ASEC Report 3월

® ASEC Report

2004. 4

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 변형 발견과 제작기법의 진화…

2004년 3월은 지난달에 갱신되었던 피해신고된 악성코드의 수를 다시 한번 갱신한 한달이었다. 즉, 피해신고 된 악성코드 종류가 가장 많았던 한달이었던 것이다. 그 원인 중 하나로는 2월 발생했던 넷스카이 웜과 베이글 웜 제작자간의 사이버 설전으로 인한 다수의 변형 제작은 3월에도 이어진 것이며, 또 다른 하나는 악성 IRCBot 류의 악성코드가 많이 발견되고 피해를 주었기 때문이다. 또한 3월에는 국내에서 제작된 애드웨어인 온반이 버그로 인하여 레지스트리 값을 삭제하는 등의 문제를 발생시키며 국내에서 단시간에 많은 피해를 주었었다. 3월의 신종 악성코드 발견의 특징 중 하나는 악성코드의 제작기법이 점차 개선된 변형들이 많이 발견되었다는 것이다. 그 예로는 베이글 웜, 아고봇 웜 등을 들 수 있다.

2004년 3월은 보안취약점이 발표된 지 이틀만에 이 취약점을 이용하여 전파되는 악성코드가 발견되어 0-day Exploit에 이어 취약점을 이용하는 악성코드의 제작에 소요되는 시간도 점점 짧아질 것임을 예고하였다.

일본과 중국의 3월 악성코드 피해 동향은 약간 다른 양상을 보였는데, 일본은 Mass Mailer에 의한 피해가 대부분을 차지한 반면 중국은 네트워크를 이용해 전파되는 악성코드에 의한 피해가 가장 컸다.

이번 테크니컬 컬럼에서는 많은 변형이 발견된 베이글 웜의 제작기법 진화과정을 통해 악성코드 제작기법의 진화에 대해 살펴보았다.

I. 3월 악성코드 Top 10

작성자 : 정진성 연구원(jsjung@ahnlab.com)

악성코드명	건수	%
Win32/Dumaru.worm.9234	1397	27.1%
Win32/Blaster.worm.6176	432	8.4%
Win32/Netsky.worm.22016	295	5.7%
Win32/Netsky.worm.25352	265	5.1%
Win32/Bagle.worm.P	167	3.2%
Win-Trojan/Onban.24576	141	2.7%
Win32/Welchia.worm.12800	102	2.0%
Win32/Welchia.worm.12800.B	96	1.9%
Win32/Agobot.worm.104960	82	1.6%
Win32/Yaha.worm.45568.B	67	1.3%
기타	2,103	40.9%
합계	**5,147**	**100**

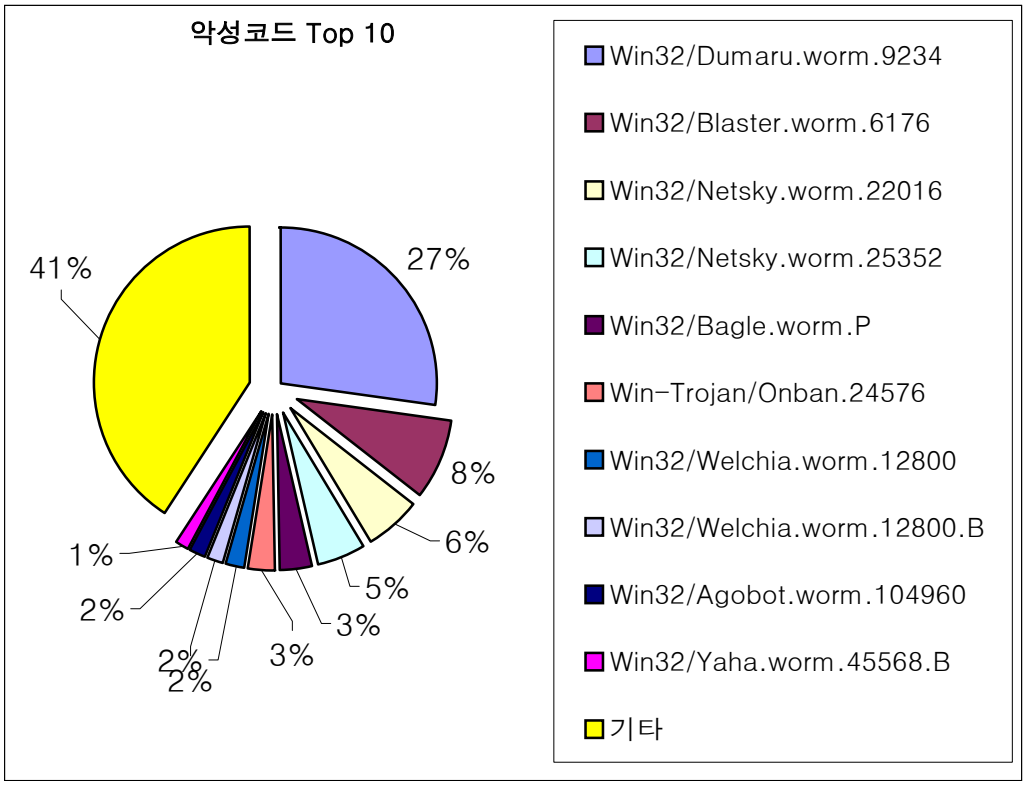
[표1]2004년 3월 악성코드 Top 10

3월 악성코드 피해 동향

3월은 지난 1월, 2월과 비교하여 Win32/Dumaru.9234(이하 두마루 웜)의 건수가 현저히 줄어든 것을 알 수가 있다. 이 웜은 작년 11, 12월 경우 수천건이 넘게 집계 되었다.[1] 그러나 올해 들어 1, 2월은 평균 2800여건씩 집계 되었고 3월은 [표1]에서도 알 수 있듯이 1400건이 조금 못 미치는 수치를 보이는 등 현저한 감소추세를 보이고 있다. 이는 방치된 시스템들이 치료되고 있는 것기 때문인 것으로 보여진다. 즉, 두마루 웜은 현재 소멸기에 접어든 것으로 파악된다. 일반적으로 Mass Mailer 중 이렇게 장기간 동안 Top을 차지하고 있는 것은 매우 드문 일이며, [표1]에서는 Win32/Yaha.worm.45568.B(이하 야하 웜)가 Top 10 내에서 오랜 수명을 유지하고 있는 웜 중의 하나이다.

3월의 악성코드 Top10을 도표로 나타내면 [그림1]과 같다.

[1] 작년 하반기에 두마루 웜의 신고가 많았던 것은 ASEC Monthly Report 2월 호에서도 언급했듯이 사용자의 신고보다는 감염되어 방치된 시스템이 보낸 것이 대부분이었기 때문이다.



[그림1]2004년 3월 악성코드 Top 10

위에서도 언급하였고 [그림1]에서도 나와 있듯이 지난달과 비교하였을 때보다 두마루 웜이 현저히 감소한 것을 알 수 있다. 참고로 지난달은 45% 정도의 비율을 차지 했었다.

이번 달은 Win32/Netsky.worm.22016, Win32/Netsky.worm.25352(이하 넷스카이 웜)이 Mass Mailer 웜 중 많은 신고건수를 보이고 있다. 정보를 작성하는 4월초 현재 20개가 넘는 변형이 나온 이 웜은 당분간은 긴 생명력을 유지할 것으로 보인다. 많은 수의 변형도 그 이유중 하나이지만 무엇보다도 넷스카이 웜 변형들이 광범위하게 확산되었기 때문이다.

[표1]에서 매우 생소하게 느껴지는 Win-Trojan/Onban.24576(이하 트로이목마 온반)은 원래 국내에서 제작되어진 애드웨어이다. 따라서 와일드하게 전세계적으로 퍼지거나 하지 않았다. 애드웨어가 트로이목마로 명명된 이유는 이 애드웨어가 버그로 인하여 레지스트리 값을 삭제하는 등의 문제가 발생하기 때문이며, 이로 인해 국내 사용자로부터 많은 신고가 접수되었다.[2] 이는 그 만큼 많은 사용자들이 애드웨어로 인해 악성코드에 버금가는 많은 피해를 입고 있다는 것을 알려주는 단편적인 예이다.

[2] 트로이목마 온반의 실체가 확인되기 전까지는 이 트로이목마가 발견되기 전날 국내에 유입된 베이글.P 웜의 치료후 나타나는 일종의 '부작용'으로 잘못 알려지기도 하였다.

넷스카이 웜 만큼이나 올 한해 큰 이슈가 되고 있는 Win32/Bagle.worm(이하 베이글 웜)는 그 악의적인 기법으로도 많은 영향을 일으켰던 웜이다. [표1]의 Win32/Bagle.worm.P(이하 베이글.P 웜)는 MS 취약점 중 하나인 오브젝트 태그 취약점을 이용하여 링크에 표시된 URL 파일을 자동으로 실행하게 하는 증상을 가지고 있어, 메일을 읽는 것 만으로도 감염될 수 있다. 또한 메일에 웜을 첨부하지 않아도 전세계의 수백대가 넘는 숙주 컴퓨터에서 웜 파일을 실행하는 형태를 가지고 있다. 이 문서를 작성하는 최근에는 베이글 웜이 더이상 Mass Mailer 형태로 전파되지 않고 이미 감염된 시스템에 있는 웜을 원격에서 업데이트하여 프록시 서버 기능을 가진 형태로 변하였다. 이러한 시스템은 주로 스팸 메일을 보내는 형태로 이용 당할 수 있다.

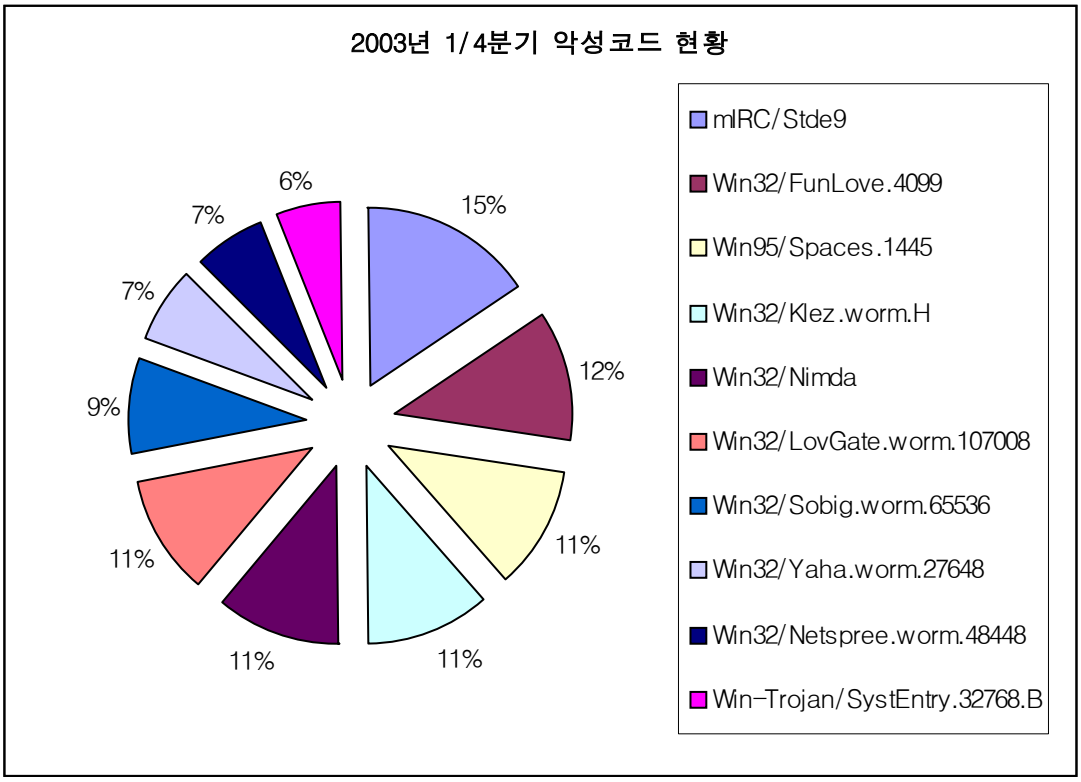
[표1]에서 Mass Mailer를 제외한 다른 악성코드는 모두 MS 보안 취약점을 이용하여 전파되는 웜들이다. 특히 Win32/Welchia.worm.12800 (이하 웰치아 웜) 시리즈 변형도 작년 8월에 웰치아 웜 원형(Win32/Welchia.worm.10240)이 나온후로 근래 들어 12800 시리즈의 변형이 계속적으로 발견되고 있다. 이렇게 보안 취약점을 이용하여 전파되는 악성코드들은 그 생명력이 길어 근본적인 패치가 안된 시스템들이 존재한다면 여전히 오랜기간 동안 사용자들을 괴롭히는 존재로 남을 것이다.

1/4분기의 악성코드 피해 현황

지난해 1/4분기 악성코드 현황에 대하여 비교를 해보면 [표2]와 [그림2]와 같이 구종의 윈도우 파일 바이러스를 비롯하여 발견, 보고된지 오래된 악성코드들이 여전히 기승을 부리고 있는 형태였다. 또한 어느 악성코드에 비중이 치우치지 않고 비슷한 건수가 보고 되었다.

악성코드명	건수
mIRC/Stde9	475
Win32/FunLove.4099	358
Win95/Spaces.1445	335
Win32/Klez.worm.H	334
Win32/Nimda	331
Win32/LovGate.worm.107008	329
Win32/Sobig.worm.65536	266
Win32/Yaha.worm.27648	210
Win32/Netspree.worm.48448	199
Win-Trojan/SystEntry.32768.B	179
합 계	**3,016**

[표2]2003년 1/4분기 악성코드 Top 10

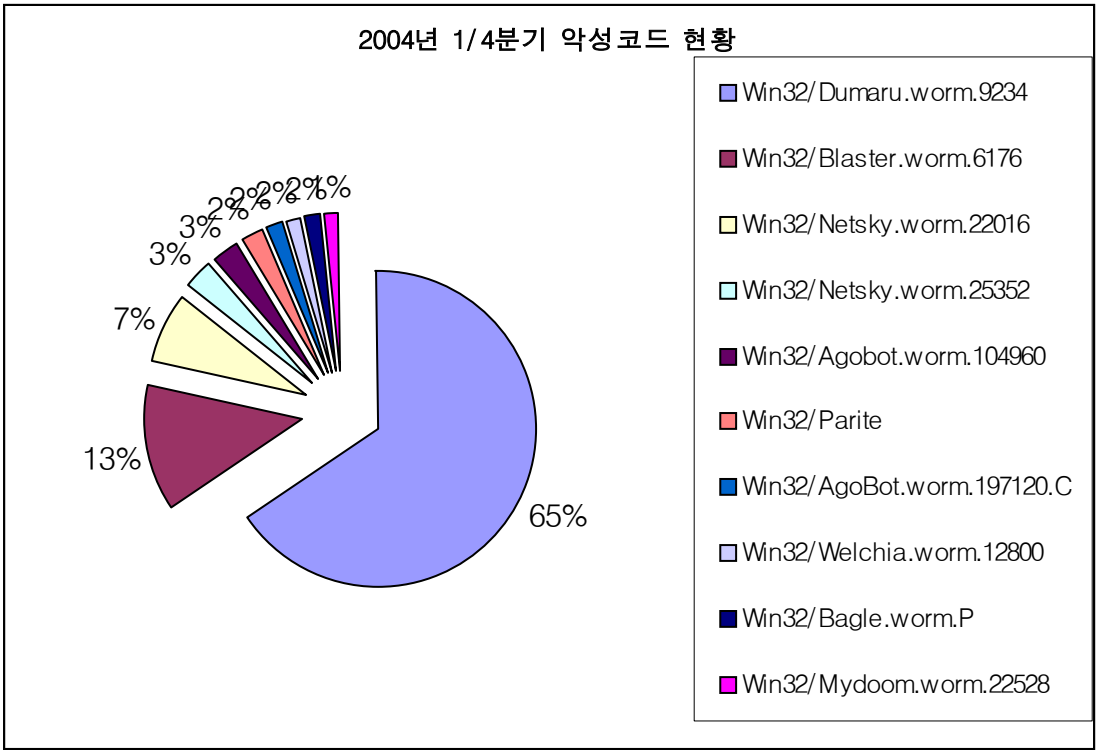


[그림2]2003년 1/4분기 악성코드 Top 10

작년 1/4분기는 전체적으로 구종의 악성코드가 대다수를 차지하고 그 피해문의 건수도 올 1/4분기와 비교해보면 작은 수치이다. 즉, [표3]과 [그림3]과 같이 올해 들어 악성코드의 수가 폭발적으로 증가하였고 고객의 피해문의 건수도 월등히 높아졌다.

악성코드명	건수
Win32/Dumaru.worm.9234	7,268
Win32/Blaster.worm.6176	1438
Win32/Netsky.worm.22016	801
Win32/Netsky.worm.25352	362
Win32/Agobot.worm.104960	282
Win32/Parite	249
Win32/AgoBot.worm.197120.C	228
Win32/Welchia.worm.12800	170
Win32/Bagle.worm.P	167
Win32/Mydoom.worm.22528	159
합 계	**11,124**

[표3]2004년 1/4 분기 악성코드 Top 10

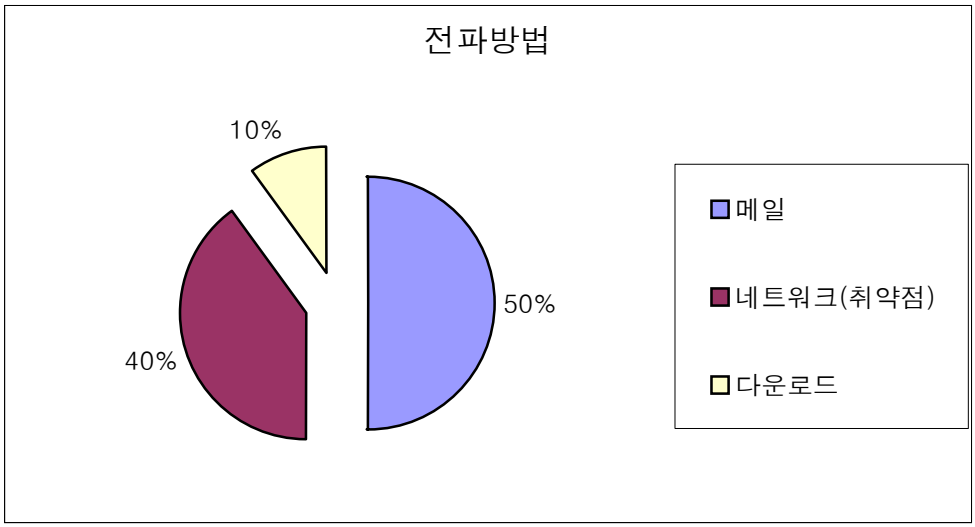


[그림3]2003년 1/4 분기 악성코드 Top 10

올 1/4분기는 전년 동기에 비해서 구종의 악성코드는 모두 자취를 감추었고 새로운 악성코드들이 등장한 것을 알 수 있다. 이들은 대부분 웜 유형으로 주로 Mass Mailer들이 많은 피해를 보이고 있다. 이렇듯 올해 1/4 분기의 악성코드의 유형은 Mass Mailer와 다양한 취약점을 이용하여 감염되는 악성 IRCBot의 대표라 할 수 있는 Win32/AgoBot.worm 시리즈의 피해가 컸던 것이라 할 수 있다.

3월 악성코드 Top 10의 전파방법 유형별 현황

다음은 위 [표1]의 악성코드 Top 10 은 주로 어떠한 감염경로를 가지고 있는지 [그림4]에서 확인해보기로 한다.

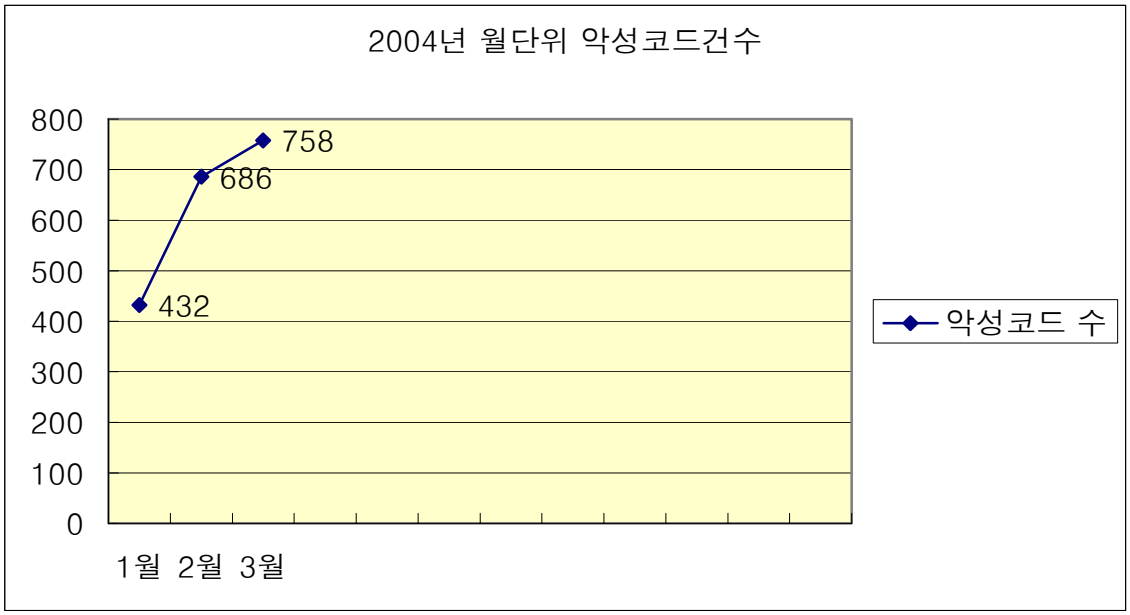


[그림4]악성코드 Top 10의 전파방법 유형별 현황

현재 상황을 잘 말해주고 있듯이 최근 들어 폭발적으로 늘어난 넷스카이 웜, 베이글 웜과 같은 Mass Mailer의 영향으로 메일을 이용한 전파수단이 약간 늘어난 것을 알 수 있다. 그러나 이것은 비록 Top 10에 대한 결과일 뿐 전체적인 유형을 본다면 단연 네트워크(취약점)을 이용한 전파방법이 가장 많은 전파유형이며, 그 이유는 기하급수적으로 늘어난 악성 IRCBot의 영향때문이라 할 수 있다.

월별 피해신고 악성코드 수 현황

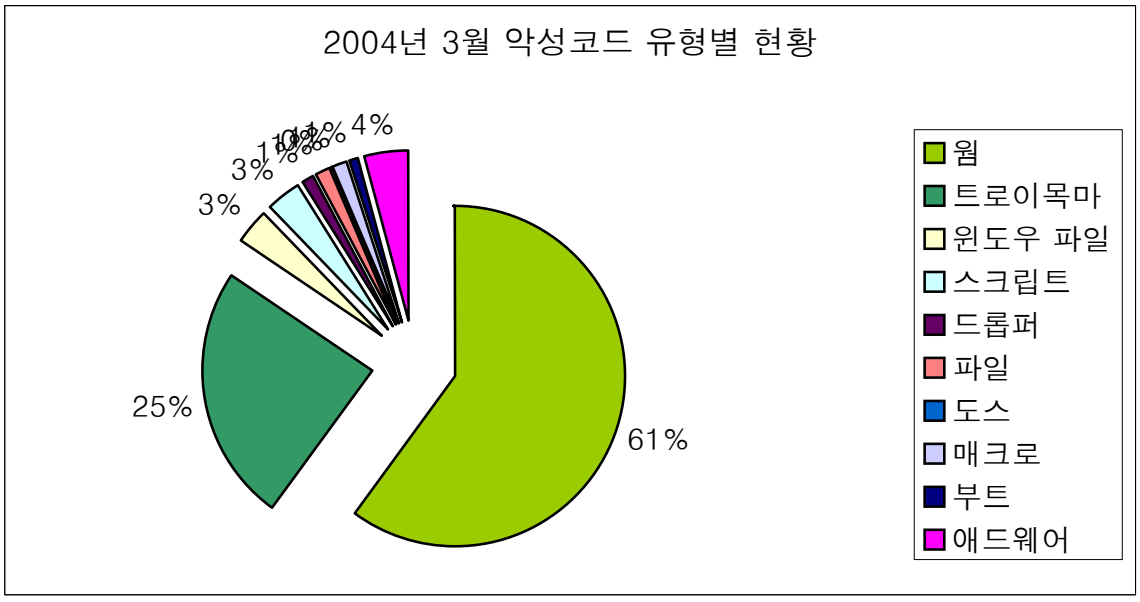
올해 들어서 고객에게 문의되는 악성코드의 종류가 매우 많아졌다. 많아진 이유는 역시 악성 IRCBot의 증가가 가장 큰 원인이다. 올해 ASEC Report 1월호에서 악성코드의 종류가 무려 400개가 넘었다고 했었다. 이는 그 당시 작년과 비교했을 때 매우 높은 수치였고 정말로 많은 악성코드들이 사용자에게 직, 간접적으로 피해를 주고 있었다. 이 기록은 곧 2월에 들어서 무려 200개가 넘는 악성코드의 수 차이로 또다시 갱신되었고, 2월 기록은 다시 3월에 갱신되었다. [그림5]에서 알 수 있듯이 3월에는 무려 758개라는 악성코드가 사용자를 직, 간접적으로 괴롭힌 것이다.



[그림5]2004년 월별 피해신고 악성코드수

물론 Top 10 혹은 20에 포함되지 않는 악성코드들은 그 건수가 단지 몇 건 또는 첫 발견 건수에 포함되어 1건에 그치지만 증가한 원인이 악성 IRCbot이라고 하였으니 이 악성코드의 특성상 1대의 시스템에서만 문제를 일으키지 않고 네트워크로 전파되므로 실제 신고되지 않은 건수까지 생각한다면 적은 수라고 해도 미치는 영향은 무시할 수 없는 수준이다.

그렇다면 758 종류나 되는 악성코드는 어떠한 유형으로 분포되어 있을까?



[그림6] 2004년 3월 악성코드 유형별 현황

[그림6]은 3월 신고된 악성코드의 유형별 현황을 나타내고 있는데, 웜이 차지하는 비율이 과반수를 넘는 것을 볼 수 있다. 이는 동년 2월과 비교했을 때 14% 증가한 것이다.

또한 올해부터 새롭게 집계되는 애드웨어 역시 전체의 4%를 차지하고 있으며 이는 점점 늘어날 것으로 보여진다. 실제로 애드웨어는 광고성 프로그램이고 시스템에 심각한 영향을 주지 않는다면 사용자들이 어떤 파일인지 알아차리기 어렵다. 단지, 성가신 성인광고나 상품광고의 팝업창만으로 인식하여 이를 방치한다면 시스템에 불필요한 리소스를 소비하고 사용자는 의도하지 않는 광고를 보게 되는 것이므로 사용자들의 활발한 신고도 필요하다고 생각된다.

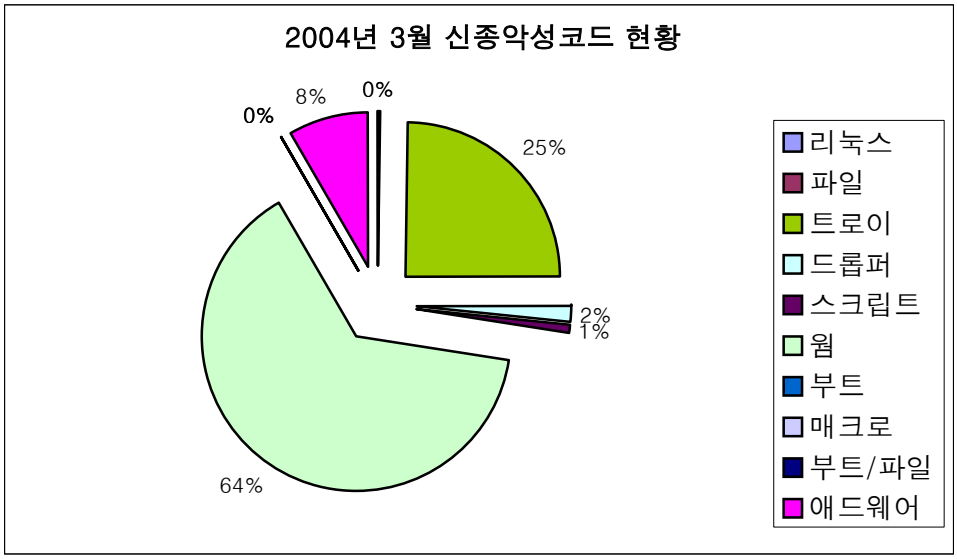
II. 3월 국내 신종 악성 코드 발견 동향

작성자 : 정진성 연구원 (jsjung@ahnlab.com)

3월 한달동안 접수된 신종 악성코드의 건수는 [표1], [그림1]과 같다.

리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	애드웨어	합계
0	1	75	5	3	196	0	0	0	25	305

[표1] 2004년 3월 유형별 신종 악성코드 발견현황

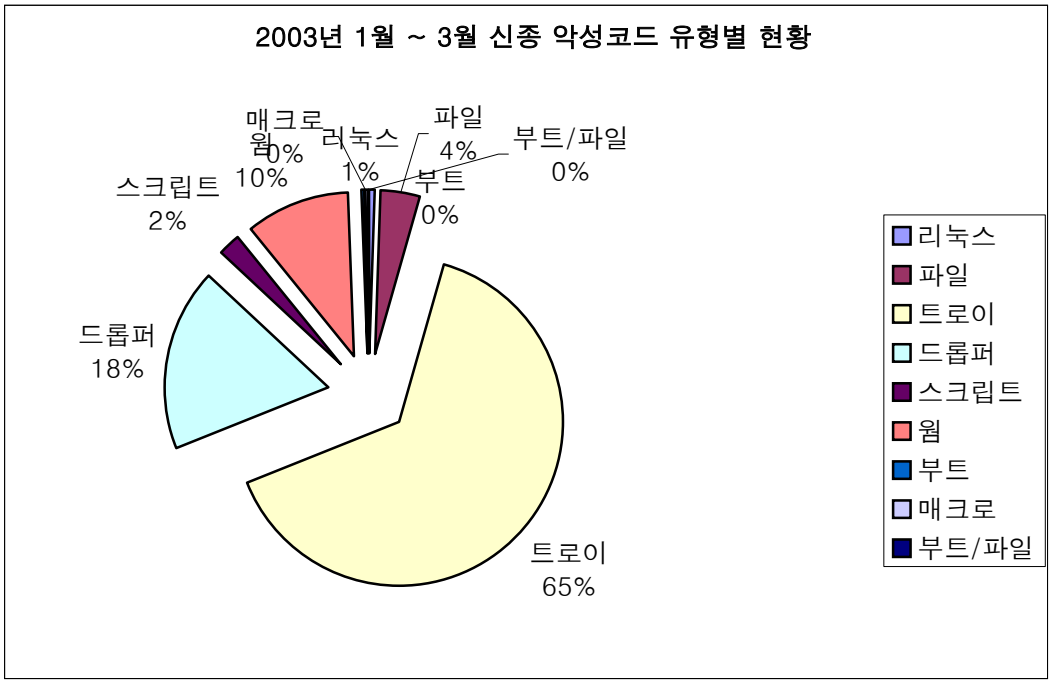


[그림1]2004년 3월 신종 악성코드 발견현황

1/4분기에 발견된 신종 악성코드 동향

올해 1/4분기에는 어떠한 유형의 악성코드가 많았는지 전년 동분기의 차트와 비교하여 보면 다음과 같다.

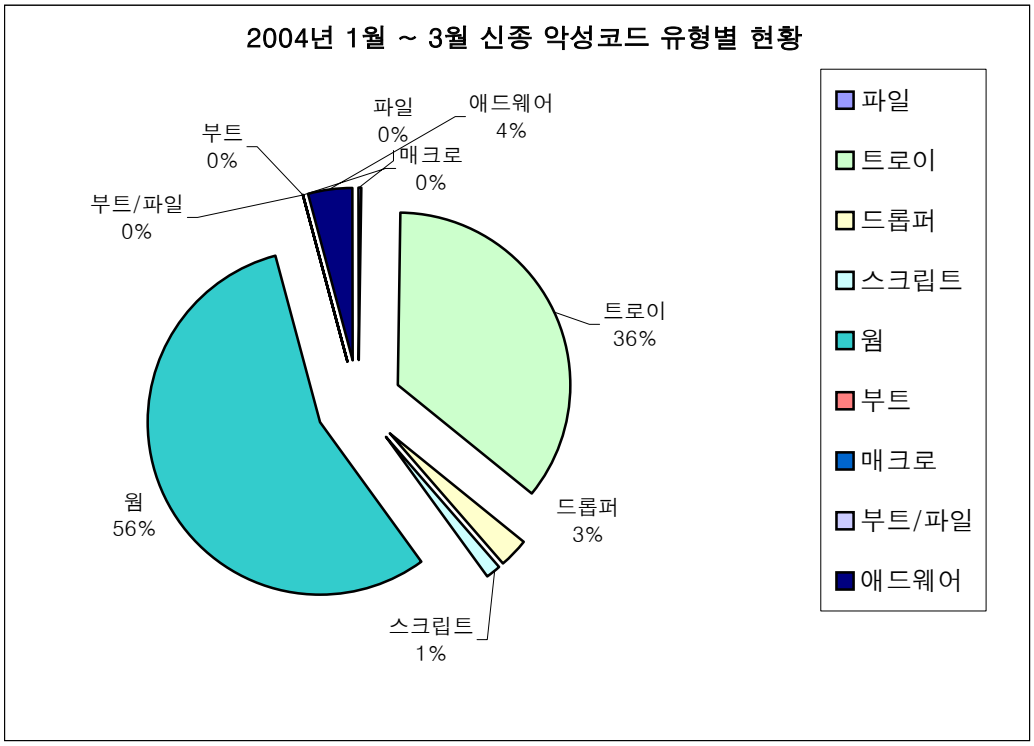
[그림2], [그림3]과 같이 작년 동분기의 신종 악성코드 유형은 트로이목마가 전체 유형에서 압도적으로 많았다. 트로이목마가 많았던 이유는 그 당시 역시 악성 IRCbot류가 증가하기 시작하는 초기 단계였기 때문이다. 악성 IRCBot들의 형태가 지금처럼 하나의 실행파일로 구성되어 있지 않고 배치파일과 원격파일 실행 툴, 패스워드 사전 등과 같이 여러 개 형식으로 구성되어 있는 것이 일반적이었다. 이들이 전파기능이 있어 웜이라고 생각될 수도 있지만 다른 파일의 도움없이는 전파가 불가능한 형태였기 때문에 이들이 트로이목마로 분류되었졌으며 발견되는 개체수가 많아져 트로이목마가 압도적으로 많았던 것이다.



[그림2]2003년 1/4 분기 신종 악성코드 유형별 현황

반면에 Mass Mailer와 같은 전통적인 웜의 수는 2001년과 2002년에 비해 2003년 동분기에는 피해가 많이 감소하다가 2004년 들어 Mass Mailer와 같은 웜에 의한 피해가 다시 급증하였다.

올해의 1/4분기는 전년 동분기에 비해 트로이목마보다는 웜의 비율이 높다. 이것은 많은 수의 악성 IRCbot들이 기술의 발전으로 인한 현상이다. 이전처럼 조잡한 형태의 여러 파일로 구성되어 있는 것이 아니라 이들의 IRC 내에서 별도의 커뮤니티 공간을 만들어두고 자신이 만들거나 변형한 버전등을 공개하면서 기술을 발전시키고 있다. 따라서 기존처럼 여러 파일들을 조합한 형태가 아닌 고급언어로 작성되어지고 쉽게 다른 모듈을 붙일 수 있는 형태로 발전하였다. 즉, 트로이목마 형태에서 웜의 형태로 발전하였으며 이것은 악성 IRCBot 의 전파방법이 변화된 것을 의미한다.



[그림3]2004년 1/4 분기 신종 악성코드 유형별 현황

[그림3]에서도 알 수 있듯이 2004년 1/4분기에 발견된 신종 악성코드의 유형은 웜의 비율이 가장 높고 그 뒤를 트로이목마가 차지하고 있다. 트로이목마의 상당수는 여전히 과거의 악성 IRCBot 형태가 대부분이다. 웜의 출현이 증가한 것은 악성 IRCBot도 한몫을 하지만 전년 동분기와는 달리 Mass Mailer 형태가 새롭게 출현하고 수많은 변형이 발견된 것도 큰 원인중의 하나이다. 또한 이러한 Mass Mailer들은 급속도의 확산력을 가지고 있어 올해 악성코드에 의한 피해가 증가한 원인 중의 하나이며 이는 피해측면에서 전년보다 더욱 증가하게 되었다.

3월 발견된 신종 악성코드 동향

3월은 신종 악성코드에서도 Mass Mailer 혹은 Network Base의 웜 유형이 많이 증가한 것을 알 수 있다. 신종 악성코드 경우에는 주로 다음과 같은 웜 유형이 많았다. 이는 지난달과 매우 유사하다.

- Win32/Netsky.worm 변형들 (이하 넷스카이 웜)
- Win32/Bagle.worm 변형들 (이하 베이글 웜)
- 악성 IRCBot 변형들

특히 넷스카이 웜과 베이글 웜은 제작자들이 경쟁적으로 변형을 만들어 짧은 기간동안 각각

20개가 넘는 변형들이 발견되었다. 특히 베이글 웜은 그 악의적인 제작 기법이 날로 발전하여 언론에서는 안티 바이러스 연구가들에게 골치 아픈 웜으로 소개되기도 했었다.

위에서도 언급한 것 처럼 베이글 웜 중 MS 보안 취약점을 이용한 것은 Win32/Bagle.worm.P(이하 베이글.P 웜)이다. 베이글.P 웜 은 HTML 내의 오브젝트 태크 취약점(MS03-032)을 이용하여 메일 본문에 웜의 첨부파일이 없어도 HTML 내의 오브젝트 태크로 명시된 URL의 파일을 자동으로 다운받아 실행하는 방식으로 웜이 동작한다.

또한 베이글 웜의 제작자는 이미 기존에 감염된 시스템 중 일부-전 세계적으로 수백대-의 베이글 웜을 베이글.P 웜으로 이미 업데이트 해 두어 이 숙주 시스템에서 웜을 다운 받는 형식으로 사용하였다. 현재는 이 숙주 컴퓨터의 IP가 모두 알려져 차단 되었지만 워낙 많은 시스템이 감염되었기 때문에 제작자는 또 다른 감염된 시스템의 베이글을 이용하여 다른 변형을 퍼뜨리는 숙주로 얼마든지 사용할 수 있다.

또한 베이글 웜과 경쟁적으로 제작되어지고 있는 넷스카이 웜 경우는 제작의 악성기법적인 측면보다는 사회공학적인 요소가 많은 웜이다. 이 웜은 사용자를 속이도록 로컬 드라이브에 생성되는 웜 파일도 마치 안티 바이러스 제품인 것처럼 속이거나 메일을 보낼 때도 역시 안티 바이러스 제품에 의해서 검사가 끝난 것과 같은 메시지를 담아 발송하여 사용자들로 하여금 혼란을 주고 있다.

이 두 웜의 제작자들은 서로를 비방하면서 경쟁적으로 웜을 제작하고 있으며 몇번째 변형까지 나올지 현재로써는 장담하기 힘들만큼 불투명하다.

올해는 작년에 발견되어 맹위를 떨쳤던 악성코드의 새로운 변형들이 자주 보고되고 있다. 몇개를 열거해보면 다음과 같다.

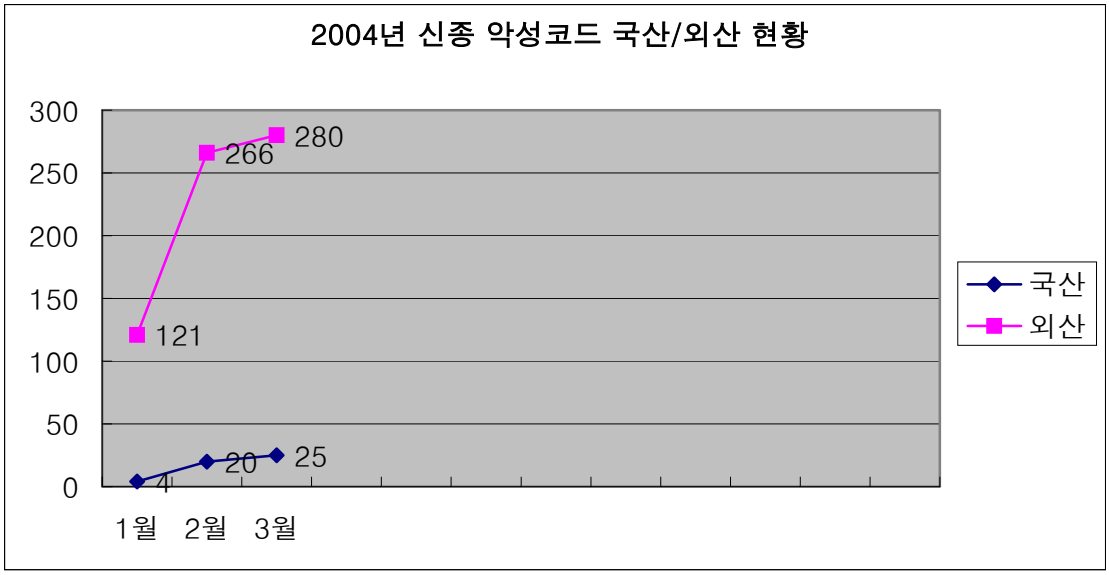
- Win32/Welchia.worm(이하 웰치아 웜)
- Win32/LovGate.worm(이하 러브게이트 웜)

이번 달에 발견된 러브게이트 웜 변형 시리즈는 이 웜이 작년에 처음 발견, 보고된 이후 발견된 변형들-누군가 고의로 실행압축을 여러번 한 형태-과 감염방법에서 차이를 보이고 있다. 원형에서는 LSASS.EXE라는 윈도우 시스템 프로세스에 백도어 모듈을 Inject하는 방법을 사용한 반면 이번에 발견된 변형은 백도어가 LSASS.EXE 프로세스에 리모트 쓰레드로 존재하는 형식을 갖고 있다. 이 경우 안전하게 치료되기 위해서는 메모리 진단/치료가 선행되어야 하며 그렇지 않을 경우에는 시스템을 불필요하게 재부팅해야만 치료가 가능하다.

또한 이번달에 발견된 악성코드로 국내에 공식적으로 유입되지는 않았지만 그 형태가 과거의 코드레드 웜이나 슬래머 웜처럼 취약점을 이용하여 감염되고 메모리 형태로만 존재하는 웜이 출현하였다. Win32/Witty.worm(이하 위티 웜)이라 명명된 이 웜은 특정 보안제품이 사용하는 모듈의 취약점을 이용하여 감염되며 초당 7200개의 패킷을 발생시킨다. 다행히도 국내에서는 해당 응용 프로그램 사용자가 적고 세계적으로도 그 피해건수가 과거의 비슷한 유형의 악성코드에 비해 보고건수가 적어 별다른 피해 없이 지나갔다.

가장 많은 발견건수를 가진 악성 IRCBot 중에서 Win32/AgoBot.worm(이하 아고봇 웜) 변형은 새로운 형태가 나타났다. 우려한 대로 은폐기법을 가지고 있으며 지난호에도 설명했듯이 다형성 코드도 함께 가진 형태가 출현하였다. 은폐기법을 사용하여 사용자 및 안티 바이러스 제품에서 진단이 되지 않게 한 것이다. 따라서 이러한 기법을 가진 아고봇 웜은 설치가 되면 수동으로 제거하기가 어려우며, 안티 바이러스 제품에서도 이를 지원하지 않아 사용자들은 치료에 상당한 어려움을 느끼고 있었다. 이에 안철수연구소는 세계 최초로 은폐기법의 아고봇 웜에 대한 메모리 진단/치료 모듈을 만들어 전용백신을 배포하기도 하였다.

다음은 신종 악성코드들의 국산/외산의 현황을 보여주고 있다. 지난달에 비해 약간 상승한 것을 볼 수 있다.



[그림4]2004년 제작지별 신종 악성코드 현황

지난달만큼 폭증한 것은 아니지만 많은 수의 신종 악성코드가 국내에 유입되었음을 알 수가 있다. 국산 악성코드경우는 모두 애드웨어이며 악성코드로서의 국산은 존재하지 않았다.

국내에서 접수된 애드웨어들은 대부분 홈페이지 고정, 팝업광고, 스팸 메일러류가 대부분이며 이들은 모두 Active X를 이용하여 다운받아지는 것들이다. 애드웨어가 악성코드 다음으로 사용자들의 골치 아픈 문제가 된 원인은 일단 다양한 광고방법의 증가도 한 원인이고 무분별한 광고업자도 책임소재가 크다고 하겠다. 그러나 대부분의 Active X가 사용자가 처음 설치할 때 모르고 설치한 경우가 많으므로 웹 사이트 방문이나 게시판의 글, 메일 등을 확인할 때 의심가는 Active X 창에서는 한번 내용을 확인하고 안전하다고 판단되면 '예' 버튼을 눌러 다운받도록 하는 습관을 가져야 하겠다. Active X는 현재 다운받지 않는다고 해서 사용하지 못하는 것이 아니라 다시 해당 사이트를 방문하면 재설치가 가능하므로 이런 점을 확인하여 필요하지 않다면 받지 않는 등의 사용자 주의와 지혜가 필요하다.

III. 3월 신규 보안 취약점

작성자 : 조경원 연구원(dubhe@ahnlab.com)

3월에는 특별한 악성 보안 취약점은 발견되지 않았다. 하지만 몇몇 취약점에 대하여 악성코드에서 사용되는 형태가 발생하였다. 이에 이번달에는 BlackIce의 취약점을 사용한 Win32/Witty.worm(이하 위티 웜)과 IE 취약점을 사용한 Win32/Bagle.worm.P(이하 베이글.P 웜) 등에 관련된 취약점에 대하여 알아보도록 하겠다.

ISS사 제품의 PAM ICQ 처리 버퍼 오버플로우 취약점

3월 18일 ISS사의 RealSecure, Proventia, BlackIce 등의 제품에서 사용되는 PAM(Protocol Analyze Module)에서 취약점이 발견되었다. 이 취약점은 PAM 안의 ICQ Server Response를 처리하는 부분에서 특정한 패킷을 받으면 Stack BOF(Buffer Overflow)가 일어나 시스템 권한을 획득할 수 있는 것이다.

PAM은 ISS사 제품의 IDS모듈로써 여러 프로토콜을 분석하는데 사용된다. 이중 ICQ 프로토콜의 Server Response 패킷을 분석할 때 SRV_META_USER Response 부분을 적절하게 검사하지 않아 Stack Buffer Overflow가 발생할 수 있다.
ICQ의 Server Response 프로토콜은 Source Port가 4000/udp로 타이트하지 않은 방화벽 룰을 통과 할 수 있는 가능성이 많으며 UDP 특성상 속도가 매우 빠르다.

이 취약점을 사용한 위티 웜이 3월 20일 출현하였는데 0-day라 불리우는 취약점 발견과 공격코드 제작 시간이 당일날 발생한다는 최근의 추세에 비추어 매우 빠르게 취약점이 악성코드로 발전한 사례로 볼 수 있다. 일반적으로 OS취약점이 아닌 Third-party 제품의 취약점을 사용하는 악성코드는 많지 않으나 위티 웜은 개인 PC 방화벽/IDS로 널리 사용되는 BlackIce를 목표로 만들어진 것으로 추정된다. 위티 웜의 경우 UDP 특성상 빠른 전파속도와 디스크 섹터 파괴 증상을 갖고 있었지만 국내에는 사용자가 많지 않아 큰 피해를 주지는 않았다. 하지만 Third-party 제품군의 취약점을 사용한다는 점과 충분한 취약점 패치 기간보다 짧은 0-day에 가까운 발생 시점을 비추어 볼 때 다른 여러 응용프로그램의 취약점을 이용한 악성코드가 추후 늘어날 가능성이 있다는 점에서 눈여겨볼 필요가 있다.

IE Security Zone bypass 취약점

최근 IE(Internet Explorer)에 대하여 많은 취약점이 발견되고 있다. 대부분 IE의 보안모델 구조인 Security Zone을 피해가는 취약점으로 IE에서는 해당 접속 사이트에 대하여 Internet, Local Intranet, Local System, Trusted sites...등의 Security Zone을 사용하여

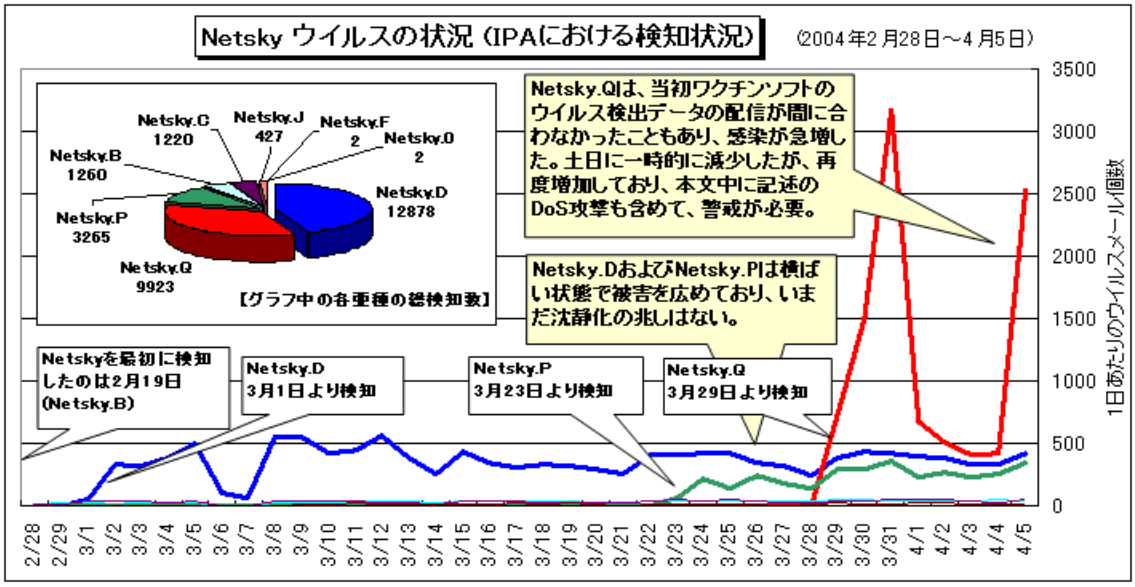
Client Side Script의 실행 유무, ActiveX 등의 실행파일 다운로드 및 설치 유무 등을 결정하게 된다. 많은 프로토콜이 이 Security Zone 보안모델을 통해 사용자에게 자동 설치, 수동 설치, 자동 실행 등의 기능을 제공해 주며 신뢰되지 않은 웹사이트 방문시에는 사용자에게 경고창을 보여주도록 설계되어 있다.

최근 IE에 발생되는 취약점은 여러 인터넷 프로토콜의 IE안에서의 파싱 순서, 로직 오류 등을 이용한 것으로 MHTML, XMLHTTP, MS-ITS, CHM, MMS, HTA 등 많은 프로토콜을 조합하여 IE Security Zone의 검사를 우회하여 스크립트를 실행하는 취약점이 발견되고 있다. 이 취약점을 악용하면 악성 코드를 사용자 PC에 자동으로 설치, 실행되는 공격이 가능하다. 더 큰 위험성은 이 취약점들이 해당 프로토콜, 프로토콜 구현 모듈에서 발생하는 것이 아닌 전체적인 보안 모델 구성 로직 오류이기 때문에 패치가 나오지 않은 취약점도 존재하며 패치가 적용되었다 하더라도 약간의 다른 접근을 통하여 패치를 무력화 시키는 공격이 수시로 등장하고 있다는 점이다. 최근에는 이러한 취약점을 사용하여 메일을 읽을 때 자동으로 악성코드가 설치되는 스크립트를 포함한 악성코드가 발견되고 있다. Win32/Bagle.worm.P의 경우가 이런 예이다. 사용자는 항상 접속하는 사이트 및 메일 확인 시 해당 사이트와 링크가 정상인지 비정상인지를 주의하여야 하며 자동 ActiveX 스크립트 실행 등의 기능을 수동으로 설정하여 이러한 공격에 의한 피해를 최소화 할 수 있다.

Ⅳ. 3월 일본 피해 동향

작성자 : 김소헌 주임연구원(sohkim@ahnlab.com)

일본의 IPA/ISEC의 자료에 의하면 2004년 3월 한달 동안 IPA에 신고된 바이러스 노출 신고건수는 4,012건으로 1,733건인 전월과 비교하여 큰 폭으로 증가한 것으로 나타났다. 주요 증가 원인은 1,795건에 달하는 W32/Netsky(Win32/Netsky.worm, 이하 넷스카이 웜)의 노출 신고건수 때문이다. 이러한 수치는 2002년 8월 유행한 W32/Klez(Win32/Klez.worm, 이하 클레즈 웜)의 신고건수인 1,062건을 상회하는 것이고 이는 최근 유행하고 있는 이메일로 확산되는 웜의 심각성을 알 수 있게 해준다.



[그림1]일본의 넷스카이 웜 발견 현황(출처 : IPA/ISEC)

[그림1]은 넷스카이 웜의 현황을 도식화한 것이다. 2월 19일 최초 발견 이후부터 새로운 변형 발생 시점 및 각 변형들의 노출 신고 현황을 알 수 있다. [그림1]의 내용에서 주목할만한 점은 Netsky.D 웜의 신고 건수가 다른 변형들에 비해서 월등히 많고 현재까지 계속 확산도가 낮아지지 않고 있다는 점이다. Netsky.D 웜 이외에도 3월 28일경 최초 발견 후 급격하게 전파되고 있는 Netsky.Q 웜의 확산도와 감염된 시스템에서 발생할 수 있는 Dos공격에 대한 주의를 요청하는 내용 또한 주목할만한 점이다.

일본 유행 악성코드 유형별 발생현황

2004년 3월 한달 일본에서 가장 유행한 악성코드는 넷스카이 웜인 것으로 나타났다. 넷스카이 웜은 2004년 2월 최초로 발견된 이후 최근까지 여러 종류의 변형들이 발견되고 있는 이

메일 웜 이다.

[표1]은 2004년 3월 한 달 동안 IPA/ISEC에 접수된 악성코드 노출 신고 건수를 집계한 자료이다. [표1]의 내용 중 Windows/Dos Virus와 관련해서 주목할 만한 것은 넷스카이 웜의 신고 건수가 전월과 비교해서 급격하게 증가한 점이다. 이외에도 마이둠 웜과 베이글 웜 등 Mass Mailer 기능을 가진 웜들의 신고 건수가 여전히 줄어들지 않고 있는 것을 알 수 있다.

Window/Dos Virus	건수	Macro Virus	건수	Script Virus	건수
W32/Netsky	1,795	Xm/Laroux	19	VBS/Redlof	68
W32/Mydoom	479	X97M/Divi	6	Wscript/Fortnight	11
W32Klez	346	W97M/Bablas	3	VBS/Loveletter	4
W32/Bagle	268	W97M/Thus	2	VBS/Netlog	2
W32/Swen	201			VBS/Haptime	1
W32/Bugbear	148				

[표1]일본의 악성코드 노출 신고 현황(출처 : IPA/ISEC)

일본 악성코드의 주요 감염경로

일본에서 발생한 악성코드 감염의 주요 감염경로는 이메일을 통한 것이다.
[표2]는 악성코드에 의해 피해를 당한 사용자들의 주요 감염경로에 대한 통계이다. 이 표에서 알 수 있는 것처럼 이메일을 통한 감염은 전체 감염경로의 대부분을 차지하고 있다.
또한 수치상으로도 전월과 비교하여 큰 폭으로 증가하였음을 볼 수 있는데 이는 [표1]의 악성코드 노출 신고현황 자료에 나타난 것처럼 넷스카이 웜의 영향에 의한 것이다.

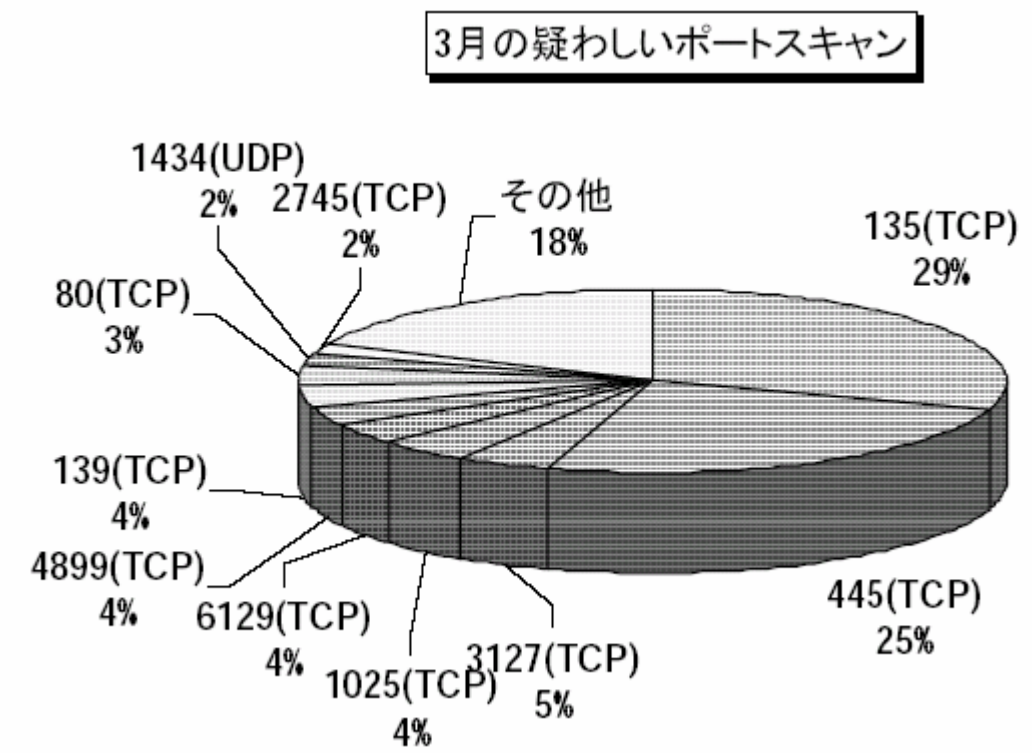
감염경로	피해 건수					
	2004년 3월		2004년 2월		2003년 3월	
메일	3,956	98.6%	1,247	94.2%	1074	90.5%
외부 감염	15	0.4%	6	0.5%	14	1.2%
다운로드	12	0.3%	1	0.1%	18	1.5%
네트워크	12	0.3%	58	4.4%	0	0%
기타	17	0.4%	11	0.8%	81	6.8%

[표2]일본사용자의 악성코드 주요 감염경로

일본 네트워크 트래픽 현황

[그림2]는 2004년 2월 일본에서 발생된 네트워크 트래픽의 포트 유형별 사용량을 나타낸 것이다. 135번과 445번 포트에서 발생하는 네트워크 사용량이 다른 포트의 사용량에 비해 현저하게 높은 것을 알 수 있고 이는 한국의 상황과 크게 다르지 않다. 이 두 포트는 윈도우 시스템에서 기본적으로 사용되는 포트이지만 블래스터 웜과 같이 RPC 취약점을 악용하여

전파되는 웜들의 감염 경로화 되고 있다. 또한 최근에는 많은 아고봇 변형들 또한 패스워드 취약점이나 RPC 취약점을 이용한 공격을 할 때 사용되고 있으므로 주의가 필요하다.
또한 3127 포트의 사용량이 매우 많은 것을 알 수 있는데 이는 마이둠 웜에 감염된 시스템에서 웜이 사용하는 포트 중 하나로, 마이둠 웜 감염으로 인한 피해가 현재까지 계속되고 있음을 알 수 있게 해준다.
이외에도 전월과 비교하여 6129 포트의 사용량이 급격하게 증가하였는데 이는 원격관리 툴인 Dameware의 취약점을 찾으려는 스캐닝 시도로 보인다. 이와 관련된 취약점은 SecurityFocus 등 해외의 보안관련 사이트에서도 보고된 적이 있다.



[그림2]일본의 네트워크 트래픽 현황

V. 3월 중국 피해 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

중국의 악성코드 피해 TOP 5

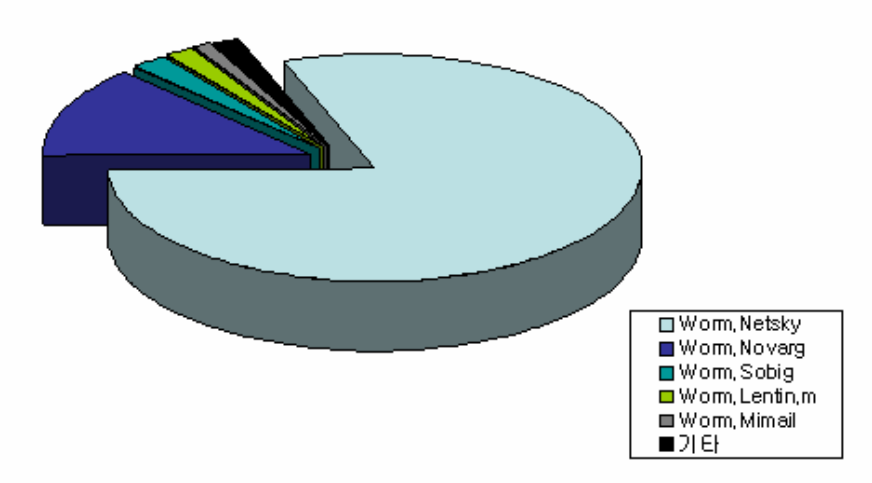
3월 중국 악성코드 동향의 전반적인 흐름은 1월 마지막 주를 시작으로 현재까지 지속적인 변형이 발견되는 Mass Mailer들 일색이었다. 이러한 Mass Mailer들의 동향은 전체 악성코드의 동향으로 이어질 정도로 큰 흐름을 만들어가고 있는 추세이다. 그리고 전자메일 주소를 갖고 있는 사람이라면 이 Mass Mailer들로 인해 수신한 메일조차 쉽게 확인하지 못하도록 만들었다. 이러한 Mass Mailer들의 확산은 인터넷 트래픽의 대부분을 차지하고 있다 하여도 과언이 아닐 정도로 높은 확산력을 보여 주었다.

순위 변화	3 월	Rising	CNCVERC
+ 2	1	Worm.Netsky	Worm_Mydoom.F
-1	2	Worm.Novarg	Worm_Netsky.D
New	3	Worm.Sobig	Worm_Bbeagle.J
-	4	Worm.Lentin.m	Worm_AgoBot
-3	5	Worm.Mimail	-

[표1]2004년 3월 중국의 악성코드 피해 TOP 5

이러한 Mass Mailer들의 확산은 중국 백신업체인 라이징(Rising)사와 정부연구기관인 중국국가컴퓨터바이러스대응중심(China National Computer Virus Emergency Response Center, 이하 CNCVERC)이 작성한 TOP 5를 볼 경우 더욱 명확해진다. 2월과 비교하여 순위상으로 가장 큰 변화는 가장 많은 변형이 등장하여 지난 달 3위에서 2계단이나 상승한 Worm.Netsky(Win32/Netsky.worm, 이하 넷스카이 웜)가 차지하고 있다. 이 넷스카이 웜의 급격한 확산으로 인해 기존의 Mass Mailer들은 모두 순위 하락을 보였으나 Worm.Sobig(Win32/Sobig.worm, 이하 소빅 웜)만 다시 순위권으로 진입하는 현상을 보였다. 그리고 넷스카이 웜와 함께 지속적인 변형이 등장하여 많은 사람들을 괴롭혔던 Worm.BBeagle(Win32/Bagle.worm, 이하 베이글 웜)은 새로운 변형들의 발견에도 불구하고 지난 달 5위를 마지막으로 순위권에서 벗어날 정도로 급격한 쇠퇴를 보였다. 이는 넷스카이 웜이 확산되면서 베이글 웜의 정상적인 실행을 방해하는 기능으로 인해 짧은 시간에 급속한 쇠퇴를 보인 것으로 추측이 된다.

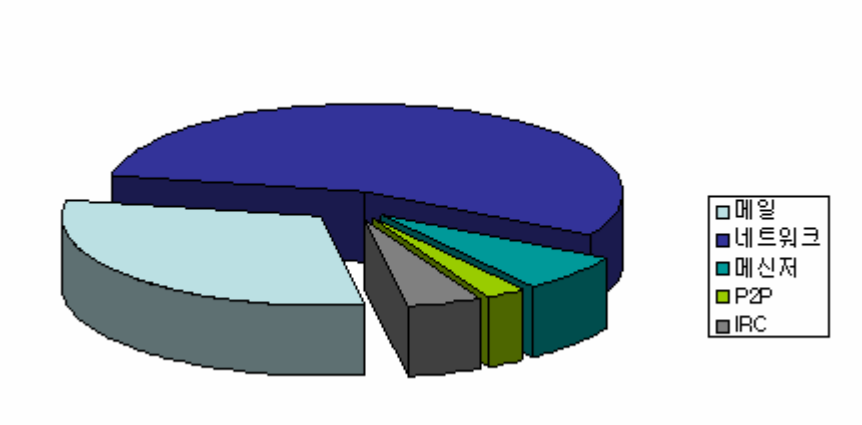
중국의 악성코드 분포



[그림1]중국의 2004년 3월 악성코드 분포현황

TOP 5에서 1위를 차지하고 있는 넷스카이 웜이 지난 달 8.2%에서 급격히 증가한 75%를 차지하고 있으며 지난 달 3위에서 1위로 2계단이나 올라섰다. 그러나 Worm.Novarg(Win32/MyDoom.worm, 이하 마이둠 웜)은 급속한 증가를 보인 넷스카이 웜과 반대로 그 영향력이 급격히 감소하여 12.6%를 차지하고 있다. 그러나 이 두 Mass Mailer가 전체의 90% 가까이 차지하고 있는 점으로 미루어 중국 내의 확산이 국외와 비교하여 많은 차이를 보이지 않고 있다는 것을 추측할 수 있다. 나머지 10% 정도를 TOP 5의 순위대로 소빅 웜이 2.27%, Worm.Lentin.m(Win32/Yaha.worm, 이하 야하 웜)이 1.74%, Worm.Mimail(Win32/Mimail.worm, 이하 미메일 웜)이 1.11%를 차지하고 있다. 그 외 4.89%를 차지하여 기타에 포함된 악성코드들로는 베이글 웜, Trojan.QQMSG.Boker, Worm.Agobot.3(Win32/AgoBot.worm, 이하 아고봇 웜), Worm.Blaster(Win32/Blaster.worm, 이하 블래스터 웜), Worm.Lovgate(Win32/Lovgate.worm, 이하 러브게이트 웜)와 Worm.Welchia(Win32/Welchia.worm, 이하 웰치아 웜)가 있다. QQ 메신저를 감염 경로로 이용하는 Trojan.QQMSG.Boker와 같은 트로이목마 역시 많은 감염은 보이지 않으나 지속적으로 다양한 형태가 발견되고 있다.

악성코드의 감염경로별 현황



[그림2]중국의 2004년 3월 감염경로별 악성코드 현황

3월에 라이징(Rising)사에서 공개한 악성코드들의 감염 경로 대부분이 [그림2]와 같이 운영체제의 취약점을 이용한 네트워크 웜과 메일을 이용한 웜 이 두 부류가 차지하고 있다. 그러나 전체적인 흐름으로 미루어 메일을 감염경로로 이용하는 Mass Mailer가 절대 다수일 것이라는 예상과는 달리 네트워크를 감염경로로 이용하는 웜이 Mass Mailer류보다 단지 양적인 면에서만 앞서고 있었다. Mass Mailer는 양적인 면에서는 그 의미가 적으나 확산도면에서는 오히려 네트워크 웜을 월등히 앞서고 있는 것은 [그림1]에서 명확히 드러난다. 그 외로는 QQ메신저, P2P, IRC등을 감염경로로 이용하는 악성코드 역시 꾸준히 발견되고 있다.

VI. 테크니컬 컬럼 – 베이글 웜으로 보는 악성코드 진화

작성자 : 차민석 주임연구원(jackycha@ahnlab.com)

컴퓨터 바이러스/웜과 생물학적 바이러스/웜은 여러 부분에서 유사점이 존재한다. 자기 복제 능력의 유사성이 가장 크지만 진화의 측면도 비교해 볼 수 있다. 생물학적 바이러스 혹은 웜은 새로운 환경에 적응하기 위해 끊임없는 돌연변이를 만들어 낸다. 이와 유사하게 컴퓨터 바이러스와 웜도 백신이나 사용자들로부터 자신의 존재를 숨기기 위해 끊임없이 개선된다. 차이점이라면 생물학적 바이러스나 웜은 자연 발생적이지만 컴퓨터 바이러스나 웜은 대부분 제작자가 인위적으로 개선한다는 차이점이 있다. 어쩌면 생물학적 바이러스나 웜도 인간이 알지 못하는 어떤 법칙이나 신과 같은 존재에 의해 개선되고 있는 건 아닐까?

일반적으로 동일인 혹은 동일 그룹에서 유사 변형을 만들며 대부분 백신의 진단을 피하면서 조금씩 새로운 기능이 추가되는 형태로 진화(?)를 한다. 2004년 1월부터 발견된 Win32/Bagle.worm (이하 베이글 웜)의 예를 들어 악성 코드가 어떻게 진화되었는지 살펴보자.

발견시기	이름	특징
2004.1.18 2004.2.17 2004.2.27 2004.2.28	Win32/Bagle.worm.15872 Win32/Bagle.worm.11264 Win32/Bagle.worm.15872.B Win32/Bagle.worm.15872.C	초기 버전들
2004.2.29 2004.2.29 2004.2.29	Win32/Bagle.worm.E Win32/Bagle.worm.F Win32/Bagle.worm.G	초기 버전들
2004.3.1 2004.3.2 2004.3.3 2004.3.3	Win32/Bagle.worm.H Win32/Bagle.worm.I Win32/Bagle.worm.J Win32/Bagle.worm.K	암호 걸린 압축 파일 사용(암호는 메일 본문에 포함시킴)
2004.3.13	Win32/Bagle.worm.N	암호 걸린 압축 파일(암호는 그림형태)
2004.3.15 2004.3.18 2004.3.18 2004.3.18 2004.3.18	Win32/Bagle.worm.O Win32/Bagle.worm.P Win32/Bagle.worm.Q Win32/Bagle.worm.R Win32/Bagle.worm.S	바이러스 기능 포함
2004.3.26 2004.3.29	Win32/Bagle.worm.U Win32/Bagle.worm.V	간단해진 웜

[표1]주요 베이글 웜의 특징

탄생

2004년 1월 19일 새벽에 최초 감염 시 계산기가 실행되고 특정 웹사이트에 접속하려는 기능이 있는 웜이 발견되었다. Win32/Bagle.worm.15872[3]로 보통 베이글 웜이라고 부르고 있다. 2월 말까지 발견된 초기 버전의 베이글 웜은 메일의 첨부 파일로 전파되는 별다른 특징이 없는 웜 중에 하나였다.

암호 걸린 압축 파일 속에 숨기

2004년 3월 1일 발견된 Win32/Bagle.worm.H(이하 베이글. H 웜)[4]는 웜 파일이 포함된 압

[3] 베이글 웜 원형, http://info.ahnlab.com/smart2u/virus_detail_1297.html
[4] http://info.ahnlab.com/smart2u/virus_detail_1331.html

축 파일을 첨부 파일로 보내며 이 압축 파일에 암호가 걸려있다. 많은 기업이 메일로 전파되는 악성코드를 차단하기 위해서 백신 제품을 설치해 둔다. 백신은 메일에 첨부되는 ZIP, RAR 와 같은 압축 파일 속 파일도 검사하지만 암호가 걸린 압축 파일은 검사에서 제외한다. 즉, 베이글.H 웜의 경우 백신이 설치되어 있어도 웜은 압축 파일 형태로 그냥 사용자에게 전달되는 결과가 발생했다. 이에 백신에서 이 웜에 대한 진단 기능이 추가되었지만 메일 서버 차원에서 막을 수 없어 고객들의 컴퓨터로 웜 파일이 포함된 메일이 그대로 전달되는 문제가 발생했던 것이다. 이에 백신 업체는 제한적이지만 암호 걸린 압축 파일 형태의 베이글 웜도 진단하게 된다. 백신 업체는 암호가 다른 형태로 도착하면 어떻게 할 것인가 심각하게 고민하게 되는데 이 고민이 현실로 나타난다.

3월 13일 발견된 Win32/Bagle.worm.N (이하 베이글.N 웜)[5]은 암호가 그림으로 되어 있어 본문에서 비밀번호를 추측하는걸 어렵게 한다. 다행히 비밀번호가 숫자로 이뤄지고 진단에 큰 문제는 없지만 향후 암호 걸린 압축 파일 형태로 전파되는 웜을 어떻게 차단할지 백신 업계는 고민하고 있다.

바이러스 기능

3월 15일 발견된 Win32/Bagle.worm.O (이하 베이글.O 웜)[6]은 윈도우 실행 파일(PE 형 EXE 파일)을 감염시키는 기능도 포함하고 있다. 웜과 바이러스의 차이점은 감염 대상이 존재하느냐 존재하지 않느냐 하는 것이다. 웜은 다른 파일을 감염시키지 않고 독립적으로 존재한다. 따라서, 웜은 웜 파일만 삭제하면 치료가 되므로 치료가 쉬운 편이지만, 바이러스는 실행 파일을 수정해 감염시키기 때문에 감염된 파일을 원래 파일로 복구해야 하므로 웜에 비해 치료가 어려운 편이다. 또한 바이러스가 파일을 감염시키면서 파일을 손상시킬 수 있고 백신으로 치료해도 이전 파일과 100% 동일하지 않을 수 있다.

다시 처음으로

3월 26일 메일 제목, 본문이 없고 실행 파일만 하나 첨부되는 웜이 발견되었다. Win32/Bagle.worm.U (이하 베이글.U 웜)[7]으로 이름 붙여진 이 웜은 아주 간단한 형태이다. 웜 제작자는 다시 처음부터 만들고 싶었을까?

앞으로 등장할 베이글 웜은?

향후 등장한 베이글 웜은 어떤 새로운 기법을 사용할까? 가장 높은 가능성은 은폐기법을 사용하는 형태가 아닐까 싶다. 최근 악성코드는 사용자나 백신으로부터 자신의 존재를 숨기는 은폐기법(Stealth Technique)을 사용하는 경우가 많다. 은폐기법은 도스 시절부터 사용되는

[5] http://info.ahnlab.com/smart2u/virus_detail_1343.html
[6] http://info.ahnlab.com/smart2u/virus_detail_1345.html
[7] http://info.ahnlab.com/smart2u/virus_detail_1355.html

바이러스 기법 중 하나이지만 윈도우 시대로 넘어오면서 기술의 한계로 한동안 시범적으로만 사용되다가 최근 윈도우의 비밀(?)이 하나 둘 벗겨지면서 많은 악성코드 제작자들이 은폐기법을 지속적으로 개선하고 있다. 백신에게 윈도우 환경에서 은폐기법은 여전히 해결해야 할 문제 중 하나이다. 향후 등장할 베이글은 은폐기법을 사용해 자신의 존재를 백신이나 사용자로부터 숨기는 기법을 사용할 가능성이 높다.