ASEC Report 9월

® ASEC Report

2004. 10

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

새로이 발표된 JPEG 처리(GDI+) 관련 취약점 주의….

올해 들어 상반기 내내 매월 기록을 갱신하며 접수되던 피해신고 건수는 9월 들어 급격한 감소세를 보였다. 그러나 9월에 접수된 총 피해신고 건수는 감소하였지만 피해신고된 악성코드의 수는 6, 7월 등과 비슷한 수치를 보이는 것으로 보아, 다양한 악성코드로 인한 피해는 여전하다는 것을 알 수 있었으며, 피해신고된 악성코드 중 IRCBot 웜이 약 65%를 차지할 정도로 많은 변형에 의한 피해가 있었다. 9월에는 9월에 발표된 JPEG 처리(GDI+)의 취약점을 이용한 트로이목마가 2개 발견되었고, 2003년 발표된 MS03-050 취약점 이용한 매크로 바이러스가 2개 발견되었다. 또한 9월에는 IRCBot 변형의 접수가 급격히 증가하였는데, 이로 인해 9월 신종 발견 건수가 전반적으로 상승하는 추세를 보였다. 9월에 발표된 JPEG 처리(GDI+)의 버퍼 오버런으로 인한 코드 실행 문제(MS04-028)는 취약점 발표 후 이를 이용한 공격코드와 트로이목마가 연달아 발견되었고, JPEG 이미지 파일을 사용하는 사용자가 많은 점으로 미루어 특히 주의를 기울여야 하는 취약점으로 보여진다.

테크니컬 컬럼에서는 아직 국내에서는 피해가 없지만 외국에서 많은 피해를 보이고 있는 피싱(Phishing)에 대해서 알아보았고, 네트워크에 영향을 미치는 악성코드에 대한 트래픽 분석에 대해 알아보았다.

I. 9월 악성코드 피해 Top 10

작성자 : 박태환 연구원(juun5@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	528	13.50%
2	3↑	Win32/Netsky.worm.17920	334	8.54%
3	5↑	Win32/Netsky.worm.16896.B	309	7.90%
4	2↑	Win32/Bagle.worm.Z	254	6.50%
5	3↓	Win32/Netsky.worm.17424	200	5.12%
6	1↑	Win32/Netsky.worm.22016	190	4.86%
7	3↑	Win32/Netsky.worm.25352	124	3.17%
8	New	Win32/LovGate.worm.128000	102	2.61%
9	-	Win32/Sasser.worm.15872	96	2.46%
10	New	Win-Trojan/Agent.57344	64	1.64%
		기타	1709	43.70%
합 계			3,910	100

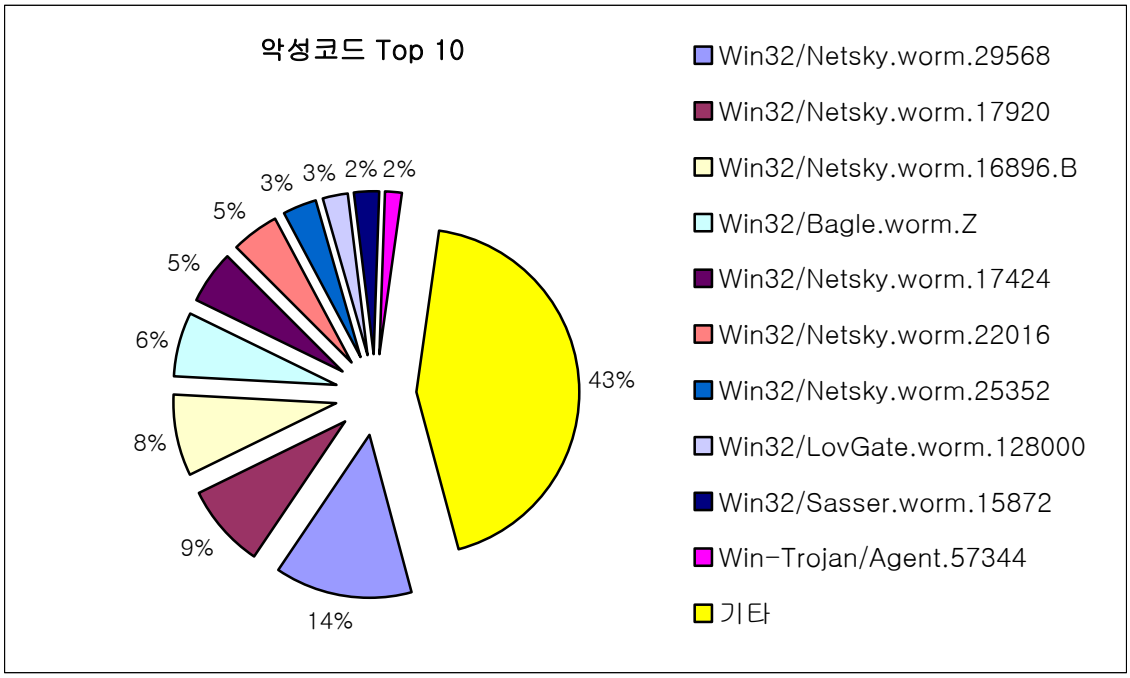
[표1] 2004년 9월 악성코드 피해 Top 10

9월 악성코드 피해 동향

바이러스, 웜, 트로이목마 등의 악성코드로 인한 피해는 올 상반기 내내 상승세를 보이다가 7월부터 급격한 감소세를 나타내기 시작하여 9월에 이르러서는 2004년 최저치를 기록했다. IRCBot 변형의 증가추세가 전체 피해통계에 큰 영향을 끼치지 못하고 있는 부분은 주목할 만 하다. 악성코드 피해통계가 일시적인 감소세인지에 대해서는 지속적인 분석이 필요할 것으로 보인다. 이러한 전체적인 감소세에도 불구하고 여전히 수위를 차지하고 있는 것은 Win32/Netsky.worm.29568을 비롯한 Mass Mailer 들임을 알 수 있다.

악성코드 피해 Top 10에 새로이 진입한 Win32/LovGate.worm.128000과 Win-Trojan/Agent.57344는 전체적인 피해접수 건의 감소에 따른 순위포함으로 볼 수 있으며, 보안 취약점을 이용하여 확산되는 Win32/Sasser.worm.15872(이하 새서 웜)에 의한 피해가 발견초기부터 꾸준히 지속되고 있는 것으로 보아 여전히 보안패치 적용에 소홀함을 알 수 있다.

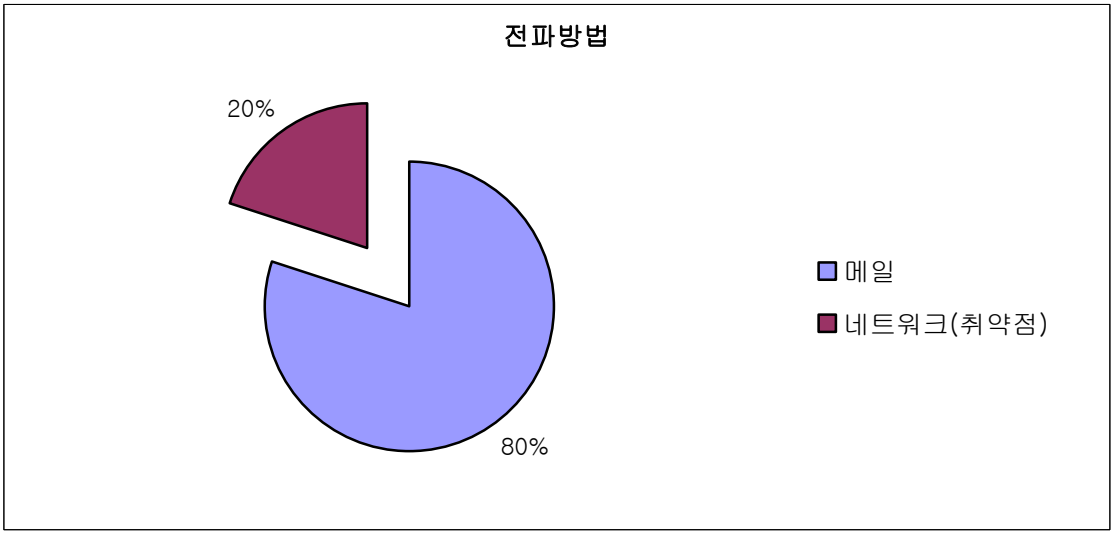
9월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다



[그림1] 2004년 9월 악성코드 피해 Top 10

9월 악성코드 Top 10 전파방법별 현황

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



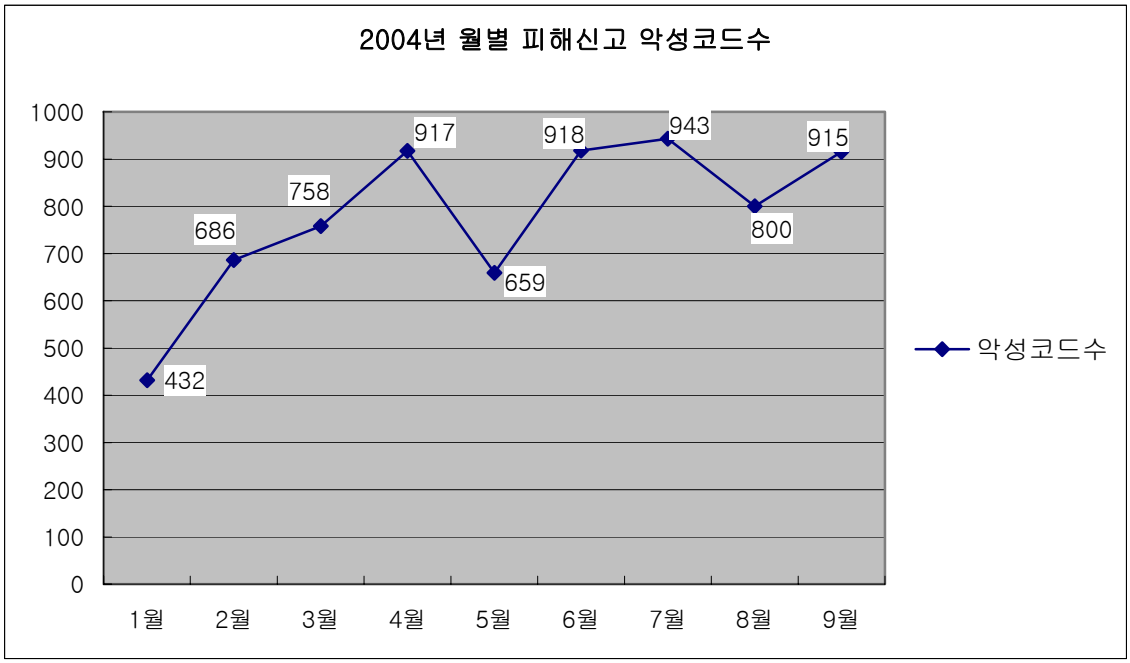
[그림2] 악성코드 Top 10의 전파방법별 현황

Top 10을 차지하고 있는 악성코드의 특징에서는 두드러진 바가 없으나 전파방법 부분에서는, 보안취약점을 이용해 네트워크로 전파되는 새서 웜과 Win-Trojan/Agent를 제외하고는

모두 메일로 전파되는 웜들이 여전히 강세를 보이고 있음을 알 수 있다.

월별 피해신고 악성코드 건수 현황

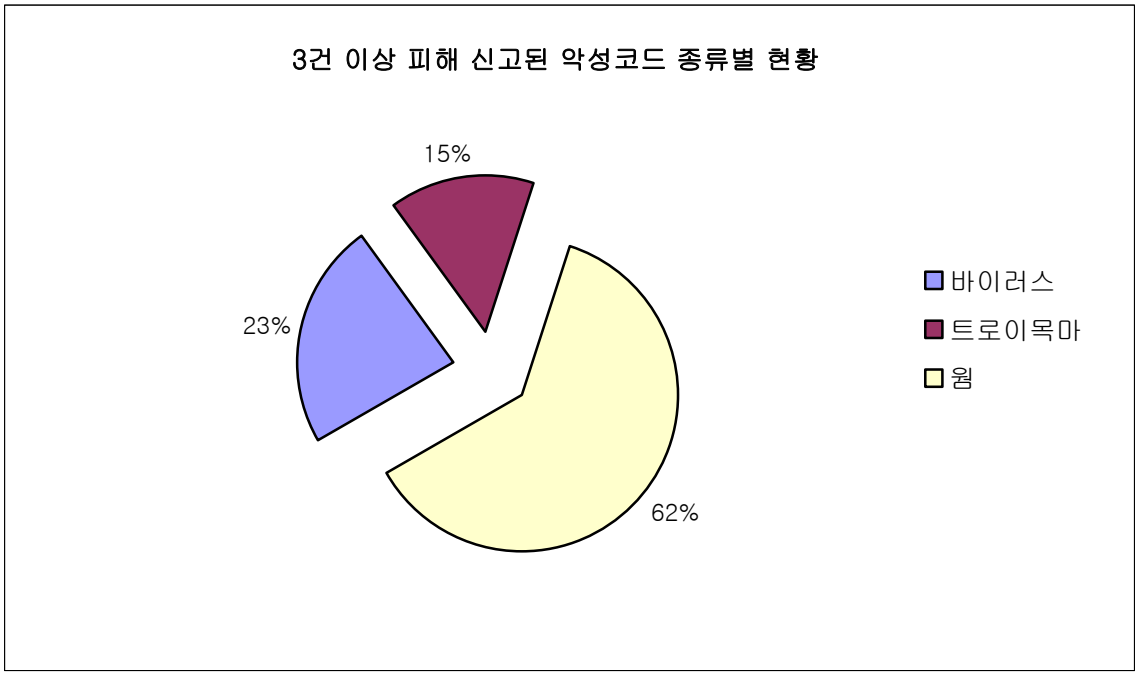
9월에 피해 신고된 악성 코드는 915개이다. 수치적으로는 지난 4월, 6월, 7월의 신고건수와 비슷한 수준으로 대부분이 악성 IRCBot류가 차지하고 있다. 다양한 종류의 악성 IRCBot이 지속적으로 발견되고 활동하고 있음을 알 수 있는 9월이었다([그림3]참조).



[그림3] 2004년 월별 피해신고 악성코드 수

주요 악성코드 현황

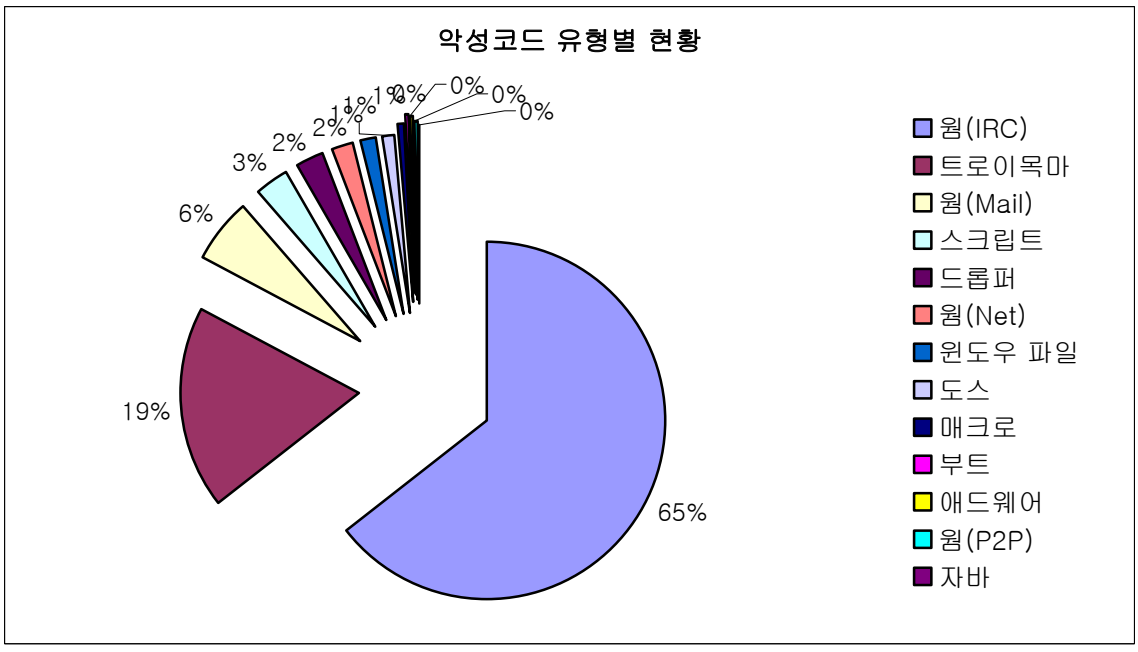
9월에 피해가 접수된 악성코드 중 3건 이상의 문의가 들어온 악성코드의 종류는 [그림4]와 같다.



[그림4] 3건 이상 피해 신고된 악성코드 종류별 현황

웜이 62%(50개)로 가장 많았으며 트로이목마 15%(12개), 바이러스 23%(19개)이다. 바이러스의 개수가 상대적으로 많아 보이는 것은 전체 피해신고가 감소한 것에 기인한다.

악성코드 유형별 현황은 [그림5]와 같다.



[그림5] 악성코드 유형별 현황

9월의 악성코드 피해건수는 눈에 띄게 감소 하였음에도 피해신고된 악성코드의 개수는 피해건수가 많았던 2004년 6월과 7월의 수준이었음을 알 수 있다. 피해신고된 악성코드 개수의 증가는 이에 따른 피해상황 및 새로운 위험요소의 증가를 나타내는 것으로 볼 수 있으므로 시스템 관리자나 PC 사용자들의 입장에서는 이들 악성코드가 주로 이용하는 네트워크 파일 공유나 IRC(Internet Relay Chat) 등에 대한 보다 향상된 관리가 이뤄져야 할 것이다

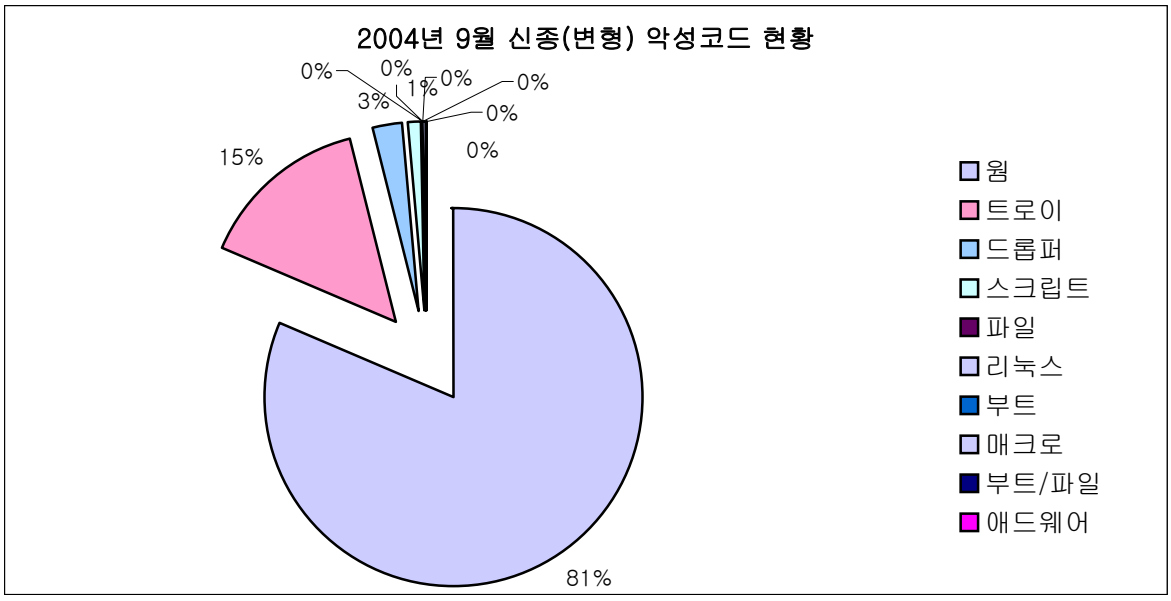
II. 9월 국내 신종 악성코드 발견 동향

작성자 : 정진성 연구원(jsjung@ahnlab.com)

9월 한달 동안 접수된 신종(변형) 악성코드 건수는 [표1], [그림1]과 같다.

웜	트로이	드롭퍼	스크립트	파일	리눅스	부트	매크로	부트/파일	애드웨어	합계
512	93	16	6	0	0	0	2	0	0	629

[표1] 2004년 9월 유형별 신종(변형) 악성코드 발견현황



[그림1] 2004년 9월 신종 악성코드 발견현황

9월 신종 악성코드 동향

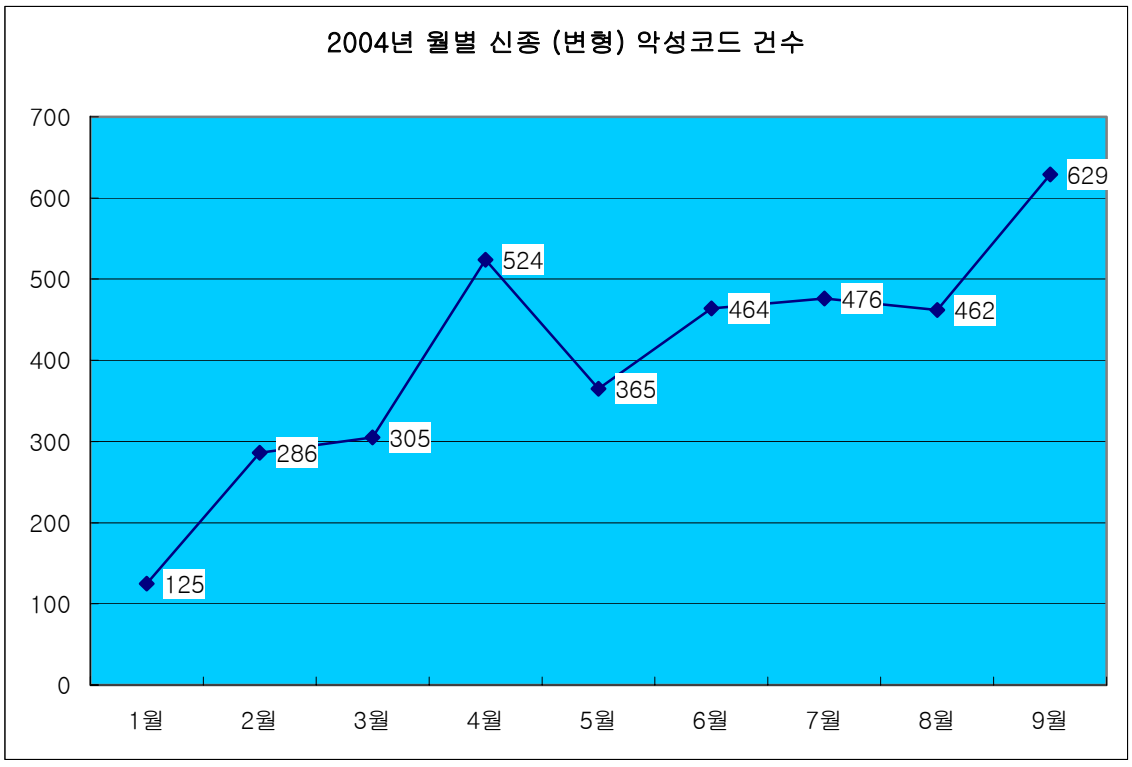
이번 달 핫이슈라면 JPEG 이미지(GDI+) 처리시 발생할 수 있는 버퍼 오버플로우 취약점(MS04-028)[1]을 이용한 악성코드들이 발견, 보고되었다는 것이다. 이 취약점에 대한 내용과 보안패치파일이 제공된지 얼마 되지 않아서 우리는 이 취약점을 이용하는 트로이목마(제작툴)들을 보고 받았다. 이 취약점은 많은 시스템들이 가지고 있으므로 이를 공격하려는 악성코드는 당분간 지속적으로 발견될 것으로 보인다.

그 동안 신종이 발견되지 않았던 매크로 바이러스 2종이 9월에 발견되었다. 특히 이 매크로

[1] MS04-028, JPEG 처리(GDI+)의 버퍼오버런으로 인한 코드 실행 문제
http://www.microsoft.com/korea/technet/security/bulletin/MS04-028.mspx

바이러스들은 MS03-050 취약점[1]을 이용하고있다. 이 취약점의 동작방식은 워드와 엑셀로 나눠지는데 워드의 경우 문서 오픈시 매크로 모듈 네임 크기에 대한 버퍼 오버플로우를, 엑셀의 경우 매크로를 이용하는 것이다. 이 취약점의 문제는 바로 매크로가 포함된 문서들이 워드나 엑셀에서 보안경고 없이 실행될 수 있다는 것이다. MS 오피스는 매크로 바이러스 예방기능으로 문서에 매크로가 존재하는 경우 사용자에게 경고하여 실행여부를 묻거나 아예 매크로를 사용하지 않고 문서를 오픈할 수 있게 한다. 그러나 이 취약점을 이용한 X97M/Netsna, W97M/Netsna 등에 감염된 문서를 실행하면 이러한 경고의 출력없이 문서가 오픈되고 바이러스가 실행되는 것이다.

이번 달은 악성 IRCBot 류의 악성코드가 무려 491개가 접수 되었다. 이러한 원인으로 전체 신종(변형)악성코드의 건수도 629개로 대폭 증가하였다. 이는 V3 엔진에서 악성 IRCBot의 진단율을 향상 했기 때문에 기인한 것으로 보여진다.



[그림2] 2004년 월별 신종(변형) 악성코드 발견 현황

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

▶ Dropper/LowZones

[1] MS03-050, MS 워드 및 MS 엑셀의 보안취약점으로 인해 임의의 코드 실행
http://www.microsoft.com/korea/technet/security/bulletin/MS03-050.asp

이 드롭퍼는 인터넷 익스플로러의 웹 컨텐츠 영역에 대한 보안설정을 변경하는 증상을 가지고 있다. 해당하는 웹 컨텐츠 영역은 다음과 같다.

- 인터넷
- 로컬 인트라넷
- 신뢰할 수 있는 사이트
- 제한된 사이트
- 로컬 시스템 (이 부분은 사용자에게 보여지지 않는다.)

드롭퍼는 위 영역들에 대한 미리 정의된 레지스트리 값을 가지고 있으며 실행되면 이 값을 드롭퍼가 가지고 있는 임의의 값으로 내용을 변경하도록 하는 것이다. 이 부분이 변경되면 변경된 값에 따라서 인터넷 익스플로러가 설정되므로 웹 서핑시 의도하지 않는 Active X 나 자바 애플릿 등이 별다른 경고 없이 다운로드 되어 실행될 수 있다. 따라서 안티 바이러스 제품에서 이 악성코드를 치료한 후에는 반드시 해당 웹 컨텐츠 영역에 대한 설정을 다시 해 주어야 한다.

▶ X97M/Netsna

위에서도 언급한 이 매크로 바이러스는 국내에서 오랜만에 발견된 신종 매크로 바이러스이다. 워드와 엑셀의 보안 취약점을 이용하여 MS 오피스의 보안 경고 없이 감염된 문서의 실행이 가능하다. 워드의 경우 버퍼 오버플로우를 발생한 후 임의의 코드를 실행할 수 있도록 할 수 있으며 엑셀의 경우 엑셀파일의 포맷내 BIFF4 Macro sheet의 값을 0x40에서 특정값으로 변경하도록 하여 보안경고을 무시하고 매크로가 포함된 문서를 실행 할 수 있다. 또한 이 매크로 바이러스는 시스템 정보를 수집 및 발송하는 트로이목마를 생성하기도 한다.

▶ JPEG-Exploit/MS04-028.Gen

JPEG 이미지 처리시(GDI+) 발생할 수 있는 취약점(MS04-028)을 이용한 악성코드 유형이 9월 중순부터 발견되기 시작 했다. 취약점 자체가 heap overflow 형태라 이러한 유형의 악성코드가 제작되어도 모든 시스템들에서 정상동작하지 않는 점이 있어 현재까지는 안심되기도 한다. 지금까지 발견된 이 취약점을 이용한 악성코드는 다음과 같은 유형이였다.

- 특정 URL 에 있는 악의적인 파일 다운로드 및 실행

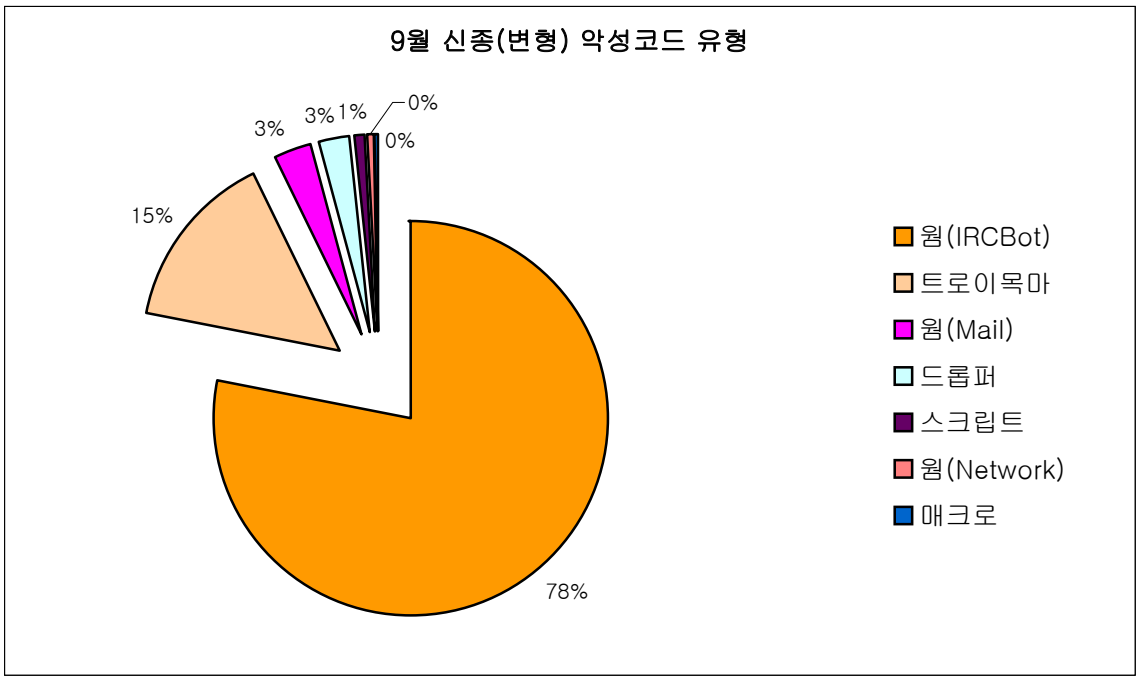
이러한 형태로 인하여 취약점이 포함된 이미지 파일을 생성할 수 있는 'Constructor'가 제작되어졌다. 이 취약점이 가지고 있는 문제는 아무래도 많은 시스템들이 취약점에 노출되어 있고 더군다나 JPEG 형식의 이미지 파일은 웹상에서 쉽게 접할 수 있다는 점에서 우려된다는 것이다. 하지만 취약점을 가진 이미지 파일을 검사하는 방법이 비교적 간단하여 안티 바이러스 제품들에 의해서 진단이 가능하다.

▶ Win32/MyDoom.worm 변형

마이둠 웜 변형이 이번 달에도 몇 개가 발견, 보고 되었다. 이번 달에 발견된 유형은 특정

호스트에서 은폐형 트로이목마를 내려 받아 실행하도록 되어 있다. 이 트로이목마들은 특정 포트를 오픈 해 두며 hosts 파일을 조작하여 안티 바이러스 업체의 홈페이지에 접속하지 못하도록 한다. 또한 자신을 은폐하여 사용자 및 안티 바이러스 프로그램들로부터 자신을 회피한다.

다음은 9월 발견된 신종 (변형) 악성코드의 유형별 현황이다.

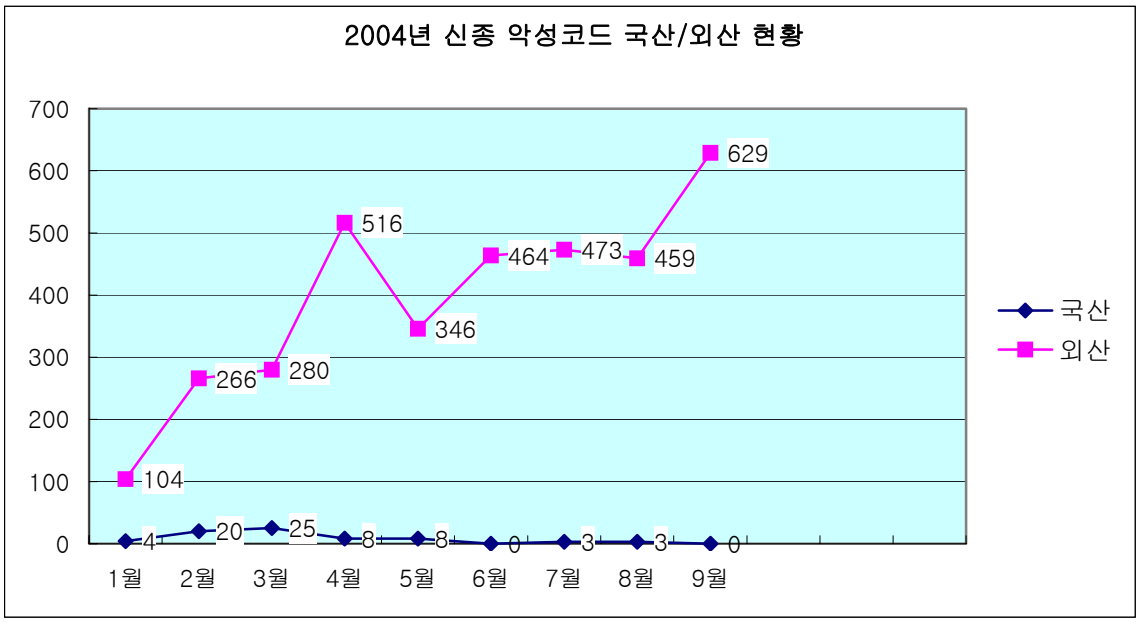


[그림3] 9월 신종 (변형) 악성코드 유형별 현황

언급한 것처럼 악성IRCBot의 비율이 상당히 높았음을 알 수 있다. 그리고 드롭퍼의 비율도 Dropper/LowZones 영향으로 소폭 증가하였다. Mass Mailer들은 기존의 마이둠 웜, 베이글 웜, 러브게이트 웜 변형이 영향을 주었다.

제작지별 신종(변형) 악성코드 현황

다음은 신종(변형) 악성코드들의 국산/외산의 현황이다.



[그림4] 2004년 제작지별 신종 악성코드 현황

상반기 들어 국산 악성코드의 제작이 현저히 줄어들었다. 현재 대부분의 악성코드가 악성 IRCBot류이고 이들 모두가 외산이다. 국산 악성코드 중 악성 IRCBot류나 Mass Mailer 형태는 없고 대부분 애드웨어인데 그 증상이 현격히 악성코드 증상과 유사하다고 판단되면 악성코드로 분류하고 있다. 이렇듯 최근 애드웨어(스파이웨어)의 동작기법들이 악성코드를 매우 닮아가고 있다. 이는 모두 안티 애드웨어 제품들로부터 진단되지 않게 하기 위함이다. 이러한 이유로 악성코드와 애드웨어의 경계가 모호해지고 있으며 앞으로 이러한 현상은 더욱 두드러지게 나타날 것으로 전망된다.

III. 9월 신규 보안취약점

작성자 : 이정형 연구원(jungh@ahnlab.com)

9월달의 중요한 보안 이슈는 JPEG 처리(GDI+)의 버퍼 오버런으로 인한 코드 실행 문제(MS04-028)이다. 이 취약점은 패치가 발표된 후 얼마 지나지 않아 이 취약점을 이용한 트로이목마가 발견될 만큼 악성코드에서 이용할 확률이 높으며, 또한 해당 취약점을 가진 시스템이 많다는 점에서 주목할 만하다. 그 외에 9월에는 한글 윈도우 XP 서비스팩2의 발표 소식이 있었다.

JPEG 처리(GDI+)의 버퍼 오버런으로 인한 코드 실행 문제(MS04-028)

JPEG 처리(GDI+) 버퍼 오버런은 JPEG 파일[1] 처리기능이 들어가 있는 gdiplus.dll 라이브러리에 JPEG 처리부분 중 COM(comment)섹션에 메모리 할당처리를 잘못하여 heap overflow가 발생하는 것이다. 이와 유사한 버그 레포트는 2000년도에 러시아 보안 전문가인 Alexander Peslyak(Solar Designer)가 발표한 JPEG COM Marker Processing Vulnerability in Netscape Browsers(Heap Overflow)가 있다.

취약한 어플리케이션 및 운영체제

취약한 GDI+(gdiplus.dll)을 사용하는 어플리케이션과 운영체제는 아래와 같다(윈도우 2000 및 이전에 발표된 운영체제의 GDI+에는 해당 취약점은 존재하지 않는다).

- Microsoft Windows XP, Microsoft Windows XP 서비스 팩 1
- Microsoft Windows XP 64-Bit Edition 서비스 팩 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server™ 2003
- Microsoft Windows Server 2003 64-Bit Edition
- Microsoft Office XP, 2003
- Microsoft Office XP, 2003
- Microsoft Project 2002 서비스 팩, 2003
- Microsoft Visual Studio .NET 2002, 2003
- Microsoft .NET Framework 버전 1.0 SDK 서비스 팩 2
- Microsoft Picture It! 2002(모든 버전)

[1] JPEG란?

JPEG는 풀 컬러와 그레이 스케일의 압축을 위하여 JPEG 그룹에서 개발되었다. JPG/JPEG는 GIF에 비해 압축 효율이 더 좋으며, 고해상등의 사진/이미지를 저장할 수 있다. 현재 GIF와 같이 인터넷상에서 가장 많이 사용되는 그래픽 이미지 파일 형식 중 하나이다

- Microsoft Greetings 2002
- Microsoft Picture It! 버전 7.0(모든 버전)
- Microsoft Digital Image Pro 버전 7.0
- Microsoft Picture It! 버전 9(모든 버전, Picture It! 라이브러리 포함)
- Microsoft Digital Image Pro 버전 9
- Microsoft Digital Image Suite 버전 9
- Microsoft Producer for Microsoft Office PowerPoint(모든 버전)
- Microsoft Platform SDK Redistributable: GDI+

취약점 분석

JPEG 파일은 JFIF(JPEG File Interchange Format) 형태이며 JFIF는 여러 개의 세그먼트 로 구성되는데 여기서 COM(Comment) 섹션은 각종 코멘트(jpeg를 만든 제작툴명, 디지털카메라 정보 등)를 입력하는데 사용되어 진다.

COM(Comment) 섹션 구조는 다음과 같다.

Marker (0xfffe)	Length (2byte)	Comment 내용

Unsigned Integer 값의 변수인 Comment의 length 값을 1 혹은 0 값을 준다면, Overflow가 발생하게 된다. GDI+ (gdiplus.dll)에서 JPEG의 해당 취약한 코드는 아래와 같다.

▶ Comment 부분의 length-2를 표현하는 코드

```
Lea     edx, [esi-2]
```

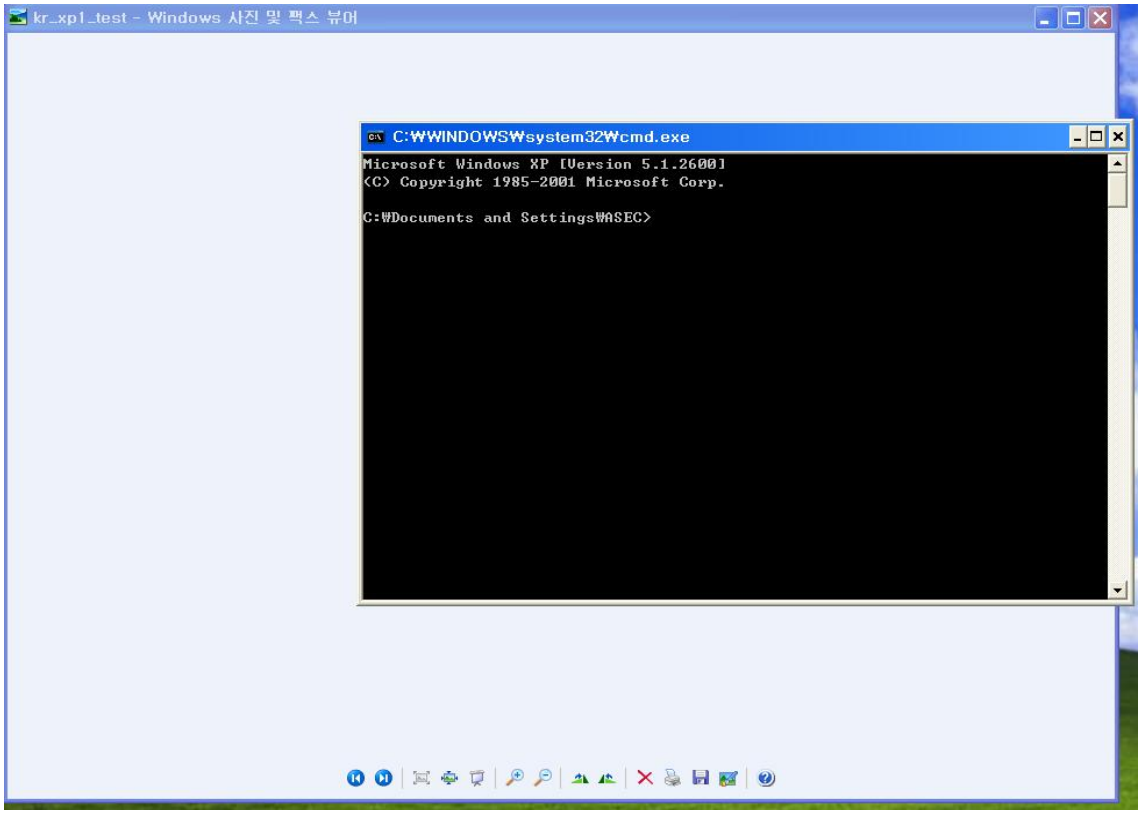
▶ Comment를 heap에 할당하는 코드

```
Mov     eax, [ebx+ 18h]
Mov     esi, [eax]
Mov     edi, [ebp+ arg_4]
Mov     ecx, edx
Mov     eax, ecx
Shr     ecx, 2
Rep     movsd
```

악성코드의 형태

파일에서는 JPEG COM(comment)섹션 취약점을 이용하는 악성 프로그램은 비정상적인 COM 섹션을 가지므로 ff fe 00 00 혹은 ff fe 00 01의 패턴을 가지게 되고, 공격자는 JPEG

의 COM(comment)섹션을 조작하여 악의적인 코드가 내장된 이미지 파일을 인터넷, 메일, 오피스 문서등에 내장시켜 임의의 코드실행, 다운로드 가능, bind port 오픈 등 여러가지 공격이 가능하다. 현재 이 취약점을 이용하는 공격코드가 인터넷상에 공개되어 있어 위험성을 내포하고 있지만, 국가별 OS마다 주소값이 달라 해당하는 웜의 출현은 약간 어렵다고 볼 수 있다.



[그림1] 한글 윈도우 XP 서비스팩 1에서 JPEG 파일 실행할 때 CMD가 자동 실행되는 화면

윈도우 XP 서비스팩 2 에서 Heap 구조 변화

9월 말경에 한글 윈도우 XP 서비스팩 2가 출시되었다. XP 서비스팩 2에서는 PEB Randomization, Heap Header cookie, Safe unlinking를 통한 Heap 보안이 향상되어 있어서, 이러한 Heap Overflow 공격은 앞으로 매우 어려워질것으로 보여진다.

보안패치

JPEG 처리(GDI+)의 버퍼 오버런으로 인한 코드 실행 문제는 최대 위험등급이 긴급이므로 아직 취약점을 패치않은 사용자는 MS-04-028를 참조하여 보안패치를 적용하도록 하자.

참고자료

http://marc.theaimsgroup.com/?l=bugtraq&m=109524346729948

http://www.openwall.com/advisories/OW-002-netscape-jpeg/

http://www.microsoft.com/korea/technet/security/bulletin/MS04-028.mspx

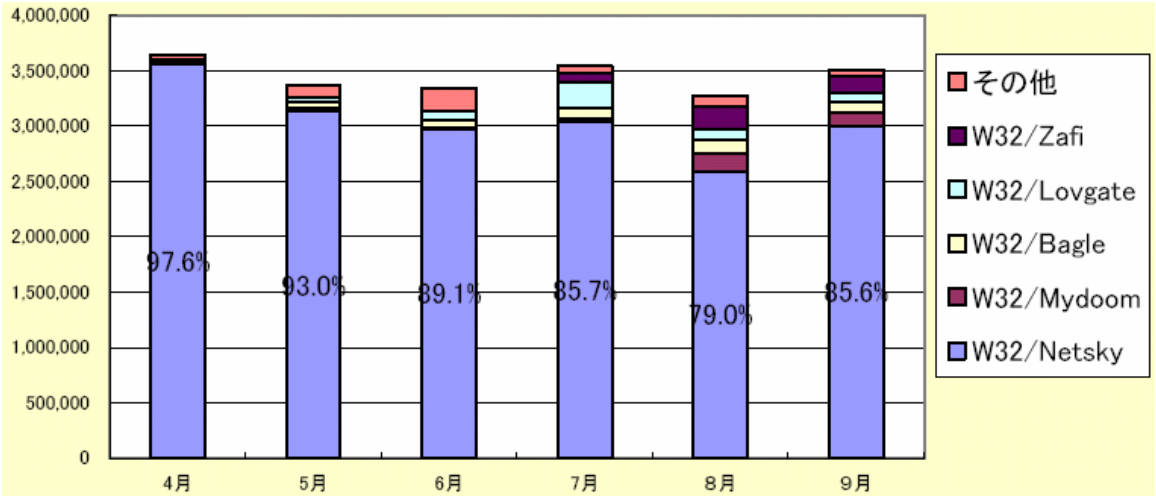
http://support.microsoft.com/default.aspx?scid=fh;KO;WINDOWSXPSP2

Ⅳ. 9월 일본 피해 동향

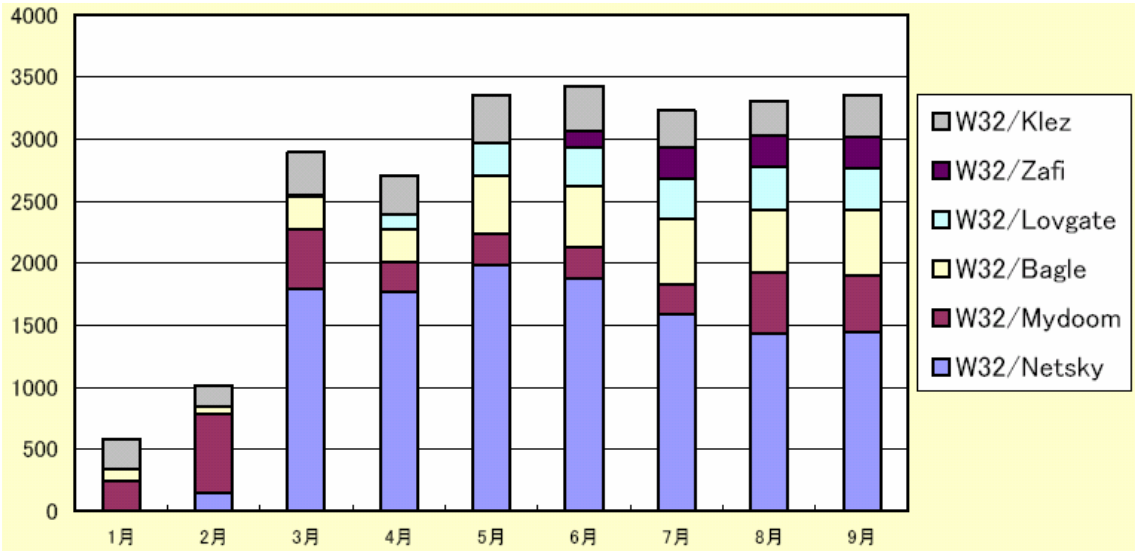
작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

일본 IPA에서는 올해 3분기 동안의 악성코드 및 보안과 관련된 피해에 대한 통계자료를 발표하였다. 아래의 [표1]과 [표2]는 그 중 월별 악성코드 감염 피해에 대한 자료를 표로 나타낸 것이다.

[표1]에서 알 수 있는 것처럼 3/4분기에도 여전히 Win32/Netsky.worm(이하 넷스카이웜)이 활발하게 유포되고 있는 것을 알 수 있다. 또한 2/4분기와 비교하여 8월과 9월에는 넷스카이웜의 확산은 상대적으로 줄어들고, Win32/Zafi.worm(이하 자피 웜)과 Win32/Mydoom.worm(이하 마이둠 웜)에 노출된 사용자가 늘어난 점을 알 수 있다. 특히 [표2]에서도 볼 수 있는 것처럼 지난 6월 발견된 자피 웜의 변형이 현재까지도 많이 감염되어 확산되고 있는 상태임을 알 수 있고 이는 자피 웜의 확산도가 그리 높지 않은 한국의 상황과 비교했을 때 주목할 만한 점이다.



[표1] 월별 악성코드 노출 통계 (출처: 일본 IPA)



[표2] 월별 악성코드 감염 통계 (출처: 일본 IPA)

일본 유행 악성코드 유형별 발생현황

아래의 [표3]은 IPA/ISEC에서 발표한 2004년 9월의 악성코드 노출에 대한 통계자료이다. [표3]에서 알 수 있는 것처럼 2004년 9월 일본에서 가장 많이 확산된 악성코드는 넷스카이 웜이다. 넷스카이 웜의 확산 정도는 전월과 비교하였을 때 크게 차이가 없는 것으로 보인다. 마이둠 웜과 자피 웜 의 노출건수 또한 전월과 마찬가지로 줄어들지 않고 많은 감염 피해가 보고된 것을 볼 수 있는데 특히 자피 웜 의 경우 2004년 6월 새로운 변형이 나타난 이후로 특별하게 다른 변형이 발견되지 않은 상태임에도 불구하고 여전히 많은 확산도를 보여주는 점이 주목할만하다.

Window/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Netsky	1,438	Xm/Laroux	23	VBS/Redlof	104
W32/Bagle	530	X97M/Tristate	4	Wscript/Kakworm	13
W32/Mydoom	455	WM/Cap	3	Wscript /Fortnight	11
W32/Klez	340	W97M/Bablas	3	VBS/ Internal	6
W32/Lovgate	328	W97M/Ethan	2	VBS/Loveletter	6
W32/Zafi	255			VBS/Haptime	2

[표3] 악성코드 노출 신고 현황

일본 네트워크 트래픽 현황

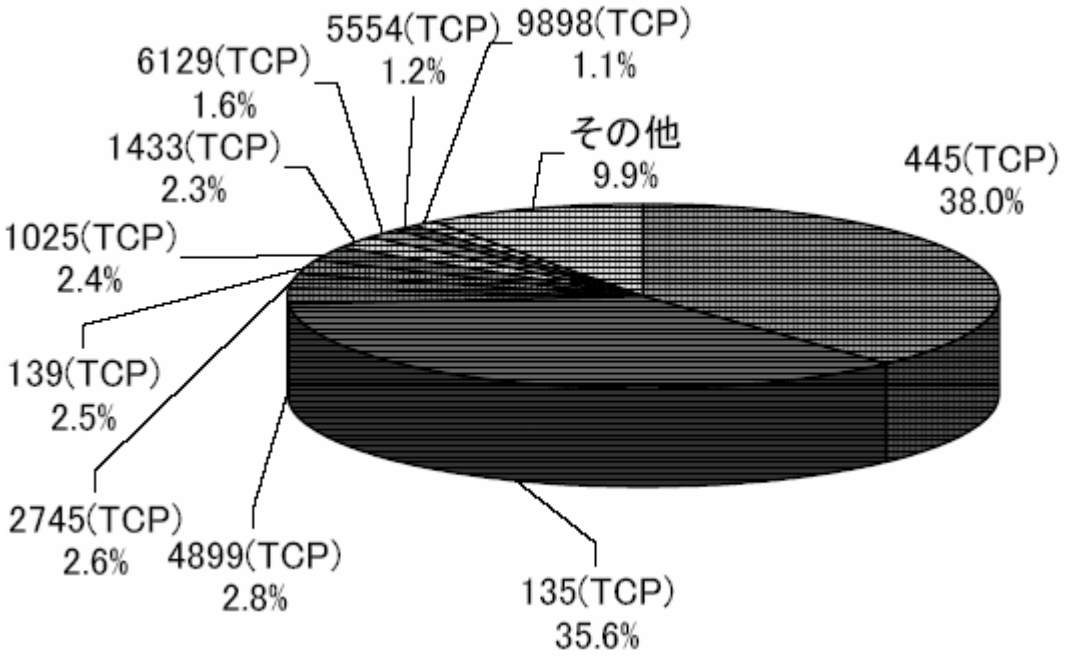
[그림1]은 2004년 9월 일본의 네트워크 포트 사용현황을 도식화한 것이다.

[그림1]의 데이터에 대해서 간략히 살펴보면 먼저 가장 많은 네트워크 트래픽이 발생한 포트는 TCP 135 와 TCP 445 이다. 이 포트들은 윈도우의 인증과 관련하여 사용되지만 최근

유행하는 네트워크를 통해 전파되는 웜들이 윈도우 운영체제의 취약점을 이용한 공격을 시도할 때 사용되는 경우도 있다. 이러한 경우 감염을 예방하기 위해서는 운영체제의 최신 패치가 필수적이다.

이외에도 TCP 4899 포트와 TCP 2745 포트, TCP 139 포트의 사용량이 많은데 이 포트들 또한 악성코드에서 이용할 가능성이 있다.

TCP 4899 포트는 상용 프로그램에서 사용되는 포트이지만 블래스터 웜에서 사용되는 포트이기도 하다. TCP 2745 포트 또한 베이글 웜에 감염된 시스템에 설치된 백도어에서 사용되는 포트이다. TCP 139 포트도 아고봇에 감염된 시스템에서 오픈되는 포트 중 하나이다.



[그림1] 일본의 네트워크 트래픽 현황

V. 9월 중국 피해 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

선선한 바람이 부는 가을의 문턱에 들어선 9월은 한 여름의 무더위를 잠시 잊게 해주는 때가 아닌가 싶다. 특히 북경과 같이 7월, 8월 무더운 날씨를 보내고 가을의 선선한 바람을 맞이하는 지역에서는 또 다른 계절의 묘미와 풍경을 느끼게 한다.
가을의 시작을 알리는 9월의 중국 악성코드 동향은 메일로 전파되는 매스메일러(Mass Mailer)들의 새로운 변형 등장과 악성코드가 이용할 가능성이 높은 새로운 마이크로소프트의 윈도우 취약점 발견이 많은 관심을 받았던 것으로 분석된다.

악성코드 TOP 5

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

[표1] 2004년 9월 악성코드 TOP 5

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

9월 중국 악성코드 동향은 서서히 감소 추세를 보이던 매스메일러 변형이 다시 대거 등장한 것이 특징이다. 8월 중국 악성코드 동향의 맺음말에서 언급했던 새로운 매스메일러들의 등장 우려는 새로운 Win32/MyDoom.worm의 변형(Win32/MyDoom.worm.18200, Win32/MyDoom.worm.18432.B, Win32/MyDoom.worm.88640 등, 이하 마이둠 웜)과 Win32/Bagle.worm의 변형(Win32/Bagle.worm.AR 등, 이하 베이글 웜)의 등장으로 현실화 되었다. 이러한 등장으로 인해 지난 2월과 같은 대규모의 매스메일러 확산을 우려하는 목소리가 적지 않았으나 다행히 많은 피해는 주지 않은 것으로 보인다. [표1]의 9월 악성코드 TOP 5를 보면 새로운 매스메일러 변형들의 등장에도 불구하고 지난 8월 달과 동일하게 순위 변동 없이 현상 유지를 보이고 있다. 새로운 마이둠 웜과 베이글 웜 변형의 등장으로 인해 9월 악성코드 분포상으로는 네트워크로 전파되는 웜들의 피해가 일시적으로 잠시 줄어들고 메일로 전파되는 매스메일러의 영향이 다시 증가했던 한 달로 분석된다.

주간 악성코드 순위

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

[표2] Rising 2004년 9월 주간 악성코드 순위 변화

순위	1주	2주	3주	4주
1	Worm_Netsky.D	Worm_Netsky.D	Worm_Netsky.D	Worm_Netsky.D
2	Worm_Lovgate.C	Worm_Lovgate.C	Worm_Lovgate.C	Worm_Lovgate.C
3	Worm_AgoBot	Worm_Bbeagle.J	Worm_Bbeagle.J	Worm_Bbeagle.J
4	Worm_Bbeagle.J	Worm_AgoBot	Worm_Mydoom.F	Worm_Mydoom.F

[표3] CNCVERC 2004년 9월 주간 악성코드 순위 변화

위 [표2]와 [표3]는 라이징(Rising)사와 CNCVERC에서 작성한 주간 악성코드 동향이다. 전체적인 주간 흐름에는 [표1]의 9월 악성코드 TOP 5에서와 유사한 동향을 보여주고 있다. 그러나 9월 마지막 주에는 일시적으로 Worm.Lovgate(Win32/Lovgate.worm, 이하 러브게이트 웜)이 Worm.Netsky(Win32/NetSky.worm, 이하 넷스카이 웜)을 누르고 1위로 도약한 것을 알 수 있다. 그러나 이러한 현상은 일시적인 것으로 추정되며 특히 9월 마지막 주는 추석 연휴와 10월 1일 중국의 국경절로 이어지는 2주가 넘는 장기간의 연휴로 인해 다른 주간에 비해 감염 신고건수가 급격하게 줄어 들은 것에 기인한다고 볼 수 있다. 특히나 기존 신고건수의 절반도 못 미치는 수치로 인해 다른 주와 단순 비교, 분석에 곤란하다 보여진다.

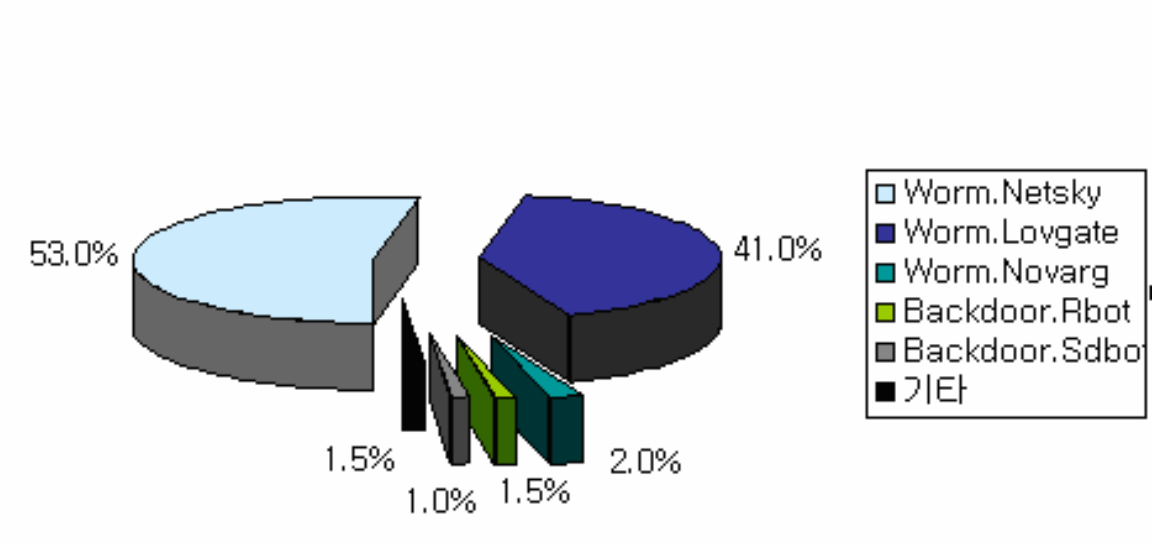
신종 악성코드 및 신규 보안 취약점 동향

중국은 전통적으로 다양한 트로이목마가 많이 발견되는 곳으로 유명했던 만큼 이번 9월달에 발견된 주목할 만한 신종 악성코드 3건 모두 트로이목마로 구성되었다. 그 중에서도 다양한 감염경로를 통해 지속적인 변형이 발견되고 있는 QQ 메신저의 트로이목마가 2건이나 발견되었다. 이번에 발견된 QQ 트로이목마는 Trojan.QQrex.a과 Trojan.QQPass.m로 9월 첫째주와 셋째주에 일시적인 감염 신고가 증가하였으나 다시 소강상태로 접어든 것으로 분석된다. 기존의 QQ 트로이목마들은 QQ 트로이목마를 통해 전파되며 인터넷 익스플로러의 메인 페이지를 특정 웹 페이지로 고정시키는 등의 기능을 가지고 있었다. 그러나 이번에 발견된 Trojan.QQrex.a은 기존의 QQ 트로이목마 기능에 해당 시스템을 원격제어 할 수 있는 백도어 기능까지 추가되어 QQ 메신저를 이용하는 사용자들의 각별한 주의가 필요하리라 여겨진

다. 또 새로이 발견된 다른 트로이목마로는 Trojan.Happyear로 기타 트로이목마 보다 많은 감염 및 문의 신고가 접수된 것으로 파악된다. Trojan.Happyear는 해당 트로이목마의 제작자로 추정되는 해커가 특정 웹사이트를 개설한 후 해당 웹 사이트를 원활하게 사용하기 위해서는 마이크로소프트에서 배포하는 최신 프로그램을 설치하도록 하여 해당 트로이목마의 설치를 유도한 것으로 추정하고 있다. 특히 메일을 통해 해당 웹사이트가 무료로 온라인 영화를 볼 수 있다고 사용자를 속이는 사회 공학 기법으로 인해 기타 트로이목마들에 피해가 많았던 것으로 분석된다.

이번 9월 달에 알려진 신규 취약점은 마지막 주에 알려져 많은 보안업체들에서 경고한 마이크로소프트 윈도우에서 발견된 JPEG GDI+ 취약점(MS04-028)이 있다. 해당 취약점은 취약한 윈도우 시스템에서 악의적인 JPEG 파일[1]을 실행할 경우 버퍼 오버플로우가 발생하게 되어 공격자가 설정한 악의적인 코드를 관리자 권한으로 실행되도록 한다. 그리고 10월 초에는 해당 취약점이 있는 JPEG 파일을 제작할 수 있는 공격툴인 Constructor/JPEG-Expliot.7664도 발견되었다. 이러한 취약점은 곧 또 다른 악성코드의 감염경로로 사용될 가능성이 높으므로 윈도우 시스템 사용자들의 각별한 주의가 필요하며 마이크로소프트에서 배포하는 패치를 반드시 설치하도록 하여야 한다.

악성코드 분포



[그림1] 2004년 9월 중국의 악성코드 분포

[표1]의 9월 악성코드 TOP 5가 지난 달과 동일한 순위를 보였듯이 [그림1]의 9월 악성코드의 분포도 8월의 것과 거의 동일한 형태를 보이고 있다. 그러나 두 웜의 분포 수치면에서는 넷스카이 웜이 1% 증가하여 전체의 절반을 넘은 53%를 차지하고 있다. 이에 반해 러브

[1] MS04-028 취약점을 이용한 악의적인 JPEG 파일을 V3에서는 JPEG-Exploit/MS04-028.Gen으로 진단하며, 라이징사에서는 Suspicious JPEG MS04-028 Exploit로 진단한다

게이트 웜은 1% 감소한 41%를 차지하고 있는 것으로 분석된다. 그리고 마이둠 웜은 새로운 변형의 발견에도 불구하고 지난 8월보다 1% 감소한 2%를 차지하고 있으며 전체 악성코드 분포면에서 유일하게 수치가 증가한 악성코드는 8월 악성코드 분포에서는 기타에 포함 될 정도 미약했던 악성 IRCBot 웜의 변형들인 Backdoor.Rbot과 Backdoor.Sdbot(Win32/IRCBot.worm, 이하 아알씨 봇 웜)이 1.5%와 1.0% 증가한 수치를 보여주고 있다는 점이다. 해당 아알씨 봇 웜은 그 수치는 적으나 이제까지 발견된 변형들의 엄청난 숫자만큼이나 다양하게 퍼져 있음을 추정할 수가 있다.

맺음말

이번 9월 중국 악성코드 동향은 새로운 변형이 발견된 베이글 웜과 마이둠 웜으로 인해 메일로 전파되는 매스메일러들의 새로운 확산 시도가 주목된다. 이러한 동향이 언제까지 지속될 것인가와 윈도우의 새로운 취약점의 발견으로 인해 악성코드의 새로운 감염경로가 발견된 점이 이번 9월 중국 악성코드 동향의 주목할 만한 점으로 분석된다. 새로운 마이크로소프트의 윈도우 취약점이 발견될 때마다 나오는 이야기지만 취약점을 제거할 수 있는 패치 적용이 안전한 컴퓨터 시스템을 사용하기 위해 지나칠수 없는 부분이라는 점을 새삼 되새겨 보게 된다.

VI. 테크니컬 컬럼 I - 또 하나의 위협, 피싱(Phishing)

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

최근 피싱의 피해가 증가하면서 피싱에 대한 관심이 높아졌다. 이 글에서는 최근 새로운 위협으로 떠오르고 있는 피싱에 대해 알아 보겠다.

피싱(Phishing)의 정의

주로 위장된(Spoofed) 메일주소, 웹페이지를 통하여 사용자의 계정, 패스워드, 주민등록번호, 카드번호 등을 수집하는 기법을 말하며, 기법 자체는 특별한 기술이 필요하지 않으나 직접적으로 범죄에 악용될 수 있고 불특정 다수의 일반 사용자를 대상으로 한다는 점에서 매우 큰 사회적 반응을 불러 올 수 있다. 미국 등에서 이미 Citibank, eBay, U.S.Bank, Paypal, AOL, VISA등을 사칭한 피싱 사건이 발생하였으며 꾸준한 증가 추세이다. 현재 피싱 기법은 영어권에서 발생하여 국내 피해는 크게 발생하지 않았지만 기법이 매우 쉽기 때문에 국내에서 발생할 경우에도 큰 피해를 낳을 수 있다. 피싱을 통한 개인 정보 취득은 안티 피싱 워킹 그룹(Anti-Phishing Working Group) 추산 5%, 가트너 추산 3% 의 성공률을 보인 만큼 매우 큰 피해를 발생 시킬 수 있다.

피싱 기법

특별한 보안취약점, 공격 코드 등을 사용하는 것이 아닌 특정 은행, 사이트의 E-mail 주소를 위장(Spoofed)하거나 이와 비슷한 E-mail 주소, URL을 사용하여 사용자를 속이게 한다. 즉 support@verify-visa.org 라는 메일주소를 사용하여 비자 카드에 대한 이벤트 정보나 확인 정보를 담은 내용의 메일을 무작위 사용자에게 보내어 이에 속은 사용자가 답신을 주게 되거나 의도된 웹사이트(URL 역시 비슷한 가짜를 사용하여 실제 사이트와 구별이 힘들게 구성)에 접속하여 사용자의 아이디(ID), 비밀번호(Password), 카드번호 등을 입력하게 하는 기법이다. 특히 최근에는 인터넷 익스플로러 주소창, 상태창 등에 나오게 되는 주소(URL)를 더 정교히 속이기 위해 보안취약점을 같이 사용하는 사례가 있어 사용자의 주의가 소홀할 경우 대부분 속게 된다.

▶ E-mail주소

피싱은 스팸처럼 무작위 사용자에게 발송되는 것이 대부분이다. 이때 스팸과 다른 점은 사용자 개인 정보 수집 목적이라는 점도 있지만 발신자의 주소를 속이거나 비슷한 메일주소를 사용하여 부주의한 사용자의 경우 쉽게 속게 된다는 점이다.

메일 발송시 사용되는 SMTP 프로토콜 자체가 갖고 있는 발신자(MAIL FROM 헤더)와 회신인의 주소가 동일하지 않을 수 있는 점을 이용하여, 발신자의 메일주소를 속이고 메일을 회신 받는 주소는 발신인과 다른 회신인(Return-Path헤더)을 사용한다. 이러한 경우 사용자는

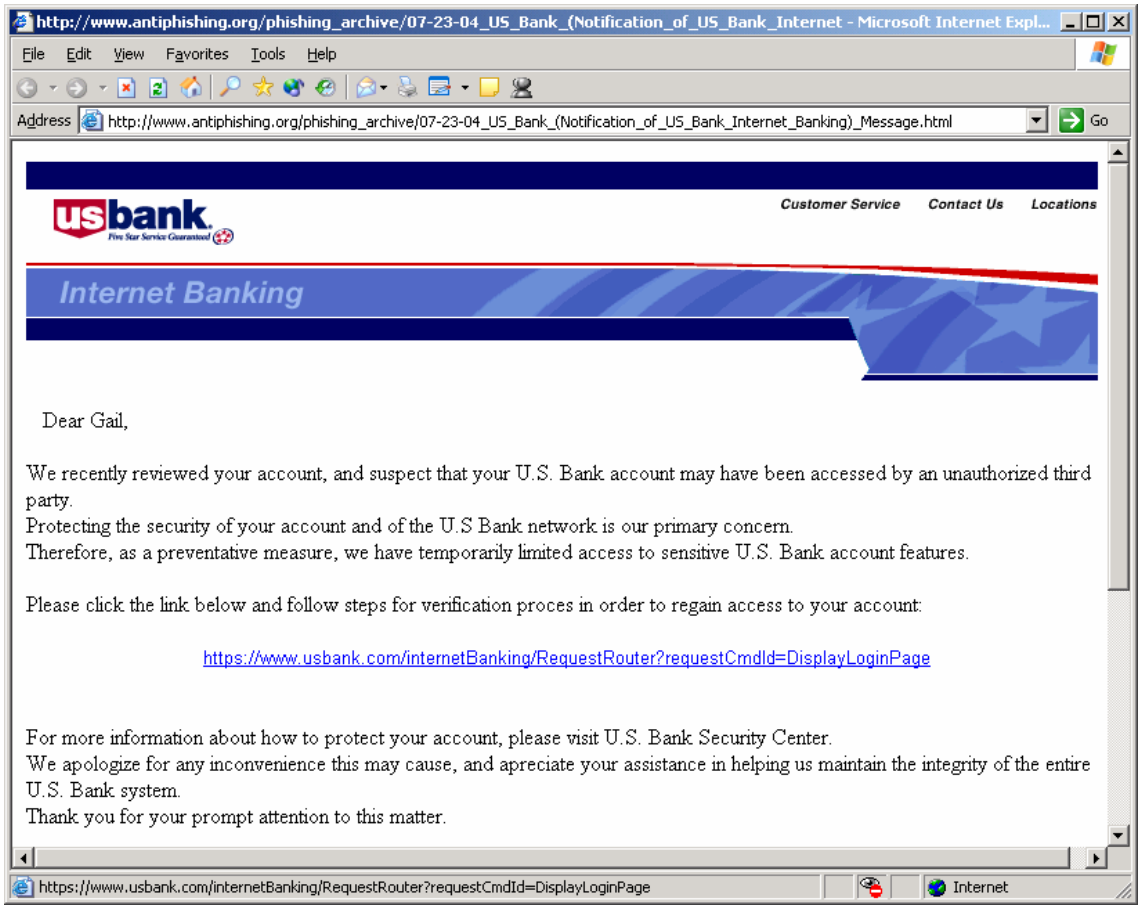
발신자만을 확인할 경우 쉽게 속을 수 있다. 또한 발신자를 속이지 않더라도 도용 대상의 비슷한 도메인을 소유할 경우-예를 들어 verify-visa.org는 실제 VISA사와는 전혀 무관한 도메인이다-역시 일반 사용자는 쉽게 속을 수 있다.

▶ 웹사이트

직접적으로 E-mail을 통해 개인 정보를 요청하여 이를 회신메일로 받아내는 피싱 기법이 있지만 이보다 더 사용자가 쉽게 속을 수 있는 방식은 이벤트, 신원확인 메일 등을 가장하여 위장된 웹사이트에 접속하게 하는 방식이 최근 피싱의 대부분이다.

사례 1

- 2004년 6월 23일 발생
- 메일 발신인: service@usbank.com (가짜 메일주소)
- 메일 제목: Notification of US Bank Internet Banking



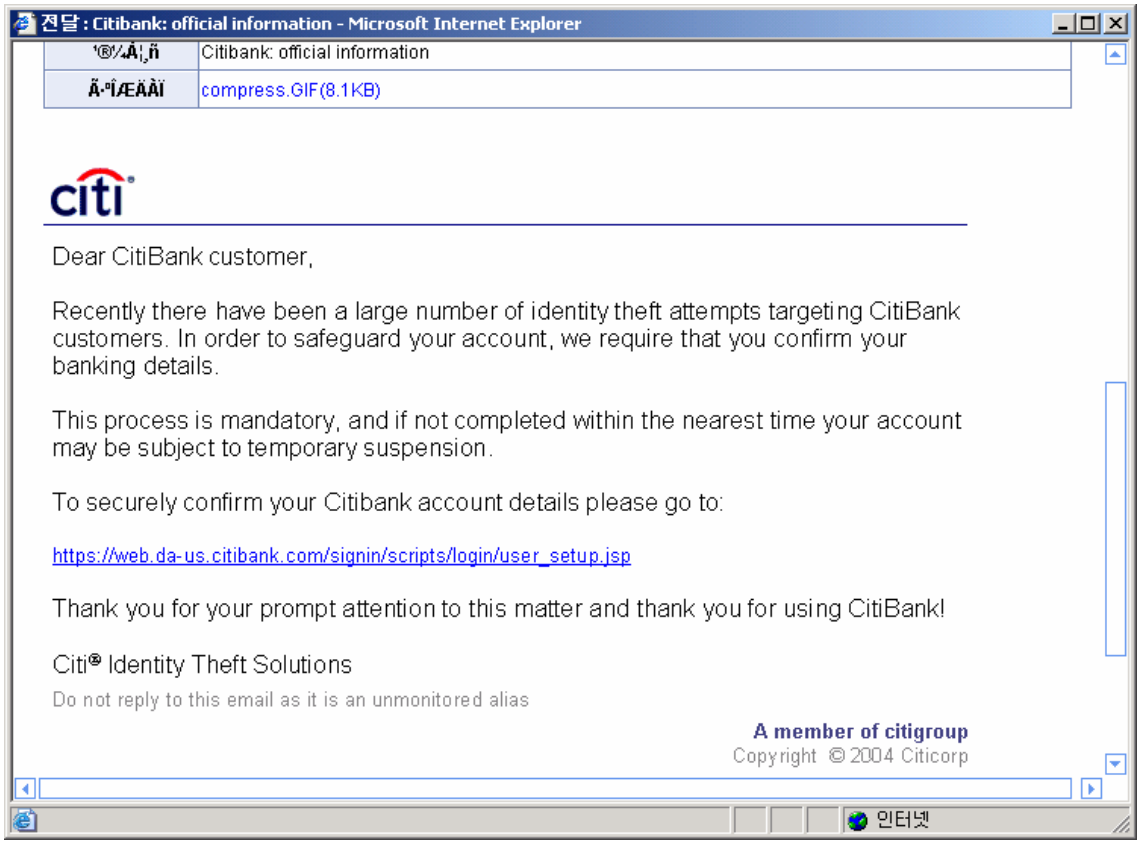
[그림1] US.Bank를 사칭한 피싱메일

해당 메일은 HTML을 포함하여 U.S.Bank를 사칭하여 U.S.Bank에 로그인하도록 위장하고 있다. 실제 해당 URL위에 마우스커서를 올려놓을 경우 상태창에는 www.usbank.com이 나

오게 되지만 실제 클릭할 경우 자바 스크립트(JavaScript)를 사용하여 http://www.usbankdate.com/에 접속되게 된다. 이 www.usbankdate.com 도메인은 실제 U.S.Bank 사이트와는 전혀 무관하며 비슷한 이름이기 때문에 사용자는 속게 된다.

사례 2

다음은 국내 사용자에게도 보내진 피싱 메일로 제목이 'Citibank: official information' 혹은 'CitiBank: Urgent Security Notification'으로 되어 있어 시티은행에서 보낸 공지인 것처럼 위장해 있다. 화면에는 https://web.da-us.citibank.com의 주소로 접속하는 것처럼 속이지만 실제 접속하는 주소는 다른 주소였다.



[그림2] 국내 사용자에게 전달된 씨티은행을 사칭한 피싱 메일

기타 더 많은 실제 사례를 http://www.antiphishing.org/phishing_archive.html에서 확인할 수 있다.

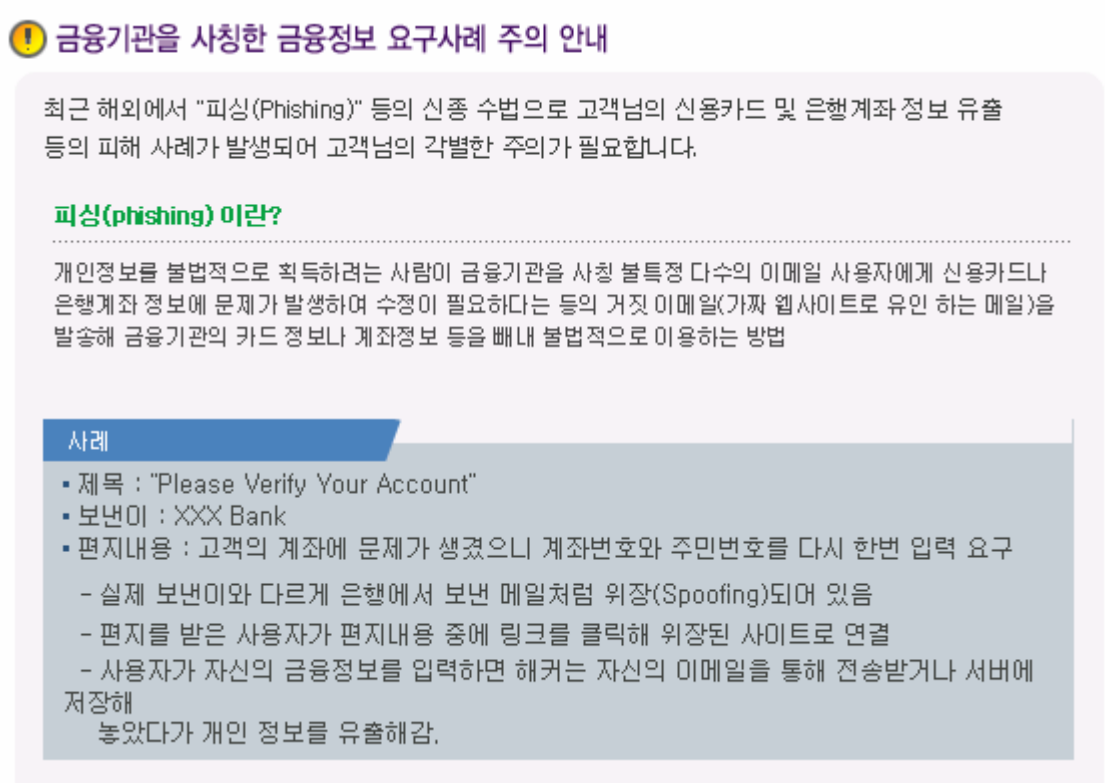
국내 사례

국내에는 현재까지 금융권을 사칭한 피싱 사건은 없었다. 하지만, 그럴듯하게 가짜로 만든 사이트를 이용해 개인의 비밀번호를 훔친 사례는 존재한다.[1] 비밀번호를 알아내려는 사용자

[1] 관련기사, 어느 e메일 해커의 고백 "간단한 속임수가 80%나 통하더라구요"

에게 가짜 메일을 보내 교묘히 작성된 가짜 사이트에 접속해 로그인하게 해 정보를 빼가는 방식이다.

국내에는 아직 금융 사기 형태의 피싱은 발생하지 않았지만 여러 금융 기관에서 고객들에게 피싱에 대한 주의 메일을 보내고 있다.



[그림3] 국내 금융기관에서 금융기관을 사칭한 피싱메일에 대한 주의를 안내하는 메일

http://news.naver.com/news/read.php?mode=LSD&office_id=031&article_id=0000030133&section_id=105&menu_id=105

VII. 테크니컬 컬럼 II - 악성코드에 의한 네트워크 위협과 분석

작성자 : 정관진 주임연구원(intexp@ahnlab.com)

산업혁명 이후 빠르게 우리 생활 깊숙이 파고 들어온 것이 IT(Information Technology)혁명이라 할 수 있다. 많은 기업들은 이제 IT 자산을 이용하여 비용을 절감하고 효율화를 추구하는 등 없어서는 안될 중요한 인프라 자원이 된 것이다. 하지만 이러한 편리함의 발전에는 또 다른 방해물인 웜, 바이러스와 같은 악성코드들이 존재하여 인프라 위협을 주고 있다. 이러한 악성코드는 기업의 네트워크 인프라에 커다란 위협으로 다가오고 있으며, 이에 대한 올바른 이해와 해결이 뒤따른다. 이번 호는 악성코드에 의한 네트워크 위협과 이에 대한 분석에 대해 알아보고 3개월에 걸쳐 연재한 트래픽분석에 대한 마침표를 찍고자 한다.

악성코드 위협과 범위

우선 악성코드의 정의부터 보면 악성코드(Malicious Code)는 말웨어(Malware), 악성 프로그램(Malicious Program) 등으로도 불리며 제작자가 의도적으로 사용자에게 피해를 주고자 만든 모든 악의적인 목적을 가진 프로그램 및 수행 가능한 매크로, 스크립트 등 실행 가능한 형태의 모든 유형을 포함하여 정의한다. 여기서 우리가 관심을 가지고 보아야 할 것은 바로 네트워크에 위협을 줄 수 있는 수준에 해당하는 악성코드들이다. 물론, 악성코드 자체로서도 위험하지만 네트워크에 영향을 주는 악성코드에 대한 것으로 이 문서에서는 범위를 한정 짓고자 한다.

그렇다면 악성코드 중에서도 네트워크에 영향을 주는 것으로는 웜(Worm)이 가장 큰 비중을 차지하게 될 것이다. 웜의 일반적인 정의는 바이러스와는 달리 다른 파일을 감염시키지 않고 자신을 복제하는 능력을 가진 프로그램을 말한다. 흔히, 말하는 자기복제의 개념이 바로 웜이다. 웜은 스스로 자기 자신을 전파하기 위하여 이메일, 공유폴더, 메신저 및 P2P 네트워크, 취약점 등 기타 다양한 전파방법을 사용하고 있다.

이러한 전파방법의 공통적인 사항은 네트워크를 기반으로 이뤄진다는 사실이다. 하지만 이러한 전파방법이 네트워크에 직·간접적으로 큰 영향을 주는 것은 일반적으로 전파방법, 전파대상, 전파속도 등에 의하여 한정지어 지게 된다.

많은 웜들이 빠른 속도로 감염시키기 위해 한 가지 이상의 전파방법을 사용하기도 하며, 대상의 범위가 내부 또는 외부가 되기도 한다. 내부 네트워크는 같은 서브넷에 255.255.255.255 주소로 브로드캐스팅(Broadcasting)이 가능하며, 외부 네트워크와 비교하면 영향을 미칠 수 있는 범위가 달라지게 된다. 즉, 환경적 요인에 영향을 받게 된다.

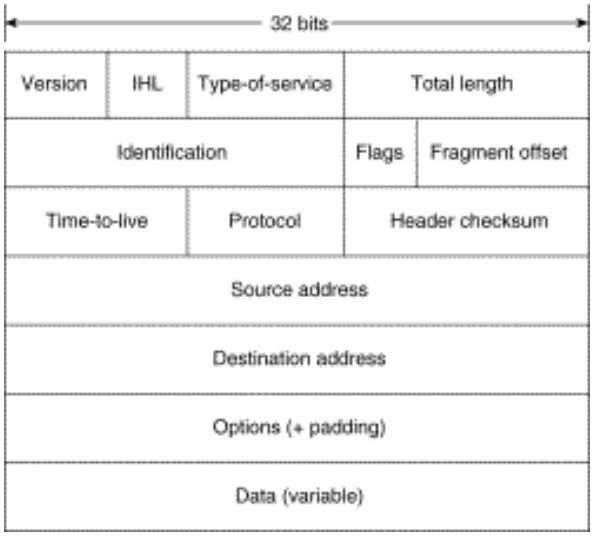
또한, 빠른 속도로 전파한다는 것은 많은 트래픽을 유발시킨다는 것과 같은 개념으로 볼 수 있게 된다. 하지만, 모든 웜들이 이에 해당하는 것은 아니다.

이와 같이 위와 같은 조건에 일정한 범위이상으로 만족하게 되면 네트워크에 위협적인 존재가 되는 것이다. 물론, 네트워크 위협에 대해 느끼는 범위는 모두 다르게 될 것이다. 이것은 크게 네트워크 사용범위와 구성환경 기준의 범위에 따라 위협의 수준을 판단하게 될 것이다. 네트워크에 의존하는 업무 비율이 높다면 이러한 악성코드가 주는 영향에 민감할 것이며, 10Mbps 또는 100Mbps 와 같은 속도 및 구성환경에 따라서도 유발하는 트래픽이 미치는 영향은 달라질 것이다.

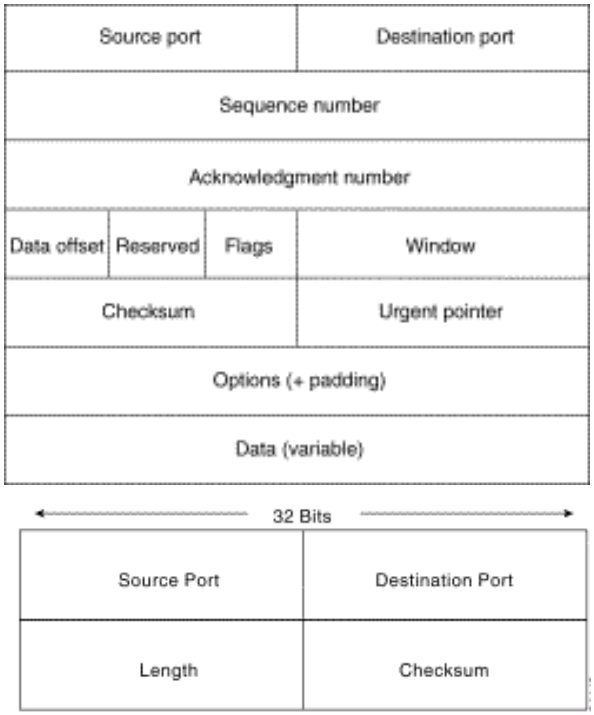
패킷 상세분석

악성코드에 의한 네트워크 트래픽 유발은 네트워크 관리자에게 해결해야 할 또 다른 숙제로 안겨지고 있다. 앞 연재에서 소개하였던 내용들이 트래픽 분석을 위한 기본 준비였다면 이번 호 에서는 악성코드가 유발하는 트래픽을 좀더 세부적으로 살펴볼 것이다.

이더리얼(Ethereal)과 같은 패킷 분석 도구를 이용하여 분석하게 되면 각 프로토콜에 대해 깊은 지식이 없더라도 각 프로토콜 구조별로 쉽게 정보를 파악할 수 있게 된다. 그렇다면 이러한 요소는 어떻게 구성되어 있는 것일까? 여기서는 가장 기본이 되는 IP(Internet Protocol) 와 TCP(Transmission Control Protocol), UDP(User Datagram Protocol) 포맷 형태에 대해서만 살펴보도록 하겠다. [그림1]과 [그림2]는 IP, TCP 프로토콜의 포맷 구조를 나타낸 것으로서 각 패킷들은 이러한 포맷 형태의 규칙에 따라 패킷이 구성되어 있는 것이다. IP 패킷 구조를 보면 IP 버전 정보를 나타내는 4bit 크기의 Version 필드가 존재하고, 출발지와 목적지 주소가 각각 32bit 식으로 구성되어 있다. TCP의 포맷구조는 출발지와 목적지 포트 Sequence 번호 등으로 이뤄졌다. TCP 헤더에 비해 UDP는 출발지와 목적지 포트, 헤더와 데이터의 길이 그리고 Checksum의 간단한 구조로 이루어져 있다.

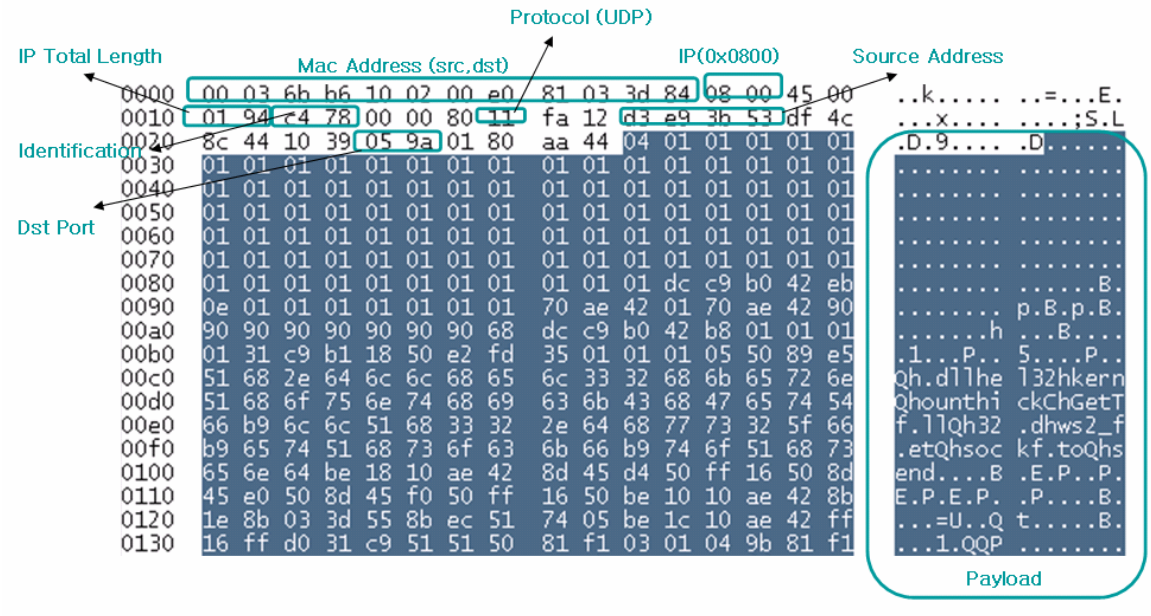


[그림1] IPv4 헤더 포맷



[그림2] TCP(상)와 UDP(하) 헤더 포맷

이러한 포맷 구조에 따라 [그림3]과 같은 하나의 패킷이 구성되어 있는 것이다. 아무 의미 없이 문자열을 배치해 놓은 것 같이 보이지만, 분명 프로토콜 구조를 따르고 있다. 프로토콜에 정의되어 있는 크기만큼 각 필드는 그 의미를 내포하고 있는 것이다.



[그림3] 슬래머 웜의 패킷 구조

[그림3]은 전세계적으로 큰 피해를 안겨주었던 슬래머 웜의 패킷 일부를 나타내고 있다. 슬래머 웜의 경우에는 파일이 존재하는 것이 아닌 메모리 상에만 존재하는 것으로, 네트워크를 통해 전송되는 패킷에 의한 공격이었다는 점이다. SQL 서버가 사용하는 UDP 1434 포트를 대상으로 하고 있고, Payload 부분이 실제 웜의 코드라 할 수 있다. 자, 그럼 [그림3]이 말하는 의미는 어떤 것인지 다음 [표1]를 통하여 각각의 의미를 간단히 알아보도록 하겠다.

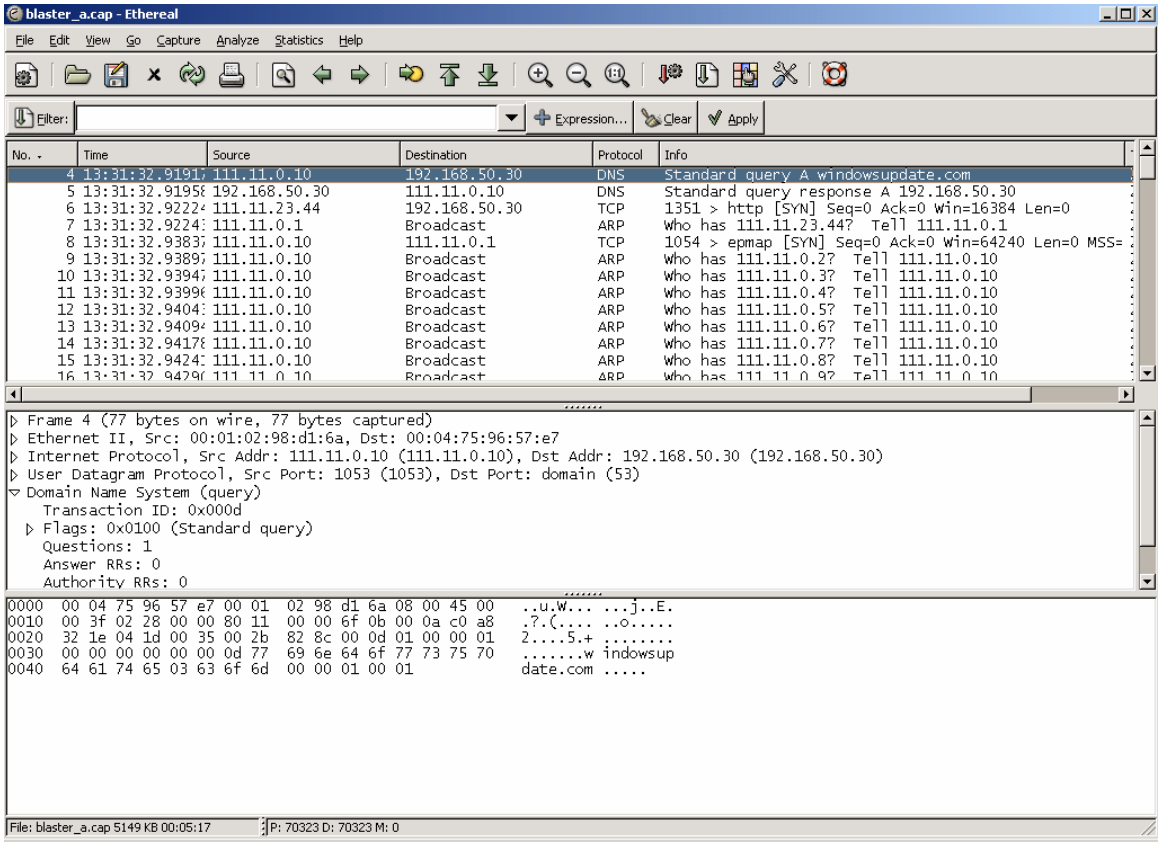
구분	패킷	설명
Ethernet	00 03 6b b6 10 02	출발지 MAC 주소 : 00:03:6b:b6:10:02
	00 50 8b e0 2c 93	목적지 MAC 주소 : 00:50:8b:e0:2c:93
	08 00	타입 : IP (0x0800)
IP(Internet Protocol)	45	IP 버전과 헤더길이 (4bit 는 버전을 나타내고, 나머지 4bit 는 헤더 길이를 나타낸다) IP 버전은 4 이며, 헤더길이는 20bytes 로 표현되었다.
	00	8bit 길이의 서비스 필드(TOS:type-of-service)
	01 94	IPv4 헤더를 포함한 IP 데이터의 전체 길이 16bit 로 여기서는 404bytes 이다.
	42 97	16bit Identification (Fragmentation 과 reassembly 에 사용)
	00	Flags (DF bit , MF bit)
	00 00	Fragment offset
	80	TTL(Time-To-Live)은 패킷이 전달되며, 각 라우터를 거칠때마다 값이 하나씩 감소된다. 128 로 설정되어 있다.
	11	8bit 의 프로토콜 필드이다. TCP는 6, UDP는 11의 값을 가지고 있다.
	fa 12	IP 헤더의 Checksum 이다.
	d3 e9 3b 53	IPv4 출발지 주소
	df 4c 8c 44	IPv4 목적지 주소
UDP(User Datagram Protocol)	10 39	UDP 프로토콜의 출발지 포트 : 1533
	05 9a	UDP 프로토콜의 목적지 포트 : 1434
	01 80	UDP 길이 : 386 bytes
	aa 44	UDP Checksum

[표1] 슬래머 웜 패킷과 프로토콜별 비교

각 프로토콜별 자료는 RFC 문서를 참고하면 더욱 상세한 정보를 얻을 수 있으며, 여기서는 패킷 구조의 형태를 이해하는 측면에서만 기본적인 내용을 기술하였다. 이제 몇 가지 '웜'이 유발하는 트래픽 형태를 통하여 악성코드가 네트워크에 어떤 영향을 주는지 살펴보도록 한다.

CASE STUDY 1

RPC DCOM[1] 취약점을 이용하여 전파되는 Win32/Blaster.worm.6176(이하 블래스터 웜)[2]은 임의의 IP 주소를 선택해 주소를 하나씩 증가시키며 취약성이 있는 시스템을 찾아 공격하게 된다. 이때 TCP 135번 포트를 이용하며, 많은 ARP(Address Resolution Protocol) 트래픽을 생성한다. ARP 트래픽은 평균 250 PPS(초당 패킷 전송 개수) 정도이며 [그림4]와 같이 windowsupdate.com에 대한 DDoS(Distributed Denial of Service) 공격을 시도하기 위하여 DNS 쿼리가 이뤄지고 있다.

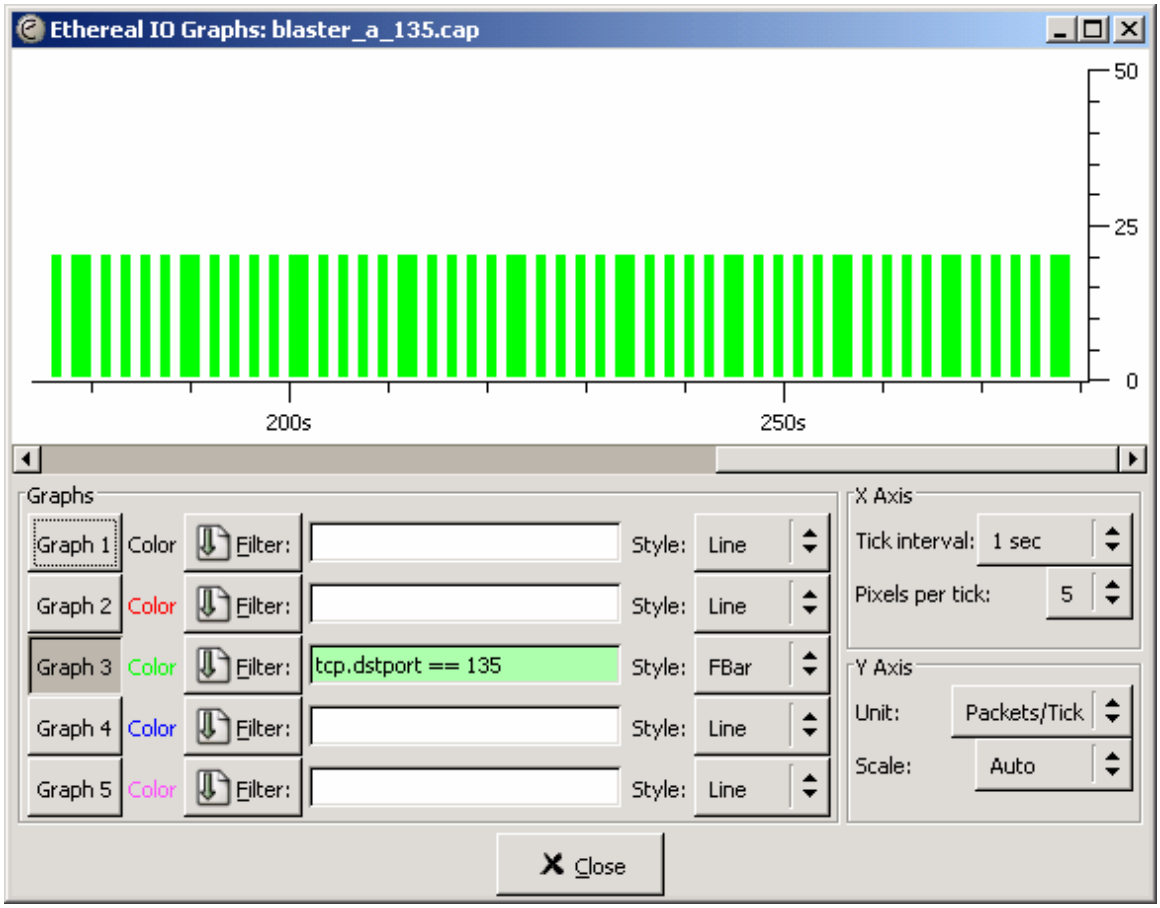


[그림4] 블래스터 웜의 네트워크적 행동

[1] ASEC Advisory : Microsoft RPC 버퍼 오버플로우 취약점
http://info.ahnlab.com/securityinfo/info_view.jsp?seq=4601

[2] http://info.ahnlab.com/smart2u/virus_detail_1202.html

블래스터 웜의 전파를 위하여 TCP 135번으로 SYN 패킷을 전송하며, [그림5]와 같이 최대 20 PPS 정도로 패킷을 유발한다. 패킷의 특징적인 것은 IP 헤더의 Checksum이 0x0000으로 정의되어 있다. 즉, 이것은 임의적으로 패킷이 조작되었다는 것을 알 수 있다.



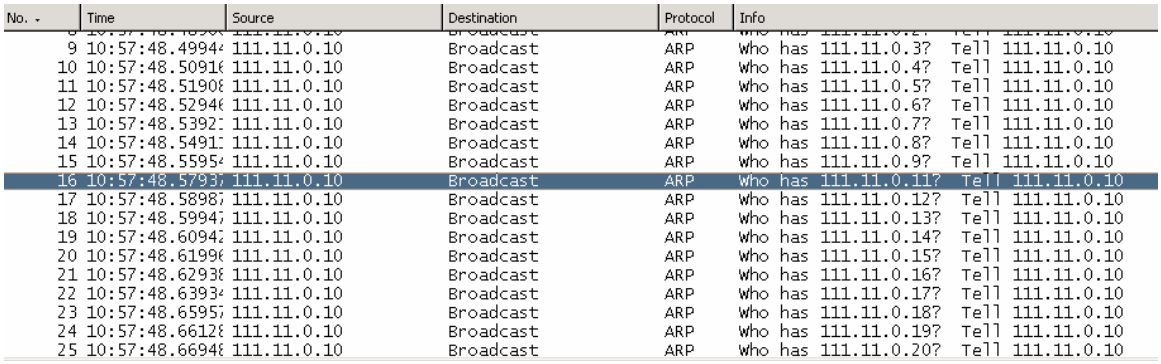
[그림5] 블래스터웜의 TCP/135 트래픽 그래프 화면

CASE STUDY 2

블래스터 웜과 마찬가지로 RPC DCOM 취약점을 이용하여 전파되는 Win32/Welchia.worm.10240(이하 웰치아 웜) [1] 은 ICMP(Internet Control Message Protocol) 패킷과 ARP 패킷 생성이 두드러지게 나타난다. ICMP 패킷 타입 8번인 Echo Request를 전송하며 설정된 시스템 IP를 기준으로 B 클래스 주소를 고정시킨 후 C 클래스 대역의 IP를 증가시키며 계속 패킷을 전송하게 된다.

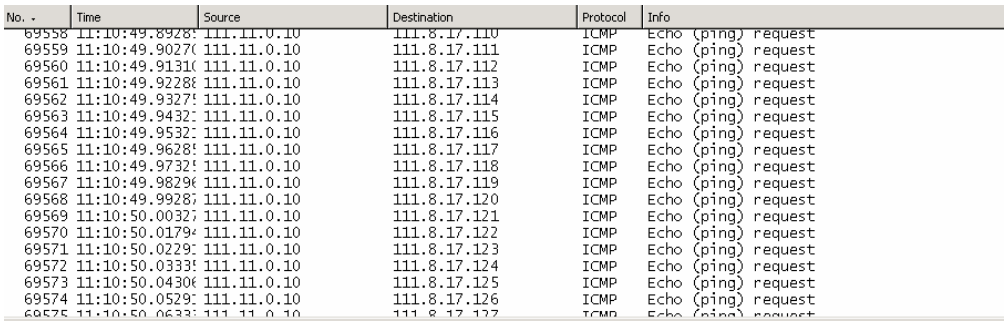
[그림6]과 [그림7]에서 보이는 것과 같이 목적지 주소는 규칙을 가지고 값이 하나씩 증가하며 패킷 전달이 이뤄지고 있다.

[1] http://info.ahnlab.com/smart2u/virus_detail_1206.html



No.	Time	Source	Destination	Protocol	Info
9	10:57:48.4994	111.11.0.10	Broadcast	ARP	Who has 111.11.0.3? Tell 111.11.0.10
10	10:57:48.5091	111.11.0.10	Broadcast	ARP	Who has 111.11.0.4? Tell 111.11.0.10
11	10:57:48.5190	111.11.0.10	Broadcast	ARP	Who has 111.11.0.5? Tell 111.11.0.10
12	10:57:48.5294	111.11.0.10	Broadcast	ARP	Who has 111.11.0.6? Tell 111.11.0.10
13	10:57:48.5392	111.11.0.10	Broadcast	ARP	Who has 111.11.0.7? Tell 111.11.0.10
14	10:57:48.5491	111.11.0.10	Broadcast	ARP	Who has 111.11.0.8? Tell 111.11.0.10
15	10:57:48.5595	111.11.0.10	Broadcast	ARP	Who has 111.11.0.9? Tell 111.11.0.10
16	10:57:48.5793	111.11.0.10	Broadcast	ARP	Who has 111.11.0.11? Tell 111.11.0.10
17	10:57:48.5898	111.11.0.10	Broadcast	ARP	Who has 111.11.0.12? Tell 111.11.0.10
18	10:57:48.5994	111.11.0.10	Broadcast	ARP	Who has 111.11.0.13? Tell 111.11.0.10
19	10:57:48.6094	111.11.0.10	Broadcast	ARP	Who has 111.11.0.14? Tell 111.11.0.10
20	10:57:48.6199	111.11.0.10	Broadcast	ARP	Who has 111.11.0.15? Tell 111.11.0.10
21	10:57:48.6293	111.11.0.10	Broadcast	ARP	Who has 111.11.0.16? Tell 111.11.0.10
22	10:57:48.6393	111.11.0.10	Broadcast	ARP	Who has 111.11.0.17? Tell 111.11.0.10
23	10:57:48.6595	111.11.0.10	Broadcast	ARP	Who has 111.11.0.18? Tell 111.11.0.10
24	10:57:48.6612	111.11.0.10	Broadcast	ARP	Who has 111.11.0.19? Tell 111.11.0.10
25	10:57:48.6694	111.11.0.10	Broadcast	ARP	Who has 111.11.0.20? Tell 111.11.0.10

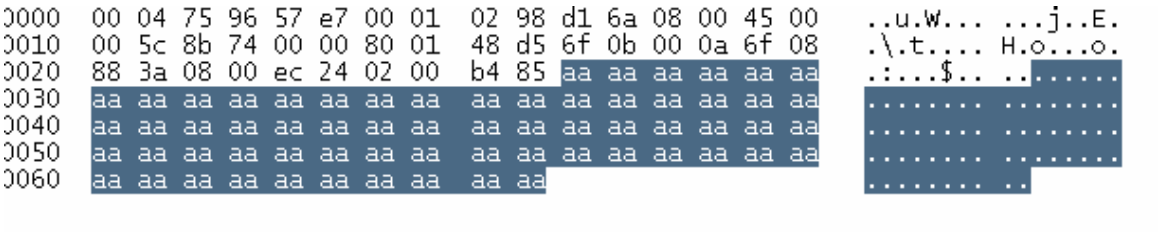
[그림6] 웰치아 윔의 ARP 트래픽



No.	Time	Source	Destination	Protocol	Info
69559	11:10:49.9027	111.11.0.10	111.8.17.111	ICMP	Echo (ping) request
69560	11:10:49.9131	111.11.0.10	111.8.17.112	ICMP	Echo (ping) request
69561	11:10:49.9228	111.11.0.10	111.8.17.113	ICMP	Echo (ping) request
69562	11:10:49.9327	111.11.0.10	111.8.17.114	ICMP	Echo (ping) request
69563	11:10:49.9432	111.11.0.10	111.8.17.115	ICMP	Echo (ping) request
69564	11:10:49.9532	111.11.0.10	111.8.17.116	ICMP	Echo (ping) request
69565	11:10:49.9628	111.11.0.10	111.8.17.117	ICMP	Echo (ping) request
69566	11:10:49.9732	111.11.0.10	111.8.17.118	ICMP	Echo (ping) request
69567	11:10:49.9829	111.11.0.10	111.8.17.119	ICMP	Echo (ping) request
69568	11:10:49.9928	111.11.0.10	111.8.17.120	ICMP	Echo (ping) request
69569	11:10:50.0032	111.11.0.10	111.8.17.121	ICMP	Echo (ping) request
69570	11:10:50.0179	111.11.0.10	111.8.17.122	ICMP	Echo (ping) request
69571	11:10:50.0229	111.11.0.10	111.8.17.123	ICMP	Echo (ping) request
69572	11:10:50.0333	111.11.0.10	111.8.17.124	ICMP	Echo (ping) request
69573	11:10:50.0430	111.11.0.10	111.8.17.125	ICMP	Echo (ping) request
69574	11:10:50.0529	111.11.0.10	111.8.17.126	ICMP	Echo (ping) request

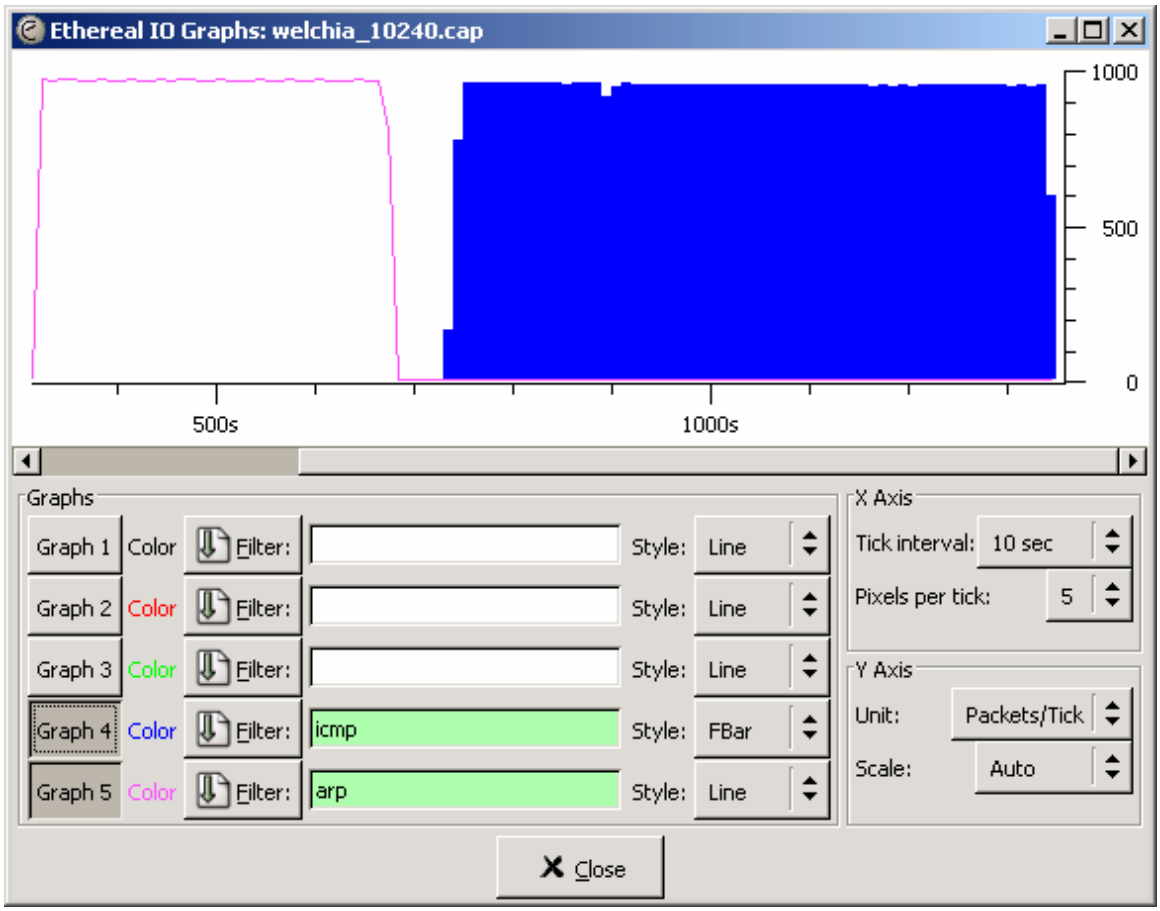
[그림7] 웰치아 윔의 ICMP 트래픽

ICMP 패킷은 92바이트(bytes)로 헤더등을 제외하면 64바이트(bytes) 데이터를 가지고 있다. [그림8]과 같이 데이터 내용은 'aa' 로 모두 채우고 있으며, 목적지 주소는 규칙에 따라 계속 변경된다. ARP와 ICMP 패킷이 약 100PPS 정도로 나타난다. [그림9]는 X축의 간격을 10초로 하여 분홍색은 ARP 트래픽을 파란색은 ICMP 트래픽을 보여주고 있다.



```
0000  00 04 75 96 57 e7 00 01  02 98 d1 6a 08 00 45 00   ..u.W... ...j..E.
0010  00 5c 8b 74 00 00 80 01  48 d5 6f 0b 00 0a 6f 08   .\.t.... H.o...o.
0020  88 3a 08 00 ec 24 02 00  b4 85 aa aa aa aa aa aa   .:...$.. ........
0030  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0040  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0050  aa aa aa aa aa aa aa aa  aa aa aa aa aa aa aa aa   ........ ........
0060  aa aa aa aa aa aa aa aa  aa aa                    ........ ..
```

[그림8] 웰치아 윔의 패킷



[그림9] 웰치아 웜의 ARP, ICMP 트래픽 그래프

CASE STUDY 3

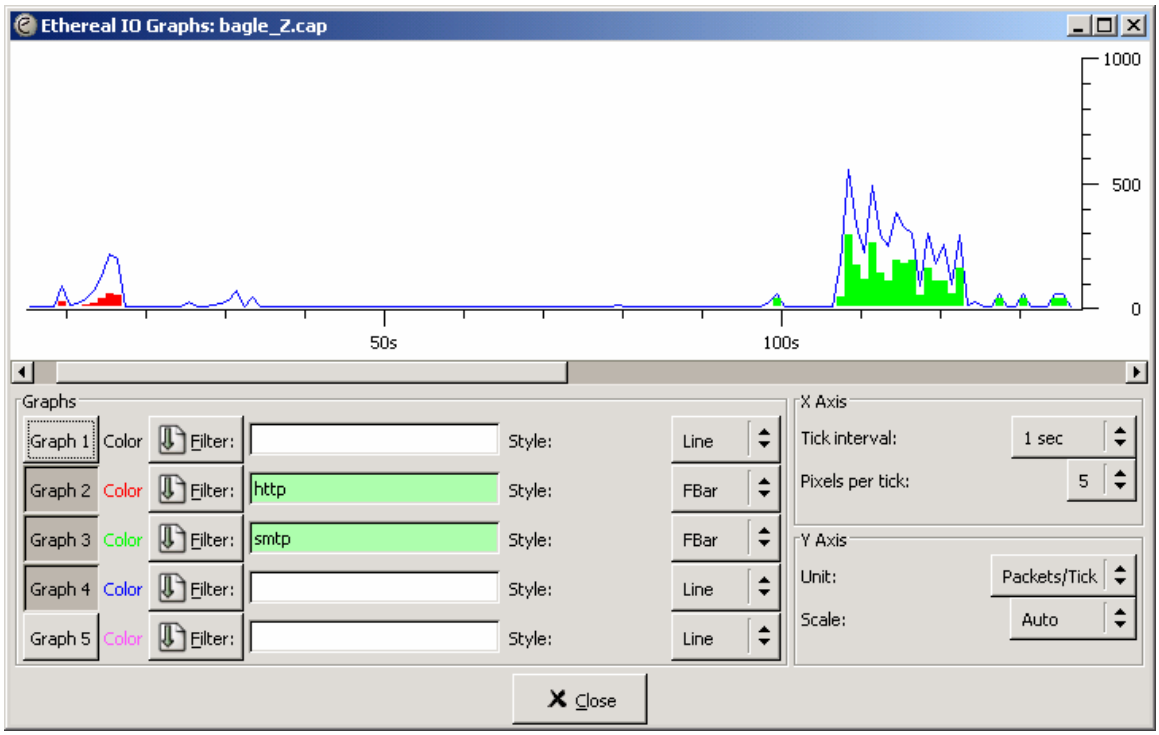
다양한 확장자의 첨부파일을 통해 전파되는 Win32/Bagle.worm.Z(이하 베이글.Z 웜)[1]은 TCP 25번인 메일 트래픽을 증가시킨다. 크게 이 웜이 사용하는 프로토콜은 DNS, SMTP, HTTP이며 초기 HTTP 트래픽이 나타나게 된다. TCP가 96%, HTTP 36%, SMTP 43% 정도의 비중을 차지한다. IP 헤더의 헤더 Checksum은 '0x0000' 값으로 고정되어 있으며, TCP 헤더의 Checksum 올바르지 않은 값을 가지기도 한다.

[1] http://info.ahnlab.com/smart2u/virus_detail_1376.html

```
▷ Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (0x06)
  Header checksum: 0x0000 (incorrect, should be 0x6ba2)
  Source: 111.11.0.10 (111.11.0.10)
  Destination: 192.168.50.30 (192.168.50.30)
▽ Transmission Control Protocol, Src Port: 3249 (3249), Dst Port: http (80), Seq: 1, Ack: 1, Len: 92
  Source port: 3249 (3249)
  Destination port: http (80)
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 93    (relative sequence number)]
  Acknowledgement number: 1    (relative ack number)
  Header length: 20 bytes
▷ Flags: 0x0018 (PSH, ACK)
  Window size: 64240
  Checksum: 0x6252 (incorrect, should be 0xab6e)
```

[그림10] 베이글.Z 웜이 유발하는 HTTP의 패킷 상세정보

HTTP 접속시에는 최대 200PPS 정도까지 나타나며, SMTP는 최대 400PPS까지 보여주었다. [그림11]에서는 패킷 덤프된 전체와 HTTP, SMTP를 함께 나타낸 것으로 여기서 언급한 수치와는 다르게 보일 수 있다.



[그림11] 베이글.Z 웜의 전체 트래픽

* 참고로, CASE STUDY로 언급한 웜의 트래픽 형태는 환경에 따라 달라질 수 있으므로 절대적인 수치가 되지는 못한다. *

맺음말

이로써 3회에 걸쳐 네트워크 트래픽 분석의 준비부터 시작하여 공개 소프트웨어 중의 하나인 네트워크 트래픽 분석 툴인 이더리얼을 이용하여 유해 트래픽의 탐지부터 분석까지의 방법을 알아보았다. 이번 연재는 네트워크에 악성코드와 같은 비정상적인 트래픽이 발생하는 경우, 네트워크 관리자들은 어떻게 준비하고 시작하여야 하는지 기본적인 가이드 역할을 해 줄 것이다.