ASEC Report 4월

® ASEC Report

2004. 5

안철수연구소의 시큐리티대응센터(Ahnlab - Security E-response Center)는 악성 코드 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

다양한 변형발견과 LSASS 취약점을 이용한 공격…

2004년 4월은 지난 3월에 이어 다시 한번 피해신고된 악성코드의 수가 갱신되었다. 아울러 올 4개월동안 국내에서 발견된 신종의 수가 지난 한해동안 국내에서 발견된 신종의 수와 거의 비슷한 수치를 보이고 있다. 그만큼 올해 들어 신종, 변형의 발견과 피해가 급증하고 있다. 이러한 원인으로는 올해 제작자들간에 경쟁적으로 변형을 제작하여 배포했던 Mass Mailer 웜인 넷스카이 웜, 베이글 웜의 발견이 그 하나이며, 악성 IRCBot 류인 아고봇 웜의 많은 변형이 발견되고 있는 것이 또 다른 하나의 이유이다.

2004년 4월은 마이크로소프트의 윈도우 제품군에 대한 보안취약점이 발표되었다. 이 보안취약점에는 총 14개의 취약점 패치가 포함되어 있고, 그 중에서 LSASS 취약점은 4월말에 이 취약점에 대한 Exploit 이 발견되었고, 바로 연이어 이 공격코드를 이용한 아고봇 웜, 새서 웜이 등장하여 전세계적으로 많은 피해를 입혔다. 이렇듯 보안취약점이 발표된 후 채 한달도 되지 않아 이 취약점을 이용한 악성코드가 출현함으로써, 향후 보안취약점을 이용한 악성코드 제작주기가 점점 짧아질 것이라는 것을 예고하고 있다.

이번 테크니컬 컬럼에서는 4월 발표된 MS 보안취약점을 이용하여 전파되어, 전세계적으로 많은 피해를 입힌 새서 웜에 대해 살펴보았다.

I. 4월 악성코드 Top 10

작성자 : 정진성 연구원(jsjung@ahnlab.com)

악성코드명	건수	%
Win32/Netsky.worm.17424	1686	29.9%
Win32/Netsky.worm.25352	549	9.7%
Win32/Netsky.worm.22016	517	9.2%
Win32/Blaster.worm.6176	207	3.7%
Win32/Netsky.worm.22016.C	142	2.5%
Win32/Bagle	107	1.9%
Win32/AgoBot.worm.104960	98	1.7%
Win32/MyDoom.worm.32256	91	1.6%
Win32/Netsky.worm.16896.B	79	1.4%
Win32/Dumaru.worm.9234	56	1.0%
기타	2,101	37.3%
	5,633	100

[표1] 2004년 4월 악성코드 Top 10

4월 악성코드 피해 동향

4월은 올해의 다른 달과 달리 Top 10 에 많은 변화가 있었다. 그것은 지난달부터 현격히 건수가 줄어든 Win32/Dumaru.worm.9234 (이하 두마루 웜)의 변화와 Win32/Netsky.worm (이하 넷스카이 웜) 변형들의 활동이 꾸준히 증가하고 있기 때문이다.

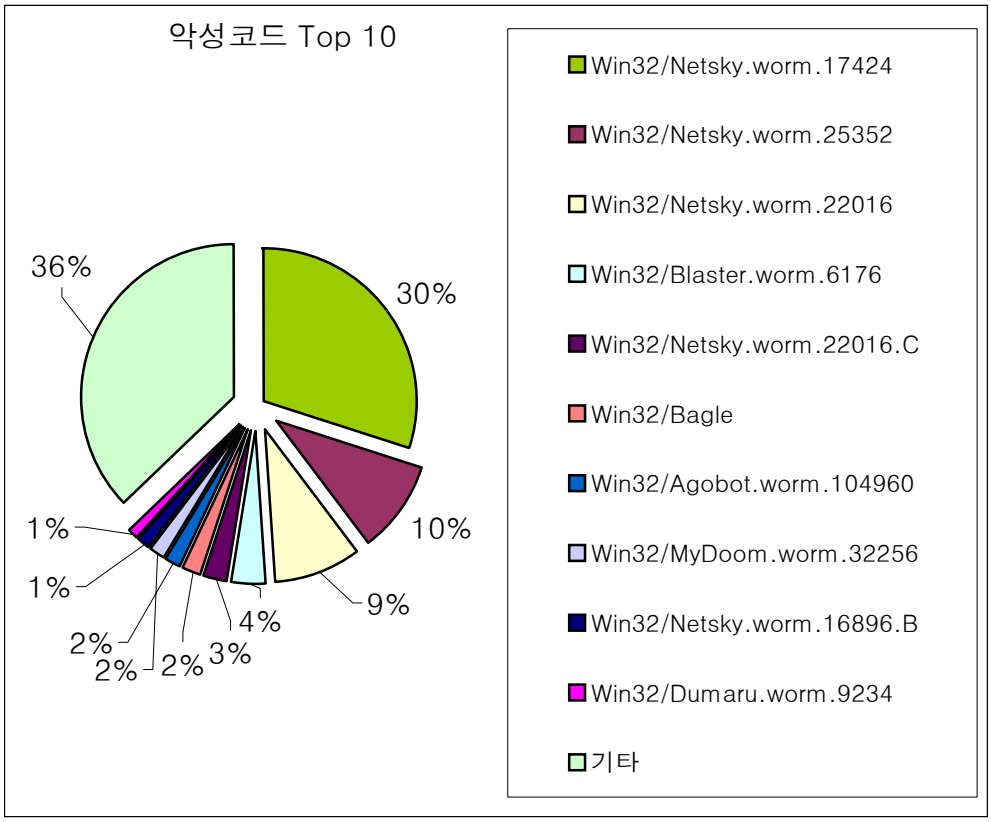
4월 Top 10 에는 넷스카이 웜의 변형들이 무려 5개나 차지하고 있다. 정보를 작성하는 현재 넷스카이 웜의 알려진 변형만 29개정도가 된다. 이는 넷스카이 웜이 처음 발견된 후 3개월 동안의 발견된 변형의 수치이며, 역대 Mass Mailer 중에서 악성코드 제작자 또는 그룹이 가장 단시간내에 많은 변형을 만든 웜이다. 짧은 기간동안 이렇게 많은 변형이 만들어진 이유는 Win32/Bagle.worm (이하 베이글 웜)과 경쟁적으로 제작되어졌기 때문이기도 하다.

이들이 개인 인지 혹은 그룹인지 알려지지는 않았으나 서로 경쟁적으로 변형을 만들어내면서 악성코드 제작에 새로운 기법들이 사용되어졌다. 예를 들면 취약점을 이용하여 첨부파일 없는 메일을 통한 감염[1]이라던가 웜 파일을 암호를 설정하여 압축한 후 암호는 별도의 텍스

[1] 취약점을 이용하여 메일을 읽는 것만으로도 웜이 실행되는 형태는 오래전에 알려졌지만 새

트나 이미지 형태로 보내는 방법, 또한 새로운 실행파일 형태로 웜을 구성하여 안티 바이러스 제품의 진단을 회피하는 등 여러가지 트릭이 사용되어 졌다.

3월의 악성코드 Top10을 도표로 나타내면 [그림1]과 같다.



[그림1] 2004년 4월 악성코드 Top 10

위에서 언급했듯이 두마루 웜에 대한 피해문의는 현저하게 급감하였다. 대신 넷스카이 웜 변형들이 5개나 포함되어 있고 이 결과는 곧 Top 10 피해문의의 50%에 이르는 결과를 가져왔다.

또한 두마루 웜처럼 그 피해문의가 급감하고 있는 웜은 이미 Top 10에서 사라진 Win32/Yaha.worm (이하 야하 웜)변형들을 들 수가 있다. 상위에 1개내지 2개가 꼭 포함되어 피해문의가 많았던 야하 웜은 지난 달 67건의 문의를 끝으로 Top 10에서 자취를 감추었다.

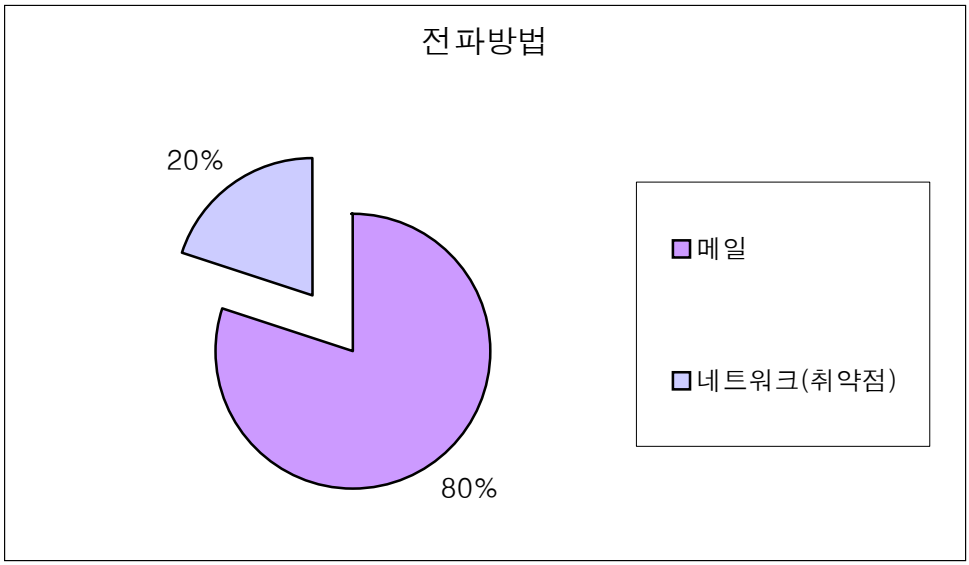
Win32/Blaster.worm.6176 (이하 블래스터 웜)의 문의가 항상 상위에 랭킹되어 있는 걸 보

로운 취약점(MS04-004)인 오브젝트 태그를 이용하여 광범위하게 피해를 준 첫 사례이다.

면 여전히 이 웜이 활동적이고 많은 시스템에 감염되었음을 알 수 있다. 이 웜은 2003년 8월 경에 처음 알려진 웜이다. RPC DCOM 이란 취약점을 이용하여 전파되는 이 웜에 대한 피해문의가 여전히 많다는 것은 아직도 많은 시스템들이 취약점에 대한 보안패치를 적용하지 않은 채 사용되고 있기 때문이라 보여진다.

4월 악성코드 Top 10의 전파방법 유형별 현황

[표1]의 악성코드 Top 10은 주로 어떠한 감염경로를 가지고 있는지 [그림2]에서 확인해 보기로 하자.



[그림2]악성코드 Top 10의 전파방법 유형별 현황

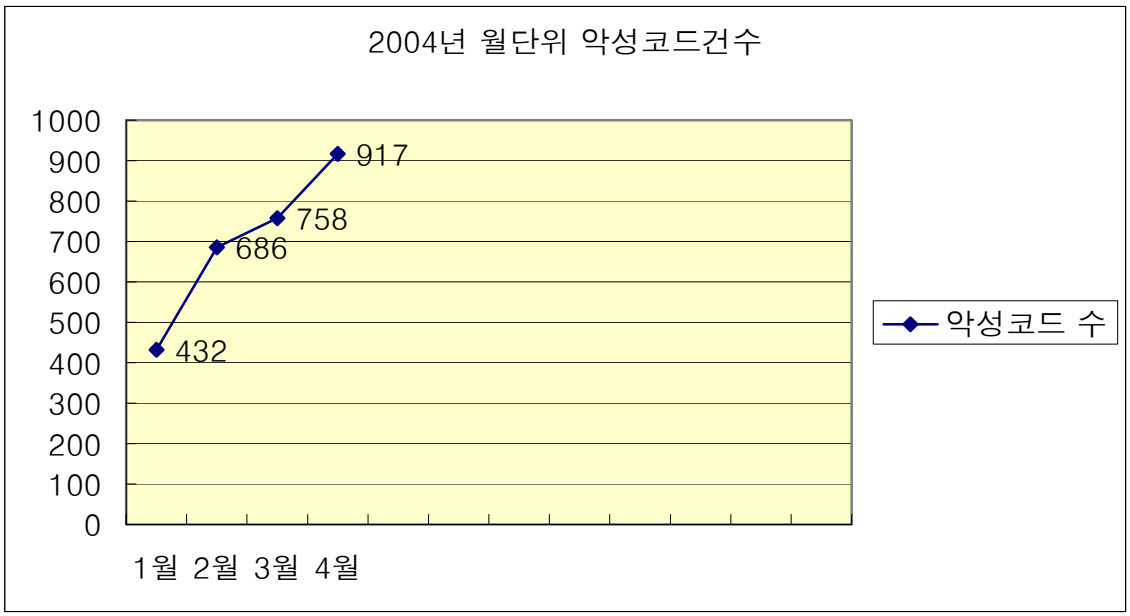
이번 달은 지난 달과 달리 네트워크로 전파되는 악성코드는 블래스터 웜과 Win32/AgoBot.worm.104960 (이하 아고봇 웜) 두가지이며, 전체의 20%에 불과하다. 네트워크 관련 악성코드가 줄어든 원인은 역시 Mass Mailer의 증가로 인한 것으로 파악된다. Top 10에서 절반 이상이 Mass Mailer인 것이 이를 잘 보여주고 있다.

4월 중순부터 다양한 넷스카이 웜 변형들에 대한 피해문의가 증가하기 시작했으며, 주로 다음과 같은 넷스카이 웜의 변형에 대한 문의가 집중하고 있다.

- Win32/Netsky.worm.17424
- Win32/Netsky.worm.25352
- Win32/Netsky.worm.22016
- Win32/Netsky.worm.22016.C

월별 피해신고 악성코드 수 현황

올해 들어서 문의되는 악성코드 종류의 수는 매월마다 기록를 경신하고 있다. 4월도 예외는 아니다. 이번달은 무려 917종에 이르는 엄청난 종류의 악성코드 문의가 있었다. 이 중 가장 문의가 많았던 것은 넷스카이 웜 변형이였다. 그리고 피해 문의가 많았던 악성코드 유형으로는 웜(Mass Mailer, Network)이 가장 많았다. 또한 악성 IRCBot (AgoBot, IRCBot)에 대한 피해문의도 무려 530 종류에 달했다.

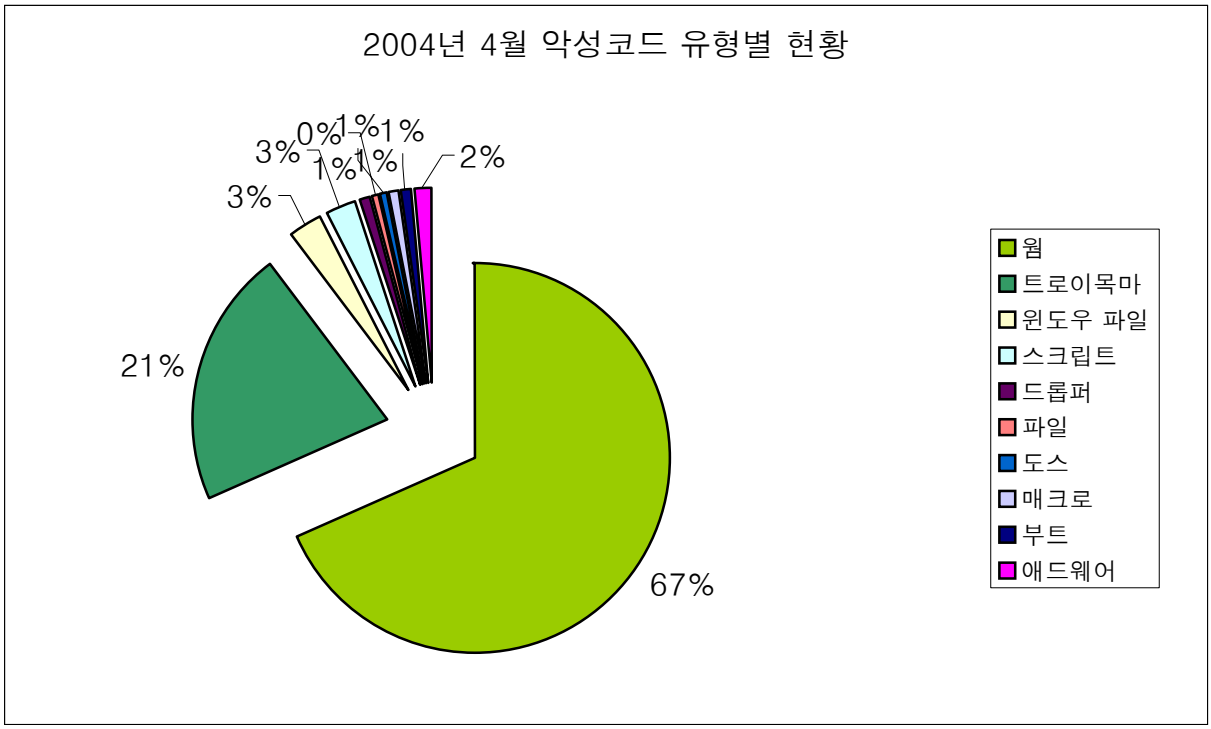


[그림3]2004년 월별 피해신고 악성코드수

지난달과 비교하여 160 종류가 증가하였으며 작년 동월 경우는 304 종류에 대한 문의가 있었을 뿐이다. 이는 300% 가량 악성코드의 종류가 증가한 것으로, 원인은 폭발적으로 늘어난 악성 IRCBot으로 인한 것이라 하겠다.

동년에 접수된 악성코드의 종류들은 주로 트로이목마 기반의 악성 IRCBot이였다. 참고로 이들은 지금의 웜 기반인 악성 IRCBot 형태가 아니여서 전파에 제한적이였으며 취약점을 이용하는 경우도 아니였기에 폭발적으로 증가하지는 못하였다.

917 종류에 이르는 다양한 악성코드들은 어떤 유형으로 분포되어 있는지 [그림4]를 통해서 확인할 수 있다.



[그림 4] 2004년 4월 악성코드 유형별 현황

웜이 압도적으로 많은 분포를 보이고 있다. 그 뒤를 이어서 트로이목마, 윈도우 파일순으로 다양한 유형의 악성코드들이 분포되어 있다. 스크립트 관련 문의는 베이글 웜 변형중에 일부가 생성하는 스크립트 기반의 파일들에 대한 피해로 문의가 많았다.

악성코드가 첨부된 메일은 사용자들에게 매우 위협적인 존재가 되었다. 이는 오늘날 뿐만이 아니라 악성코드가 메일이라는 전파수단을 이용하는 날까지 계속되어질 것이다. 메일이라는 악성코드의 전파경로는 악성코드 전파에 있어 매우 기본적인 수단이 되었다.

악성코드 제작자들이 이용하는 사회공학기법은 아주 그럴듯한 메일 내용으로 여전히 사용자들을 속이고 있다. 예를들어 넷스카이 웜 변형 중의 하나는 첨부된 파일이 마치 유명 안티바이러스 업체의 검사를 통과한 아무런 문제가 없는 파일인 것처럼 첨부된 파일이 이상이 없다는 그럴듯한 결과를 보여주고 있다. 많은 사용자들이 이러한 결과 내용을 쉽게 믿고 첨부된 파일을 실행하고 있는데, 메일에 첨부된 파일을 실행할 때는 취약점을 이용한 형태의 악성코드가 아니라면 한번쯤은 악성코드 유무를 의심해 보고 실행하는 습관을 갖는것도 누구나 기본적으로 알고 있는 예방법 중 하나이다.

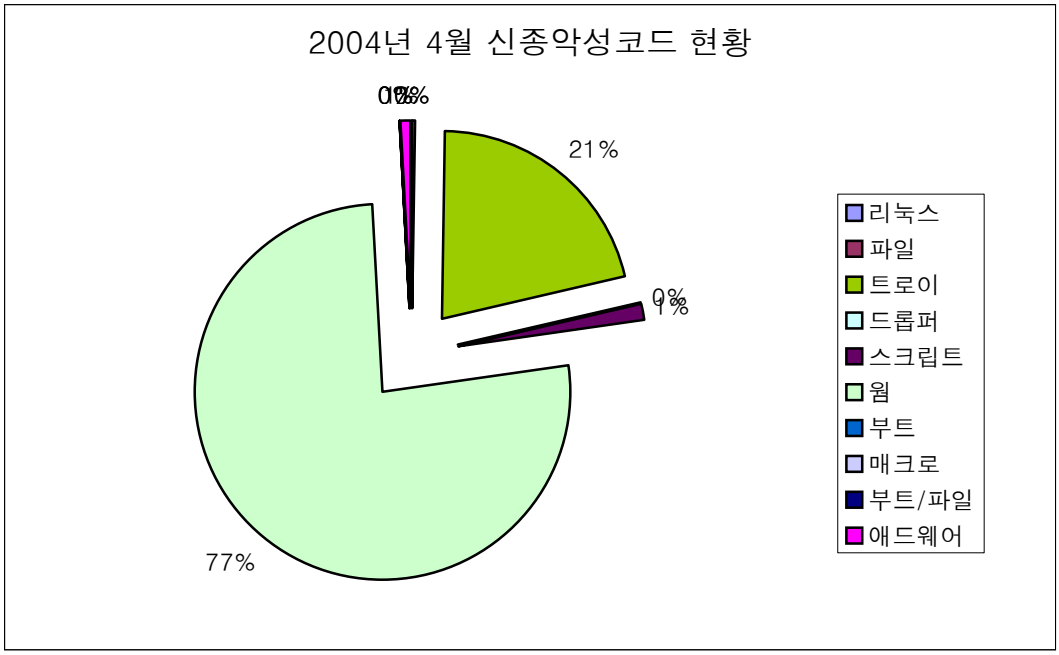
II. 4월 국내 신종 악성 코드 발견 동향

작성자 : 정진성 연구원 (jsjung@ahnlab.com)

4월 한달동안 접수된 신종 악성코드의 건수는 [표1], [그림1]과 같다.

리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	애드웨어	합계
0	1	111	0	7	401	0	0	0	4	524

[표1] 2004년 4월 유형별 신종 악성코드 발견현황



[그림1]2004년 3월 신종 악성코드 발견현황

4월 발견된 신종 악성코드 동향

4월은 무려 524 종류의 악성코드가 신고 접수되었다. 이는 하루에 17건꼴로 신종 또는 변종에 대한 접수가 이루어졌다는 뜻이다. 올해 들어 신종 또는 변종에 대한 악성코드의 수가 폭발적으로 증가하고 있지만 524 종류는 통계상 가장 많은 수이다.

접수된 대부분은 Win32/AgoBot.worm (이하 아고봇 웜)과 같은 악성 IRCBot 기반의 악성코드들이 대부분을 차지하고 있다. 특히 아고봇 웜이 다른 악성 IRCBot 기반의 악성코드보다 문제가 되는 원인은 다양한 취약점을 이용했다는 것이고 많은 제작자들이 Private한 변형을 만들어 낸다는 점이다. 이러한 Private 버전으로 인하여 새로운 취약점이 곧바로 응용되기도

하고, 은폐기법이라던가 다형성 기법이 추가되고 있다. 이렇게 추가된 제작기법들은 IRC 상에서 다른 제작들이 이를 다운받아 자신만의 버전으로 변형후 유포하는 식이 반복되어져 수많은 변형이 제작되어 지고 있다.

아고봇 웜이 이용하는 보안 취약점

다양한 취약점과 관리목적 공유폴더의 사용자 로그인 계정을 유추하여 전파되는 아고봇 웜이 사용하는 취약점에 대해 간략히 알아보도록 하자. 아고봇 웜은 무려 10가지가 넘은 다양한 취약점을 이용하고 있다.

(1) Win32/Bagle.worm -> TCP/2745
베이글 웜에 감염된 경우 오픈된 TCP/2745 를 이용한다.
* 해결방법
안티 바이러스 제품으로 베이글 웜을 치료해야 한다.

(2)RPC DCOM2 vulnerability : (MS03-039) -> TCP/135
관련 보안패치를 적용해 주어야 한다.
* 패치정보
http://www.microsoft.com/korea/technet/security/bulletin/MS03-039.asp (한글)
http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx (영문)

(3)RPC DCOM vulnerability : (MS03-026) -> TCP/135 , 445 , 1025
관련 보안패치를 적용해 주어야 한다.
* 패치정보
http://www.microsoft.com/korea/technet/security/bulletin/MS03-026.asp (한글)
http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx (영문)

4. Win32/MyDoom.worm -> TCP/3127
마이둠 웜에 감염된 경우 오픈된 TCP/3127를 이용한다.
* 해결방법
안티 바이러스 제품으로 마이둠 웜을 치료해야 한다.

5. DameWare Mini Remote Control Server Overflow vulnerability -> TCP/6129 -> DameWare 라는 원격제어 툴의 취약점
3.72.00 버전에서만 취약점이 존재하므로 4.x 로 업데이트 하면 된다.

6. RPC Locator vulnerability : (MS03-001) TCP/445

관련 보안패치를 적용해 주어야 한다.

* 패치정보

http://www.microsoft.com/korea/technet/security/bulletin/MS03-001.asp (한글)

http://www.microsoft.com/technet/security/bulletin/MS03-001.mspx (영문)

7. NetBios -> 관리목적공유폴더 대상, -> TCP/139, 445

* 예방법

암호를 반드시 설정하거나 설정한 암호는 유추하기 힘든 것이어야 한다. 또한 불필요하게 관리자 권한을 다른 유저에게 설정하지 않도록 한다.

8. MS-SQL : Elevation of Privilege in SQL Server Web Tasks vulnerability -> TCP/1433 -> (MS02-061)

관련 보안패치를 적용해 주어야 한다.

* 패치정보

http://www.microsoft.com/korea/technet/security/bulletin/MS02-061.asp (한글)

http://www.microsoft.com/technet/security/bulletin/MS02-061.mspx (영문)

9. WebDav vulnerability : (MS03-007) -> TCP/80

관련 보안패치를 적용해 주어야 한다.

* 패치정보

http://www.microsoft.com/korea/technet/security/bulletin/MS03-007.asp (한글)

http://www.microsoft.com/technet/security/bulletin/MS03-007.mspx (영문)

10. Workstation service buffer overrun vulnerability : TCP/139 (MS03-049)

관련 보안패치를 적용해 주어야 한다.

* 패치정보

http://www.microsoft.com/korea/technet/security/bulletin/MS03-049.asp (한글)

http://www.microsoft.com/technet/security/bulletin/MS03-049.mspx (영문)

11. UPnP vulnerability : TCP/5000 -> (MS01-059)

이 취약점은 윈도우 2000 계열에서는 영향을 주지 않으며 윈도우 9x 와 XP에서만 영향을 준다고 알려졌다. 관련 보안패치를 적용해 주어야 한다.

* 패치정보

http://www.microsoft.com/korea/technet/security/bulletin/MS01-059.asp (한글)

http://www.microsoft.com/technet/security/bulletin/MS01-059.mspx (영문)

12. MS03-043 -> Messenger Service Buffer Overrun Vulnerability

관련 보안패치를 적용해 주어야 한다.
* 패치정보
http://www.microsoft.com/korea/technet/security/bulletin/MS03-043.asp (한글)
http://www.microsoft.com/technet/security/bulletin/MS03-043.mspx (영문)

13. LSASS BufferOver flow Exploit -> (MS04-011) -> TCP/135, 445, 1025
관련 보안패치를 적용해 주어야 한다.
* 패치정보
http://www.microsoft.com/korea/technet/security/bulletin/MS04-011.asp (한글)
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx (영문)

위와 같이 최근 발견되는 아고봇 웜은 다양한 보안 취약점을 이용하여 자신을 전파시키는 것을 알 수가 있었다. 따라서 보안 취약점에 대한 패치를 소홀히 해서는 안되는 것을 다시 한번 명심하여야 한다.

경쟁적으로 제작된 베이글 웜과 넷스카이 웜의 변종

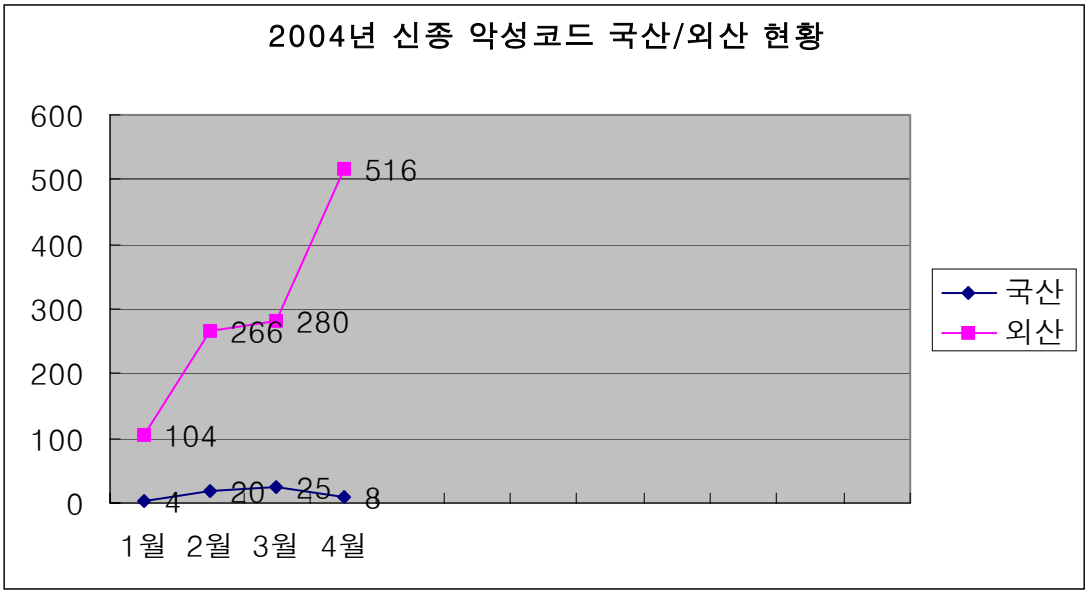
베이글 웜과 넷스카이 웜이 서로 경쟁적으로 변종을 계속 만들어 이 또한 피해가 많았다. 이들은 변종에 부여하는 알파벳 26자를 넘길 만큼 많은 변종이 나왔다. 특히 베이글 웜 변종 중 하나는 한 가지 웜을 파일의 형태를 바꾸어 *.CPL, *.VBS, *.HTA 확장자로 웜 복사본을 생성한다. 이 확장자는 무늬만 확장자가 아니라 실제 CPL Stub 헤더를 가진 *.EXE 형태의 실행파일과 VBScript 를 가진 *.VBS, *.HTA 확장자들이였다. 이 스크립트 기반의 파일들은 내부에 웜의 바이너리 코드를 가지고 있어, 실행시 바이너리의 파일로 재구성하여 웜을 실행하도록 되어 있었다. 또한 CPL 형식의 파일은 두개의 실행파일 구조로 되어 있어 앞 부분은 CPL 형식의 확장자임을 표시하고 실행해주는 파일과 뒤에는 실제 웜코드가 있었다. 이러한 형태는 안티 바이러스 제품의 진단방법을 회피하는 방법으로 사용되었다.

러브게이트 웜 변형의 지속적인 발견

이외에도 Win32/LovGate.worm (이하 러브게이트 웜)도 계속 변형이 만들어지고 있음을 알 수가 있다. 지난 3월에 소개된 변형에 대한 내용과 더불어 계속적으로 제작기법의 향상을 보여주고 있다. 최근에 알려진 러브게이트 웜 변형은 *.EXE 파일을 *.ZMX 로 변경하고 웜 자신을 해당 *.EXE 인 것처럼 속이는 증상이 있었다. 대부분의 안티 바이러스 제품들이 파일을 삭제하거나 파일내 일정부분을 수정하는 일만 가능했었는데 이러한 형태가 출현하면서 안티 바이러스 제품에는 파일의 이름도 변경하는 기능이 추가 되어야만 했었다. 또한 러브게이트 웜은 자신의 Drop한 백도어 모듈을 RemoteThread 로 실행하여 특정 윈도우 시스템 프로세스에 Inject시키고 이를 은폐하는 증상도 있어 사용자가 이를 확인하고 치료하기 어려운 형태를 보였다.

제작지별 신종 악성코드 현황

다음은 신종 악성코드들의 국산/외산의 현황을 보여주고 있다. 외산 악성코드가 대폭 상승한 것을 볼 수 있다.



[그림2] 2004년 제작지별 신종 악성코드 현황

외산 악성코드의 폭발적인 증가원인은 악성 IRCBot에 의한 현상이다. 국산 악성코드들은 주로 약간의 트로이목마 형태와 사용자 동의 없이 홈페이지 초기 페이지를 수정하는 애드웨어 형태가 발견되었다.

LSASS 보안 취약점 문제 사례

4월말 국내에 많이 보고된 현상 중 하나가 LSASS.EXE의 오류로 시스템이 재부팅 되는 현상이다. 원인을 찾던중 이러한 현상이 LSASS 보안 취약점(MS04-011)을 이용한 공격 때문이라는 것을 알게 되었다. 이 취약점은 4월 13일 발표된 취약점으로, 이를 공격할 수 있는 Exploit 코드는 4월말경 발견되었다. 이 중 첫번째 발견된 Exploit 코드가 요즘 문제시되는 아고봇 웜에 사용되어 졌다. Exploit 코드는 특정한 OS 버전에서만 정상적으로 버퍼 오퍼플로우을 일으키고 그외 OS 에서는 위와 같은 LSASS의 오류를 발생시켜서 많은 사용자들로부터 이유없이 재부팅된다는 문의가 접수되었다.

안철수연구소는 이에 대하여 'V3 FirstBlock'라는 전용 차단 및 탐지툴을 만들어 공개 및 배포하였다. 이러한 상황을 보듯 악성코드가 취약점을 이용하는 그 주기는 점점 짧아지고 있음을 알 수가 있다. 항상 취약점을 이용한 악성코드가 출현 하였을 때 근본적인 예방은 바로

취약점에 대한 보안패치를 실시하는 것이다. 단지 자신의 시스템을 악성코드로부터 지킨다는 생각 뿐 아니라 나로 하여금 다른 사람에게 피해를 주지 것을 예방하겠다는 생각을 가지고 패치 작업이 이루어진다면 좀더 사용하기 쾌적한 인터넷 환경이 되지 않을까 생각해본다.

III. 4월 신규 보안 취약점

작성자 : 조경원 연구원(dubhe@ahnlab.com)

4월의 최대 보안 이슈는 MS04-011로 발표된 마이크로소프트사의 윈도우 제품군에 관한 취약점이다. 이 MS04-011패치에는 총 14개의 취약점 패치가 들어 있으며 이중 LSASS 취약점과 PCT 취약점에 대한 공격코드가 발표되었다. 특히 LSASS 취약점의 경우 Sasser웜 (이하 새서 웜)을 통해 전세계에 이슈가 되었다.
기타 특이한 이슈로 TCP RST 공격(BGP Protocol 공격)에 대한 이슈가 있었다.

LSASS 취약점

4월 정기 패치중 하나인 MS04-011에 포함되어 있으며 eEye Digital Security에서 발표한 마이크로소프트 윈도우에서 발생하는 취약점이다. 5월 1일(외국시각 4월 30일) 발생한 새서 웜이 사용한 취약점으로, 새서 웜 이전에 4월 29일경부터 Agobot류에서도 사용된 취약점이다. 해당 취약점 공격코드는 4월 24일경 외국에 최초로 공개되었으며 취약점 발견이후 한달이 채 되지 않은 시점에서 악성코드로 발전되어 전세계 많은 피해를 준 사례이다.

LSASS(Local Security Authority Subsystem Service)는 NT기반의 윈도우 시스템에서 로컬 보안 및 도메인, Active Directory 관리에 관련된 서비스로 특정 RPC 요청에 대하여 버퍼 크기를 체크하지 않아 발생하는 버퍼 오버플로우 취약점이 존재한다. LSASS서비스는 135, 139, 445, 593, 1025/tcp를 통해 접근할 수 있으며 윈도우 2000, XP 에서 취약점이 발생한다. 윈도우 2003과 64bit XP의 경우 취약점이 존재하지만 원격(remote)에서 취약점을 공격할 수는 없다. 취약점은 LSASS에서 사용되는 로그파일 중 하나를 기록하는 부분에서 버퍼 오버플로우가 일어나는 것으로써 해당 로그파일을 읽기전용(Read-Only)로 변경할 경우 취약점을 제거할 수 있으나 취약점 자체를 근본적으로 제거하기 위해서는 MS04-011 패치를 적용하는 것이 바람직하다. 또한 향후 발생할 수 있는 보안 취약점과 보안 정책 강화를 위하여 NetBIOS관련 포트(137,138,139,445/udp, 135,139,445,593,1025/tcp)는 외부와 인가되지 않은 네트워크에서는 접근하지 못하도록 하는 것이 권장된다.

새서 웜의 활동으로 많은 시스템이 리부팅되는 문제가 발생하였는데 그 원인은 윈도우 시스템은 중요 서비스가 Crash 될 경우 자동적으로 시스템을 리부팅하는 기능이 포함되어 있다. LSASS 서비스는 윈도우에서 인증을 관리하는 중요 서비스로 LSASS 서비스(lsass.exe)가 Crash될 경우 윈도우는 자동으로 리부팅하게 되며 새서 웜에서 사용된 공격코드가 공격을 실패하였을 때 발생하는 증상이다. 특히 한국어 버전의 윈도우는 영문 윈도우와 공격코드가 호환이 되지 않는 경우가 많기 때문에 리부팅의 문제는 미영어권의 국가에서 더욱더 심했을

것으로 생각된다.

PCT 취약점

역시 4월 정기 패치중 하나인 MS04-011에 포함된 취약점으로 ISS(Internet Security Systems)에서 발표하였다.

PCT(Private Communications Transport)프로토콜은 마이크로소프트의 SSL(Secure Sockets Layer)라이브러리에 포함된 보안관련 프로토콜이다. IIS에서 PCT를 지원하는 SSL 서비스를 사용할 경우 버퍼 오버플로우 취약점이 발생할 수 있다. PCT프로토콜은 IIS 4.0, 5.0, 5.1, 5.5, Microsoft Exchange Server 2000, 2003, Microsoft Analysis Services 2000에서 PCT가 사용되며 윈도우 서버 2003과 IIS 6.0은 기본적으로 PCT가 비활성화 되어 있다. SSL서비스를 사용할 때만 취약점이 발생하며 기본적으로 SSL서비스는 비활성화 되어 있다. PCT취약점의 공격코드는 4월 24일경 발견되었으며 아직 악성코드에서의 직접적인 사용은 알려져 있지 않다. 공격 대상이 IIS, Exchange등의 서버용 어플리케이션이기 때문에 일반 PC 사용자보다는 서버급에 대한 해킹 공격으로 악용될 가능성이 높다.

TCP RST 공격

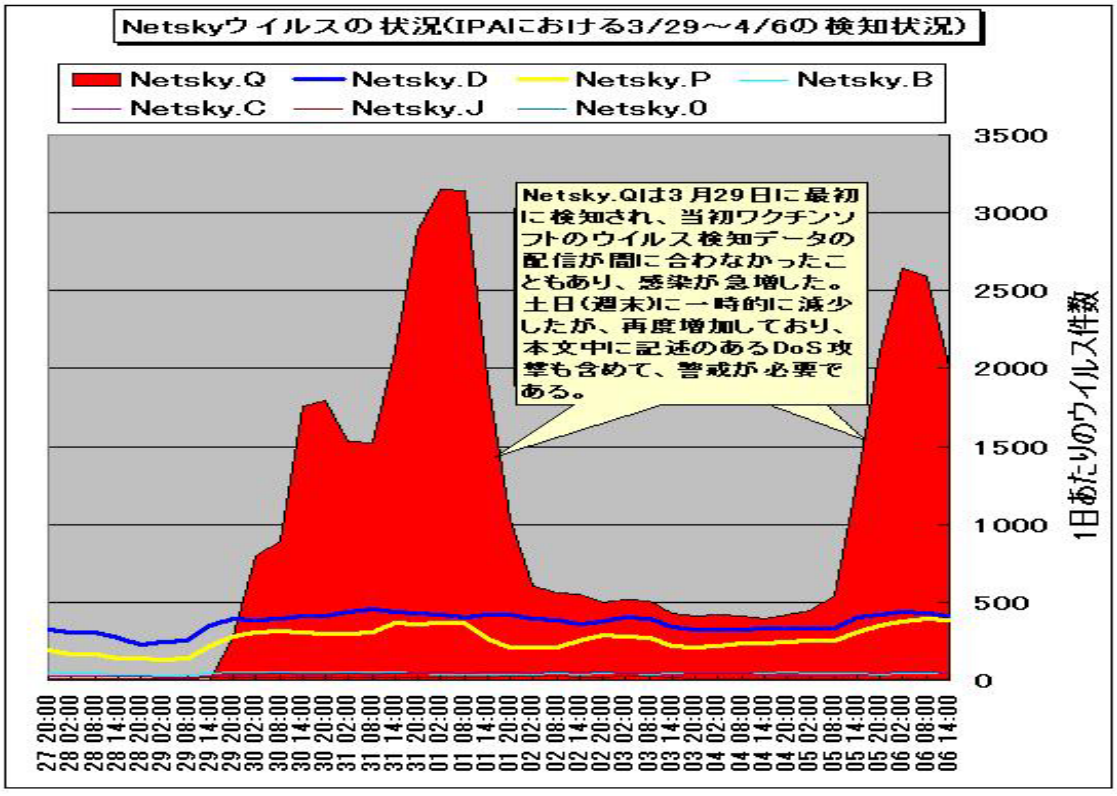
TCP 프로토콜은 RST(Reset) Flag를 세팅한 패킷을 보낼경우 해당 TCP 세션은 끊어지도록 설계되어 있다. 이때 SEQ(Sequence) Number를 맞추어야 실제 세션을 끊게 되며 SEQ Number가 다를 경우는 무시하게 된다. SEQ Number를 맞추기만 한다면 어떠한 TCP 세션이던지 끊을 수 있기 때문에 이에 대한 이슈는 오래전부터 알려져 있었으나 이론상 SEQ Number를 추측하기란 매우 힘들기 때문에 이론상으로만 가능하다고 알려져 있었다. 최근 이 SEQ Number가 정확히 해당 세션의 SEQ Number가 아닌 윈도우Size와 결합하여 윈도우 Size내의 SEQ Number일 경우 RST가 허용된다는 결과가 알려졌다. 이는 TCP RST Kill기법을 보다 쉽게 할 수 있는 기법이며 이를 사용하는 공격 툴이 알려지게 되었다. TCP 세션을 끊을 경우 직접적으로 일반적인 TCP 연결상에서는 큰 장애가 발생하는 것은 아니지만 큰규모의 인트라넷에서 DB간의 연결, 2 Teer, 3 Teer 환경의 서버 운영 환경에서 세션 Kill은 서비스 장애를 줄 수 있으므로 매우 심각한 결과를 줄 수 있다. 또한 매뉴얼한 해킹 공격에서도 악용될 여지가 매우 많다. 라우터간의 라우팅테이블 교환을 위한 BGP 프로토콜의 경우 특히 이 취약점에 매우 크게 노출 될 수 있으며 BGP 프로토콜이 공격 당할 경우 네트워크가 마비되거나 교란되는 큰 장애를 불러 올 수 있다. 이 공격은 자동화되어 인터넷 웜이나 악성코드안에 탑제되기에는 공격 구조와 환경상 적합하지 않으므로 수동적인 해킹 공격 등에서 사용될 가능성이 높다.

Ⅳ. 4월 일본 피해 동향

작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

W32/Netsky.Q 급속 확산

2004년 4월 한달동안 일본에서 가장 이슈가 되었던 악성코드는 W32/Netsky.Q (Win32/Netsky.worm.28008, 이하 넷스카이.Q)이다. 넷스카이.Q는 2004년 3월 29일 최초로 발견된 넷스카이 웜의 여러 변형 중 하나로, 윈도우 OS의 보안취약점을 이용하여 첨부된 파일이 자동으로 실행되어 사용자의 PC를 감염시키는 Mass Mailer이다.
아래의 도표는 넷스카이.Q가 최초 발견된 후 감염되는 정도를 넷스카이 웜의 다른 변형들과 비교하여 도식화한 것으로써 일본에서 넷스카이.Q의 확산 정도를 짐작할 수 있게 해준다.

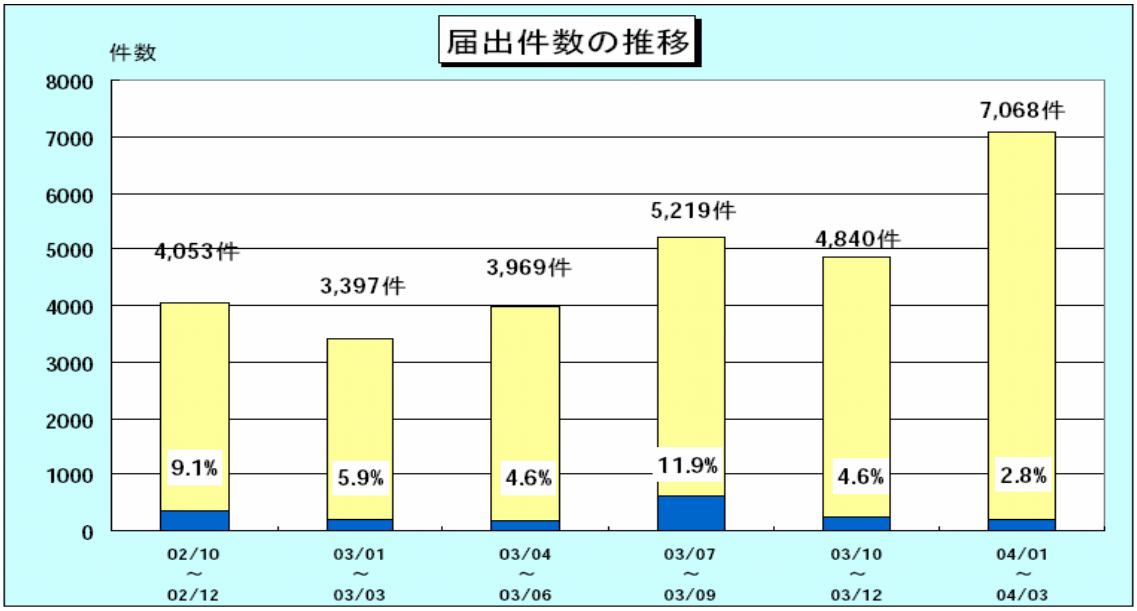


(자료출처 : 일본 IPA)

Mass Mailer로 인한 악성코드 노출 빈도 증가

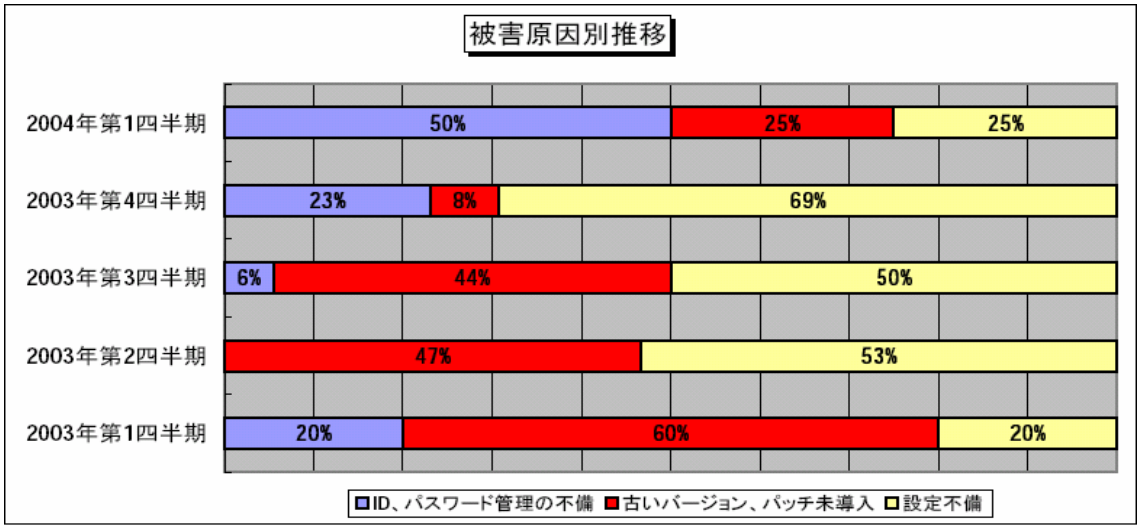
일본에서는 2004년 1/4분기의 기간 동안 다른 시기와 비교해서 악성코드에 노출 신고 건수가 급격히 증가하였다. 이러한 악성코드의 피해가 급격하게 늘어난 주요 원인은 넷스카이 웜과 베이글 웜 등 이메일을 통해 전파되는 악성코드들의 여러 변형들이 발생하였고 그 중의 일부가 널리 확산되었기 때문이다. 아래의 도표는 분기별 악성코드 노출 건수를 그래프로 나

타낸 것으로써 다른 분기에 비해 2004년 1/4분기의 악성코드 노출 건수가 두배에 가까운 증가수치를 보여주는 것을 알 수 있다. 그러나 실제로 감염된 경우는 2.8%에 불과한 것으로 보아 감염으로 인한 피해가 심각하지는 않은 상태임을 짐작해볼 수 있다.



Security 관련 사고의 원인은 패스워드 관리 부족

IPA에서 발표한 Security 관련 1/4분기 통계자료 중 주목할 만한 사항중의 하나는 최근 발생하는 보안 사고 발생원인의 대부분을 차지하고 있는 것이 시스템의 패스워드 관리 소홀로 인한 것이라는 점이다. 아래의 도표는 Security 관련 사고의 피해 원인별 추이를 분기별로 비교한 것이다. 아래의 도표에서도 볼 수 있는 것처럼 패스워드 관리 부재로 인한 피해 발생 빈도는 2003년 상반기와 비교해서 월등히 증가하고 있다. 최근 유행하는 웜과 같은 악성코드들이 윈도우 로그인 계정의 패스워드 취약점을 이용하여 전파되는 경우가 많다. 따라서, 패스워드 관리는 시스템 관리자는 물론이고 일반 사용자에게도 시스템을 안정적으로 유지하기 위한 중요한 요소가 되어가고 있다.



장기 휴가에 대비한 보안 대책 마련 권고

JP-CERT는 4월 말부터 시작된 황금연휴 기간 중 발생할 수 있는 보안 사고를 예방하기 위하여 아래와 같이 실천 지침을 발표하였다.

- 최신 보안패치가 적용되어 있는가
- 불필요한 서비스가 정지되어 있는가
- 각종 서비스의 접근제어가 적절히 설치되어 있는가
- 휴가중 사용하지 않는 기기의 전원을 끄는 순서를 정확히 알고 있는가

올해 일본의 황금연휴는 4월28일 부터 5월5일까지 1주일에 이르는 기간이고 이 기간 동안은 모든 경제활동이 중단된다.

V. 4월 중국 피해 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

악성코드 TOP 5

3월까지의 중국 악성코드 동향은 연초부터 이어진 Mass Mailer들이 주축을 이루고 있었다고 해도 과언이 아니었다. 그러나 4월에는 새로운 악성코드들이 새롭게 순위를 차지하고 있으며 기존의 Mass Mailer들은 조금씩 하향세를 보이고 있다. 이러한 흐름은 기존 악성코드가 주로 메일을 통해 감염되었던 것에 반해 윈도우 취약점을 이용하여 네트워크를 통해 감염되는 것으로 서서히 변화가 이루어지고 있기 때문이라고 할 수 있다. 그러나 이러한 변화가 보인다고 하여 기존의 Mass Mailer들의 절대적인 영향력이 줄어 들었다고 보기는 힘들다. 그 이유는 아래 중국의 4월 악성코드 TOP 5를 보면 잘 나타난다.

순위 변화	4 월	Rising	CNCVERC
*	1	Worm.Netsky	Worm_Nesky
NEW	2	Worm.Lovgate	Worn_MyDoom
NEW	3	Worm.Agobot.3	Worm_AgoBot
- 2	4	Worm.Novarg	Worm_Bagle
NEW	5	Trojan.QQMSG.Boker	-

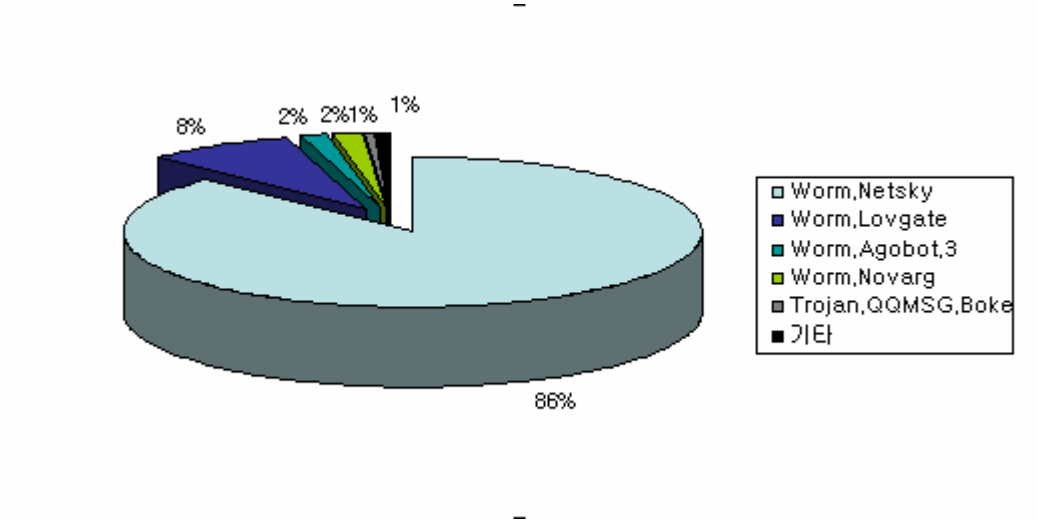
[표1] 중국의 2004년 4월 악성코드 TOP 5

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

위 [표1]은 중국 백신업체인 라이징(Rising)사와 정부연구기관인 중국국가컴퓨터바이러스대응중심(China National Computer Virus Emergency Response Center, 이하 CNCVERC)이 작성한 4월 중국 악성코드 TOP 5이다. 위에서 상술한 이러한 흐름의 변화가 조금씩 이루어지고 있는 것이 위 표를 통해서 잘 나타나고 있다. 1위에는 3월달에 이어서 Worm.Netsky(Win32/Netsky.worm, 이하 넷스카이 웜)가 1위를 차지하고 있다. 넷스카이 웜은 본 보고서가 작성되는 5월 초 현재까지도 지속적으로 변형이 등장하고 있으며 변형의 기능이나 형태가 더욱더 지능적으로 변화되고 있어 백신 개발자와 분석자들이 많은 어려움을 겪고 있다. 2위와 3위에 랭크된 웜은 4월에 새롭게 등장한 악성코드이나 이미 다양한 기능과 많은 변형으로 인해 익히 알려진 Worm.Lovgate(Win32/Lovgae.worm, 이하 러브게이트 웜)과 Worm.Agobot.3(Win32/AgoBot.worm, 이하 아고봇 웜)이 차지하고 있다. 특히 아고봇 웜은 다양한 전파경로 중에서 4월말 마이크로소프트에서 발표한 MS04-011 취약점을 이용하는 새로운 변형도 발견되었다. 이로 인해 윈도우 보안 패치의 중요성과 윈도우 시스템

관리의 문제를 사용자들에게 다시 한번 인식시키고 있다. 그 뒤를 이은 4위는 3월보다 2계단 하락하여 영향력이 많은 줄어든 것으로 보이는 Worm.Novarg(Win32/MyDoom.worm, 이하 마이둠 웜)이 차지하고 있다. 마이둠 웜의 순위 하락은 확산이 많이 줄어든 것으로도 볼 수 있지만 다양한 Mass Mailer들의 확산으로 인해 사용자들 역시 수상한 메일을 함부로 열어보거나 첨부된 파일들을 함부로 실행하지 않는 등 보안에 대한 인식이 많이 향상된 것도 중요한 작용이 아니었나 추측이 된다. 5위에는 그 감염율은 그리 높지 않지만 지난 해 말부터 꾸준히 등장한 QQ 메신저를 이용한 트로이목마인 Trojan.QQMSG.Boker가 차지하고 있다. 2004년으로 해가 바뀌면서 새로운 QQ 트로이목마 변형의 등장이 많이 줄어드는 것으로 보였다.. 그러나 다시 새로운 변형이 등장하는 것으로 미루어 신고되지 않은 QQ 트로이목마는 더 있을 것으로 추정되며 중국 내에서도 해당 악성코드가 꾸준히 제작되고 있는 것으로 추정된다.

악성코드 분포



[표2] 중국의 2004년 4월 악성코드 분포

위 악성코드 분포를 참고할 경우 [표1]에서 보여준 순위를 그대로 반영하고 있으나 악성코드 분포를 통해서 새로운 변화가 나타나고 있다는 것을 알 수 있다. 특히 글 문두에서 기술한 것과 같이 Mass Mailer의 영향력이 점점 줄어들고 네트워크로 전파되는 악성코드가 늘어나는 추세인 것으로 파악된다. 그러나 네트워크 웜의 영향력이 급격하게 늘어난 것은 아니며 아직까지는 신고된 악성코드의 절대다수가 넷스카이 웜에 의한 것을 [표2]를 통해서 알 수 있다. 감염경로에 따른 변화의 조짐이 있다는 것은 새롭게 신고되는 네트워크 웜의 종류가 늘어나고 Mass Mailer는 그 종류가 줄어들고 있다는 점이다. 특히 이번 달에 새롭게 순위에 올라온 러브게이트 웜이 전체 비율에서 8%나 차지하고 있다는 점과 지난 3월 악성코드 분포에서 기타에 포함될 정도로 그 영향이 미약한 아고봇 웜이 2%로 증가했다는 점은 다음과 같은 사항들을 반영하고 있는 것이라 여겨진다. 그것은 중국 사용자들의 시스템이 네트워크

로 전파되는 웜에 취약한 부분이 많다는 점과 사용하고 있는 시스템이 윈도우 98을 벗어나 윈도우 2000 또는 윈도우 XP 계열을 많이 사용하고 있다는 것을 반영하고 있다는 것이다. 이러한 변화가 운영체제에 상관없던 Mass Mailer와는 달리 관리목적 공유폴더의 비밀번호 취약점, 윈도우 보안 패치 미적용에 따른 문제들로 인해 네트워크로 전파되는 다양한 웜에 의한 피해가 언제든지 폭발적으로 늘어날 수도 있다는 점을 보여주고 있다.
그 외 기타에 포함된 악성코드에는 TrojanClick.book, Worm.BBeagle(Win32/Bagle.worm), Worm.Mimail(Win32/Mimail.worm), Worm.Lentin(Win32/Yaha.worm)이 포함되어 있다. 이 중에서 4월 셋째주에 새롭게 발견된 TrojanClick.book는 QQ 메신저를 이용해 전파되는 트로이목마와 유사하게 특정 웹 사이트를 접속하게 될 경우 시스템에 설치가 된다. 그리고 인터넷 익스플로어의 메인 페이지가 특정 웹 사이트로 고정되는 증상이 발생한다.

결론

중국의 악성코드 동향은 3월에 이어서 Mass Mailer가 강세를 보이는 현상이 유지되고 있다. 하지만 전체적인 흐름으로 미루어볼 때 네트워크로 전파되는 웜들의 감염신고가 조금씩 증가하고 있어 5월달에는 그 영향력이 4월과 비교하여 더 커질 것으로 예측된다. 그러나 이러한 현상이 한국 등 국가 네트워크 인프라가 잘 구축된 국가에서는 벌써 사회적인 이슈가 될 만큼 심각한 현상으로 대두되었다는 점으로 미루어 중국에서도 5월과 6월에는 이러한 현상이 크게 증가하리라 보인다. 그리고 5월 초에 등장하여 마이크로소프트의 MS04-011 취약점을 이용하여 전파되는 Win32/Sasser.worm이 한국과 기타 국가에서처럼 중국에서 얼마나 큰 파장 일으켰는지도 큰 관심거리가 된다.

VI. 테크니컬 컬럼 – 블래스터 웜의 부활? 새서 웜

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

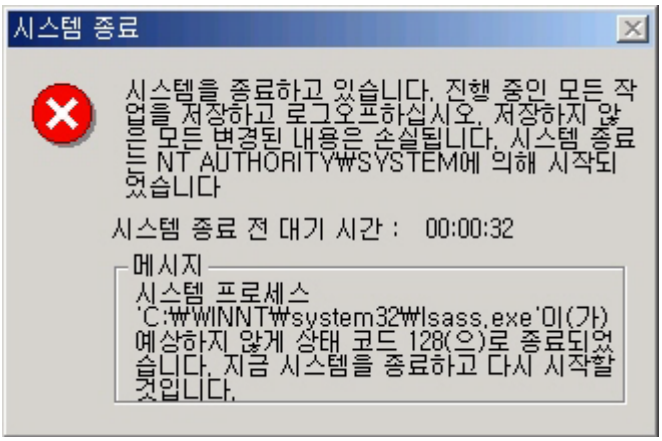
2003년 여름 우리는 윈도우의 취약점을 이용하여 전파되며 시스템을 종료시키는 부작용을 가지고 있는 블래스터 웜을 경험했다. 당시 윈도우 업데이트의 중요성이 크게 강조되었다. 반년이 지난 2004년 5월 1일, 전파 방법과 증상에서 유사한 새서 웜이 등장했다. 반년 동안 무엇이 변했을까?

MS04-011 취약점

2004년 4월 14일 마이크로소프트사는 새로운 보안 업데이트를 발표했다.
여기에 LSASS 취약점이 포함되어 있었고 이 취약점을 이용해 원격에서 코드를 실행 할 수 있었다. 보안 업데이트 발표 후 몇 가지 익스플로잇(exploit)이 발표되었고 웜에서 사용될 수 있을 거라 예상되었다. 2003년 여름 발생한 블래스터 웜(Win32/Blaster.worm.6176)과 같은 사태가 발생할 가능성이 우려되었다.

악성코드 등장

취약점 공격 익스플로잇이 발표된 며칠 후 2004년 4월 26일 모 대학에서 갑자기 에러가 발생하면서 시스템이 종료된다는 문의가 접수되었다. 이에 LSASS 취약점을 이용한 공격을 예상할 수 있었고 해킹이나 웜 등의 공격으로 추정했다.



[그림1] 잘못된 LSASS 취약점 공격 패킷을 받을 때 발생할 수 있는 오류 창

아고봇 최신 버전이 MS04-011 취약점을 이용한다는 소문이 돌았고 Win32/AgoBot.worm.138752.B에서 MS04-011 취약점을 이용하는 것이 확인되었다. 이후 새롭게 등장하는 아고봇 변형 상당수가 MS04-011 취약점을 이용했다.

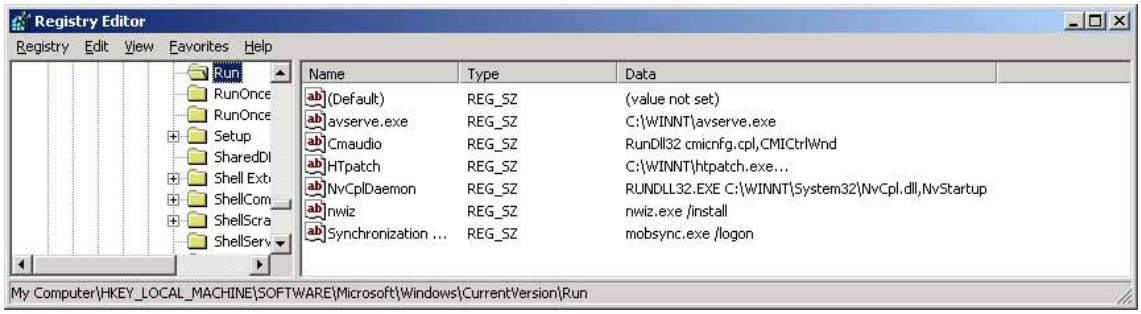
사서, 사세르, 새서

2004년 5월 1일(외국 시간 4월 30일) 발견된 새서 웜(Win32/Sasser.worm.15872) 은 외국에서 발견 후 곧 한국에서도 발견되었다.

새서 웜에 감염되면 윈도우 폴더에 avserve.exe 파일이 만들어진다.

[그림2] 새서 웜 감염 시 윈도우 폴더에 avserve.exe 생성

레지스트리에 웜 파일을 등록해 윈도우가 시작될 때 자동으로 실행되게 한다.



[그림3] 레지스트리에 등록

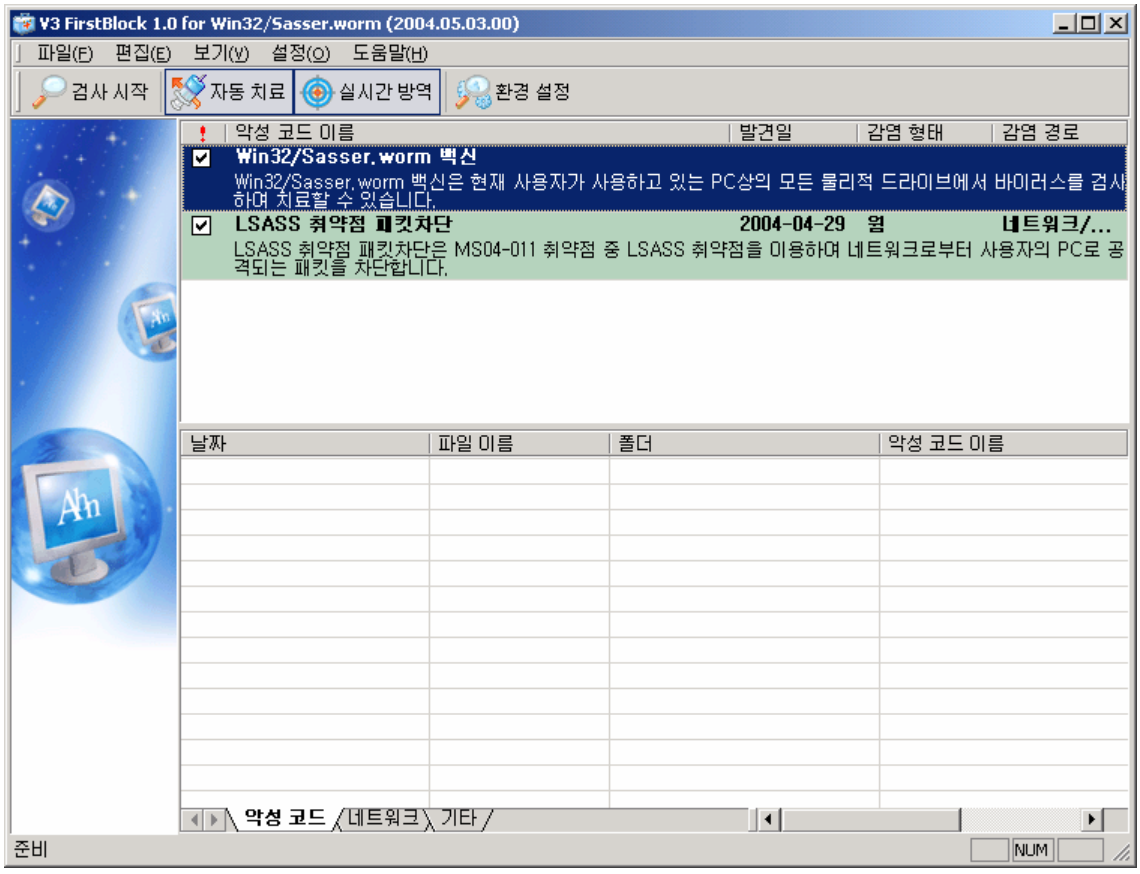
임의의 IP를 선택해 MS04-011 취약점 공격 패킷을 보내고 감염시킨다. 상대 컴퓨터가 잘못된 공격 패킷을 받으면 시스템이 종료되는 문제점을 가지고 있다. 그 외 시스템의 CPU 사용률을 100%까지 올려 시스템 속도가 매우 느려지게 하는 문제가 있었다.

안철수연구소를 비롯한 백신 업체는 새로운 엔진을 제공했다. 하지만, 국내 보도자료와 해외 자료가 동시에 나오면서 사서, 사세르 등으로 한글 이름이 불려졌다. 한글 이름은 많은 사람들에게 혼란스럽게 했고, 현재는 새서라는 이름으로 통일되고 있지만 사세르라는 이름도 여전히 불리고 있다.

안철수 연구소의 솔루션

취약점을 이용해 전파되는 웜은 패킷 차단 기능이 없는 백신으로는 예방할 수 없다. 패치가 가장 완벽한 예방법이지만 패치가 불안정해 시스템이 문제가 발생하는 경우가 많아 사용자

들이 패치를 꺼리는 경우도 있다. 이에 네트워크 패킷을 분석해 공격을 차단하는 솔루션이 요구되었다. 안철수연구소는 네트워크로 전파되는 신종 웜에 대처하기 위해 작년부터 V3 FirstBlock을 준비했다. V3 FirstBlock은 메모리와 파일에서 악성코드를 진단/치료하고 공격 패킷을 차단하는 역할을 하는 전용백신이다. 안철수연구소는 MS04-011 취약점 공격 패킷을 차단 할 수 있는 V3 FirstBlock for LSASS Vulnerability을 4월 29일 배포했으며 29일 발표된 개선된 공격 방식을 차단하는 버전을 30일 배포했다. 초기 버전은 단순히 MS04-011 취약점 공격 패킷을 차단해주는 기능을 가지고 있었고 이는 윈도우 업데이트를 하고 싶어도 공격패킷으로 인해 시스템이 종료되어 버려 윈도우 업데이트를 하지 못하는 시스템을 위한 것이다. 기존 백신 업체는 파일 검사 기반의 백신 제품만 개발해 네트워크를 통해 전파되는 악성코드를 예방하는 데는 한계가 있어 많은 업체에서 패킷을 차단하는 솔루션을 준비하고 있다.



[그림4] V3 FirstBlock 1.0 for Win32/Sasser.worm

새서 웜의 교훈

새서 웜의 피해는 비단 개인용 컴퓨터 뿐이 아니었다. 과장된 측면도 있겠지만 여러 기사를 보면 전세계적으로 100만대가 감염된 것으로 추정되며 골드만삭스, 브리티시 에어웨이, 영국 마리타임 박물관의 19개 지역 사무소, 영국 해안경비국, 통신회사인 보다폰, 유럽연합 집행

위원회 사무실 등도 피해를 입었다고 한다. 독일 우편배송회사 도이체포스트도 30만대가 감염되어 직원들에게 현금을 내줄 수 없었으며 뉴올리언스의 병원 500여 군데도 몇 시간 동안 폐쇄되고 워싱턴주의 사회보장 서비스 역시 웜의 공격을 받았다고 한다.

새서 웜의 증상이 시스템 종료로 확연히 눈에 띄어 상대적으로 다른 웜에 비해 피해감이 크게 느껴지기도 했지만 이 웜이 널리 퍼졌음은 확실하다. 우리는 6개월 전에도 이와 같은 일을 경험했지만 여전히 피해를 많이 입는 건 사용자의 안전불감증에도 원인이 있을 것이다. 사용자들이 한 달에 한번 발표되는 윈도우 패치만 제대로 했어도 이런 류의 웜으로부터 자신의 컴퓨터를 지킬 수 있었을 것이다. 하지만, 일반 사용자에게 보안 패치가 지나치게 어렵고 백신 역시 초보자들이 사용하기에는 어렵다는 건 관련 업계가 해결해야 할 문제로 생각된다.

현재 파일 검사 기반의 백신 프로그램은 네트워크로 전파되는 악성코드를 예방하는 기능까지 포함해 백신의 시스템 보호 범위는 더욱 넓어질 것으로 보인다.