ASEC Report 2월

® ASEC Report

2004. 3

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

다양한 악성코드와 Mass Mailer에 의한 피해 증가...

2004년 2월은 무려 686종의 악성코드로부터 피해신고가 접수되어 역대 가장 다양한 악성코드로부터의 피해가 접수된 달로 기록된다. 또한 작년 동월과 비교하여 Mass Mailer를 비롯한 악성 IRCBot으로 인한 피해가 크게 증가하였습니다. 특히 Mass Mailer의 급증은 한국 뿐 아니라 일본, 중국을 비롯한 세계적인 증상으로, 이런 유형의 악성코드가 가장 활발하게 발견되었던 2001년, 2002년과 비슷한 양상을 띠어 다시 한번 Mass Mailer 악성코드의 중흥기가 오는 것은 아닌지 우려가 된다. 다만, 예전의 Mass Mailer에 비해 올해 발견되고 있는 Mass Mailer가 다른 점은 단지 메일을 통해서만 전파되는 것이 아니라, 취약점, P2P 프로그램 등 다양한 전파경로를 함께 가지고 있어 예년보다 능동적인 전파력을 가지고 훨씬 빠른속도로 전파된다는 것이다. 2월에 발견된 악성코드 중 주목할 만한 것은 넷스카이 웜과 베이글 웜이다. 이 웜들은 제작자간 사이버 설전으로 인해 2월에 많은 변형들이 발견되기도 하였다.

2월에는 ASN.1 취약점에 대해 살펴보고 마이크로소프트의 윈도우 2000과 NT 소스코드 유출 사건과 관련된 위험성을 조명해 보았다. 테크니컬 컬럼에서는 백신이 제공되기 전에 웜이나 트로이목마와 같은 악성코드를 수동으로 제거하는 방법과 MBSA 툴을 이용하여 윈도우 패치를 관리하는 방법에 대해서 알아보도록 하겠다.

I. 2월 악성코드 Top 10

작성자 : 정진성 연구원(jsjung@ahnlab.com)

악성코드명	건수	%
Win32/Dumaru.worm.9234	2,981	44.9%
Win32/Netsky.worm.22016	506	7.6%
Win32/Blaster.worm.6176	505	7.6%
Win32/Mydoom.worm.22528	159	2.4%
Win32/AgoBot.worm.197120.C	137	2.1%
Win32/Agobot.worm.104960	128	1.9%
Win32/Netsky.worm.25352	97	1.5%
Win32/Yaha.worm.45568.B	84	1.3%
Win32/Parite	78	1.2%
Win32/Welchia.worm.12800	68	1.0%
기타	1,898	28.6%
합 / %	6,641	100

[표1] 2004년 2월 악성코드 Top 10

이번 달도 지난 1월과 비교해보면 다소 새로운 악성코드가 Top 10에 등장한 것을 알 수 있다. 건수로는 기존에 있었던 Win32/Dumaru.worm.9234(이하 두마루 웜)가 1위를 차지하고 있다. 이는 실제 통계 표본이 될 수 있는 사용자의 피해문의 뿐만 아니라 1월 ASEC Report에서도 언급한 것처럼 웜에 의해 감염된 시스템으로부터 발송되어 접수된 건수도 포함하고 있기 때문에 두마루 웜을 제외하면 2월에 새로 발견된 Win32/Netsky.worm.22016 (이하 넷스카이 웜)과 그 변형들이 강세였던 것을 알 수 있다.

Top 10을 포함 2월 악성코드의 전체적인 피해유형을 본다면 Mass Mailer와 Worm들로 양분 되어 있는 것을 볼 수가 있는데, 작년 동월과 달리 올해는 뚜렷이 Mass Mailer를 비롯하여 악성 IRCBot 유형의 웜들이 그 피해와 수적으로 트로이목마를 압도하여 출현하고 있다. 특히 Mass Mailer는 이러한 유형이 가장 유행했던 (즉, 피해문의가 많았던) 2001년, 2002년과 비슷한 양상을 보이는 것 같아 다소 우려가 된다.

실제로 이 보고서를 작성하는 날짜기준으로 넷스카이 웜은 9가지의 변형이 무려 15일 사이에 발견, 보고되었다. 이렇게 많은 변형이 발견된 원인에 한 몫을 하는 것 중 하나는 다른 악성코드의 제작자들끼리의 설전이 한몫을 한 것으로 보여진다.

단시일에 많은 피해를 입히고 많은 변형이 발견된 넷스카이 웜

이처럼 피해문의가 많았던 넷스카이 웜을 좀더 알아보면 다음과 같다.

- 자체 SMTP 엔진을 가지며 자신을 첨부한 메일을 발송
- 맵핑된 네트워크 드라이브로 자신을 복사
- P2P 응용 프로그램의 공유폴더에 자신의 복사본 생성
- 다른 웜이 생성한 레지스트리 삭제 (더 이상 실행되지 않도록)

넷스카이 웜이 많이 확산된 가장 확실한 원인 중 하나는 분명 메일을 통한 확산일 것이다. 넷스카이 웜은 메일 발송시에 수집된 메일주소의 도메인에 대한 MX 쿼리를 요청하여 정확한 MX 주소를 얻어온 후 이를 토대로 메일을 발송하게 된다. 이는 불필요한 MX 쿼리를 요청하므로 이 역시 네트워크 부하를 일으키기도 한다.

또한 P2P를 이용한 전파시에는 다른 웜들도 그렇지만 P2P 응용 프로그램의 프로토콜 자체를 이용하는 것이 아니라 단지 해당 응용 프로그램의 공유폴더에 웜을 복사해두는 것이다. 이를 일반적인 전파 원리로 본다면 넷스카이 웜은 좀더 특별한 방법을 사용하였다. 그것은 이전까지 P2P 웜들은 특정한 P2P 응용 프로그램을 대상으로만 하였다. 즉, 웜 자신을 복사하려는 폴더는 특정 P2P 응용 프로그램 공유폴더에 맞게 웜 내부에 하드코딩 되었다.

그러나 넷스카이 웜과 그 변형들 그리고 이를 모방한 다른 웜들은 'shar' 라는 문자열이 존재하는 폴더는 무조건 웜의 복사본을 생성해 둔다. 이것은 전파에 약간의 제약 (영어가 아닌 OS 에서는 큰 위협이 되지 못함)이 있지만 간단한 아이디어만으로 다수의 P2P 응용 프로그램을 대상으로 삼았다는 것이다. 이는 역시 자신을 널리 전파하려고 하는 의도로 보여진다.

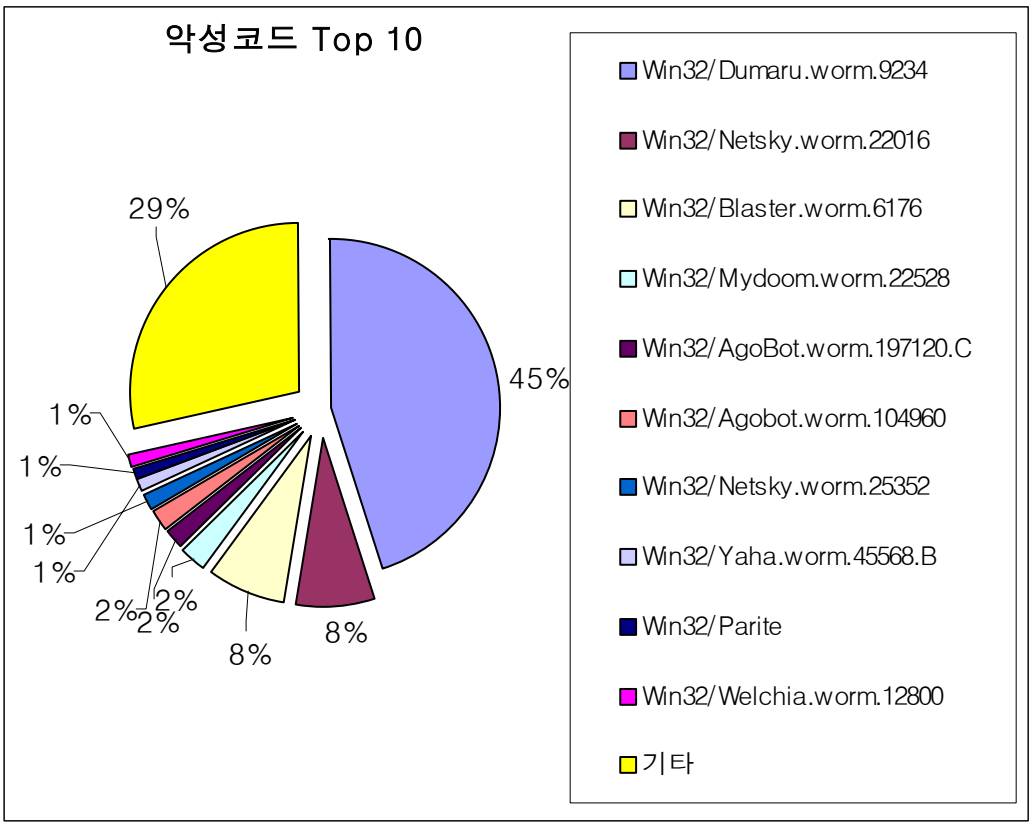
위 P2P 전파방법은 약간의 제약은 있지만 대부분의 악성코드들이 영어권의 나라에서 제작되어지고 전파되는 것을 본다면 이는 새로운 전파방법으로 자리잡을 수도 있을 것이다.

넷스카이 웜에서 볼 수 있는 특이한 점은 다른 악성코드가 생성해둔 레지스트리 값을 삭제한다는 것이다. 이러한 유형 역시 처음 보고된 것은 아니지만 넷스카이 웜은 거의 경쟁적으로 다른 악성코드가 생성한 레지스트리 값을 삭제한다. 이렇게 되면 웜 자체가 삭제된 것은 아니지만 재부팅을 하면 실행되지 못하므로 결과적으로는 다른 웜을 실행하지 못하게 하는 꼴이 된다.

또한 웜은 맵핑된 네트워크 드라이브에 자신을 복사한다. 하지만 공유폴더를 찾기 위해 고유폴더(자원)를 스캔하지는 않는다. 이 방법을 사용할 경우 불필요한 곳까지 웜은 자신을 복사

하려고 시도할 것이며 이는 곧 쉽게 발견되는 결과를 초래하기도 하기 때문으로 추측된다.

다음은 2월의 악성코드 Top 10 의 분포를 [차트1]로 나타내었다.

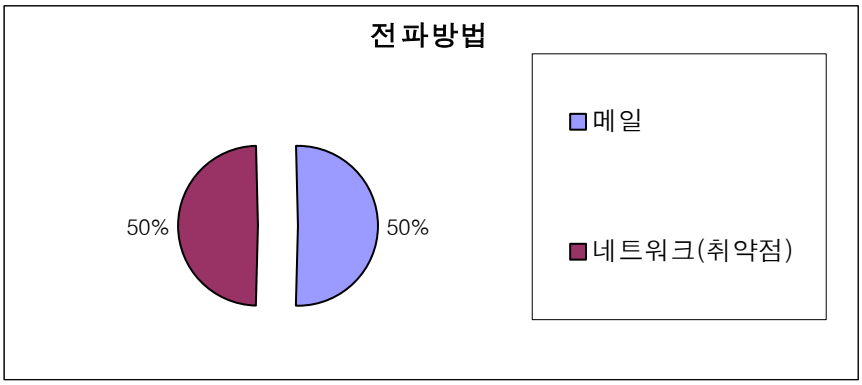


[차트1] 2004년 2월 악성코드 Top 10

1월과 비교하여 두마루 웜이 차지하는 비율은 약간 줄어들었다. 이러한 원인은 상대적으로 다른 악성코드 피해 비율이 늘어났기 때문인 것으로 보인다. 특히 위에서 기술한 넷스카이 웜은 새로이 등장하였고, 블래스터 웜은 지난달과 동일한 비율을 보여주고 있다. 또한 순위 권내에 다른 웜들도 역시 지난달에 비해 다소 피해규모가 증가하였다.

Mass Mailer 웜의 증가

악성코드 Top 10은 주로 어떠한 감염경로를 가지고 있는지 [차트2]에서 확인해 보기로 한다.



[차트2] 악성코드 Top 10 의 전파방법별 현황

이번 달은 RPC DCOM 과 같은 특정 취약점을 따로 분류하지 않고 네트워크라는 항목으로 모두 같이 묶었을 때, [차트2]와 같이 이번 달은 메일과 네트워크가 동일한 비율로 양분되어 있는 것을 알 수가 있다. 특히나 위에서 언급한 것처럼 점점 Mass Mailer가 그 종류나 확산 정도에 따라서 점점 늘어나는 것을 알 수 있다.

또한 네트워크를 이용한 악성코드는 늘 그랬던 것 처럼 AgoBot 웜 변형들이 그 주류를 이루고 있으며 Win32/Welchia.worm.12800 (이하 웰치아 웜)이 원형 발견후 몇 개월만에 변형이 발견되어 관심을 받았다. 웰치아 웜은 다양한 MS 윈도우 취약점을 이용하여 전파되는데 이용하는 취약점만해도 4가지나 된다. 이와 같은 복합적인 취약점 이용도 점점 다른 악성코드가 모방하는 형태로 발전하여 더 많은 악성코드를 양산하게 될 것이다. 그 시작이 바로 AgoBot 웜이다.

즉, 복합적인 형태의 악성코드에서 복합적인 취약점을 가진 악성코드로 점점 발전하고 있는 것이다. 복합적인 형태라 하는 것은 File Infector + Mass Mailer(Network work) + BackDoor 형태를 말하는 것이다. 이제는 이와 같은 복합적인 형태를 가지거나 단독적인 형태를 가지고 있더라도 하나 이상의 취약점을 이용한다는 것이다. 여러가지 취약점을 이용하면 할수록 그 악성코드는 보다 널리, 보다 빠르게 확산 될 수 있는 것이다.

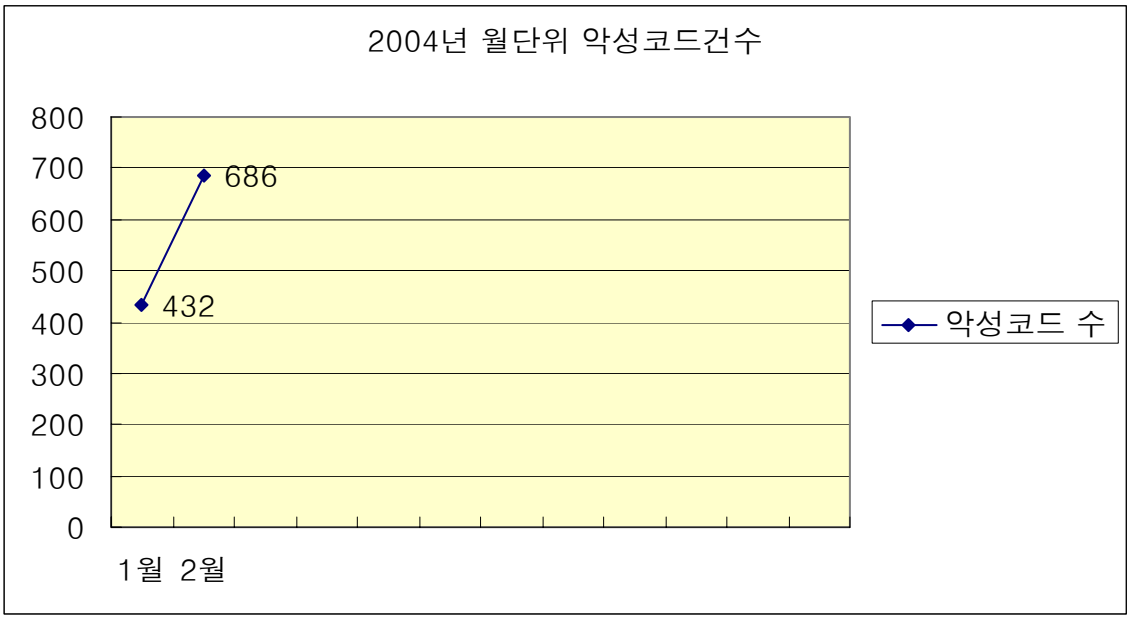
새로운 취약점은 그게 어떤 OS에서 동작하는 형태이던지 매일 새로운 것이 보고 되고 있다. 또한 블래스터 웜 이후 이러한 취약점은 '0Day-Exploit' 라는 용어를 탄생 시켰다. 이는 곧 취약점을 이용한 새로운 악성코드를 빠른시간내 양산 할 수 있다라는 것을 의미한다.

역대 가장 다양한 악성코드로부터의 피해

2월의 피해문의 악성코드 종류의 수는 무려 686종이다. 이는 지금까지 집계상 최고의 수치이다. 또한 이는 불과 지금까지 최고 수치 였던 1월의 결과를 한 달만에 다시 역전시킨 것이

기도 하다. 이것은 또한 직, 간접적으로 사용자들은 686종이나 되는 수백가지의 악성코드들에 시달리고 있다는 것이기도 하는 것이다. 686종류라는 수치는 작년 동월에 비하여 52.6% 가량 증가한 수치이다. (참고로 작년 동월은 359 종)

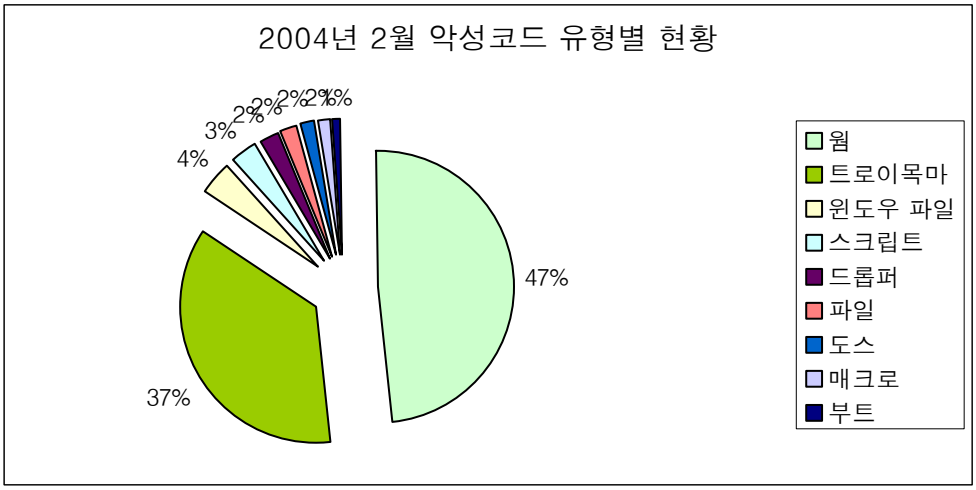
종류가 급격히 증가한 원인으로는 AgoBot 과 같은 악성 IRCBot 변형의 급격한 증가를 들 수 있겠다.



[차트3] 2004년 월별 피해신고 악성코드수

686종류나 되는 악성코드들은 어떠한 유형들이 존재하는지 살펴보면 웜 > 트로이목마 > 윈도우 파일 > 스크립트 > 드롭퍼 > 파일 > 도스 > 매크로 > 부트 순서이다.

위에서 '파일'은 주로 악성코드가 만들어낸 Textimage 나 배치파일등을 '파일' 이라는 별도의 항목으로 분류하였다.



[차트4] 2004년 2월 악성코드 유형별 현황

[차트4]에서도 보여지듯이 2월에 피해를 입힌 악성코드 중 '웜'이 전체의 반 정도의 비율을 차지하고 있는 것을 볼 수 있다(수치로는 무려 329 종이다). 이중에서 AgoBot 과 같은 악성 IRCBot 형태의 웜은 약 250 종이 넘게 피해를 입혔다. 나머지는 Mass Mailer 또는 취약점을 이용한 네트워크 웜들이 차지하고 있다.

이 많은 웜들중에서 특이한 형태가 하나 있는데 일본에서 접수된 Win32/Antinny.worm.383488 이다. 다소 생소하지만 일본에서 제작 되어진 이 웜은 일본어 OS 에서만 정상적으로 동작하며 일본내에서 사용되는 P2P 응용 프로그램의 공유폴더에 웜 복사본을 생성한다. 또한 해당 공유 프로그램의 Cache 폴더내 파일을 삭제함으써 결과적으로 다운 받는 파일을 삭제하는 결과를 가져온다. 또한 이 웜이 특이하다고 말한 것은 압축 관련 모듈을 가지고 있다는 것이다. 다소 큰 크기를 가지고 있는 (383,488 바이트) 웜은 LZH 와 ZIP 관련 모듈을 가지고 있으며 웜 자신이 이 모듈을 이용하여 자신을 압축 할 때 이용한다.

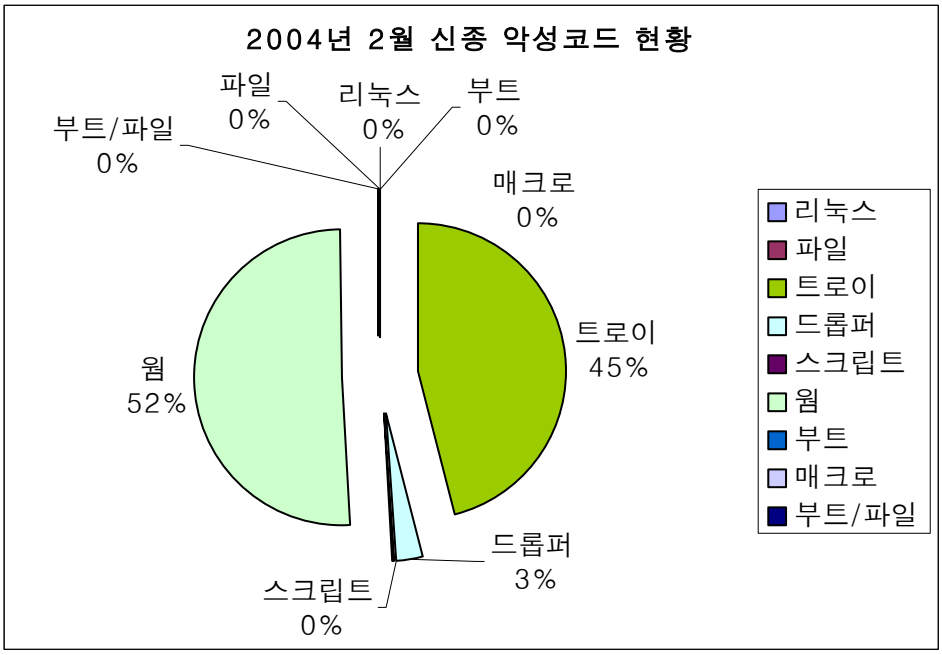
Ⅱ. 2월 국내 신종 악성 코드 발견 동향

작성자 : 정진성 연구원 (jsjung@ahnlab.com)

2월 한달 동한 접수된 신종 악성코드의 건수는 [표1], [차트1]와 같다.

리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	합계
0	1	130	8	1	146	0	0	0	286

[표1] 2004년 2월 유형별 신종 악성코드 발견현황



[차트1] 2004년 2월 신종 악성코드 발견현황

Mass Mailer 웜 변형 발견 강세

신종 악성코드들 중 역시 웜이 가장 많은 비율을 차지하고 있는 것을 알 수가 있다. 그 중에서도 새로운 Mass Mailer 가 2월에는 많이 발견, 보고 되었다. 다음과 같은 것들이 있었다.

- Win32/Netsky.worm 변형들 (이하 넷스카이 웜)
- Win32/Mydoom.worm 변형들 (이하 마이둠 웜)
- Win32/Bagle.worm 변형들 (이하 베이글 웜)

특히 마이둠 웜은 소스가 공개되어 많은 변형들이 발생했다. 또한 소스 공개로 인하여 아이

러니 하게도 마이둠 웜에 감염된 시스템을 찾아 웜을 제거하는 웜이 다수 출현 하기도 하였다.

베이글 웜은 이미 1월 말경 처음 원형이 보고 되었고 거의 한달여 만에 변형이 출현하였다. 2월말경에 집중적으로 발견된 베이글 웜은 넷스카이 웜과 더불어 많은 발견, 보고가 있었으며 연구소내 Virus Blocking Service (VBS)에서도 상당수 차단되었었다.

베이글 웜을 살펴보면 다음과 같은 증상이 있다.

- 자체 SMTP 엔진을 가지고 있으며 이를 이용하여 자신이 첨부된 메일을 발송한다.
- 보낸이는 Spoofed 되어 실제 보낸이를 알 수 없게 한다.
- 특정한 TCP/ 포트를 오픈한다.
- 안티 바이러스 제품의 업데이트 관련 프로세스를 강제종료한다.

특히 베이글 웜은 TCP/ 포트를 이용하여 웜을 업데이트 할 수 있으며 파일/실행/삭제와 같은 원격제어도 가능하다. 무엇보다도 이 웜의 변형들은 안티 바이러스의 제품군에 대한 업데이트 프로세스를 강제로 종료하는 기능이 있는데 이 기능은 매우 위협적으로 판단된다. 이 포트를 이용해서 웜은 자신을 삭제하거나 업데이트 할 수도 있으며 나아가 누군가에 의해서 원격제어를 당할 수 있기도 하다. 행여 감염된 시스템들이 DDoS의 Agent 로 사용되면 대규모의 네트워크 불통사태가 발생할 가능성도 있다.

소위 anti-anti-virus 라는 기법중에 하나인 이것은 악성코드가 안티 바이러스 제품들을 타켓으로 공격하는 기능을 통틀어 말하는 용어이다. 위와 같이 프로세스를 강제로 종료할 경우 웜에 감염된 시스템은 안티 바이러스 프로그램을 최신엔진(패턴)으로 업데이트 하지 못하게 된다. 따라서 결국 웜을 치료할 수 있는 엔진을 업데이트 할 수 없게 되는 현상이 발생하는 것이다.

위에서도 언급한 것 처럼 위와 같은 Mass Mailer 들로 하여금 올해는 2001년, 2002년 때와 비슷하게 Mass Mailer들이 급증할 것이라는 추정을 해보게 된다. 무엇보다는 이러한 웜들은 많은 시스템을 감염시켰고 역시 위에서 언급한 것처럼 복합적인 형태를 가지고 있다.

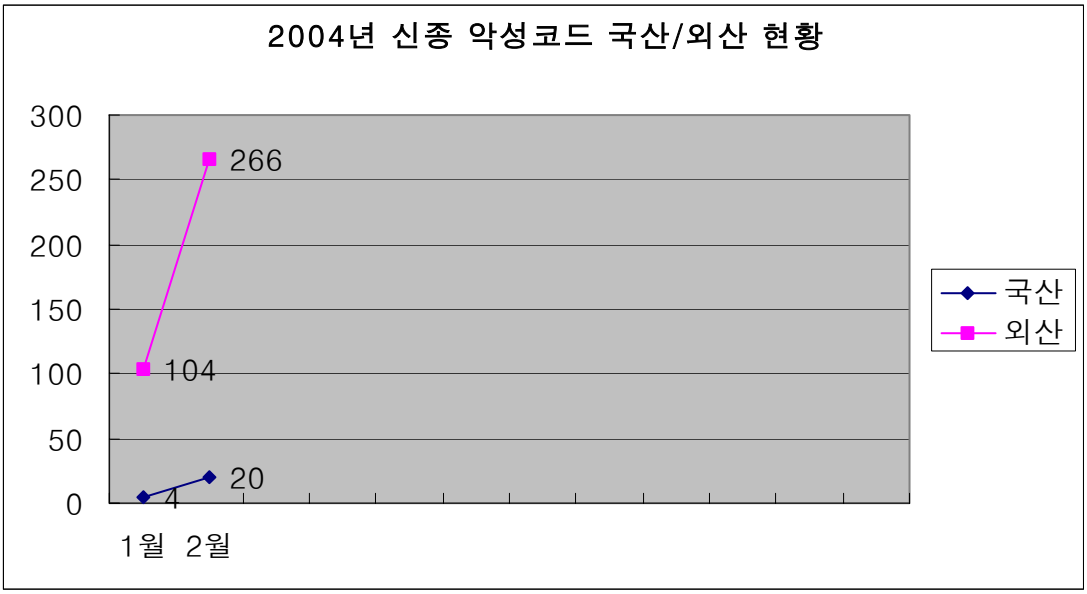
Mass Mailer 웜에 이어 다양한 취약점을 이용한 Welchia 웜도 다양한 변형이 발견, 보고 되었다. 원형에 비해 다른 취약점이 몇 개 더 추가 되었으며 특정 사건을 연상하는 문장을 가지고 있다. 이 문장을 Html 파일과 같은 몇몇의 스크립트 파일에 덮어쓰는 증상도 가지고 있다.

다형성 AgoBot 웜의 출현

또한 가장 많은 변형 건수를 가지고 있는 AgoBot 경우는 다형성 형태가 출현하였다. 처음에 발견된 다형성 AgoBot은 몇가지의 암호화 방법을 사용했지만 다른 변형이 발견될수록 더 많은 암호화 방법을 사용하였다. 이 다형성 기법은 실제 AgoBot 웜 코드에 있는 형태가 아니라 별도의 Tool로 보여지는 형태로 되어 있었다. 이는 마치 도스시절의 평범한 (일반적인) 바이러스가 다형성 엔진에 의해서 수백만가지의 변형으로 다시 만들어지는 결과와 매우 비슷한 경우로 보여진다. 나아가 AgoBot의 발전방향을 점쳐보면 안티 바이러스의 진단으로부터 피하거나 쉽게 사용자들에게 발견되지 않도록 하기 위해서 Stealth 기법을 사용할 것으로 예상된다.

이렇듯 악성코드들은 점점 발전하고 있으며 나아가 안티 바이러스 제품들도 악성코드의 대응 관점에서 빠르게 변화 되어야만 살아 남을 수 있을 것이고 사용자들로부터 신뢰를 받을 수 있을 것이다.

다음은 신종 악성코드들의 국산/외산 현황을 보여주고 있다. 지난달에 비해 국산과 외산 모두 급격히 증가한 것을 볼 수가 있다.



[차트2]2004년 제작지별 신종 악성코드 현황

이는 지난달에 비해 39.1% 증가한 수치이다. 국산에서 제작된 악성코드의 수는 1월 4건에서 2월은 20건으로 역시 크게 증가하였다. 증가한 원인으로는 국내 제작의 트로이목마의 증가였는데 이 트로이목마의 유형은 대부분은 홈페이지의 시작 페이지를 특정한 사이트로 변경하는 형태이다. 또한 여전히 문제가 되고 있는 SPAM Mailer들도 꾸준히 새로운 변형들이

발견 되었다. 이 모든 것이 성인광고 목적으로 사용되어지는 것들이다. 악성코드 다음으로 사용자들이 심각하게 느끼는 것이 바로 SPAM과 애드웨어 일 것 이다.

이러한 사용자들의 요구와 악성코드의 대응관점에서의 제품개발 결과로 대부분의 안티 바이러스 제품들은 애드 온 형태 또는 자체적으로 Anti- SPAM과 애드웨어 차단 기능을 탑재하고 있다. 실제로 악성코드에 감염되지 않은 사용자는 많지만 SPAM과 애드웨어에 의해 피해를 당해보지 않는 사용자들이 없을 만큼 심각한 수준에 와 있다.

III. 2월 신규 보안 취약점

작성자 : 정관진 연구원(intexp@ahnlab.com)

2004년 2월, 어김없이 시간의 흐름은 계속 되고 있다. 2월에 주목할 만한 사건중의 하나가 윈도우 소스코드의 유출이다. 건물을 짓기 위해서 필요한 것이 무엇인가? 바로 오랜 시간과 정성을 들여서 만드는 설계도면이다. 이 설계도면이 없이는 건물을 지을 수가 없는 것이다. 이렇게 건축을 주 업으로 하는 기업들에게는 설계도가 중요한 것이고, 소프트웨어를 제조하는 기업에게는 소스코드가 중요한 것이다. 한 마디로 소스코드는 건물의 설계도와 같은 것이기 때문이다. 이번 2월호에서는 소스코드의 유출과 관련한 위험을 조명해 보고 ASN.1 취약점을 살펴보도록 하겠다.

ASN.1 취약점을 이용한 원격 코드 실행

마이크로소프트사는 2004년2월10일(미국시간) MS04-007 패치를 발표하면서 관리자들의 빠른 패치 업데이트를 권고하였다. 이번에 발표된 ASN.1(Abstract Syntax Notation)의 취약점은 원격에서 임의의 코드를 실행 가능하게 만들어 커다란 위험성을 내포하고 있다. 이 취약점은 ASN.1 라이브러리의 버퍼를 제대로 체크하지 않아 버퍼오버플로우를 이용한 공격이 가능하게 되는 것이다. 일단 공격에 성공하게 되면 시스템권한으로 임의의 코드 실행이 가능하게 되어 계정생성, 소프트웨어 설치, 데이터 변조, 삭제등의 명령 수행이 가능하다. ASN.1은 다양한 시스템간의 데이터 교환을 위하여 각종 문자열, 숫자, 기타 데이터들에 대한 표현 방식을 정의한 프로토콜이다. 윈도우 시스템을 운영하는 관리자들은 안철수연구소에서 배포하는 ASEC Advisory를 참고하여 업데이트 할 것을 권고한다.

[ASEC Advisory] Microsoft ASN.1 라이브러리 취약점
http://b2b.ahnlab.com/securityinfo/info_view.jsp?seq=5563

마이크로소프트 윈도우 2000 과 NT 소스코드 유출에 따른 위험성

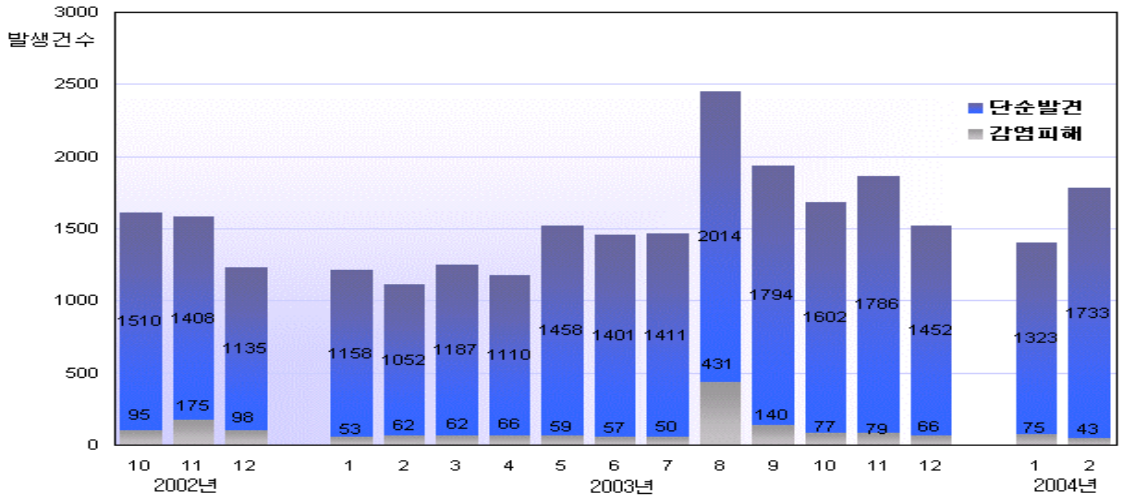
전세계 PC의 운영체제로 폭 넓게 쓰이고 있는 마이크로소프트사(이하 MS)의 윈도우 2000과 NT 소스코드가 유출되었다는 소식은 큰 사건이 아닐 수 없다. 현재 인터넷상에 공개된 코드는 약 600M 정도로 전체 운영체제 코드에 비하면 작은 일부분이지만 이것이 시사하는 바는 크다. 우선, 어떻게 하여 이 소스코드가 유출될 수 있었나 하는 점이다. 더군다나 일반 응용프로그램의 코드가 아닌 운영체제의 코드라는 것이며 핵심 정보가 일반인을 포함하여 해커에게까지도 그 정보가 노출된 것이다. 기업의 입장에서는 크나큰 문제가 아닐 수 없다. 물론, 이번 소스코드 유출 사건은 MS의 협력업체를 통해 유출되었다고는 하나 다시 한번 기

업의 보안이 얼마나 중요한 것인지를 새삼 느끼게 해 주는 일례라고 할 수 있다.
금번 MS 뿐만 아니라 기업에서는 보안정책 등 기업의 정보를 외부로부터 안전하게 지키기 위한 방안들을 강구해 보아야 할 것이다. 어찌되었든 이미 윈도 소스코드는 인터넷 상에서 불법적으로 유통되고 있으며, 이에 대한 위험은 감수해야 한다. 이 소스코드를 악용하려는 사용자는 소스코드를 분석해 취약점을 찾아내려고 노력할 것이며, 만약 취약점이 존재하지 않는다고 하더라도 소스코드에서 사용되었던 코드의 패턴 등 다양한 추가적인 정보는 해커들에게 향후 또 다른 취약점을 찾아내는데 일조할 수도 있을 것이다. 분명한 것은 해킹위험이 존재하는 것은 사실이며, 향후 이번 소스코드를 통한 취약점 발견으로 작년 SQL_Overflow 웜(일명 Slammer 웜)과 같이 커다란 사건이 일어나지 않으리라는 것은 배제할 수 없다. 이미 이러한 사실에 동조하듯이 2월15일 SecurityTracker.com 사이트에 유출된 소스코드를 이용하여 취약점을 발견하였다는 내용의 글이 게재되었다. 이 글에 따르면 조작된 비트맵파일을 이용하여 사용자의 컴퓨터를 제어할 수 있다는 내용으로, 인터넷 익스플로러를 이용하여 해당 파일을 로드하는 경우 에러를 유발시켜 임의의 코드를 실행할 수 있게 된다는 점이다. 이것은 어떻게 보면 시작에 불과할지도 모른다. 다만 우리는 이것이 한낮 기우에 끝났으면 하는 것이 바람일 것이다.

Ⅳ. 2월 일본 피해 동향

작성자 : 김소헌 연구원(sohkim@ahnlab.com)

일본 IPA/ISEC의 악성코드 피해 추이 통계에 의하면 한국의 경우와 마찬가지로 올해 1-2월 두 달 동안 발생한 악성코드 피해가 작년 동기간과 비교하여 현저하게 늘어난 것으로 파악되었다.



[표1] 일본의 월별 악성코드 피해 통계

[표1]은 일본에서 발생한 악성코드 피해 상황의 월별 통계를 나타낸 것이다.
올해 1, 2월 발생한 악성코드 피해 건수는 각각 1,323 건과 1,733건으로 2003년 1월과 2월에 발생한 피해 건수인 1,158건과 1,152건에 비해 800여건 이상이 증가한 것이다. 이러한 악성코드 피해 건수 증가의 원인은 W32/Mydoom(AhnLab 명 : Win32/MyDoom.worm, 이하 마이둠 웜)과 W32/Netsky(AhnLab 명 : Win32/Netsky.worm, 이하 넷스카이 웜)등 1월 말부터 발생한 Mass Mailer 웜의 영향으로 인한 것이다. 그러나 실제 감염되어 피해를 당한 경우는 작년과 비슷함을 알 수 있고 결과적으로 악성코드 전파의 강도는 심해졌으나 이로 인한 감염 피해가 심각한 상황은 아니라는 것을 유추해 볼 수 있다.

일본 유행 악성코드 유형별 발생현황

2004년 2월 일본에서 가장 유행한 악성코드는 마이둠 웜으로 나타났다. 마이둠 웜은 2004년 1월 27일 최초로 발생하여 전 세계에 급속히 전파된 이메일을 통해 전파되는 웜이다. 마이둠 웜은 2월 들어서도 여러 가지 변형의 형태로 나타나 가장 많은 신고 건수를 기록하였다.
2월에 일본에서 발견된 주요 신종 악성코드는 넷스카이 웜과 W32/Parite, W32/Bereb 등이

있다. 이중 넷스카이 웜 Mass Mailer 웜으로 150건의 피해 보고가 접수되어 있는 상태이다.

Window/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Mydoom	637	Xm/Laroux	13	VBS/Redlof	52
W32/Klez	171	WM/Cap	2	Wscript/Fortnight	14
W32 Mimail	163	X97M/Ethan	1	VBS/Loveletter	2
W32/Netsky	150	W97M/Story	1	VBS/Haptime	1
W32/Bugbear	103			VBS/Netlog	1
W32/Bagle	95				

일본 악성코드의 주요 감염경로

한국과 달리 일본에서 발생한 악성코드 감염의 주요 감염경로는 이메일이다. [표2]는 악성코드에 의해 피해를 당한 사용자들의 주요 감염경로에 대한 통계이다. 2004년 2월의 메일에 의한 감염 통계 수치는 95.4%로 거의 대부분의 감염피해가 메일을 통한 것이라는 것을 알 수 있다.

이메일을 통한 감염 이외에 악성코드의 전파 경로로 주로 사용되는 매체는 네트워크이다. 전월과 비교하여 매체의 이용도는 감소하였지만 메일을 제외한 다른 매체를 통한 것보다 두 배가 넘는 사용률을 보여준다.

또한 작년 2월의 감염경로 통계와 비교하여 보았을 때 가장 크게 달라진 점이 네트워크를 통해 전파되는 악성코드가 크게 증가했다는 것에 주목할 필요가 있다.

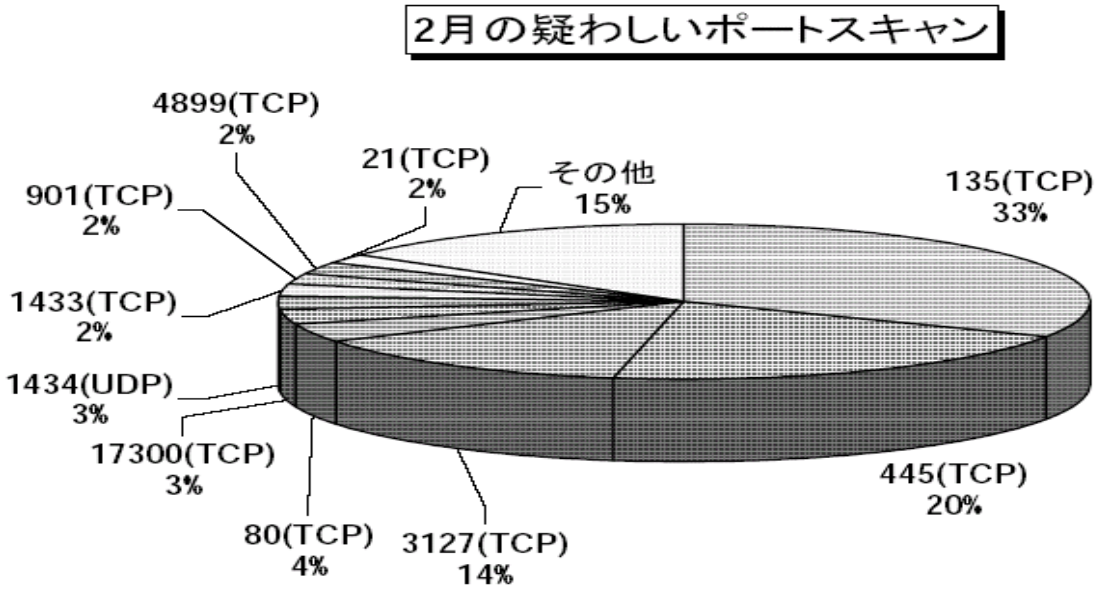
감염경로	피해 건수					
	2004년 2월		2004년 1월		2003년 2월	
메일	1,654	95.4%	1,247	94.2%	1009	95.9%
외부 감염	19	1.1%	6	0.5%	15	1.4%
다운로드	17	1.0%	1	0.1%	10	1.0%
네트워크	34	2.0%	58	4.4%	0	0%
기타	9	0.5%	11	0.8%	18	1.7%

[표2]악성코드 주요 감염경로

일본 네트워크 트래픽 현황

[차트1]은 2004년 2월 일본에서 발생된 네트워크 트래픽의 포트 유형별 사용량을 나타낸 것이다. 주목할만한 점은 135 포트와 445 포트의 사용량이 다른 포트에 비해 현격히 높다는 것이다. 이 두 포트는 윈도우 시스템에서 주로 사용되는 포트들이지만 블래스터 웜과 같은 RPC 취약점을 이용하여 전파되는 웜에서 사용되는 포트이기도 하다. 주목할만한 사항은 전

월에 전체 사용량의 17%를 차지했던 139번 포트에 대한 트래픽이 현저하게 줄어들었다는 것이다. 이는 관리목적 공유폴더의 패스워드 취약점을 이용하여 전파되는 웜에 의한 트래픽이 아직 많이 존재하는 우리나라와 비교되는 점이라고 할 수 있다.
또한 TCP 3127 포트에 대한 트레픽이 급격하게 발생하였는데 이는 마이둠 웜에 감염된 시스템에서 열리는 포트들 중 하나로 마이둠 웜 감염의 심각성을 짐작할 수 있게 해준다.



[차트1]2월 일본에서 발생된 네트워크 트래픽 포트 유형별 사용량

V. 2월 중국 피해 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

2004년 2월 중국의 악성코드 동향은 메일로 전파되는 웜의 형태인 Mass Mailer 웜이 TOP 5의 1위에서 5위까지 기록되는 형태를 보이고 있다. 또한 5종의 웜 모두 공통적으로 현재까지도 다양한 변종들이 계속 발견이 되었거나 발견되고 있다는 점이 특이하다. 중국에서의 이러한 동향은 한국을 포함하여 전세계적으로 비슷한 동향을 보일 것으로 추측이 되며 작년을 기준으로 보아 Mass Mailer의 확산이 특히나 많았던 한 달이라는 점도 특이하다고 볼 수 있다.

순위 변화	2 월	Rising	CNCVERC
(-)	1	Worm.Novarg	Worm_Mydoom
(-)	2	Worm.mimail	Worm_Mimail
New	3	Worm.Netsky	Worm_Netsky
(-1)	4	Worm.Lentin	Worm_lentin
New	5	Worm.BBeagle	Worm_Bbeagle

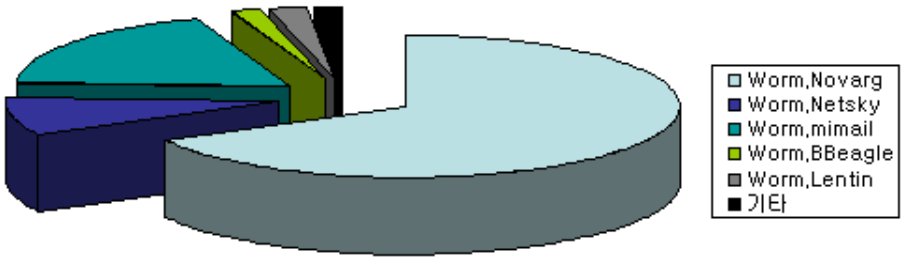
[표1]2004년 2월 중국의 악성코드 피해 TOP 5

위 [표1]의 악성코드 TOP 5는 2월 한달 동안 중국 로컬 백신업체인 라이징(Rising)사와 정부연구기관인 중국국가컴퓨터바이러스대응중심(China National Computer Virus Emergency Response Center, 이하 CNCVERC)의 통계를 나타낸 것이다. 두 곳의 통계가 동일하며 다만 감염 신고 건수와 기타 악성코드의 감염 건수에서만 차이를 보일 뿐이다.

Mass Mailer 웜의 강세

악성코드 TOP 5의 순위상으로는 지난 1월 말에 발견되어 현재까지 H형의 변형까지 발견된 Worm.Novarg(AhnLab 명 : Win32/MyDoom.worm 원형 및 변종)과 작년 이후 현재까지 변형이 발견되며 꾸준히 신고가 되고 있는 Worm.mimail(AhnLab 명 : Win32/Mimail.worm 원형 및 변종)이 지난 달에 이어 순위변동 없이 각각 1위와 2위를 차지하고 있다. 그러나 Worm.Novarg와 Worm.mimail은 2월에 등장한 새로운 웜 들로 인해 지난 달과 비교하여 그 감염건수가 줄어 들었다고 볼 수 있으나 아직까지도 확산이 지속적으로 진행되고 있는 것으로 분석된다. 현재까지도 TOP 5에 지속적으로 등장하는 Worm.Lentin(AhnLab 명 : Win32/Yaha.worm 원형 및 변형)은 한 계단 하락한 4위를 차지하고 있으며 감염건수 역시 지난 달과 비교하여 많이 줄어 든 것으로 보고되고 있다. 3위와 5위는 2월에 새로 등장한 악

성코드들이 차지하고 있으며 이 두 웜 역시 지속적인 변형이 발견되고 있는 Mass Mailer 종류이다. 3위를 차지하고 있는 Worm.Netsky(AhnLab 명 : Win32/Netsky.worm 원형 및 변형)은 현재까지 H형의 변형까지 발견되었으며 그 원형은 2월 16일 밤 유럽에서 최초 발견된 이후 급속한 확산이 진행되었다. 중국에서는 17일 오전에 최초 감염신고가 있었던 것으로 보고되었다. 5위에는 Worm.Netsky와 거의 비슷한 시기에 발견되어 K형의 변형까지 발견된 Worm.BBeagle(AhnLab 명 : Win32/Bagle.worm 원형 및 변형)이 차지하고 있다.



[표2]2004년 2월 악성코드 피해분포

전체 분포를 나타낸 [표2]는 감염신고 건수를 백분율로 구분한 것이다. 악성코드 피해 TOP 5 중 1위인 Worm.Novarg이 67%를 차지하고 있으며 2위인 Worm.mimail은 19%, 3위인 Worm.Netsky 8.2%, 4위인 Worm.Lentin 2.20%, Worm.BBeagle이 1.6%를 차지하고 있으며 이 외에 기타 악성코드들 1.5%를 차지하고 있다.

그 외 1.5%를 차지하고 있는 기타에 포함된 악성코드들에는 총 4종이 차지하고 있다. 트로이목마의 한 종류로 사용자의 개인정보를 특정 메일 주소로 전송하는 Trojan.Legend.Syspoet(AhnLab 명 : Win-Trojan/Lemir 원형 및 변형)이 0.7%를 차지하고 있다. Trojan.Legend.Syspoet은 2월 마지막 주에 처음 발견되어 실제 연구소의 중국 내 협력사로부터 해당 악성코드에 대한 문의가 있었다. 그리고 지난 달 악성코드 TOP 5에서 4위를 차지하였던 Worm.Klez.L(AhnLab 명 : Win32/Klez.worm 원형 및 변형)이 감염신고가 많이 줄어들어 0.65%를 차지하고 있다. 2월 둘째 주에 최초 신고된 Trojan.Binghe2004(AhnLab 명 : Win-Trojan/GDoor.272991)이 0.1%를 차지하고 있다. Trojan.Binghe2004는 기존에 발견된 Trojan.Binghe(AhnLab 명 : Win-Trojan/GDoor 원형)의 새로운 변형이며 TCP/7626 포트를 사용하여 외부에서 원격제어가 가능해 질 수 있으며 전형적인 윈도우용 트로이목마 형태로서는 제법 많은 감염 신고가 보고 되었다. 마지막으

로는 기존에 알려진 Worm.Welchia(AhnLab 명 : Win32/Welchia.worm.10240)의 변형들인 Worm.Welchia (AhnLab 명 : Win32/Welchia.worm.12800 및 변형)이 0.15%를 차지하고 있으며 현재까지도 꾸준히 변형이 발견되고 있다.

글머리에서 이미 언급하였지만 2월에는 특히나 많은 Mass Mailer들이 발견되고 급속한 확산으로 유달리 많은 피해가 발생하였다. 또한 변종 역시 거의 매일 발견되어 안철수연구소 시큐리태응센터는 매일 발생하는 긴급대응으로 인해 매우 분주한 한달을 보내었다. 현재도 진행형인 Worm.Netsky와 Worm.BBeagle이 어디까지 변종이 등장할 지는 알 수가 없으나 그 피해만은 더 이상 나타나지 않기를 바란다.

VI. 테크니컬 컬럼 1 – 악성코드 수동 조치법

작성자 : 차민석 연구원(jackycha@ahnlab.com)

현재까지 백신은 웜, 바이러스, 트로이목마로 대표되는 악성코드에 가장 효과적인 프로그램이지만 이미 알려진 악성코드만 진단/치료(삭제) 할 수 있기 때문에 신종에 대해서는 무력하다. 최근 폭발적으로 증가하는 악성코드는 백신이 아무리 빨리 업데이트되어도 백신이 업데이트 되기 전에 피해자가 발생하기 마련이다. 최근의 악성 코드는 대부분 웜, 트로이목마로 바이러스와 달리 독립적인 파일로 실행되는 경우가 많다. 따라서, 백신이 나오기 전에 사용자가 해당 파일의 실행을 중지시키고 삭제하면 백신 없이도 치료 할 수 있다.

악성 코드 확인

일반적인 수동 조치법은 실행 중인 프로세스 중에서 악성 코드를 찾아 프로세스를 중지하고 해당 파일을 삭제하는 것이다. 하지만, 일반적인 사용자가 사용중인 프로세스 중 악성 코드를 확인하는 방법은 쉽지 않다. 가장 손쉬운 방법은 안철수연구소에서 제공하는 안리포트 프로그램을 이용해 리포트 결과를 안철수연구소에 의뢰하는 것이다. 하지만, 분석 결과를 받는데 시간이 걸리므로 직접 자신의 컴퓨터를 확인하는 능력을 기르는 것이 중요하다.

* 참고

안리포트 사용법과 프로세스를 확인 하는 방법은 다음과 같다.

- 이상 네트워크 패킷 발생시 조치 방안
(http://info.ahnlab.com/securityinfo/info_view.jsp?seq=5431&category=02)

프로세스 확인 및 종료

실행 중인 프로세스 중에 수상한 파일을 찾는 건 평소 실행 중인 프로세스를 확인했다면 비교적 쉽게 확인 할 수 있다. 프로세스를 확인하기 전에 반드시 가능한 모든 프로그램을 종료시키는 게 중요하다. 여러 프로그램이 실행 중이면 다수의 프로세스로 수상한 프로세스를 찾기 힘들어 진다.

프로세스를 확인하는 방법은 크게 Windows 작업 관리자와 프로세스 뷰어가 있다.

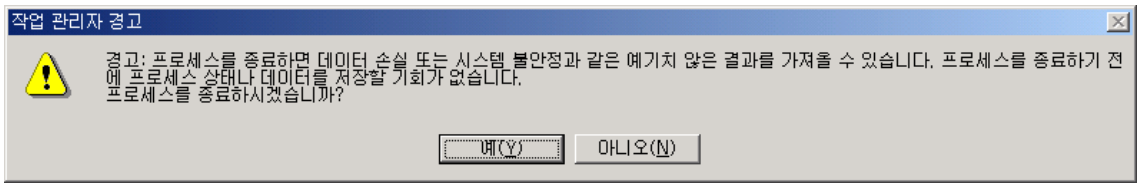
(1) Windows 작업 관리자

윈도우 NT/2000 이상 사용자는 [Ctrl]+[Alt]+[Del] 키를 눌러 [작업관리자]를 선택하거나 [Ctrl]+[Shift]+[Esc]키로 'Windows 작업 관리자'를 실행할 수 있다.

작업 관리자의 '프로세스' 탭으로 현재 실행 중인 프로세스 목록을 확인 할 수 있다. '이미지 이름'을 선택하고 '프로세스 끝내기(E)'를 선택하면 해당 프로세스가 종료된다.

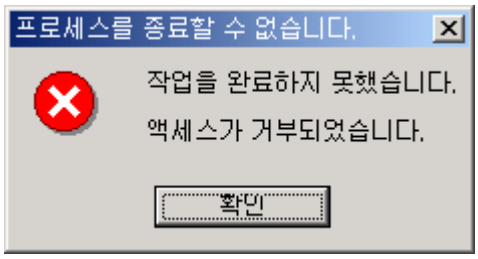
[그림1]현재 실행 중인 프로세스들

해당 프로세스를 끝내려 할 때 '작업 관리자 경고'가 뜰 수 있다.



[그림2]작업 관리자 경고

단, [그림3]과 같이 프로세스를 종료할 수 없는 경우도 존재한다. 이때는 해당 프로세스가 중요한 파일이거나 다른 파일과 같이 실행 중이기 때문이다. 이 경우는 안전모드로 시작해 지우거나 파일 이름을 변경하는 방법을 사용 할 수 있다.

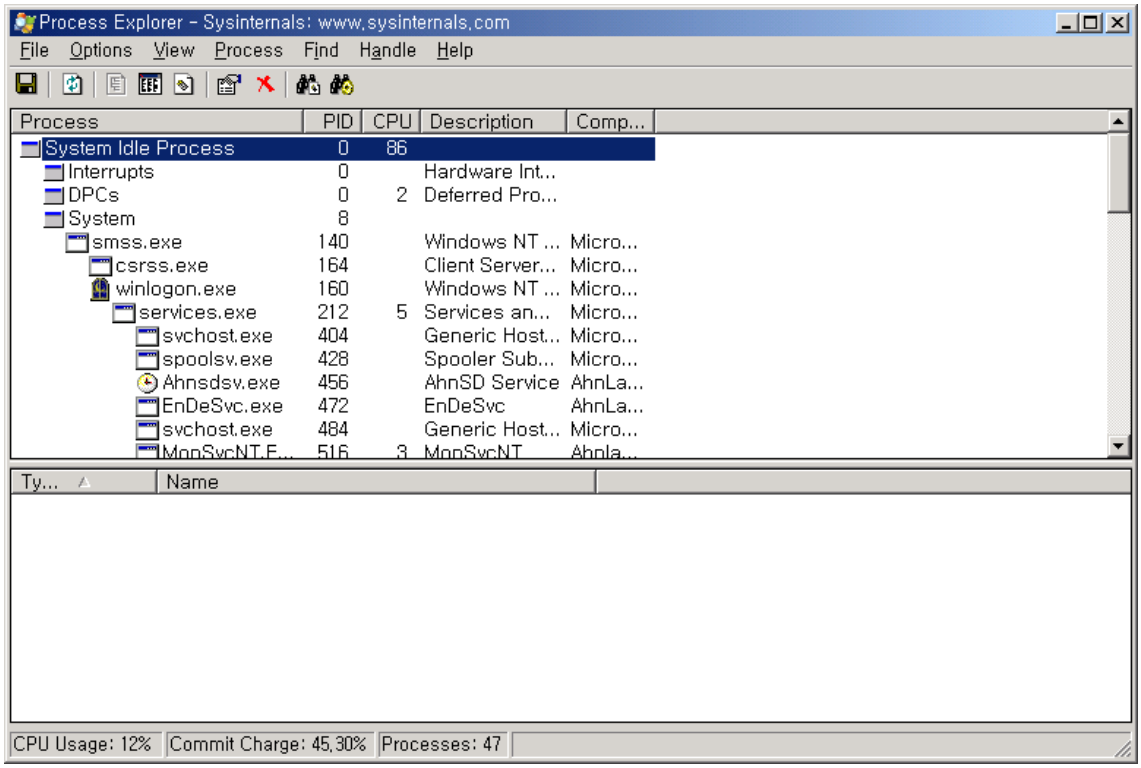


[그림3]프로세스 종료 불가 메시지

(2) 프로세스 뷰어

프로세스 뷰어는 여러 종료가 있는데 여기서는 프리웨어인 'Process Explorer'에 대해 알아보겠다.

'Process Explorer'은 http://www.sysinternals.com에서 다운로드 할 수 있으며 윈도우 작업 관리자보다 더 상세한 프로세스 관련 정보를 보여준다. 이외에도 많은 셰어웨어나 상용 프로세스 뷰어가 있다.



[그림4]Process Explorer 실행 화면

수동 조치법

악성 코드가 파악되면 레지스트리에서 자동 실행 키를 찾아 삭제하거나 해당 파일을 삭제하는 것으로 치료가 대부분 가능하다. 하지만, 실행 중인 파일은 삭제할 수 없으므로 해당 프로세스의 종료가 필요하다. 프로세스를 종료할 때 시스템에 문제가 발생할 수 있으므로 실행 중인 프로그램 중 종료 가능한 프로그램은 모두 종료한다.

(1) 프로세스 종료 후 삭제

가장 쉬운 방법은 현재 실행 중인 프로세스를 'Windows 작업 관리자'나 프로세스 뷰어를 통해 중지 시킨 후 해당 파일을 삭제하는 것이다. 단, Win32/Sober.worm.C[1]와 같은 웜은 몇 개의 프로세스가 웜 프로세스를 서로 감시해 하나의 프로세스가 강제 종료되면 다시 재실행 하는 방법으로 프로세스 종료를 방해하는 형태도 존재한다.

(2) 파일 이름 변경 후 재 부팅 후 삭제

프로세스가 강제로 종료되지 않을 때 일반적으로 파일 이름 바꾸기는 가능하다. 탐색기로 해당 프로세스를 찾아 이름을 바꾼 후 재부팅 하면 일반적으로 웜이 실행 되지 않는다. 하지만, 일부 악성 코드는 파일 이름을 변경도 되지 않는 경우가 존재한다.

[1] Win32/Sober.worm.C : http://info.ahnlab.com/smart2u/virus_detail_1262.html

(3) 안전 모드 부팅 후 삭제

프로세스도 종료되지 않고 파일 이름 변경도 되지 않는 경우 안전 모드 부팅 후 해당 파일을 삭제할 수 있다. 일반적으로 안전 모드로 부팅 하려면 윈도우 시작 시 [F8]키를 누르고 있으면 윈도우 시작 모드를 선택 할 수 있는데 이때 [안전모드]를 선택하면 된다. 보통 안전 모드로 부팅 시 평소 부팅 시간 보다 더 오래 걸린다. 최근 악성 IRCBot이 증가하면서 이상 네트워크 트래픽이 과다하게 발생해 CPU 점유율을 거의 다 차지해 윈도우 실행이 힘들어 웜을 제거 하기 힘든 경우도 있다. 이때도 안전 모드로 부팅하면 대부분 해결되지만 가급적 네트워크 선을 뽑고 제거 작업을 하는 게 좋다.

주의할 사항

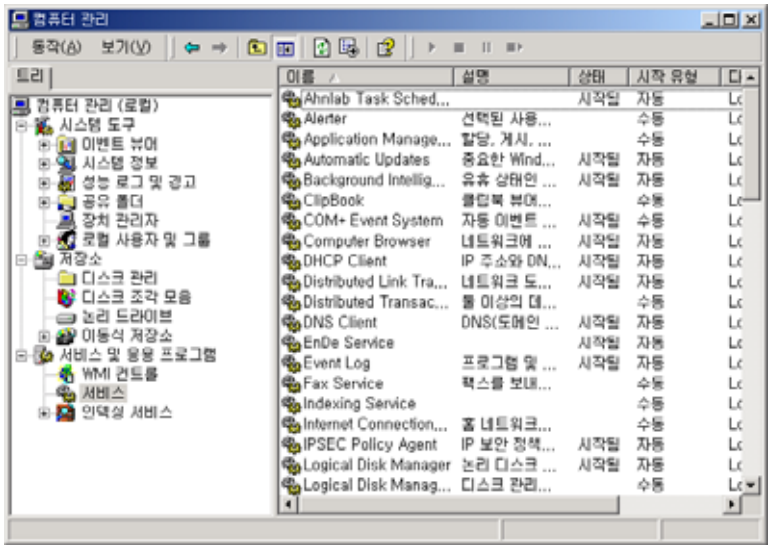
이 작업을 수행할 때 아래와 같은 경우가 발생할 경우에는 다음과 같이 조치한다.

(1) 레지스트리 에디터나 Windows 작업 관리자가 실행 안 되는 경우

사용자가 자신을 제거하지 못하게 하기 위해 레지스트리 에디터(regedit.exe)이나 Windows 작업 관리자(taskmgr.exe)가 실행되면 강제 종료시키는 경우가 있다. 이 경우 이들 프로그램의 파일 이름을 변경해 주면 실행 가능하다. 예를 들어 regedit.exe는 rrr.exe, taskmgr.exe는 ttt.exe로 파일이름을 바꾼 후 실행해 본다.

(2) 프로세스를 찾을 수 없는 경우

악성코드 종류에 따라 프로세스를 찾을 수 없는 경우가 있다. 이 경우 서비스로 올라와 있는 경우가 많다. 서비스는 윈도우 2000의 경우 [내컴퓨터]->마우스 오른쪽 버튼->[관리(G)]->[서비스 및 응용 프로그램]->[서비스]에서 확인 할 수 있다(그림5 참조).



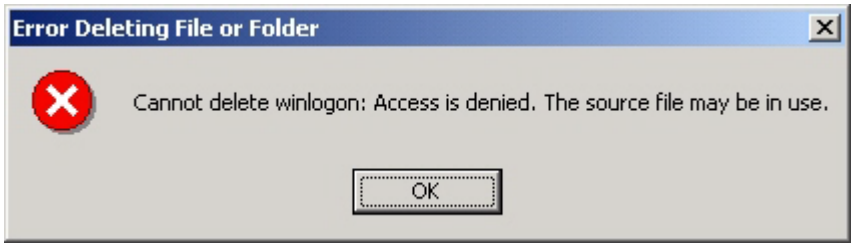
[그림5]실행 중인 서비스 확인

수작업 조치 예 – Win32/Netsky.worm.17424

그럼 실제 웜을 예로 들어 수작업으로 삭제하는 방법을 살펴보자.

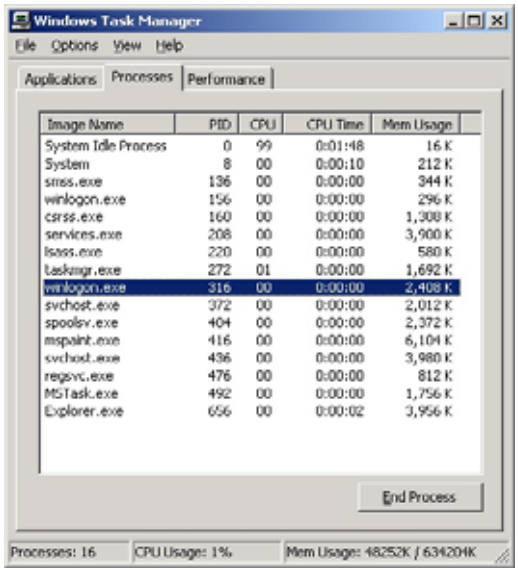
Win32/Netsky.worm.17424[2]는 윈도우 폴더에 winlogon.exe 파일을 만들고 윈도우 시작 시 자동 실행된다. 치료를 위해서 윈도우 폴더의 winlogon.exe 파일만 삭제하면 된다.

① 탐색기로 윈도우 폴더(보통 C:₩Windows 혹은 C:₩WinNT)로 이동해 winlogon.exe 파일을 삭제하려 했지만 에러 메시지만 출력된다. 이는 웜 파일이 실행 중이기 때문이다.



[그림6]삭제를 시도하지만 실패

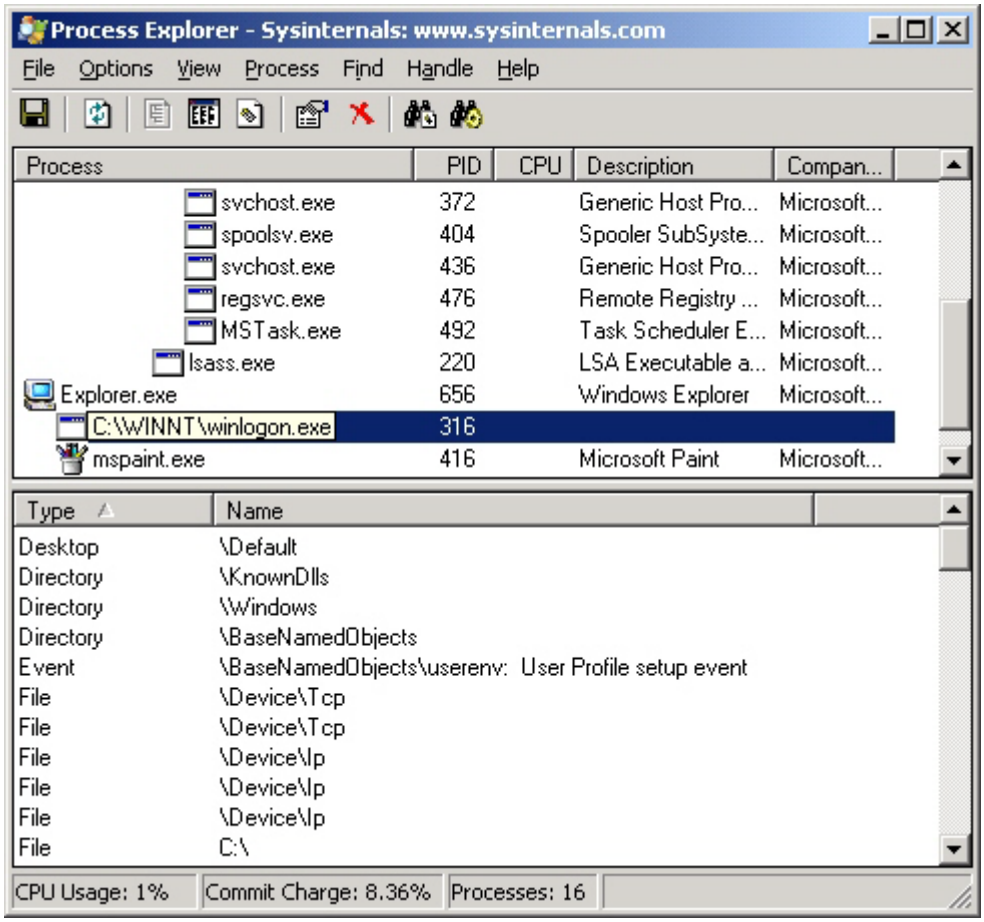
② 윈도우 작업 관리자로 실행 중인 winlogon.exe를 중지시키려고 확인했지만 winlogon.exe 파일이 2개가 있어 어느 파일인지 알 수 없다. 윈도우 시스템 폴더(일반적으로 C:₩Windows₩System, C:₩WinNT₩System32, C:₩Windows₩System32)의 winlogon.exe 파일은 정상 파일이다. 이외에도 svchost.exe 파일로 위장해 실행되는 웜들도 다수 존재한다.



[그림7]윈도우 작업 관리자로 본 화면

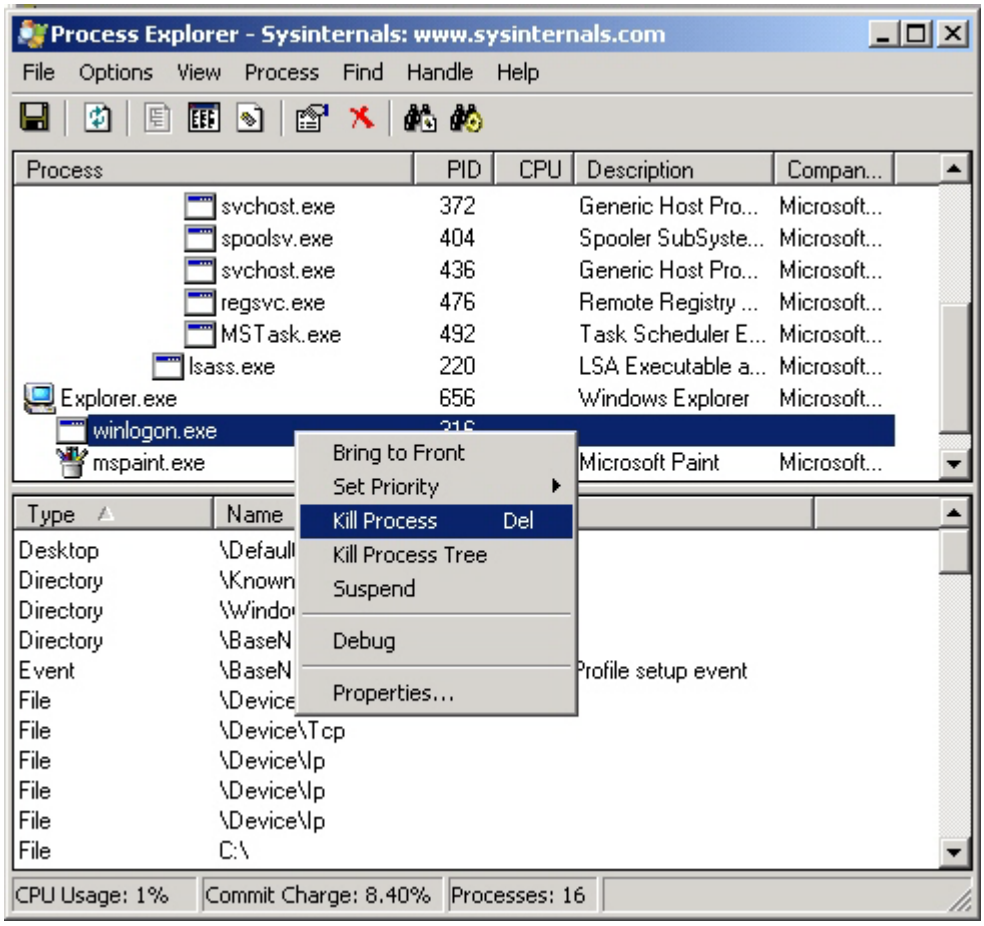
[2] Win32/Netsky.worm.17424 : http://info.ahnlab.com/smart2u/virus_detail_1330.html

③ ‘Process Explorer’로 실행 중인 프로세스를 확인하면 파일 경로도 나오는데 웜 파일인 ‘C:₩WINNT₩winlogon.exe’이 실행 중임을 확인했다.



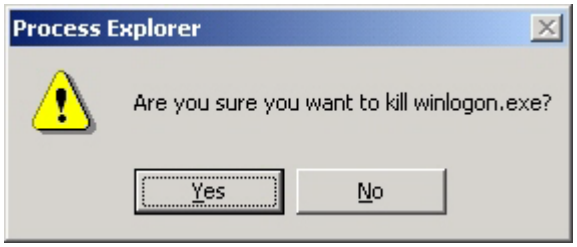
[그림8]Process Explorer로 찾은 웜 프로세스

④ 해당 프로세스를 강제 종료시킨다. 프로세스를 선택하고 오른쪽 마우스 버튼을 누르면 여러 메뉴가 나오는데 이중 ‘Kill Process’를 선택하면 된다.



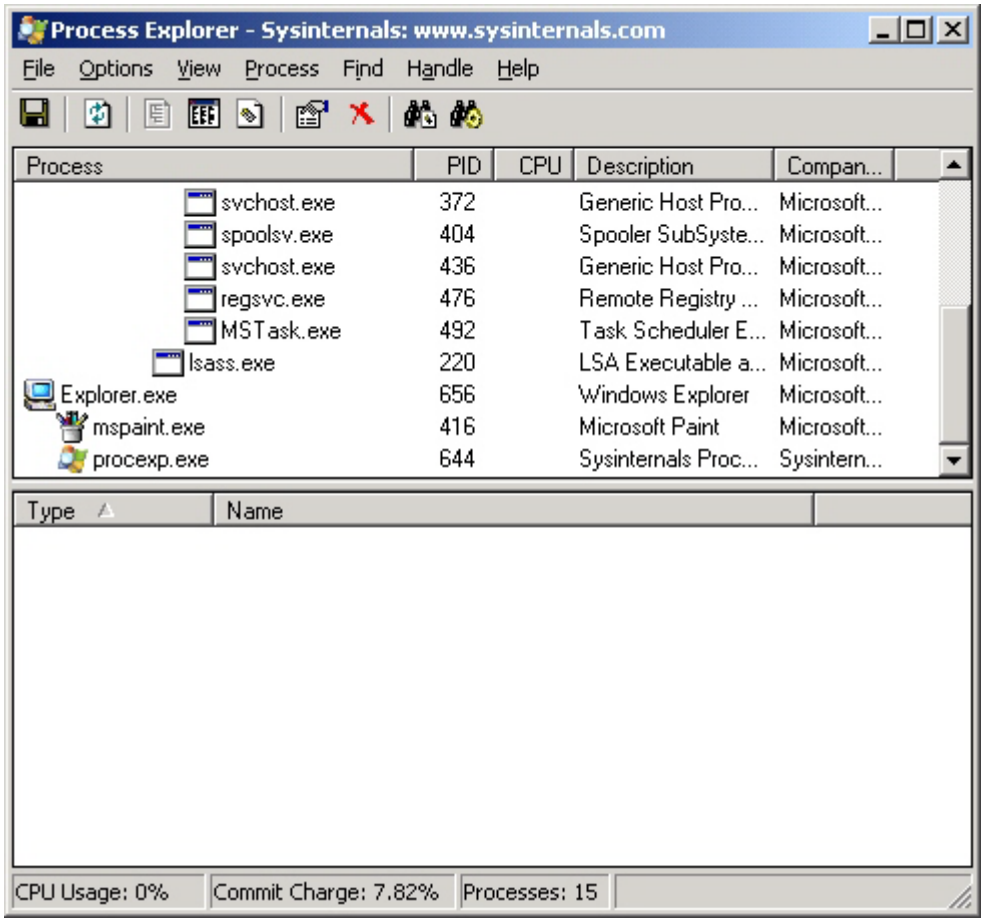
[그림9]웜 프로세스 종료

⑤ 사용자에게 확인을 받는다. '예(Yes)'를 눌러주면 프로세스가 종료된다.



[그림10]프로세스 강제 종료 확인 창

⑥프로세스가 종료되었음을 확인 할 수 있다.



[그림11]웜 프로세스 종료 확인

⑦ 탐색기로 윈도우 폴더의 winlogon.exe 파일을 삭제하면 웜 치료는 종료된다.

⑧필요하다면 웜이 만든 레지스트리 내용도 찾아 삭제한다. 레지스트리는 중요한 정보가 많이 저장되며 잘못 수정하면 시스템에 문제가 발생할 수 있으므로 익숙하기 전까지 함부로 고치지 않는 것이 좋다.

수작업 조치의 필요성

백신 업체는 악성 코드가 발견되면 가급적 빨리 업데이트 된 백신을 제공하려 하지만 여전히 몇 시간에서 몇 일의 간격이 존재한다. 업데이트 전 사용자의 피해를 최소화 하기 위해서는 사용자가 기본적인 프로세스 종료와 같은 응급 조치 방법을 알아두는 게 중요하다.

VII. 테크니컬 컬럼 2 – MBSA 툴을 이용한 윈도우 패치

작성자 : 조경원 연구원(dubhe@ahnlab.com)

개요

마이크로소프트사(이하 Microsoft)는 주요 보안 패치에 대하여 2004년부터 매월 둘째주 화요일(미국시간) 발표하며 긴급 보안 패치의 경우에는 상시 제공을 기본으로 하고 있다. 1998년 이후 보안 패치가 릴리즈 된 개수는 현재 [표1]과 같다.

연도	갯수
1998	20
1999	61
2000	100
2001	60
2002	72
2003	51
2004	7
누계	371

[표1] 연도별 릴리즈된 보안패치 개수

매년 50개 이상의 보안 패치가 릴리즈 되고 있으며 이 모든 보안 패치는 모든 제품에 적용되는 것이 아닌 각 제품별 버전별 언어별로 각기 다른 패치이며 이 모든 패치들을 각 사용자의 제품에 알맞게 적용 및 관리는 매우 힘든 것이 현실이다.

대부분의 보안 패치는 일반 유저가 사용하는 윈도우 98, 2000, XP OS의 패치와 Office, IE 등의 어플리케이션 패치, 서버에서 사용되는 IIS, Exchange, SQL Server등의 서버군 제품에 한 패치가 모두 포함 되어 있다.
이러한 모든 패치는 윈도우의 Windows Updates기능을 통해 커스터마이징된 패치를 적용할 수 있으나 이에 대하여 보안 감사 관점에서 패치 적용 유무의 확인은 현재 발표된 300여 개가 넘는 패치중 설치된 OS, 어플리케이션과 의존성 관계에 의해서 수동으로 점검하기는 매우 힘들다.

이번 테크니컬 컬럼에서는 Microsoft에서 공식적으로 제공하고 있는 MBSA(Microsoft Base Security Analyzer)를 사용하여 패치 적용 유무를 확인 하는 것을 알아 보도록 한다.

MBSA란

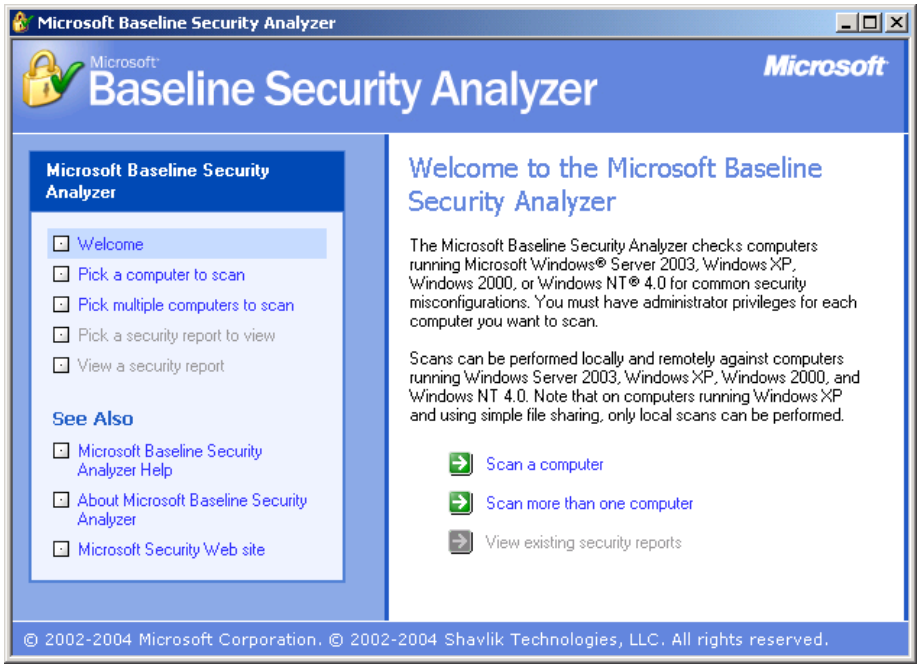
MBSA는 Shavlik Technologies LLC (http://www.shavlik.com/)에서 개발한 HFNetChk툴을 전신으로 개발되었다. HFNetChk는 패치 점검 툴로써 무료 배포 버전과 HFNetCHK Pro의 상용 배포버전이 있으며 Microsoft에서는 HFNetChk를 기반으로 GUI버전으로 MBSA를 개발하여 무료 배포하고 있다.
MBSA는 HFNetChk의 기능인 패치 적용유무 점검 기능 외에 추가적으로 기본 보안 설정 유무 점검등의 기능이 포함되어 있으며 GUI를 통해 제공된다.
v1.2의 버전까지 개발 되었으며 현재는 영문 UI만을 제공하며 CLI(Command Line Interface)방식으로 사용 할 수 있도록 MBSA안에 mbsacli.exe파일을 통해 HFNetChk과 비슷한 환경 역시 제공 해 준다.
기본적인 동작 원리는 보안 패치의 상세 정보, 파일 정보, 레지스트리 정보 등이 담긴 XML 파일을 Microsoft 홈페이지에서 다운로드 받아 이를 기초로 시스템의 보안 패치 적용 유무를 검사하게 된다.
XML(mssecure.xml)파일은 현재 영어, 일본어, 프랑스어, 독일어 4가지 버전이 제공되며 아직 한국어 버전은 제공되지 않는다.
언어 차이는 실제 파일 무결성(Integrity) 검사시에 언어별로 체크섬이 다른 파일이 존재하기 때문에 필요한 것으로, 이로 인해 위의 4가지 언어가 아닌 제품에서 MBSA를 사용할 경우 File Integrity Check 기능이 제공되지 않는다.

MBSA에 관한 상세 자료는 다음 URL에서 확인 할 수 있다.

MBSA 메인 페이지(영문)
http://www.microsoft.com/mbsa
MSBA 1.2 Q&A(영문)
http://www.microsoft.com/technet/security/tools/mbsaqa.mspx

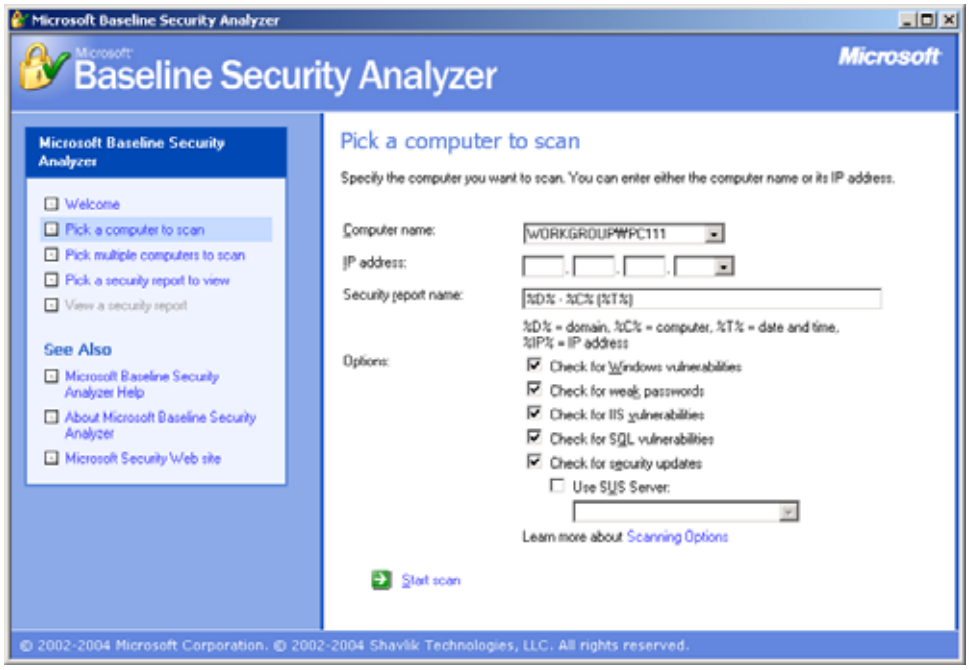
MBSA 사용법

MBSA는 http://www.microsoft.com/mbsa 를 통해 무료로 다운로드가 가능하며 일반적인 MSI 설치 프로그램과 설치 방법이 같다.
실행 화면은 [그림1]과 같다.



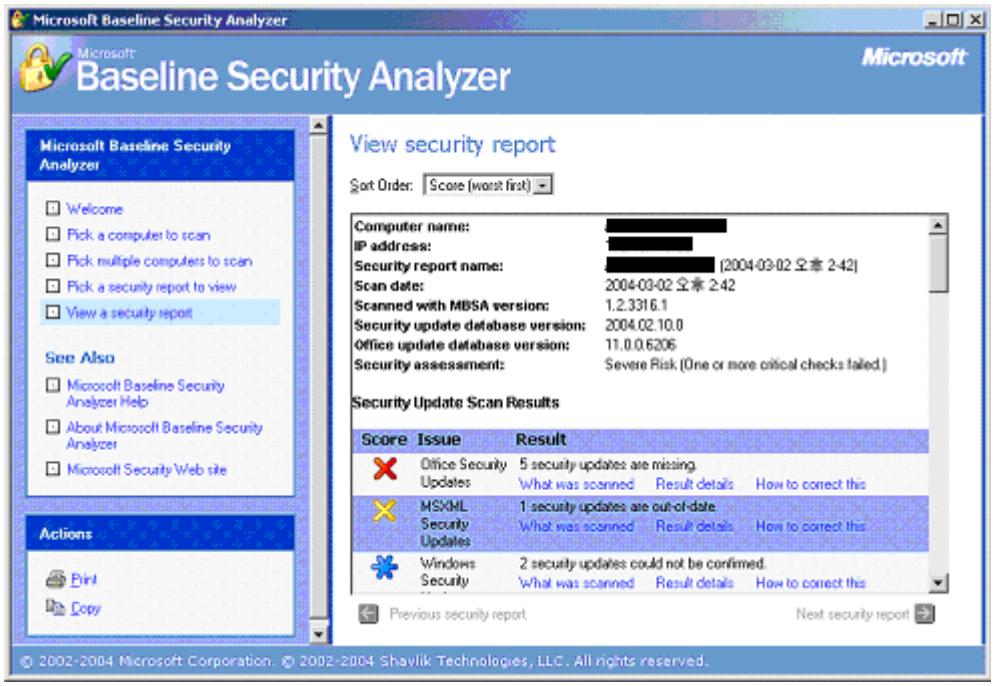
[그림1]MBSA 실행화면

기본적으로 자신의 시스템과 Administrator연결이 가능한 다른 시스템에 대하여 검사가 가능하다. 다른 시스템을 검사할 경우 Administrators권한이 있어야 하므로 직접 admin$ 연결을 통한 인증을 먼저 설정하거나 Domain 으로 Domain Admins 연결이 되어 있어야 가능하다.

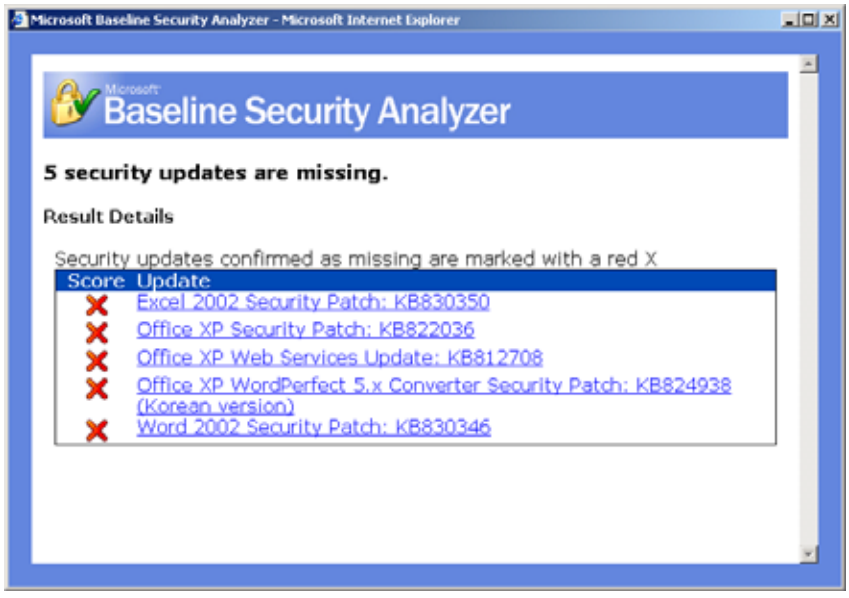


[그림2]다른 시스템을 검사하는 화면

해당되는 시스템을 지정 후 “Start Scan”을 선택하면 해당 시스템에 대하여 보안 패치 적용 유무 분석 및 기본 보안 설정 체크를 실행하게 된다. 결과물은 다음과 같이 출력되며 각 항목을 클릭하면 상세한 정보를 확인 할 수 있다.



[그림3]다른 시스템 검사 결과화면



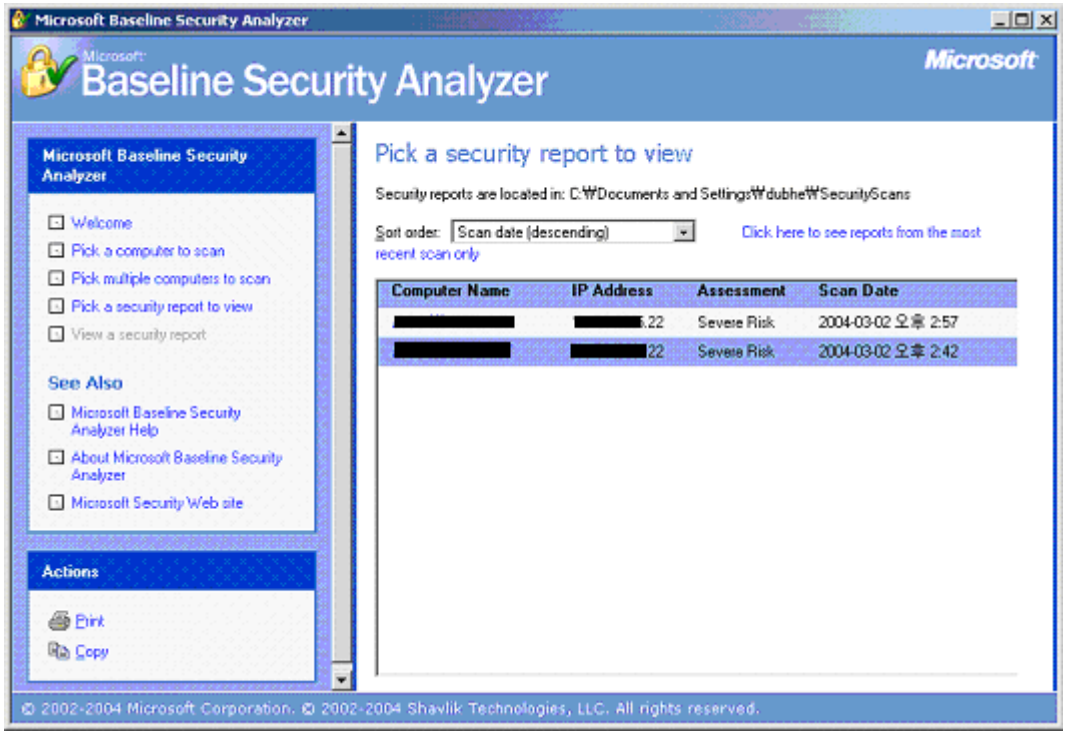
[그림4]검사 결과 5가지 패치가 적용되지 않았다는 경고 화면

위의 시스템은 실제 PC한대에 대해서 테스트를 한 결과이며 위의 PC는 모든 Windows Updates사이트를 통해 패치를 적용한 상태이나 Office 제품군에 대하여 5가지의 패치가 적

용되지 않았음을 경고하고 있다. 이는 Windows Updates에서는 직접적으로 위험한 보안 취약점만을 제공하며 위험도가 높지 않은 Office 제품군의 패치는 Office Updates를 통해 (http://office.microsoft.com/officeupdate/default.aspx) 제공되어 해당 패치를 적용하지 않았기 때문이다.

이와 같이 사용자가 쉽게 놓칠 수 있는 Office 제품군 패치 부분까지 확인 이 가능하여 통합적인 패치 확인이 용이하다.

모든 검사 결과는 시스템 내부에 저장되어 날짜별, 시스템별로 Report 관리가 가능하다.



[그림5]모든 검사결과가 저장된 화면

기타

MBSA외에 패치 점검을 할 수 있는 툴로써는 Shavlik사의 HFNetChk외에 Windows 2000 Resource Kit 및 Windows XP Support Tool에서 제공하는 srvinfo.exe 가 있다. 이 툴은 현재 적용되어 있는 모든 패치의 QNumber를 출력하는 기능을 제공한다. 기타 많은 상용 패치 관리 툴이 있지만 상용인 관계로 생략하기로 한다.

현재 MBSA v1.2에서 검사 가능한 제품은 다음과 같다.

- Microsoft® Windows NT® 4.0, Windows 2000, Windows XP, Windows Server 2003

- Internet Explorer 5.01 이후 버전
- Windows Media Player 6.4 이후 버전
- Microsoft Office
- Internet Information Server (IIS) 4.0, IIS 5.0, IIS 6.0
- SQL Server™ 7.0, SQL Server 2000 (including Microsoft Data Engine 1.0 and 2000)
- Exchange Server 5.5, Exchange Server 2000, Exchange Server 2003 (including Exchange Admin Tools)
- Microsoft Data Access Components (MDAC) 2.5, MDAC 2.6, MDAC 2.7, MDAC 2.8
- Microsoft Virtual Machine (VM)
- MSXML 2.5, MSXML 2.6, MSXML 3.0, MSXML 4.0
- Content Management Server 2001, Content Management Server 2002
- Commerce Server 2000, Commerce Server 2002
- BizTalk® Server 2000, BizTalk Server 2002, BizTalk Server 2004
- SNA Server 4.0, Host Integration Server 2000, Host Integration Server 2004

기타 추가적인 기능으로 다음 보안 설정을 검사한다.
- ICF(Internet Connection Firewall) 설정 검사
- Automatic Updates 설정 검사
- IE zone 설정 검사
- 새로운 MBSA 버전 검사