ASEC Report 6월

® ASEC Report

2004. 7

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

Mass Mailer의 여전한 강세와 휴대폰 웜의 등장..

6월에도 여전히 Mass Mailer에 의한 피해신고가 많아, 악성코드 피해신고 Top 10 중 1가지를 제외하고는 모두 Mass Mailer가 순위를 차지했다. 또한 6월에는 지난 4월에 이어 또 한 번 피해신고 된 악성코드 수가 918종으로, 역대 최고를 기록했다. 이처럼 많은 피해신고 된 악성코드 수가 역대 최고를 기록한 것은 악성 IRCbot 변형의 잦은 출현이 그 원인으로, 이는 6월에 발견된 신종 악성코드의 97%를 악성 IRCBot 변형이 차지하고 있는 것으로도 알 수 있다.

6월에 발표된 취약점 중에는 악성코드에서 이용될 것으로 예상되는 것은 없어, 크게 위협적이지는 않았다. 그러나 아직 보안패치가 발표되지 않은 인터넷 익스플로어의 취약점을 이용한 악성코드가 발견되어 사용자 및 보안업계를 긴장시키기도 했다.

한국 이외의 지역의 동향을 살펴보면 일본은 여전히 Mass Mailer에 의한 피해가 많은 반면, 중국은 네트워크를 이용하여 확산되는 웜이 크게 증가하였고 한국에서 크게 문제시되고 있는 애드웨어 성향을 가진 트로이목마가 피해순위에 등장하는 특이한 점을 보였다.

6월에 발견된 특징적인 신종으로는 LSASS.EXE 버퍼 오버플로우 취약점(MS04-011)을 이용하여 전파되는 Win32/Korgo.worm(코르고 웜)을 들 수 있고, 특히 일부 심비안(Symbian) 운영체계의 스마트폰에서 감염되는 최초의 휴대폰 웜이 등장하였다. 이 휴대폰 웜의 등장과 향후 휴대폰 웜의 등장 가능성에 대해 테크니컬 컬럼에서 간략하게 조명해 보았다.

그리고 2004년의 상반기를 마무리하는 시점에서 2004년 상반기 동안의 악성코드 동향과 시큐리티 동향에 대해서도 간략히 살펴 보았다.

I. 6월 악성코드 피해 Top 10

작성자: 정진성 연구원 (jsjung@ahnlab.com)

순위		악성코드명	건수	%
1	-	Win32/Netsky.worm.29568	9985	45.0%
2	-	Win32/Netsky.worm.17424	2065	9.3%
3	-	Win32/Dumaru.worm.9234	1709	7.7%
4	-	Win32/Netsky.worm.28008	1351	6.1%
5	2↑	Win32/Netsky.worm.17920	1128	5.1%
6	New	Win32/Sasser.worm.15872	898	4.0%
7	1↓	Win32/Netsky.worm.25352	644	2.9%
8	3↓	Win32/Netsky.worm.22016	586	2.6%
9	-	Win32/Bagle.worm.Z	360	1.6%
10	-	Win32/Netsky.worm.22016.C	234	1.1%
		기타	3,249	14.6%
합 계			22,209	100

[표1] 2004년 6월 악성코드 피해 Top 10

6월 악성코드 피해 동향

이번 달 악성코드 피해 Top 10은 5월과 비슷한 현황을 보여 주고 있다. 여전히 Win32/Netsky.worm.29568(이하 넷스카이.29568 웜)이 가장 많은 신고건수를 차지하고 있다. 이 넷스카이.29568 웜에 대하여 간단히 살펴보면 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

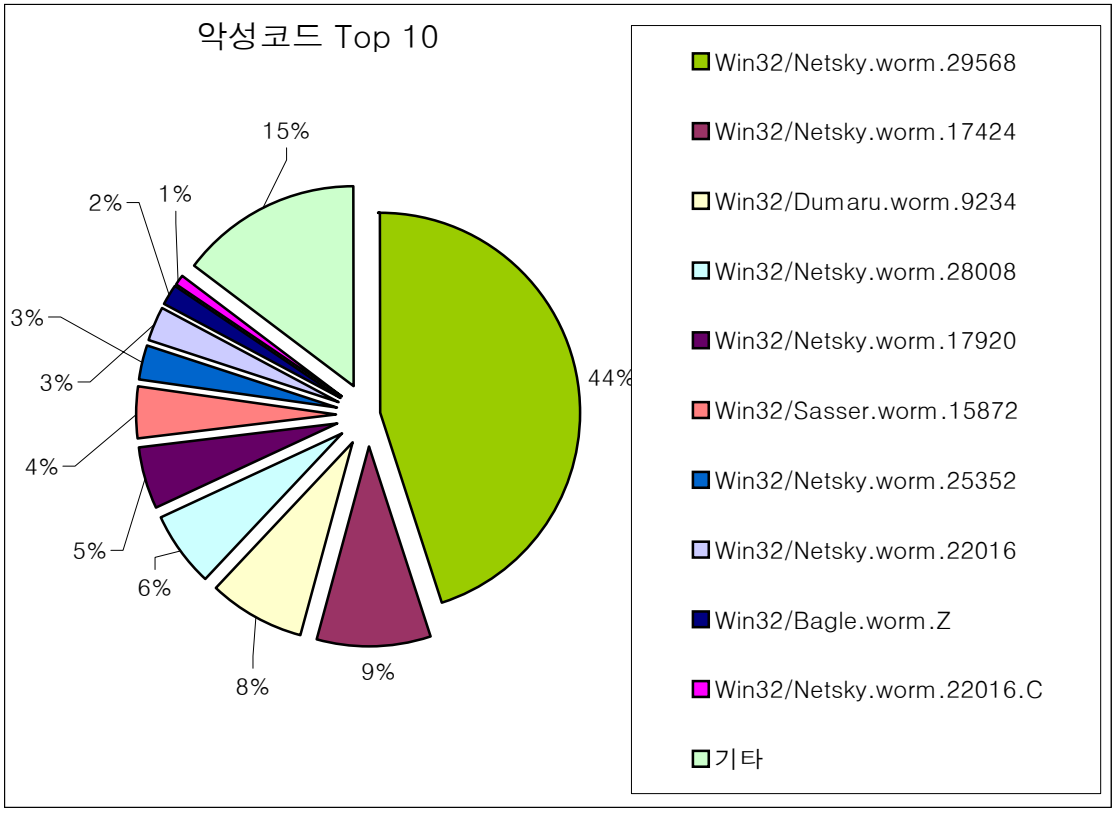
다른 변형의 넷스카이 웜과 크게 다른 점은 찾을 수 없지만 3월 중순경에 처음 발견된 이 웜은 초기 확산시 상당히 많은 시스템에 감염되었고 현재도 감염된 시스템들에서 대량의 메일을 발송하고 있는 것으로 보인다.

지난달에 다시 등장한 Win32/Dumaru.worm.9234(이하 두마루 웜)는 이번 달에도 같은 순위를 차지하고 있다.

Win32/Sasser.worm.15872 (이하 새서 웜)은 4월말에 Exploit(이하 익스플로잇) 코드가 알려지고 몇 일 지나지 않은 5월 1일, 이를 이용하여 제작되어진 웜이다. 과거에는 익스플로잇

코드가 공개되면 보통 몇 개월정도의 시간이 소요되어 악성코드로 제작되어졌으나 새서 웜은 2일 정도 지난 후 빠르게 악성코드로 제작되어졌다. 이른바 Zero-Day 익스플로잇 실현을 보여준 악성코드라 하겠다. 새서 웜은 취약점의 위험성만 가지고 평가할 때 2003년 8월에 발견되었던 Win32/Blaster.worm(이하 블래스터 웜)과 비슷한 수준이지만, 백신업체의 빠른 대응과 많은 사용자들이 보안관리의 문제점을 인식으로 인해 블래스터 웜과 같은 대규모 피해는 발생하지 않았다. 이러한 이유로 새서 웜은 이 웜이 가지고 있는 심각성에 비해 악성 IRCBot 웜 변형 등에 밀려 5월 악성코드 Top 10 에서는 순위권 밖에 머물렀었다.

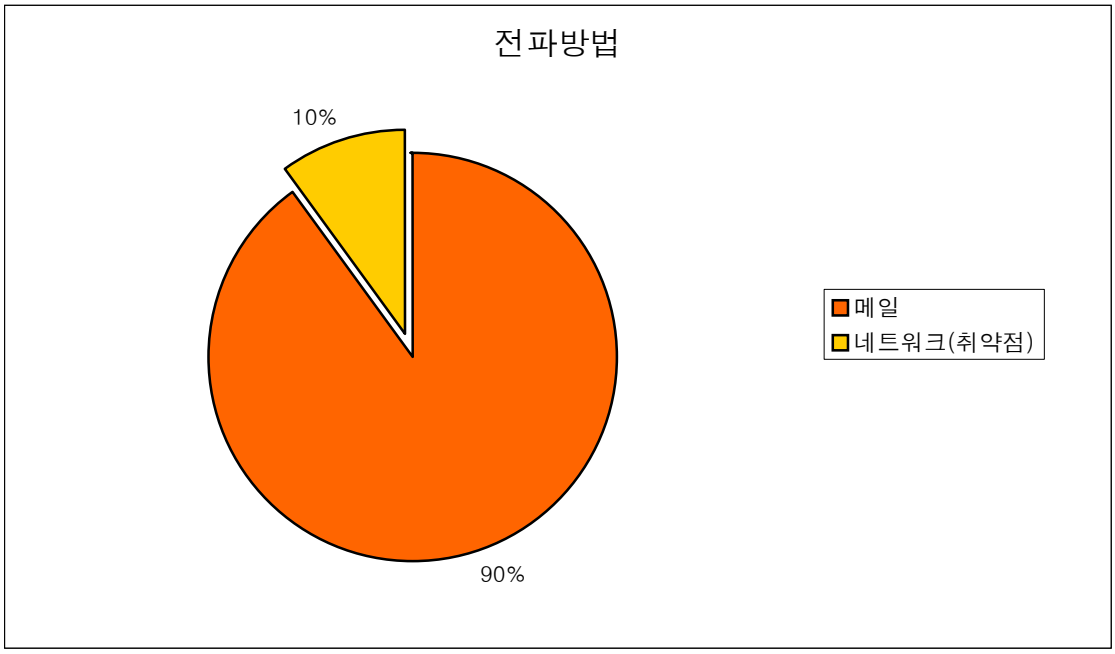
6월의 악성코드 피해 Top10을 도표로 나타내면 [그림1]과 같다



[그림1] 2004년 6월 악성코드 피해 Top 10

6월 악성코드 Top 10 전파방법별 현황

[표1]의 Top 10 악성코드들은 주로 어떠한 감염경로를 가지고 있는지 [그림2]에서 확인해 보기로 한다.

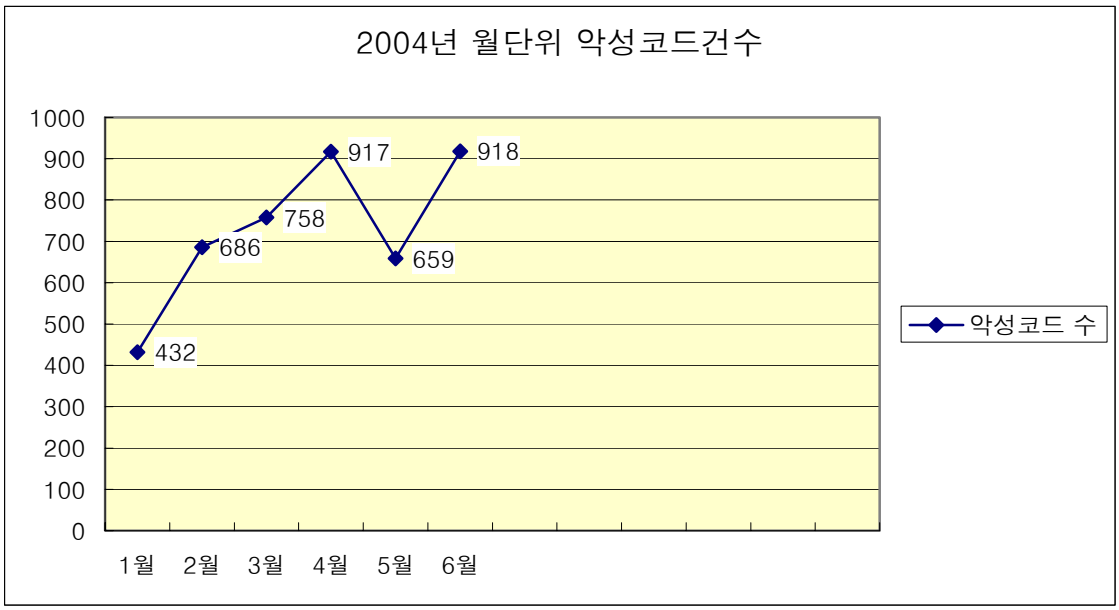


[그림2] 악성코드 피해 Top 10의 전파방법별 현황

지난 5월은 모두 메일로 전파되는 악성코드만 있었던 것과는 달리 이번 달에는 새서 웜으로 인하여 취약점이 있는 시스템을 감염대상으로 하여 네트워크로 전파되는 악성코드 유형이 다시 등장하였다.
우연의 일치일지는 모르지만 지난 5월경 넷스카이 웜 제작자가 체포된 이후로 새로운 형태의 Mass Mailer 출현은 다소 감소하고 있다. 현재 발견되는 Mass Mailer들은 모두 구종들이다.

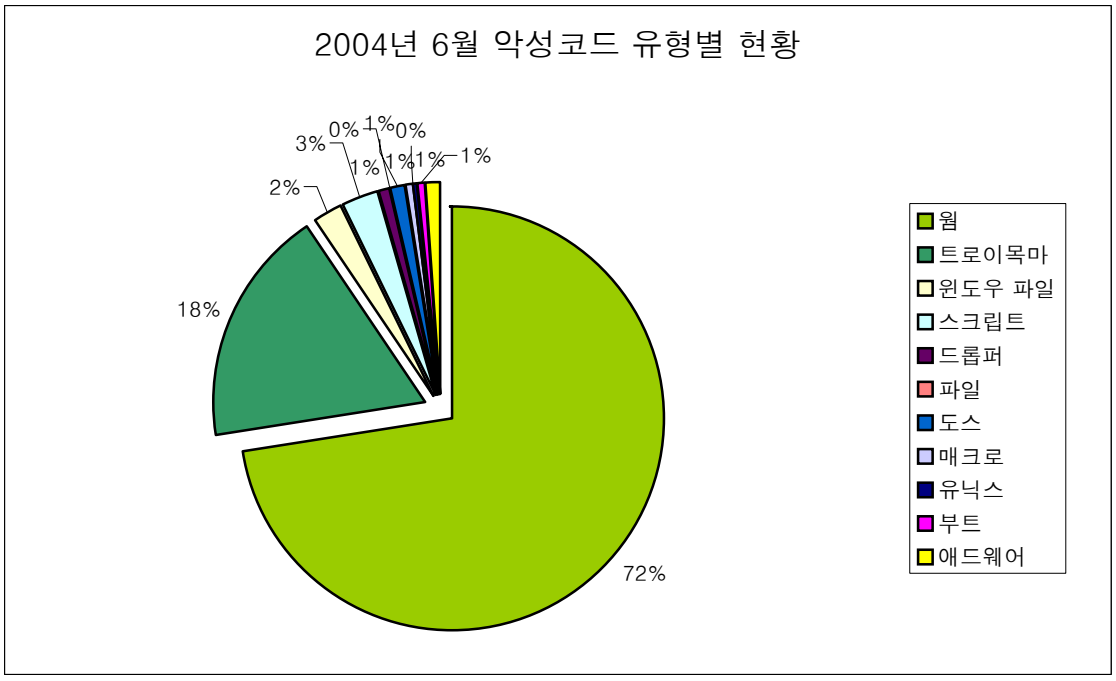
월별 피해신고 악성코드 건수 현황

6월에는 문의된 악성코드의 종류 수가 다시 증가하였다. 4월에 문의된 악성코드의 종류가 917종이였고 5월은 다소 감소하였으나, 이번 달은 4월보다 1개가 많은 918종이며 역대 최고의 수치이다. 이중 대부분이 악성 IRCBot 류가 차지하고 있다. 이와 같은 결과는 지난 4월과 마찬가지로 많은 종류의 악성 IRCBot이 발견, 보고 되었기 때문이다. 즉, 6월은 4월과 비슷한 경향을 보여주고 있다([그림3]참조).



[그림3] 2004년 월별 피해신고 악성코드 수

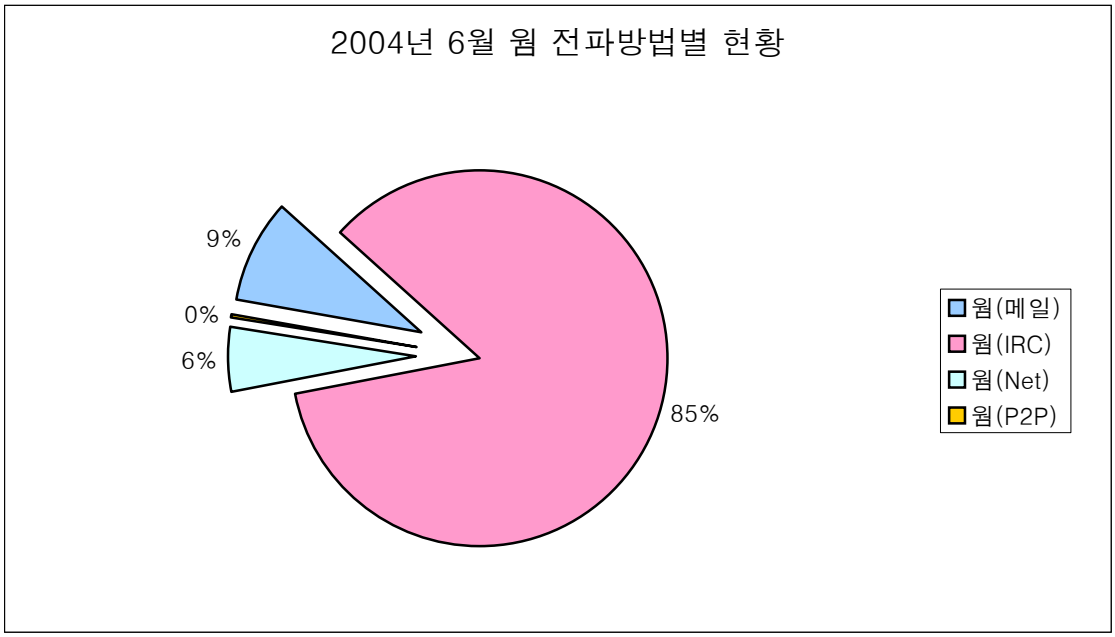
6월에 문의된 악성코드들은 어떤 유형으로 분포되어 있는지 [그림4]를 통해서 확인할 수 있다.



[그림4] 2004년 6월 악성코드 유형별 현황

기존에 발견된 악성 IRCBot 류와 6월에 새로 발견된 다수의 악성 IRCBot 변형으로 인해 웜

유형이 가장 많은 악성코드 분포를 보이고 있다. 이중에서 가장 많은 수치를 차지하는 웜을 전파방법별로 구분 해보면 다음과 같다.



[그림5] 2004년 6월 웜 전파방법별 현황

[그림5]에서 알 수 있듯이 단연코 악성 IRCBot 웜이 가장 많은 유형을 차지하고 있다. 이를 이어 Mass Mailer, 네트워크를 통하여 취약점이 있는 시스템을 대상으로 감염되는 유형, 그리고 P2P 응용 프로그램의 공유폴더를 이용하여 확산되는 유형 순으로 분포하고 있다. 참고로 6월에 문의된 웜 유형은 총 665 종이었다.

6월의 악성코드 피해 동향을 총평 해 본다면 지난 4월과 마찬가지로 다양한 악성 IRCBot 류에 의하여 가장 많은 종류의 악성코드가 집계되었고 그 만큼 이를 위한 대응도 많았던 달이다.

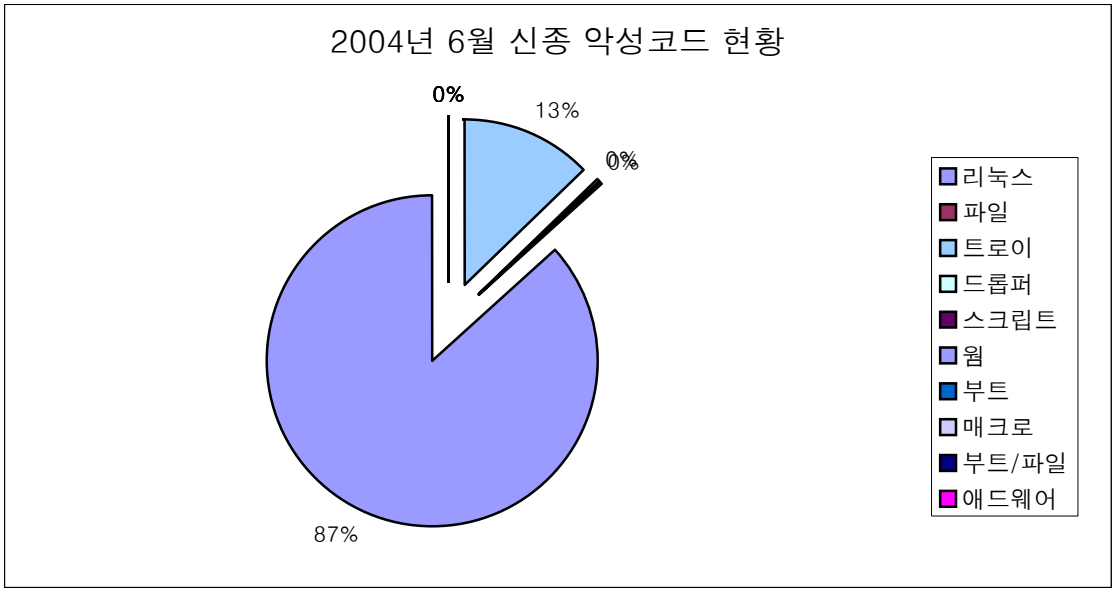
II. 6월 국내 신종 악성코드 발견 동향

작성자: 정진성 연구원 (jsjung@ahnlab.com)

6월 한달 동안 접수된 신종 악성코드의 건수는 [표1], [그림1]과 같다.

리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	애드웨어	합계
0	0	59	2	1	402	0	0	0	0	464

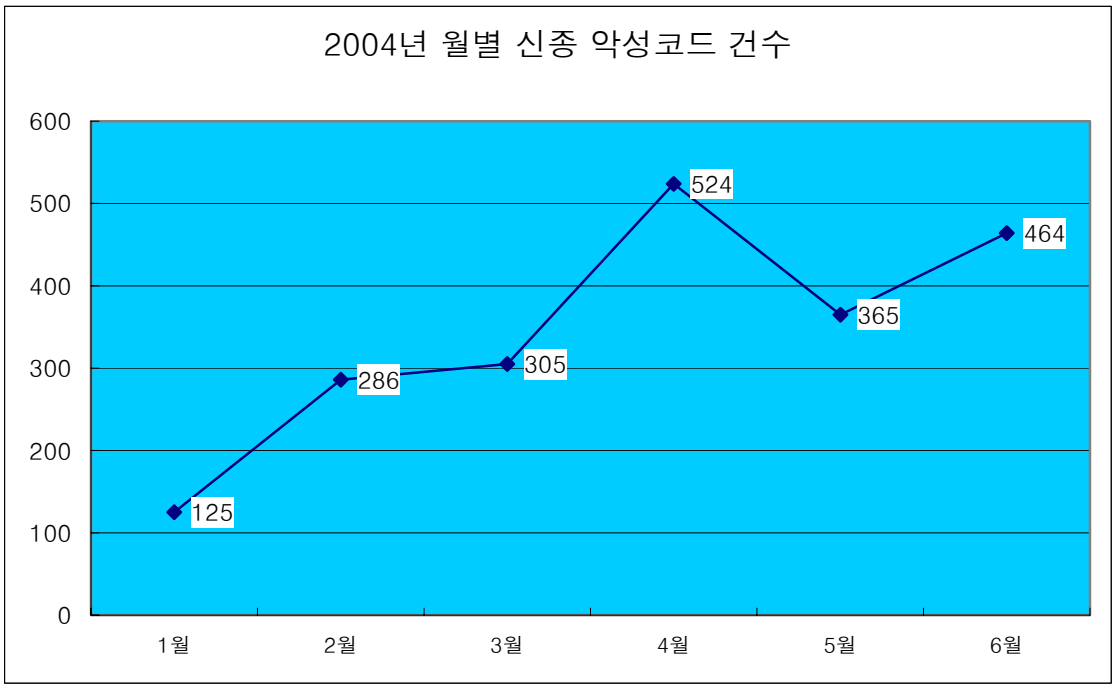
[표1] 2004년 6월 유형별 신종 악성코드 발견현황



[그림1] 2004년 6월 신종 악성코드 발견 현황

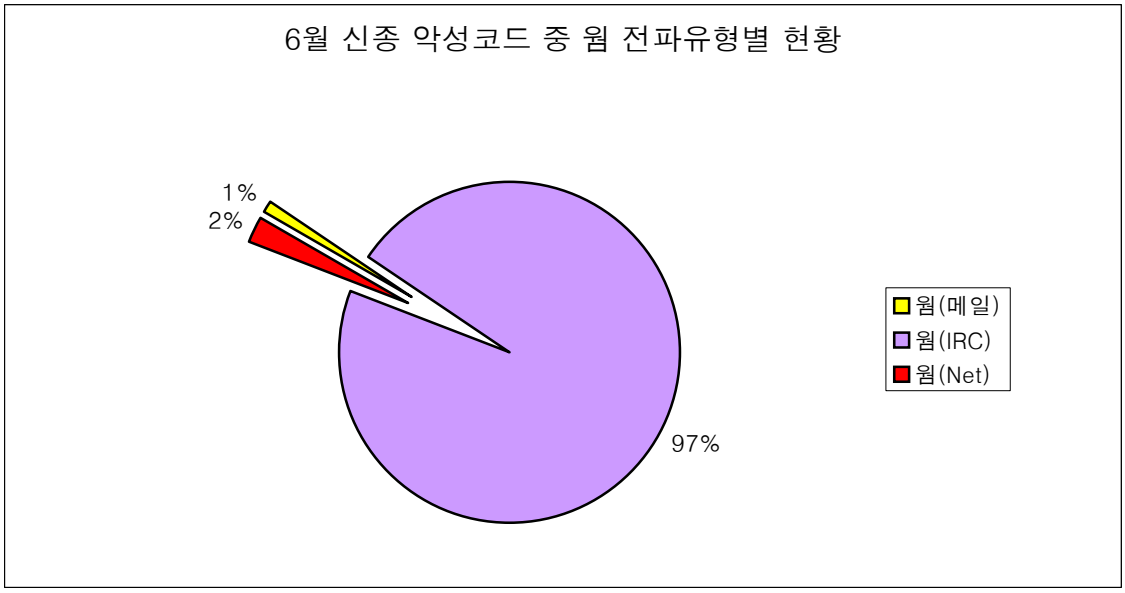
6월 발견된 신종 악성코드 동향

6월은 지난 4월의 신종 악성코드 발견 동향과 유사한 모습을 보여주고 있다. 우선 464건이라는 엄청난 숫자의 신종 및 변형에 대한 악성코드가 접수되었다. 이는 5월 건수에 비해서 100건 정도 증가한 수치이다. 지난해 동월에 72건이었던 것과 비교해 보면 무려 600% 이상 증가한 것이다.



[그림2] 2004년 월별 신종(변형) 악성코드 발견현황

6월에 발견된 신종 중 웜이 차지하는 비율은 87%에 이른다. 유형별로는 악성 IRCBot 웜, Mass Mailer 그리고 취약점이 있는 시스템을 대상으로 네트워크를 통해 전파되는 유형 등이다. 웜 유형별로는 [그림3]과 같다.



[그림3] 2004년 6월 신종 악성코드 중 웜 전파유형별 현황

6월 악성코드 피해동향과 마찬가지로 6월에 발견된 신종 악성코드의 동향도 악성 IRCBot 웜의 비율이 매우 높다. 6월의 경우 메일로 전파되는 신종 및 변형의 Mass Mailer 발견은 아주 적다. [그림3]에서 보듯이 6월에는 오히려 네트워크를 이용하여 취약점이 있는 시스템을 감염대상으로 하는 악성코드가 Mass Mailer 보다 약간 많았다.

6월 신종 코르고 웜

6월에는 특이한 감염방법으로 피해를 일으켰던 Win32/Korgo.worm(이하 코르고 웜)이 발견되었다. 이 문서를 작성하는 현재까지도 코르고 웜에 대한 많은 변형이 발견되었다.

이 웜은 Win32/Sasser.worm (이하 새서 웜)이 이용했던 LSASS.EXE의 버퍼 오버플로우 취약점(MS04-011)을 이용하여 시스템에 감염된다. 감염된 이후 웜은 Explorer.exe에 Thread(이하 쓰레드)형태로 존재한다. 쓰레드로 존재하지 못할 때는 Process (이하 프로세스)형태로 실행된다.

이렇듯 코르고 웜은 CreateRemoteThread API를 이용하여 Explorer.exe 프로세스에 쓰레드로 존재하는데 이와 같이 정상적인 윈도우 프로세스 또는 기타 응용 프로그램의 프로세스에 Code Injection되는 감염기법을 사용한다. 이는 기존 악성코드에서도 찾아 볼 수 있는데, Win32/LovGate.worm (이하 러브게이트 웜) 변형 중 일부가 그렇다.

코르고 웜의 경우 자신이 프로세스 형태로 실행되는 경우, 치료에 큰 어려움은 없으나 웜이 쓰레드로 실행되는 경우 완벽히 치료하기 위해서는 메모리 치료가 선행되어야 한다. Explorer.exe를 강제로 종료하는 방법도 있으나 이는 약간의 안정성에 문제가 있다.

이와 같이 윈도우 프로세스나 서비스 또는 응용 프로그램의 서비스나 프로세스에 쓰레드 형태로 존재하는 경우 감염을 확인하기 매우 어려우며 또한 진단/치료 역시 힘들다. 악성코드 제작자들은 이러한 점을 악용하여 이와 같은 감염기법을 사용하는 악성코드를 제작하는데 열을 올리고 있다. 따라서 앞으로도 이와 같은 감염기법을 사용하는 악성코드는 점차 증가할 것으로 추정된다.

6월 신종 기타

이번 달 특이할 만한 신종 악성코드 중 코르고 웜 이외에는 다음과 같은 것들이 있었다.

- Win-Trojan/DDoS_Boxed 시리즈 (이하 박스드 트로이목마)
- Win-Trojan/Padodor (aka Win-Trojan/Berbew) 시리즈 (이하 파도도르 트로이목마)

박스드 트로이목마는 일반적인 DDoS 공격 에이전트이다. 즉, 트로이목마 내부에 하드코딩된 특정한 호스트에 대한 서비스 거부 공격을 일으킨다. 이와 같은 DDoS 공격 에이전트가 처음 발견된 경우는 아니지만, 한달이란 짧은 기간 동안 연이어 다수 발견된 경우는 매우 드문 일이다.

다른 하나인 파도도르 트로이목마는 러시아에서 제작되어진 것으로 추정된다. 이 트로이목마

의 전파방법은 처음에는 알려지지 않았지만 이후 이 트로이목마가 러시아의 한 해커그룹에 의해서 조직적으로 만들어지고 전파되었다는 것을 알 수가 있었다.

파도도르 트로이목마는 HTML/Ject, HTML/Scob에 의해서 설치된다. 이 스크립트 트로이목마는 먼저 해커들이 특정 웹 사이트에 대하여 해킹을 시도한 뒤 IIS 서버의 바닥글 기능을 활성화하여 HTML/Scob 트로이목마가 IIS 서버 내 모든 페이지에 감염되도록 해둔다. 이후 방문자가 인터넷 익스플로어를 이용하여 해당 웹 페이지에 접근하면 인터넷 익스플로어의 ADODB 스트림 오브젝트 취약점을 이용하여 원격 호스트에 올려진 파일(여기서는 트로이목마)을 로컬 드라이브에 다운로드 및 실행할 수 있는 위험성을 갖고 있다.

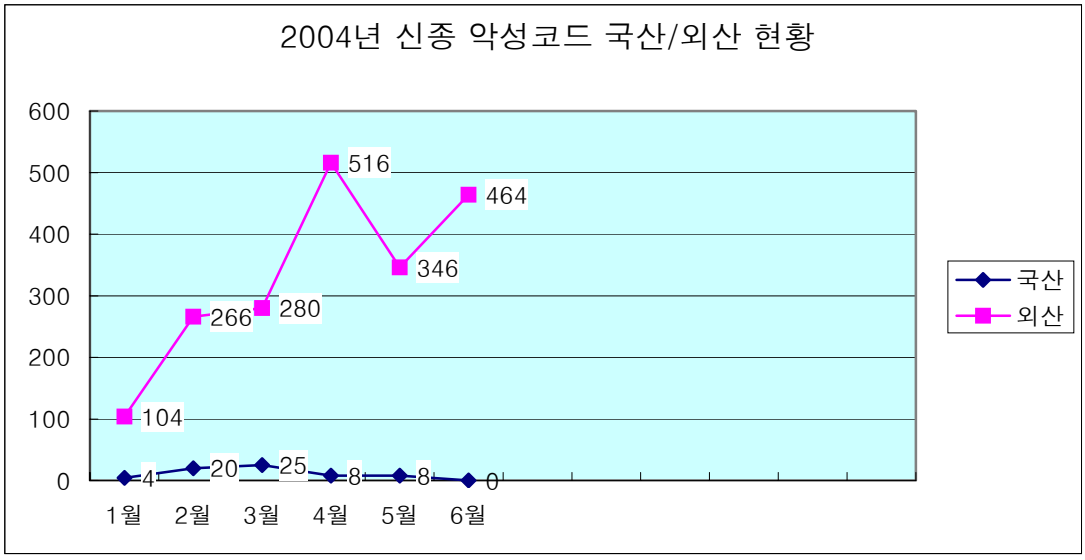
이렇게 설치된 파도도르 트로이목마는 특정한 포트를 오픈해 두며 시스템에 있는 암호들(캐쉬에 저장된 암호 또는 인터넷 익스플로어로 접근할 수 있는 웹 사이트에 대한 암호 등)을 훔쳐내어 별도의 파일로 저장해 둔다. 또한 이 트로이목마는 Stealth 기법을 사용하는데 다음과 같은 API 메모리 주소 내 JMP 코드를 삽입하여 트로이목마가 정의한 메모리 주소를 가리킴으로써 후킹되도록 해 둔다.

- Process32Next
- NtQuerySystemInformation

이와 같은 방법으로 프로세스에서 자신을 숨겨 사용자들은 일반적인 방법으로는 감염 사실을 알기 어렵고 백신 제품을 이용하지 않고는 치료 또한 힘들다.

제작지별 신종 악성코드 현황

다음은 신종 악성코드들의 국산/외산의 현황을 보여주고 있다.



[그림4] 2004년 제작지별 신종 악성코드 현황

6월에는 모두 외산 악성코드가 발견 되었고 국산 악성코드는 발견, 보고 되지 않았다. 보통

엔진에 추가되는 국산 악성코드들 중 일부는 애드웨어이나 트로이목마-사용자의 동의를 받지 않고 윈도우 환경을 변경하는 등-의 성격이 짙어 분석 후 엔진에 추가되는 유형이 많았다. 이번 달 경우는 국산에서 제작된 이러한 유형의 것마저 발견되지 않았다.

III. 6월 신규 보안 취약점

작성자: 이정형 연구원(jungh@ahnlab.com)

6월에도 LSASS 취약점(MS04-011)을 이용한 악성 프로그램들이 여전히 유행하였다. 또한 예전에 발견된 취약점이지만 아직 이에 대한 패치가 제공되지 않은 인터넷 익스플로어(Internet Explorer)의 취약점을 이용한 HTML/Ject, HTML/Scob 등이 발견되기도 하였다.

이번 호에서는 6월에 마이크로소프트사에서 발표한 보안패치와 HTML/Ject, HTML/Scob이 이용한 인터넷 익스플로어의 취약점에 대해 알아보기로 하자.

MS의 6월 보안 패치

마이크로소프트사는 2004년 6월 9일 MS04-016 패치[1]를 발표하면서 패치 업데이트를 권고하였다. 이번에 발표된 보안패치는 DirectPlay의 IDirectPlay4 응용 프로그램 인터페이스(API)에 서비스 거부 취약점이 존재하는 것으로, 이 취약점을 악용한 침입자는 응용 프로그램에 장애를 일으킬 수 있다.

DirectPlay는 게임 개발자가 복잡한 네트워크 프로토콜을 구현할 필요 없이 멀티 플레이어 네트워크 게임을 만드는 데 도움을 주기 위해 마이크로소프트 DirectX와 함께 제공되는 네트워크 프로토콜이다. 이 DirectPlay에 IDirectPlay4 API 구현은 엄격한 패킷 유효성 검사를 수행하지 않음으로써 서비스 거부 공격이 일어날 수 있는 것이다. 멀티 플레이어 게임에 사용되는 시스템이라면 패치를 적용하기 권고한다

인터넷 익스플로어의 임의적인 스크립트 실행 취약점

지난 4월에 제기된 인터넷 익스플로어에서 Windows Help 파일을 다루는 데 있어 로컬 컴퓨터에 임의의 코드를 실행하는 버그[2]이다

6월에 발견된 HTML/Ject[3], HTML/Scob[4]는 러시아 해커그룹이 제작한 악성 스크립트로, 이 취약점을 이용하여 헤더부분에 Location: URL:을 첨부하여 로컬의 리소스에 접근한다. 이중 HTML/Scob은 윈도우 2000에서 웹 서비스를 할 수 있는 IIS(Internet Information Server) 서버가 설치된 시스템에서 발견, 보고되었다. 이 자바 스크립트는 어떤 드롭퍼

---

[1] 마이크로소프트, http://www.microsoft.com/korea/technet/security/bulletin/MS04-016.asp

[2] Secunia, http://secunia.com/advisories/10523/
Bugtraq, http://seclists.org/lists/bugtraq/2004/May/0153.html

[3] AhnLab, http://info.ahnlab.com/smart2u/virus_detail_1444.html

[4] AhnLab, : http://info.ahnlab.com/smart2u/virus_detail_1443.html

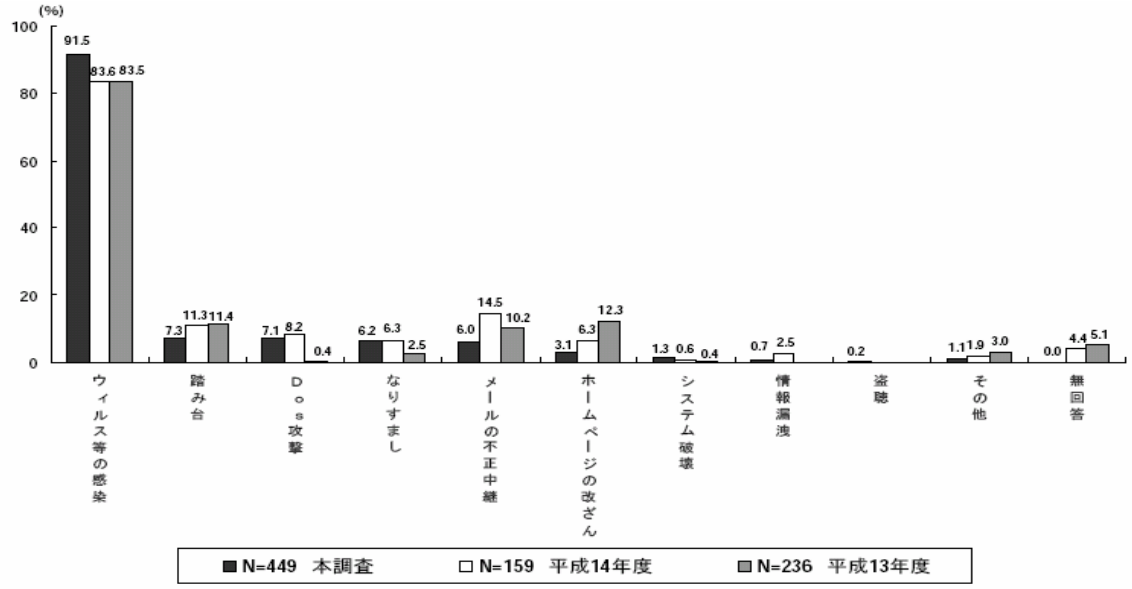
(Dropper)에 의해서 시스템에 설치되며, IIS 설정 중 특정 기능을 활성화하여 웹 서버 내 모든 웹 페이지에 해당 자바 스크립트 트로이목마를 붙게 만든다. 이 스크립트는 특정 웹 사이트로부터 파일을 다운로드 하는데, 이 파일에는 인터넷 익스플로어의 취약점을 이용하여 특정 웹 서버에 올려진 트로이목마를 자동으로 다운로드 및 실행되게 한다.

이러한 HTML/Ject, HTML/Scob이 이용하는 인터넷 익스플로어 취약점으로부터 안전하기 위해서는 마이크로소프트사의 패치가 나올 때까지 기다리는 방법뿐이다. 임시적인 해결책으로는 신뢰할 수 없는 사이트는 접속하지 않거나 인터넷 익스플로어의 옵션에서 스크립트 실행을 제거 하는 방법, 다른 브라우저(Mozilla, Netscape, Opera 등)를 이용하는 방법이 있을 수 있다.

IV. 6월 일본 피해 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

일본 경찰청에서 발표한 자료에 의하면 최근 인터넷 관련 피해의 내용에서 가장 많은 부분을 차지하고 있는 것은 바이러스 등 악성코드의 감염에 의한 것으로 나타났다. 흥미로운 점은 이전에 비해 악성코드나 도스공격 등에 대한 감염피해가 점점 증가하고 있고 홈페이지의 변조와 같은 특정 대상에 대한 직접적인 공격은 줄어들고 있다는 것이다.



일본 유행 악성코드 유형별 발생현황

2004년 6월 한달 동안 일본에서 가장 이슈가 된 악성코드는 Win32/Netsky.worm(이하 넷스카이 웜)과 Win32/Bagle.worm(이하 베이글 웜)이다. 넷스카이 웜과 베이글 웜은 올해 초에 최초 발견된 후 급속하게 전파되었으며 최근까지 여러 형태의 변형으로 제작되어 확산되고 있다. 전파 방식도 초기에는 단순하게 메일을 통해 전파되는 일반적인 형태의 웜이었으나 여러 변형들이 생겨나면서 마이크로소프트 아웃룩의 보안 취약점과 같은 OS의 취약점을 이용하는 등 제작 기법이 다양해지고 있다.

[표1]은 2004년 6월 IPA/ISEC에 접수된 악성코드 노출에 대한 통계자료이다. 넷스카이 웜의 신고건수가 월등하게 많음을 알 수 있다.

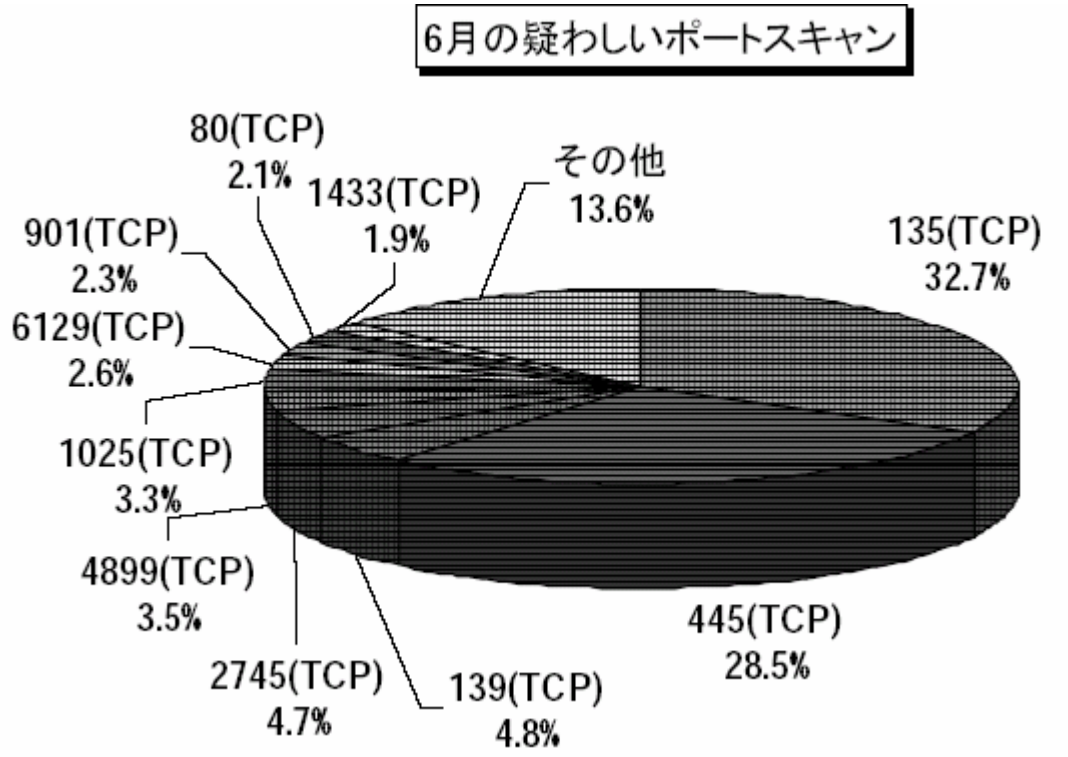
Window/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Netsky	1,875	Xm/Laroux	29	VBS/Redlof	167
W32/Bagle	502	X97M/Tristate	6	Wscript/Fortnight	22
W32Klez	362	X97M/Divi	4	Wscript /Kakworm	5
W32/LovGate	303	W97M/Bablas	3	VBS/Netlog	4
W32/Mydoom	249	XM/Sic	2	VBS/Haptime	2
W32/Bugbear	176	W97M/Marker	2	VBS/Loveletter	2

[표2] 악성코드 노출 신고 현황 (출처:IPA/ISEC)

일본 네트워크 트래픽 현황

[그림1]은 2004년 6월 한달동안 일본에서 발생한 네트워크 포트 사용현황을 나타낸 것이다. 가장 많은 트래픽을 유발하고 있는 포트는 TCP 135와 TCP 445 포트이다. 135 포트는 윈도우 OS에서 RPC 관련 통신을 위해서 사용되고, 445 포트 또한 SMB 프로토콜로 사용된다. 그러나 최근 유행하는 웜들이 윈도우 OS의 RPC 관련 취약점을 이용한 공격을 시도할 때에도 사용된다.

두 포트 이외에도 TCP 1745 포트를 사용하는 트래픽이 많은 것을 알 수 있는데 이는 베이글 웜에 감염된 시스템에 의한 것일 가능성이 있다.



[그림1] 일본의 네트워크 트래픽 현황

일본 경찰청의 Phishing에 대한 경고문 발표

일본 경찰청은 최근 개인의 정보를 불법으로 획득하기 위해 가공의 웹페이지를 만들고 은행 등 신뢰성이 있는 공공 기관을 사칭하여 계좌 정보 등을 입력하도록 속여 사용자 정보를 수집하는 행위인 Phishing에 대한 주의를 당부했다.

Phishing은 유럽이나 미국에서 최근 유행하고 있으며 일본에서도 이와 관련한 사고 발생의 위험이 높으므로 수취인이 불분명한 메일이나 홈페이지에 게재된 정보를 열람할 때 주의가 필요하다.

V. 6월 중국 피해 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

올 1월부터 이어진 매스메일러(Mass Mailer)들의 영향은 이제 더 이상 중국 악성코드의 전반적인 흐름으로 이어가지 못하는 것으로 분석된다. 5월부터 이어진 네트워크로 전파되는 웜들의 영향력은 매스메일러들을 수적으로나 양적으로나 크게 압도하고 있다. 이러한 웜들의 확산은 6월 중국 악성코드 동향의 커다란 대세로 이어지고 있다는 것이 이번 동향 분석의 흥미로운 점이라고 볼 수 있다.

중국의 악성코드 피해 TOP 5

순위 변화	6월	Rising	CNCVERC
*	1	Worm.Netsky	Worm_Sasser.A
*	2	Worm.Lovgate	Worm_AgoBot
NEW	3	Worm.Lentin.m	Worm_Netsky.D
NEW	4	Backdoor.Sdbot	Worm_Bbeagle.J
NEW	5	Trojan.Win32.LaSta	-

[표1] 2004년 6월 중국의 악성코드 TOP 5>

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

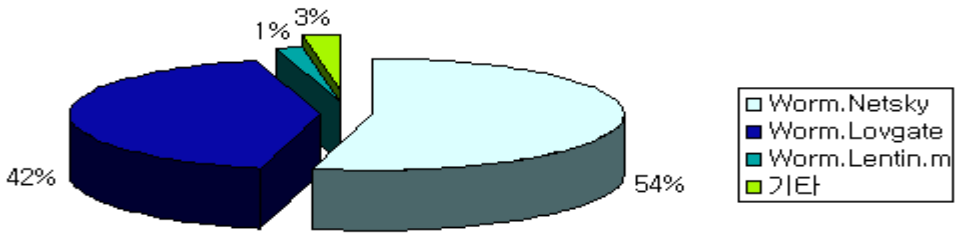
[표1]은 중국 로컬 백신업체인 라이징(Rising)사와 정부연구기관인 중국국가컴퓨터바이러스대응중심(China National Computer Virus Emergency Response Center, 이하 CNCVERC)이 작성한 6월 중국 악성코드 TOP 5이다. 위 두 기관의 통계 순위의 차이는 집계 방식과 통계를 위한 자료의 차이로 인한 것으로 추정된다. 하지만 두 기관의 통계를 통해서도 알 수 있듯이 매스메일러들의 영향은 줄어들고 네트워크로 전파되는 웜의 영향력이 5월에 비해 더 커졌다는 것을 쉽게 파악할 수 있다.

라이징사의 통계를 볼 경우 순위상의 1위와 2위는 지난 5월과 동일하게 Worm.Netsky(Win32/Netsky.worm, 이하 넷스카이 웜)과 Worm.Lovgate(Win32/LovGate.worm, 이하 러브게이트 웜)이 차지하고 있다. 하지만 넷스카이 웜은 달이 바뀔수록 그 영향력이 줄어들고 러브게이트 웜의 영향력이 커지고 있다. 그 실례로 라이징사의 6월 마지막 주 통계에 러브게이트 웜이 넷스카이 웜을 제치고 1위로 올라온 것으로 조사되었다.

3위는 이번달에 다시 순위권으로 진입한 Worm.Lentin(Win32/Yaha.worm, 이하 야하 웜)이 차지하고 있으나 전체적인 분포에서는 극히 적은 부분을 차지하고 있다. 그 뒤를 이은 4위에

는 순위권에 처음으로 진입한 Backdoor.Sdbot[1](Win32/SdBot.wrom, 이하 에스디봇 웜)이 차지하고 있다. 에스디봇 웜은 네트워크로 전파되며 기존에 알려진 Win32/IRCBot.worm과 유사한 부분을 많이 가지고 있다. 순위의 마지막인 5위에는 순위권에 처음으로 진입한 Trojan.Win32.LaSta가 차지하고 있다. Trojan.Win32.LaSta는 애드웨어의 일종이지만 정상적인 시스템 사용을 방해하는 증상으로 인해 트로이목마로 분류된 것으로 라이징사는 밝히고 있다.

악성코드 분포



[표2] 2004년 6월 중국의 악성코드 분포

[표2]는 6월 한달 동안 조사된 중국 악성코드의 분포도이다. 이 분포도를 참고할 경우 1위인 넷스카이 웜과 2위인 러브게이트 웜이 전체의 96%를 차지하고 있다. 이 두 웜이 메일로 전파되는 매스메일러들과 네트워크로 전파되는 웜을 대표해 중국 악성코드 흐름을 두고 마치 서로의 힘겨루기가 이루어지고 있는 것으로 보일 정도이다. 그러나 기타에 포함된 웜들까지 포함해 본다면 네트워크로 전파되는 웜들의 판정승으로 분석된다. 기타 3%에 포함된 악성코드에는 매스메일러는 한 건도 포함되어 있지 않고 있다.

기타에 포함된 악성코드는 다시 트로이목마 류와 네트워크로 전파되는 웜류로 크게 나누어 볼 수 있다. 트로이목마 류에는 TrojanDropper.WhBoy, Trojan.PSW.WhBoy.4가 차지하고 있으며 네트워크로 전파되는 웜류에는 에스디봇 웜, Worm.Agobot.3(Win32/AgoBot.wrom)과 Backdoor.Rbot(Win32/IRCBot.worm)이 차지하고 있다. 그리고 한국에서 개발된 특정 온라인게임의 사용자 계정과 암호를 가로채는 트로이목마인 Trojan.PSW.LMir.gs도 한부분을 차지하고 있으며 그 영향력은 미비하지만 꾸준히 발견되고 있는 중국에서 제작된 QQ 트로이목마 류인 Trojanl.QQtail도 한 부분을 차지하고 있다.

[1] AhnLab, http://info.ahnlab.com/smart2u/virus_detail_1361.html

6월 중국 동향을 분석하면서 특이한 점은 애드웨어 형태인 Trojan.Win32.LaSta의 등장이다. Trojan.Win32.LaSta가 기타에 포함되어 영향은 미비하다고 보일 수 있으나 중국 동향에서 애드웨어가 처음으로 등장하였으며 이러한 점은 곧 악성 애드웨어로 인해 중국 내에서도 사회적인 문제로 발전될 가능성이 높다는 것을 시사하고 있다.

결론

6월 중국 동향은 크게 두 가지 사항이 특이점으로 발견된다. 그 첫 번째가 네트워크로 전파되는 웜들의 대거 등장으로 인해 기존에 중국 악성코드 동향을 크게 점유하고 있던 매스메일러들을 밀어내고 있다는 것이다. 네트워크로 전파되는 웜들은 수적으로 절대 우세를 점유하고 있어 한여름의 시작인 7월 달에는 그 영향력이 더 커질 것으로 보인다. 두 번째로는 중국 동향 사상 처음으로 애드웨어 형태의 트로이목마가 순위에 올라 왔다는 점이다. 악성 애드웨어에 의한 피해는 이미 한국에서는 사회적인 문제로까지 발전하였으며 애드웨어를 전문적으로 제거해 주는 프로그램을 개발하는 업체까지 등장한 상황이다. 이러한 흐름이 중국에서도 이어질 것으로 조심스럽게 예측해 본다.

VI. 테크니컬 컬럼 - 휴대폰 웜의 등장과 향후 전망

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

휴대폰 웜의 출현

2004년 6월 14일(한국 시각 6월 15일 오후) 세계 최초의 휴대폰 웜 발견 소식이 알려졌다[1]. 블루투스(Bluetooth)[2] 기능을 지원하는 일부 심비안(Symbian) 운영체계의 스마트 폰(Smart phone)에서 감염되는 웜으로, 현재까지 일반에 감염 보고되지 않았다. 이 웜의 제작자는 바이러스 제작 그룹의 회원으로 확인되었으며 휴대폰 악성코드를 제작할 수 있다는 것을 증명하는 것으로 보이며, 이런 유형을 보통 개념 바이러스(Concept Virus)라고 부르고 있다. 따라서 이 웜은 휴대폰에서도 활동할 수 있는 웜을 만들 수 있음을 세계 최초로 증명한 웜이다.

카비르(Cabir) 웜의 특징

카비르 웜으로 불리는 이 웜은 EPOC.Cabir, EPOC_CABIR, Symbian.Cabir, Symbian/Cabir, Worm.Symbian.Cabir 등으로도 불리고 있다. 이 웜은 심비안 운영체계에서 실행되며 전파를 위해 근거리 무선통신 규격인 블루투스를 이용한다. 따라서 이 웜은 모든 휴대폰이 아닌 일부 휴대폰에서 전파되어 한계가 존재한다. 현재 이 웜에 감염될 수 있는 기기는 노키아 3650, 6600, N-Gage로 알려져 있었다. 노키아 외 다른 업체에서도 심비안 운영체계를 이용한 스마트 폰을 개발하고 있는 것으로 알려져 있다.

실제 감염 가능성 낮음

현재까지 이 웜에 실제 감염되었다는 보고는 없다. 또 여러 전문가들이 다음과 같은 이유로 웜이 실제로 문제가 될 가능성은 없다고 한다.

- 심비안 운영체계에서만 실행된다.
- 전파에 이용되는 블루투스 기능은 기본적으로 꺼져 있다.
- 블루투스를 통한 통신 가능한 반경이 10m 내외이다.
- 프로그램 설치 시 사용자의 동의를 구해야 한다.

이 웜은 심비안 운영체계에서만 사용되므로 심비안 운영체계 폰을 거의 사용하지 않는 한국 등의 지역에서는 이 웜에 감염될 가능성이 낮다. 또한 블루투스는 기본적으로 꺼져 있어 기본 사용자들에게는 파일 전송이 되지 않는다. 또한 블루투스 기능을 사용한다고 해도 통신 가능한 반경이 10m 내외이므로 빠른 시간에 감염 대상을 찾기 어렵다. 어렵게 웜이 감염 대

[1] News.com, http://news.com.com/Worm+ ready+ to+ wriggle+ into+ smart+ phones/2100-7349_3-5233517.html?tag=html.alert

[2] Terms Korea and whatis.com Inc, http://www.terms.co.kr/Bluetooth.htm

상을 찾아 웜 파일을 보내려고 해도 프로그램 설치 시 사용자의 동의(Installation security warning. Unable to verify supplier. Continue anyway?)를 구하므로 감염 가능성은 매우 낮아지게 된다.

하지만, 이 같은 이유로 휴대폰 웜이 앞으로도 문제되지 않는 것은 아니다.

- 보안보다 기능을 우선시 함
- 미흡한 사용자 보안 의식
- 보안 취약점

새로운 편리한 기술이 선보일 때 마다 기능과 보안에서 편리한 기능을 우선시 하고, 보안 강화는 사용자를 불편하게 한다는 이유로 적용되지 않는 것이 많다. 그리고 컴퓨터 사용자들도 보안 의식이 부족하거나 보안에 대해 잘 몰라 웜 등의 악성코드게 감염되는 경우가 많았다. 휴대폰 사용자는 컴퓨터 보다 더 사용자가 많으며 더구나 보안에 무지한 사용자가 많으므로 보안 경고 창이 떠도 사용자가 "예"를 누를 가능성이 매우 높다. 또한 무선으로 인터넷이 가능할 때 보안 취약점 가능성도 늘 존재하므로 보안 취약점을 이용해 사용자 동의 없이 자동으로 감염될 수 있다. 휴대폰은 컴퓨터만큼 켜져 있는 경우가 많으므로 우려되는 부분이다.

휴대폰 악성코드 전망

바이러스를 포함한 모바일 악성코드의 등장 가능성은 예전부터 예상 되었다. 카비르 웜의 등장으로 시기가 조금 앞당겨지긴 했지만 필자의 생각으로는 아래 내용을 몇 가지 혹은 한 두 가지라도 충족해야 실제 일반 사용자들에게 위협이 되는 휴대폰용 악성코드가 등장할 것으로 전망된다.

- 플랫폼 통일
- 많은 동일 플랫폼 사용자
- 무선 네트워크 연결
- 보안 취약점 존재 유무
- 손쉬운 프로그램 다운로드 및 설치 유무

휴대폰용 악성코드가 등장하려면 무엇보다 플랫폼 통일과 그로 인한 많은 사용자가 필요하다. 일반적으로 악성코드를 제작해 퍼뜨리는 사람들은 감염 대상이 많을수록 만족감을 느끼게 된다. 따라서 현재와 같이 국가별, 지역별로 사용하는 폰 종류와 운영체계가 다른 상황에서는 해당 악성코드는 특정 기기, 특정 회사, 특정 지역에서만 한정적으로 활동하게 되어 그만큼 해당 악성코드의 감염 대상도 줄어 들게 되고 악성코드 제작자들의 동기부여도 줄어들게 된다. 하지만, 플랫폼 통일 이전에도 특정 플랫폼에서 활동하는 악성코드는 등장할 것으로 보인다.

플랫폼의 통일과 사용자가 많다고 해도 현재의 컴퓨터 악성코드처럼 메일이나 네트워크 등의 전파 방법이 필요하다. 만약 이런 전파 방법이 없다면 당분간 휴대폰 주소록 정보 등을 파괴하는 정도의 트로이목마가 제작될 가능성은 높다. 현재의 휴대폰 프로그램은 보통 특정 사이트에서 요금을 결제하고 프로그램을 다운로드 하는 방식을 이용하고 있다. 따라서 트로

이목마 제작자는 다운로드 사이트를 해킹해 파일을 바꿔 치기 해야 하는 등의 문제가 발생한다. 하지만, 컴퓨터의 경우처럼 공짜로 프로그램을 사용하고 싶은 사람들이 존재하고 불법 복제는 항상 문제가 되고 있다. 최근 휴대폰 보안에 우려되는 상황이 발생했다.

불법 모바일 게임 다운로드 비상[1]

휴대폰용 프로그램은 예전에는 해당 서비스 업체 등이 인터넷을 통제했지만 이렇게 불법 복제 프로그램이 나돌고 휴대폰용 웹사이트가 여기 저기 생기면 분명히 게임 등으로 가장한 트로이목마, 웜이 발생할 수 있다. PC로 본다면 1980년대 말과 1990년 대 초반의 국내 PC 통신과 유사하다. 당시에는 PC 통신망에 올려진 프로그램을 다운로드 해 바이러스에 감염되는 경우가 많았다. 우선 퍼스널 컴퓨터용 악성코드의 발전처럼 초기에는 불법 모바일 게임 다운로드 등을 통해 트로이목마가 제작될 가능성이 높다. 휴대폰용 트로이목마는 주소록 내용 삽입/삭제/수정, 단문 문자 서비스(SMS) 자동 발송 등을 할 수 있을 것으로 예상된다.
휴대폰 웜이나 바이러스가 다른 휴대폰으로 전파되기 위해서는 현재와 같은 상황에서는 불법 프로그램이나 블루투스 등 외에는 없다. 따라서 휴대폰 웜이나 바이러스가 다른 기기로 전파되기 위해서는 무선 인터넷 연결이 필요할 것으로 보인다. 현재 휴대폰을 이용한 인터넷은 요금도 비싸고 사용자가 적지만 기술이 발전해 휴대폰이 인터넷에 쉽게 접속할 수 있다면 더욱 빠른 속도로 전파될 수 있을 것이다. 이외 무선 인터넷에 연결된 휴대폰에 보안 취약점이 존재한다면 휴대폰이 켜져 있는 것만으로도 웜에 감염될 수 있다.
또한 여러 업체에서 휴대폰, 가정 기기, 컴퓨터를 연결하는 추세이므로 향후 하나의 악성코드가 여러 기기를 감염시킬 가능성도 존재한다.

백신 업체의 대응

현재 몇몇 백신 업체는 모바일용 백신을 개발하고 있거나 개발에 성공했다. 안철수연구소도 세계 최초로 위피(WIPI)용 휴대폰 백신 개발에 성공[2]하였다.
하지만, 현재 백신 업체들은 특정 플랫폼에 대해서만 백신을 개발하고 있다. 플랫폼 통일의 경쟁 속에서 휴대폰용 백신의 생존도 동일하게 진행될 것으로 보인다. 여전히 대부분의 업체는 휴대폰용 백신이 없으며 카비르 웜의 경우처럼 윈도우용 백신에서 휴대폰용 웜을 진단/치료(삭제) 할 것이다.

결론

휴대폰, PDA 등의 모바일용 악성코드 가능성은 몇 년 전부터 예상되어 왔었다. 카비르 웜은 단지 휴대폰에도 악성코드가 가능하다는 것을 증명하는 수준이지만, 머지 않아 실제 사용자들에게 전파되는 악성코드가 등장할 가능성은 점점 높아지고 있다고 할 수 있다. 아직 플랫폼 통일화 등의 문제가 남아 있지만 플랫폼이 통일화되고 사용자 수가 증가하고 웜, 바이러

[1] http://erunnews.freechal.com/news/contents.asp?docid=844
[2] AhnLab, http://info.ahnlab.com/ahnlab/report_view.jsp?num=341

스 등이 활동하기 좋은 환경(?)이 된다면 휴대폰 등의 모바일 장비에도 현재 컴퓨터와 같은 웜 등의 악성코드 문제가 대두될 것으로 예상된다.

VII. 2004년 상반기 동향 분석

(1) 악성코드 동향 분석

작성자: 차민석 연구원(jackycha@ahnlab.com), 정진성 연구원(jsjung@ahnlab.com)
김소헌 주임연구원(sohkim@ahnlab.com), 장영준 연구원(zhang95@ahnlab.com)

한국의 악성코드 동향

피해 동향

지난 2003년 한 해는 2002년에 비해 많은 악성코드에 대한 피해문의가 급증했던 한 해였다. 그러나 2003년의 기록은 2004년 상반기 동안에 깨지고 말았다. 악성 IRCBot 유형들의 폭발적인 증가와 다시 유행처럼 찾아온 Mass Mailer의 급격한 증가가 주된 원인이다.

2004년 상반기 안철수연구소가 피해신고 문의를 받았던 통계를 2003년도 상반기 자료와 함께 비교해 보면 [표1]과 같다.

구분	1 월	2 월	3 월	4 월	5 월	6 월	합계
2003 년	2,680	2,234	2,369	3,087	4,185	2,993	17,548
2004 년	5,580	6,641	5,147	5,633	22,104	22,209	67,314

[표1] 2003년, 2004년 상반기 월별 국내 악성코드 피해 신고 통계

[표1]의 합계가 보여주듯이 작년 상반기에 비해 올 상반기는 무려 380% 이상 피해문의가 폭발적으로 급증하였다. 2003년 한해 전체 피해문의가 67,012 건인데 비해 올해 상반기는 이를 벌써 넘은 수치로, 안철수연구소 통계집계상 역대 최고의 피해문의 건수이다. 이러한 피해문의 급증은 위에서 언급한 것처럼 악성 IRCBot 변형의 폭발적인 증가, 짧은 기간 동안 확산된 Mass Mailer의 증가와 이들이 보내는 대량 메일들이 주된 원인이다. 위와 같은 기록적인 피해문의 건수를 가능하게 했던 Mass Mailer들은 다음과 같다.

- Win32/Bagle.worm (이하 베이글 웜)
- Win32/Netsky.worm (이하 넷스카이 웜)
- Win32/MyDoom.worm (이하 마이둠 웜)
- Win32/Dumaru.worm (이하 두마루 웜)

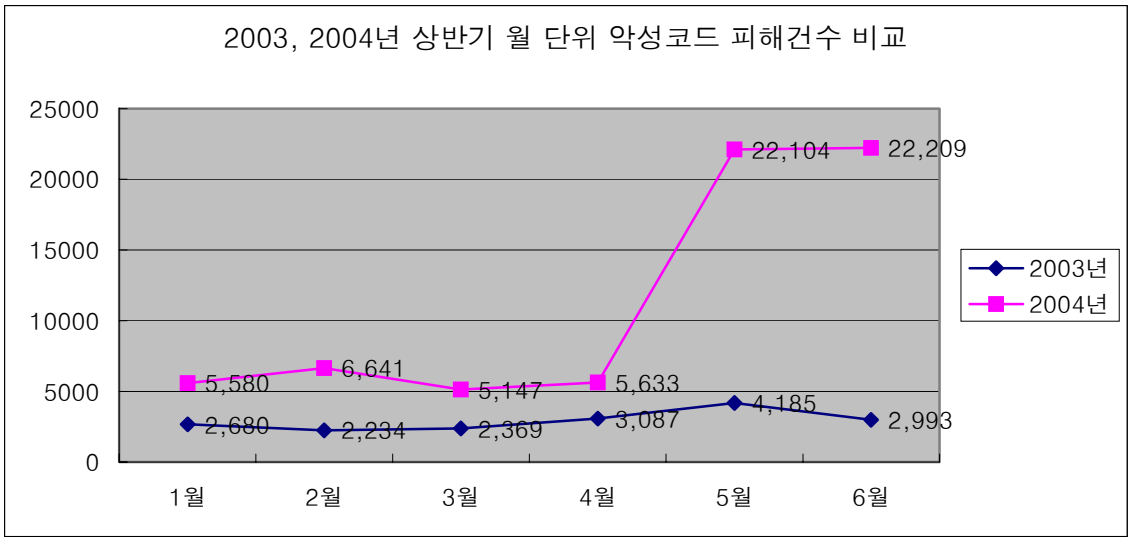
작년 상반기와 올해 상반기의 악성코드 피해 중 Top 10을 차지한 것을 정리해보면 Mass

Mailer에 의한 피해문의가 많은 것은 작년 상반기와 올해 상반기가 동일하다. 그러나 2003년 상반기 경우 Mass Mailer를 비롯하여 악성 IRCBot 트로이목마, 그리고 구종의 윈도우 파일 바이러스 등이 다양하게 보고된 반면, 2004년 상반기는 1종을 제외하고 Top 10에 속한 대부분의 악성코드들이 모두 Mass Mailer들이다. 다음의 [표2]가 이를 잘 말해주고 있다.

순위	2003 / 악성코드명	건수	2004 / 악성코드명	건수
1	Win32/Yaha.worm.45568.B	2,373	Win32/Netsky.worm.29568	19,708
2	Win32/LovGate.worm.107008	1,456	Win32/Dumaru.worm.9234	11,130
3	Win32/FunLove.4099	532	Win32/Netsky.worm.17424	6,571
4	Win95/Spaces.1445	488	Win32/Netsky.worm.28008	2,805
5	mIRC/Stde9	475	Win32/Netsky.worm.22016	1,922
6	Win32/Klez.worm.H	463	Win32/Netsky.worm.17920	1,747
7	Win32/Nimda	408	Win32/Blaster.worm.6176	1,645
8	Win32/Parite	356	Win32/Netsky.worm.22016	801
9	Win32/Elkern.B	296	Win32/Bagle.worm.Z	686
10	Win32/Sobig.worm.65536	266	Win32/Netsky.worm.22016.C	684

[표2] 2003년, 2004년 상반기 악성코드 피해 10 Top 비교

[표2] 에서도 알 수 있듯이 올해 1월~3월에는 두마루 웜이 가장 많은 피해를 주었고 [그림1]에서 확인되듯이 5월과 6월은 넷스카이 웜 피해로 인해 지금까지 보지 못했던 기록적인 피해문의 건수가 집계되었다.



[그림1] 2003, 2004년 상반기 월 단위 악성코드 피해건수

올해 상반기에 Mass Mailer류에 의한 피해문의가 급증한 이유는 예년에 비해 다수의 새로운

Mass Mailer 출현, 웜 제작자간의 경쟁으로 인한 수많은 변형의 출현, 그리고 웜에 감염된 시스템도 이전에 비해 많이 증가한 것을 들 수 있다. 하지만 가장 주요한 원인은 감염된 시스템에서 웜 파일이 첨부된 메일을 발송하는 양이 크게 증가한 것이 Mass Mailer에 의한 피해신고가 크게 증가한 주요 원인 중 하나일 것으로 추정된다.

신종 발견 동향

올해 상반기의 신종 악성코드 추세는 다음과 같다.

- Mass Mailer의 급격한 증가
- 악성 IRCBot 웜 변형의 폭발적인 증가
- 운영체계 및 응용 프로그램의 취약점을 이용한 악성코드 급증
- 진단/치료하기 어려운 악성코드 증가

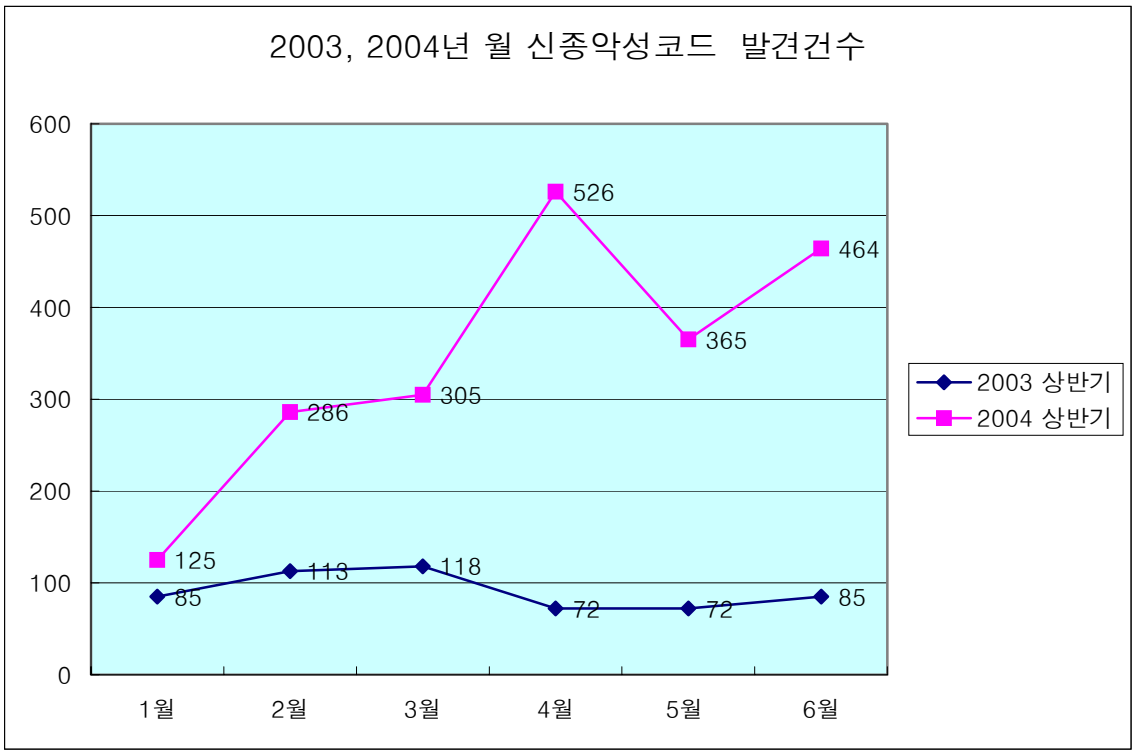
2004년 상반기 국내 발견된-변형 포함-신종 악성코드는 모두 2,071종으로, 지난해 동기 545종에 비하여 거의 4배가 넘게 증가하였는데 [표3], [표4]와 같다.

월	리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	합계
1월	0	7	50	18	3	7	0	0	0	85
2월	0	2	78	15	3	13	1	1	0	113
3월	2	3	76	24	1	12	0	0	0	118
4월	0	1	46	11	3	11	0	0	0	72
5월	0	4	39	14	2	13	0	0	0	72
6월	0	2	52	6	4	21	0	0	0	85
합계	2	19	341	88	16	77	1	1	0	545

[표3] 2003년 상반기 신종 악성코드 유형별 집계표

월	리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	애드웨어	합계
1월	0	0	50	7	6	58	0	0	0	4	125
2월	0	1	130	8	1	146	0	0	0	0	286
3월	0	1	75	5	3	196	0	0	0	25	305
4월	0	1	111	0	7	403	0	0	0	4	526
5월	0	1	32	3	2	322	0	0	0	5	365
6월	0	0	59	2	1	402	0	0	0	0	464
합계	0	4	457	25	20	1527	0	0	0	38	2071

[표4] 2004년 상반기 신종 악성코드 유형별 집계표



[그림2] 2003, 2004년 월 신종 악성코드 발견 건수

작년 동기에 비해 4배 가까이 증가한 원인의 대부분은 다음과 같은 종류의 악성 IRCBot 웜류에 의한 것이다.

- Win32/AgoBot.worm (이하 아고봇 웜)
- Win32/Rbot.worm. (이하 알봇 웜)
- Win32/SdBot.worm (이하 에스디봇 웜)
- Win32/SpyBot.worm (이하 스파이 봇)

상반기 악성 IRCBot 웜 유형이 폭발적으로 증가한 반면 악성 IRCBot 트로이목마는 동년과 대비하여 상당수 감소한 것을 알 수가 있다. 2003년에는 악성 IRCBot 웜 보다는 트로이목마가 주로 보고되었다. 이와 같은 원인은 악성 IRCBot이 기술적으로 발전했기 때문이다. 즉, 기존 트로이목마 형태에서 자신을 전파시키기 위해서 네트워크를 스캔하고, 감염대상 시스템의 서비스 또는 작업 스케줄러에 기록하는 등 자신을 전파 및 실행시키기 위해 다른 유틸리티의 도움을 받지 않는 웜으로 발전했기 때문이다.

[표5]는 1998년부터 2003년까지 연구소가 집계한 국내 발견된 신종 악성코드 종류 수이다. 올 상반기에만 2,071종이 발견되었으니 올 상반기 얼마나 많은 종류의 악성코드가 사용자를 괴롭혔는지 짐작할 수 있겠다.

연도	88	89	90	91	92	93	94	95	96	97	98	99	2000	2001	2002	2003	총계
합계	1	6	28	21	17	34	76	128	226	256	276	379	572	435	277	1,239	3,971

[표5] 1998년~2003년 국내 발견 악성코드 통계

올 상반기에 신종 악성코드가 증가한 또 하나의 이유는 바로 다양한 Mass Mailer들이 발견, 보고되었다는 것이다. 주목할 것은 이러한 Mass Mailer들이 약 석달이라는 짧은 기간에 무려 각각 30가지가 넘는 변형이 나왔다는 것이고, 변형이 나올 때마다 악성코드의 제작기법이 기술적으로 발전하였다.

올해 발견된 악성코드가 지난해와 다른 점은 다음과 같은 기법을 자주 사용했다는 것이다.

- 메모리 형태로만 존재 또는 리모트쓰레드(Remote Thread)로 존재
- 커널 모드 백도어 (커널 드라이버를 이용하여 Native API 후킹)
- Stealth 기법 (다수의 Win32 API 를 가로채서 자신의 존재를 숨김)

이와 같은 기법을 사용하는 것은 악성코드에 대한 치료 백신의 개발의 지연을 불러온다. 따라서, 이것 또한 상반기 악성코드 제작자가 의도한 현상인 것으로 파악된다.

일본의 악성코드 동향

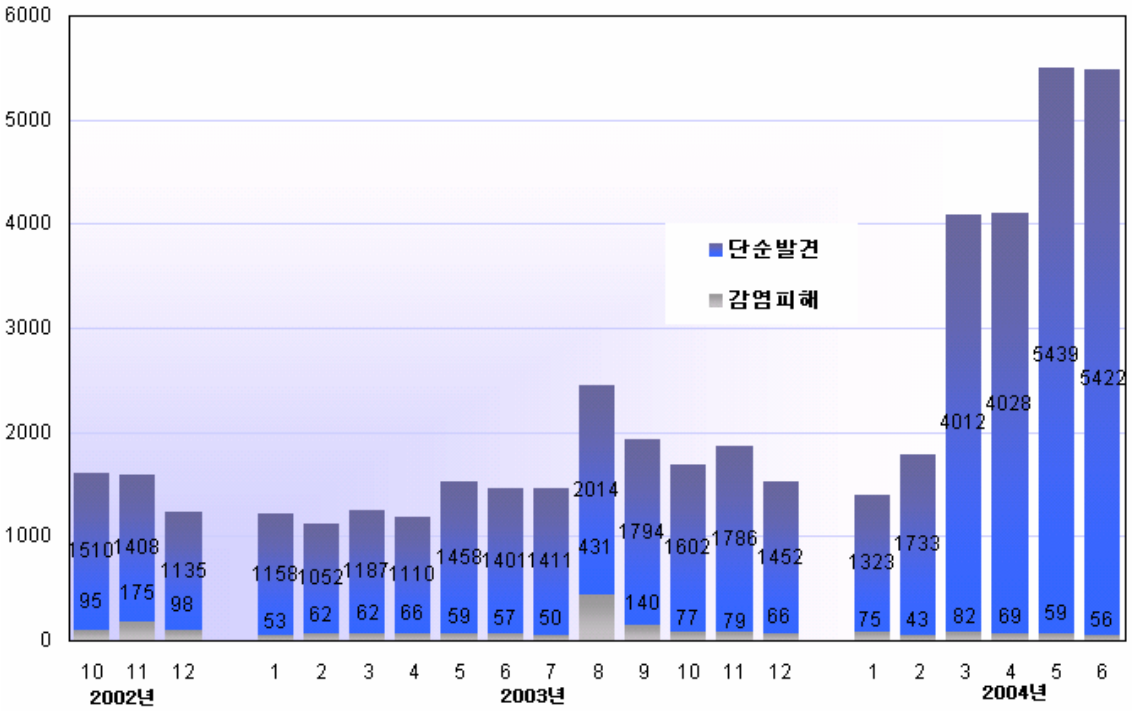
2004년 상반기에 일본에서 가장 많이 확산된 악성코드는 넷스카이 웜인 것으로 나타났다.
아래의 도표는 일본의 IPA(정보처리추진기구)에서 집계한 월별 악성코드 노출 현황을 집계한 것이다. 도표에서 보는 것처럼 넷스카이 웜에 의한 노출 건수가 다른 악성코드에 비해 월등히 많은 것을 알 수 있다.
넷스카이 웜 이외에도 마이둠 웜과 베이글 웜 등 올해 초부터 유행했던 Mass Mailer의 변종들이 일본에서도 많은 피해가 있었음을 알 수 있다.
특이할 만한 점은 아직도 Win32/Klez.worm(이하 클레즈 웜)에 노출되는 경우가 여전히 많이 남아있다는 점이다. 아마도 OS의 취약점을 이용하는 클레즈 웜 전파방식과 Win32/Elkern 바이러스 (이하 엘컨 바이러스)등과 중복 감염됨으로 인해 일반 사용자들이 백신을 이용하여 쉽게 고치기 어려운 점이 아직까지 클레즈 웜에 노출되는 원인으로 생각된다.

Win/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Netsky	7571	Xm/Laroux	99	VBS/Redlof	571

W32/Mydoom	2106	X97M/Divi	18	Wscript/Fortnight	106
W32/Klez	1818	W97M/X97M/Tristate	14	VBS/Loveletter	17
W32/Bagle	1689	W97M/Marker	9	Wscript /Kakworm	14
W32/Swen	877	W97M/Bablas	7	VBS/Netlog	11
W32 Mimail	606	X97M/Poorboy	4	VBS/Haptime	5
W32/Bugbear	530			VBS/Freelink	2

[표6] 일본의 월별 악성코드 노출 현황(출처:IPA)

[그림3]의 그래프는 월별 악성코드 노출 현황을 도식화한 것이다.



[그림3]일본의 월별 악성코드 노출 현황(출처:IPA)

[그림3]에서 나와있는 것처럼 2004년 현재 악성코드에 노출된 사용자가 이전에 비해 급격하게 증가함을 알 수 있다. 이는 2월 말부터 전파되기 시작한 넷스카이 웜 등 Mass Mailer의 영향이 매우 크다고 할 수 있다.

그러나 일반 사용자들에게 노출되는 빈도수에 비해서 실제로 감염되어 피해를 당한 경우는 그리 많지 않은 것으로 나타났다. Mass Mailer가 발송하는 메일의 양이 늘어난 것이 이처럼 사용자들이 악성코드에 노출되게 된 주요 원인 중의 하나로 추정된다. 이는 작년 중반기에 발견되어 다량의 메일을 생성함으로써 전세계적으로 큰 피해를 주었던 Win32/Sobig.worm(이하 소빅.F 웜)과 비슷한 현상으로 보아야 할 것이다.

중국의 악성코드 동향

상반기 중국 악성코드 동향을 시기별로 나누어 본다면 메일로 전파되는 Mass Mailer가 급속하게 확산되고 유입된 1월~3월, 네트워크로 전파되는 웜이 대거 등장한 4월~5월, 그리고 애드웨어 성향을 가진 트로이목마가 등장한 6월로 구분해 볼 수 있다.

그렇다면 중국 현지의 백신업체와 정부기관에서 지켜본 상반기의 동향은 과연 어떠한지 살펴보자. 중국 내 시장 점유율 2위를 차지하고 있는 강민(江民, www.jiangmin.com)에서 작성한 자료를 토대로 살펴보기로 하자.

순 위	강민 진단명	AhnLab 진단명
1	I-Worm/Sasser	Win32/Sasser.worm
2	I-Worm/NetSky	Win32/Netsky.worm
3	Trojan/PSW.HidWebmon	-
	Trojan/KeyLog.Dingxa	
	TrojanSpy.Elelist	
4	I-Worm/Mydoom	Win32/MyDoom.worm
5	I-Worm/BBEagle	Win32/Bagle.worm
6	I-Worm/Supkp	-
7	I-Worm/Sobig	Win32/Sobig.worm
8	I-Worm/Chian	-
9	I-Worm/Klez	Win32/Klez.worm
10	PolyBoot (WYX.B)	-

[표7] 중국 백신업체 강민의 2004년 중국 악성코드 TOP 10

[표7]의 자료를 참고로 볼 경우 10위권 안에 포함되어 있는 악성코드에는 Mass Mailer 형태가 4건이 포함되어 있으며 네트워크로 전파되는 웜은 1건만 포함되어 있는 것이 특이하다. 즉, 중국 내의 상반기 악성코드 동향은 세계적인 흐름인 Mass Mailer의 확산에서 네트워크로 전파되는 웜으로의 변화를 충실하게 따르고 있음과 동시에 중국 내에서만 발생하는 트로이목마의 확산이라는 특이점을 동시에 내포하고 있는 것으로 보인다.

중국 로컬 백신업체인 강민(江民, www.jiangmin.com)에서 작성된 보고서 뿐 아니라 중국 정부기관인 중국 CERT(www.cert.org.cn)에서 작성된 보고서를 보더라도 중국의 이런 흐름은 동일하게 나타난다.

2004년 상반기 중국 내외에서 본 중국 악성코드의 동향을 살펴본 결과, 한국을 비롯한 세계

적인 악성코드 피해동향의 추세와 중국의 것이 유사한 것을 알 수 있으며, 이는 중국 역시 더 이상 악성코드에 대한 안전지대가 될 수 없다는 것을 보여주고 있다. 이와 동시에 다양한 트로이목마의 등장은 중국만의 특징이 아닌가 싶다. 그리고 6월을 기점으로 하여 서서히 등장하고 있는 애드웨어 성향을 가진 트로이목마는 중국 내에서의 보고가 아직 미비하지만 조만간 하나의 큰 흐름을 이루게 될 것으로 예상되며 이는 곧 중국 내에서 악성코드 감염경로의 변화를 넘어서 악성코드 형태 자체의 변화로도 이어질 것으로 예측 된다.

결론

2003년 한 해의 악성코드 동향을 정리하며 2004년은 힘겨운 한 해가 될 것으로 예상했다. 그런 우려는 현실이 되었고 2004년 역시 악성코드의 증가추세가 꺾이지 않았다.
2004년 1월 말 발견된 마이둠 웜부터 봄에는 베이글 웜과 넷스카이 웜 제작자의 감정 싸움으로 많은 변형이 양산되면서 일반 컴퓨터 사용자와 백신 업체 직원들의 고생이 많았던 상반기이다. 5월 1일 전 세계를 강타한 Win32/Sasser.worm (이하 새서 웜)은 작년 여름 발생한 Win32/Blaster.worm(이하 블래스터 웜)만큼의 피해를 줬다.

상반기는 메일로 전파되는 웜이 대부분의 나라에서 높은 감염율을 보였다. 하지만, 상반기 악성코드 동향에서 빼 놓을 수 없는 것이 아고봇 웜, 에스디봇 웜 등으로 대표되는 악성 IRCBot 류이다. 악성 IRCBot 변형은 상반기에만 수천 개의 변형이 발견되었다. 악성 IRCBot 류는 광범위하게 피해를 주기 보다는 주로 기업체 등에 감염되어 사내 인터넷 망을 마비시키는 등의 부작용을 일으켰다.

상반기 또 하나의 특징으로는 기술적으로 사용자나 백신이 발견을 어렵게 하는 은폐형 기법(Stealth Technique)을 이용하는 형태가 점차 증가했다는 것이다. 아직 은폐형 기법을 사용하는 악성코드 수는 많지 않지만 은폐형 기법을 사용하는 악성코드에 감염되면 감염 파일을 찾는 것 조차 어려운 형태가 많다. 이에 안철수연구소는 이런 은폐 기법을 사용하는 악성코드를 무력화하는 기술을 개발했다.

6월에는 세계 최초의 휴대폰 웜이 발견되었다. 현재 실제적으로 위협을 주는 것은 아니지만 이로써 휴대폰도 악성 코드의 안전 지대가 아님이 증명되었다. 몇 년 후에는 악성코드 집계에 윈도우용과 모바일용이 따로 집계되는 날이 오는 것이 아닌지 걱정스럽다.

마지막으로 바이러스 등의 전통적인 악성코드는 아니지만 애드웨어(Adware)의 피해도 계속 증가하고 있다. 특히 홈페이지를 고정하는 피해가 가장 많았으며 보기 싫은 광고 창을 지속적으로 띄워 많은 사람들을 불편하게 있다. 백신 업체는 애드웨어를 바이러스 등의 악성코드로 분류하지 않아 기본적으로 진단하지 않는 정책을 취하고 있지만 애드웨어의 범위를 벗어

나 홈페이지를 고정하는 등의 형태는 트로이목마로 분류하여 백신에서 퇴치하도록 하고 있다. 이들 애드웨어의 기술도 계속 발전하여 파일명을 변경하거나 사용자가 쉽게 제거하기 힘든 형태로 발전하게 되었다. 애드웨어는 돈과 직접적으로 관련되어 점점 트로이목마화 되어 발전하고 있다.

(2) 시큐리티 동향 분석

작성자: 정관진 주임연구원(intexp@ahnlab.com)

어느새 2004년의 반이 흘러 따뜻한 여름을 맞이하고 있다. 여름 휴가철로 많이 찾는 곳 중의 하나가 바로 이 시원한 바다인데, 드넓기만 한 이 바닷속이 인류가 아직 완전히 정복하지 못한 신천지중 하나라고 한다. 보안영역도 바다에 비유되는 인터넷과 같이 넓은 가상의 공간이라는 점 때문에 쉽게 정복하지 못하는 부분 중의 하나가 아닌가 싶다.
이러한 이유는 과거와 비교해 봤을 때 발생하는 위협들이 더욱 지능화, 복잡화 되어 가고 있다는 점에서다. IT(Information Technology)는 현 우리 생활 깊숙이 들어와 하나가 되어가고 있으며, 초고속 인터넷망의 보급은 가정의 컴퓨터 및 가전기기까지 전세계의 어느 곳이라도 연결될 수 있는 기반을 마련해 주고 있다. 그만큼 인터넷 공간에 노출되고 있는 범위가 넓어지고 있으며, 이것은 외부의 위협으로부터 보호를 더욱 강조해 주고 있다. 해가 거듭하면 할수록 보안 영역은 더욱 넓어지게 되고, 이를 방어하기 위한 기술과 악용 및 공격하기 위한 기술이 계속 교차하게 될 것이다.

특히 올해는 작년과 비교해 보면 웜들이 더욱 극성을 부렸는데 이러한 현상은 아고봇, IRCBot 등과 같은 봇(Bot) 종류에 의한 수 많은 변종들이 나타나면서부터이다. 이들이 이렇게 많은 변종과 확산이 가능했던 것은 바로 현재의 IT 인프라도 한 몫을 담당했기 때문이다. 더불어 취약점을 이용하여 웜이 나오는 시간적 주기도 점점 짧아지며 취약점이 나온 후 이를 이용한 웜이 하루내에 나올 수 있는 '0-day' 시간에 근접하고 있다. 일례로 2004년 3월 20일 발견된 Win32/Witty.worm(이하 위티 웜)은 3월 8일 해당 취약점이 처음 발견되었고, 3월 18일에 공개되었다. 취약점이 공개된 이후 웜이 나오기까지의 시간이 상당히 짧았다는 점이다.

취약점 중에서 올해 많이 이용된 취약점중의 하나가 마이크로소프트 윈도우의 LSASS(Local Security Authority Subsystem Service)이다. 특히, 5월 1일 발생한 새서 웜은 LSASS 취약점을 이용하여 전세계적으로 많은 피해를 입혔고 Win32/Korgo.worm(이하 코르고 웜), 아고봇 등의 웜들도 이 취약점을 이용하였다. 특히 윈도우 운영체제의 취약점이 공개되는 경우 이를 이용한 웜들이 나타나는 경우가 빈번한데, 이것은 다수의 사람들이 사용하고 있다는 점에서 효과적으로 전파에 이용될 수 있기 때문이다. 이런 경우에는 패치가 반영되어 있으면 문제없지만 패치가 나왔는데도 불구하고 반영이 늦어져 해당 취약점을 이용하는 웜이 나타날 경우 문제가 커지게 된다. 작년 2003년 8월의 블래스터 웜과 같이 패치가 나왔어도 반영이 늦어져 큰 문제가 생긴 것 같이 앞으로도 관리자들의 패치 이슈는 계속 될 것으로 생각된다.

이와 함께 올해 들어 소스코드가 배포되는 형태가 나타나고 있다. 소스코드는 건물을 설계할 때 설계도에 해당하는 부분으로 소프트웨어로 따진다면 그 해당 소프트웨어의 모든 것을 알고 있다는 것과 같다. 소스코드 유출은 크게 웜에 의해 의도적으로 배포된 형태와 사고에 의해 유출된 것으로 나눠볼 수 있다. 마이둠 웜과 최근의 베이글 웜이 소스코드를 의도적으로 유포하였다. 또한, 언더그라운드 커뮤니티에서는 음성적으로 교환하고 있는 것으로 알려지고 있다. 이렇게 소스의 유출은 많은 변형의 창출 가능성과 다른 웜 제작자들이 활용하는데 쓰이게 되어 유심히 지켜볼 일이다. 의도적인 배포 이외도 올해 2월 MS사의 윈도우 2000 운영체제의 소스코드 일부가 유출되었으며, 5월에는 시스코사의 네트워크 장비 운영체제인 IOS 12.3 소스코드 800 메가 중 일부가 공개되었다. 소스코드 유출로 인한 큰 사고는 아직까지 보고되지 않았지만 유의 주시해야 필요성이 있다.

2004년의 하반기에는 또 어떤 일들이 우리에게 일어날지 지켜보아야 하겠지만, 현재와 같은 추세라면 지능적, 복합적인 위협은 계속 증대되게 될 것이다. 웜 뿐만 아니라 많은 보안 사고들이 이제는 단순히 과거의 기술만을 이용하는 것이 아니라 컴퓨터 기술의 변화발전에 따라 변화하고 있다는 사실을 잊어서는 안되겠다. 위협의 범위는 이제 우리에게 더욱 가까이 다가오고 있는 것이다.