ASEC
Annual Report
2004

안철수연구소의
시큐리티대응센터(AhnLab Security E-response Center)는
악성코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여
바이러스와 보안 전문가들로 구성되어 24시간 운영되는
보안대응 전문조직입니다.

ASEC Annual Report는 안철수연구소의 ASEC에서
고객에게 보다 다양한 정보를 제공하기 위하여
2004년 한해동안의 바이러스, 웜 등 악성코드와 시큐리티에 대한
종합된 정보와 보안동향을 요약하여 리포트 형태로 제공하고 있습니다.

Ahn 안철수연구소

Ahn 안철수연구소

목 차

Ⅰ. 2004년 악성코드 피해 동향

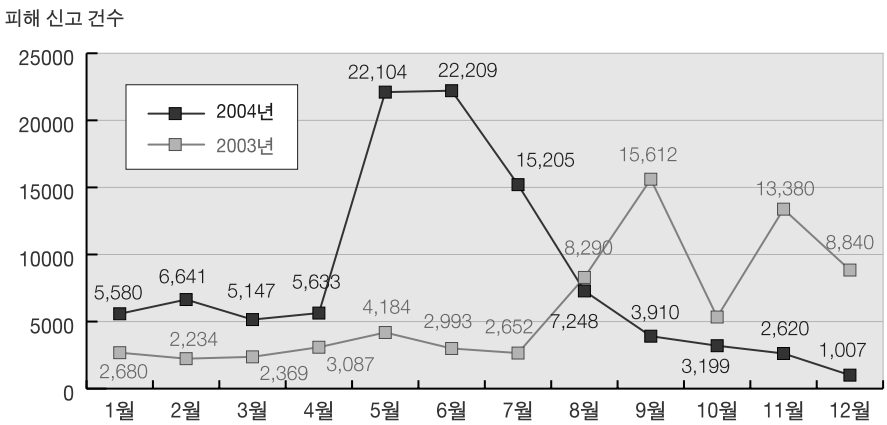
작성자 : 안철수연구소 허종오 연구원(maha96@ahnlab.com)

2004년 바이러스 피해 통계

작년 2003년 한 해는 2002년에 비해 악성코드에 대한 피해 문의가 급증했던 한 해였다. 그러나 2003년의 기록은 2004년 상반기 동안에 깨지고 말았다. 이는 매스메일러(Mass Mailer)의 급격한 증가와 다양한 유형의 악성 IRC봇(IRCBot) 출현이 주된 원인이다. 하지만 6월에 22,209건의 피해 신고 건수를 정점으로 피해건수가 줄어들어 8월부터는 작년 동 기간보다 피해 신고 건수가 감소하였다. 여러가지 원인이 있으나, 7월부터 피해 신고 통계에서는 악성코드에 감염된 시스템이 안철수연구소 바이러스신고센터의 메일계정으로 직접 발송하는 매스메일러 웜의 건수를 통계에 제외함에 따라 감소가 발생하였다. 하지만, 상위 Top 20에 기록된 악성코드의 순위는 변동사항이 없어, 통계추출 방법에 상관없이 매스메일러의 감염도는 여전히 높다는 것을 알 수 있다.

	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	합계
2003년	2,680	2,234	2,369	3,087	4,185	2,993	2,652	8,290	15,612	5,339	13,380	8,840	71,661
2004년	5,580	6,641	5,147	5,633	22,104	22,209	15,205	7,284	3,910	3,199	2,620	1,007	100,539

[표1] 2003, 2004년 국내 악성코드 피해신고 통계 수치(2004년은 12월 10일까지 데이터)



[그림1] 2003, 2004년 월 단위 피해신고 건수 비교

[표1]에서와 같이 2004년 총 피해신고 건수는 100,539건으로 전년대비 140%나 증가한 것을 볼 수 있다. 이를 그래프로 나타내면 [그림1]과 같이 특정 월에 비약적으로 증가한 것을 볼 수 있다.

이렇게 특정 월에 피해신고가 급증한 것은 그만큼 해당 월에 큰 피해를 주었던 악성코드가 많았기 때문이다. 대표적으로 1월부터 3월은 두마루 웜(Win32/Dumaru.worm), 5, 6월에 매스메일러인 넷스카이 웜(Win32/Netsky.worm)으로 인해 지금까지 보지 못했던 기록적인 피해 문의건수가 집계되었다. 이는 새로운 매스메일러의 출현도 이유일 수 있으나, 제작자간의 경쟁으로 인한 수 많은 변형의 출현, 감염된 시스템 증가로 메일을 발송하는 양이 늘어난 것이 이처럼 기록적인 피해 문의건수가 접수된 주요 원인 중의 하나일 것으로 추측된다. 7월부터는 신고건수가 급격히 줄어 들었으나, 넷스카이 웜 변형은 지속적으로 매월 최다 피해 신고를 기록하였다. 이는 제작자가 만들어 유포시킨 변형이 끈질긴 생명력을 유지한 채로 남아 있어 피해를 유발하고 있기 때문이다.

악성코드 피해 Top 20

2003년과 올 한해 피해를 많이 주었던 악성코드는 어떤 것이 있었는지 Top 20을 뽑아보면 [표2], [표3]과 같다.

악성코드명	건수
Win32/Sobig.worm.F	14,949
Win32/Dumaru.worm.9234	14,741
Win32/Blaster.worm.6176	4,901
Win32/Yaha.worm.45568.B	4,732
Win32/LovGate.worm.107008	1,571
Win32/Parite	1,174
Win32/Parite.B	1,000
Win32/FunLove.4099	899
Win32/Welchia.worm.10240	819
Win32/Valla.2048	803
JS/Fortnight	728
Win95/Spaces.1445	725
Win32/Klez.worm.H	682
MIRC/Stde9	608
Win32/Yaha.worm.27648	544
HTML/Redlof	538
Win32/Nimda	499
Win32/Opasoft.worm.28672	489
Win32/Elkern.B	443
Win32/Yaha.worm.45568	436

[표2] 2003년 악성코드 피해 Top20

악성코드명	건수
Win32/Netsky.worm.29568	28,344
Win32/Dumaru.worm.9234	13,026
Win32/Netsky.worm.17424	9,164
Win32/Netsky.worm.28008	4,491
Win32/Netsky.worm.17920	4,221
Win32/Netsky.worm.22016	4,106
Win32/Netsky.worm.25352	3,187
Win32/Bagle.worm.Z	2,316
Win32/Sasser.worm.15872	1,879
Win32/Blaster.worm.6176	1,652
Win32/Netsky.worm.16896.B	1,132
Win32/Netsky.worm.22016.C	686
Win32/MyDoom.worm.32256	404
Win32/Agobot.worm.104960	385
Win32/Bagle.worm.Y	338
Win32/Parite	256
Win32/Yaha.worm.45568.B	247
Win32/LovGate.worm.128000	270
Win32/AgoBot.worm.197120.C	228
Win32/Welchia.worm.12800	172

[표3] 2004년 악성코드 피해 Top 20

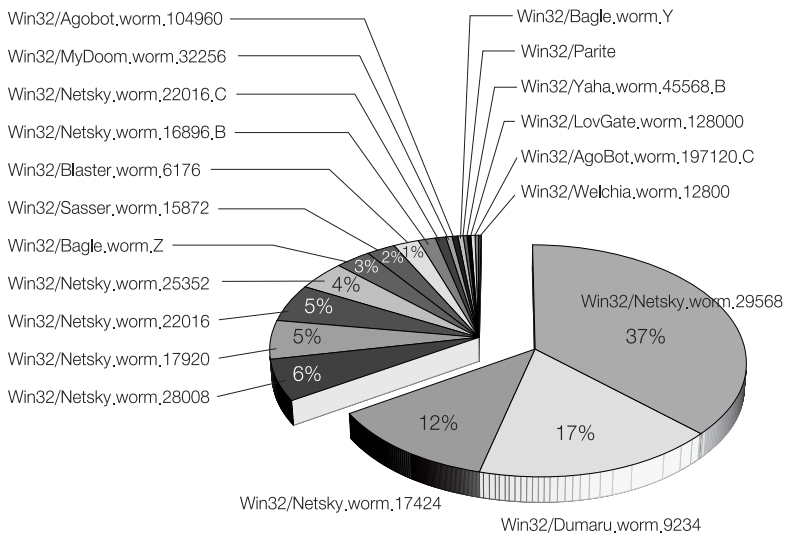
* 2004년 자료는 2004년 12월 10일까지의 자료임

[표1]의 전체피해 문의건수도 차이가 나지만 특히 올해는 넷스카이 웜 변형들이 상위 Top 10의 대부분을 차지하였으며, 매스메일러 중에서 이와 같이 많은 변형으로 피해를 입혔던 적은 없었다.

[표3]의 피해신고 기준으로 선정한 악성코드 Top 5를 순서대로 간략히 정리해보면 다음과 같다.

- Win32/Netsky.worm.29568
- Win32/Dumaru.worm.9234
- Win32/Netsky.worm.17424
- Win32/Netsky.worm.28008
- Win32/Netsky.worm.17920

1, 2위의 비중이 전체 신고의 41%에 달해 피해의 파급력이 소수의 악성코드에 집중됐으며 Top 5 중 4개가 2004년도 상반기에 발견된 악성코드라는 것이 특징이다.
피해신고의 월별 상황을 보면 전체적으로 전년 대비 증가한 것은 공통적이나, 상반기에 집중적으로 넷스카이 웜 변형이 30개 이상 발견되었으며, 넷스카이 웜 제작자가 체포되고 난 후부터 더 이상 변형이 제작되지 않았으나, 제작자가 만들어 유포시킨 변형이 여전히 생명력을 유지한 채로 피해를 유발하고 있다. [표3]의 올해의 악성코드 Top 20 자료를 비율로 확인해 보면 [그림2]와 같다.



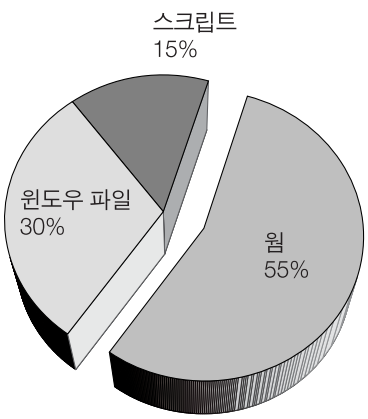
[그림2] 2004년 악성코드 피해 문의건수 Top 20

[그림2]를 보면 상위에 속해 있는 악성코드들은 모두 메일로 전파되는 매스메일러 웜으로, 기본적으로 메일로 자동 발송될 뿐 아니라 아웃룩 주소록은 물론 다양한 파일에서 주소를 추출해 웜

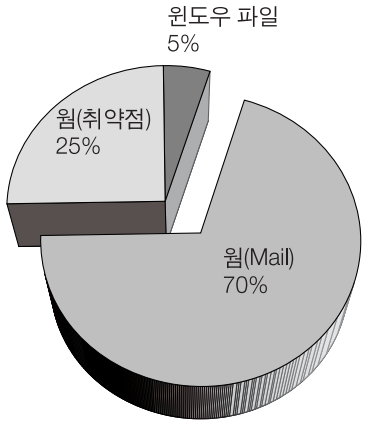
메일을 발송하기 때문에 동시에 다수의 사용자에게 웜 메일이 발송되었다. 두마루 웜의 경우 또한 마이크로소프트(Microsoft)사에서 발송한 패치정보로 오인하게끔 발송자를 속이기도 하여 피해의 규모가 컸다.
넷스카이 웜 변형 중 넷스카이.28008 웜(Win32/Netsky.worm.28008)은 메일과 윈도우 익스플로러 취약점을 이용하여 전파되는 형태로써, 이용하는 취약점은 2001년에 발견된 매우 오래된 취약점(MS01-020)이지만, 피해 문의건수는 4위를 차지하고 있다. 이는 사용자들이 아직까지 보안 패치의 중요성에 대한 의식이 낮다는 것을 반증하고 있다.

2003년, 2004년 악성코드 Top 20 유형별 현황

2003년, 2004년 악성코드 Top 20 의 유형별 분류를 살펴보면 [그림3], [그림4]와 같다.



[그림3] 2003년 Top 20 악성코드 유형별 현황



[그림4] 2004년 Top 20 악성코드 유형별 현황

2003년도는 웜과 윈도우 파일 바이러스, 스크립트 세 유형의 악성코드로 나누어졌다. 순위에 포함된 악성코드들은 모두 Win32 환경에서 동작되었으며 특히 많은 비중을 차지하는 웜의 경우 전통적인 형태의 매스메일러가 주를 이루고 있다. 또한 윈도우 파일 바이러스가 많았던 것은 악성 IRC봇 트로이목마에 바이러스가 감염되어 널리 확산되었기 때문이다. 스크립트라는 항목을 차지하고 있는 것은 악성 IRC봇 트로이목마에 의해서 설치된 mIRC 스크립트를 뜻한다.

2004년도 피해문의 대부분은 매스메일러가 전부라고 해도 과언이 아닐 정도로 메일로 전파되는 악성코드 유형이 많았다. 웜(취약점)은 올 악성코드의 주요한 동향인 '취약점'을 이용하여 네트워크로 전파되는 악성코드류이다. 대표적으로 악성 IRC봇 웜들이 이에 해당된다. 메일에 의한 전파방법이 전통적이라면 취약점과 네트워크로의 확산은 오래 전에 선보였지만 이제는 확고한 하나의 악성코드 전파경로로 자리 매김하고 있다. 전통적인 악성코드인 윈도우 파일은 불

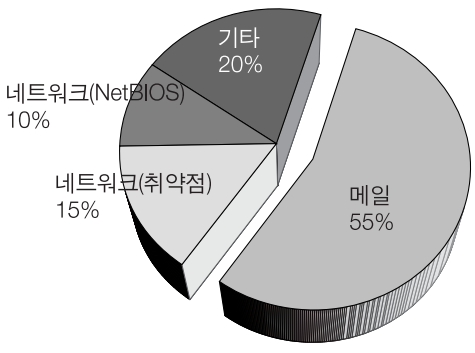
과 5%만의 점유율을 차지하고 있다. 이는 윈도우 파일 바이러스 제작의 어려움과 확산의 어려움 등이 감소 원인일 수 있으나, 급격히 증가한 매스메일러로 인한 상대적 감소로 볼 수 있다.

2003년, 2004년 악성코드 Top 20 의 전파방법별 현황

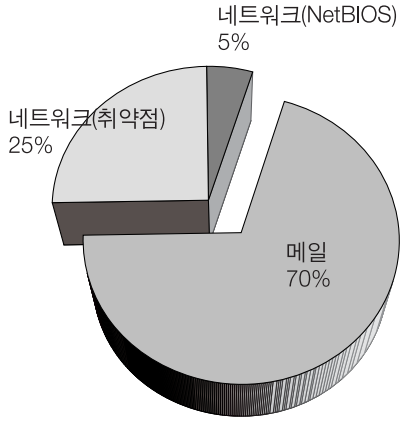
2003년의 악성코드 전파방법은 악성 IRC봇 류에 감염된 채로 전파된 윈도우 파일 바이러스 때문에 공유폴더 즉, 관리목적 공유폴더로 전파되는 악성코드들이 많았던 것을 알 수 있다. 이는 악성코드가 기존에 사용자의 실행을 필요로 하는 수동적인 감염형태에서 능동적인 감염형태로 발전하는 양상을 보인 것이다.
2004년에 들어서 웜은 2003년과 같이 메일을 이용한 전파가 대부분이었으나, 윈도우 네트워크 취약점을 적극 활용하는 기술적으로 한 단계 진화한 지능형 전파방법을 사용하는 웜이 증가하였다.
2003년과 2004년도의 악성코드 Top 20을 비교하여 어떠한 전파방법을 많이 이용하였는지 파악하여 분류한 결과는 [그림5], [그림6]과 같다. 그 기준은 해당 악성코드가 하나 이상의 전파방법을 가지고 있다면 가장 많이 사용되고 피해가 많았던 것을 기준으로 하였다.

- 메일
- 네트워크(취약점)
- 네트워크(NetBIOS)
- 기타

위 항목 중 네트워크 취약점과 NetBIOS로 분류한 것은 2003년에 들어서부터 취약점 (윈도우 관리목적공유폴더 포함)을 이용하여 전파되는 악성코드들이 많았기 때문이다. 기타로 분류한 것은 대부분 윈도우 파일 바이러스들로서 직접 실행되어야만 감염활동을 하는 것이고 다른 분류에 비하여 건수가 작아 기타로 분류하였다.



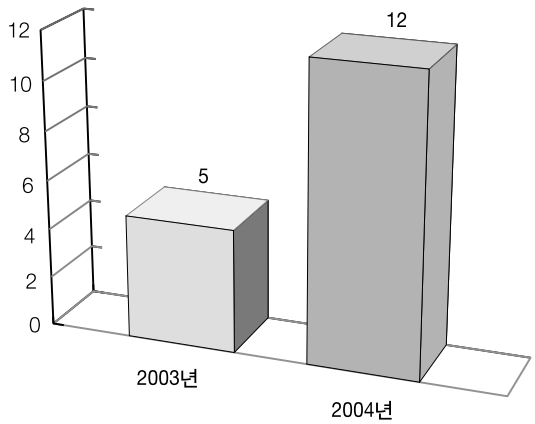
[그림5] 2003년 악성코드 Top 20 전파방법



[그림6] 2004년 악성코드 Top 20 전파방법

[그림5]에서도 알 수 있듯이 수적으로는 메일로 전파되는 방법이 더 많았지만 2003년부터 두드러지게 나타나는 것이 바로 취약점과 사용자의 관리소홀 문제로 전파되는 유형의 웜이 증가한 현상이다. 2003년 8월 RPC DCOM 관련 취약점을 이용한 블래스터 웜을 시작으로 이 취약점을 이용하는 악성코드가 큰 파란을 일으킨 후에도 여전히 많은 악성코드들이 취약점을 사용하고 있다. 또한 사용자들의 관리소홀로 인하여 관리목적 공유폴더를 이용한 전파방법(weak 및 null password session)도 악성코드 제작자들이 즐겨 사용하는 전파방법이 되었다.
2004년에는 넷스카이 웜의 영향으로 메일로 전파되는 방법이 대다수를 차지하였으나, IRC봇과 같이 네트워크 취약점을 이용하는 방법이 증가되었다는 것을 알 수 있다. IRC봇은 처음에는 아주 조악한 형태로 IRC 클라이언트에 배치파일, IRC 스크립트 그리고 원격의 파일을 실행해 주는 툴 등으로 구성되어 전파되었다. 그 후 2003년 하반기부터 등장하기 시작하여 2004년 상반기에 급격히 증가한 악성 IRC봇 웜들은 이전과 다르게 별다른 유틸리티의 도움없이 자체적으로 네트워크를 스캔하여 윈도우 취약점이 있는 시스템에 감염되도록 설계되었다. 악성 IRC봇이 올해 수적으로 증가함에도 불구하고 피해문의에 있어서 많은 점유율을 차지하지 못한 이유는 불특정 다수에게 전파되지 못했기 때문이며, 다수의 여러 변형이 만들어져 공격에 실패한 IRC봇은 바로 제작자들이 이용하지 않았기 때문이다. 즉 매스메일러처럼 어느 한 웜에 피해문의가 집중되지 못하고 수많은 변형으로 분산되다보니 수적으로 증가하여도 피해문의는 분산될 수 밖에 없는 것이다. 이런 악성 IRC봇류의 변화와 맞물려 2004년에는 네트워크를 통하여 취약점이 존재하는 시스템을 감염시키는 악성코드가 늘어났다.

2003년도와 같이 올해도 악성코드들은 자신을 전파하기 위해서 메일 및 네트워크 등을 기본적으로 이용하며, 윈도우 취약점까지 이용한 지능적인 전파방법을 사용하고 있다. 따라서 악성코드들은 하나 이상의 전파경로를 가지는 것은 이제 일반적인 것이 되어 버렸다. 2003년과 2004년의 악성코드 Top 20을 비교하여 하나 이상의 전파방법을 가진 악성코드의 비율이 어떤지, 그 방법은 무엇인지 확인해보자.



[그림7] 2003년, 2004년 다수의 전파경로를 가진 악성코드 수

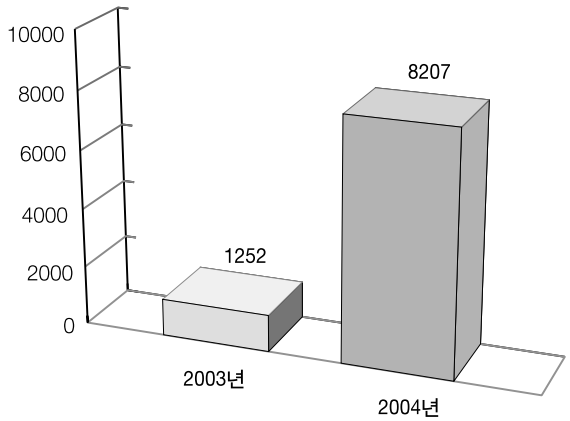
[그림7]에서도 볼 수 있듯이 2003년도는 Top 20 중 5개로 25%를 차지했던 것이 2004년도에는 12개로 60%를 차지할 만큼 폭발적인 증가를 보였다. 이는 사용자들이 의심메일에 대한 미열람 및 공유폴더 관리에 대한 관심이 높아짐에 따라 악성코드 제작자 역시 지능적으로 변모하여 다수의 전파경로를 가진 악성코드를 제작하였기 때문이다. 다수 이상의 전파경로를 가지는 악성코드 주요 경로는 다음과 같다.

- 메일(SMTP, MAPI 등의 두개의 프로토콜을 사용)
- 네트워크(공유폴더)
- 네트워크(취약점, 관리목적공유폴더)
- 메신저(하나 이상의 메신저를 이용, 예를 들어 MSN, Yahoo Messanger 등)
- P2P 응용 프로그램(다양한 종류의 P2P 응용 프로그램을 이용한 전파)

2003년, 2004년 피해문의 접수된 악성코드의 종류

세상에는 얼마나 많은 종류의 악성코드가 존재할까? 그 중 우리에게 실질적으로 피해를 입히고 있는 것은 과연 몇 종류나 될까? 많은 사용자들이 이러한 궁금증을 가지고 있다. 실제로 세상에는–변형 분류기준에 따라 조금씩 차이는 있지만–수 만개의 악성코드가 존재한다. 하지만 이 중에서 실제로 사용자들에게 큰 피해를 입히고 있는 것은 몇 종류에 불과하다.

올해 악성코드 종류 수는 안철수연구소가 통계를 집계한 이후로 최다를 기록하였다.
다음은 2003년, 2004년 상반기 고객들에게 문의된 악성코드 종류에 대한 통계이다. 물론 이중에 상위 20개 정도만 다수의 감염보고를 일으키는 악성코드이고 그 이하는 하나 또는 몇 건의 신고에 그친 것이 대부분이다. 하지만 사용자들이 얼마나 많은 종류의 악성코드의 위협에 노출되어 있는지 알 수 있다.



[그림8] 2003년, 2004년 피해문의 접수된 악성코드 수

[그림8]에서 알 수 있듯이 2004년도는 피해문의 접수된 악성코드 수가 전년도에 비해 무려 655%나 증가했다. 증가의 주된 원인은 바로 아고봇 웜(Win32/AgoBot.worm)과 같은 악성 IRC봇 웜 유형이 폭발적으로 증가했기 때문이다. 일례로 2004년 6월에 문의된 악성코드 중 웜으로 분류되는 것만 665종이었으며, 이후 매월 피해문의 접수 건 중 80~90% 이상이 악성 IRC봇 류이다.

2004년의 악성코드 피해동향을 정리해 보면 다음과 같다.

- 전년도와 같이 다양한 매스메일러에 의한 대량 메일발송과 그로 인한 피해문의건수 증가
- 악성 IRC봇 웜 변형의 폭발적인 증가로 인하여 피해 문의되는 악성코드 종류 증가

2004년도는 메일러(Mailer)들과 악성 IRC봇 웜 변형의 증가로 각종 통계의 기록을 매월 경신하였다. 특히 매일 새로운 IRC봇 웜의 출현으로 백신업체들은 2004년 한 해 동안 IRC봇과의 전쟁을 하였으며, 이 전쟁은 2005년에도 계속될 것으로 예상된다.

II. 2004년 신종(변형포함) 악성코드 동향

작성자 : 안철수연구소 정진성 연구원(jsjung@ahnlab.com)

올해 신종(변형포함) 악성코드 동향을 한 문장들로 정의해 본다면 다음과 같다.

- 매스메일러(Mass Mailer)의 급격한 증가
- 악성 IRC봇 웜 변형의 폭발적인 증가
- 취약점을 이용한 악성코드 증가
- 모바일 및 64비트 악성코드의 등장
- 스팸(SPAM) 증가와 피싱(Phishing) 등장
- 금전적인 이익을 노린 악성코드 제작
- 애드웨어의 심각성 증가

올해는 모바일과 64비트 악성코드와 같이 새로운 악성코드 유형의 등장과 피싱과 같은 금전적인 피해유형이 등장했다는 점에서 지난해와 달리 그 의미가 있다고 하겠다. 새롭게 등장한 이러한 유형들은 2005년에는 올해보다 증가하여 피해를 줄 것으로 보고있다.

2004년 12월 10일까지 국내 발견된 신종(변형포함) 악성코드는 모두 4,406종으로, 지난해 동기 1,239종에 비하여 거의 4배 가까이 증가하였는데 [표1], [표2]와 같다.

월	트로이	웜	드롭퍼	파일	스크립트	리눅스	부트	매크로	합계
1월	50	7	18	7	3	0	0	0	85
2월	78	13	15	2	3	0	1	1	113
3월	76	12	24	3	1	2	0	0	118
4월	46	11	11	1	3	0	0	0	72
5월	39	13	14	4	2	0	0	0	72
6월	52	21	6	2	4	0	0	0	85
7월	59	10	4	3	1	0	0	0	77
8월	92	20	13	2	3	0	0	0	130
9월	78	28	7	1	2	0	0	0	116
10월	60	30	3	0	0	0	0	0	93
11월	61	58	2	0	2	0	0	0	123
12월	88	59	8	0	0	0	0	0	155
합계	**630**	**165**	**115**	**25**	**22**	**2**	**1**	**1**	**1239**

[표1] 2003년 상반기 신종(변형포함) 악성코드 유형별 집계표

월	웜	트로이	드롭퍼	스크립트	파일	리눅스	매크로	합계
1월	58	50	7	6	0	0	0	121
2월	146	130	8	1	1	0	0	286
3월	196	75	5	3	1	0	0	280
4월	403	111	0	7	1	0	0	522
5월	322	32	3	2	1	0	0	360
6월	402	59	2	1	0	0	0	464
7월	379	80	10	4	2	0	0	475
8월	358	87	9	8	0	0	0	462
9월	512	93	16	6	0	0	2	629
10월	274	82	13	0	0	2	0	371
11월	213	95	11	10	0	0	0	329
12월	64	38	1	3	1	0	0	107
합계	**3327**	**932**	**85**	**51**	**7**	**2**	**2**	**4406**

[표2] 2004년 상반기 신종(변형포함) 악성코드 유형별 집계표

다음은 1988년부터 집계된 국내 악성코드 발견 수이다. 올해는 다른 어느해보다 급증한 것을 볼 수 있다.

연도	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	총계
합계	1	6	28	21	17	34	76	128	226	256	276	379	572	435	277	1239	4406	8,377

[표3] 1998년 ~ 2004년 국내 발견 악성코드 통계(2004년 12월 10일 통계까지만 포함)

작년에 비해 4배 가까이 증가한 원인의 대부분은 악성 IRC봇 웜류에 의한 것이다. 보통 다음과 같은 종류가 있다.

- Win32/AgoBot.worm (이하 아고봇 웜)
- Win32/Rbot.worm. (이하 알봇 웜)
- Win32/SdBot.worm (이하 에스디봇 웜)
- Win32/SpyBot.worm (이하 스파이봇 웜)
- Win32/WootBot.worm (이하 우트봇 웜)
- Win32/ForBot.worm (이하 포봇 웜)

악성 IRC봇 웜 유형이 폭발적으로 증가한 반면 시초라 할 수 있는 악성 IRC봇 트로이목마는 동년과 대비하여 상당수 감소한 것을 알 수 있다. 2004년에는 악성 IRC봇 웜이 크게 증가하였는데, 그 원인은 다음과 같이 악성 IRC봇이 기술적으로 발전했기 때문이다.

- 자체 IRC 클라이언트 기능을 가지고 있어 별도의 IRC 클라이언트가 필요하지 않음
- 전파 및 원격실행 그리고 공격명령을 내리기 위해서 별도의 파일들이 필요했으나 이제는 이를 포함하고 있음, 단 하나의 실행파일로 동작함
- 악성 IRC봇 소스가 공개되고 제작 커뮤니티 등이 활성화됨

2004년 신종(변형포함) 악성코드의 특징

앞에서 언급한 2004년 신종(변형포함) 악성코드의 특징을 좀 더 자세히 살펴보자.

(1) 취약점을 이용한 악성코드 급증

지난해만 해도 해킹과 악성코드의 접목이라는 말로 IT 관련 매스컴에 보도되었던 취약점은 이제 더 이상 익스플로잇(Exploit) 코드발표에 그치지 않고 이를 이용한 악성코드의 출현으로 이어지고 있는 것이 당연시되고 있다. 물론 모든 취약점이 악성코드 제작에 이용되는 것은 아니다. 하지만 작년에 비하면 악성코드에 이용되는 취약점 수가 늘어나고 그 제작기간은 보안패치 파일이 나오기 전에 악성코드로 제작되어 확산되기도 하였다.
지난해 블래스터 웜(Win32/Blaster.worm)이 이용하였던 취약점은 발견된지 약 보름 후에 악성코드 제작에 이용되었던 반면 최근에는 취약점이 발표된 후 얼마 지나지 않아 익스플로잇이 공개되는 소위 말하는 Zero-Day 익스플로잇이 현실화되고 있다. 취약점 발표 후 가장 짧은 시간에 악성코드 제작이 된 경우는 위티 웜(Win32/Witty.worm)이다. 특정 보안제품의 취약점이 발표된지 2일만에 관련 악성코드가 발견되었다. 또한 11월에 발견된 보프라 웜(Win32/Bofra.worm)에서 사용하는 인터넷 익스플로러의 iFrame 태그 취약점의 경우 취약점이 공개되고 한 달정도 후에나 보안패치가 나올 정도로 사용자들이 위협에 노출되어 있는 시간도 길어지게 되었다.

이렇듯 많은 사용자들이 사용하는 윈도우 운영체계는 물론 이에 포함된 인터넷 익스플로러, 그리고 인터넷 기반의 FTP 및 WWW 서버까지, 취약점이 있다면 악성코드 제작자들은 이를 이용한 악성코드 제작에 열을 올리고 있다. 일례로 아고봇 웜에서는 무려 10가지가 넘는 다양한 윈도우 및 응용 프로그램의 취약점 공격코드를 이용하고 있다. 아고봇 웜의 전파에 이용되는 취약점은 일반적으로 다음과 같다.

- RPC DCOM2 Vulnerability (MS03-039)
- RPC DCOM Vulnerability (MS03-026)
- RPC Locator Vulnerability (MS03-001)
- WebDav Vulnerability (MS03-007)

- UPnP Vulnerability (MS01-059)
- Messenger Service Buffer Overrun Vulnerability (MS03-043)
- LSASS Buffer Overflow Exploit (MS04-011)
- Workstation Service Buffer Overrun Vulnerability (MS03-049)
- NetBIOS (관리목적공유폴더 대상)
- DameWare의 Mini Remote Control Server Overflow Vulnerability

이러한 취약점을 이용하여 전파되는 악성 IRC봇은 네트워크 트래픽 유발이라는 부작용(Side Effect)을 가져오기도 한다. 참고로 악성 IRC봇 웜들의 소스코드는 모듈화되어 있어 다른 누군가 새로운 취약점에 대한 익스플로잇 소스를 제공하면 이를 추가하여 새로운 변형 제작이 가능하도록 설계되었다.

올 9월에 알려진 JPEG 관련 GDI+ 익스플로잇은 대중적으로 많이 사용되는 JPEG 형식의 이미지 파일도 악성코드로부터 안전하지 못하다라는 인식을 주었다. 이와 더불어 윈도우 XP 시스템에서 사용되는 .EMF(확장메타파일)라고 알려진 이미지 파일에서도 이를 처리할 때 버퍼 오버플로우를 발생시킬 수 있는 익스플로잇이 공개되어 문제가 되었다. 이 두개의 취약점은 '사용자들이 주로 이용하는 이미지 파일과 같은 멀티미디어 파일들도 결코 안전하지 못할 수 있다'라는 점에서 적잖은 충격을 주었다.

또 하나의 변화는 이러한 취약점을 악성코드 제작자만 이용하는 것이 아니라 소위 애드웨어 제작자 또는 스팸메일을 보내는 스패머들도 OS 나 응용 프로그램의 취약점을 이용한다. 보통 스팸메일을 받는 사람이 메일 확인시 스크립트가 실행되거나 ActiveX를 사용하여 사용자 시스템에 애드웨어를 설치하고 불필요한 광고를 지속적으로 내보내게 하기도 한다.

(2) 악성 IRC봇 기반의 웜 폭발적 증가

악성 IRC봇 웜의 폭발적 증가 원인은 다음과 같이 정리된다.

- 제작자간의 커뮤니티를 이용한 조직적인 활동(Script Kiddies[1] 가 많음)
- 커뮤니티를 이용한 소스 공유
- 공격(확산, 감염)실패에 따라 추가 변형 제작
- 실행압축 프로그램류로 인한 변형 제작

1) 스크립트 키즈(Script Kiddies) : 해킹에 관련하여 특별한 코딩실력없이 다른 사람이 만들어 둔 툴 또는 소스등을 그대로 사용 또는 수정하여 악의적인 행위를 일삼는 사람을 지칭

주로 실력이 뛰어난 제작자가 커뮤니티에 소스를 공개하면 다른 제작자들이 이를 다운로드하여 자신만의 변형을 만들거나 개량하여 다시 커뮤니티 내에 공유하는 방식으로 여러 가지 변형이 제작, 유포되었다.

이러한 웜이 확산된 큰 이유 중 하나는 시스템에 대한 사용자들의 관리지식이 부족해서 오는 경우가 대부분이다. 즉, 보안패치 파일에 무관심하거나 윈도우 NT 기반의 시스템에서 로그인 암호가 없거나 누구나 유추하기 쉬운 암호를 사용한 경우 이러한 악성 IRC봇 웜에 쉽게 감염된다 하겠다. 또한 변형의 제작이 많았던 이유는 확산에 실패하면 또다른 변형을 제작하거나 추적을 피하기 위해 채널-IRC 상에서 대화방을 뜻함-을 보통 1~2일 정도만 유지하기 때문으로 추정되고 있다.

(3) 다양한 매스메일러(Mass Mailer)들의 등장

올해 두드러지는 또 하나의 특징은 바로 다양한 매스메일러들이 발견, 보고 되었다는 것이다. 주목할 것은 이러한 매스메일러들이 약 석달이라는 짧은 기간에 무려 각각 30가지가 넘는 변형이 나왔다는 것이고, 변형이 나올 때마다 기술적으로 발전하여 백신업체로서는 골치 아픈 존재였다. 주로 다음과 같은 것들이 있었다.

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

특히 베이글 웜과 마이둠 웜은 소스를 공개하였는데 마이둠 웜의 경우 이를 이용한 변형이 제작되었으며 다른 악성코드가 마이둠 웜이 감염된 시스템을 이용하여 자신을 감염시키는 유형도 발견되었다. 베이글 웜은 상반기가 끝난 7월초 자신의 소스를 웜 내부에 하드코딩하여 메일로 전파되도록 제작된 변형이 발견되기도 하였다. 또한 이러한 웜들은 지난해 다른 매스메일러와 달리 감염된 시스템에서 대량의 메일을 지속적으로 보내어 피해문의 건수가 대폭 증가하기도 하였다.

이러한 이메일(E-Mail) 웜 중에서는 경제적인 이익을 노린 악성코드 제작자 또는 집단이 제작한것으로 추정되는 것도 있어 충격을 주고 있다. 이는 더 이상 악성코드 제작이 과거와 달리 호기심이나 실력과시가 아닌 경제적인 이익획득을 노린것이어서 더욱 더 지능적이고 많은 변형을 제작하게 된 것은 아닐까 하는 추정도 해볼 수 있겠다.

(4) 진단/치료하기 어려운 악성코드 증가

또한 올 상반기에는 악성코드에 대한 진단/치료 백신개발을 지연시키기 위한 의도로, 다음과 같은 기법을 사용하는 악성코드가 여러 건 발견되기도 하였다.

- 메모리 형태로만 존재 또는 리모트쓰레드(RemoteThread)로 존재
- 커널모드 백도어(커널 드라이버를 이용하여 Native API 후킹)
- 스텔스(Stealth) 기법(다수의 Win32 API를 가로채서 자신의 존재를 숨김)

위와 같은 기법을 사용하는 악성코드의 수는 조금씩 증가하고 있다. 대표적으로 Explorer.exe에 리모트쓰레드로 기생하는 코르고 웜(Win32/Korgo.worm)을 들 수 있으며, 작년에 많은 피해를 주었던 러브게이트 웜(Win32/LovGate.worm) 역시 올해 들어 수 많은 변형이 발견되면서 역시 자신을 다른 프로세스의 리모트쓰레드로 기생하는 기법을 사용하였다. 이와 같은 기법을 사용하는 악성코드는 앞으로도 더욱 증가될 것으로 보인다. 이러한 형태의 악성코드는 V3를 제외한 대부분의 백신 제품에서 검사해 내지 못했다. 따라서 지원되지 않는 백신 업체들은 전용 백신이 아닌 자사의 제품에서 이를 진단하기 위해 제품의 수정 또는 별도의 개발이 이루어져야 할 것으로 보인다.

(5) 모바일 기기 관련 악성코드 등장

모바일 기기에 대한 보안위협은 계속적으로 문제제기 되어왔다. 그러던 중 올해 6월경 심비안 OS를 탑재한 특정 시리즈의 노키아 휴대폰에서 동작하는 세계 최초의 휴대폰 악성코드가 발견되었다. 카비르(Cabir)라고 알려진 이 웜은 블루투스(BlueTooth)를 이용하여 전파된다. 즉, 감염된 휴대폰 반경으로 일정거리에 위치한 휴대폰이 있다면 연결요청을 보내고 사용자가 이를 응답하면 해당 휴대폰도 감염되는 방식으로 전파된다.

```
!:#system#apps#caribe#caribe.rsc
!:#system#apps#caribe#flo.mdl
File will be run during install: !:#system#apps#caribe#caribe.app
```

[그림1] 카비르 설치파일

그 후 11월말 스컬스.B(Skulls.B)라고 명명된 또다른 휴대폰 악성코드가 등장했다. 이 악성코드는 변형된 카비르 웜을 포함하고 있었으며 설치되면 기존 휴대폰에 있는 *.AIF 파일(응용프로그램 정보파일)을 스컬스.B가 가지고 있는 것으로 겹쳐쓰게 된다.

```
C:¥System¥Apps¥WALLETAVMGMT¥WALLETAVMGMT.APP
C:¥System¥Apps¥WALLETAVOTA¥WALLETAVOTA.AIF
C:¥System¥Apps¥WALLETAVOTA¥WALLETAVOTA.APP
C:¥System¥CARIBESECURITYMANAGER¥CAMTIMER.sis
C:¥System¥CARIBESECURITYMANAGER¥caribe.app
C:¥System¥CARIBESECURITYMANAGER¥caribe.rsc
```

[그림2] 스컬스.B 설치파일들(일부생략)

카비르와 스컬스.B는 유럽지역의 GSM 단말기에서만 동작하므로 국내의 CDMA 환경에서는 동작하지 않지만, 국내도 위피(WIPI) 플랫폼이 대중화되면 위피 역시 보안위협으로부터 안전하지 못할 것으로 보인다. 또한 모바일 기기의 플랫폼으로 이용되는 윈도우 CE에서도 악성코드가 제작되어 보고 되고 있다. 모바일 관련 보안위협은 2~3년전부터 제기되어 왔고 관련 연구가 진행되었다. 따라서 일부 백신업체들은 관련 보안제품을 출시했거나 2005년에 출시를 목표로 개발중인 곳이 많다. 이렇듯 올해 들어 모바일 기기에 대한 보안 위협은 급격히 증가했고 악성코드 또한 출현한 상태로, 내년에는 모바일 기기 보안에 대한 새로운 백신 제품의 출시 등이 기대된다 하겠다.

(6) 64비트(Bit) 악성코드의 등장

현재 64비트 시장은 프로세서 제조사에 의해서 양분되고 있다. 바로 AMD64와 IA64이다. 인텔은 64비트 시장을 서버시장을 타켓으로 했지만 데스크탑용 64비트 프로세서 (EMT64)를 최근 선보이고 있다. 이에 반해 AMD는 인텔보다 먼저 64비트 프로세서를 개발, 생산하여 국내에도 제법 시장이 갖춰져 있다.

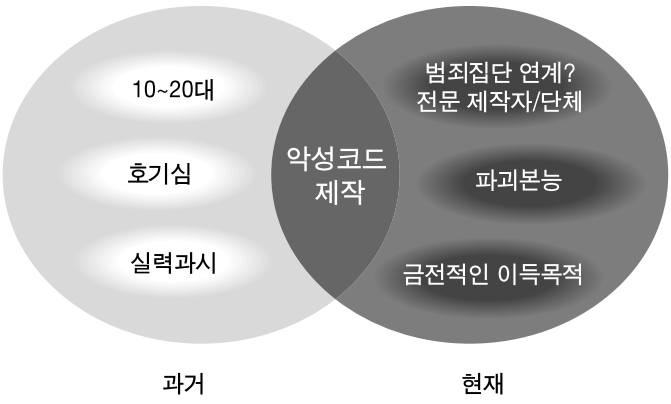
이러한 가운데 국외에서는 IA64, AMD64 환경에서 동작하는 악성코드가 5월과 8월에 각각 발견, 보고되었다. 물론 일반 사용자에게서 보고된 것은 아니며 악성코드 제작자가 제작 후 이를 백신업체에 보낸 것으로 추정된다. 이 두 악성코드는 모두 윈도우 파일 바이러스로 각 프로세서에 설치된 64비트 윈도우 XP에서 완벽히 동작하여 다른 파일을 감염시킨다.
백신업체들은 대부분 2003년에 자사의 서버 제품군들을 64비트로 포팅하거나 새롭게 개발하여 출시하였다. 또한 기존 악성코드와 64비트 관련 악성코드에 대한 대응연구도 진행하여 컨퍼런스를 통해서 발표하기도 하였다.
64비트 시장은 아직 운영체제 및 관련 응용 프로그램 지원의 미약으로 많은 사용자가 64비트 CPU에서 32비트 OS 및 응용 프로그램을 사용하는 반쪽짜리 64비트를 사용중이다. 이로 인하여 아직은 64비트 악성코드로부터 안전하다고 생각되지만 방심할 수는 없다. 운영체제 제작사가 관련 윈도우를 정식으로 출시하여 사용자가 많아지면 이를 노리는 악성코드 출현과 더불어 악성코드의 피해도 예상되기 때문이다.

(7) 스팸(SPAM) 증가와 피싱(Phishing)의 출현 그리고 검은 돈(Black Money)

스팸은 지난해에 이어 아주 골치 아픈 존재이다. 해마다 스팸은 증가하고 있다. 스팸을 보내는 스패머들은 지능적으로 발전했다. 이들은 과거에 메일서버 또는 스팸 메일러(SPAM Mailer)를 가지고 있었다. 그러나 이들은 더 이상 자신이 메일서버를 운영하지 않는다. 확인되지 않은 정보에 의하면 최근 피해를 많이 입혔던 특정 이메일 웜 또는 이 웜이 다운로드하는 트로이목마들 중 일부가 프락시(Proxy) 기능을 지원하는 SMTP 서버의 역할을 한다는 것이다. 즉, 스패머들이 스팸을 발송하기 위해, 그리고 추적을 피하기 위해서 이메일 웜에 감염된 불특정 다수의 PC를 이용한다는 것이다. 이는 매우 설득력 있는 추론이다. 또한 최근 문제가 되는 피싱 역시 '사기'라는 전통적인 범죄수법이지만 이를 온라인상에서 이용하여 금전적 이익을 노린 '디지털 사기'라 불리우고도 있다.

최근 들어 악성코드 제작자의 제작 동기가 변화하였다. 과거 악성코드 제작자들은 호기심과 자신의 능력을 과시하기 위해서 악성코드를 제작했다. 하지만 최근에 이들은 자신의 경제적인 이익추구를 목적으로 스패머들에게 감염된 시스템의 정보를 알려주거나 위장된 은행계정 입력을 요구하는 메일을 작성하여 유포하고 있다. 따라서 앞으로도 자신의 이익을 추구하기 위한 악성코드 및 애드웨어의 제작동기가 많아질 것이고 이는 곧 더욱 많은 양의 악성코드 및 복잡한 악성코드의 출현을 예고하고 있다.

악성코드 제작자와 제작동기



(8) 애드웨어의 심각성 증가

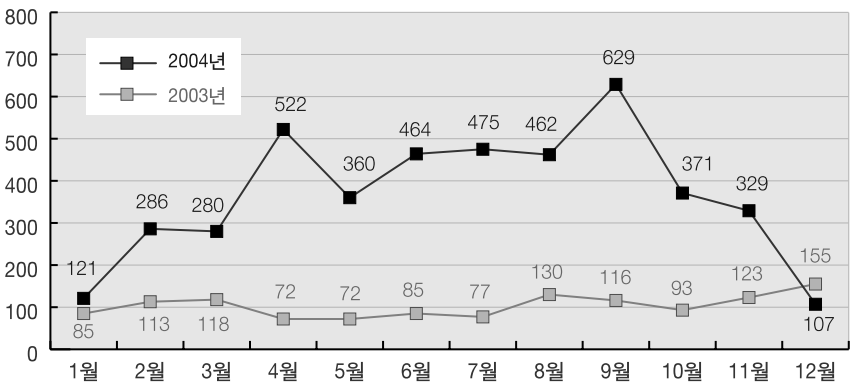
애드웨어는 원래 광고목적으로 만들어진 프로그램들을 말한다. 그러나 간혹 프로그램의 버그로 인하여 웹 브라우저를 사용하지 못하게 하거나 시스템의 중요한 파일을 삭제하는 등 시스템 운영에 중대한 손실을 가져와 원래 목적과는 다르게 보여지는 경우가 있다.

실제로 사용자들은 불쑥불쑥 튀어 나오는 팝업창이나 웹 브라우저의 홈페이지 고정 등의 문제가 악성코드의 피해보다 더 현실감 있게 다가올 것이다. 이러한 증상은 대부분 눈에 보이므로 악성코드와 사뭇 구분이 되기 때문이다. 현재 안철수연구소 뿐만 아니라 다른 백신업체들도 애드웨어 중 그 성질이 유해하다고 판단되는 것은 유해가능 프로그램으로 별도로 분류해 두고 있으며 애드웨어 뿐만 아니라 원격의 파일을 실행시키거나 시스템에서 쓸모없는 리소스를 차지하는 프로그램들도 모두 유해 가능한 프로그램으로 보는 경향이 매우 강하다. 그래서 이러한 프로그램들을 엔진에 직접 포함하는 경우가 많다.

또한 애드웨어로써 팝업이나 홈페이지 고정 등과 같은 문제를 일으키는 파일 또는 레지스트리 값, ActiveX 등은 별도로 스파이웨어라 분류하여 안티 스파이웨어 제품들을 출시하여 진단/치료하고 있다.
스파이웨어에 대한 문제는 오래전부터 있었지만 제품에 대한 시장이 형성되고 사용자들도 이들이 유해하다는 인식이 팽배해져 올해 들어 그 위협과 시장이 급성장하였다. 악성코드보다 체감적으로 느끼는 스파이웨어에 대한 피해는 내년에도 더 기승을 부릴 것으로 전망된다.

2003, 2004년 신종(변형포함) 악성코드의 유형별 현황

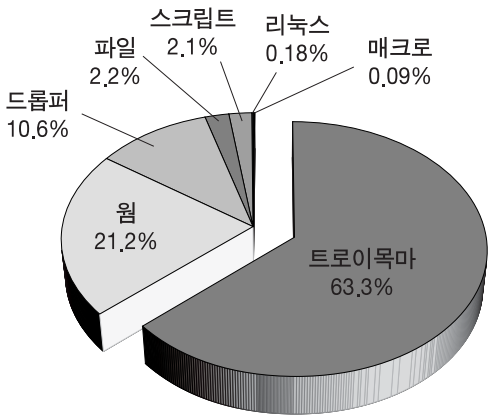
[표1], [표2] 의 악성코드 유형별 집계를 아래와 같이 나타내 보았다.



[그림3] 2003, 2004년 월 신종(변형)악성코드 발견 건수

2004년 경우 4월과 9월에 비약적으로 증가한 신종(변형포함) 악성코드의 수치를 볼 수 있는데 이는 모두 악성 IRC봇 웜 변형에 의한 것이다. 이는 2003년 수치와 비교했을 때 폭발적으로 증가한 수치이다. [그림3]에서 2004년 10월부터는 갑자기 건수가 떨어진 것을 볼 수 있는데 이것은 V3 엔진의 악성 IRC봇 진단기능이 향상된 결과이다.

다음은 2003년, 2004년 10월까지 신종(변형포함) 악성코드들은 어떠한 유형들이 있었는지 [그림4], [그림5]의 내용을 확인해보자.

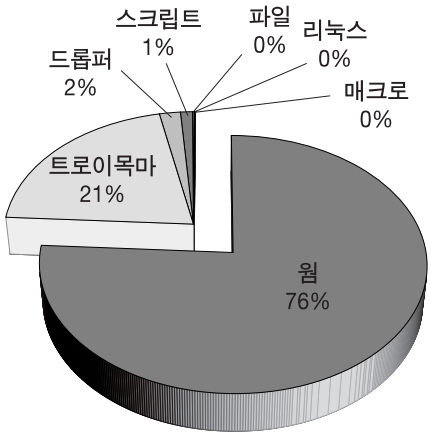


[그림4] 2003년 신종(변형포함) 악성코드 유형

2003년은 트로이목마가 강세인 것을 알 수 있다. 이 트로이목마를 다시 분류한다면 보통 다음과 같다.

- 악성 IRC봇 트로이목마
- 원격제어 트로이목마
- 기타 트로이목마 (Proxy, 다운로더)

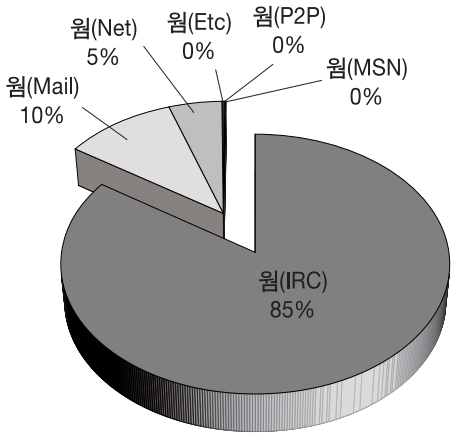
이중 가장 많은 문의를 가졌던 것은 악성 IRC봇 트로이목마이다. 트로이목마 형태인 IRC봇은 2004년에 들어서면서 자체확산력을 가진 웜으로 발전하였다.



[그림5] 2004년 신종(변형포함) 악성코드 유형

[그림4], [그림5]를 보듯이 2003년은 웜보다는 트로이목마류－대부분이 악성 IRC봇 트로이목마－비중이 높았던 반면, 2004년은 트로이목마보다는 웜－대부분 악성 IRC봇 웜－이 증가하였다.

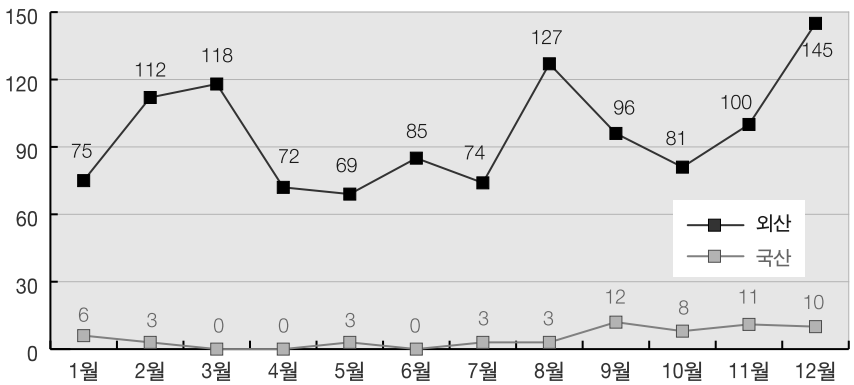
증가된 웜들도 다음과 같은 유형으로 분류하여 분포를 확인해 보았다.



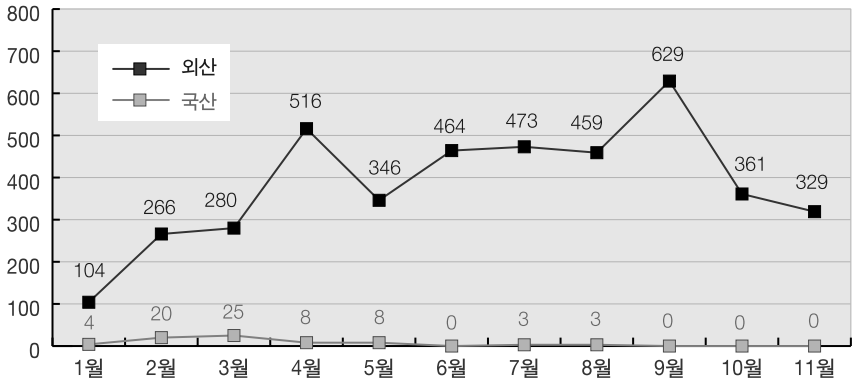
[그림6] 2004년 웜 유형별 현황

악성 IRC봇 웜이 전체의 85%를 차지하고 있는 것을 알 수 있다. 취약점만 이용해서 전파되는 웜들도 5%를 차지하고 있었다.
또한 [그림5]에 기입되지는 않았지만 유해 프로그램으로 분류된 애드웨어 및 응용 프로그램들도 분류의 한 기준으로 자리를 잡았다.

올해 발견된 국산/외산 제작 악성코드의 비율은 역시 외산 제작 악성코드가 월등히 많다. 외산 제작 악성코드 경우 전년 대비 4배 정도가 증가하였다.



[그림7] 2003년 신종 악성코드 국산/외산 현황



[그림8] 2004년 상반기 신종 악성코드 국산/외산 현황

대부분 발견되고 있는 악성코드의 유형이 외산인 것을 감안한다면 국산 악성코드들의 발견건수는 매우 적다고 하겠다. 2004년 국산 악성코드는 대부분이 유해 가능한 애드웨어이다. 또한 스팸메일러류는 현저히 줄었으며 대신 ActiveX와 BHO(Browser Helper Object)를 사용하여 시스템에 설치되고 동작하는 스파이웨어들 때문에 사용자들은 더욱 피해를 입었다.

미래를 예측하기는 어렵지만 최근 악성코드 동향을 살펴보면 어느정도 가늠할 수 있다. 앞서 소개된 유해 가능한 프로그램이 마치 악성코드처럼 자신을 실행하고 숨기는 현상도 보이고 있어 앞으로 유해 가능한 프로그램에 대한 심각성은 내년에도 크게 대두 될 것으로 보여진다. 이러한 유해 가능 프로그램에 대한 대책으로써 윈도우 XP SP2에서는 웹 브라우저에서 ActiveX를 제어하는 등의 신뢰할 수 있는 브라우징 기술을 선보였다. 게이트웨이(Gateway)에서 악성코드와 유해 트래픽을 차단하는 IPS/IDS의 하드웨어 보안장비도 대거 선보였다. 이러한 장비들이 등장한 이유는 악성코드의 급격한 확산속도와 Zero-Day 익스플로잇을 예방하기 위해서이다. 올해 첫 등장한 모바일 악성코드와 64비트 악성코드의 등장도 새로운 보안위협으로 다가왔으며 내년에 더 많은 수가 출현할 것으로 전망된다.

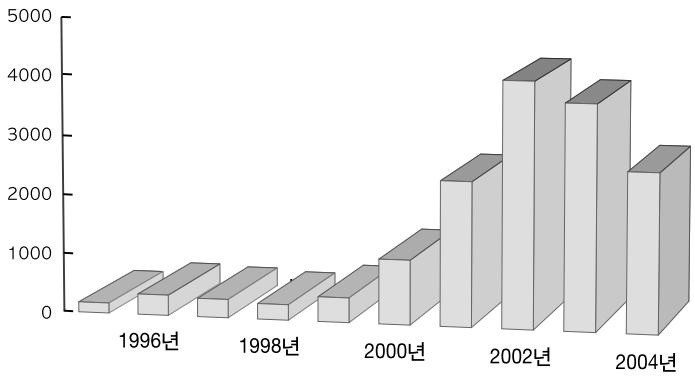
전산자원에 대한 인프라가 발전하고 증가함에 따라서 새로운 보안위협이 발생되고 이를 예방 및 대응하는 연구와 개발은 끊임없이 이루어졌다. 변화가 너무도 빠른 현 시대에 앞으로 어떤 새로운 보안위협이 우리를 위협할지 예측하기 어렵다. 하지만 우리는 어떤 보안위협들이 발생할 수 있는지 정도는 나열할 수 있고 그 중 가장 문제시 되는 것들에 대한 예방 및 대응연구를 통해서 앞으로 보다 안전한 컴퓨팅 환경을 맞이할 수 있을 것으로 전망된다.

III. 2004년 취약점 동향

작성자 : 안철수연구소 정관진 주임연구원(intexp@ahnlab.com)

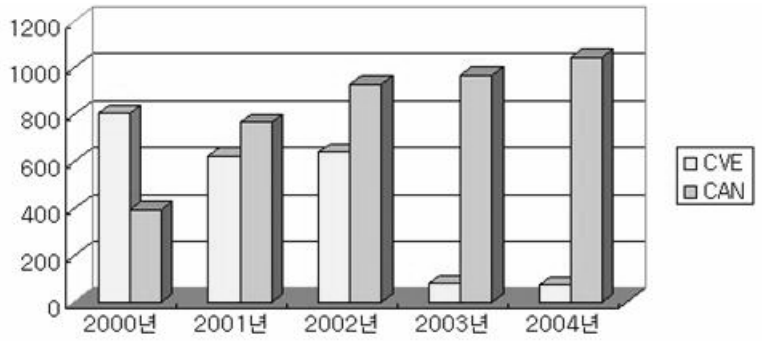
작년 2003년 1월 25일은 우리에게 보안의 중요성을 다시 한번 느끼게 해 주었던 한 해였다. 2004년 지금 현재 우리의 보안수준은 어느 정도 와 있는 것일까? 무엇보다도 국가차원에서의 인식이 달라져 공공분야에는 국가사이버안전센터(NCSC: National Cyber Security Center), 민간분야에는 인터넷침해사고대응지원센터 등 다각적인 면에서 '보안의 중요성' 에 대한 인식이 달라지고 있다. 하지만 점점 더 증가하고 있는 시큐리티 위협과 IT(Information Technology) 기반 인프라 환경의 확대는 더욱 큰 위협을 가져다 줄 가능성을 높여주고 있다.

우선, 올해 2004년 또한 예외 없이 새서 웜(Win32/Sasser.worm)이 출현해 전 세계적으로 큰 피해를 안겨다 주었고 웹 환경의 증가로 이를 이용한 취약점과 공격이 증가하며 방화벽과 같은 보안체제를 우회하여 접근할 수 있는 다양한 방법들이 나타나고 있다는 점이다. 주목할 만한 점은, 올해도 2003년과 마찬가지로 악성코드들이 취약점을 이용하는 형태가 크게 증가하였다는 것이다. 이것은 과거에 취약점이 해커들에 의해서 주로 이용되었던 것과는 달리 악성코드의 확산과 지능화된 복합적인 위협에 취약점이 큰 역할을 담당하고 있다는 것이다. 바로 과거의 악성코드들이 수동적인 행동을 필요로 하던 것에 비해 악성코드 스스로가 능동적으로 전파하기 위한 방법으로 취약점과 같은 시큐리티의 여러 보안적인 면을 이용하고 있다.



[그림1] CERT에 보고된 취약점 현황 (2004년은 3/4분기 까지만 취합)

[그림1]은 CERT에 보고된 취약점 현황으로 1995년부터 시작하여 2000년부터는 증가추세가 뚜렷이 나타나고 있다. 앞으로도 보고되는 취약점은 지속적으로 증가 또는 2002년~2004년에 보고된 수준 정도를 유지하게 될 것으로 생각된다. 다만, 전체적으로는 큰 폭으로 누적되게 되어 위협에 노출되는 범위 수준은 높아질 것으로 보인다. 이는 2000년에 발견된 취약점이 2004년 현 시점까지 계속 위협의 대상이 될 수 있다는 것이다. 즉, 취약점에 대한 지속적인 해결이 이뤄져야 하는데 그렇게 되지 못하면서 관리적인 이슈가 크게 부상할 것이다.

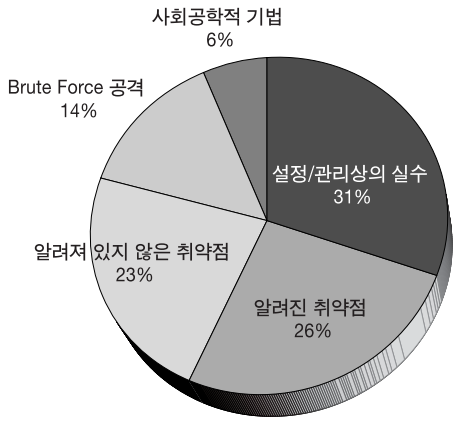


[그림2] CVE 와 CVE Candidates 현황(2004년11월 말 기준)

[그림2]는 CVE(Common Vulnerabilities and Exposures)에 2004년 11월까지 등록된 정보를 기준으로 작성된 도표이다. 2003, 2004년도에는 CVE 비율이 높지 않지만 대기중인 CAN을 보면 그 수치가 2000년부터 계속 증가되고 있는 것을 볼 수 있다.[1] 전체적으로 취약점은 큰 폭으로 증가하지 않았으나, 취약점이 누적되는 수와 위협의 수준을 고려하면 전체적인 위협은 증가하고 있다 할 수 있다.

취약점과 악성코드의 활용 증대

[그림3]은 어느 보안관련 사이트에서 공격에 주로 이용되는 방법을 조사한 것으로, 취약점을 이용한 것이 50% 가까이 차지하고 있다. 그만큼 공격에 취약점을 이용하는 비중이 높은 것으로



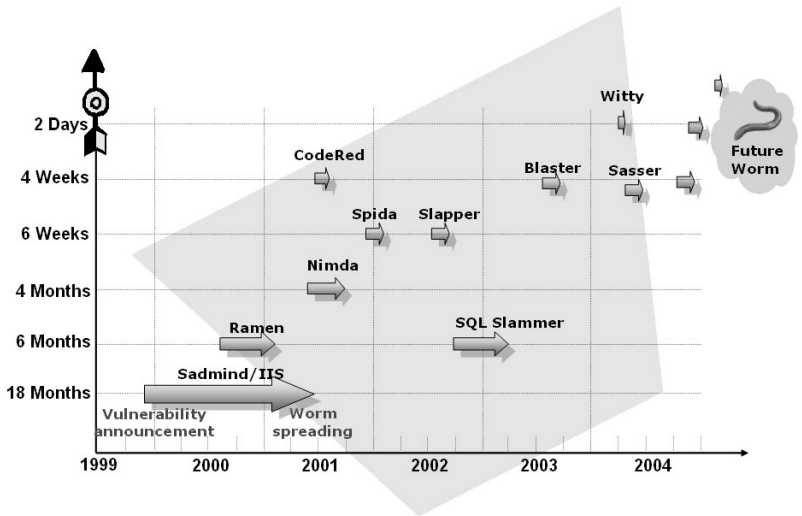
[그림3] 공격에 이용되는 방법

1) CAN은 CVE로 할당되기 이전에 대기중인 것을 말한다.

추정해 볼 수 있으며, 알려져 있는 취약점뿐만 아니라 언더그라운드에서만 알려져 있고 아직 공개되지 않은 취약점을 이용하는 형태도 그 비중이 높은 것으로 나타났다. 취약점이 공개되어 있지 않은 경우, 관리자 입장에서는 어떠한 위협에 노출되어 있는지 알 수 없으므로 위험성이 크게 증가하게 된다.

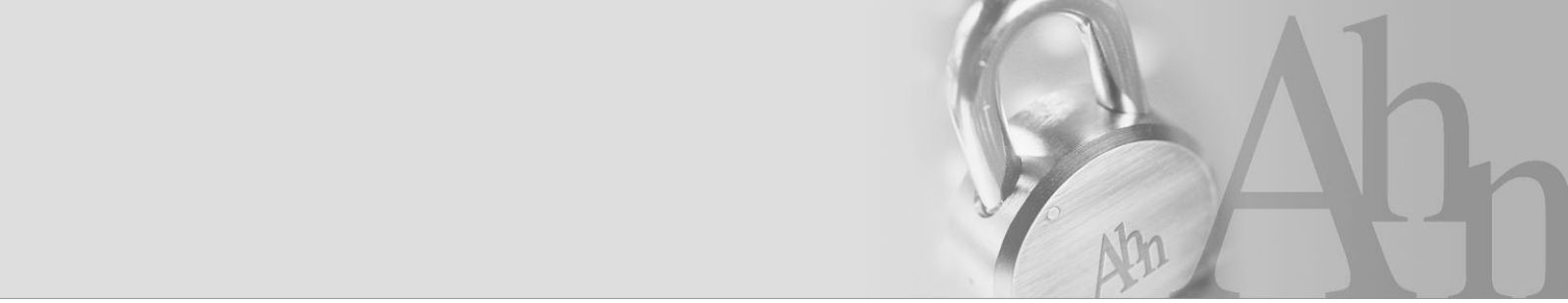
작년과 같이 올해도 취약점을 이용하여 능동적으로 공격하는 악성코드가 크게 증가하였는데, 이것은 취약점을 이용한 전파방법이 큰 효과가 있기 때문이다. 이러한 관계로 보았을 때 악성코드는 취약점을 이용하는 형태가 계속적으로 진행될 것이고, 취약점이 나오자 마자 이를 이용하는 'Zero-Day' 웜의 비중이 높아질 것으로 추정된다.

[그림4]는 처음 취약점이 발표된 시간과 이를 이용하여 웜이 출현하기까지의 시간을 나타낸 것으로 그 간격이 점점 좁아지고 있음을 알 수 있다. 새드마인드(Sadmind) 웜은 취약점이 나온 후 18개월이 걸렸고, 슬래머(Slammer, SQL_Overflow) 웜은 6개월, 블래스터 웜은 26일, 그리고 보안제품의 취약점을 이용한 위티 웜(Win32/Witty.worm)이 나오기까지는 2일이 걸렸다. 점점 취약점을 이용하여 웜이 나타나는 시간적 추이는 좁아지고 있어 향후 이 행보는 더욱 빨라지고 형태가 많아질 것으로 판단된다.



[그림4] 취약점을 이용한 웜의 출현시기

또한, SANS(http://www.sans.org)에서 발표한 윈도우 취약점 TOP 10에 해당하는 내용들이 악성코드에서 모두 이용했던 취약점일 만큼 향후 악성코드와 취약점의 상생관계는 계속될 것이다.



■ 윈도우 취약점 TOP 10(출처: SANS)

- 웹 서버 및 관련 서비스
- 워크스테이션(Workstation) 서비스
- 윈도우 원격 접속 서비스 (RPC)
- 마이크로소프트 SQL 서버
- 간단한 패스워드와 같은 윈도우 인증관련 취약점
- 웹 브라우저
- 파일 공유 프로그램
- LSASS 취약점
- 메일 클라이언트
- 인터넷 메시징

다양한 보안 정책에 맞서는 외부의 위협

취약점을 이용한 악성코드가 증가되며 이에 대한 보안 정책 및 소프트웨어 또한 과거와 달리 변화하고 있다. 이러한 사항을 잘 반영한 것이 윈도우 XP SP2로, 외부의 위협으로부터 보호하기 위한 기능을 많이 반영하였다는 점이다. 과거의 운영체제는 독립형 구조로 디자인되어 외부와의 연결없이 개인적으로 사용되는 경우가 많았던 반면, IT 인프라의 발전에 힘입어 컴퓨터가 네트워크에 연결되는 비중을 높였고 이에 따라 자연스럽게 외부에 노출되는 기회도 높였다. 거기다 이메일, 웹 브라우저의 사용, P2P 등 과거에 비해 환경 그 자체가 크게 변화하였기 때문에 운영체제 또한 이러한 변화의 흐름에 따라 보안을 한단계 업그레이드 시켜주었다 할 수 있다. 방화벽, 메모리 보호기술, 브라우저의 안전한 사용 등 여러 기능들을 반영하여 웜과 같은 악성코드가 활동할 수 있는 영역의 범위를 축소시켜줄 것으로 생각된다.

하지만 베이글 웜(Win32/Bagle.worm) 변형 중 일부와 백쯔 웜(Win32/Bagz.worm), 자피 웜(Win32/Zafi.worm.15993)은 이러한 기술을 무력화 또는 우회하기 위한 방법을 사용하였다. 또한 해외 일부 포럼에서는 윈도우 XP SP2 방화벽의 기능해제는 물론 버퍼오버플로우(Buffer Overflow)를 방지하는 DEP(Data Execution Prevention), 그리고 TCP/IP의 동시 연결횟수제한을 해제하는 프로그램들이 소개되었다. 이렇게 다양한 보안 정책에 맞서는 외부의 위협들이 있기 때문에 이에 대한 방법들은 계속적으로 연구되며 앞으로 큰 이슈가 될 것으로 보인다.

소스코드의 유출과 위험

올해는 특히나 소스코드의 유출 사고가 큰 이슈가 되었다. 2월에 윈도우 2000 운영체제의 소스코드 일부가 유출되었고, 5월에는 시스코(Cisco)사의 네트워크 장비 운영체제인 IOS(Internet Operating System)버전 12.3 소스코드가 유출되었다고 러시아 보안 사이트(SecurityLab.ru)에 보고되었다. IOS 소스는 전체 800M중 2.5M가 공개되었고 코드 유출로 인한 위협은 현재까지 윈도우 소스코드의 유출로 인한 IE의 관련 취약점 이외에 크게 보고된 적이 없다. 다만 앞으로 악용될 가능성이 존재하기 때문에 예의주시할 필요성이 있다. 또한, 악성코드 중에 하나인 마이둠 웜과 베이글 웜은 웜의 소스코드를 포함하여 전파하기도 하여 또 다른 악성코드 제작에 이용되거나 많은 변형을 가져올 가능성을 안겨주었다.

다사다난한 2004년 한 해

2004년은 소스코드의 유출, 취약점 이용의 증가 등 '보안'적으로 다사다난한 한 해였다고 할 수 있다. 취약점이 발표된 후 이를 이용하여 웜이 나오기까지의 시간은 짧아지고 있으며 악성코드는 더욱 지능적 복합적인 형태를 갖춰가고 있다. 앞으로도 취약점은 많은 사용자층을 확보하고 있는 윈도우 시스템을 중심으로 취약점을 이용하는 형태가 더욱 전개될이며, 이를 이용한 공격코드는 앞으로도 계속 큰 이슈로 남게 될 것이다.

Ⅳ. 2004년 악성코드 사건사고

작성자 : 안철수연구소 차민석 주임연구원(jackycha@ahnlab.com)
김소헌 주임연구원(sohkim@ahnlab.com)
장영준 주임연구원(zhang95@ahnlab.com)

한국의 악성코드 사건사고

2004년 한해를 정리하자면 베이글 웜, 마이둠 웜, 넷스카이 웜 삼총사의 맹활약(?)과 악성 IRC봇류의 물량 공세로 정리할 수 있다. 보안 프로그램을 회피하는 여러 기술이 사용되었으며 악성코드 제작 동기가 자신의 지식을 뽐내기 위한 장난 수준에서 금전적 이익을 목적으로 하는 경우가 점점 많아지고 있다. 악성코드는 아니지만 스파이웨어와 피싱에 대한 관심도 커졌다. 또한 2004년은 미래형 악성코드의 첫 발을 내딛었다고 할 수 있다. 64비트 바이러스, 휴대폰, PDA와 같은 모바일 악성코드가 등장했다. 이중 심비안 OS에서 실행되는 카비르 웜은 세계 몇 지역에서 실제 감염 보고되어 휴대폰 악성코드로 인한 피해가 현실화 되었다. 하지만, 국내에는 심비안 OS를 사용하는 휴대폰이 거의 없으므로 피해가 발생할 가능성은 낮다.

이 장에서는 2004년 한국에서 발생한 악성코드 중 기술이나 피해 측면에서 관심을 끌었던 악성코드를 정리해 보았다.

■ 베이글 웜, 마이둠 웜, 넷스카이 웜 삼총사의 활약

2004년은 베이글 웜, 마이둠 웜, 넷스카이 웜 삼총사가 많은 피해를 입혔다. 첫 시작은 베이글 웜(Win32/Bagle.worm.15872)으로 2004년 1월 19일에 등장했다. 이후 1월 27일 아침부터 급속히 전파된 마이둠 웜(Win32/MyDoom.worm.22528)은 기존의 소빅.C 웜(Win32/Sobig.worm.C)이 가지고 있던 가장 널리 확산된 웜의 기록을 깼다. 넷스카이 웜(Win32/Netsky.worm.21504)은 2월 16일에 최초 발견되었으며, 이후 베이글, 마이둠, 넷스카이 삼총사는 서로 경쟁하듯 변형이 출몰하였고 많은 피해를 입혔다. 또한 베이글, 마이둠, 넷스카이에는 상대방의 웜에 대해 비방하는 내용이나 상대의 웜을 치료하는 기능을 포함해 제작자들끼리 서로 다투며 경쟁하는 모습도 연출되었다. 특히 베이글 제작자는 다른 파일을 감염시킬 수 있는 바이러스 버전을 만들기도 하고 크기가 아주 작은 변형도 만드는 등 여러가지 시도를 했다.

■ 스파이웨어의 피해

2003년부터 조금씩 문제를 일으킨 스파이웨어(애드웨어)는 2004년 들어 급속히 증가하게 되었고, 이로 인해 국내외에 스파이웨어 전문 퇴치 프로그램이 속속 등장하게 되었다. 2004년에도 애드웨어의 버그로 윈도우가 제대로 실행되지 않게 하는 온반(Win-Trojan/Onban.24576)

사건이 발생했다. 특히 이 스파이웨어는 베이글.Q 웜(Win32/Bagle.worm.Q)이 퍼지고 나서 바로 발견되어 베이글.Q의 치료가 잘못된 것이 아니냐는 의혹도 받았다. 애드웨어의 버그로 시스템의 레지스트리 키를 임의로 지워버려 윈도우 95/98 시스템에서 오동작이 발생했었다.

■ 악성 IRC봇의 대량 발견[1)]

2003년부터 증가하기 시작한 악성 IRC봇류는 2004년 초부터 수 많은 변형이 발견되었다. 2004년 12월 현재까지 약 7,000 개 이상의 악성 IRC봇류가 존재하는 것으로 추정된다. 하지만 이 수치도 분류 기준 등에 따라 달라질 수 있다. 악성 IRC봇은 에스디봇(SdBot), 아고봇(AgoBot), 알봇(Rbot), 포봇(Forbot) 등의 종류가 있다. 이들은 모두 SdBot 소스를 바탕으로 계속 개량된 것으로 보인다. 특히 악성 IRC봇은 여러 명의 제작자들이 협력을 통해 계속 개량되면서 사용자나 백신으로부터 자신을 속이는 은폐기법(Stealth Technique), 취약점을 이용한 전파, 다형성 기법(Polymorphic)을 사용하는 형태도 있다. 악성 IRC봇은 한번에 대규모로 감염시키는 경우는 드물지만 회사나 학교 등에서 확산되어 일부 네트워크를 마비시키는 등의 개별적인 문제를 일으키고 있다.

■ 블래스터 웜의 환생? 새서 웜!

한국 시간으로 2004년 5월 1일 오후부터 시스템에서 에러 메시지를 출력하고 시스템이 재부팅되는 현상이 증가했다. 이는 새서 웜(Win32/Sasser.worm.15872) 때문으로 2003년 8월에 발생한 블래스터 웜과 유사한 증상이었다. 새서 웜은 광범위하게 퍼졌으며 웜 제작자는 넷스카이 웜을 제작한 동일인으로 밝혀졌고 독일에서 체포되었다.[2)]

■ 돈을 목적으로 제작된 악성코드들

2004년의 악성코드 경향 중 하나가 금전적 이익을 위해 악성코드를 제작하는 비중이 커진 점이다. 기존의 악성코드 제작자들은 자신의 능력을 시험하거나 자신의 악성코드가 퍼져 사람들이 피해를 입는 것에 만족을 느끼는 유쾌범이었지만 2004년에 등장하는 상당수 악성코드는 돈이

---

1) AhnLab, 악성 IRC봇 관련 참고 자료
- 악성 IRC봇의 의미와 동작원리,
  http://info.ahnlab.com/securityinfo/info_view.jsp?seq=5318
- AgoBot 웜 분석 보고서,
  http://info.ahnlab.com/securityinfo/info_view.jsp?seq=5661&category=02

2) ZDNet, 새서 웜 제작자 체포
http://www.zdnet.co.kr/news/internet/0,39024414,10068647,00.htm

목적인 경우가 증가하고 배후에 스팸 업자나 마피아가 연루되었다는 의혹도 있다. 코르고 웜(Win32/Korgo.worm.10752)은 러시아에서 제작되었으며 특정 은행 고객의 개인 정보를 빼내기 위해 제작된 것으로 알려져 있다. 이외 베이글 웜, 마이둠 웜 역시 스팸 메일을 발송하는 목적으로 제작된 것으로 추정되고 있다. 악성 IRC봇 중 최근에 발견된 변형은 애드웨어를 퍼뜨리거나 스팸 메일 발송에 이용되는 형태도 있다.

백신업계에서 악성코드로 분류하고 있지 않지만 애드웨어도 광고 수익을 위해 제작되며 일부 애드웨어는 사용자를 무척 불편하게 한다. 특히 애드웨어를 퍼뜨리는 악성코드와 스팸 메일을 발송하는 악성코드의 등장은 애드웨어 제작 업체들과 악성코드 제작자들이 유착되어 있음을 생각해 볼 수 있다. 대표적인 애드웨어 설치 트로이목마는 로우존드롭퍼(Dropper/LowZones.51048)로 웹 서핑 중 취약점을 이용해 시스템에 설치되는 것으로 추정된다.

■ 국가기관 해킹 시도 사건

2004년 6월 누군가 국가기관의 컴퓨터로 해킹 프로그램을 보낸 것이 확인되었다. 불확실한 정보와 언론의 과장 보도 등의 문제가 있었지만 핍뷰어(Win-Trojan/PeepViewer.81920)를 이용해 누군가 해킹을 시도한 것이다.[3] 이 사건은 대대적으로 보도되었지만 중국 지역으로 추정될 뿐 제작자의 신원이나 의도는 밝혀지지 않았다.

■ 취약점을 이용한 악성코드들

2004년에도 취약점을 이용한 악성코드는 꾸준히 등장했다. 넷스나(X97M/NetSna)는 엑셀의 취약점을 이용해 문서를 열면 사용자에게 매크로 경고를 띄우지 않고 바로 실행되게 했다. 다행히 특정 버전의 엑셀에서만 실행된다. 11월 초에 발견된 보프라 웜(Win32/Bofra.worm.20751)은 보안 패치가 나오기 전에 취약점을 이용한 웜이다. 이에 마이크로소프트사는 12월 2일 보안 패치를 발표했다. 이는 마이크로소프트사가 매달 둘째주 수요일에 보안 패치를 배포하는 원칙을 어길 정도로 큰 피해가 우려되었었다.

---

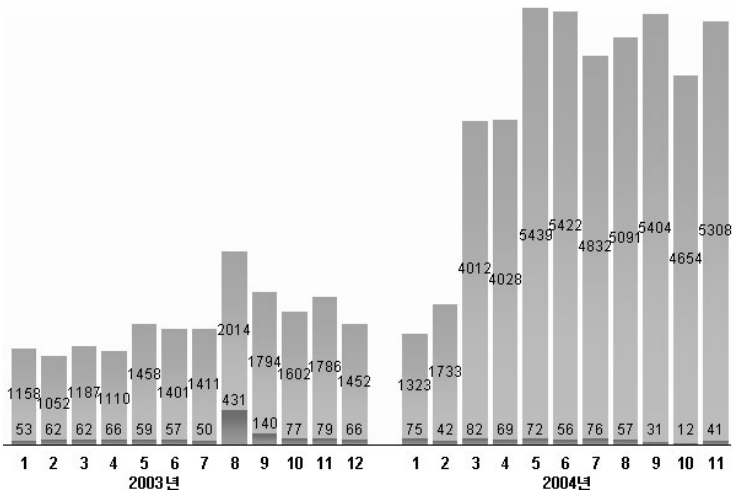
3) iNews24,
- 사이버 공안 정국을 우려한다
  http://www.inews24.com/php/news_view.php?g_serial=119649&g_menu=021400
- '변종 피프' 바이러스 감염 피해 컸다. 국정원, 애초 발표보다 2배 이상 감염
  http://www.inews24.com/php/news_view.php?g_serial=119455&g_menu=020200
- AgoBot 웜 분석 보고서,
  http://info.ahnlab.com/securityinfo/info_view.jsp?seq=5661&category=02

일본의 악성코드 사건사고

2004년 일본의 악성코드 동향과 관련하여 가장 이슈가 되었던 악성코드는 넷스카이 웜이다. 넷스카이 웜은 올해 2월 말경 최초 발견된 이후 여러 변형들이 추가로 발견되었으며 일본 뿐 아니라 전 세계적으로도 가장 많은 피해를 준 악성코드이다.

■ 악성코드의 피해 분석

[그림1]은 2003년과 2004년 일본의 IPA(www.ipa.go.jp)에 접수된 악성코드 관련 피해에 대한 합계를 나타낸 것으로, 상단 막대의 수치는 전체 신고 건수를, 하단 막대의 수치는 실제로 악성코드에 감염된 신고 건수에 대한 통계를 나타낸다. [그림1]의 내용 중 올 3월 들어 갑자기 큰 폭으로 감염 피해 접수가 늘어난 것을 볼 수 있는데 이는 넷스카이 웜이 3월에 들어서면서 본격적인 활동을 시작했기 때문이다.

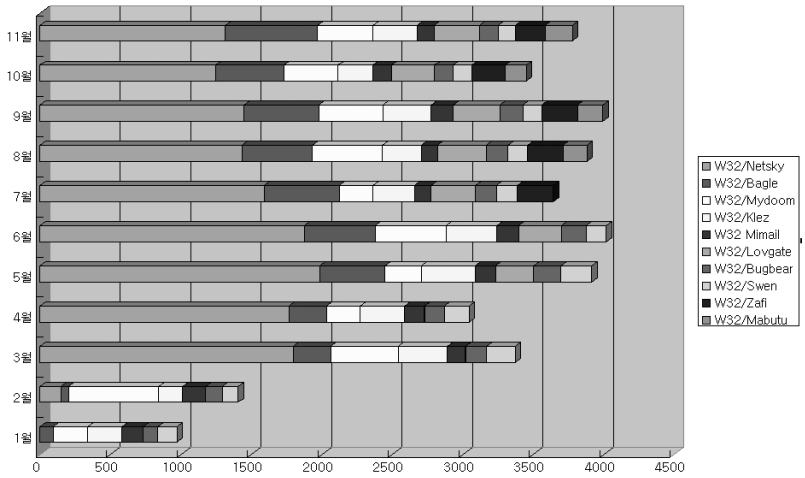


[그림1] 2004년 발생한 악성코드 감염 통계

또한 5월부터 피해신고가 이전 달보다 급격하게 증가했는데 이는 새로운 넷스카이 웜 변형과 러브게이트 웜(Win32/LovGate.worm) 변형이 전파되기 시작하였기 때문이다.

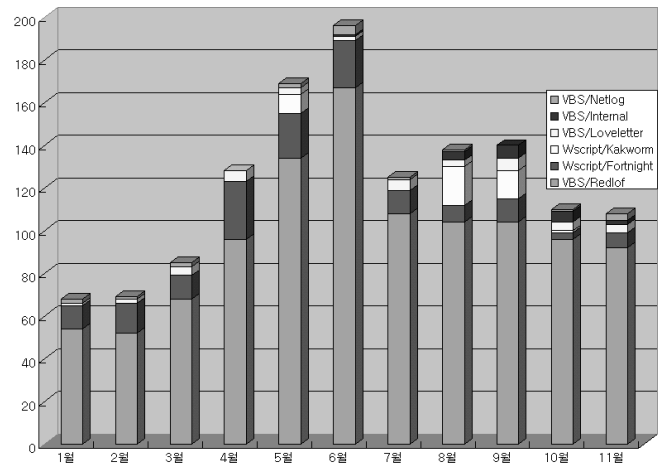
[그림2]는 악성코드 종류별 감염신고 통계를 표로 나타낸 것이다. 4월까지는 러브게이트 웜 에 대한 감염 피해 신고가 존재하지 않았으나 5월에 들어서면서 급격하게 피해 내역이 증가하는 것을 볼 수 있다.
한국의 경우에도 러브게이트 웜은 여러 변형들을 가지고 있고 확산되는 웜 중의 하나이다. 그러나 통계에 나온 것과 같이 많이 전파되는 것으로 보이지는 않으나 일본의 경우는 현재까지도 감염 피해에 대한 통계 건수가 줄어들지 않고 있다.

마지막으로 작년과 비교하여 전체 감염자들에 대한 실제 감염자의 비율이 훨씬 줄어든 것을 알 수 있다. 2003년의 경우 실제 감염 피해 문의는 전체의 5% 정도였으나 2004년 그래프에서는 2% 수준으로 나온 것을 볼 수 있다. 이는 더 이상 일반 사용자들이 내부에 포함된 악성코드 파일을 직접 실행해야 하는 메스메일러에 속는 비율이 많이 줄어들 수 있게 되었기 때문으로 생각된다.



[그림2] 이메일 웜 감염 통계

[그림3]은 스크립트 바이러스의 피해 통계를 나타낸 것이다. 레드롤프(VBS/Redlof)의 감염 피해가 여전히 줄어들지 않고 있는 것을 알 수 있다. 이외에도 포트나이트(VBS/Fortnight)나 러브게이트(VBS/LovGate) 등은 발견된 후 시간이 많이 지난 지금에도 사라지지 않고 감염 피해가 발생하는 것을 볼 수 있다.



[그림3] 스크립트 바이러스 감염 통계

중국의 악성코드 사건사고

2004년의 악성코드 동향은 연초부터 이어진 악성코드들의 급격한 확산으로 시작하여 7, 8월 여름에 이르러서는 애드웨어의 급격한 증가와 함께 폭발적인 증가치를 보이게 되었다. 그리고 악성코드의 다양한 공격 및 확산 방법들로 인해 세계 각국의 백신업체들은 다양한 대응 방안을 만들고 있는 실정이다. 이러한 변화 속에서 2004년 중국 현지의 악성코드 동향 역시 이러한 세계적인 변화에서 예외는 아니었던 것으로 보여진다. 한 해가 저물어가는 12월, 2004년 중국 악성코드 동향은 어떠한 변화가 있었는지 살펴보도록 하자.

■ 메일로 확산되는 웜들의 대거 등장

2004년 1월 말, 급속한 등장과 함께 많은 피해를 입혔던 마이둠 웜을 시작으로 메일로 전파되는 매스메일러 웜들이 대거 등장하였다. 마이둠을 비롯하여 베이글 웜, 넷스카이 웜 등으로 이어지면서 급격한 확산을 보였었다. 이 중에서도 넷스카이 웜과 베이글 웜은 현재까지도 변형이 지속적으로 등장하여 사용자들의 주의를 요하고 있다. 이러한 매스메일러 웜들이 예년과 비교하여 유달리 많이 등장하게 된 배경에는 해당 웜 제작자들간의 감정적인 싸움으로 인한 부분도 있는 것으로 알려져 있다. 그리고 일반 사용자들 사이에서 전자메일의 사용빈도가 그 만큼 많이 증가한 것으로도 볼 수 있다. 이러한 세계적인 상황은 중국에서도 유사하게 1월말 마이둠을 시작으로 하여 베이글, 넷스카이까지 현재까지도 소멸되지 않고 지속적인 보고가 이루어지고 있다. 이러한 매스메일러들의 중국 내 확산은 2004년 상반기까지 하나의 큰 흐름으로 이어졌으며 현재까지도 네트워크로 전파되는 웜들과 함께 중국 악성코드 동향의 큰 축을 이루고 있다.

■ 네트워크로 전파되는 웜으로 인한 피해

네트워크로 전파되는 웜들 역시 중국 현지에서 많은 보고가 있었는데 그 중에서도 많은 변형과 피해를 발생한 웜들로는 러브게이트 웜과 아알씨봇 웜, 에스디봇 웜, 아고봇 웜으로 분류되는 악성 IRC봇 웜으로 분석된다. 이러한 네트워크로 전파되는 웜들은 4월에 이르러서 조금씩 보고되기 시작하여 현재는 마이둠 웜, 베이글 웜과 함께 중국 악성코드 동향에서 하나의 커다란 축을 이루고 있다. 그러나 특이한 점은 한국은 러브게이트 웜이 일시적으로 증가하였던 것과 달리 중국은 현재까지도 꾸준히 피해가 보고 되고 있다는 것이다. 악성 IRC봇 웜은 수많은 변형과 심각한 피해 증상으로 인해 중국뿐만 아니라 전세계적으로 큰 이슈를 만들었다. 특히 해당 웜의 소스가 인터넷에 공개되면서 다양한 변형들이 기하급수적으로 늘어나게 되었으며 그 공격 형태도 윈도우 시스템의 취약점들까지 다루게 되면서 급격하게 퍼져나가게 되었다.

■ 광고를 목적으로 제작된 애드웨어의 등장

애드웨어의 제작과 확산은 2004년 악성코드 동향에서 중국뿐만 아니라 전세계적으로 많은 이슈들을 낳았다고 볼 수 있다. 중국 역시 이러한 애드웨어가 6월달부터 보고 되기 시작하여 통계상으로는 극히 작은 부분을 차지하고 있지만 매달 꾸준히 일정 수준 이상 보고 되고 있다. 애드웨어가 급격하게 확산된 점에는 애드웨어가 악성코드와는 달리 상업적인 목적으로 제작되다보니 그 피해가 심각해진 것으로 분석된다. 그러나 아직 한국이나 유럽권과 달리 애드웨어로 인한 피해가 심각한 수준에 이르지는 않은 것으로 분석된다. 이러한 원인으로는 중국에서는 아직까지 애드웨어와 같이 상업적인 용도의 프로그램 시장이 활성화되지 않은 점으로 인해 다른 국가와는 달리 애드웨어에 의한 피해가 상대적으로 적은 것으로 보여진다.

■ 다양한 형태의 악성코드 발견

중국은 전통적으로 백도어와 트로이목마가 강세를 보였었다. 2004년도 백도어와 트로이목마가 등장함으로써 이러한 흐름을 그대로 이어가고 있다는 것을 보여주고 있다. 그 중에서 가장 많은 변형이 알려진 것으로는 QQ 트로이목마와 온라인 게임의 사용자 계정과 암호를 유출하는 키로거 형태의 트로이목마이다. 이러한 다양한 트로이목마 중에서도 특히 QQ 트로이목마는 많은 확산을 보이고 있지 않지만 매월 일정 수준이상이 발견되고 있으며 피해 사례도 다양하게 알려지고 있다. QQ 트로이목마는 중국 현지에서 사용되고 있는 QQ 메신저를 이용하여 전파되는 트로이목마를 총칭하고 있다. 트로이목마라는 분류에서 알 수 있듯이 자체적인 전파기능은 없으나 QQ 메신저를 통하여 사용자로 하여금 특정 웹사이트로 접속을 유도하는 문구를 전송한다. 그리고 사용자가 해당 웹사이트를 접속하게 될 경우 트로이목마가 자동으로 다운로딩하여 설치하게 된다.

세계의 악성코드 사건사고

2004년을 정리하면 다음과 같은 키워드로 정리해 볼 수 있다.
'매스메일러 웜 삼총사의 활약', '악성 IRC봇', '미래형 악성코드 등장', '제작 동기 변화'

대량의 메일을 발송하는 매스메일러 웜인 베이글, 넷스카이, 마이둠이 2004년 한 해 가장 많은 피해를 준 악성코드들이다.

개별적인 악성코드가 전체적으로 피해를 주지 않았지만 악성 IRC봇은 특정 기업 등을 괴롭히며 엄청난 물량 공세로 사용자들을 괴롭혔다. 2004년 12월 현재 약 7,000 개 이상의 악성 IRC봇이 존재하는 것으로 예상된다. 2005년에도 악성 IRC봇은 계속 증가할 것으로 보인다. 악성

IRC봇은 웜 제작자가 감염된 시스템을 마음대로 조정할 수 있어 다른 시스템을 공격할 수 있을 뿐 아니라 스팸 메일 발송, 애드웨어 설치 등 금전적인 이익을 위해서도 이용되고 있다. 특히 악성 IRC봇은 한 두명의 제작자가 제작하는 것이 아니라 수 많은 사람들이 계속 새로운 변형을 만들고 새로운 기능을 추가하고 있다.

휴대폰, PDA 등 모바일 장비의 악성코드 출현은 계속 예상되었다. 6월에 심비안 OS 휴대폰에서 활동하는 카비르 웜이 발견되었다. 가을부터 싱가폴, 중국, 인도, 필란드 등지에서 조금씩 보고되어 휴대폰 악성코드가 실제 위협으로 다가오게 되었다. 현재까지 휴대폰은 국가별로 통일되지 않고 있어 하나의 악성코드가 전 세계를 감염시킬 가능성은 낮지만 휴대폰도 하나의 운영체계로 통일되면 하나의 악성코드가 전 세계 휴대폰을 감염시키는 날도 올지 모른다. 현재 많은 백신업체에서 휴대폰 백신을 개발 중이거나 시판 중에 있다.

전통적으로 바이러스와 같은 악성코드는 대부분 자신의 지식을 뽐내거나 자신의 바이러스가 퍼지는 것에서 희열감을 느끼기 위해 제작되었다. 하지만, 2004년에 발생한 악성코드 동향을 보면 이런 유쾌범에서 금전적 이익을 목적으로 작성되는 악성코드가 증가하게 되었다. 스팸 업자와 결탁해 자신이 만든 악성코드로 감염된 시스템에서 스팸 메일을 발송하거나 돈을 받고 경쟁사를 공격하는 경우도 있다. 이에 많은 백신 연구가들은 미래에서 악성코드 배후에 마피아와 같은 범죄 단체가 연루될지도 모른다는 우려를 하고 있다.

V. 2004년 Key Issue I – 금전적 이익을 노린 보안위협

작성자 : 안철수연구소 김소헌 주임연구원(sohkim@ahnlab.com)
최동균 연구원(cdk@ahnlab.com)
장혜윤 연구원(planet@ahnlab.com)

인터넷의 발달은 우리에게 많은 생활의 변화를 가져다 주었다. 인터넷을 통해 상품을 구매하거나 은행의 웹사이트에 접속해서 계좌를 관리하는 것은 처음 인터넷이 보급될 당시에는 전혀 예상할 수 없는 일이었겠지만 인터넷뱅킹은 은행 창구 앞에서 줄을 서야 하는 수고를 덜어주고 있다.
인터넷이 생활의 도구가 되어가기 시작하면서 이에 대한 부작용 또한 여러 형태로 발생하고 있는데 해킹이나 악성코드는 사용자에게 직접적인 피해를 입히는 부작용의 대표적인 예가 될 수 있을 것이다. 과거에는 이러한 악성코드 제작자들이나 해커들이 자기과시를 위한 것이 대부분이었고 실제로 이를 이용하여 개인적인 영리를 취하려는 시도는 일부에 지나지 않았으나 최근에는 개인이나 기업의 정보를 가로채고 이를 이용하여 금전적 이익을 얻으려는 시도가 점점 증가하고 있는 추세이다.

이 글에서는 인터넷상의 여러 보안 위협 중 금전적인 이윤 추구를 주목적으로 하는 대표적인 공격 형태인 스팸과 애드웨어, 피싱(Phishing)에 대하여 알아보도록 하겠다.

1. 스팸

스팸은 이메일을 통해 사용자가 원하지 않는 광고 메일을 대량으로 살포하는 행위를 말한다. 이메일을 통한 광고는 비용이 저렴하고 효과가 매우 크다는 점 때문에 유용하게 사용되는 마케팅 수단이지만 최근에는 발신처를 속일 수 있는 메일의 특성을 악용하여 대량의 메일을 불특정 다수에게 지속적으로 배포하는 행위가 빈번하게 발생하고 있다. 정부에서는 스팸메일 유포 방지를 위해 발송자에게 부과하는 벌금을 대폭 상향하는 등 방지를 위한 노력을 기울이고 있으나 아직까지는 현실성이 없어 보이며 발신자를 추적하는 것도 쉽지 않은 일이다.

스팸메일은 사용자가 메일을 열고 광고의 내용을 확인하도록 유도하는 것이 목적이므로 메일 자체가 보안취약점을 이용하거나 별도의 악성코드 파일을 따로 첨부하지는 않는 것이 일반적이다. 그러나 스팸을 이용하여 광고하는 대상 사이트들이 주로 성인사이트와 관련되어 있으므로 스파이웨어의 설치나 안전하지 않은 사이트에 가입함으로 인해 발생할 수 있는 개인 정보 노출 등의 위협요소는 항상 존재하고 있고 최근에는 OS의 취약점을 이용하여 파일을 다운로드 하도록 유도하는 경우도 있어서 주의가 필요하다.

A. 스팸 기법에 대한 소개

초기에 제작되어 발송된 스팸메일은 한정된 고객에 대해 회사의 이벤트 정보와 같은 특정한 정보나 제품홍보를 위한 카다로그와 같은 단순한 컨텐츠를 포함한 메일을 발송하는 것이 대부분이었으나 스팸메일로 인한 문제점들이 사회문제화되고 이를 막기 위한 스팸 차단 솔루션이 도입된 최근에는 인터넷 익스플로러의 취약점을 이용하는 등 이를 우회하려는 기법들이 등장하고 있다.

● 스팸차단 솔루션 우회기법 (E-mail masking)

이 기법은 스팸 필터에서 메일 내용에 들어있는 특정 단어를 필터링의 기준으로 삼는 것에 착안하여 특정 단어의 철자 사이에 html 태그를 넣거나 단어 사이에 다른 특수 문자를 넣어 사람이 눈으로 볼 때는 의미 전달이 가능하지만 메일에 쓰여진 데이터는 전혀 다른 것처럼 만들어서 필터링을 우회하는 방법이다.

'H<!-- annon -->e<!-- dinosaur -->K<!-- hexagon -->K<!-- tow -->o<!-- mouse -->~' 와 같이 작성되어 메일에 포함된 데이터는 아무런 의미가 없어 보이는 단어의 조합이지만 html을 지원하는 메일 뷰어를 이용하여 보았을 경우 < > 안의 내용은 주석으로 처리가 되기 때문에 뷰어에는 Hello~ 라는 단어만 볼 수 있다. 이러한 방법으로 단어를 조합하였을 경우 스팸 필터의 기준에 Hello~라는 단어가 들어있어도 위의 문자의 조합은 필터링하지 못할 것이다.

● 시스템 보안 취약점 코드를 이용한 기법 (IFRAME, ActiveX)

이 기법은 인터넷 익스플로러의 보안취약점을 악용하여 메일을 열었을 때 파일이 자동으로 실행되어 설치되도록 하거나 ActiveX를 설치하도록 유도하는 소스가 포함된 메일을 발송하는 방법이다. 인터넷 익스플로러의 취약점 패치가 되어 있지 않은 시스템에서는 애드웨어가 설치되어 시작페이지가 변경되는 등 사용자의 피해가 발생할 수 있다.

● 악성코드를 포함한 매스메일러

시스트엔트리(Win-Trojan/SystEntry)와 같은 일부 악성코드들은 사용자의 PC에 프로그램을 설치하고 정기적으로 외부에 스팸메일을 발송하는 기능을 가지고 있다. 이러한 악성코드들은 정기적으로 외부에서 메일 컨텐츠를 다운로드하여 발송할 수도 있으므로 스팸메일 컨텐츠가 변경될 때마다 최신의 광고를 발송해 주는 에이전트로서의 역할을 할 것이다.

B. 스팸으로 인한 피해

스팸메일로 인해 공통적으로 겪게 되는 가장 큰 피해는 아침에 출근 후 일정 시간을 스팸메일을 지우는 의미 없는 시간을 보내야 하는 점일 것이다. 선정적인 화면이 미성년자에게 아무런 여과 없이 노출되는 것 또한 심각한 문제이다.

[표1]은 2004년 상반기에 나라리서치에서 조사한 자료이다.

스팸메일 처리관련 비용	
스팸메일 수신	1조7494억원
스팸메일 저장	668억원
스팸메일 삭제	3조1849억원
합 계	5조9억여원

수신 메일 관련 통계	
개인 일일평균	20통
전체 일일평균	14억 973만통
전체 연간평균	5145억통
스팸 삭제시간	연간 30여시간

스팸메일 유형 통계	
성인 음란물	71.9%
쇼핑관련	12.2%
광고성메일	6.3%
경품메일	6.0%

[표1] 스팸메일 수신에 관한 자료(출처: 나라리서치)

일반 사용자의 입장에서 스팸메일은 삭제하는 번거로움 외에 겪어야 하는 피해는 없을 수 있지만 메일 서버를 관리하는 관리자의 입장에서는 이러한 메일들로 인해 낭비되는 하드디스크의 용량관리나 릴레이(Relay)서버로 악용될 위험성에 대한 대비가 필요하다. 콤터치(www.commtouch.com) 자료에 따르면 전체 스팸 메일 중 중국 서버를 경유한 비율이 73.58%로 가장 높고 그 다음으로 한국(10.91%), 미국(9.47%), 러시아(3.5%), 브라질(2.23%) 순이라고 한다. 발송량에 비해 스팸메일을 발송하는 국가의 비율이 그리 많지 않다는 것을 알 수 있는데 이는 메일 서버 관리자의 관리 중요성을 알 수 있게 해준다.

C. 스패머들은 어떻게 돈을 버는가

일반적으로 스팸메일에 설정된 웹 사이트의 링크들에는 스팸메일을 제작하여 발송한 발송자를 인식할 수 있도록 설정되어 있다. 스팸메일 내부의 html 코드를 보면 아래와 같은 형태로 링크 주소가 되어 있는 것을 볼 수 있다.

<a href= “http://www.antispam.com/test.php?pid=3333&bnum=Bxxx”>

위의 샘플로 제공된 html 코드를 간단하게 설명하면 사용자가 메일을 열고 하이퍼링크를 클릭하면 http://www.antispam.com/test.php 사이트로 이동을 하고 해당 웹서버에서는 test.php 파일 내부의 스크립트를 실행하게 된다. 그리고 해당 사이트에는 PID별 접속 횟수에 대한 기록이 남게 되고[1], 회사측에서는 이에 대한 카운트를 해서 스팸메일 제작자에게 비용을 지불하는 것이 일반적이다. 애드웨어나 스파이웨어와 같은 다른 프로그램들에서도 이러한 형태의 과금 체계가 일반적인 것으로 생각된다.
스패머들에게 비용을 지불한 고용업체가 어떤 방식으로 이를 이용한 수익을 창출하는지에 대해서는 해당 업체의 성격에 따라 차이가 많이 있으므로 따로 열거하지는 않겠다.

1) PID는 어떤 링크를 클릭해서 접속한 것인지 스팸메일 제작자를 식별할 수 있도록 해주는 기능을 할 것이다

D. 스팸의 문제점

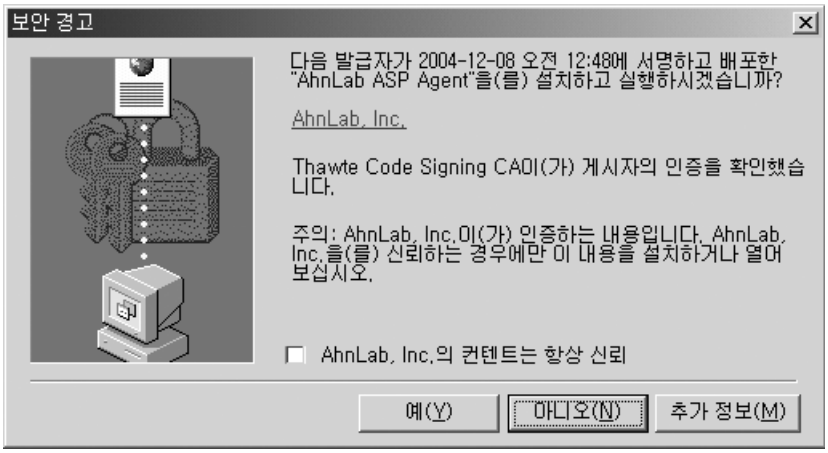
스팸메일은 인터넷상에서의 건전한 상도덕을 해치는 요인이 된다. 개인 사용자들의 입장에서 이러한 광고메일의 무분별한 발송은 삭제하는데 드는 시간적인 낭비 외에도 사용자들이 꼭 필요한 정보를 획득하는 것에 어려움을 초래하도록 할 수 있다.
또한 타인에게 피해를 입힌 대가로 영리를 취하는 부도덕성이 스팸메일이 가지고 있는 문제이다. 또한 스팸메일의 광고 내용 자체에 선정성 등 문제가 있는 경우가 많으나 메일 주소 추출기 등을 이용하여 수집한 메일 주소를 대상으로 무작위 메일을 발송하기 때문에 해당 메일을 받지 않아야 할 연령대에 노출되는 것도 우려할 만한 점이다. 국가적으로는 위에서 설명한 것처럼 스팸메일로 인해 입는 경제적 피해는 물론 스팸 릴레이 서버로 이용되는 경우 해외에 스팸메일 발송국가라는 나쁜 이미지를 가지게 되는 점 또한 심각한 문제이다.

2. 스파이웨어

스파이웨어는 유해가능 프로그램 중 사용자가 명확히 해당 프로그램의 목적을 제대로 알지 못한 상태에서 설치되어 사용자가 의도하지 않은 기능을 수행함으로써 사용자의 사생활을 침해할 수 있는 프로그램을 칭한다.
OS의 취약점을 이용하여 설치되는 일부를 제외한 대부분의 스파이웨어는 설치 전 팝업창을 보여주고 사용자에게 설치에 대한 동의를 묻는다. 그러나 배포자의 입장에서는 사전에 동의를 구한 후 설치를 한 것이라고 하더라도 사용자의 입장에서 이 프로그램이 어떤 프로그램인지 알고 설치를 하는 사람은 많지 않을 것이다. 만약 시작페이지를 고정시키거나 PC가 느려지는 증상이 발생하는 것을 사전에 알게 된다면 아무도 해당 프로그램을 설치하지 않으려고 할 것이기 때문이다.

A. 스파이웨어 기법에 대한 소개

스파이웨어는 ActiveX의 형태로 설치되는 것이 가장 일반적이다. 그러나 일부 악성 애드웨어 프로그램들은 드롭퍼(Dropper) 파일이 따로 존재해서 일단 드롭퍼를 설치한 후 다른 파일들을 인터넷에서 다운로드하여 설치하는 등 여러 가지 형태로 사용자의 시스템에 설치될 수 있다.



[그림1] ActiveX 설치 동의 여부를 묻는 보안경고창

보통 스파이웨어의 범주에는 애드웨어나 트랙웨어 등 기능별로 몇 가지 종류로 나누어볼 수 있다.

● **트랙웨어 (Trackware)**

트랙웨어는 일반적으로 우리가 알고 있는 스파이웨어에 가까운 기능을 한다. 트랙웨어는 사용자의 PC에서 발생하는 특정 이벤트에 대해서 정보를 수집하기 위해 설치되는 프로그램이다. 주요 수집대상은 방문사이트 리스트나 검색 키워드 등이고 이러한 자료들은 마케팅을 위한 기초 데이터로 사용되는 경우가 많다.

● **애드웨어 (Adware)**

말 그대로 광고를 하기 위한 목적을 가지고 있는 프로그램이다. 인터넷 익스플로러에 툴바를 설치하거나 시작페이지를 변경시키고 주기적인 팝업 광고창을 생성하는 등의 기능을 한다. 많은 웹사이트들에서 이러한 기능을 하는 프로그램들을 배포하고 있으며 이로 인한 문제가 매우 심각한 상태이다.

● **다이얼러 (Dialer)**

전화를 통해 포르노 사이트 등에 접속하도록 유도하는 프로그램이다. 일부 사이트에서는 과도한 통화료를 부과하는 등 사용자에게 피해를 끼치는 경우가 많고 애드웨어와 함께 설치되는 경우가 대부분이다.

● **다운로더 (Downloader)**

외부에서 애드웨어 등을 다운로드하여 설치하는 프로그램이다. 사용자가 애드웨어 프로그램을 삭제하는 경우 다운로더가 동작하여 삭제한 애드웨어 프로그램을 재설치한다. 보통 시작프로그

램에 파일을 등록해서 OS 부팅시 자동으로 실행되도록 하거나 빈번하게 사용되는 다른 프로그램이 실행될 때 함께 실행되도록 설정되어 있다.

이외에도 키보드 동작을 모니터링하는 키로거나 상용 원격관리 프로그램 등도 스파이웨어의 범주에 속한다.

B. 스파이웨어로 인한 피해

그렇다면 이런 스파이웨어들로 인해 입을 수 있는 피해는 어떤 것들이 있을까?

● 개인정보 유출의 가능성

스파이웨어가 설치됨으로 인해서 생길 수 있는 가장 큰 문제점은 개인 정보 유출의 가능성이 존재하고 있다는 것이다. 사용자 정보를 가져가는 트랙웨어의 경우 사용자의 정보를 어디까지 가져갈 것인지에 대한 문제가 제기된다. 트랙웨어 뿐 아니라 애드웨어와 같은 다른 프로그램들에서도 사용자들이 쉽게 알 수 없는 기능들로 인한 피해의 발생 가능성은 항상 상존하고 있다.

● 사용자에게 불편을 야기하는 행위

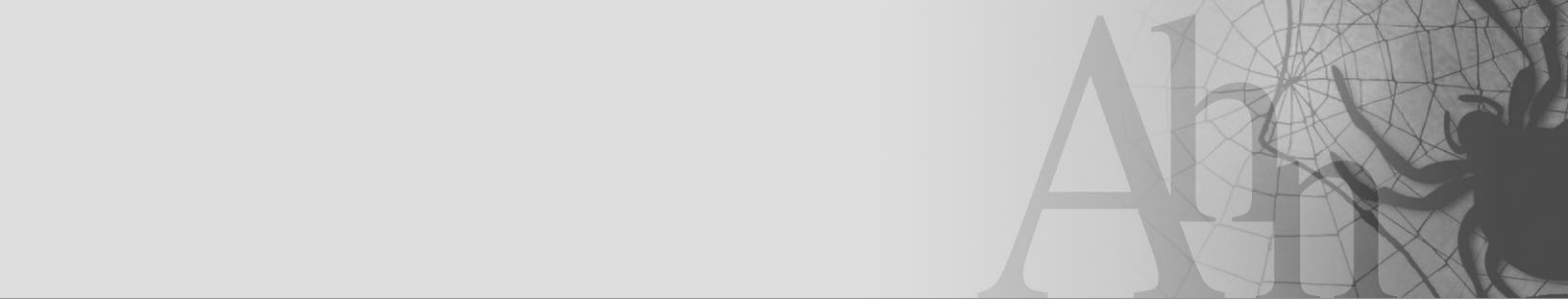
개인 사용자들이 악성 스파이웨어로 인해 겪게 되는 가장 큰 고통 중 하나는 시작페이지가 음란 사이트로 고정되어 변경할 수 없는 현상일 것이다. 가정에서 사용되는 PC들은 자녀들과 함께 사용하는 경우도 많기 때문에 이는 매우 곤란한 상황이며, 스파이웨어가 주기적으로 실행시키는 팝업광고창을 일일이 닫아야 하는 것도 사용자의 입장에서는 매우 불편한 일이다.
이러한 불편함들은 시스템에 미치는 위협은 미약하지만 사용자의 입장에서는 매우 중요한 요소들이 될 수 있다.

● 불법적인 시스템 설정의 변경

스파이웨어 프로그램이 설치되는 경우 바탕화면에 단축아이콘이 생성되거나 Hosts 파일을 변경하여 웹 브라우저에서 특정 URL을 입력했을 때 자신들의 사이트로 이동하도록 설정하는 경우가 많다. 또한 인터넷 익스플로러에 툴바를 설치하는 등 인터넷 사용환경을 마음대로 바꾸는 등의 행위가 행해지고 있다. 이러한 불법적인 파일의 설치나 설정의 변경은 전체적인 시스템의 성능이 저하되는 원인이 된다.

C. 스파이웨어 제작과 배포의 문제점

개인정보 유출 등의 피해를 입힐 수 있는 스파이웨어는 그 피해로 인한 문제 뿐 아니라, 제작 배포의 관점에서도 여러가지 문제점을 가지고 있다.



● **사용자는 설치될 프로그램에 대해 모르는 경우가 대부분**

스파이웨어의 가장 큰 문제점은 사용자가 해당 프로그램의 기능을 충분히 인지하지 못한 상태에서 설치한다는 것이다. 그리고 사용자들이 기능을 제대로 인지하지 못하는 가장 큰 원인은 보통 다른 사이트에서 팝업이나 링크의 형태로 설치프로그램을 배포하기 때문이다.
이러한 경우 사용자는 어떤 프로그램인지 전혀 인지하지 못한 상태에서 프로그램을 설치하게 되는 것이므로 이런 식으로 프로그램의 설치를 유도하는 것은 사용자를 속이는 행위로밖에 볼 수 없다.

● **무분별한 배포 형태**

초기의 스파이웨어들은 사용자가 직접 해당 사이트에 접속하거나 별도로 제공되는 프로그램을 설치하는 경우 동작을 하였지만 요즘에는 카페나 유명 사이트의 게시판만 가더라도 애드웨어 설치 프로그램들이 올라와 있는 것을 볼 수 있다. 웹서핑을 하는 도중 게시판을 열거나 내부의 그림을 클릭하는 경우 보안 경고창이 뜨는 것을 경험해 보지 못한 사람은 없을 것으로 생각된다. 스팸도 스파이웨어 설치를 유도하기 위한 중요한 수단중의 하나이다.
만약 보안 경고창에서 설치를 선택하면 애드웨어가 설치되어 곤란을 겪게 될 것이다.

● **설치된 프로그램에 대한 정보의 부재**

애드웨어의 경우 한 두개의 실행파일이나 dll파일이 윈도우 디렉토리에 설치되고 레지스트리가 추가되는 경우가 많기 때문에 사용자들은 어떤 파일이 그러한 기능을 하고 있는지 찾기가 쉽지 않다. 또한 더 이상 해당 기능을 사용하고 싶지 않은 경우라도 삭제를 할 수 있는 기능이 없는 것도 문제이다.

D. 사용자의 주의점

인터넷을 이용하는 사용자들의 가장 큰 문제점은 습관적으로 "예"를 클릭한다는 것이다.
웹 서비스를 제공하는 업체에서 ActiveX를 제공하는 것은 서비스를 더 잘 이용할 수 있도록 도움을 주기 위한 것이다. 이 말은 바꾸어 말하면 서비스를 제공받고 싶지 않은 사이트에서 제공하는 ActiveX는 설치하지 않아야 한다는 것이다.
대부분의 사이트들에서는 ActiveX를 설치하지 않은 상태에서도 대부분의 페이지들을 열람할 수 있도록 되어 있다. 그리고 ActiveX가 설치되어 있지 않으면 동작을 할 수 없는 기능을 가진 웹페이지에 접속을 하게 되면 다시 팝업창이 생성되어 설치를 요청하게 될 것이다. 만약 ActiveX가 설치되어 있지 않는 경우에 내부의 정보를 볼 수 없는 사이트라면 가지 않아도 크게 무리가 없는 사이트일 것이다. 따라서 보안 경고창이 뜨면 꼭 설치를 해야 할 가치가 있는 사이트인지 먼저 생각해 보는 습관을 가지는 것이 피해 예방을 위해서 바람직하다.

3. 피싱

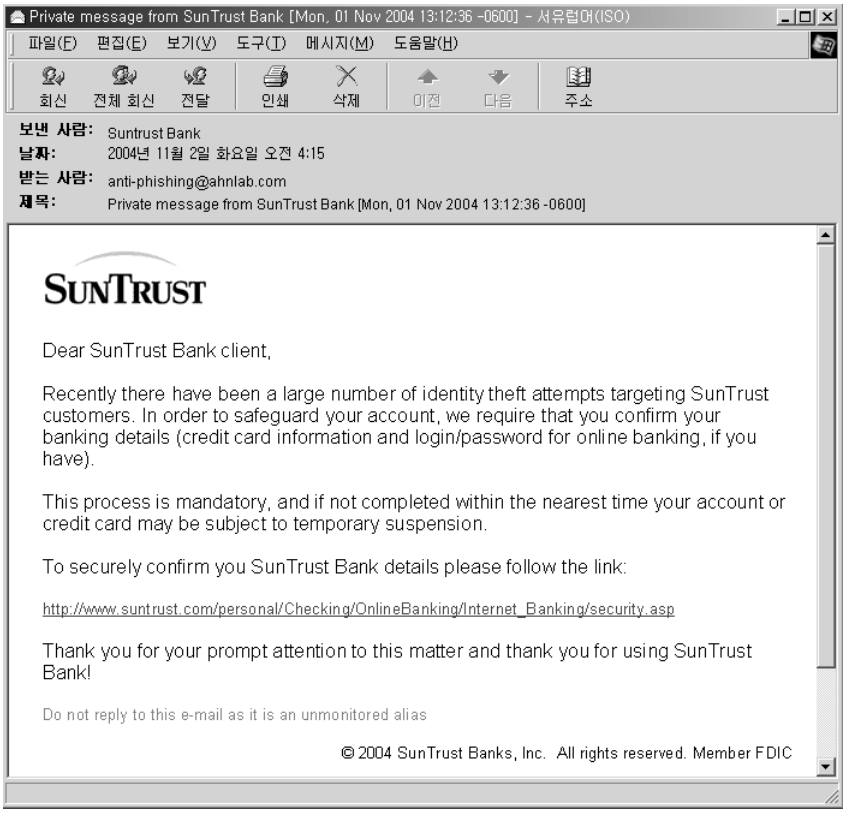
피싱은 Private Data와 Fishing의 합성어로 인터넷을 사용하는 불특정 다수에게 공신력을 가진 기관인 것처럼 가장한 메일을 보내 개인의 정보를 입력하도록 유도하는 사회공학적(Social Engineering) 사기 수법을 말한다.
피싱 제작자가 불특정 다수에게 무작위로 메일을 전송하는 것은 스팸과 비슷하지만 스팸이 광고를 목적으로 하는 것이라면 피싱은 수신자가 카드번호나 은행의 계정과 패스워드와 같은 민감한 정보를 입력하게 하고 이를 통해 개인의 정보를 취득하는 것이 목적이므로 개인의 피해는 스팸과 비교할 수 없을 정도로 심각해질 수 있다.
국내의 경우 은행의 서비스를 이용하기 위해서는 공인인증서 사용이 의무화되어 있으므로 피싱으로 인한 피해 발생 가능성이 상대적으로 낮지만 잠재적인 위협은 항상 존재하고 있다.

A. 피싱 기법에 대한 소개

초기에 만들어진 피싱 기법은 인터넷을 이용하는 대부분의 사용자가 인지하는 기존의 유명 도메인과 유사한 도메인(철자 하나를 변경하는 등)을 등록한 후 홈페이지를 동일하게 구성하여 인터넷 이용자가 실수로 이 유사한 도메인에 접속하여 개인정보를 기입하기를 기다리는 것이었다. 그러나 최근의 기법들은 사용자 개인정보 취득 목적의 위조된 홈페이지를 개설하고 개인정보 수정을 공식요청하는 변조된 메일을 불특정 대다수에게 전송하여 메일 수신자로 하여금 이 메일에 속아 링크된 주소의 위조된 홈페이지에 접속하여 개인정보를 입력하도록 유도한다.
[그림2]는 은행의 안내메일처럼 보이지만 실제로 클릭해보면 전혀 다른 웹사이트로 이동한다.

내부의 html 소스를 살펴보면 실제로 접속하는 서버의 주소를 유니코드 형식으로 변환하여 내부의 소스를 알 수 없도록 한 것을 볼 수 있는데 이러한 형태의 속임수는 피싱 사이트로 접속을 유도하는 메일들에서 흔히 사용되는 기법이며, 이외에도 사용자로 하여금 피싱 사이트임을 눈치채지 못하게 하기 위한 여러 가지 방법들이 이용되고 있다.

피싱에 이용되는 서버와 위조된 홈페이지들은 대부분 타사의 서버를 해킹하여 사용된다. [그림3]은 Anti-Phishing Working Group(APWG)에서 조사한 피싱 사이트 호스팅을 실시하는 국가별 통계이다. 한국의 경우 전체 피싱 사이트의 20% 정도가 운영되고 있는 것으로 보고된 것을 볼 수 있다. 아직 국내에서 피싱과 관련한 피해가 많지 않은 것으로 미루어보아 국내에서 이러한 사이트를 운영하는 것보다는 국외에서 취약점을 지닌 서버를 크래킹 후 불법적으로 사이트를 운영하는 것이 대부분일 것으로 생각된다.



[그림2] 피싱 메일 화면

[그림3] 국가별 피싱 사이트 호스팅 현황 (출처: APWG)

B. 피싱으로 인한 피해

일반 사용자를 속이기 위한 가짜 사이트로 주로 이용되는 대상은 대부분 은행이나 쇼핑몰 등 직접 금전적인 거래가 가능한 사이트들이 대부분이므로 피싱은 개인에게 있어서 매우 심각한 위험에 빠질 수 있는 공격이다. 피싱은 직접적인 개인정보를 노린 공격이므로 만약 공격자가 만들어 놓은 가짜 사이트에 접속해서 정보를 입력하고 그 결과 은행의 계좌가 노출되는 경우 금전적인 피해로 이어질 가능성이 매우 높기 때문에 주의가 필요하다.

C. 피싱을 이용한 피해사례

가트너에 따르면 지난 한 해 동안 피싱으로 인해 200만명의 이용 고객들이 12억 달러에 이르는 피해를 입었다고 한다. 또한 미국의 경우 피싱 메일을 받은 미국인 5700만명 중 1100만명이 메일을 열람해 이 가운데 178만명이 피싱 메일 발송자에게 금융 및 개인정보를 제공해 큰 문제가 되었다.
국내에서도 피싱을 이용하여 개인 정보를 습득, 이를 악용한 사례가 있다.
가해자들은 인터넷에 'e메일을 해킹해 드립니다' 라는 광고를 띄워 의뢰자를 모집한 뒤 유명 포털 사이트로 위장한 메일을 보낸 뒤 수신자가 메일 확인을 위해 사이트에 접속할 때 입력하는 ID와 패스워드를 빼돌려 의뢰자에게 넘겨준 혐의로 구속되었다.

지금까지 금전적 이익을 목표로 한 공격의 몇 가지 형태에 대해서 알아보았다.
빠르게 발달하는 인터넷의 다른 여러 기술들처럼 보안에 대한 이슈들 또한 변화하는 주기가 점점 짧아지므로 일반 사용자들이 최신 기법들을 이해하고 그에 적절하게 대처하는 것은 쉽지 않은 일이다. 그러나 위에서 열거한 공격 기법들은 모두 최신의 보안 지식을 사용하기 보다는 오히려 피공격자의 실수를 노리는 경향-이러한 공격 형태도 일종의 사회공학적(Social Engineering)기법으로 볼 수 있다-이 강하다는 것을 알 수 있을 것이다.
일반 사용자의 입장에서는 피해를 당하지 않기 위해 피싱 사이트로 유도하는 메일의 내용이 어떤 방법으로 사람의 눈을 속이는지 꼭 알아야 할 필요는 없다. 오히려 그보다는 신뢰할 수 있는 경로를 통해서 인터넷을 이용하는 습관이 더 중요하다. 이러한 습관은 불필요한 스파이웨어나 스팸으로 인한 피해를 예방하는 것에 있어서도 마찬가지로 중요한 요소이다.
개인의 이익을 추구하기 위해 보안에 취약한 시스템을 공격하거나 중요한 자료를 빼내려는 시도가 발생한 것은 오래 전부터 있어온 일이지만 이러한 위협의 대상들은 대규모의 기업들로만 인식되었고 개인 사용자들은 이러한 위협에 안전한 것으로 인식되어 왔다. 그러나 위에서 열거한 보안 위협들은 모두 개인을 공격대상으로 하고 있다는 점에서 주목할만하다. 금전적 이익을 노린 공격의 형태가 점점 증가하고 있는 최근의 상황으로 미루어 볼 때 이러한 위협으로 인한 개인의 피해 또한 언제든지 발생할 수 있는 일이 될 것이므로 인터넷 사용에 있어서 주의가 필요하다.

VI. 2004년 Key Issue II – 보안제품을 우회하는 감염기법

작성자 : 안철수연구소 정진성 연구원(jsjung@ahnlab.com)
차민석 주임연구원(jackycha@ahnlab.com)
이정형 연구원(jungh@ahnlab.com)
장영준 연구원(zhang95@ahnlab.com)

올 한해 악성코드의 감염기법은 어떤 것이 있었을까? 올해는 유난히 안티 바이러스 연구가를 혼란스럽게 하여 진단/치료를 어렵게 하기 위한 기법을 이용한 악성코드가 많이 발견되었다. 이러한 기법은 일반 사용자들은 알 수도 없고 알 필요도 없을 지 모른다. 그러나 자기도 몰래 실행된 후 그 존재조차도 확인하기 어렵다면 어떨까? 어떤 파일을 신고해야하는지 증상이 어떤것인지 눈으로 확인되지 않기 때문에 뭔가 찜찜하지만 멍하니 모니터만 바라보고만 있을 수 밖에 없을 것이다. 이런 악성코드들이 어디서, 어떻게 내 시스템을 노리는 것인지 감염되어도 그 존재를 알 수 없는 형태의 악성코드에 대해서 조금이나마 알아 보도록 하자.

올 한해동안 피해를 주거나 이슈가 되었던 악성코드들은 대부분 다음의 감염기법을 사용하였다.

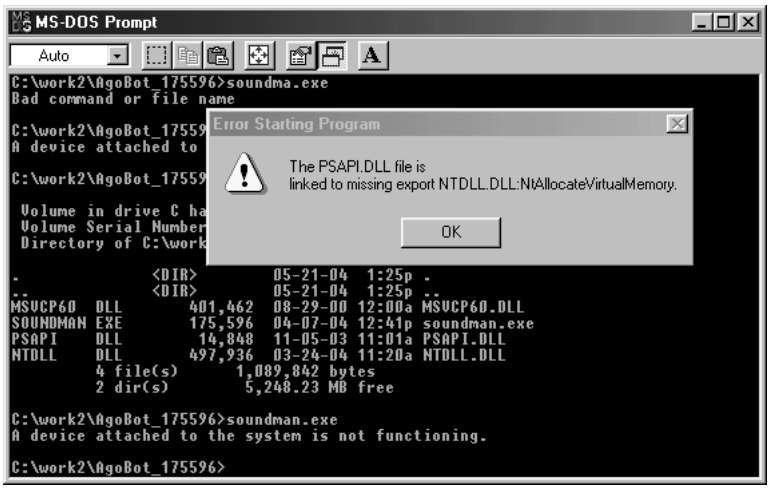
- 은폐형 악성코드
- 메모리 형태로 존재하는 악성코드
- 윈도우 XP SP2 보안기능 우회
- 암호화된 ZIP 파일을 이용한 백신제품 우회
- Reverse connection 을 이용한 보안장비 우회

1. 은폐형 악성코드

윈도우 NT 계열 (NT, 2000, XP)의 사용자들이 많아지면서 해당 기반에서 동작하는 은폐형 악성코드들이 전년에 비해 다소 증가하였다. 근래에는 파일을 감염시키는 윈도우 파일 바이러스보다는 프로세스로 실행되는 웜 또는 트로이목마가 대부분이다.
은폐형 악성코드는 도스 시절부터 악성코드 제작자들이 이용하는 방법이었고 그 수법도 발전하였는데 일반적으로 NT 계열에서 은폐기능을 동작하기 위해서는 Win32 API와 같은 유저모드의 함수들만 악성코드가 후킹하는 형태가 많았다. 하지만 최근들어 핵데프(Win-Trojan/HackDef), 헥스도어(Win-Trojan/Hexdoor)와 같은 커널 드라이버를 이용하여 커널함수를 후킹하여 동작하는 형태가 부쩍 증가하였다.

■ 은폐형 악성코드 동작환경 방법

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. 올해 알려진 악성코드의 은폐기법에서 사용하는 API들은 모두 윈도우 NT 이상에서만 존재하는 기능이기 때문이다.



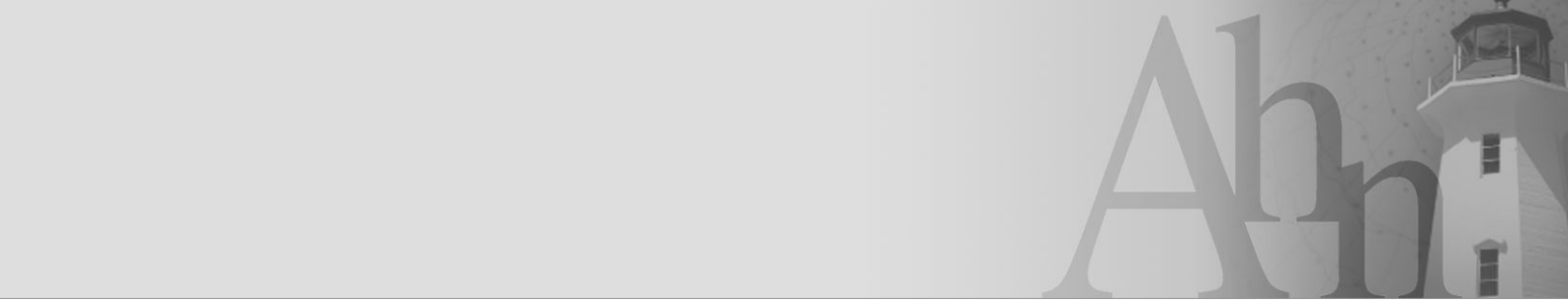
[그림1] 윈도우 98에서 은폐형 악성코드 실행 시 발생하는 에러 화면

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 감염시킬 숙주가 필요 없으므로 은폐 기법은 다음과 같이 바뀐다.

1. 로컬 드라이브에 존재하는 파일을 찾지 못하게 숨긴다.
2. 실행중인 프로세스에서 찾지 못하게 한다.
3. 연결된 포트 및 TCP/UDP 정보를 알아차릴 수 없게 한다.

이와 같은 은폐기능을 동작하기 위해서 다음과 같은 함수들이 사용된다.

- 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

■ 은폐형 악성코드 동향과 대응

은폐기법은 웜, 바이러스, 트로이목마의 효과적인 생존 방법 중 하나이다. 윈도우에서 은폐 기법은 이미 실제 사용자들을 위협하는 수준이 되었지만 상당수 백신제품들은 메모리에서 은폐형 악성코드를 진단 및 치료해 무력화하는 기능이 제외되어 있다. 시스템 감시(실시간 감시)에서 이러한 악성코드를 찾아 내는 경우는 있지만 이것은 부팅시나 해당 악성코드에 의한 파일 I/O가 발생할 경우에만 해당되어 치료를 못하는 경우가 많다. 하지만, 많은 악성코드 제작자들은 백신제품의 시스템 감시뿐 아니라 안전 모드에서도 자신을 숨기는 형태의 은폐형 악성코드 제작을 시도하고 있고 커널 모드 드라이버를 이용하여 더욱 치료하기 어려운 형태로 발전하고 있다. 앞으로 은폐형 악성코드 진단 기술은 계속 발전해 갈 것이다. 물론 백신제품들 역시 악성코드의 은폐기법을 무력화하기 위해 개선되고 있다.

2. 메모리 형태로 존재하는 악성코드

최근 백신제품 또는 특정 악성코드에 대한 전용백신은 진단과 치료를 위해서는 반드시 메모리 진단/치료기능이 선행되어야 한다. 웜 또는 트로이목마를 진단하기 위해서 지금까지 백신제품들은 프로세스라는 메모리 영역만을 검사하면 되었다. 하지만 올해 들어 부쩍 증가한 리모트 쓰레드(Remote Thread) 형태로 동작하는 악성코드를 진단/치료하기 위해서 프로세스 이외에 쓰레드 영역까지 그 진단범위를 넓혀야만 했다.
새서 웜이라고 알려진 악성코드가 전파에 이용했던 MS04-011 취약점을 똑같이 이용하는 코르고 웜은 Explorer.exe에 웜이 생성한 쓰레드를 주입(Injection, 인젝션)하여 동작한다. 따라서 악성코드가 발생하는 트래픽과 같은 증상등이 모두 Explorer.exe가 하는 것으로 보여져 사용자를 속일 수 있다.

■ 동작방식

코르고와 같은 악성코드가 이용하는 리모트 쓰레드 방식은 2003년 7월경 인터넷을 통해 알려지기 시작하였으며, 'CreateRemoteThread & WriteProcessMemory' 라고 표현 되기도 한

다. 악성코드뿐만 아니라 응용 프로그램들이 이용하는 정상 프로세스에 다른 코드를 주입하는 방법은 여러가지가 알려져 있다. 리모트 쓰레드 방식은 이중 하나일 뿐이다. 보통 다음의 방법이 알려져 있다.

- 레지스트리를 이용하는 방법
- 시스템 전역 윈도우 후크
- 리모트 쓰레드를 이용한 DLL Injection
- 리모트 쓰레드를 이용한 Code Injection
- BHO를 이용한 방법 (특정 프로세스만 해당)
- 오피스 플러그인 방법 (특정 프로세스들만 해당)

이 방법들도 은폐형 악성코드가 이용하는 것처럼 운영체제에 따라서 동작되지 않는 형태가 존재한다. 이중 악성코드에 많이 이용되는 형태가 리모트 쓰레드를 통한 DLL 및 Code Injecton 이다. 이를 이용한 악성코드로는 대표적으로 러브게이트 웜, 코르고 웜, 보프라 웜 등이 있다. 이 악성코드 이외에도 최근에는 애드웨어(스파이웨어)에서도 레지스트리를 이용한 은폐기법을 사용하고 있는 것으로 확인되었다.

Code Injecton 경우 보통 다음과 같은 단계로 해당 프로세스에 리모트 쓰레드로 동작하게 된다.

1. 대상 프로세스 오픈, OpenProcess (시스템 프로세스에 접근하려면 디버그 권한 선행)
2. 대상 프로세스에 주입되는 데이터를 메모리에 할당, VirtualAllocEx
3. 2에 할당된 데이터를 메모리에 기록, WriteProcessMemory
4. 대상 프로세스에 주입되는 코드를 메모리에 할당
5. 시작을 위해 메모리에 할당된 쓰레드를 콜백(초기화), ThreadFunc
6. 리모트 쓰레드 실행, ThreadFunc = CreateRemoteThread

■ 진단/치료

윈도우 백신제품들이 처음 출시 되었을 때, 그리고 위와 같은 방법이 알려지기 전에는 당연히 이러한 유형의 악성코드는 존재하지 않았다. 그러므로 불필요하게 프로세스 메모리 영역 이외에 다른 메모리 영역을 검사하는 것은 시간 낭비였다. 하지만 작년부터 이러한 방법이 인터넷에 공개되어 악성코드 제작자들이 이를 악의적인 방법으로 많이 이용하였다. 따라서 백신업체들도 프로세스 이외의 영역에 대한 메모리 검사/치료를 수행 할 수 있는 대안을 강구하게 되었다.

우선 이러한 형태의 악성코드를 효과적으로 진단하기 위해서는 다음과 같은 조건이 필요하다.

- 프로세서에 존재하는 모든 메모리 영역을 검색
- 악성코드가 사용한 쓰레드를 검색

쓰레드 검사와 치료를 위한 간단한 동작원리는 다음과 같다.

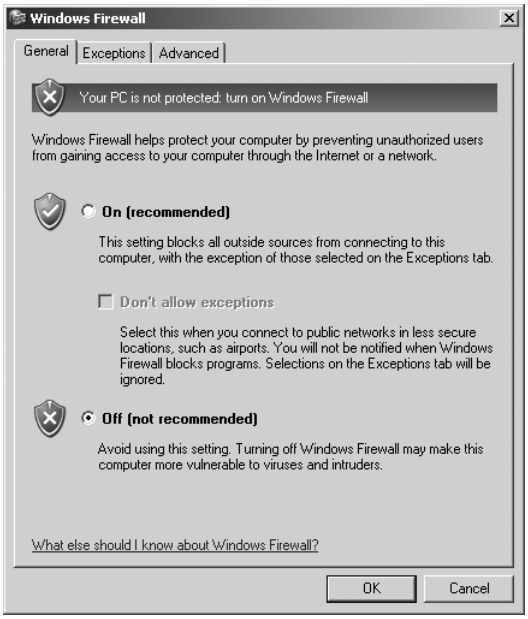
1. 악성코드 영역에 대한 Address 얻기
2. 쓰레드 List 얻기
3. 검사할 쓰레드 일시정지
4. 악성코드가 이용한 쓰레드 여부를 검사
5. 악성코드일 경우 제거

대부분의 외산 백신제품들은 제품에 위와 같은 악성코드에 대한 치료기능을 포함하기 보다는 전용백신을 만들어 배포하고 있다. V3 경우 V3Pro 2004에 위와 같은 악성코드도 검색할 수 있는 메모리 진단/치료 기능이 포함된 것은 물론이고 전용백신도 제작하여 배포하고 있다.

백신업체들은 코드레드(Code_Red), 슬래머(Slammer, SQL_Overflow) 악성코드 이후로 윈도우 메모리 검사와 치료가 얼마나 중요한 것 인지 깨닫게 되었다. 하지만 이것은 로컬 드라이브에 존재하는 악성코드를 검사하는 것과 같은 쉬운 문제가 아니었다. 어떻게 효율적으로 악성코드가 존재하는 메모리 영역을 정확히 검사 할 것인지, 검사된 코드를 어떻게 제거시킬 것인지가 중요한 문제였다. 치료보다 분석에 더 많은 자원 소요가 필요한 메모리 존재 형태의 악성코드는 2004년 안티 바이러스 연구원들에게는 하나의 새로운 도전이었지만, 이전에 없었던 새로운 유형이었다는 것과 그 수가 많았다라는 것을 제외하면 이것은 단지 그동안 코드레드나 슬래머를 통해서 연구되어온 결과로 대응이 가능하였다.

3. 윈도우 XP SP2 보안기능 우회

윈도우 XP SP2를 설치하면 이전 윈도우 버전의 시리즈와는 달리 많은 면에서 보안기능이 향상된다. 하지만 그 기능이 일반 사용자들이 느끼기에는 번거러울 정도로 귀찮게 여겨질 수도 있다. 그 중 하나가 바로 '방화벽' 기능이다. 물론 윈도우 XP 출시부터 인터넷 연결 방화벽(Internet Connection Firewall, ICF)이라 불리우는 방화벽이 포함되어 있었지만 그 기능은 사용자가 설정하지 않는 한 비활성화되어 있었고 기능을 활성화하기도 매우 어려웠다. 하지만 윈도우 XP SP2부터는 기본으로 그 기능이 활성화되어 있고 윈도우 시작시 제일 먼저 실행되도록 되어 있다.



[그림2] 윈도우 XP SP2 방화벽

이전 윈도우 XP 방화벽은 인터넷 연결 방화벽(ICF)/인터넷 연결 공유(ICS) 서비스가 성공적으로 시작되었을 경우에만 방화벽 기능이 활성화되었다. 따라서 윈도우 XP를 실행하는 컴퓨터를 시작하면, 컴퓨터가 네트워크에서 활성화되는 시간과 ICF를 사용해 연결이 보호되는 시간 사이에 지연이 발생했고 이 지연으로 인해 윈도우 부팅을 시작하는 동안 허가받지 않은 악성(유해) 트래픽이 차단되지 못하여 악성코드에 감염될 위험이 매우 높았다. 하지만 윈도우 XP SP2는 이러한 연결보다 우선적으로 시행되는 '시작정책'에 의해서 방화벽이 우선적으로 수행되도록 되어 있다.

■ 악성코드로부터의 도전

기능이 강화된 윈도우 XP SP2의 방화벽으로 인하여 일단 악성(유해)패킷은 외부로부터 차단되고 내부에서 외부로의 연결이 있을시 이를 요청하는 응용 프로그램에 대한 경고를 사용자에게 보내주어 사용자가 선택적으로 차단할 수 있게 해 두었다. 또한 윈도우가 사용하는 기본 포트이외에 모든 포트를 방화벽에서 차단하고 있어 인터넷 관련 응용 프로그램을 사용하는 사용자는 불편할지 몰라도 악성코드의 위협으로부터는 이전 윈도우보다 훨씬 안전하게 되었다. 그러나 윈도우 XP SP2가 배포되고 얼마 지나지 않아 악성코드 제작자는 윈도우 XP SP2의 방화벽을 무력화하기 위한 도전을 시도하였고 이는 벌써 몇몇의 악성코드에 의해서 현실로 나타났다. 바로 베이글 웜 변형 중 일부와 백쯔 웜(Win32/Bagz.worm), 자피 웜(Win32/Zafi.worm.15993)들이다. 또한 해외 일부 포럼에서는 윈도우 XP SP2 방화벽의 기능해제는 물론 버퍼오

버플로우를 방지하는 DEP(Data Execution Prevention) 설정 해제, 그리고 TCP/IP의 동시 연결횟수제한을 해제하는 프로그램들이 소개되었다. 이러한 것들은 충분히 악의적인 목적에 이용될 수 있는 만큼 윈도우 XP SP2의 보안기능은 여러모로 도전을 받고 있다.

가장 최근에 알려진 Win32/Bagle.worm.AR, Win32/Bagle.worm.AM, W32.Beagle.AV@mm, W32/Bagle.bb@mm, WORM_BAGLE.AT 라고 불리우는 베이글 웜 변형은 서비스 중지를 통한 ICF, ICS 기능해제를 시도하였다. 또한 최근 베이글 웜 변형 중 일부는 서비스 중지 및 설정해제를 통한 방법으로 윈도우 XP SP2 보안센터와 ICS를 중지하거나 기능을 해제한다.

[그림3] 윈도우 XP SP2 보안센터

최근에 알려진 정보에 의하면 윈도우가 지원하는 간단한 서비스 관련 명령만으로도 쉽게 보안센터의 기능을 해제하는 방법이 알려지기도 하였다.

백쯔라고 불리우는 이 웜은 현재 이 글을 작성하고 있는 동안 원형을 포함 8개의 변형이 발견, 보고되었다. 이 웜은 원형부터 여러가지 방법을 통하여 윈도우 XP SP2의 방화벽과 보안센터의 경고기능을 해제하는 증상을 가지고 있었다. 다음과 같다.

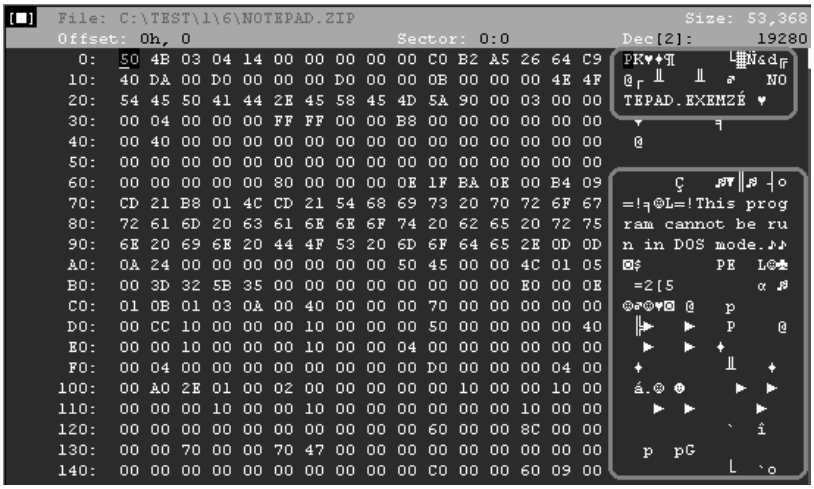
- netsh 명령을 이용 윈도우 방화벽 기능해제
- 네트워크 디바이스 드라이버를 이용하여 제3사의 방화벽도 우회

Win32/Zafi.worm.15993, WORM_ZAFI.C, W32.Erkez.C@mm라고도 불리우는 자피 웜 변형은 윈도우 XP SP2 방화벽과 보안센터 관련 레지스트리 값을 조작하여 이 기능을 무력화시킨다. 원형을 포함한 자피 웜 변형의 경우 국외에서 많은 피해문의가 있었던 악성코드이나, 다행히 국내에서는 그리 확산되지 않았으며 최근에 발견된 C형은 다행스럽게도 원형 등에 비하면 널리 확산되지 못했다.

최근 들어 복합적인 보안위협에 대응하기 위해서 방화벽은 매우 중요한 보안 소프트웨어로 자리잡았다. 방화벽은 네트워크 기반에 설치되는 것과 클라이언트에 응용 프로그램으로 설치되는 형태로 나눠질 수 있으며 윈도우 XP SP2는 당연 후자에 속한다. 윈도우 XP에 방화벽 기능이 포함될 때부터 이러한 악성코드의 출현은 예견되어 왔다. 윈도우 XP SP2라고 다를바는 없다. 윈도우 XP SP2 방화벽은 제3사의 방화벽과는 달리 기능을 중지하거나 설정 등을 변경하는데 있어서 다른 제약을 받지 않도록 되어 있다. 제3사 방화벽의 경우 암호를 설정하거나 방화벽과 관련된 중요한 파일을 보호함으로써 외부로부터의 공격에 대응하고 있다. 하지만 윈도우의 방화벽은 운영체제에 포함된 형태라 이러한 기능이 있다면 사용자로부터 쉽게 다가서지 못할 것이다. 따라서 윈도우 XP SP2의 방화벽과 보안센터를 무력화시키는 방법은 위에 알려진 베이글 웜, 백쯔 웜, 자피 웜이 이용하는 방법도 있지만, 윈도우가 기본으로 제공하는 서비스 관련 명령줄 프로그램을 사용해서도 이를 쉽게 무력화시킬 수 있어 언제든지 악성코드로부터 시스템이 노출되어 있다. 하지만, 이 방법은 로컬에서 사용자가 메일이나 P2P를 이용하여 다운로드한 악성코드가 실행될 때에만 가능하다. 향후 윈도우 XP SP2를 더욱 많은 사용자들이 선택하면 그만큼 윈도우 방화벽과 보안기능을 무력화하려는 악성코드는 더욱 늘어날 것으로 전망된다.

4. 암호화된 ZIP 파일을 이용한 백신제품 우회

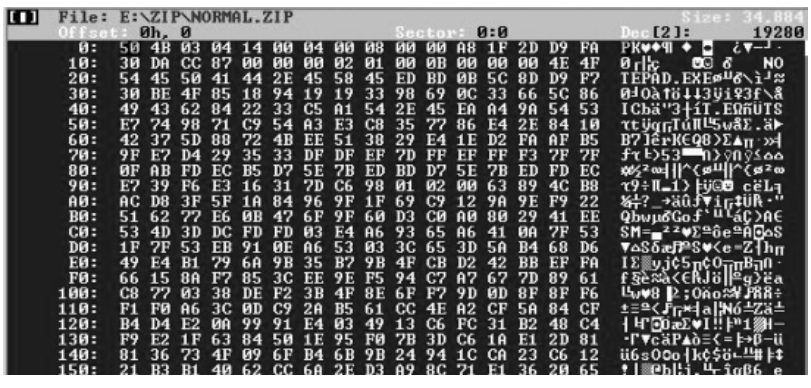
악성코드에서 네트워크 기반의 보안장비 및 백신제품에서의 진단/방어를 어렵게 하기 위해서 ZIP 파일에 암호를 추가해 메일 등으로 전송하는 기법이 올해 알려졌다. 언뜻 보면 너무도 쉬운 방법이지만 암호가 설정된 ZIP 파일의 암호를 어떻게 사용자에게 알려주는가가 관건이라 하겠다. 이 기법은 2004년에 베이글 웜에서 처음으로 사용되었다.
일반적으로 메일을 이용한 악성코드중에서도 ZIP으로 압축된 경우가 있다. 하지만 이러한 형태는 실제로 압축된 것이 아니다. Stored 방식이라고 불리우는 이 방법은 압축대상 파일에 ZIP헤더만 붙이는 것으로 대상파일은 실제로 압축되지 않는다.
다음은 Stored 된 ZIP 파일이다. 실제로 데이터는 압축되지 않았다.



[그림4] Stored 된 ZIP 파일

하지만 ZIP 헤더정보가 존재하므로 ZIP 파일로 인식될 수 있다. 그러나 베이글 웜이 사용한 방법은 압축관련 라이브러리를 가지고 있어 실제로 랜덤한 암호를 가진 ZIP 파일을 생성하고 암호가 적힌 텍스트를 메일로 발송한다.

아래는 일반 notepad.exe를 zip 으로 압축한 파일의 내부를 확인한 그림이다.



[그림5] ZIP 으로 압축된 정상파일

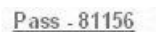
다음은 Notepad.exe를 ZIP으로 압축할 때 암호를 넣어서 압축한 파일과 위의 일반적인 ZIP 파일과 비교한 그림이다.

[그림6] 암호가 설정된 ZIP 파일과 일반적인 ZIP 파일을 비교한 화면

[그림6]을 보면 알 수 있듯이 ZIP파일에 암호를 추가함으로써 기존의 일반 ZIP 파일과는 내부의 내용이 달라진다. 이는 매우 수학적인 ZIP의 암호알고리즘으로, 같은 암호를 사용해 똑같은 파일을 암호화하여도 매번 다른 코드를 가진다.

■ 악성코드의 출현

올 7월 인터넷상에 유포된 베이글 웜 중에서 베이글.AA 웜(Win32/Bagle.worm.AA)은 ZIP 파일에 암호를 넣어 메일에 첨부된 형태로 유포되는 대표적인 케이스이다. 첨부파일 ZIP의 암호는 본문내용에 [그림7]과 같은 그림의 형식으로 표시하였다. 숫자암호는 랜덤하게 변경된다. 이 암호도 처음에는 메일본문에 텍스트 형태로 존재하였다. 그러자 백신제품들이 메일 본문에서 암호가 있는 텍스트만 파싱하여 암호를 풀고 웜을 진단 할 수 있게 되었다. 이 방법이 백신제품에서 구현되자 베이글 제작자는 암호를 텍스트가 아닌 [그림7]과 같은 이미지로 첨부하게 되었다.



[그림7] 베이글 웜 변형에 첨부된 ZIP 파일의 암호 이미지

이미지로 되어 있다고 해도 이미지 프로세싱을 통해서 얼마든지 암호가 어떤 글자인지 알 수 있었지만 이를 제품군에 적용하는 것에 대한 정책적인 결단과 적용후 리소스를 얼마만큼 차지하는가에 대한 문제가 새로운 이슈로 떠올랐다.

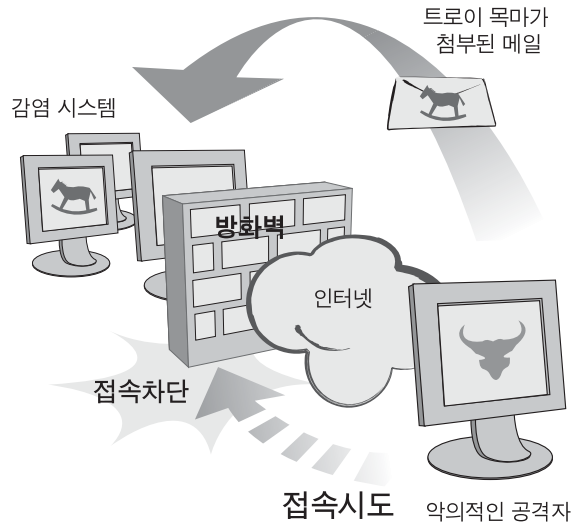
■ 대처방안

ZIP 파일에 임의의 값으로 암호를 넣은 경우는 ZIP 파일의 내용이 모두 다르게 되므로, 보안 장비나 보안 프로그램을 무력화시키기 위해 악성 프로그램 등에서 사용되기 시작하였다. 특히 네

트워크 기반의 보안장비에서는 파일의 내용을 가지고 패턴을 거의 만들 수가 없으나, 백신제품은 해당 ZIP과 압축되어 있는 내용의 몇몇 패턴과 기타방법을 가지고 진단할 수 있다.
사용자들은 위와 같이 ZIP 파일에 암호가 걸린 형태의 메일과, 암호가 이미지로 전달되는 메일은 삭제하며, 의심스러운 파일은 열어보지 않는 것이 예방책으로는 최선이다.

5. 리버스 커넥션(Reverse connection)을 이용한 보안장비 우회

2004년에 발견된 트로이목마와 일부 웜들의 경우 2004년 이전에 사용되던 수동적인 공격방법에서 벗어나 능동적인 공격방법을 모색하기 시작하였다. 그 중에서도 2004년 6월 초여름 관공서와 국가연구기관의 시스템들에 감염되어 언론의 많은 주목을 받았던 핍뷰어(Win-Trojan/PeepViewer) 변형들의 공격기법을 들 수 있다.
일반적으로 전통적인 트로이목마와 백도어류는 특정 공격목표가 되는 시스템의 사용자에게 사회공학기법(Social Engineering)을 이용하여 사용자로 하여금 수동적으로 악성코드를 설치하도록 유도하는 것에 많은 초점이 맞추어져 있었다. 그리고 감염된 시스템에서 특정 포트를 오픈하여 외부에서 해당 트로이목마의 제작자 또는 공격자로 하여금 해당 포트를 통하여 감염된 시스템에 사용자 모르게 접속할 수 있도록 유도하는 형태를 많이 보였었다.



[그림8] 전통적인 트로이목마와 백도어를 이용한 공격기법

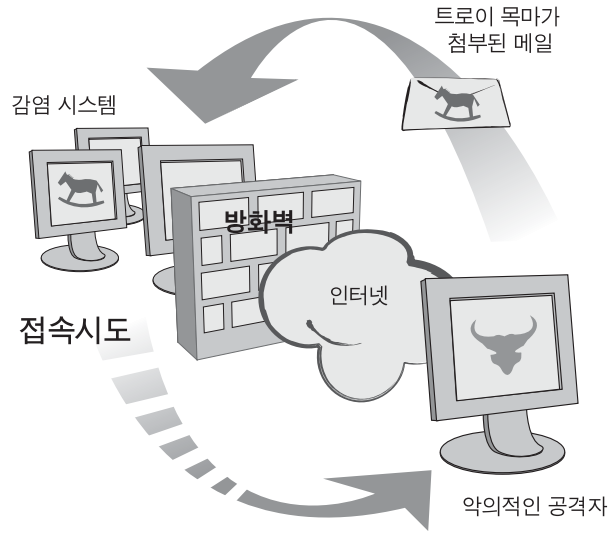
■ 동작방법

그러나 핍뷰어 변형들의 경우 전통적인 트로이목마와 백도어류 같이 사회공학기법을 이용하여 이를 취하고 있으나 전통적인 방식이 아닌 색다른 방법을 사용하였다. 이 방법은 감염된 시스템에 대한 공격자의 태도가 수동적인 태도가 아닌 감염된 시스템에 대한 능동적인 형태로 변화하였는데 이러한 변화를 이끌었던 방법이 바로 리버스 커넥션이다. 리버스 커넥션 기법은 감염된 시스템에서 공격자가 지정한 특정 시스템으로 역으로 접속을 시도하여 IP 주소 또는 시스템 정보들을 유출하는 방식을 통칭하고 있다.

핍뷰어 변형들을 예로 들어 볼 경우, 공격자는 최초 공격 대상이 되는 시스템들로 '워크샵내용과 일정.MDB' 라는 시스템 사용자들이 호기심을 끌만한 첨부파일을 첨부하는 전형적인 사회공학기법을 이용한 메일을 다량으로 발송하게 된다. 해당 메일을 수신한 시스템의 사용자가 해당 MDB 파일을 실행하게 될 경우, 사용자에게는 일반적인 문서를 보여주게 된다. 그러나 그 문서가 실행됨과 동시에 사용자 모르게 핍뷰어 트로이목마가 시스템에 설치되며 일반적인 트로이목마들과 달리 핍뷰어 변형들은 잘 알려진 포트를 통해 공격자의 시스템으로 접속을 시도하게 된다. 이러한 문제로 인해 앞서 언급한 것과 같이 다양한 보안 소프트웨어와 보안 장비들로는 핍뷰어 변형과 같이 리버스 커넥션 공격기법을 사용하는 악성코드들을 탐지하기가 어렵게 된다.

■ 리버스 커넥션 기법 발달 배경

이러한 리버스 커넥션 기법이 발달하게 된 배경은 다양한 안티 바이러스 기법과 보안 장비들이 개발되기 시작했기 때문이다. 특히 초고속네트워크 인프라가 갖추어지면서 개인용 컴퓨터에서도 컴퓨터 부팅과 동시에 인터넷과 같은 불안전하고 익명을 보장받을 수 있는 네트워크로 접속이 가능하게 되었다. 이러한 문제로 개인 사용자들의 경우에도 이제는 백신제품 외에도 개인용 방화벽(Personal Firewall)을 사용하기 시작하였고 정보보안과 인트라넷 보호에 신경을 기울이는 기업 사용자들 역시 방화벽과 함께 침입탐지시스템(IDS)과 침입차단시스템(IPS)들을 도입하여 사용하고 있다. 이러한 보안 소프트웨어와 보안 장비로 인해 예전과 달리 인터넷과 같은 외부 네트워크 환경에서 기업 내부의 보호된 인트라넷에 존재하는 특정 시스템에 대한 공격이 점점 어려워지게 되자 악의적인 공격자들 또한 이러한 보안 소프트웨어와 보안 장비들을 회피하기 위하여 리버스 커넥션과 같은 방법을 모색한 것으로 보여진다.



[그림9] 리버스 커넥션(Reverse Connetion) 기법을 이용한 공격

일반적으로 대부분의 방화벽, IDS, IPS들은 외부 네트워크에서 내부 네트워크로 유입되는 인바운드(InBound) 형태의 패킷에 대해서는 불법적인 또는 인증되지 않은 형태에 대해 자동으로 탐지하고 차단하게 된다. 그러나 내부 특정 시스템에서 외부 네트워크로 발송하게 되는 아웃바운드(OutBound)형태의 패킷에 대해서는 인바운드 형태만큼 면밀한 검사를 하지 않는 것이 일반적이다. 게다가 TCP 80 포트와 같이 일반적인 웹 어플리케이션에서 많이 사용하는 포트를 이용하여 외부로 접근을 시도하게 될 경우에는 방화벽, IDS, IPS들이 이러한 패킷을 탐지하기 어려운 것이 사실이다. 이러한 방화벽, IDS, IPS들의 맹점을 핍뷰어 변형과 같은 트로이목마와 백도어류가 리버스 커넥션 기법을 이용하여 공격을 시도한 것이다.

VII. 2005년 예측

작성자 : 안철수연구소 차민석 주임연구원(jackycha@ahnlab.com)

2005년의 악성코드 동향은 2004년과 유사할 것으로 보인다. 악성 IRC봇류는 여러 제작자의 개량과 변형 생산으로 끊임없이 등장하고 이런 악성 IRC봇류에 대해 백신업체도 엔진 업데이트 없이 유사 변형을 진단하는 일반적 진단(General detection) 혹은 코드를 분석해 알려지지 않은 변형을 유추해 내는 휴리스틱 진단(Heuristic detection)을 계속 강화할 것으로 보인다.

이외 2004년 이슈가 된 스파이웨어, 피싱에 대해서도 계속적인 솔루션이 등장할 것으로 보인다. 상당수 백신업체는 스파이웨어 문제를 안티 스파이웨어 진영에서 처리하기를 바라고 있지만 몇몇 백신업체는 자체적으로 스파이웨어 퇴치 프로그램을 제공하거나 기존의 스파이웨어 퇴치 프로그램을 라이센스 혹은 인수하고 있다. 다만 피싱에 대한 대처는 현재까지 확실한 해결방안 없이 다각도로 논의만 되고 있으며 피싱 방지 솔루션도 개인 정보 유출 금지 등으로 한정되어 있다.

2004년은 64비트 바이러스 등장, 휴대폰 웜의 등장 및 일부 지역 확산 등 향후 문제가 될 미래형 악성코드의 시작 년도로 볼 수 있다. 2005년은 64비트 보급과 모바일 환경에 따라 일반 사용자들이 피해를 입게 될 64비트 바이러스 등장, 다양한 모바일 악성코드 등장 및 확산을 예상할 수 있다. 다만 이런 예상은 2005년에 64비트 컴퓨터와 모바일 환경이 어떻게 변하는가에 따라 시기가 2~3년 후에 발생할 수도 있다. 일반적으로 악성코드는 많은 사용자가 동일 플랫폼을 이용할 때 퍼지기 시작하기 때문이다. 국내에도 2005년부터 위피로 동일된 플랫폼이 사용되므로 위피용 악성코드가 등장할 가능성이 있다. 하지만, 이미 사용되고 있는 구형 폰이 위피 지원 폰으로 교체되기 전까지는 휴대폰 악성코드가 널리 퍼지는 일은 나타나지 않을 것이다. 하지만, 64비트 CPU의 보급이나 휴대폰 플랫폼의 통일화가 앞당겨지면 악성코드의 등장 및 피해 시기도 달라질 수 있다.

별첨 : 2004년 ASEC Monthly Report 목차

● ASEC Report 2004년 1월

(http://b2b.ahnlab.com/securityinfo/asec_report/200402.html)

1월 악성코드 Top 10
1월 국내 신종 악성코드 발견 동향
1월 신규 보안 취약점
1월 일본 피해 동향
1월 중국 피해 동향
테크니컬 컬럼 – 마이둠 웜의 뒷 이야기

● ASEC Report 2004년 2월

(http://b2b.ahnlab.com/securityinfo/asec_report/200403.html)

2월 악성코드 Top 10
2월 국내 신종 악성코드 발견 동향
2월 신규 보안 취약점
2월 일본 피해 동향
2월 중국 피해 동향
테크니컬 컬럼 I – 악성코드 수동 조치법
테크니컬 컬럼 II – MBSA 툴을 이용한 윈도우 패치

● ASEC Report 2004년 3월

(http://b2b.ahnlab.com/securityinfo/asec_report/200404.html)

3월 악성코드 Top 10
3월 국내 신종 악성코드 발견 동향
3월 신규 보안 취약점
3월 일본 피해 동향
3월 중국 피해 동향
테크니컬 컬럼 – 베이글 웜으로 보는 악성코드 진화

● ASEC Report 2004년 4월

(http://b2b.ahnlab.com/securityinfo/asec_report/200405.html)

4월 악성코드 Top 10
4월 국내 신종 악성코드 발견 동향
4월 신규 보안 취약점
4월 일본 피해 동향
4월 중국 피해 동향
테크니컬 컬럼 – 블래스터 웜의 부활? 새서 웜

● ASEC Report 2004년 5월

(http://b2b.ahnlab.com/securityinfo/asec_report/200406.html)

5월 악성코드 Top 10
5월 국내 신종 악성코드 발견 동향
5월 신규 보안 취약점
5월 일본 피해 동향
5월 중국 피해 동향
테크니컬 컬럼 – 최신 은폐형 악성코드

● ASEC Report 2004년 6월

(http://b2b.ahnlab.com/securityinfo/asec_report/200407.html)

6월 악성코드 피해 Top 10
6월 국내 신종 악성코드 발견 동향
6월 신규 보안 취약점
6월 일본 피해 동향
6월 중국 피해 동향
테크니컬 컬럼 – 휴대폰 웜의 등장과 향후 전망
2004년 상반기 동향 분석

● ASEC Report 2004년 7월

(http://b2b.ahnlab.com/securityinfo/asec_report/200408.html)

7월 악성코드 피해 Top 10
7월 국내 신종 악성코드 발견 동향
7월 신규 보안 취약점
7월 일본 피해 동향
7월 중국 피해 동향
테크니컬 컬럼 I – 자동 이메일 추출 수집기 대응방법
테크니컬 컬럼 II – 트래픽 분석의 시작과 준비

● ASEC Report 2004년 8월

(http://b2b.ahnlab.com/securityinfo/asec_report/200409.html)

8월 악성코드 피해 Top 10
8월 국내 신종 악성코드 발견 동향
8월 신규 보안 취약점
8월 일본 피해 동향
8월 중국 피해 동향

AhnLab 안철수연구소