ASEC Report 5월

® ASEC Report

2004. 6

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

은폐형 악성코드

2004년 5월 11일 안철수연구소는 은폐형 웜 치료 기술 개발을 발표했다. 은폐기법은 악성코드가 실행 중일 때 자신의 존재를 사용자와 백신을 포함한 프로그램에서 숨기는 기법이다. 물론 은폐기법을 사용하는 악성코드도 실행되기 전에 백신에서 진단은 다르지 않다. 하지만, 일단 실행된 후에 은폐형 악성코드를 찾는 건 쉽지 않으며 특히 많은 사용자들이 컴퓨터 사용에 익숙하지 않고 백신도 정기적으로 업데이트 하지 않음을 생각하면 결코 쉽게 생각할 부분은 아니다.

5월에 발견된 은폐형 악성코드는 Win-Trojan/Padodor.45770, Dropper/Haxdoor.39024 등이다. 앞으로 은폐형 악성코드는 계속 증가할 것으로 예상된다.

I. 5월 악성코드 Top 10

작성자: 정진성 연구원 (jsjung@ahnlab.com)

악성코드명	건수	%
Win32/Netsky.worm.29568	9723	44.0%
Win32/Netsky.worm.17424	2820	12.8%
Win32/Dumaru.worm.9234	2097	9.5%
Win32/Netsky.worm.28008	1454	6.6%
Win32/Netsky.worm.22016	819	3.7%
Win32/Netsky.worm.25352	772	3.5%
Win32/Netsky.worm.17920	619	2.8%
Win32/Bagle.worm.Y	326	1.5%
Win32/Bagle.worm.Z	326	1.5%
Win32/Netsky.worm.22016.C	308	1.4%
기타	2,480	11.2%
합 계	**22,104**	**100**

[표1] 2004년 5월 악성코드 Top 10

5월 악성코드 피해 동향

이번 달은 메일을 이용하여 전파되는 즉, Mass Mailer의 피해문의가 압도적으로 많았다. 지난 달에 있었던 네트워크(취약점)로 전파되는 악성코드인 Win32/Blaster.worm(이하 블래스터 웜), Win32/AgoBot.worm(이하 아고봇 웜)들이 Mass Mailer들 때문에 대부분 순위 밖에서 머물고 있다.

특히 Win32/Netsky.worm(이하 넷스카이 웜) 시리즈가 전체 피해문의의 과반수를 넘는다. 넷스카이 웜 피해문의 경우, 상당수가 감염된 시스템으로부터 직접 발송된 건도 포함한 터라 상대적으로 많은 피해문의 건수를 보이고 있다. 실제로 외국 안티 바이러스 업체의 통계를 보더라도 넷스카이 웜 변형들은 Top 10 에 대부분을 차지하고 있는 것으로 보아 넷스카이 웜 변형으로 인한 피해는 세계적인 추세로 보인다. 이번 달 전체 피해문의에서 넷스카이 웜만 별도로 통계를 내보았다.

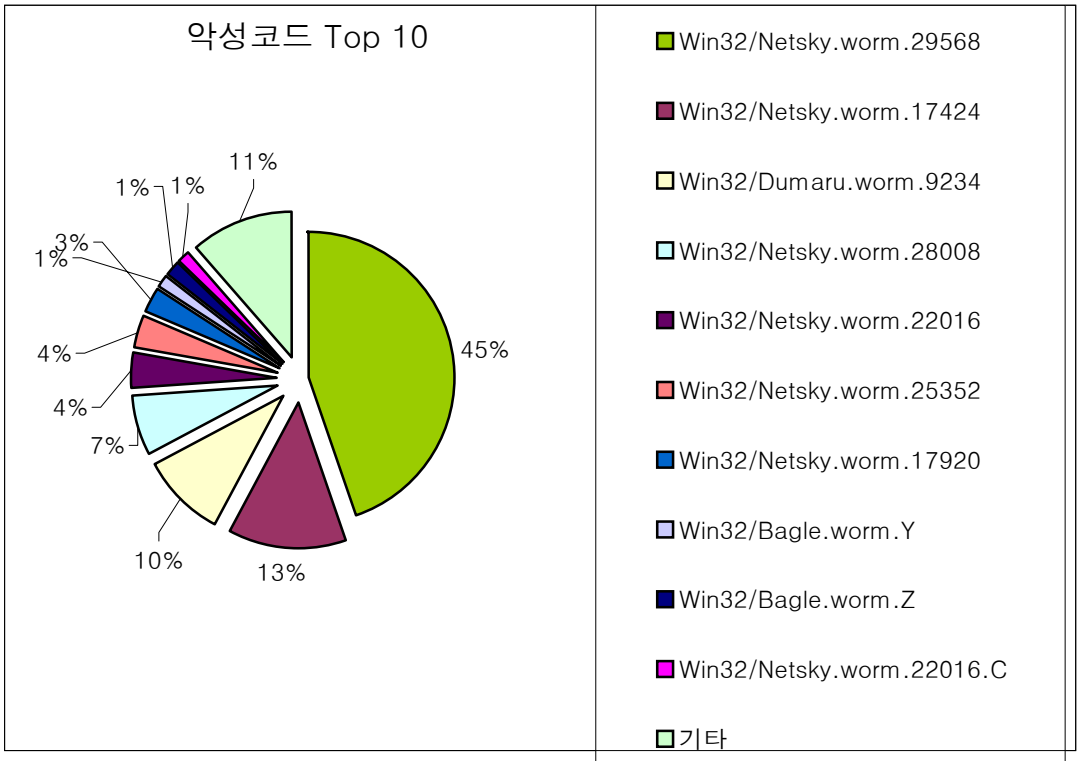
Win32/Netsky.worm.29568	9723
Win32/Netsky.worm.17424	2820
Win32/Netsky.worm.28008	1454

Win32/Netsky.worm.22016	819
Win32/Netsky.worm.25352	772
Win32/Netsky.worm.17920	619
Win32/Netsky.worm.22016.C	308
Win32/Netsky.worm.16896.B	225
Win32/Netsky.worm.18432.B	53
Win32/Netsky.worm.24064	50
Win32/Netsky.worm.26112	31
Win32/Netsky.worm.31744	30
Win32/Netsky.worm.18432.C	18
Win32/Netsky.worm.18944.B	5
Win32/Netsky.worm.24064.B	4
Win32/Netsky.worm.22016.D	2
Win32/Netsky.worm.20624	1
Win32/Netsky.worm.23040	1
합 계	**16935**

[표2] 2004년 5월 넷스카이 웜 피해문의건수

30개 정도나 되는 넷스카이 웜 변형 중 무려 18종의 넷스카이 변형들의 피해문의가 5월 한 달동안에 접수된 것을 알 수가 있다. 이는 2003년에 있었던 Win32/Yaha.worm(이하 야하 웜)의 통계와 비슷한 유형을 보여주고 있다. 야하 웜도 그 당시 많은 변형을 가지고 있었으며 각 변형이 다수의 피해문의 건수에 포함되었다.

5월의 악성코드 Top 10을 도표로 나타내면 [그림1]과 같다.



[그림1] 2004년 5월 악성코드 Top 10

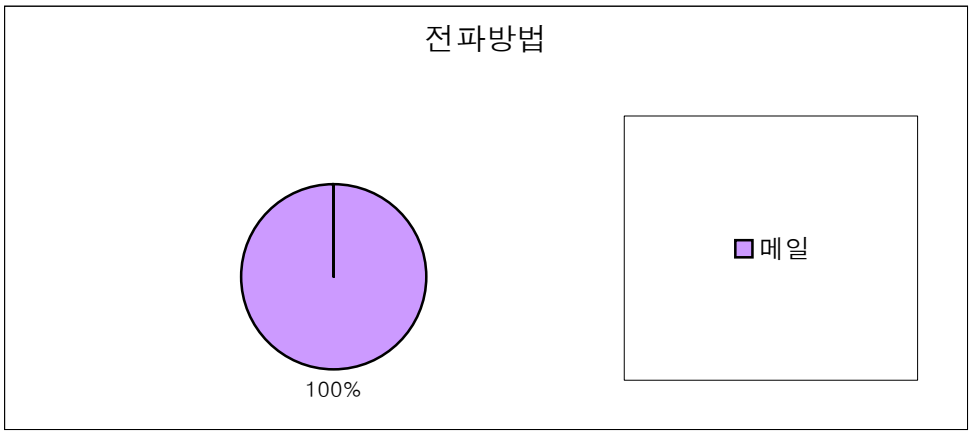
지난달에 현격히 문의가 줄어든 Win32/Damaru.worm의 문의가 다시 증가한 것을 알 수가 있다. 또한 Win32/Bagle.worm.Y, Z의 문의도 다시 순위권내에 진입하여 피해문의가 늘어났음을 알 수 있다.

대부분 사용자들이 자신이 시스템이 감염될 줄 모르고 방치하거나 전산자원의 증가로 역시 관리자가 미처 신경 쓰지 못한 시스템들이 여전히 많은 것으로 보인다.

5월 악성코드 Top 10의 전파방법 유형별 현황

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

위에서 언급한 것처럼 네트워크(보안 취약점을 이용하는) 웜이 피해문의 순위 밖에 있는 영향으로 모두 메일을 이용하여 전파되는 악성코드가 차지하고 있다.

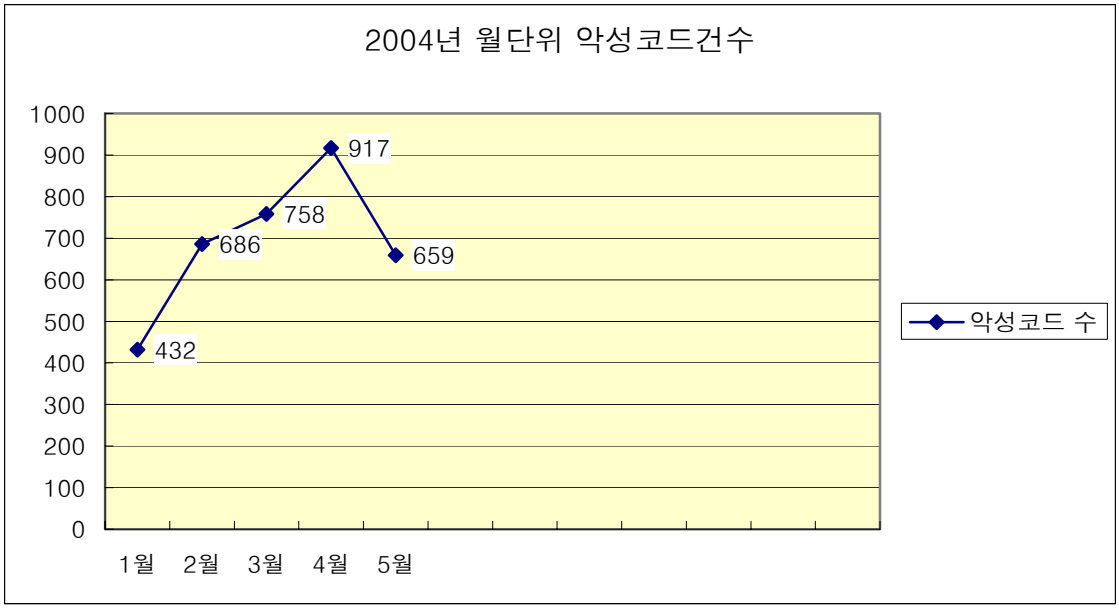


[그림2] 악성코드 Top 10의 전파방법 유형별 현황

이는 지난달과 비슷한 동향으로써 구종 및 신종의 Mass Mailer 의 영향이 점점 증가하고 있는 것으로 보고 있다.

월별 피해신고 악성코드 수 현황

이번 달은 올해 들어서 처음으로 피해 신고된 악성코드의 수가 감소하였다. 하지만 작년 동월이나 올해 다른 월과 비교 시 적은 수치는 아니다.

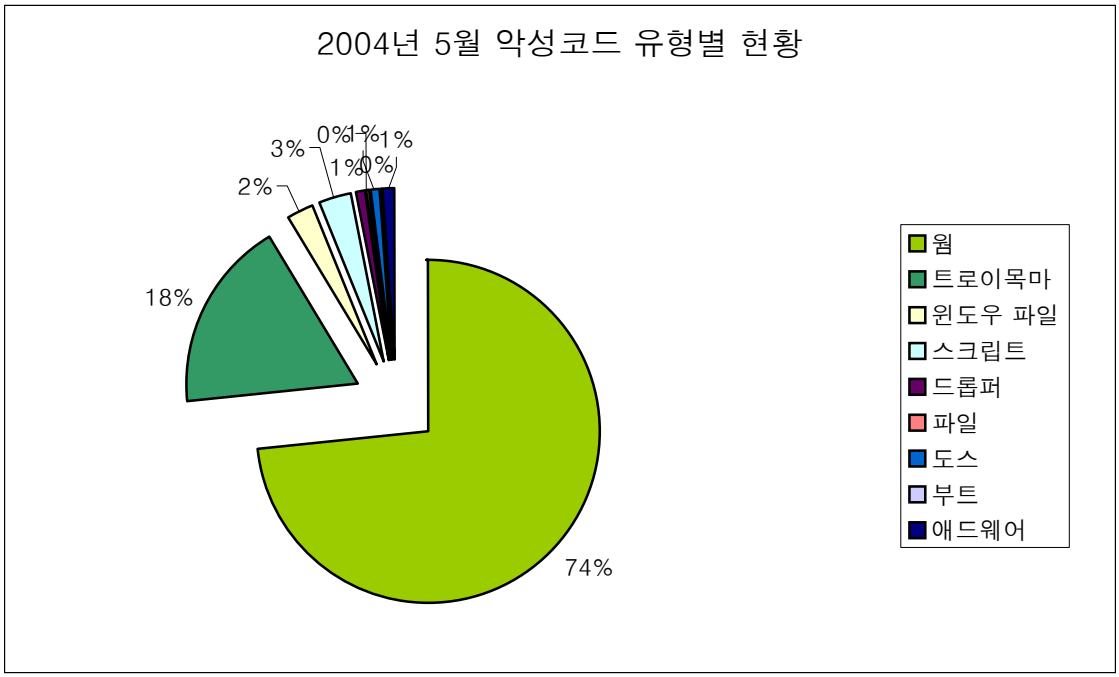


[그림3] 2004년 월별 피해신고 악성코드 수

이러한 원인으로는 기존의 악성코드들에 대한 피해문의가 급증한 반면 새로운 악성코드의 피해문의는 주춤한 것으로 파악된다. 즉, 악성코드 Top 10처럼 구종의 Mass Mailer들이 많

은 피해문의를 차지한 것처럼 이번 달은 구종의 악성코드에 대한 문의가 증가한 반면 신종이나 변형들에 대한 보고 건수가 다소 주춤한 것으로 보인다.

659종류에 이르는 악성코드들은 어떤 유형으로 분포되어 있는지 [그림4]를 통해서 확인 할 수 있다.



[그림4] 2004년 5월 악성코드 유형별 현황

일반적으로 Mass Mailer 웜과 취약점을 이용하여 전파되는 아고봇 웜과 같은 악성 IRCBot 웜들이 대부분을 차지하고 있다.

악성코드 유형에서 빠지지 않고 포함되는 것이 바로 도스 악성코드에 대한 통계이다. 아직까지 도스를 사용하는 사용자 또는 도스에서 사용되는 파일형식을 가지고 있는 사용자들을 찾아 볼 수가 있다. 일례로 고전 도스 게임을 즐기는 사용자던가, 윈도우 9x 시스템을 사용하는 사용자들이 포함된다.

이번 달 연구소로 피해문의가 접수된 도스 악성코드들은 다음과 같다.

- BachKhoa.3999
- Bleah.D
- Dir_II

- Trojan/CdKey.19120
- VCL.#3-2

필자는 가끔 부트 바이러스에 대한 문의를 받는 편이다. 이번 달은 지난 달과 달리 근래 들어 가장 많이 발견되는 WXY 부트 바이러스가 신고되지 않았다. 대신 Bleah.D 부트 바이러스가 신고 되었다. 이를 제외하면 나머지는 모두 도스 파일 바이러스들이다. Dir_II 바이러스가 여전히 존재하는 것이 매우 이채롭다.

도스 악성코드들은 그 피해문의 건수가 대부분 1건으로 미비하지만 여전히 도스 운영체제와 관련 파일을 사용하는 사용자들이 있는 한 계속 존재할 것으로 보여진다.

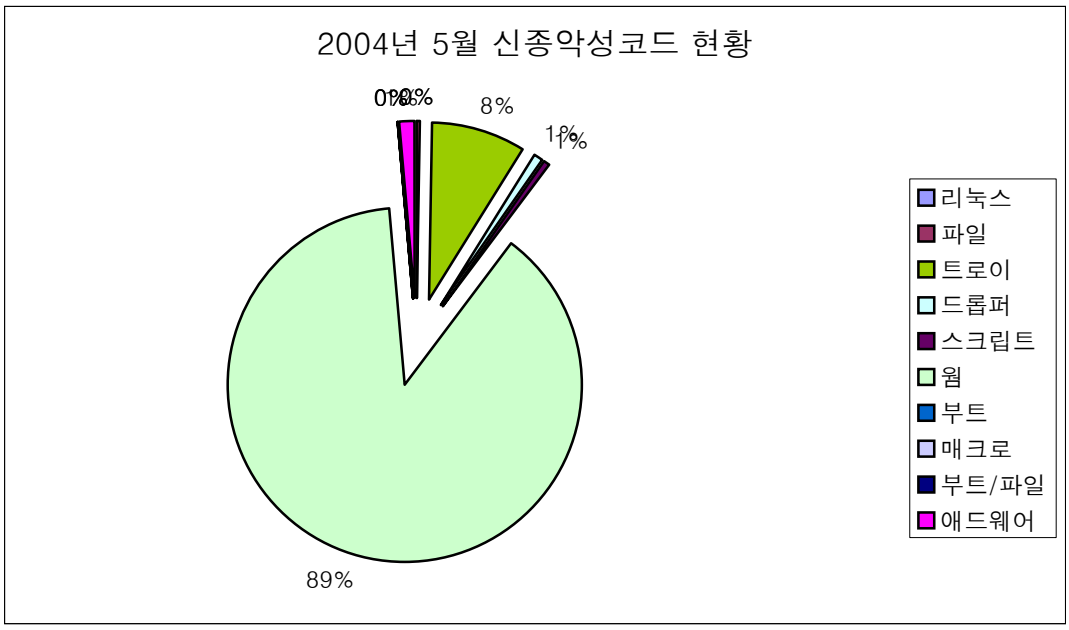
II. 5월 국내 신종 악성 코드 발견 동향

작성자: 정진성 연구원 (jsjung@ahnlab.com)

5월 한 달 동안 접수된 신종 악성코드의 건수는 [표1], [그림1]과 같다.

리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	애드웨어	합계
0	1	30	3	2	313	0	0	0	5	354

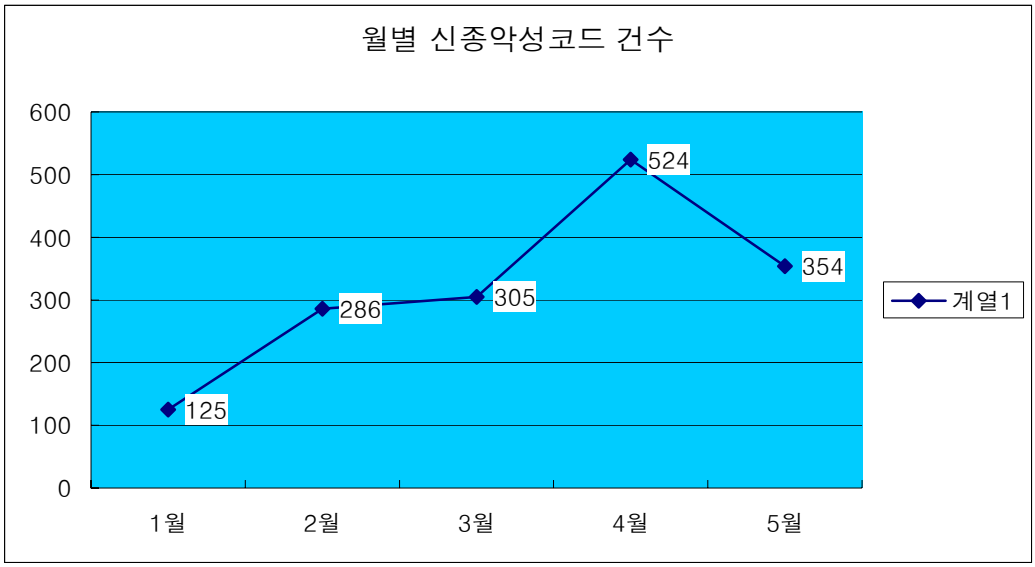
[표1] 2004년 5월 유형별 신종 악성코드 발견현황



[그림1] 2004년 5월 신종 악성코드 발견현황

5월 발견된 신종 악성코드 동향

5월은 354종의 신종 및 변형에 대한 악성코드가 발견되었다. 이는 올해 들어 두번째로 많은 수치이다. 발견된 악성코드들은 대부분 악성 IRCBot 웜 및 트로이목마 류가 주를 이루고 있다.



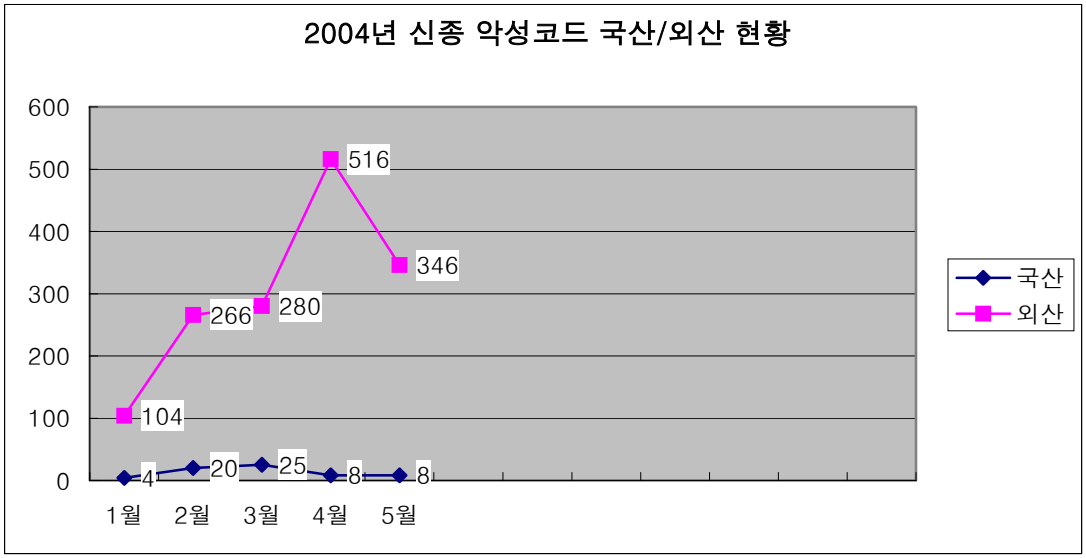
[그림2] 2004년 월별 신종(변형) 악성코드 발견현황

이번 달에 새롭게 발견된 악성코드 중 특이할 만 한 것은 Win32/Sasser.worm(이후 새서 웜)이다. 이 웜은 MS04-011 취약점이 있는 시스템을 대상으로 감염된다. 이 웜은 공개된 공격코드를 사용하였다. 안철수연구소는 이 웜이 출현하기 전 미리 해당 공격코드를 차단할 수 있는 전용백신인 V3 FirstBlock을 제작하여 제공하였다.

이후 새서 웜이 이용하는 MS04-011 취약점을 이용하는 악성코드가 다수 발견되기도 하였다. 작년 8월에 MS03-026 취약점을 이용한 블래스터 웜과의 피해현황을 비교하면 새서 웜의 피해는 낮다고 볼 수 있다. 이러한 이유 중에 하나로 안철수연구소를 비롯한 각 보안업체 및 ISP 업체 등에서 대응이 다소 빨랐던 점을 들 수 있겠다.

제작지별 신종악성코드 현황

다음은 신종 악성코드들의 국산/외산의 현황을 보여주고 있다.



[그림3] 2004년 제작지별 신종 악성코드 현황

지난 달에 많은 종류의 신종 및 변형에 대한 악성코드가 발견 및 보고되었던 것에 비하면 이번 달에는 지난 달에 비해 수치가 떨어진 것을 알 수 있다. 이렇게 발견된 외산 악성코드들은 대부분 악성 IRCBot 종류가 차지하고 있다.

국내발견 악성코드들은 악의적인 목적으로 의도적으로 제작된 악성코드는 없었다. 다만 애드웨어 류가 발견, 보고 되었는데 이중에서는 의도하지 않는 애드웨어의 버그로 인하여 발생된 것도 있었다. 대부분의 애드웨어가 BHO를 이용하여 익스플로어에 Inject되어 실행되는데, 버그가 존재하는 경우 자칫 인터넷 익스플로어마저 실행되지 않는 문제점을 가져올 수 있다. 이번 케이스도 이와 유사하였다. 또한 다른 증상으로는 웹 브라우저의 시작페이지를 변경하는 형태가 압도적으로 많았다.

이들 대부분은 성인 사이트에서 ActiveX를 이용하여 설치된 케이스가 많았다. 웹 서핑 시 무심코 누르는 마우스 클릭에 낯뜨거운 성인 광고로 당황스러움을 경험했던 사용자라면 앞으로는 그러한 점을 주의하는 것은 첫번째이고 V3Pro 2004를 비롯한 애드웨어 관련 대응 제품을 사용하는 것도 쾌적한 웹 서핑을 하는데 도움이 될 수 있을 것이다.

III. 5월 신규 보안 취약점

작성자: 정관진 주임연구원(intexp@ahnlab.com)

5월의 첫 시작, 매월의 시작되는 첫 날인 1 일은 뭔가 새로운 느낌을 가지게 만든다. 마음먹고 준비하던 일의 첫 시작의 발돋움을 하는 날로 잡는데도 이러한 이유가 있는 것인가 보다. 하지만, 첫 시작 때부터 웬일인지 컴퓨터가 아무 이유 없이 부팅되는 등 이상한 일들이 벌어졌다. 바로 마이크로소프트사의 MS04-011 의 취약점 LSASS을 이용한 새서(Sasser)웜이 전세계를 강타한 것이다. 물론, 작년의 블래스터 만큼의 큰 피해를 가져오지는 않았지만 블래스터와 마찬가지로 사전에 충분히 막을 수 있었던 일이었는데도 불구하고 또 다시 상황은 반복되고 말았다. 이번 5월호에서는 새서 웜을 다시 재 조명해 보고, 시스코사의 IOS 소스 유출 사건 및 5월의 MS 취약점을 알아보도록 하겠다.

보안 취약점이 가져온 또 다른 위협, 새서 웜

5월1일 국내에 보고된 Win32/Sasser.worm.15872[1]는 MS04-011 취약점을 이용한 것으로, 보안패치가 안된 시스템을 전파대상으로 삼고 있다. TCP 445번 포트를 이용한 전파시도로 관련 패킷이 증가하고 TCP 5554번 포트를 오픈한다. 이로 인하여 네트워크 트래픽을 증가시켜 대역폭 소모를 가져왔고, 사용자들이 컴퓨터를 제대로 사용할 수 없는 현상이 나타났다. 새서 웜의 출현은 곧 개인, 기업 그리고 국가 기간 망까지 피해 영역을 확산시키게 되었다. 델타항공, 아메리칸 익스프레스를 포함해 비즈니스를 수행하는 업체와 대학, 병원 등 영역의 구분에 상관없이 인터넷이 연결되어 있고 취약점을 보유하고 있는 시스템 모두를 대상으로 하고 있어 피해 영역은 클 수 밖에 없었다. 이번 새서 웜은 감염된 시스템에 TCP 5554 번 포트를 오픈하여 FTP로 해당 웜을 다운 받아갈 수 있도록 하고 있다. 이러한 형태는 다른 웜들에서도 사용되는 기술이었지만, 이번 새서 웜에 배포된 FTP 서버가 버퍼오버플로우 취약점이 존재한다는 것이 다른 점이다. 이는 새서 웜에 감염된 시스템의 5554번 포트를 통해 또 다른 공격이 가능하게 된 다는 것이다. 이를 증명이라도 하듯 5월 13일에는 새서의 FTP 서버 취약점을 이용하여 전파되는 Win32/Dabber.worm.29696[2]이 발견되었다.

하지만 이런 피해가 발생하기 전에 사전에 예방할 수는 없었을까? MS04-011 취약점 패치가 4월 14일 발표되었고, 새서 웜 최초 발견일이 4월30일(외국 시각 기준)인 점을 감안하면

[1] AhnLab, Win32/Sasser.worm 15872
http://b2b.ahnlab.com/smart2u/virus_detail_1379.html
[2] AhnLab, Win32/Dabber.worm.29696
http://b2b.ahnlab.com/smart2u/virus_detail_1386.html

2주간의 사전 예방 시간이 있었다. 피해를 크게 줄일 수 있었지만, 이러한 바람은 여지없이 무너지고 만 것이다. 개인의 보안의식 그리고 기업의 보안관리자들의 역할이 더욱 강조되는 때이다

MS 의 5월 보안 패치

마이크로소프트사는 2004년 5월 12일 MS04-015 패치를 발표하면서 패치 업데이트를 권고하였다. 도움말 및 지원센터(Help and Support Center)를 지원하는 HCP 프로토콜의 URI 처리 부분에 취약점이 존재하여, 공격자는 해당 시스템을 완전히 제어할 수 있게 된다. 즉, 프로그램 설치, 데이터보기, 변경 및 삭제 등이 모두 해당된다. HCP 프로토콜은 URL 과 비슷하게 사용되는 것으로 이 취약점을 이용하여 공격자는 악의적인 HCP URI를 포함한 링크를 사용자가 클릭하도록 유도하여 공격자가 의도한 프로그램이 설치 될 수 있다. 윈도우 시스템을 운영하는 관리자들은 안철수연구소에서 배포하는 ASEC Advisory[3]를 참고하여 업데이트 할 것을 권고한다.

시스코 사의 IOS 코드 유출

시스코(CISCO)사의 네트워크 장비 운영체제인 IOS(Internet Operating System)버전 12.3 소스코드가 유출되었다고 러시아 사이트중의 하나인 SecurityLab.ru에 보고되었다. 전체용량은 800 메가 바이트(Megabytes)로 이중 다음 코드만이 공개되었다.[4]

- ipv6_discovery_test.c (Neighbor Discovery unit tests)
- ipv6_tcp.c (IP version 6 support functions for TCP)
  (현재 위 코드는 해당 사이트에서 삭제되었다.)

지난 2월의 윈도우 2000 운영체제의 소스코드 일부분이 유출된 것과 마찬가지로 또 다시 같은 상황이 벌어진 것이다. 코드 유출로 인한 위협은 현재까지 보고되지 않았지만 분명 가능성이 존재하는 만큼 주시할 필요는 있다. 그리고 이번 사건의 당사자 뿐만 아니라 각 기업의 중요정보에 대한 관리의 중요성을 다시 한번 되새겨 볼 때이다.

---

[3] [ASEC Advisory] 도움말 및 지원 센터 HCP 프로토콜 처리 취약점
http://b2b.ahnlab.com/securityinfo/info_view.jsp?seq=5923

[4] SecurityLab
http://www.securitylab.ru/45221.html

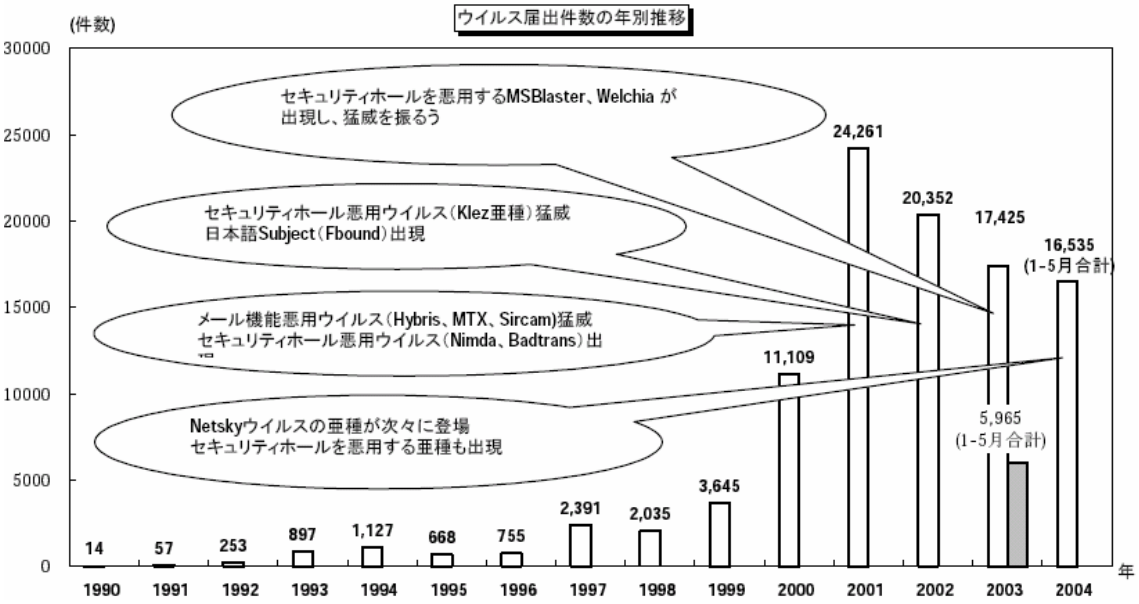
Ⅳ. 5월 일본 피해 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

일본은 Win32/Netsky.worm(이하 넷스카이 웜)이나 Win32/MyDoom.worm(이하 마이둠 웜)과 같은 Mass Mailer의 감염으로 인한 피해가 심각한 상태이다.

[표1]는 일본 IPA/ISEC에서 발표한 연도별 악성코드 노출건수를 도표로 나타낸 것이다. 2004년 1월부터 5월까지 집계된 악성코드 노출 신고건수의 합계는 16,535건으로 이는 작년 한 해 동안 집계된 악성코드 노출건수의 총합에 육박하는 값으로써 올해에 악성코드에 노출된 사례가 급격하게 증가한 것을 알 수 있다.

올해에 발생한 노출신고와 관련하여 주목할만한 점은 Mass Mailer에 의한 피해가 대다수를 차지한다는 점이다. 이러한 특징은 보안 취약점을 악용하여 전파되는 웜들이 주류를 이루었던 작년의 상황과 확연히 구분되는 특징이라고 볼 수 있으며 특히 넷스카이 웜의 신고건수가 많은 양을 차지하고 있는 것도 주목할만한 점이다..



[표1] 연별 악성코드 노출 현황(자료출처: 일본 IPA/ISEC)

일본 유행 악성코드 유형별 발생현황

2004년 5월 일본의 악성코드 동향과 관련하여 가장 주목할만한 이슈는 넷스카이 웜 변형들이 여전히 활발하게 전파되고 있는 점이다. 넷스카이 웜은 2004년 2월 최초로 발견되어 급

속히 확산된 이메일을 통해 전파되는 악성코드이다. 현재 넷스카이 웜은 계속해서 여러 변형들이 발견되고 있으며 감염 및 전파 방법과 증상도 메일을 통한 전파와 대량의 감염 파일을 첨부한 메일 발송이라는 단순한 기능에서 특정 사이트에 대한 공격 기능을 포함하는 등 다양해지고 있는 추세이다.

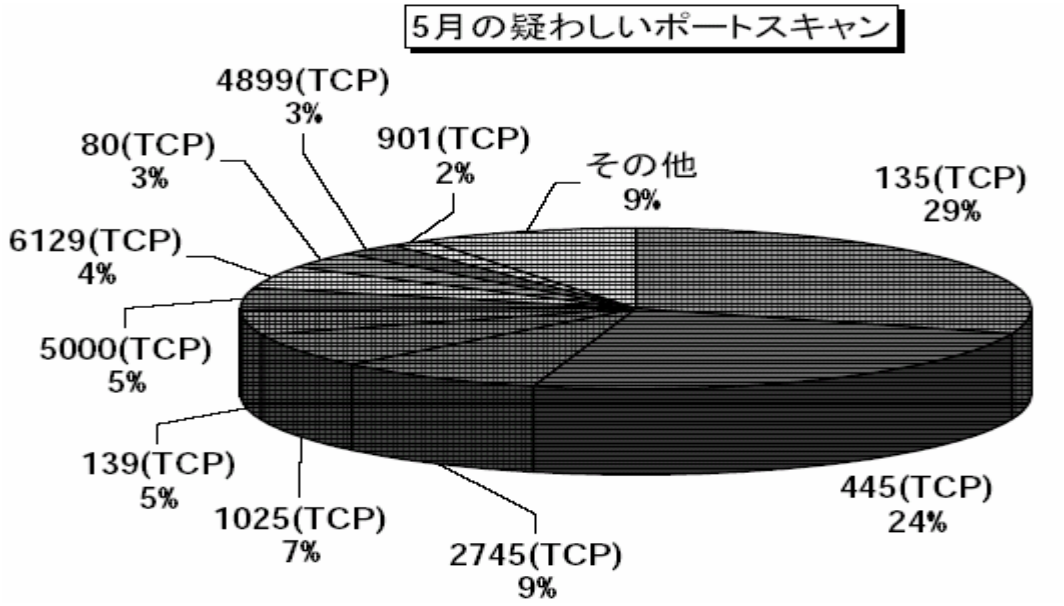
[표2]는 2004년 5월 IPA/ISEC에 접수된 악성코드 노출 신고 건수를 집계한 자료로써 넷스카이 웜의 신고건수가 월등하게 많음을 알 수 있다.

Window/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Netsky	1,984	Xm/Laroux	21	VBS/Redlof	134
W32/Bagle	464	X97M/Tristate	4	Wscript/Fortnight	21
W32Klez	383	X97M/Poorboy	4	Wscript/Kakworm	9
W32/LovGate	268	W97M/Marker	3	VBS/Loveletter	3
W32/Mydoom	256	X97M/Divi	3	VBS/Netlog	2
W32/Swen	218				

[표2] 악성코드 노출 신고 현황(자료출처: 일본 IPA/ISEC)

일본 네트워크 트래픽 현황

[그림1]은 2004년 5월 일본에서 발생된 네트워크 포트 유형별 사용현황을 나타낸 것이다. 135번과 445포트에서 발생하는 네트워크 사용량이 현저하게 많은 것을 알 수 있는데 두 포트는 윈도우 OS에서 기본으로 사용되는 포트들이지만 최근 유행하는 웜들이 윈도우 OS의 취약점을 이용한 공격을 시도할 때에도 사용된다. TCP 1745번을 이용한 트래픽이 많은 것을 볼 수 있는데 이는 Win32/Bagle.worm에 감염된 시스템에 의한 것일 가능성이 있다.



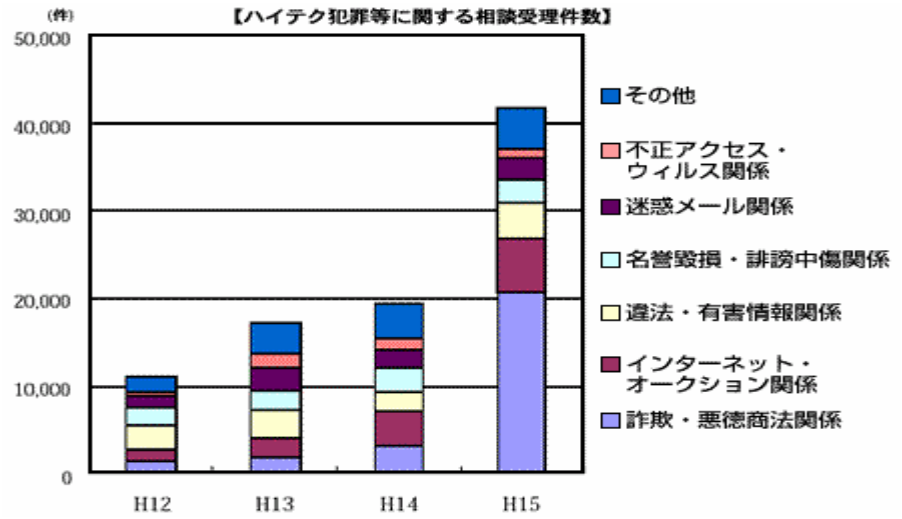
[그림1] 일본의 포트별 네트워크 트래픽 현황

윈도우 보안 취약점을 이용하여 전파되는 새서 웜

JPCERT 등 일본의 인터넷 보안 관련 기관들은 OS의 패치와 방화벽의 사용 등 새서 웜에 의한 감염 피해를 예방하기 위한 권고문을 발표하였다. 새서 웜은 2004년 4월 발표된 최신 윈도우 보안 취약점(MS04-011)을 악용하여 전파되는 악성코드이다.

인터넷을 통한 범죄 증가

작년 한 해 동안 발생한 인터넷 관련 범죄들 중 가장 많은 피해를 당한 것은 사기나 악덕 상법과 관련된 것으로 나타났다. 일본 경찰청에서 발표한 자료에 의하면 실제로 사용자가 이용하지 않은 요금에 대한 청구서를 발송하여 이를 제대로 인지하지 못한 피해자가 요금을 지불하는 것과 같은 방식으로 피해를 당하는 사례가 급격하게 증가하고 있는 것으로 나타났다. 아래의 표는 연도별 인터넷 관련 범죄들에 대한 상담내용을 유형별로 분류한 것으로 2002년과 비교해서 2003년에 사기와 악덕상법과 관련된 것이 급속히 늘어난 것을 알 수 있다. 이러한 범죄는 올해에 들어서도 사라지지 않고 피해가 계속되고 있고 경찰청에서는 이에 대한 주의를 요하는 권고문을 발표했다.



[표3]인터넷 관련 범죄 현황(자료출처: 일본 경찰청)

V. 5월 중국 피해 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

5월의 중국 악성코드 동향은 지난 4월과 유사하게 Mass Mailer가 강세를 보이나 그 영향력은 현격하게 떨어지고 있다. 지난 4월 중국 악성코드 동향 보고에서 언급하였듯이 네트워크로 전파되는 웜의 영향력이 점점 증가하고 있다. 그리고 운영체제의 취약점을 이용하는 웜의 영향력도 눈에 띄게 증가한 것이 이번 5월 중국 악성코드 동향의 특징이라고 볼 수 있다.

중국의 악성코드 TOP 5

순위 변화	5월	Rising	CNCVERC
*	1	Worm.Netsky	Worm.Sasser
*	2	Worm.Lovgate	Worm.Netsky
NEW	3	Worm.Sasser	Worm.Novarg
NEW	4	Worm.Klez.L	Worm_Bagle
- 2	5	Worm.Agobot.3	-

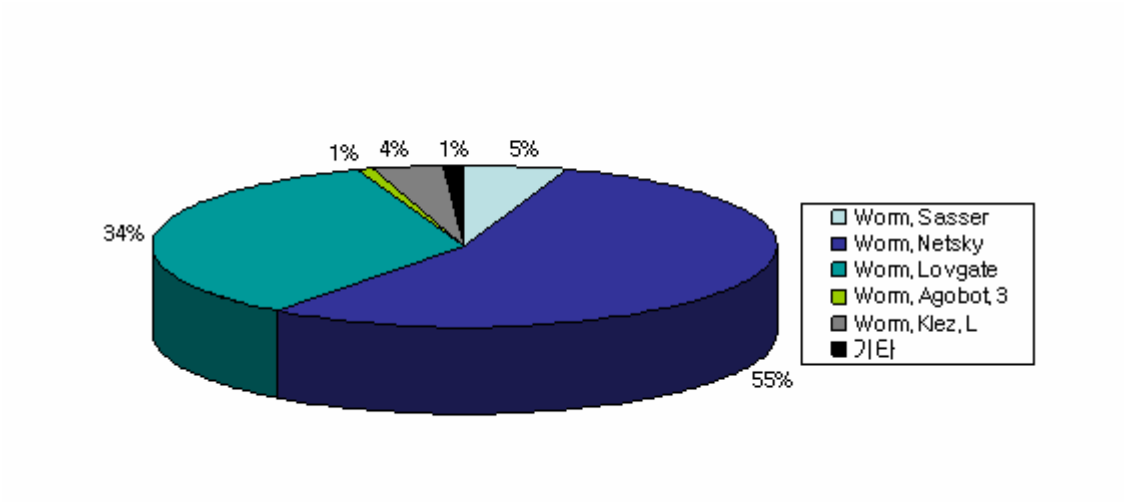
[표1] 2004년 5월 중국의 악성코드 TOP 5

'*' - 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 5월 중국 악성코드 TOP 5이다. 위 두 기관의 통계 순위의 차이는 집계 방식과 통계를 위한 자료의 차이로 인한 것으로 추정된다. [표1]에서 보면 1위와 2위는 4월과 동일하다는 것을 알 수 있으며 새로 순위에 진입한 악성코드 2건은 모두 네트워크로 확산되는 웜인 것을 알 수 있다. 2월부터 현재까지도 1위 자리를 차지하고 있는 Worm.Netsky(Win32/Netsky.worm, 이하 넷스카이 웜)는 순위상으로는 1위를 차지하고 있으나 전체적인 감염신고 통계상으로는 영향력이 지난 달과 비교하여 많이 줄어든 것으로 분석된다. 그리고 그 뒤를 따라서 2위에는 순위 변동 없이 Worm.Lovgate(Win32/LovGate.worm, 이하 러브게이트 웜)가 차지하고 있다. 이 웜은 지난 달에 처음으로 순위에 진입하였으나 이번 5월달에는 그 영향력이 더욱 확대된 것으로 분석된다. 3위에는 Worm.Sasser(Win32/Sasser.worm, 이하 새서 웜)가 차지하고 있다. 이 웜은 4월 13일 마이크로소프트에서 발표한 MS04-011 취약점 중 윈도우 2000 계열의 Lsass 취약점을 공격한다. 이러한 문제로 인해 5월 1일 중국 대륙 전역에서도 급격한 확산으로 인해 문

제가 되었을 뿐만 아니라 전세계적으로도 많은 감염 신고가 있었다. 4위에는 이번 달 순위 차트에 새로 진입하였을 뿐만 아니라 4월에도 신고가 전무하였던 Worm.Klez.L(Win32/Klez.worm, 이하 클레즈.L 웜)가 차지하고 있다. 그리고 지난 달 3위를 차지하였으나 이번달에는 2계단 하락한 5위에는 Worm.Agobot.3(Win32/AgoBot.worm, 이하 아고봇 웜)가 뒤를 이어가고 있다.

악성코드 분포



[표2] 2004년 5월 중국의 악성코드 분포

[표2]를 보면, 지난 달과 비교하여 새로운 변화 2가지가 가장 눈에 띄게 된다. 그 첫번째가 넷스카이 웜의 영향력 감소이다. 넷스카이 웜의 경우에는 지난 달까지만 하여도 전체 분포에서 86%를 차지하고 있으나 5월 달에는 전체의 절반을 겨우 넘긴 55%를 차지하고 있다. 그리고 두 번째로는 러브게이트 웜의 급격한 증가이다. 4월에는 10%에도 못 미치는 8%를 차지하고 있었으나 이번 달에는 4배 이상 증가한 34%를 차지하고 있다. 그리고 5월 1일 등장하여 급격한 확산을 보였던 새서 웜은 예측과는 달리 전체 분포에서 5%를 차지하고 있으며 클레즈.L 웜은 전체 4%를 차지하며 그 뒤를 이어 4위를 차지하고 있다. 그러나 지난 달 예측과는 아고봇 웜은 1%대를 차지하며 그 영향력이 줄어 들었다. 그 외 1%를 차지하고 있는 기타에는 Worm.Novarg(Win32/MyDoom.worm), Worm.Lentin(Win32/Yaha.worm)의 Mass Mailer와 지난 달부터 다시 새로운 변형들이 등장하기 시작한 QQ 트로이목마의 변형 중 하나인 Trojanl.QQtail와 Trojan.QQ3344가 차지하고 있다. QQ 트로이목마 변형의 지속적인 등장 요인 중 하나는 Win-Trojan/QQSoftKit.448000[5] 와 같은 QQ 트로이목마를 제작할 수 있는 툴이 일반화 되어 있기 때문이라고 추측된다.

---

[5] AhnLab, Win-Trojan/QQSoftKit.448000
http://info.ahnlab.com/smart2u/virus_detail_1405.html

결론

5월의 중국 악성코드 동향은 기존의 Mass Mailer가 감소 추세를 보인 반면 네트워크로 전파되는 웜의 증가추세로 볼 수 있다. 위에서 상술한 바와 같이 네트워크로 전파되는 웜이 전체 악성코드 분포에서 50%에 달하고 있다는 점은 중국 악성코드 동향의 커다란 변화가 진행되고 있다는 것을 증명하는 것으로 분석된다. 이러한 커다란 변화는 결국에는 운영체제의 취약점에 대한 공격과 네트워크 트래픽 폭주 현상 등으로 이어질 것으로 예측된다.

VI. 테크니컬 컬럼 - 최신 은폐형 악성코드

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

은폐형 Win32/AgoBot.worm, Dropper/Haxdoor.39024, Win-Trojan/Padodor.45770 등 최근 자신의 존재를 사용자와 백신 등에 숨기는 웜이나 트로이목마가 꾸준히 등장하고 있다. 기법도 점점 발전하고 있으며 찾기도 어려워지고 있다. 이 글에서는 최근 윈도우 NT계열(NT/2000/XP)에서 사용되는 은폐기법에 대해 알아보겠다.

은폐형 악성코드의 발전

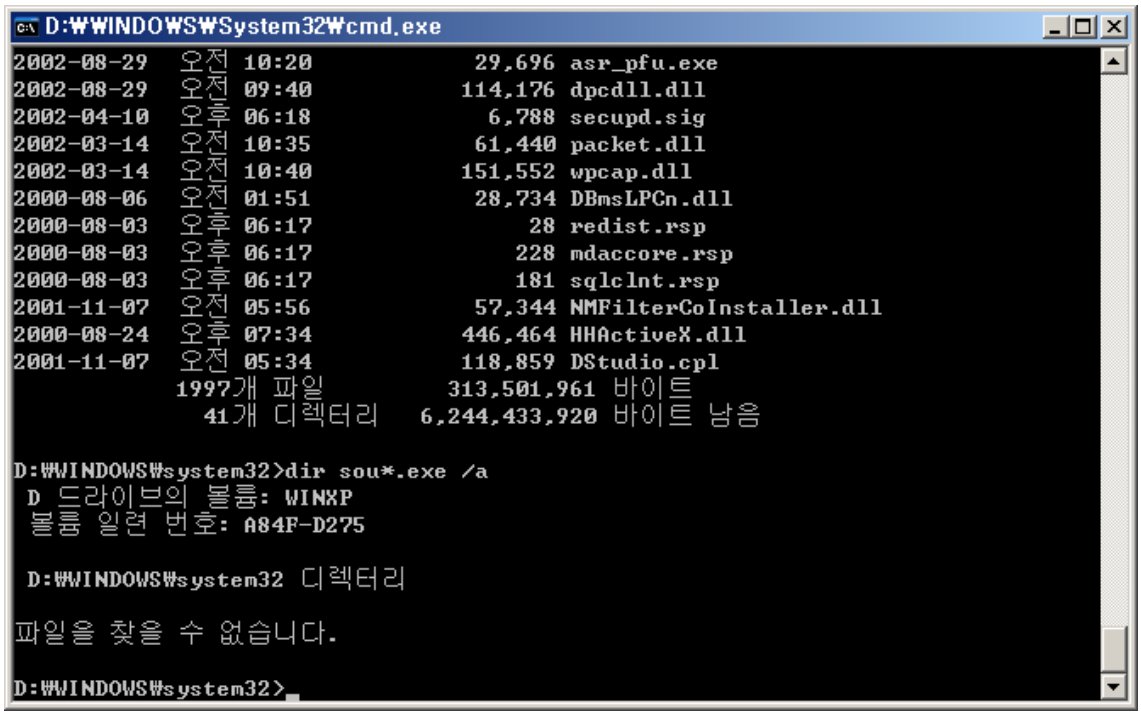
1998년 여름 Win95/CIH 바이러스가 사용자들 사이에 널리 퍼지면서 윈도우 바이러스가 널리 퍼지는 것도 불가능하지 않다는 것을 일깨워줬다. 여러 바이러스 제작자들이 도스 바이러스에서 윈도우 바이러스 제작을 시도하게 되고 은폐기법을 사용하는 윈도우 바이러스도 제작되었다. 최초의 은폐기법을 사용하는 윈도우 바이러스는 Win95/Zerg 바이러스로 알려져 있다. 윈도우 9x 계열 (95/98/Me) 에서만 실행되지만 도스 시절에 사용되었던, 사용하려는 파일 치료 후 파일 닫기 시 감염 시키는 방법을 사용해 사용자나 백신 프로그램 등이 감염된 파일을 찾기 어렵게 한다. 하지만, 이 바이러스는 버그가 많아 자주 컴퓨터를 정지시키는 등의 문제가 있어 실제로 사용자들에게 퍼지진 않았다. Win32/Cabanas 바이러스는 윈도우 9x(95/98/Me) 뿐 아니라 윈도우 NT (NT/2000)에서도 감염되는 바이러스로 감염 길이를 속이는 간단한 은폐기법이 사용되었다. 하지만, 윈도우에서는 길이가 바이트 단위가 아니라 대략적인 크기인 킬로 바이트로 표현되고 사용자들이 길이를 확인하는 경우가 드물어 길이 은폐는 큰 이점이 없다. Win95/Sma는 버그도 적고 큰 문제 없이 다른 파일을 감염시키며 은폐기법에도 크게 문제가 없는 바이러스이다. 감염된 파일이 열릴 때 바이러스를 치료하고 파일 사용을 마치고 닫을 때 파일을 감염시키는 방법을 사용한다. 하지만, 윈도우 9x 계열에서만 실행되고 일반에 감염 보고는 없는 실험용 바이러스이다. 윈도우 파일 바이러스는 윈도우 웜, 백도어의 홍수 속에 제작 수는 점점 줄어 들게 된다. 윈도우는 도스와 달리 여러 파일이 동시에 사용되므로 파일이 열릴 때 감염된 파일에서 바이러스를 치료하고 파일 닫을 때 재감염 시키는 방법은 시스템 성능을 떨어뜨리거나 충돌 문제를 일으킬 소지가 많다.

여기까지가 지금까지 ASEC Report 2003년 7월호에 정리된 작년 상황이었다. 약 1년이 지난 2004년 6월의 상황은 어떨까 ?

윈도우도 95, 98 이 아닌 윈도우 NT 계열(NT/2000/XP)의 사용이 증가하고 바이러스보다 트로이목마(백도어)와 웜이 대세가 되면서 은폐 기법도 변화하게 되었다. 바이러스는 다른 파일을 감염시키기 때문에 파일 길이의 변화를 효과적으로 숨기는 노력이 필요했다. 하지만, 웜이나 트로이목마는 감염 시킬 숙주가 필요 없으므로 은폐 기법은 다음과 같이 바뀐다.

1. 파일을 찾지 못하게 숨긴다.
2. 작업관리자에서 찾지 못하게 한다.
3. NETSTAT 등으로 사용중인 포트를 알아차릴 수 없게 한다.

은폐형 악성코드는 자신의 존재를 시스템에서 숨긴다. 탐색기나 명령 프롬프트에서 웜 파일인 soundman.exe 파일을 찾아보면 찾을 수 없다[그림1].



[그림1] soundman.exe 파일을 못 찾음

은폐기법 원리

도스 시절 은폐형 바이러스들은 DIR 명령과 관련된 인터럽트를 가로채 사용자를 속였다. 윈도우 역시 기본 원리는 비슷하다. 대신 윈도우 NT 계열은 프로세스 별로 권한이 존재하며 물리적 메모리와 논리적 메모리의 처리도 필요하다.

Win NT/2000/XP에서 API를 가로채 은폐기법을 사용하는 방법은 다음과 같다.

1. OpenProcessToken()을 사용해 특권 조절(adjust privileges)
2. NtQuerySystemInformation()을 이용해 프레세스 리스트 얻기
3. OpenProcess()를 이용해 프로세스 열기
4. VirtualProtectEx()와 WriteProcessMemory()를 이용해 코드에 쓰기

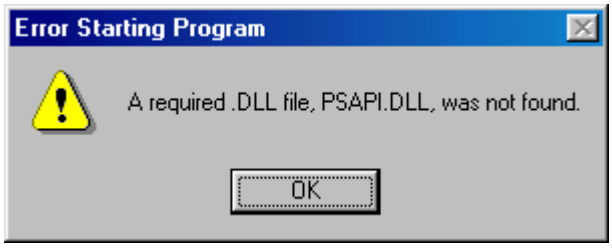
이미 만들어진 프로세스의 경우 NtResumeThread()를 가로챈다. 이 API는 모든 프로세스 존재하므로 이 API만 가로채고 있으면 다른 프로세스의 기능도 가로 챌 수 있다.

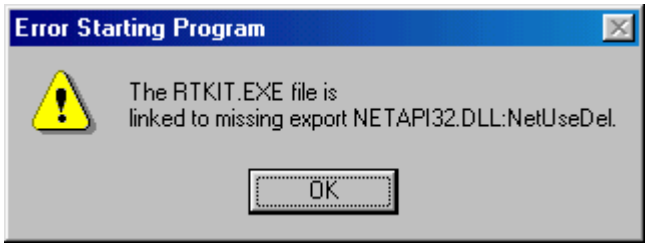
은폐형 악성코드는 대체로 다음 API를 가로채 자신을 숨긴다.

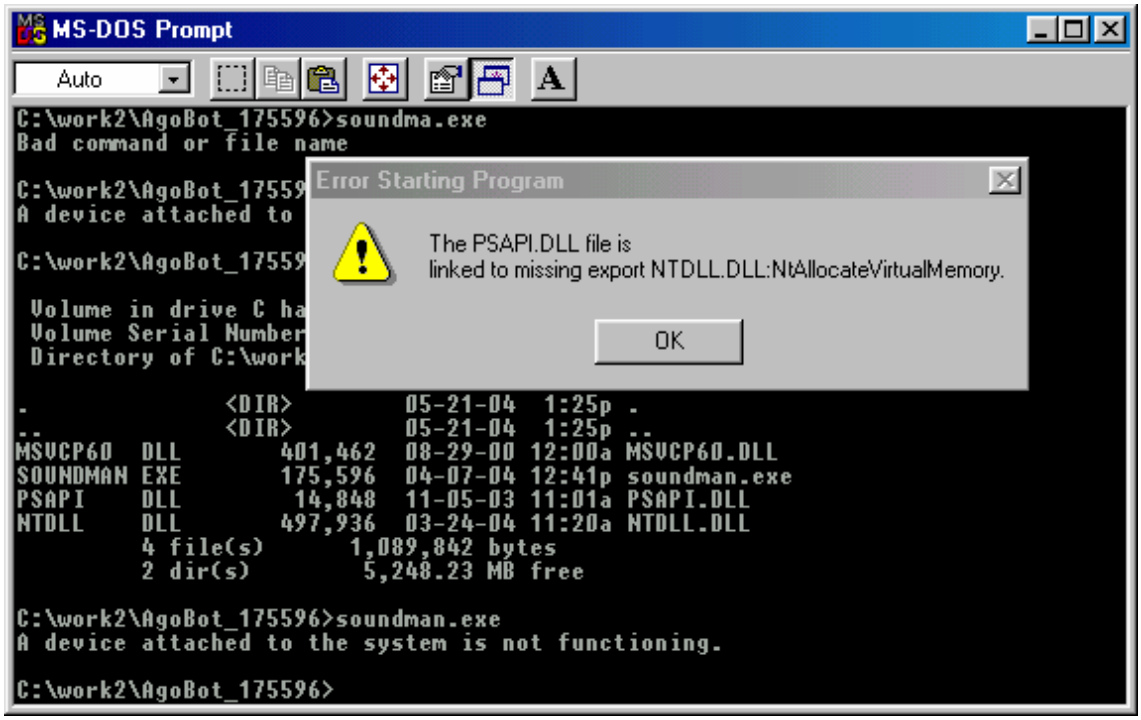
- NTDLL.NtQuerySystemInformation : 작업관리 리스트에서 숨기
- NTDLL.NtResumeThread: 새로운 프로세스 생성시 감염
- NTDLL.LdrGetDllHandle: KERNEL32/ADVAPI32 패치
- KERNEL32.FindFirstFileExW: 파일 찾기 숨김
- KERNEL32.FindNextFileW: 파일 찾기 숨김
- ADVAPI32.EnumServicesStatusA: 서비스 매니저에서 숨기
- ADVAPI32.EnumServicesStatusW: 서비스 매니저에서 숨기
- ADVAPI32.RegEnumKeyExW: 레지스트리 편집기에서 숨기
- ADVAPI32.RegEnumKeyW: 레지스트리 편집기에서 숨기
- IPHLPAPI.GetTcpTableFromStack: NETSTAT에서 숨기
- IPHLPAPI.GetUdpTableFromStack: NETSTAT에서 숨기

윈도우 98/ME 테스트

아직 윈도우 98/ME의 사용이 여전히 높지만 윈도우 9X 계열과 윈도우 NT 계열은 내부적으로 차이점이 많다. 윈도우 98/ME에서 이들 은폐형 악성코드를 실행하면 보통 에러가 발생하며 실행되지 않는다[그림2]. 은폐기법에서 사용하는 API 들은 모두 윈도우 NT 이상에서만 존재하는 기능이기 때문이다.







[그림2] 윈도우 98에서 실행 시 발생하는 에러 화면

결론

최근 알려진 은폐형 악성코드는 다음과 같다.

- Win-Trojan/RtKit(http://info.ahnlab.com/smart2u/virus_detail_1222.html)
- Win-Trojan/HackDef(http://info.ahnlab.com/smart2u/virus_detail_1227.html)
- Win-Trojan/Padodor.45770(http://info.ahnlab.com/smart2u/virus_detail_1404.html)
- Dropper/Haxdoor.39024(http://info.ahnlab.com/smart2u/virus_detail_1407.html)

은폐기법은 웜, 바이러스, 트로이목마의 효과적인 생존 방법 중 하나이다. 윈도우에서 은폐기법은 이미 실제 사용자들을 위협하는 수준이 되었지만 상당수 백신은 메모리에서 은폐형 악성코드를 진단 및 치료해 무력화하는 기능이 빠져있다. 시스템 감시(실시간 감시)에서 이들 웜을 찾아 내는 경우는 있지만 치료를 못하는 경우가 많다. 하지만, 많은 악성코드 제작자들은 백신의 시스템 감시뿐 아니라 안전 모드에서도 자신을 숨기는 형태의 은폐형 악성코드의 제작을 시도하고 있어 앞으로 은폐형 악성코드 진단 기술은 계속 발전해 갈 것이다. 백신 역시 악성코드의 은폐기법을 무력화하기 위해 개선되고 있다. 도스 시절 많이 사용되던 은폐기법은 윈도우에서도 문제가 되고 있다.