릴레이 및 HTTP 프록시 증상을 가지고 있는 형태이다. 또한 트로이목마는 은폐기능이 있어 자신의 서비스와 파일 등을 숨기고, 특정 웹 사이트에 대한 접속을 하지 못하도록 방해한다.

유형별 신종(변형)악성코드 현황

다음은 8월 발견된 신종(변형) 악성코드의 유형별 현황이다.

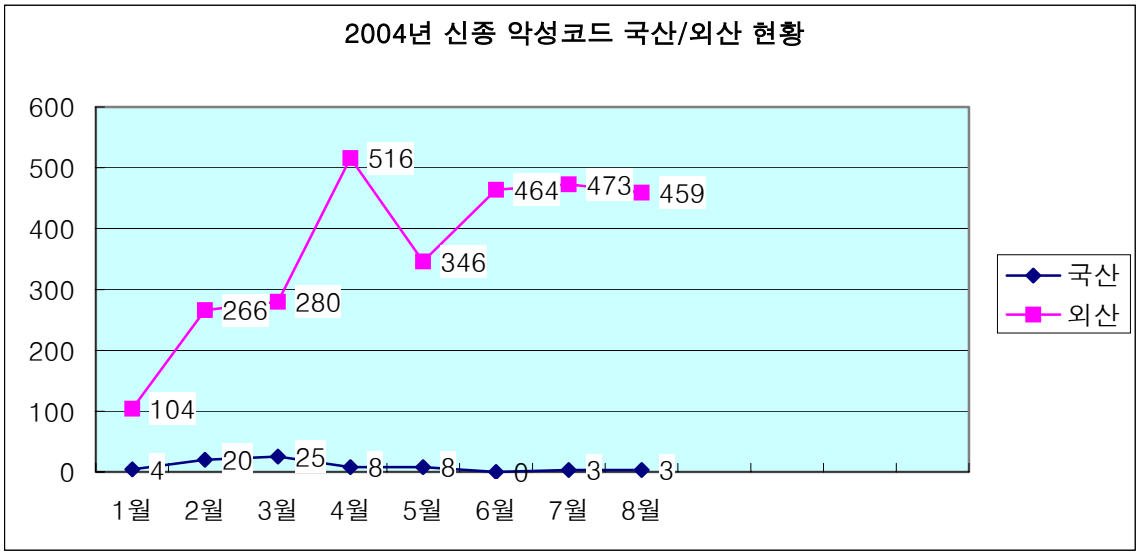


[그림3] 8월 신종(변형) 악성코드 유형별 현황

트로이목마류가 지난달에 비하여 2%정도 증가하였다. 발견된 트로이목마들은 주로 다운로더와 FTP 데몬, 악의적인 애드웨어류, 전형적인 백도어 등이다. 트로이목마들은 자체 확산력은 없지만 관리목적 공유폴더를 이용해서 전파되는 드롭퍼류에 포함되어 발견된 경우가 더러 있었다. 메일로 전파되는 유형은 단 2종류로, 베이글 웜과 러브게이트 웜 변형들이였다. 그리고 드롭퍼는 mIRCPack 형태가 많았다.

제작지별 신종(변형) 악성코드 현황

다음은 신종(변형) 악성코드들의 국산/외산 현황이다.



[그림4] 2004년 제작지별 신종 악성코드 현황

8월은 스파이웨어 및 애드웨어에 대한 관심이 높아진 달이다. 일부 사이트에서 제공하는 진단/치료 프로그램이 진단 범위와 위험등급에 대한 문제로 매스컴 등에 보도되어 사용자들에게 정확한 알 권리를 인지시켜 주지 못한 것이 문제가 되었다. 8월에 발견된 국산 악성코드 3종 역시 애드웨어이지만 특정 사이트에 접속하지 못하게 하는 증상이 있어 트로이목마로 분류되었다.

지난 Report 끝맺음과 같은 얘기를 다시 강조하고 싶다. 스파이웨어 또는 애드웨어에 대한 궁금증이 높아진 요즘 반드시 이에 대한 정확한 정의와 대응 방법을 알고 있다면 대처하는데 별다른 오해나 어려움은 없다. 그러므로 이를 이용하는 사용자들은 반드시 신뢰할 수 있는 정보를 주는 사이트에서 관련 내용이나 진단/치료 툴을 비교해 보는 등 꼼꼼히 선택하는 것이 중요하다.

III. 8월 신규 보안취약점

작성자 : 이정형 연구원(jungh@ahnlab.com)

8월에는 1개의 마이크로소프트 정기보안 패치 발표와 윈도우 XP Serivce Pack2의 발표소식이 있었다(한글버젼은 9월출시예정).

Exchange Server 5.5 OWA(Outlook Web Access) 스크립팅 취약점(MS04-026)[1]

아웃룩 웹 액세스(Outlook Web Access)는 MS 익스체인지 서버(Microsoft Exchange Server)의 메일을 인터넷(웹)상에서 사용할 수 있도록 지원해 주는 서비스로, 이 서비스에서 사이트 간 스크립팅(Cross-Site Scriping), 스푸핑(Spoofing) 취약점이 발견되었다.

이 취약점을 이용하면 외부에서 악의적인 스크립트가 포함된 메일을 해당 사용자에게 보내 악성 스크립트를 실행하도록 할 수 있다. 공격이 성공하면 개인 사용자가 액세스할 수 있는 아웃룩 웹 액세스 서버의 모든 데이터에 액세스할 수 있고, 웹 브라우저 캐시 및 중간 프록시 서버 캐시를 변경할 수 있으며 이러한 캐시에 스푸핑된 콘텐츠를 저장할 수 있다. 또한 사이트 간 스크립팅 공격을 수행할 수도 있다. 이 취약점은 MS 익스체인지 서버 5.5 SP4에만 해당된다

현재 직접적으로 공격에 악용된 사례는 알려지지 않았지만, 외부에서 메일을 이용한 공격이 가능하므로 보안 패치를 적용하도록 한다.

Windows XP Service Pack 2 발표[2]

지난달 마이크로소프트사(Microsoft)의 향상된 보안정책이 적용된 윈도우 XP 서비스팩 2가 발표 되었다. 이번 서비스팩2에서 크게 변경된 내용은 아래와 같다.

1. 네트워크 보안강화

기존 XP의 ICF (Internet Connection Firewall)의 기능이 개선되어, 블래스터 웜과 같은 네트워크 기반의 공격에 대해서 더 나은 방어를 할 수 있도록 해준다. 이번에 개선된 주요 특징은 다음과 같다.

- 설치 후 default로 작동
- 사용되지 않는 포트 차단 (local에서 명시적으로 open해 놓지 않은 포트로 들어오는 패킷을 자동 차단)
- UI 개선
- 응용 프로그램과의 충돌 최소화

[1] http://www.microsoft.com/korea/technet/security/bulletin/MS04-026.mspx

[2] http://www.microsoft.com/windowsxp/sp2/preinstall.mspx
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx

- Group Policy를 통한 전사적인 ICF 정책관리 (Active Directory 구조를 기반으로 함)

2. 메모리 보안강화

마이크로프로세스(CPU) 레벨에서 버퍼오버런 [1] 공격을 막는 DEP(Data Execution Prevention) 기술이 적용되었다. 그러나 현재 적용되는 CPU는 NXE bit (No-EXecute)가 지원되는 AMD의 옵테론(64bit CPU)계열과 이번에 출시된 인텔의 펜티엄4F 프로세스이다. VIA는 에스터(사이릭스 4)에 이 기능을 지원할 예정이다. 참고로, 버퍼오버런은 기본적으로 데이터 부분이 넘쳐서 코드처럼 실행되는 원리에 기반하고 있기 때문에 이런 feature가 하드웨어적으로 구현된다면 악성 코드가 실행되는 것은 더욱 어려워 질 것이다.

3. 브라우저 보안강화

웹상의 악성 컨텐츠를 차단할 수 있는 보안 기능이다. 웹에서 유해한 파일을 다운로드 받거나 악성 스크립트가 수행되는 것을 브라우저 레벨에서 차단한다. 요즈음 개인 사용자들이 많이 겪는 문제인 팝업창(광고창 등)방지와 악성 스크립트 방지(ActiveX 등) 기능을 지원한다.

4. 이메일 보안강화

Win32/Sobig.worm.F(소빅.F 웜)처럼 이메일이나 메신저를 통해 확산되는 바이러스를 차단하는 보안 기술이다. 이 기술은 아웃룩 익스프레스(Outlook Express)나 윈도우 메신저의 보안 수준을 강화하여, 안전하지 못한 첨부파일이 다른 시스템에 영향을 줄 수 없도록 안전하게 격리시킨다.

5. 업데이트 기능강화

최신 소프트웨어를 업데이트시켜 컴퓨터를 항상 최신으로 유지해 주는 기능으로, 보안에 있어 매우 중요하다. 또한 최신의 보안 사고나 동향에 대해 정보를 제공한다. 취약점 패치/업데이트에 의해 바이러스나 웜에 의한 공격을 차단하고, 시큐리티 센터라는 것을 통해 보안에 대한 정보를 더욱 쉽게 파악할 수 있도록 하였다.

전체적으로 SP2에는 많은 보안 기능 강화를 통해 악성코드를 어느정도 방지할 것으로 생각되지만, 이런 보안 기능을 무력화시키는 악성코드도 등장할 것으로 보여진다. 실제로 8월에 발견된 Win-Trojan/Bagle.12800에는 SP2의 방화벽을 무력화시키는 기능이 내장되어 있다.

그러나 보안기능이 보다 강화된 윈도우 XP 서비스팩 2는 기업에서 많이 사용되는 애플리케이션들과 하드웨어 에 대한 호환성 문제[2]등이 남아 있어 IBM 등의 기업에서는 아직까지 서

[1] 버퍼오버런 : 악성프로그램등에서 많이 사용되는 임의 실행기법

[2] 안철수연구소의 V3Pro 2004는 Service Pack 2 와의 호환성 문제를 9월 1일 해결하였다. http://info.ahnlab.com/ahnlab/report_view.jsp?num=356

비스팩 2의 사용을 미루고 있다. 업무와 관련된 소프트웨어나, 새로운 하드웨어를 사용하는 계층에서는 서비스팩 2의 사용을 서두르지 말고, 조금 더 지켜보는 것이 좋겠다.
참고로 안철수연구소의 V3Pro 2004 제품은 9월 1일부터 윈도우 XP 서비스팩 2와의 호환성 문제를 해결한 패치파일을 제공[1]하고 있다.

[1] http://info.ahnlab.com/download/patch_list.jsp

Ⅳ. 8월 일본 피해 동향

작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

일본 경찰청은 올해 상반기에 발생한 불법 접근위반 행위와 관련한 통계를 발표하였다. 아래의 [표1]은 경찰청 통계 중 불법접근이 발생한 상황을 처음 인지한 기관에 대한 통계이다.

불법접근 인지단서	2000년	2001년	2002년	2003년	2004년 상반기
관리자로부터의 검출	30	168	47	12	20
접근권한자의 검출	23	118	92	78	85
경찰 활동	35	930	185	100	95
발견자의 통보	7	21	0	19	1
기타	11	16	5	3	2
합계	**106**	**1,253**	**329**	**212**	**198**

[표1] 불법접근 인지 단서 통계 (출처 : 일본 경찰청)

[표1]의 내용 중 관심을 가져볼만 한 사항은 작년과 비교하여 불법 접근이 발생한 횟수가 증가하고 있다는 점이다. 또한 불법접근이 발생한 위기상황을 초기에 인식하는 주체가 변화하고 있다는 점도 주목할 만한 내용이다. 이전에는 경찰과 같은 공공기관에서 주로 불법접근 상황을 인지하던 것에서 관리자나 개인 유저와 같은 직접 사용자에 의해서 발견되는 경우가 증가하고 있다는 사실은 이전에 비해서 일반 사용자들의 보안에 대한 의식이 높아지고 있음을 반증해 준다고 할 수 있다. 내, 외부에서의 불법 접근과 같은 보안 위반 사항이 발생하였을 때 이를 빨리 인지하고 대응하는 것은 피해를 최소화하기 위한 중요한 요소이므로 직접 사용자가 조기에 발견하는 경우가 증가하고 있다는 사실은 정보보호의 측면에서 볼 때 고무적인 현상이라고 할 수 있다.

일본 유행 악성코드 유형별 발생현황

2004년 8월 한달 동안 일본에서 가장 많이 전파된 악성코드는 Win32/Netsky.worm(이하 넷스카이 웜)과 Win32/Bagle.worm(이하 베이글 웜)이다. 이는 전월과 비교하여 크게 차이가 없다.

[표2]는 IPA/ISEC에서 집계한 2004년 8월의 악성코드 노출에 대한 통계자료이다.

전월과 마찬가지로 넷스카이 웜과 베이글 웜 에 노출된 건수가 많음을 알 수 있다.

한가지 주목할만 한 사항은 마이둠 웜의 노출 건수가 전월에 비해서 크게 증가한 것인데, 이는 지난 8월 16일경 발견되어 확산된 새로운 변형 Win32/MyDoom.worm.27136(이하 마이둠.27136 웜)으로 인한 것이다. 새롭게 확산된 마이둠.27136 웜은 감염 경로나 감염시의 위험도 등에 있어서는 이전에 발견된 다른 변형들과 크게 차이가 없으나 매우 많은 양의 감염

메일을 다수에게 지속적으로 발송함으로 인해 사용자들에게 많은 피해를 주었다.

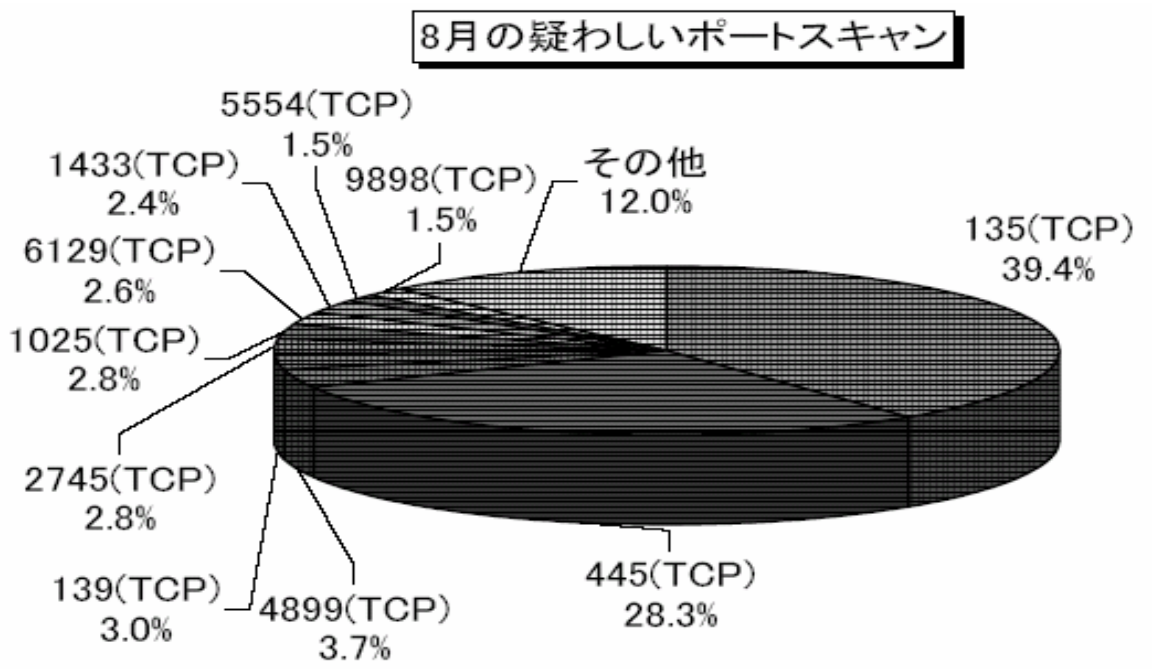
Window/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Netsky	1,431	Xm/Laroux	16	VBS/Redlof	104
W32/Bagle	502	X97M/Divi	8	Wscript/ Kakworm	18
W32/Mydoom	496	X97M/Tristate	6	Wscript / Fortnight	8
W32/Lovgate	347	W97M/Ethan	3	VBS/ Internal	4
W32/Klez	277	WM/Opey	3	VBS/Loveletter	3
W32/Zafi	252			VBS/Netlog	1

[표2] 악성코드 노출 신고 현황(출처 : IPA/ISEC)

일본 네트워크 트레픽 현황

아래의 [그림1]은 2004년 8월 일본에서 발생한 네트워크 포트 사용현황을 나타낸 것이다. 가장 많은 네트워크 트래픽이 발생한 포트는 TCP 135와 445 포트로써 이 두 포트들은 윈도우 OS에서 인증과 관련하여 사용된다. 그러나 이 포트들은 최근 유행하는 네트워크를 통해 전파되는 웜들이 윈도우의 RPC 관련 취약점을 이용한 공격을 시도할 때에도 사용되기 때문에 감염을 예방하기 위해서는 OS의 최신 패치가 필수적이다.

TCP 4899 포트의 트래픽이 많은데 이는 Radmin이라는 원격 제어 툴에서 사용되는 포트 이지만 최근에는 이러한 상용 툴을 웜과 같은 악성코드에서 백도어의 기능을 하도록 사용되는 경향이 있으므로 이에 대한 주의가 필요하다.



[그림1] 일본의 네트워크 트래픽 현황

V. 8월 중국 피해 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

무더웠던 8월의 여름이 지나가고 9월 가을의 문턱에 접어들었다. 9월에는 한국에서 한가위라 불리는 추석 명절이 있는 것과 마찬가지로 중국에도 가을의 한가운데 있다는 중추절 명절을 보낸다. 가을의 문턱에서 무더웠던 8월 여름, 중국의 악성코드 동향은 새로운 악성코드에 의한 피해보다는 기존에 알려진 악성코드들에 의한 피해 신고가 증가하였다.

악성코드 TOP 5

순위 변화	7월	Rising	CNCVERC
*	1	Worm.Netsky	Worm_Netsky.D
*	2	Worm.Lovgate	Worm_AgoBot
NEW	3	Worm.Novarg	Worm_Lovgate.C
NEW	4	Backdoor.Rbot	Worm_Bbeagle.J
NEW	5	Backdoor.Sdbot	Worm_Mydoom.N

[표1] 2004년 8월 악성코드 TOP 5

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

위 [표1]은 2004년 8월 중국 로컬 백신업체인 라이징(Rising)사와 정부연구기관인 중국국가컴퓨터바이러스대응중심(China National Computer Virus Emergency Response Center, 이하 CNCVERC)이 작성한 8월 중국 악성코드 TOP 5이다. 두 기관에서 조사한 악성코드 피해 신고는 몇 달째 지속적으로 1위를 차지하고 있는 Worm.Netsky(Win32/Netsky.worm, 이하 넷스카이 웜)을 제외하고는 순위상의 차이만 있을 뿐 두 기관에서 발견된 악성코드의 종류와 형태에 차이는 없는 것으로 분석된다. 그리고 네트워크로 전파되는 웜과 메일로 확산되는 웜의 양극체제는 4월부터 이어지기 시작하여 이번 달에도 동일한 현상을 보여주고 있다.

주간 악성코드 순위

순위	1주	2주	3주	4주
1	Worm.Netsky	Worm.Netsky	Worm.Netsky	Worm.Netsky
2	Worm.Lovgate	Worm.Lovgate	Worm.Lovgate	Worm.Lovgate
3	Worm.Mabutu	Backdoor.Rbot	Worm.Novarg	Worm.Novarg
4	Backdoor.Sdbot	Backdoor.Sdbot	Backdoor.Rbot	Backdoor.Sdbot
5	Backdoor.Rbot	Worm.BBeagle	Worm.BBeagle	Backdoor.Rbot

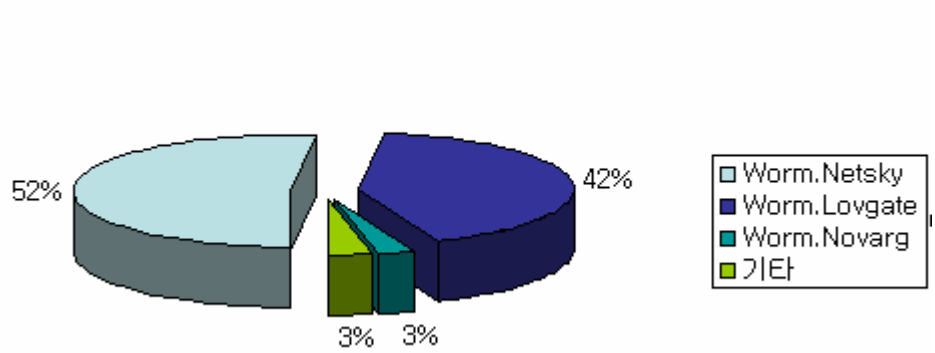
[표2] 2004년 8월 주간 악성코드 순위 변화

라이징(Rising)사에서 작성한 2004년 8월 주간 악성코드 순위 변화를 참고할 경우에도 [표 1]의 악성코드 TOP 5에서 상술한 넷스카이 웜과 Worm.Lovgate(Win32/Lovgate.wrom, 이하 러브게이트 웜)의 1위, 2위 차지는 4달째 이어져오고 있는 현상과 동일하다. 그리고 7월 말에 발견된 Worm.Mabutu(Win32/Mabutu.worm.32768, 이하 마부추 웜)만이 8월 첫째주에 잠시 신고건수가 증가하는 현상을 보였으나 둘째주부터는 급격한 감소가 이루어졌다. 그리고 둘째주와 셋째주에는 기존에 발견되었던 Worm.BBeagle(Win32/Bagle.worm, 이하 베이글 웜)과 Worm.Novarg(Win32/MyDoom.worm, 이하 마이둠 웜)의 신고건수가 잠시 증가하는 현상을 보였으나 수치적인 면과 악성코드 분포적인 면에서는 넷스카이 웜과 러브게이트 웜, 이 두 웜에 비해 그 신고건수가 적은 것으로 분석된다. 그리고 악성 IRCBot 웜의 변형인 Backdoor.Sdbot(Win32/SdBot.worm, 이하 에스디봇 웜)과 Backdoor.Rbot (Win32/IRCBot.worm, 이하 아알씨봇 웜)은 엄청난 변형의 숫자만큼 매주 마다 꾸준히 피해 신고가 있는 것으로 분석되며 수치상의 데이터보다 실제 개인고객 또는 기업고객의 시스템에는 더 많이 확산되어 있는 것으로 추정되니 각별한 주의가 필요하다고 여겨진다.

신종 악성코드 동향

이번 8월에 신고된 악성코드 중 새롭게 발견된 악성코드는 XF_NetSnake.A가 있으나 그 신고건수는 많지 않은 것으로 분석된다. XF_NetSnake.A는 마이크로소프트의 오피스 제품 중 엑셀과 워드 파일형태로 되어 있으나 해당 파일을 실행할 경우 해당 윈도우 시스템에 다수의 트로이목마 파일들이 설치되는 특징이 있다. 그리고 7월 말에 발견된 마부추 웜이 8월 첫째주에 잠시 신고 건수가 증가하고 그 이후에는 급격한 감소를 보였다. 마부추 웜은 7월 마지막 주에 발견된 메일로 전파되는 매스 메일러(Mass Mailer) 형태이다. 마부추 웜은 기존에 발견된 매스 메일러와 동일한 전파 방식을 취하고 있지만 해당 웜에는 기존에 잘 알려진 아이알씨봇 웜의 악의적인 기능을 추가적으로 가지고 있는 것이 특징이다. 이러한 마부추 웜과 동일하게 확산 방식은 메일을 이용하나 감염 이후의 다른 시스템에 대한 공격 방식은 악성 아이알씨봇 웜의 방식을 취하는 것과 같은 유사한 형태의 악성코드가 지속적으로 나타날지도 주목된다.

악성코드 분포



[표3] 2004년 8월 중국의 악성코드 분포

8월 악성코드 분포는 넷스카이 웜과 러브게이트 웜의 양극화 현상을 그대로 보여주고 있다. 이 두 웜이 전제 감염 신고 중에서 94%를 차지 할 정도로 많이 확산되어 있는 것으로 추정된다. 그리고 악성코드 TOP 5 에서 3위를 차지하고 있는 마이둠 웜만이 3%로 간신히 악성코드 분포에서 한 자리를 차지 할 수가 있었다. 그 외 기타에 포함된 악성코드들은 4위와 5위를 차지하고 있는 에스디봇 웜과 아이알씨봇 웜, 그리고 순위에 포함되지 않은 마부추 웜, Worm.Agobot.3(Win32/AgoBot.worm, 이하 아고봇 웜), 베이글 웜 등 기존에 잘 알려진 메일로 전파되는 매스 메일러 웜들이 대부분을 차지하고 있다. 그러나 기타에 포함된 악성코드들이 전체 분포에서 3%를 차지하고 있는 만큼 개별적인 악성코드의 수치는 극히 적은 것으로 분석된다. 주간 악성코드 순위에서 언급한 것과 같이 에스디봇 웜, 아이알씨봇 웜, 아고봇 웜의 경우는 변형의 숫자가 많은 만큼 개별적인 수치는 작을 수 있으나 전체적인 형태로 보았을 때에는 더 높을 수가 있다.

맺음말

여름의 한가운데 있었던 8월 중국 악성코드 동향은 지난 4월부터 있었던 러브게이트 웜과 넷스카이 웜의 양극화 현상이 4개월째 지속되고 있으며 이러한 현상이 언제까지 이어질 지도 미지수이다. 그리고 이 두 웜에 이어서 꾸준히 발견되고 있는 악성 아이알씨봇 웜 변형인 에스디봇 웜, 아알씨봇 웜의 영향력이 다음 달에는 어떻게 변화될지도 주목이 된다. 현재 이 글을 쓰고 있는 9월 첫째 주에는 또 다른 베이글 웜의 변형이 발견되어 확산 및 전파에 대한 새로운 시도가 있었다. 새로운 베이글 웜 변형의 등장이 마이둠 웜과 넷스카이 웜의 또 다른 변형 등장에 대한 예고가 될 지 우려된다.

VI. 테크니컬 컬럼 I – 스파이웨어 위험과 과장

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

기술이 발전하면서 여러가지 생활은 편리해졌다. 하지만, 그 기술이 오히려 사람을 감시하고 통제할 수 있는 상황이 되면서 많은 사람들이 사생활(프라이버시) 보호에 관심을 가지게 되었다. 개인용 컴퓨터 역시 인터넷과 연결되면서 개인의 정보 혹은 사생활이 외부로 유출될 수 있는 문제가 부각되었다. 웜, 바이러스, 트로이목마와 같은 악성코드를 통해서도 개인 정보 유출이 되지만 사용자들의 잘못된 습관 혹은 프로그램의 문제로 개인 정보가 유출될 수 있다. 최근 스파이웨어로 불리는 프로그램에 의해 개인의 성향이 수집되고 개인 정보가 유출될 수 있는 등의 문제가 발생하고 있다. 이 글에서는 스파이웨어의 정의에 대해 알아보고 스파이웨어의 위험성과 그와 함께 과장된 부분에 대해서도 알아 보겠다.

스파이웨어, 혼란의 시작

많은 사람들이 스파이웨어(Spyware)라고 하면 스파이라는 용어에서 개인 정보 유출을 가장 먼저 떠오른다. 하지만, 스파이웨어는 정확하게 개인 정보 유출 보다는 개인 정보 수집에 목적이 있다. 정보 유출은 프로그램 제작자가 고의로 개인의 정보를 빼가기 위해서 악성코드를 제작하는 것이다. 하지만, 개인 정보 수집은 주로 광고에 활용하기 위해서 사용되는 것이다. 즉, 이들 프로그램 제작자들은 개인의 비밀번호, 신용카드 정보가 필요한 것이 아니라 개인이 어떤 웹사이트를 방문하며 어떤 것에 관심이 있는가를 수집하는 역할을 한다. 백신업체에서 보면 이는 일종의 영업 활동이므로 악의적인 행동이라고 볼 수 없어 진단하지 않는 정책을 취하게 된다. 하지만, 온라인 마케팅 업자들은 개인의 컴퓨터에 몰래 혹은 사람들이 잘 읽어보지 않는 동의서에 한 줄 넣어 사용자 동의를 얻어 특정한 프로그램을 설치해 개인 정보를 수집하게 되었다. 이에 반기를 든 사람들이 스파이웨어 진단 프로그램을 만들어 배포하기 시작했다. 문제는 스파이웨어에 대한 용어의 통일성과 기준이 명확하지 않다는데 있다. 스파이웨어는 국내에서는 악성코드(백신업체에서 부르는 악성코드와는 다른 의미임), 트랙웨어(Trackware), 페스트(Pest), 비 바이러스(Non-virus) 등으로도 불리고 있으며 업체별로 스파이웨어에 대한 정의와 범위가 제각각이다. 기본적으로 개인 사생활을 침해할 수 있는 유형은 스파이웨어라고 부르지만 백신업계 등 기존 보안업체에서 처리하고 있던 백도어(Backdoor)류의 트로이목마도 일부 업체에서는 스파이웨어에 분류하고 있다. 특히 몇몇 업체는 제품 홍보를 위해서 일부 트로이목마를 진단하면서 모든 악성코드를 진단하는 것처럼 광고하고 있어 많은 사용자들이 스파이웨어에 대해서 잘못된 오해를 일으키고 있다.

안철수연구소는 악성코드 외 사용자 컴퓨터를 위협할 수 있는 형태를 유해가능 프로그램으로 분류하고 있으며 스파이웨어가 많이 알려져 있어 편의상 스파이웨어로 정리했다.[1] 따라서

[1] 자세한 내용은 백신 회사와 안철수연구소의 스파이웨어 정책 참고

안철수연구소의 스파이웨어를 **"유해가능 프로그램 중 사용자가 명확히 해당 프로그램의 목적을 알지 못하고 설치되어 사용자의 사생활을 침해할 수 있는 프로그램"**으로 정의한다. 하지만, 일반 사용자들은 스파이웨어를 "자신의 허락을 받지 않고 설치되어 자신도 모르게 실행되는 프로그램"으로 받아 들이고 있다.

스파이웨어의 문제점

스파이웨어로 발생할 수 있는 문제점은 다음과 같다.

1) 개인 정보 유출 가능성
2) 시스템 속도 저하
3) 버그 등으로 인한 시스템 문제 발생 가능성
4) 심리적 불안감

스파이웨어 진단 프로그램을 제작하는 가장 많은 사람들이 주장하는 내용은 스파이웨어가 개인 정보를 유출한다는 것이다. 하지만, 스파이웨어를 백신업체에서 백도어로 부르는 원격 제어 프로그램까지 확장할 경우에 개인 정보 유출이 가능하며, 일반적으로 스파이웨어로 분류되는 트랙웨어, 애드웨어는 개인 정보 유출과는 거리가 멀다. 개인 정보 유출 보다는 개인 정보 유출 가능성이 있다고 하는 것이 정확한 표현이라고 생각된다. 즉, 악성코드는 개인 정보를 유출하기 위해 제작된 것이며 스파이웨어는 개인 성향을 수집하는 과정 중 개인 정보를 유출할 수도 있다는 것이다.

개인 정보 유출 가능성보다 더 큰 문제는 시스템 이상과 심리적 불안감이라 할 수 있다. 모든 프로그램은 문제가 존재할 수 있고, 광고나 사용자 정보 수집을 위해 실행 중인 프로그램도 문제가 존재할 수 있다. 실제로 애드웨어의 문제로 시스템이 제대로 실행되지 않는 등의 문제가 발생했었다. 또 광고 창이 뜨는 등의 애드웨어가 설치되면 일반적인 사람은 바이러스에 감염된 것으로 생각한다.

사례 및 과장된 부분

스파이웨어의 문제점과 함께 지나치게 과장된 부분도 존재한다. 이런 과장된 부분은 관련 업체와 언론을 통한 지나친 위험성 확대와 일반 사용자들의 이해 부족과도 맞물리게 되었다. 초기의 스파이웨어 논쟁은 개인 정보 유출이었지만 2002년 이후 발생하기 시작한 시작페이지 고정과 지나친 광고 창 출력은 사람들을 불편하게 만들었다. 이에 국내에서도 2003년부터 시작페이지 고정과 광고 창을 띄우는 애드웨어를 진단/삭제하는 프로그램이 제작 배포되었고 많은 사람들의 사랑을 받았다. 하지만, 이후 타 제품보다 많이 진단한다는 점을 강조하기 위해서 지나치게 위험도가 낮은 형태도 스파이웨어로 분류해서 진단하는 제품이 늘어났다.

1) 추적 쿠키(Tracking Cookie)

스파이웨어 진단 프로그램 중 상당수는 쿠키를 진단한다. 쿠키는 2000년부터 쿠키가 사용자의 사생활 침해 가능성이 계속 제기되고 있다.[1] 하지만, 현재의 쿠키는 안전하다는 것이 대부분의 의견이다. 하지만, 일부 스파이웨어에서 진단하는 추적 쿠키는 단순히 이 사용자가 어떤 사이트를 방문했었다는 것으로, 개인 정보 유출과는 큰 상관이 없는 것이 대부분이다. 하지만, 일부 업체에서 이를 스파이웨어 쿠키(Spyware-Cookie)와 같은 표현을 사용하고 있다. 스파이웨어 업체에서 진단하는 쿠키는 사용자가 A사이트 방문 여부를 B사이트가 알고 있다는 것 때문에 진단하는 것이다.

쿠키는 인터넷 익스플로러에서 '도구(T)' -> '인터넷 옵션' -> 임시 인터넷 파일에서 '쿠키 삭제(I)'로 간단히 삭제 할 수 있다.

2) Aureate/Radiate

2000년쯤 국내에 스파이웨어라는 용어를 처음으로 알려준 대표적인 트랙웨어이다. 이 트랙웨어 모듈은 여러가지 프리웨어 혹은 애드웨어에 포함되었다. 처음 문제를 제기한 사람은 Aureate/Radiate 사의 광고 모듈이 광고를 보여주며 사용자 개인 정보를 빼간다고 주장했다. 이후 이 내용은 사실이 아님이 밝혀졌고 백신회사에서는 이들 프로그램을 악성코드로 분류하지 않는다고 발표했다.[2] 하지만, 일부 스파이웨어 진단 프로그램은 여전히 해당 프로그램을 개인정보의 유출 우려와 불필요한 네트워크 패킷 발생 등의 이유로 스파이웨어로 분류해 진단하고 있다.

스파이웨어 진단 프로그램은 개인 사생활 보호를 위해 만들어 졌으므로 누군가 자신의컴퓨터를 감시하는 것 자체를 싫어해 이들 프로그램을 진단하고 있다. 따라서 자신이 어떤 광고를 선택했는지의 정보가 정보가 외부로 나갈 경우는 진단해야 한다는 정책으로 이들 프로그램을 진단하고 있다.

3) 알렉사(Alexa)

상당수 스파이웨어 진단 프로그램이 윈도우 기본기능에 포함된 '관련링크표시' 기능을 스파이웨어로 진단한다. 마이크로소프트사가 개인 정보를 수집하기 위해서 이 프로그램을 설치한

---

[1] ZDNet Korea, 일부 사이트 쿠키 보안 비상
http://www.zdnet.co.kr/news/internet/0,39024414,10067354,00.htm
ZDNet Korea, 프라이버시 보호, 쿠키 단속이 급선무
http://www.zdnet.co.kr/news/network/0,39024416,10034077,00.htm

[2] Kaspersky Labs, http://www.kaspersky.com/news.html?id=16
Vmyths.com, http://vmyths.com/hoax.cfm?id=36&page=3
F-Secure, http://www.europe.f-secure.com/v-descs/aureate.shtml
OptOut, http://grc.com/oo/aureate.htm

것일까? 결과적으로 심각하지 않다.[1] 이 기능은 인터넷 익스플로러의 도구(T) -> 관련링크표시(R)를 선택할 경우 방문 사이트 정보가 알렉사로 전달된다. 이 과정에서 개인이 어떤 사이트를 방문하는지 수집되므로 사생활 침해의 관점에서는 일부 스파이웨어 진단 프로그램에서 추가해 기능을 막고 있다.

[그림1] 알렉사 기능 사용 화면(좌측 화면)

4) TCP.EXE

2004년 7월 중순 다수의 TCP.EXE와 WINSYSTEM.EXE가 접수되었다. 프로그램을 확인 결과 포털 사이트에서 입력되는 검색어를 수집해가는 트랙웨어(Trackware)이며, 7월 한 스트리밍 음악 사이트에서 배포한 프로그램으로 확인되었다.[2] 이후 개발사와 확인 해본 결과 다음부터는 프로그램의 사용 목적과 동의를 구한 후에 설치하는 것으로 사건은 일단락되었고 음악 재생 프로그램에서도 이 파일이 제거되었다.

이 프로그램이 음악 재생 프로그램에 포함되어 배포되었는데 많은 사람들이 바이러스로 오해하고 해당 스트리밍 음악 사이트 업체가 바이러스를 배포하는 것으로 오해 받기도 했다.

이 프로그램은 개인정보를 유출하는 것이 아니라 사용자의 검색어를 수집해 최근 사람들이

[1] Alexa Spying On You?, http://www.imilly.com/alexa.htm
[2] AhnLab, http://info.ahnlab.com/smart2u/virus_detail_1463.html

관심 있어하는 내용을 수집하는 목적을 가졌지만, 사용자의 동의를 구하지 않은 점이 문제가 되었다. 이 사건은 사용자들의 사용자 성향 조사 수집에 대한 거부감을 업체가 인지하지 못하여 발생한 문제이다.

결론

스파이웨어는 사용자 동의를 거치므로 합법이라는 논리를 내세워 사용자 불편을 생각하지 않고 사용자 컴퓨터를 마케팅 목적으로 사용하는 제작업체와, 약관 등을 꼼꼼히 읽지 않는 사용자의 부주의, 규제 등을 제대로 마련하지 못한 법률적 미비 등이 만들어낸 합작품이다. 또 백신업체가 악성코드가 아니라는 이유로 진단/치료하지 않는 사이 지나치게 과장된 내용으로 사용자들을 겁주는 스파이웨어 진단업체도 등장하고 있다.

스파이웨어에 대한 올바른 인식과 퇴치를 위해서는 사용자, 마케팅 업체, 스파이웨어 진단 업체, 정부 모두 앞장서야할 것 이다.

사용자는 자신이 사용하는 프로그램에 광고기능이나 자신의 컴퓨터 사용 경향을 수집하는 프로그램이 설치되었을 가능성이 있음을 알고 프로그램 설치시 동의서를 잘 읽고 웹사이트를 돌아다니면서 액티브 X 컨트롤 경고를 무작정 설치하지 않아야 한다. 또한 자신이 사용하는 스파이웨어 진단 프로그램의 정확한 정책을 알아야 한다.

트랙웨어와 애드웨어 제작 업체는 자신들이 하려는 목적을 프로그램 설치 중 분명히 알려주고 사용자의 동의를 받은 후 설치 과정을 사용자에게 알려주며 제거도 쉽게 해야 할 것이다. 스파이웨어는 인터넷 정보 수집 현황이나 광고 출력 자체에 있는 것이 아니라 컴퓨터 사용자가 자신이 언제 설치했는지 조차 모르고 어떤 프로그램에서 그런 일을 하는지 모르기 때문에 문제가 발생하고 있다.

스파이웨어 진단 프로그램도 사용자에게 검색 전 스파이웨어에 대한 바른 이해와 진단되는 프로그램의 정확한 진단 이유와 발생 가능한 문제점을 알려줄 필요성이 있다. 또 사용자들을 지나치게 겁주는 행위는 자제해야 한다. 또한 용어와 진단 범위에 대한 업체의 통일화도 필요하다.

정부도 스파이웨어류에 대한 법적인 규제를 해야할 것으로 생각된다. 다음과 같은 내용만 구체적으로 명시하게 해도 많은 도움이 될 것으로 생각된다.

- 프로그램 설치 시 사용자 동의
- 언 인스톨 프로그램 제공
- 광고 출력 시 프로그램 이름 표시
- 웹사이트에서 프로그램 다운로드시 사용자 동의 구함

VII. 테크니컬 컬럼 II - 유해트래픽의 탐지와 판단

작성자 : 정관진 주임연구원(intexp@ahnlab.com)

전산자원의 증가와 보안의식의 부재로 인하여 외부로부터의 위협은 증가되어 가고 있으며, IT화의 빠른 발전에 힘입어 기업의 네트워크 구조는 더욱 복잡다양하고 거대해지고 있다. 네트워크의 발달 속도 증가는 악성코드의 확산력을 증가시켜 주었고, 지금 이 순간에도 여러분들의 네트워크 망에는 어떠한 유형의 트래픽에 의해 네트워크 대역폭의 일정부분을 잠식당하고 있을지도 모른다. 이번 호에서는 유해 트래픽 범위와 탐지 및 판단을 하기 위한 방법에 대해서 알아보도록 하겠다.

유해트래픽 범위와 현실

컴퓨터와 네트워크 연결은 이제 우리에게 일상화되었고 이에 따라 네트워크 트래픽 증가는 자연스럽게 나타났다. 트래픽 형태는 장비와 장비간의 통신, 컴퓨터 상호간의 통신, 브로드캐스팅(Broadcasting) 등 일반적인 통신의 범위에 해당하는 것도 있지만, 악성코드 또는 공격에 의한 것도 있다. 그렇다면 과연 이러한 유해트래픽은 네트워크망에서 얼마나 큰 비중을 차지하고 있을까? 필자는 이에 대해 적지 않은 유해트래픽이 존재할 것으로 예상한다. 물론, 내/외적인 환경 요인과 네트워크 구조적인 영향에 따라 비중은 달라지겠지만, 분명한 것은 의도치 않은 유해트래픽에 의해 네트워크 대역폭의 상당부분이 잠식당하고 있다는 것이다. 유해트래픽의 증가는 네트워크 운영 효율에 상당한 영향을 주게 되므로 유해트래픽을 빠르게 인지하고 대처할 수 있는 능력이 필요하게 된다. 우선, 이러한 유해트래픽은 크게 다음과 분류해 볼 수 있다.

- 웜, 트로이목마등과 같은 악성코드(Malicious Code)에 의한 트래픽
- 공격(Attack)에 의한 트래픽
- 비 이상적인 트래픽

유해트래픽의 가장 큰 원인으로는 악성코드와 공격에 의한 영향이 가장 클 것이다. 이 모든 범주가 내부에서 외부로 또는 외부에서 내부로 영향을 미치는 것들이다. 내부에서 외부로의 트래픽 증가는 내부 네트워크(LAN:Local Area Network)에 전체적으로 영향을 주게 되어 외부로부터 내부로 들어오는 유형보다 미치는 영향이 더욱 크다고 할 수 있다. 많은 기업 및 개인들은 방화벽(개인은 개인용 방화벽), 백신 소프트웨어 등을 이용하여 내부와 외부의 통신 접점이 되는 곳에서 많은 방어정책을 가지고 있지만, 내부에서 웜에 감염되어 트래픽을 유발하거나 공격자가 되는 것에 대한 방안은 뚜렷하지가 않다. 따라서, 내부로부터의 트래픽 증가로 인해 더욱 큰 위협을 유발하게 되는 경우에 대한 대책이 필요하다.

트래픽의 탐지와 판단

유해트래픽이 내부에 발생하였거나 또는 외부로부터의 유입이 나타나는 경우 빠른 분석이 필요하다. 물론, 사전에 이러한 유해트래픽이 완벽하게 차단될 수 있다면 더욱 좋은 경우이겠지만 그렇지 않은 상황이라면 무엇보다도 문제해결을 위하여 빠른 원인 분석이 필요하다. 트래픽 탐지 및 판단하기 위하여 저번 호에서 설명하였던 공개용 패킷 모니터링 툴인 Ethereal(이하 이더리얼)을 가지고 살펴보기로 한다.[1]

우선 유해트래픽을 탐지하고 판단하기 위해서는 네트워크상에서의 패킷을 캡쳐해야 한다. 만약 분석하기 위한 데이터의 사이즈가 큰 경우에는 작은 경우보다 그만큼 분석에 많은 시간이 소요되게 된다. 충분한 시간이 있다면 상세분석을 하여 원인파악 하는 것도 의미 있지만, 이미 내부 네트워크에 큰 영향을 주고 있다면 분석의 순서를 정하여 어떠한 것에 의해 영향을 받고 있는지 파악이 되어야 한다. 이더리얼의 기능 중 분석에 활용할 수 있는 것을 보면 다음과 같다.

- Packet Summary 의 요약 정보
- Protocol Hierarchy Statistics 프로토콜별 상태
- EndPoints
- IO Graph
- Conversation List
- TCP Follow Stream
- 사전에 정의된 Coloring Rule 을 이용한 빠른 판단
- Capture Filter, Display Filter 를 이용한 범위의 축소
- Protocol, IP 주소별 등의 정렬

패킷요약(Statistics->Summary) 정보는 전체 패킷 수와 평균 초당 전송한 패킷과 사이즈 그리고 전체 트래픽을 알려준다. 초당 전송한 패킷수가 과도하게 클 경우 의심해 볼 수 있게 된다. 이와 함께 프로토콜별 상태 (Statistics ->Protocol Hierarchy)정보를 보면 트리구조로 프로토콜별 패킷의 퍼센트와 패킷수, 바이트(Bytes) 정보를 알 수 있다. 전체 트래픽 정보를 한눈에 프로토콜별로 살펴볼 수 있기 때문에 어떤 프로토콜에서 큰 비중을 차지하고 있는지 알아볼 때 유용하다. 예를 들어, 전체 프로토콜 중 UDP(User Datagram Protocol)가 차지하는 비중이 현격히 차이 나는 경우 UDP를 중심으로 분석을 시작하면 된다.

UDP를 중심으로 분석을 시작한다면 “Display Filter”를 통하여 UDP 프로토콜로 출력을 제한한다. Analyze->Display Filters 또는 메인 화면의 필터 입력 부분에서 바로 넣어주면 된

[1] 이더리얼을 처음 접해보는 독자라면 ASEC Monthly Report 7월호를 먼저 읽어볼 것을 권장한다.

다. 즉, “UDP” 라고 입력해 주고 적용을 하게 되면 UDP 프로토콜만 화면상에 나타나게 된다. 출력된 패킷을 확인하며 다음과 같은 비 이상적인 형태들을 확인하여 본다.

- 패킷이 연속적으로 반복되는 경우
- 외부의 특정한 곳으로 계속 접속을 시도
- 출발지 주소가 내부 네트워크에 할당된 주소가 아닌 경우 (IP Spoofing)
- 한 IP 주소에서 외부로 랜덤한 IP 주소를 연속적으로 사용
- IP 주소가 규칙을 가지고 지속적으로 증가

또한, 다음의 사항을 염두해 두고 살펴본다.

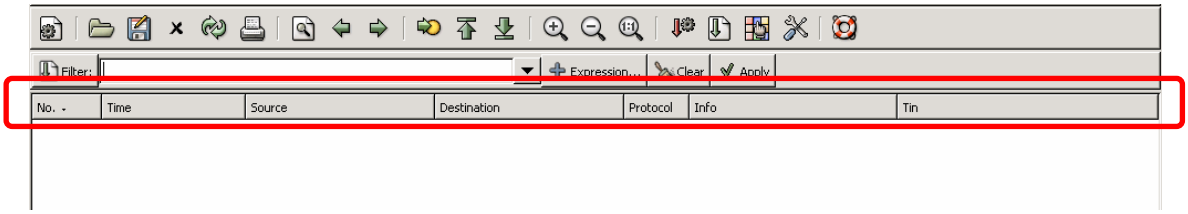
- 일정한 시간범위 안에서 두드러지게 나타나는 패킷 과찰
- 반복적으로 지속적인 패킷 관찰
- 스위치, 라우터등의 일반적인 네트워크 구조 환경에서 장비들이 생성하는 패킷은 출력 필터에서 제외 (STP, HSRP 등)

패킷을 캡쳐하는 네트워크의 규모가 큰 경우에는 유해트래픽 이외의 정상적인 통신에 의한 패킷 또한 상당히 많게 나타나게 된다. 이런 경우, 패킷 분석에 있어 어려움이 따르므로 필터를 통하여 범위를 좁혀나가는 것이 필요하다. 필터는 프로토콜의 필드별로 세부적 지정이 가능하므로 분석에 있어서 상당히 효율적이다. 물론 필터를 사용하기 위한 규칙을 알아야 하지만, 상세하게 출력되는 화면에서 해당 필드의 오른쪽 버튼을 클릭하여 “Apply as Filter” 또는 “Prepare a Filter” 를 사용할 수 있고, 필터에서 단계별로 조건을 지정하는 화면도 있으므로 편리하게 사용할 수 있다. 출력필터에 대한 몇 가지 사용 예는 [표1]과 같다.

필터	설명
udp.dstport == 138	UDP 목적지 주소가 138번에 대해 필터링 한다.
eth.src == 00:50:da:93:eb:cd	출발지 이더넷 맥 주소가 00:50:da:93:eb:cd인 것을 찾는다.
ip.checksum_bad	IP CheckSum이 올바르지 않은 것을 필터링 한다.

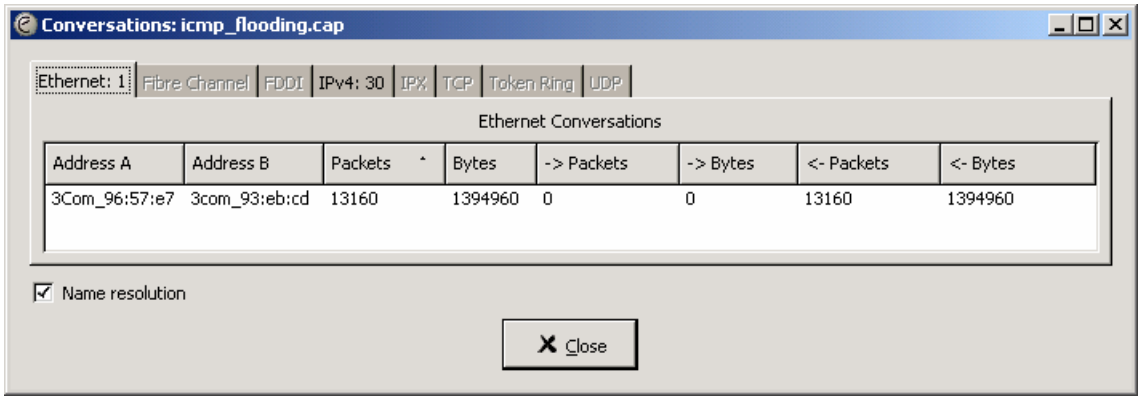
[표1] 출력필터 사용 예제

출력된 상태에서는 [그림1]의 필드를 클릭하여 정렬을 수행할 수도 있으므로 상황에 따라 요긴하게 사용할 수 있을 것이다.

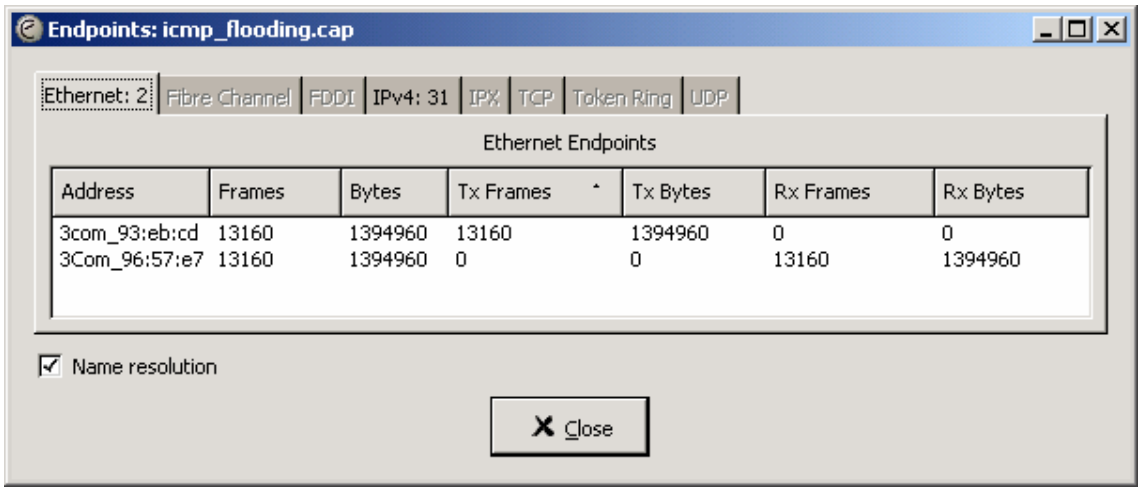


[그림1] 필드별 정렬

이더리얼의 상태(Statistics)기능 중 또 하나 유용한 것이 Conversations, Endpoints, IO Graphs이다. Conversations은 이름에서 말해주는 것과 같이 출발지와 목적지간의 통신 내용에 대해 패킷수와 바이트 등을 나타내 준다. Endpoints는 최종 목적지에 대해 보여주는 것으로 Conversations 기능과 유사하다. 이 두 기능에는 이더넷, IPv4, TCP, UDP와 같이 형태별로 탭을 구분하여 보여준다. 어느 IP가 많은 트래픽을 생성하는지 확인해 보고자 할 때 유용하게 사용할 수 있을 것이다. [그림2,3]



[그림2] Conversation 기능 실행 화면



[그림3] Endpoints 기능 실행 화면

IO Graph(Statistics->IO Graph)는 캡쳐된 패킷에 대해 그래프를 보여준다. 5가지의 색상별 그래프를 정의하여 만들 수 있으며, 그래프별 필터와 스타일을 정의할 수 있다. 캡쳐된 패킷의 전체 상태에 대해서 그래프화하여 쉽게 볼 수 있다.

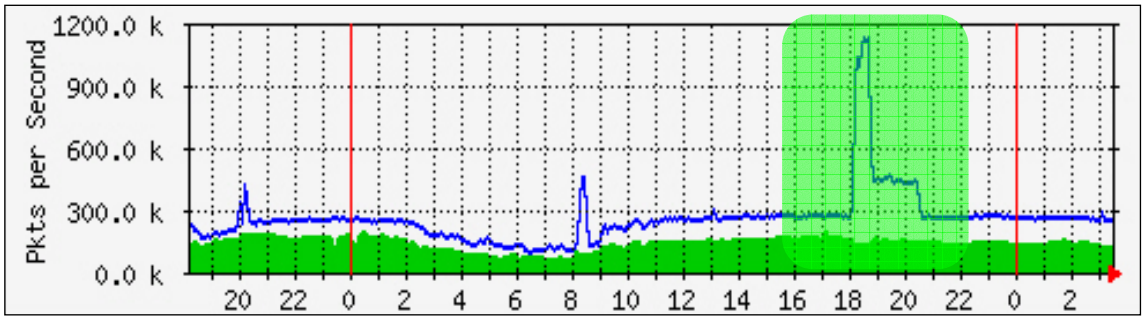
또 하나 TCP 프로토콜을 이용하는 경우, "Follow TCP Stream" 이 빠른 정보를 제공해 준다. 패킷 리스트에서 TCP 프로토콜을 사용하는 패킷을 선택하여 오른쪽을 클릭하면 해당 메뉴를 볼 수 있으며, 클릭시 해당 IP와 통신하는 상대측의 IP에 대하여 필터를 자동으로 만들어 서로간에 주고받았던 내용이 나타난다. 패킷 하나를 보아야 하는 불편함 없이 쉽게 통신 내용을 확인할 수 있다.

더불어 칼라 룰을 사전에 만들어 사용하면 패킷 분석시에 더욱 효율적이다. 지정한 조건에 따라 색깔을 정의할 수 있기 때문에 여러 패킷 정보가 있어도 조건에 부합되는 패킷이 있으면 칼라 룰이 적용되어 시각적인 효과가 크다. View -> Coloring Rules를 선택하여 조건을 만들고 필요시마다 사용할 수 있다.

지금까지의 과정을 가지고 몇 가지 사례를 통해 알아보도록 한다.

CASE STUDY 1

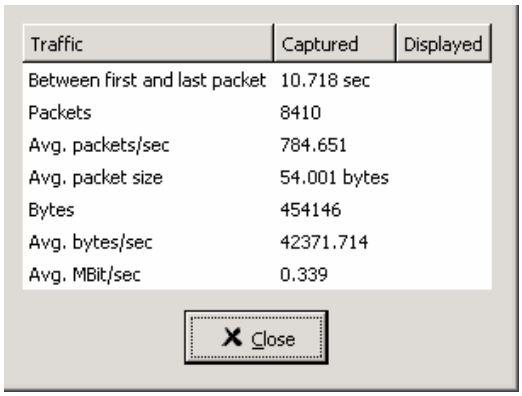
모 ISP(Internet Service Provider)로부터 트래픽이 과다 생성된 경우로, 패킷이 초당 30,000개에서 140,000개로 급격히 증가한 사례이다. [그림4]와 같이 18시 이후 급격하게 증가되는 것을 보여주고 있으며, 특정 IP에서 트래픽을 크게 유발하는 것이 확인되어 라우터에서 Null Routing[1] 처리 후 트래픽이 정상으로 돌아왔다.



[그림4] TCP SYN 공격에 의한 트래픽 급격 증가

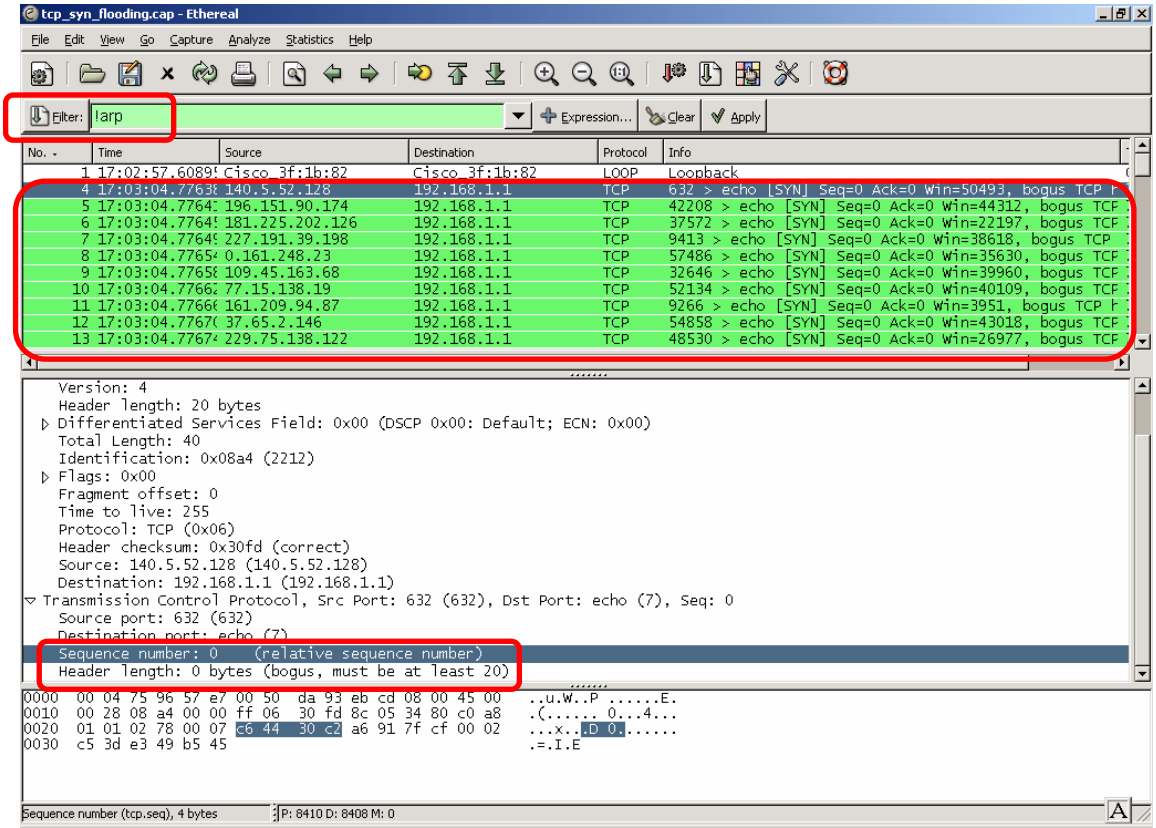
[그림5]는 위 상황과 같은 형태인 SYN 패킷 증가에 따른 또 다른 패킷의 요약정보를 나타낸 것으로써 초당 평균 784개가 전송되었다.

[1] 라우팅을 하지 않고 Null 값으로 보내는 것



[그림5] 패킷요약 정보

[그림6]은 Coloring Rules을 이용하여 패킷의 세부 내용을 보고있는 화면으로 필터에 "!arp"를 적용하여 ARP 패킷은 제외하여 화면 출력을 하였다. 리스트화면을 보면 출발지 IP 주소가 랜덤하게 생성되고 있으며, 특정 IP 주소인 192.168.1.1로 공격이 시도되고 있다. 목적지 포트는 6번 포트이며 SYN 패킷을 과도하게 생성해 내고 있는 것으로, 출발지 주소는 Spoofing되어 발송되는 것을 알 수 있다. 세부 내용을 보면 Header length가 0 bytes로 조작되어 있다. Coloring Rules에는 사전에 "tcp.hdr_len < 20" 와 같이 헤더의 길이가 20바이트 이하인 것에 대해 색깔을 정의해 놓았다.

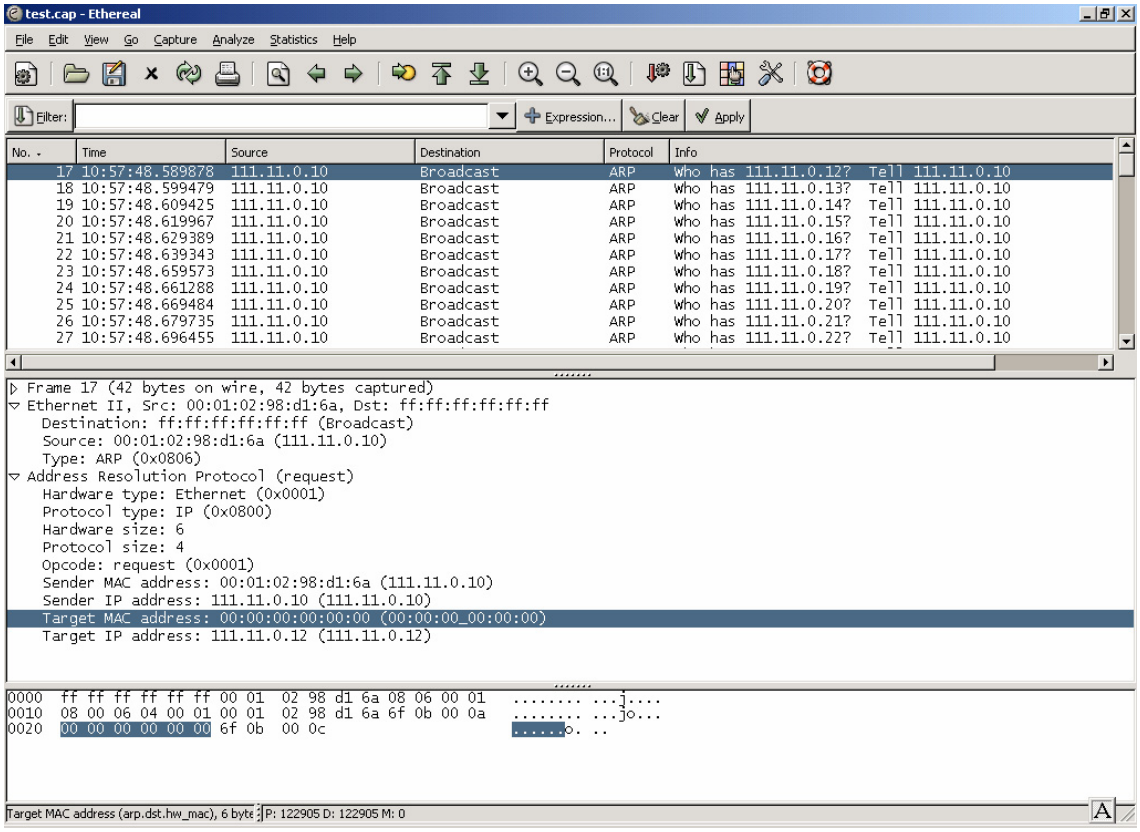


[그림 6] 칼라 룰을 적용해 살펴본 TCP SYN 공격 형태

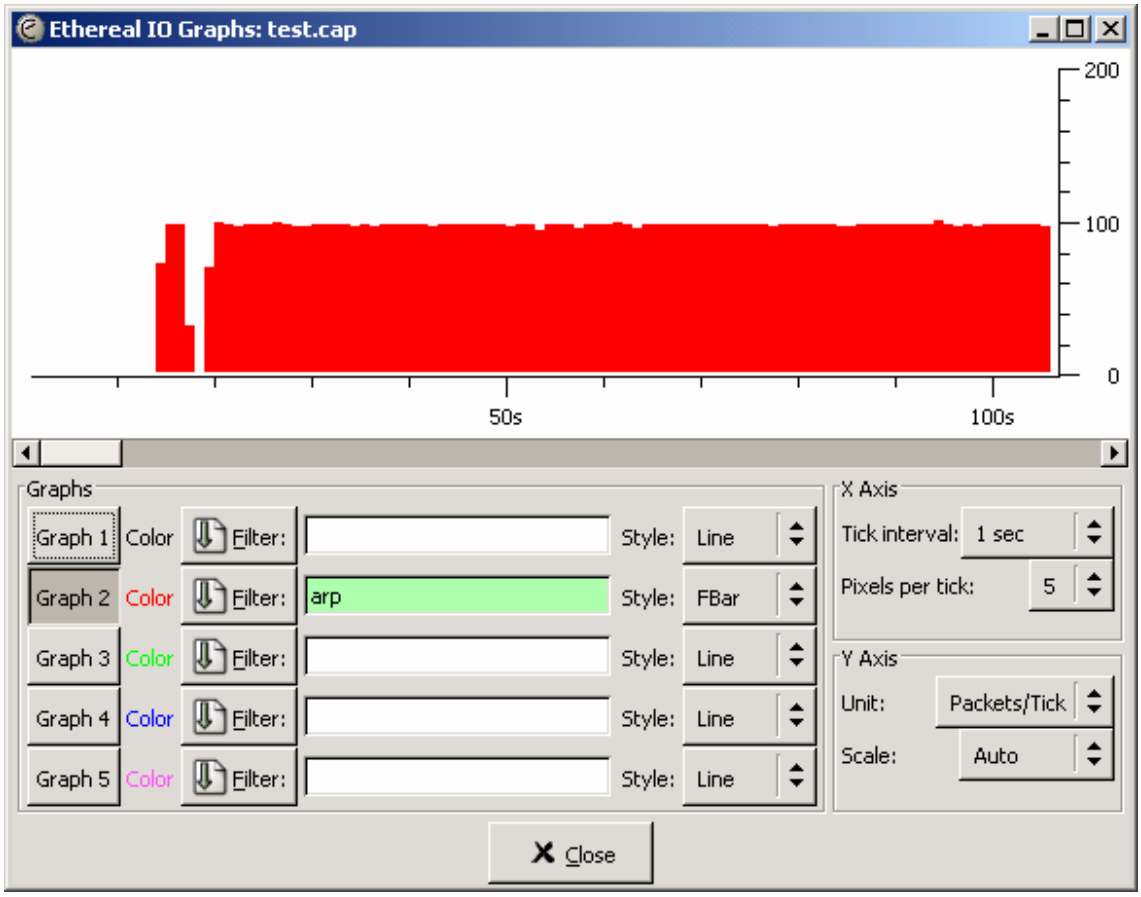
CASE STUDY 2

ARP(Address Resolution Protocol) 트래픽이 급격하게 증가되는 경우로, 프로토콜별 상태 정보 추이를 보면 ARP 트래픽의 비중이 90% 이상으로 나타났다. 이에 따라 ARP에 의한 문제로 초기에 추정해 볼 수 있다. 실제 패킷의 흐름을 보면 ARP 요청 IP 주소가 증가되는 것을 알 수 있다. 즉, 공격형태이기 보다는 어떤 악성코드에 의한 가능성이 더욱 높은 것으로 추정할 수 있으며, 패킷의 상세 정보에서도 위 변조형태를 지니고 있지 않은 것으로 나타난다. 그렇다면 111.11.0.10 번의 IP 주소를 가지는 시스템을 찾는다면 문제의 원인을 찾아볼 수 있을 것이다.

[그림7]은 메인 화면을 보여주고 있고, [그림8]는 전체 트래픽 중 ARP 프로토콜로 한정지어 그래프를 생성한 것이다.



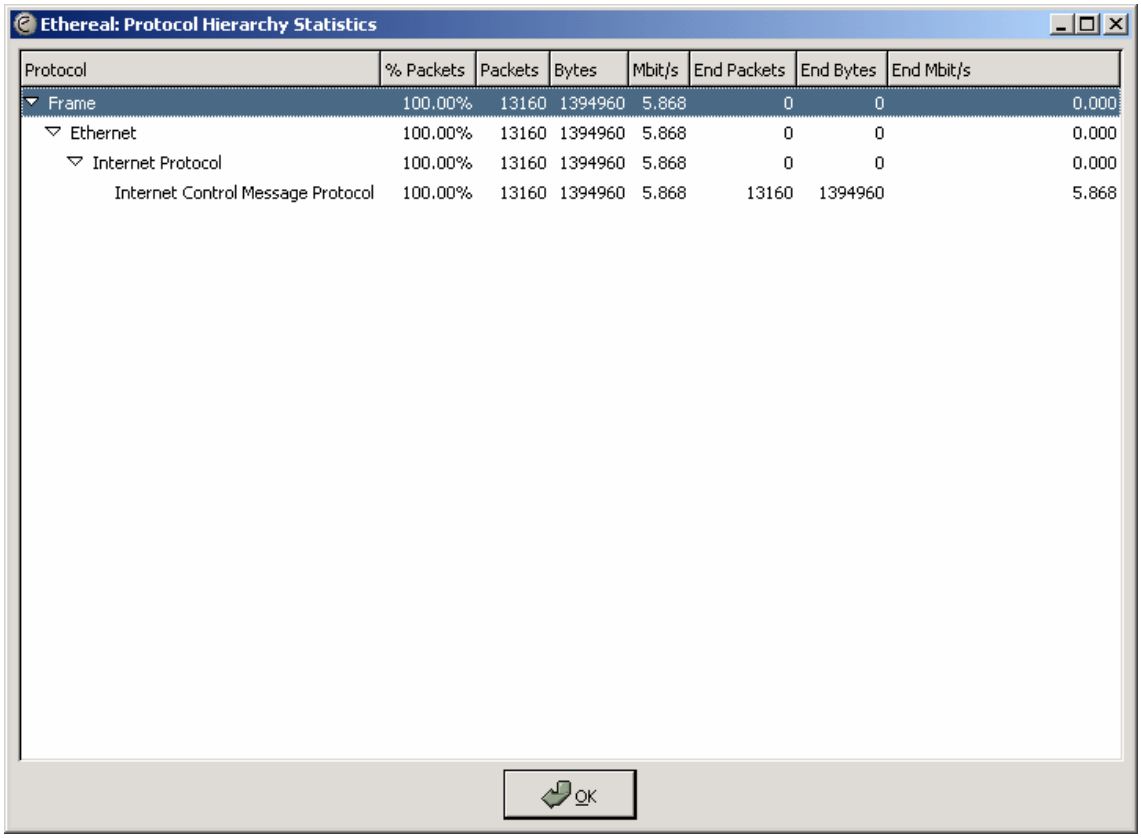
[그림7] ARP 트래픽 캡쳐 화면 예제



[그림8] IO Graphs 를 통해 살펴본 ARP 트래픽

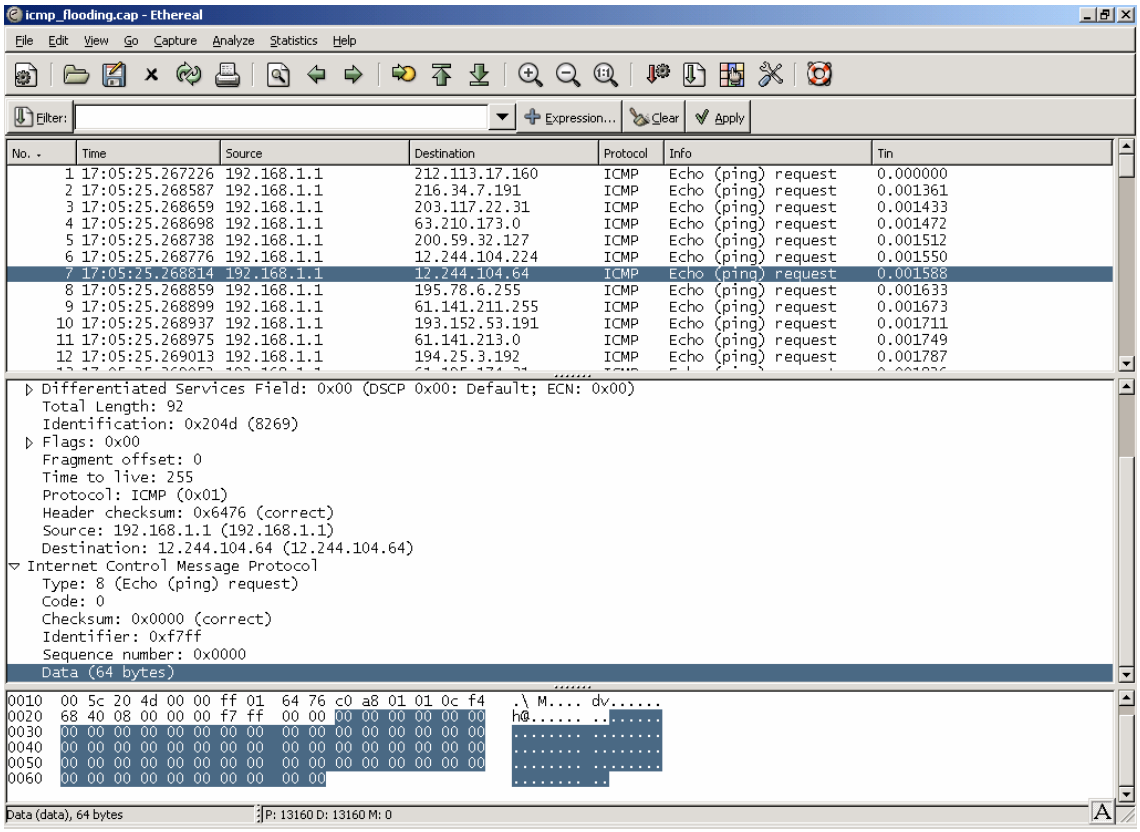
CASE STUDY 3

ICMP(Internet Control Message Procotol) 패킷이 크게 증가한 사례로, [그림9]를 통해서 본 프로토콜 별 상태에서도 ICMP 패킷 하나만 나타나고 있다. 초당 약 7,000 개 정도 발생한 것이다.



[그림9] 프로토콜별 상태 정보 화면

목적지 주소는 랜덤하게 ICMP의 Echo 요청이 연속적으로 이뤄지고 있다. 과도한 ICMP와 목적지 주소가 랜덤하게 변경되는 걸 보면 조작된 공격형태로 추정할 수 있다. 일반적인 상황에서는 ICMP 트래픽이 초당 몇 천개 이상으로 발생되는 경우가 없기 때문이다.



[그림10] ICMP 공격 형태를 보여주는 화면

이상 유해트래픽 발생시 탐지하고 판단하기 위한 방안들에 대해 이더리얼을 기준으로 설명해 보았다. 물론, 여기서 언급한 내용들이 모든 사항에 부합되는 것은 아니지만 기본적으로 유해트래픽을 탐지하고 판단하는 데는 가이드를 제시해 줄 수 있을 것이다. 다음 호에서는 악성코드에 의한 네트워크 위협과 악성코드 사례를 들어 패킷 분석을 좀더 세부적으로 알아보고 네트워크 상의 유해트래픽 분석에 대한 글을 마무리 짓고자 한다.