ASEC Report 2월

® ASEC Report

2006. 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.

I. 2월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자: 박태환 주임연구원(juun5@ahnlab.com)

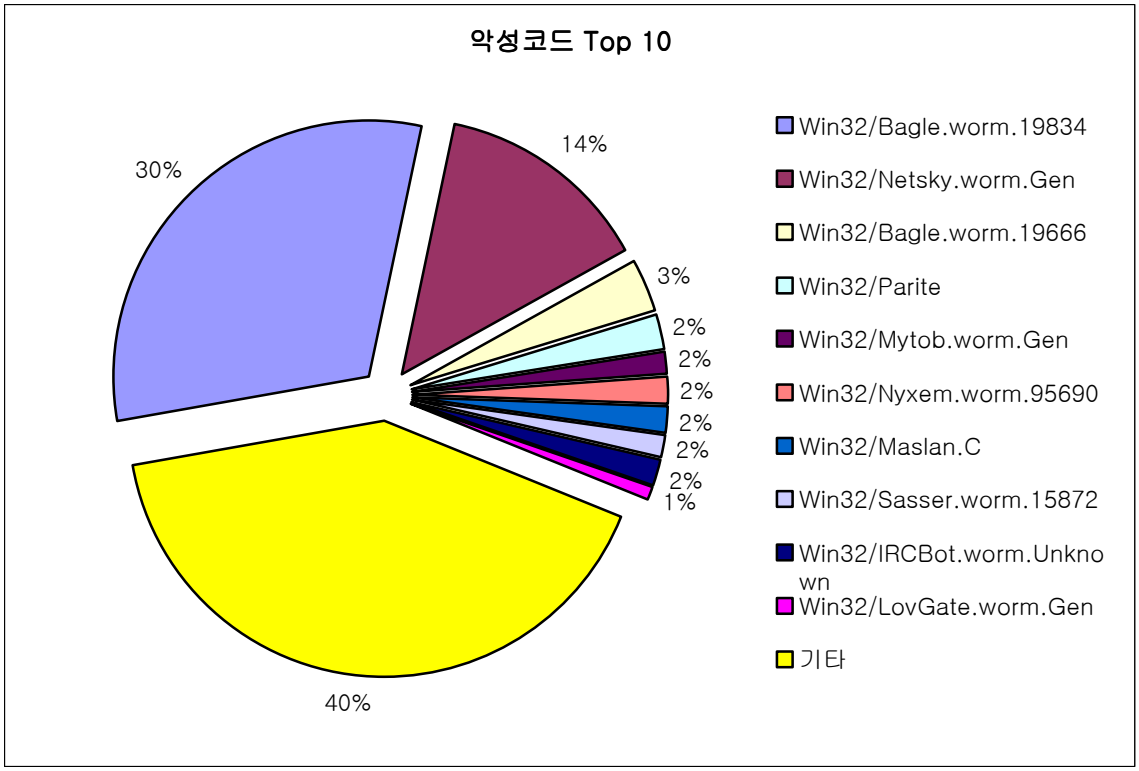
순위		악성코드명	건수	%
1	new	Win32/Bagle.worm.19834	327	31.02%
2	↓1	Win32/Netsky.worm.Gen	145	13.76%
3	new	Win32/Bagle.worm.19666	34	3.23%
4	↓2	Win32/Parite	23	2.18%
5	new	Win32/Mytob.worm.Gen	17	1.61%
	new	Win32/Nyxem.worm.95690	17	1.61%
7	↓3	Win32/Maslan.C	16	1.52%
	↓3	Win32/Sasser.worm.15872	16	1.52%
	↓6	Win32/IRCBot.worm.Unknown	16	1.52%
10	↓3	Win32/LovGate.worm.Gen	11	1.04%
		기타	432	40.99%
합계			**1,054**	

[표1] 2006년 2월 악성코드 피해 Top 10

2월 악성코드 피해 동향

이번 달은 2006년 2월에 출현한 베이글.19834 웜(Win32/Bagle.worm.19834), 베이글.19666 웜 (Win32/Bagle.worm.19666)이 출현과 동시에 많은 피해를 입혀 각각 1위, 3위를 차지하며 Top 10에 랭크 되었다. 그리고 5위에 랭크된 나이젬.95690 웜(Win32/Nyxem.worm.95690)은 매월 3일에 파일을 손상시키는 증상이 있어, 최초 활동일인 2월 3일에 1999년의 Win95/CIH 피해와 같은 큰 피해가 발생할 것으로 예상되었으나, 다행히 많은 피해는 보고되지 않았다. 그 외 넷스카이 웜(Win32/Netsky.worm.Gen), 패리테 바이러스(Win32/Parite), 마슬란.C(Win32/Maslan.C) , 아이알씨봇 웜(Win32/IRCBot.worm.Unknown), 러브게이트 웜(Win32/LovGate.worm.Gen), 새서.15872 웜(Win32/Sesser.worm.15872) 은 순서만 조금씩 변경된 상태로 상위권에 자리하였으며 지난 달 9위를 차지했던 소버.55390 웜(Win32/Sober.worm.55390)은 순위권 밖으로 밀려났다. 2월 악성코드에 의한 전체 피해신고 건수는 2006년 1월에 비해서 다소 증가한 수치를 보이고 있으나, 2005년 동월에 비해 크게 감소하여 전년도 대비 53.25%에 해당하는 1,054건이 접수되었다.

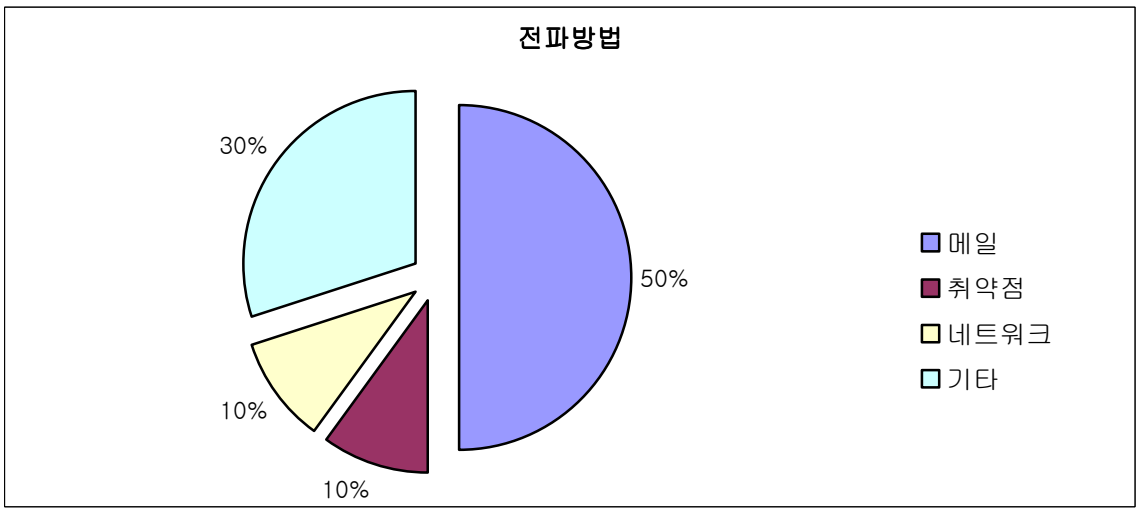
2월의 악성코드 피해 Top 10을 도표로 나타내면 [그림1]과 같다.



[그림1] 2006년 2월 악성코드 피해 Top 10

2월 악성코드 Top 10 전파방법 별 현황

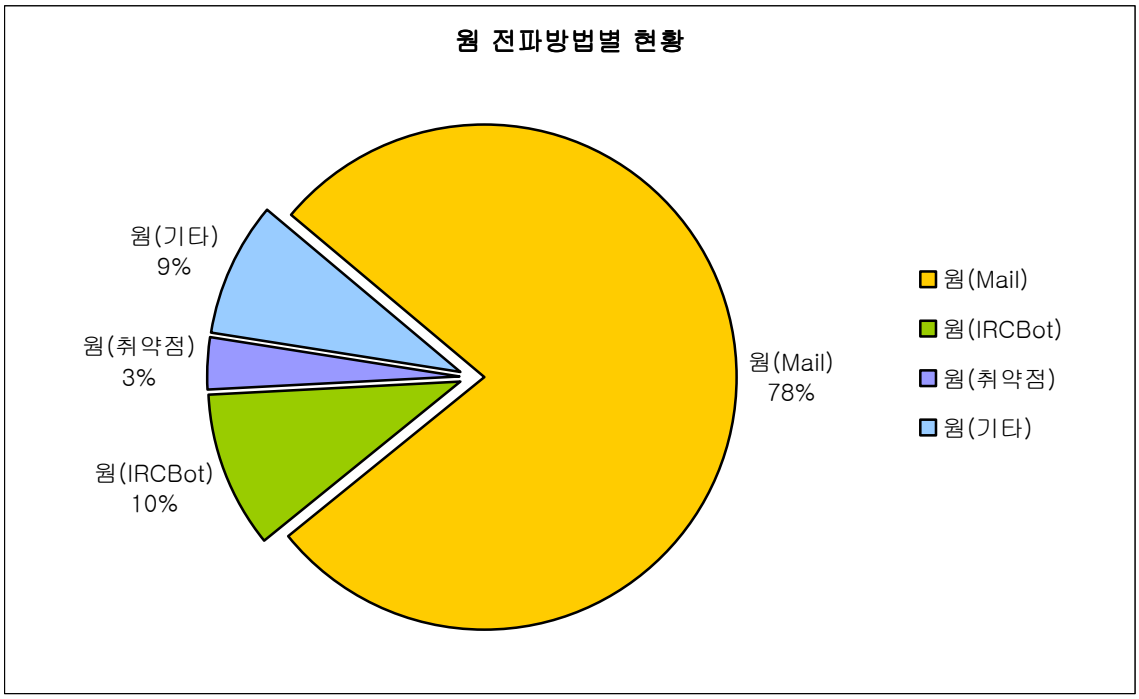
[표1]의 Top 10 악성코드들은 주로 어떠한 감염 경로를 가지고 있는지 [그림2]에서 확인할 수 있다.



[그림2] 2006년 2월 악성코드 Top 10의 전파 방법별 현황

메일로 전파되는 특징이 있는 베이글 웜 이나 마이톱 웜이 꾸준히 발견되고 있기는 하나 기

존의 전파기법을 답습하는 형태를 취하다 보니 큰 영향력을 끼치지는 못하고 있다. 다만 지난 1월, 60%이상을 차지하고 있던 매스메일러의 수치가 조금 줄어 들었다는 점과, 기타 30%에 해당하는 다양한 형태의 악성코드들이 조금씩 증가하고 있다는 점에 주목할 만 하다.



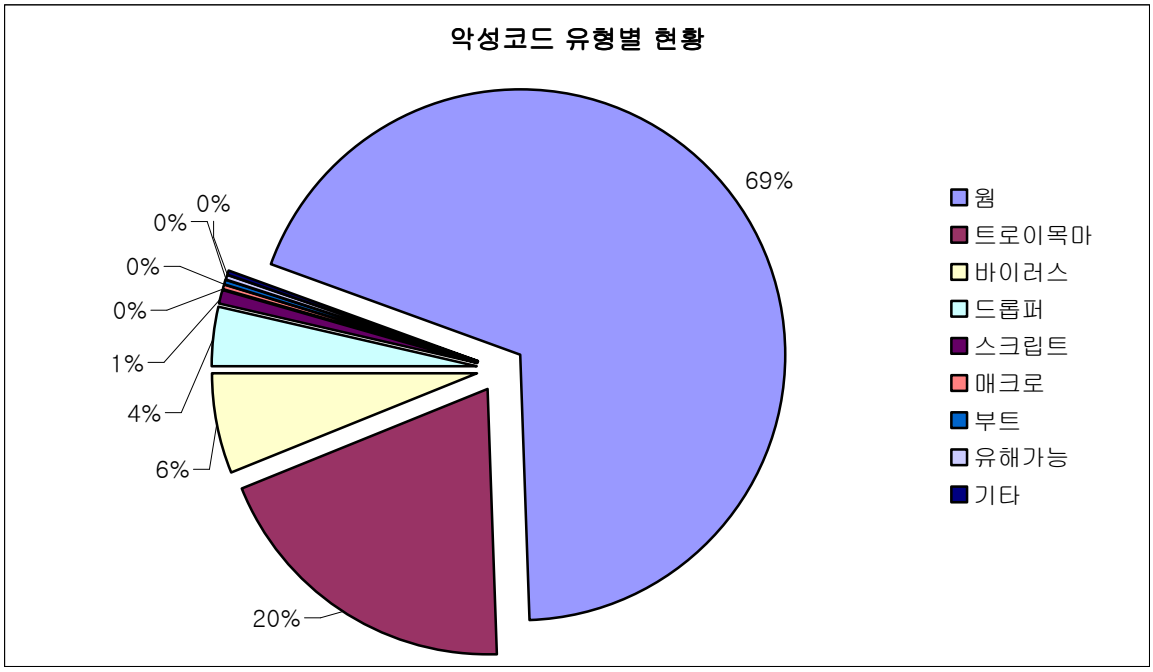
[그림3] 2006년 2월 웜의 전파방법 별 현황

[그림3]은 2월에 피해 신고된 웜의 전파방법에 대한 현황이다.
2월에 악성코드 피해 신고된 웜이 이용하는 전파방법 중 메일을 통한 전파방법이 78%로, 여전히 최고의 비중을 차지하고 있다. 그 외에 아이알씨봇 웜은 10%로 줄어든 반면 취약점 및 기타 웜들의 비중은 조금 증가하였다.

피해신고 된 악성코드 유형 현황

2월에는 웜과 트로이목마가 각각 69%와 20%로 거의 90%이상을 차지하였다. 이 수치만으로 웜이 대세임을 알 수 있으나 개인정보 유출을 노리는 트로이목마와 드롭퍼도 지속적으로 증가할 것으로 보인다.

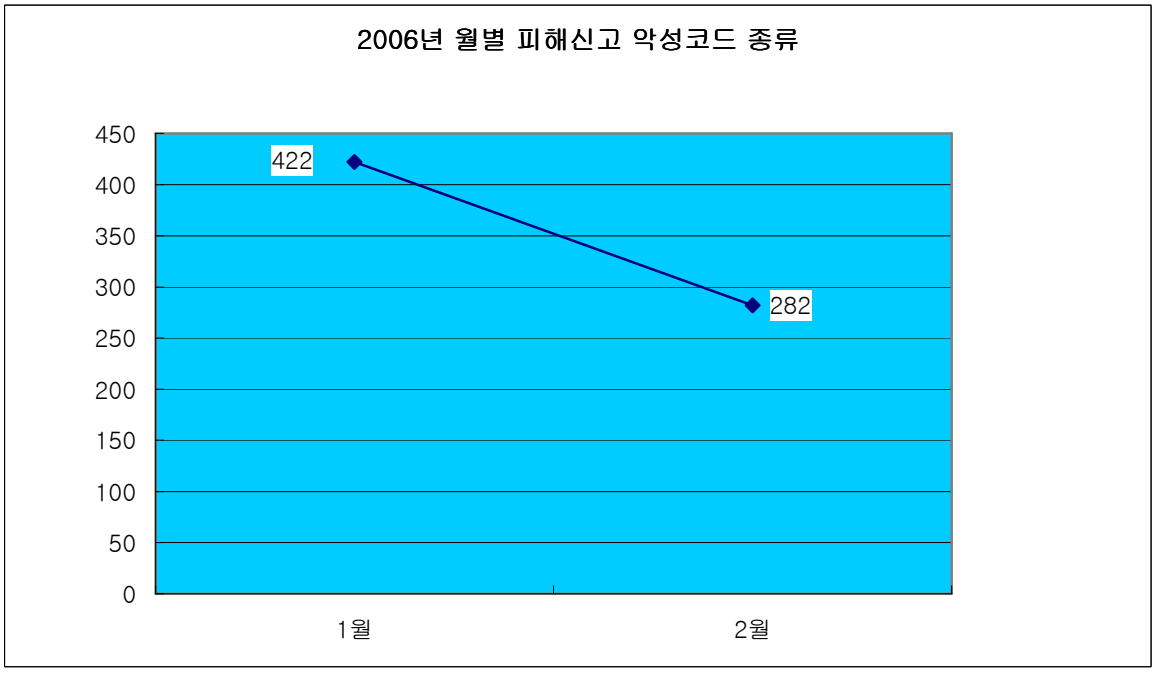
악성코드 유형별 현황은 [그림4]와 같다.



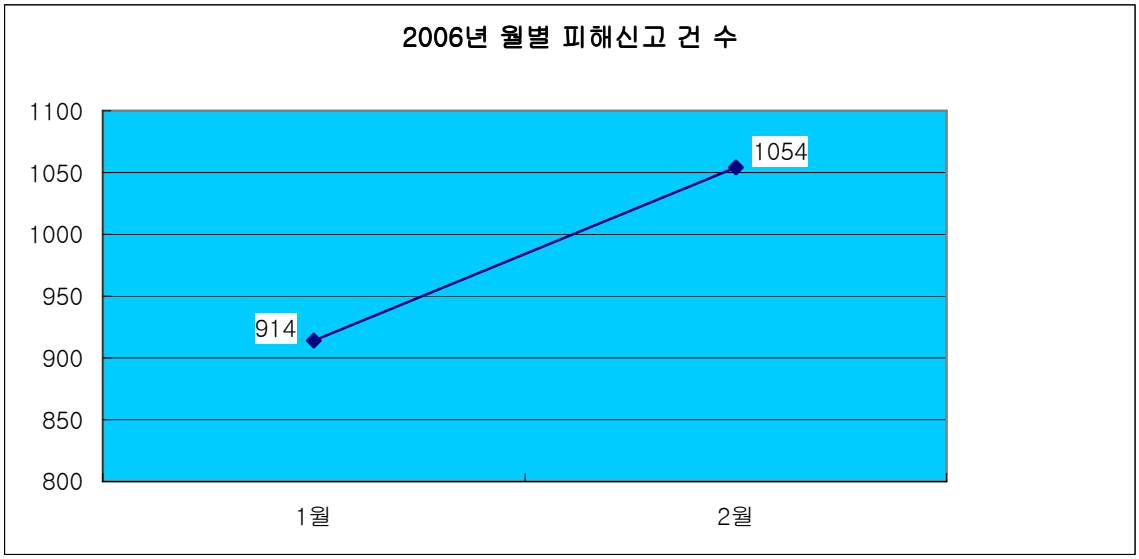
[그림4] 2006년 2월 피해 신고된 악성코드 유형별 현황

월별 피해신고 된 악성코드 종류 현황

2월에 피해 신고된 악성코드 진단명은 282개이다.



[그림5] 2006년 월별 피해신고 악성코드 종류



[그림6] 2006년 월별 피해신고 건수

2006년 1월에 비해 피해신고가 되고 있는 악성코드의 수는 줄어 들었으나 피해신고 건수가 증가하였다는 것은 그만큼 전파력이나 위험도가 높은 악성코드가 등장하였던 2월이었음을 의미한다. 매스메일러의 수가 줄어든다 할지라도 여전히 존재하는 보안위협과 개인정보 유출을 노리는 P2P, 드롭퍼 , 다운로더 등이 증가하는 추세이므로, 항상 주의를 기울이는 것을 잊지 말아야 하겠다.

(2) 신종(변형) 악성코드 발견 동향

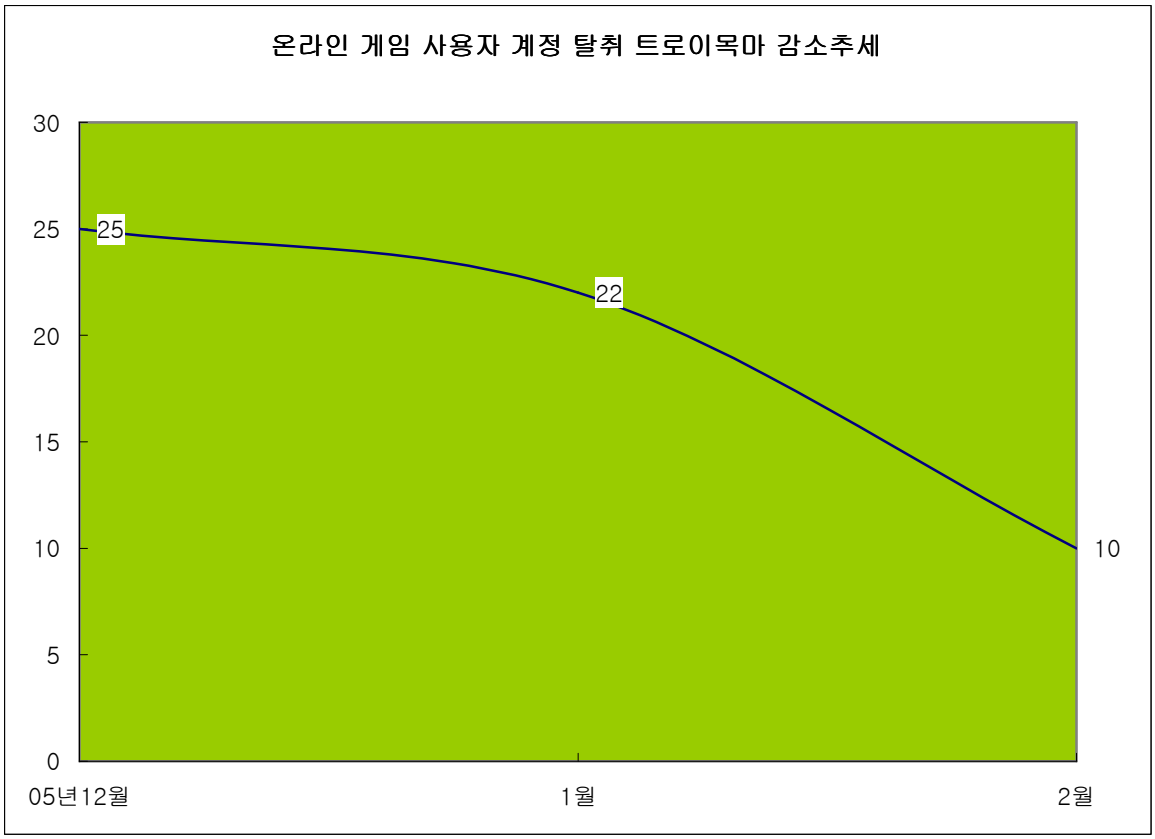
작성자: 정진성 주임연구원 (jsjung@ahnlab.com)

2월 한달 동안 접수된 신종(변형) 악성코드의 건수는 [표1], [그림2]와 같다.

웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
26	80	25	0	1	0	0	0	0	0	132

[표1] 2006년 2월 유형별 신종 (변형) 악성코드 발견현황

총 132개의 신종(변형) 악성코드가 발견되었는데 이는 지난 1월과 비교하여 무려 126건이나 감소한 수치이다. 특정 악성코드의 감소보다는 전체적으로 모든 유형의 악성코드가 감소하는 현상을 보이고 있다. 지난 1월도 2005년 12월에 비해 30건 감소하는 추세를 보였는데, 지속적인 감소추세가 일시적인 현상인지 아니면 지속될 것인지는 좀 더 지켜보아야 할 것으로 보인다. 2006년 들어 2개월 동안 신종(변형)의 악성코드가 감소한 원인으로는 중국발 해킹에 의한 악성코드 출현이 감소하고 있는 것이 그 한 원인으로 추정된다. 이는 지난달 동향에서도 나타난 현상이지만, 2월 역시 온라인 게임의 사용자 계정을 훔쳐내는 트로이목마나 백도어 기능을 갖는 트로이목마들의 수가 [그림1]과 같이 눈에 띄게 줄어 들었다.

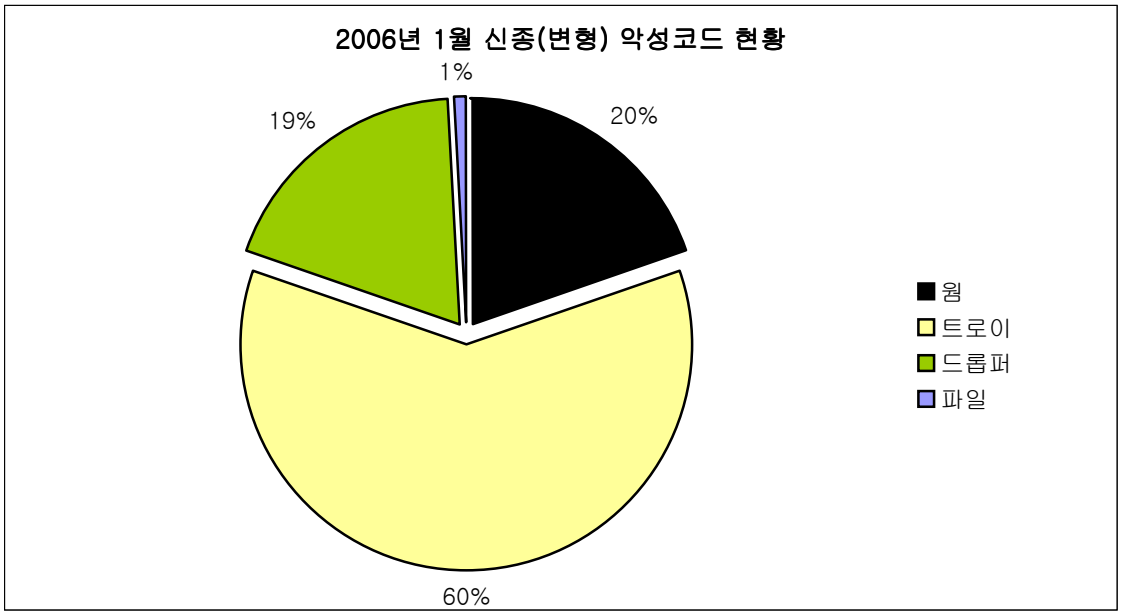


[그림1] 온라인 게임 사용자 계정 탈취 트로이목마 현황

이러한 현상은 뒤에서 소개되는 2006년 2월 악성코드 변형별 유형 중 중국산 악성코드 비

율 감소 현상을 통해 다시 확인해 보도록 하겠다.

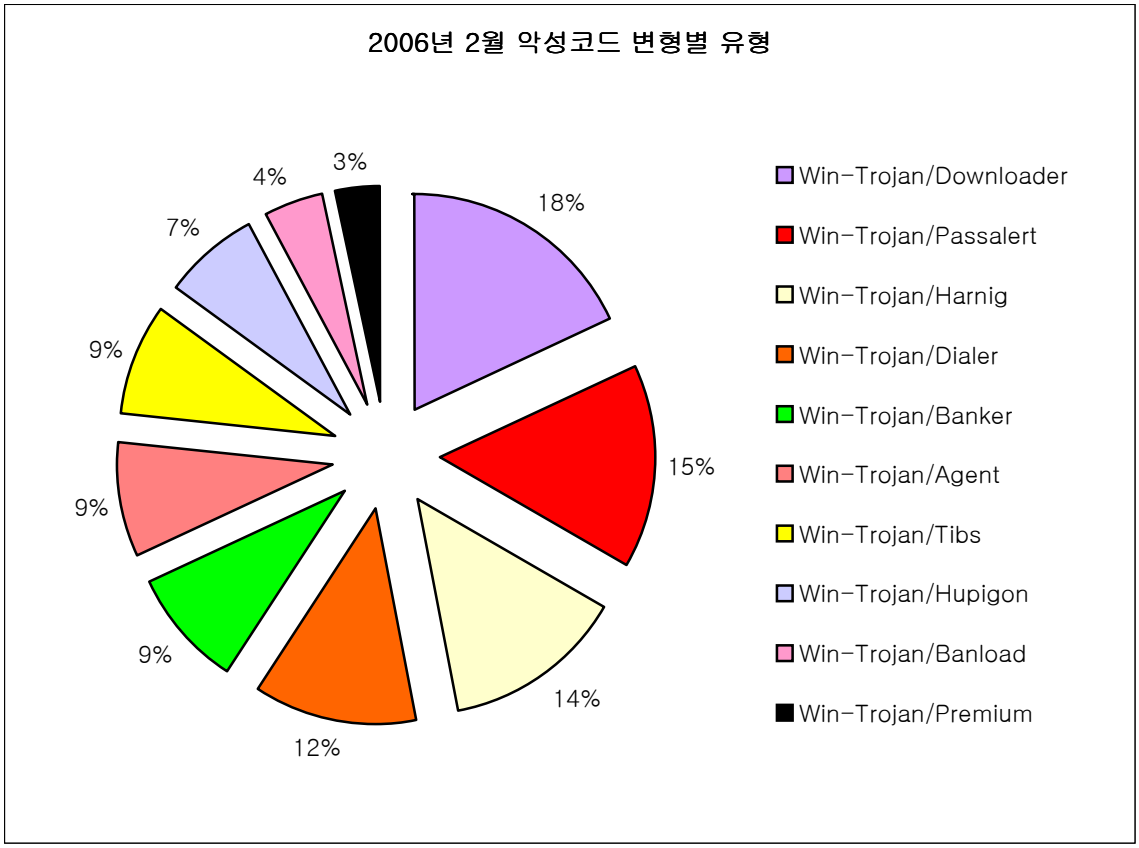
[그림2]는 2월 신종(변형)악성코드의 비율을 나타낸 것이다.



[그림2]2006년 2월 신종(변형) 악성코드 비율

트로이목마가 차지하는 비율은 여전히 높은 것을 알 수 있다.
그러나 2월에는 파일을 감염시키는 바이러스가 몇 건 보고 되었다는 것이 다소 특이하다. 이 바이러스는 샐리티 바이러스(Win32/Sality.20480) 라고 명명 되었다. 이 바이러스는 러시아에서 제작된 것으로 추정하고 있으며 감염된 경우 애드웨어를 특정 호스트로부터 다운로드 하거나 혹은 가짜 안티 스파이웨어를 다운로드하여 시스템이 위험한 것처럼 거짓된 정보를 출력 하기도 한다. 이 바이러스의 감염 특징은 다음과 같다.

- ✓ 감염된 파일의 시작주소는 변경되지 않는다.
- ✓ 감염된 파일은 섹션이 하나 추가되며 섹션명은 원래 섹션명 중에서 알파벳 하나를 무작위로 붙여 만든다. 추가된 섹션의 크기는 20,480 바이트이며 바이러스의 코드가 담겨 있다(단순하게 암호화 되어 있다).
- ✓ 감염된 파일은 시작주소부터 106 바이트만큼 바이러스가 생성한 Stub 코드가 변경되고 원래 코드는 추가된 섹션에 저장되어 있다.
- ✓ 바이러스는 암호화된 자신을 디코드하기 위하여 x87 명령어를 사용하며 이는 안티 에뮬레이터 기법의 일종으로 일부 안티 바이러스의 제너릭(Generic) 진단을 무력화 하는 것으로 보인다.



[그림3] 악성코드 변형별 유형 및 분포율

[그림3]은 2월 발견된 신종(변형) 악성코드 중 가장 많이 발견된 신종(변형) 악성코드 유형을 집계하여 Top 10을 추려본 것이다. 이 자료는 사용자 접수와 기타 경로로 접수된 악성코드를 모두 합한 자료이다. 앞서 언급한 것처럼 이번 2월 경우는 대표적인 중국산 악성코드가 후피곤 트로이목마(Win-Trojan/Hupigon) 이외에는 보이지 않는다. 이 트로이목마는 지난 1월에는 동일한 항목에서 5위에 랭크될 만큼 많은 변형이 발견되었던 것이었다. 하지만 이번 달은 Top 10 중에서 7% 비율만 차지할 만큼 변형이 발견되는 비율이 감소하였다. 이 트로이목마뿐 아니라 흔히 볼 수 있는 온라인 게임의 사용자 계정을 훔쳐내는 악성코드들도 역시 순위에서 찾아 볼 수가 없다. 이렇듯 2월은 중국산 악성코드의 비율이 전체적으로 감소한 것을 알 수 있었다. 이에 대한 정확한 원인은 찾기 어렵지만-참고로 2월에는 중국최대 명절인 '춘절'이 있었으며 보통 보름이상 휴식을 즐긴다고 한다- 중국산 신종(변형)악성코드 출현 감소가 전체적으로 2월 악성코드의 수가 현저히 줄어드는데 한 몫을 한 것으로 보인다.

2월 주요 신종(변형) 악성코드

큰 피해가 없이 끝난 나이젬 웜(Win32/Nyxem.worm) 때문에 2월은 매우 바쁘게 시작하였다. 또한 2월말에 등장한 새로운 플랫폼에서 동작하는 악성코드들의 출현으로 윈도우 환경 이외에서 동작하는 악성코드 출현이 부쩍 늘어날 것이라는 우려도 있었다. 국내의 경우 악성코드가 안티 바이러스나 사용자로부터 자신이 제거되지 못하도록 하거나 자신의 생명력을

끊임 없이 유지시키는-사용자 입장에서는 재감염되는 현상- 형태가 있어 많은 고객들이 불편을 호소했던 악성코드가 발견되었다. 또한 은폐기법을 사용하는 상용 DRM 관련 응용 프로그램이나 드라이버가 2종류나 확인되어, 작년 소니 BMG(SONY BMG) 사건과 유사한 사건이 또 다시 발생할 수 있는 잠재적인 위험이 확인되었다.

이슈가 되었던 이번 달의 악성코드 및 주요사건은 다음과 같다.

► 나이젬.95690 웜(Win32/Nyxem.worm.95690)

1월 중순에 보고된 이 악성코드는 매월 3일에 오피스 문서와 몇몇 압축파일의 확장자에 대하여 특정 데이터로 겹쳐 쓰는 증상이 있는데, 감염된 시스템을 3일에 부팅했을 경우 일정 시간이 지나면 겹쳐 쓰는 증상이 발생하는 것이다. 이 웜은 유럽지역에 상당히 확산된 것으로 확인 되었다. 국내에서도 감염문의가 다수보고 되었지만 매스컴과 안티 바이러스 업체들의 사전 주의메일 등 홍보를 통하여 실제 데이터 손실이 발생한 피해보고는 받지 못했다. 최근 악성코드들은 국지적으로 확산되는 경향이 있어 예전만큼 전세계를 동시에 강타하고 있지 못하다. 물론 이런 현상은 제작자가 고의로 의도한 현상일 수도 있으며 국가마다 컴퓨터 사용자들에 대한 보안환경이나 마인드에 따라 달라지기도 한다. 이 나이젬.95690 웜은 1월 중순에 발견되었고 첫 번째 피해를 일으키는 2월 3일 전까지 그 파괴력이나 확산도가 언론을 통해서 여러 번 보도 되었다. 그러므로 사용자들이 대비할 시간이 충분하여 그 피해가 적었다고도 할 수 있지만 그 근본은 국내 확산율이 국외 만큼 높지 않았다는데 그 이유가 있는 것으로 추정하고 있다.

► 토리노 동계 올림픽과 베이글 웜(Win32/Bagle.worm)

베이글 웜(Win32/Bagle.worm) 변형이 또다시 확산 되었다. 이번에는 올림픽이라는 주제를 담은 메시지가 포함된 형태도 발견 되었다. 악성코드가 사회 및 문화적인 이슈를 소재로 하는 것은 이미 오래 되었다. 그러나 2월에 발견된 베이글 웜 변형이 특이한 이유는 바로 감염 컴포넌트의 발송 방법을 변경 했다는 것이다. 이전에 알려진 베이글 트로이목마(Win-Trojan/BagleDownloader)는 메일에 웜을 첨부하지 않았다. 메일에 첨부된 것은 다운로더 증상이 있는 트로이목마였으며 이를 통하여 역시 제작자가 변형을 업로드 한 특정 호스트로부터 내려 받도록 하였다. 그런데 2월에 발견된 베이글 웜 변형은 메일에 웜을 첨부하여 해당 웜이 직접 특정 호스트로부터 다른 증상을 갖는 베이글 트로이목마를 다운로드 하였으며 또한 감염된 시스템은 다른 시스템으로 메일을 발송할 수 있도록 해두었다. 제작자가 어떠한 의도로 이를 변경 했는지 알 수 없지만 이번 변형 역시 국외에서 보고된 지 얼마 되지 않은 시간이 흘러 국내에도 유입 되었다.

► Mac OS X 에서 동작하는 악성코드 출현

올해는 PC와 윈도우 환경 이외의 이 기종에서 활동하는 악성코드 출현을 예상 하고 있었다. 우리는 작년에 이미 휴대용 게임기 트로이목마 소식을 접했기 때문에 이러한 예상은 충분히

할 수가 있었다. 첫 번째 발견된 악성코드는 Mac OS X가 포함된 iChat를 통해서 자신을 전파하며 로컬 드라이브에 존재하는 모든 응용 프로그램의 실행파일을 감염시킨다. 두 번째 발견된 악성코드는 Mac OS X의 블루투스(Bluetooth) OBEX (Generic Object Exchange Profile) Push 취약점을 이용하여 다른 시스템을 감염시킬 수도 있다. 최근 들어 인텔기반의 Mac이 출시되고 또한 기존의 Mac OS X를 x86 머신에서 동작하려는 움직임이 많아졌다. 이러한 결과들로 인하여 근래 Mac과 OS X 에 대한 취약점 발견 소식이 연달아 들려오고 있으며 미공개된 취약점으로 인하여 Mac OS X를 손쉽게 해킹 할 수도 있는 소식이 들려오고 있다. 일반적으로 홈브루(Homebrew)와 해킹(Hacking)은 일맥상통하기 때문에 점점 Mac 관련 보안 이슈가 제기될 것으로 예상된다.

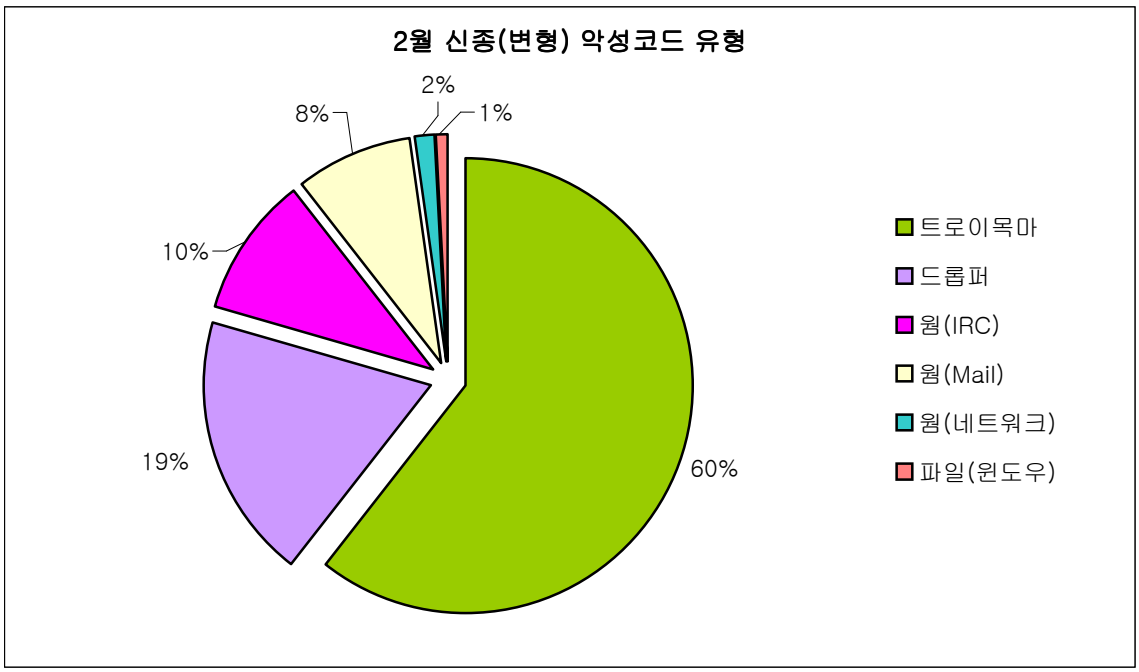
► 자바 플랫폼에서 동작하는 악성코드 출현

J2ME (Java 2 Platform, Micro Edition)는 휴대폰이나 PDA와 같은 모바일 기기에서 자바 프로그래밍 기술을 사용하게 해주는 기술이다. 이번에 출현한 악성코드인 '레드브라우어(RedBrower)' 는 바로 J2ME 기반에서 동작하므로 대부분의 자바 플랫폼을 지원하는 휴대폰과 PDA와 같은 모바일 기기에서 동작이 가능하다. 이 악성코드는 SMS를 발송하는 증상이 있어 휴대폰의 과금을 발생하여 사용자로 하여금 금전적인 피해를 줄 수도 있다. 현재 많은 자바 환경의 응용 프로그램이 제작되고 있어, 이러한 악성코드의 출현은 앞으로도 충분히 예상될 수 있다.

► 은폐기법을 사용하는 국산 DRM 프로그램들

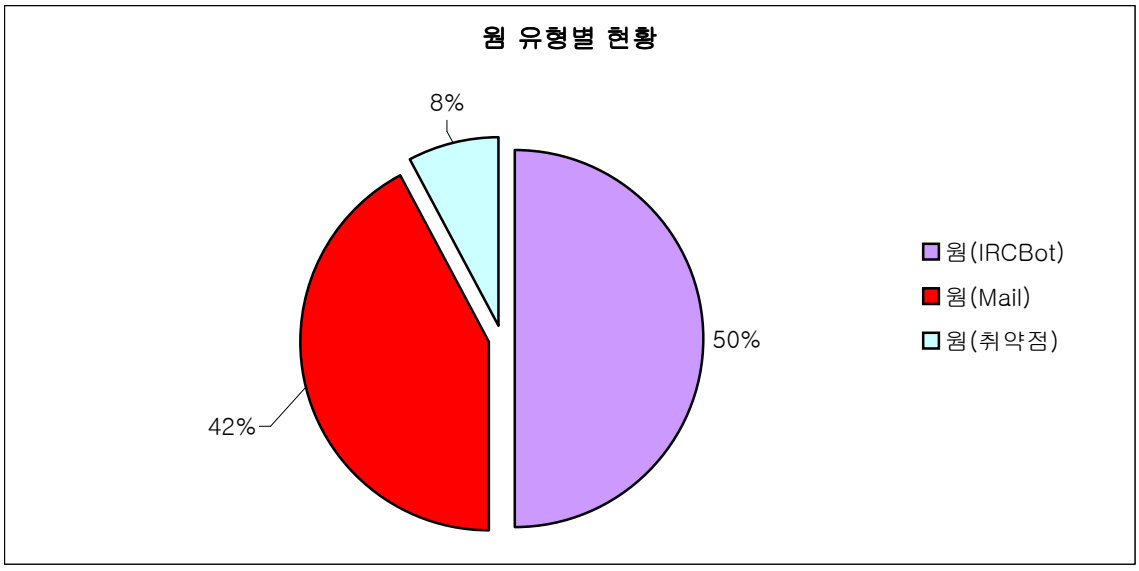
일명 'Stealth by Design'이라고 불리어지는 기법은 사용자나 특정 프로그램으로부터 자신을 은폐하도록 설계된 것을 지칭한다. 보통 이 용어는 은폐형 악성코드에 사용하기 보다는 은폐기법이 적용된 정상 프로그램들을 얘기할 때 곧잘 사용되곤 한다. 작년에 우리는 소니 BMG의 루트킷 사건을 외신을 통해서 접할 수 있었으며, 이런 방식의 정상 프로그램은 증가할 것으로 예상했었다. 그런데 2월에 확인된 Stealth by Design 기법을 사용한 2종의 프로그램들이 발견되었고, 모두 DVD DRM 관련 프로그램과 관련이 깊은 프로그램이었다. 흥미로운 점은 이 프로그램들이 모두 국산이라는 점이다. 이러한 프로그램의 은폐기법은 일반적으로 은폐형 악성코드가 사용하는 커널 SDT(Service Descriptor Table) 후킹 방식이다. 주로 대상 프로세스, 파일, 폴더 또는 레지스트리 키 값을 은폐하도록 하고 DRM 관련 특정 동작을 수행하도록 되어 있었다. 이러한 은폐방식은 소니 BMG 사건처럼 잠재적인 위험요소를 갖고 있는데, 먼저 해당 프로그램이 은폐기능을 사용하고 있는 것에 대한 고객 동의나 사전설명이 일반적으로 없다는 점이다. 그리고 이러한 은폐사용 사실은 악의적인 목적의 사용자로부터 충분히 악용되어 마치 악성코드를 해당 응용 프로그램인 것처럼 위장하여 별다른 노력 없이 은폐된 채로 악성코드가 동작할 수도 있다는 점이다. 다행히 국내에는 아직까지 이러한 사실이 그다지 알려져 있지 않기 때문에 악용되는 사례는 없지만 잠재적인 위험을 갖고 있는 것은 여전히 위험스러운 일임은 틀림 없다.

다음은 이번 달에 발견된 신종 및 변형 악성코드에 대한 유형별 분포이다.



[그림4] 2월 신종 (변형) 악성코드 유형별 현황

[그림4]의 악성코드 유형별 현황을 살펴보면 이번 달에 발견된 악성코드 수는 감소했어도 여전히 트로이목마의 비율이 높은 것을 알 수 있다.



[그림5] 2월 신종 및 변형 웜 유형별 현황

근래 들어서 트로이목마가 그 비율이 높고 또한 그 피해도 개인정보나 금융정보 등을 탈취

하기 때문에 매우 우려되는 악성코드라 할 수 있다. 하지만 여전히 웜도 그 세력과 비율을 일정하게 유지하고 있는데 2월은 이메일로 전파하는 악성코드가 지난달 8%에 비하여 큰 폭으로 증가하였다. 이러한 수치는 여전히 이메일이 효과적인 악성코드의 전파수단이며, 매스메일러 웜 자체에 대한 확산력을 보여주는 단편적인 예라고 할 수 있다.

II. 2월 AhnLab 스파이웨어 동향

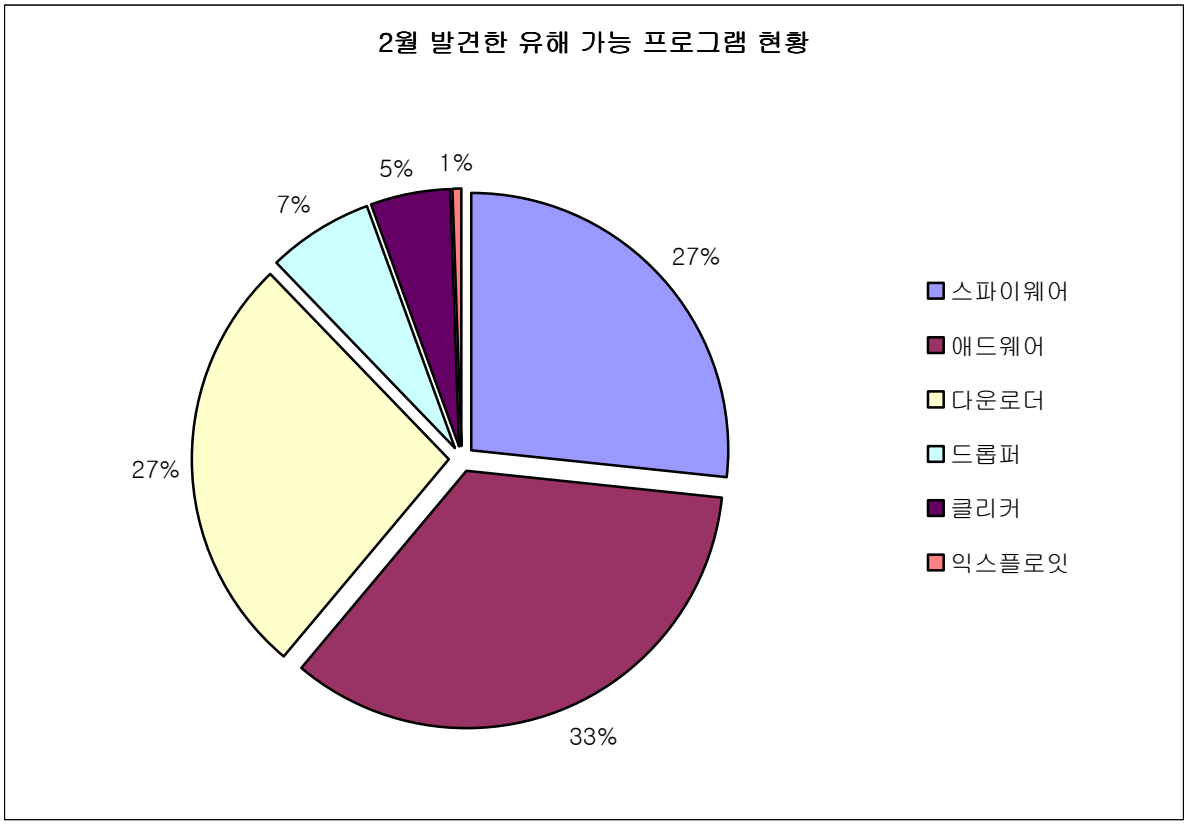
작성자: 장혜윤 연구원(planet@ahnlab.com)

2월 한달 동안 접수된 신종(변형) 유해 가능 프로그램 건수 및 비율은 [표1], [그림1]과 같다.

스파이웨어	애드웨어	다운로더	드롭퍼	클리커	익스플로잇	합계
53	68	53	13	10	1	202

[표1] 2006년 2월 유형별 신종(변형) 유해 가능 프로그램 발견 현황

이번 달에 발견된 신종(변형) 유해 가능 프로그램은 애드웨어가 스파이웨어 보다 많은 수를 차지하고 있다. 이는 1월달과 마찬가지로 허위(Rogue) 안티 스파이웨어의 꾸준한 증가와 바로가기 생성 증상을 가지고 있는 애드웨어 등의 신규 샘플이 많이 접수되었기 때문이다.



[그림1] 2006년 2월 발견된 유해 가능 프로그램 비율

[그림1]에서 보는 바와 같이 유해 가능 프로그램의 반 이상이 애드웨어와 스파이웨어로 구성되어 있음을 확인할 수 있다. 다운로더는 1월보다 증가하여 애드웨어와 같은 비율을 나타내고 있는데, 이는 애드로드 다운로더(Win-Downloader/Adload)가 2006년 초부터 꾸준히

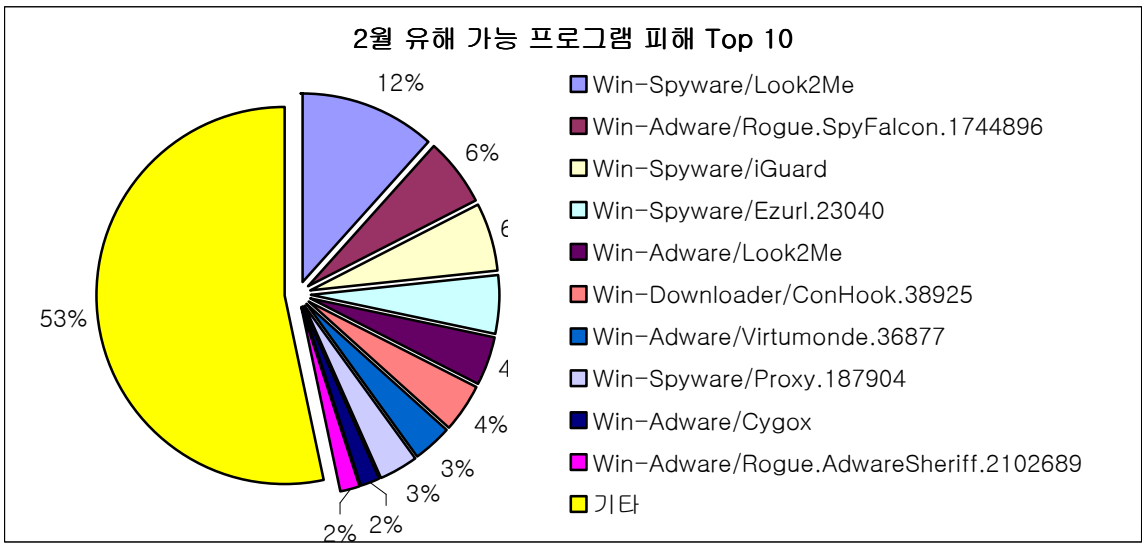
접수되었기 때문이다.

2월에 피해 신고된 유해 가능 프로그램 Top 10을 살펴보면 [표2], [그림2]와 같다.

순위		유해 가능 프로그램명	건수	%
1	1 ↑	Win-Spyware/Look2Me	14	12
2	-	Win-Adware/Rogue.SpyFalcon.1744896	7	6
3	2↑	Win-Spyware/iGuard	7	6
4	5↑	Win-Spyware/Ezurl.23040	6	5
5	2↓	Win-Adware/Look2Me	5	4
6	-	Win-Downloader/ConHook.38925	5	4
7	6↓	Win-Adware/Virtumonde.36877	4	3
8	-	Win-Spyware/Proxy.187904	4	3
9	-	Win-Adware/Cygox	2	2
10	-	Win-Adware/Rogue.AdwareSheriff.2102689	2	2
		기타	64	53
합 계			120	

[표2] 2006년 2월 유해 가능 프로그램 피해 Top 10

1위를 차지한 룩투미(Win-Spyware/Look2Me)는 다운로더에 의해 설치된다. 이 스파이웨어는 DLL 파일의 형태로, CLSID와 파일 이름이 랜덤한 값으로 생성되며 레지스트리 Notify에 등록되어 시스템이 로그온 될 때 Winlogon.exe에 인젝션(injection) 되며, 로그오프 할 때 파일 이름과 Notify에 등록된 정보를 랜덤한 값으로 재생성, 수정한다.

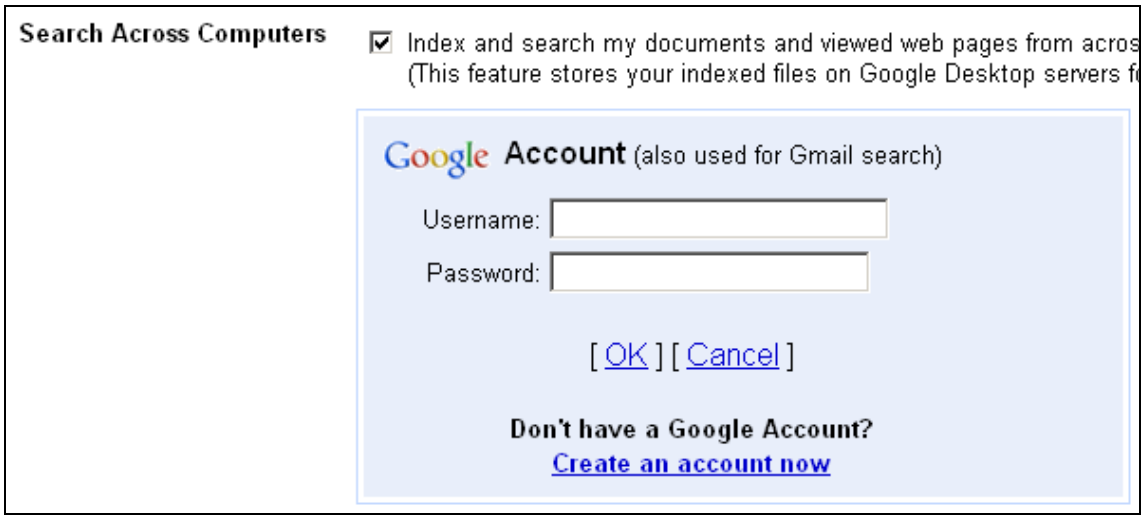


[그림2] 2006년 2월 유해가능 프로그램 피해 Top 10

정보유출 우려로 외면 받는 '구글 데스크톱3'

구글(Google)이 2월초에 공개한 '구글 데스크톱3'에는 여러 대의 컴퓨터 내에 있는 파일을 검색할 수 있는 옵션(Search Across Computeres Option)이 포함되어 있다. 이를 위해 구글의 서버상에서 파일을 최대 1개월간 자동적으로 보존을 하게 되며, 전송 중이거나 구글의 서버상에서 보관 중인 데이터는 암호화 되어 있다고 한다. 이 기능은 초기 설정 상태에서는 해제되어 있지만, 보안 관계자들은 '구글 데스크톱3' 에 대해서 기밀성이 높은 데이터가 유출될 우려가 있다고 경고하고 있다.

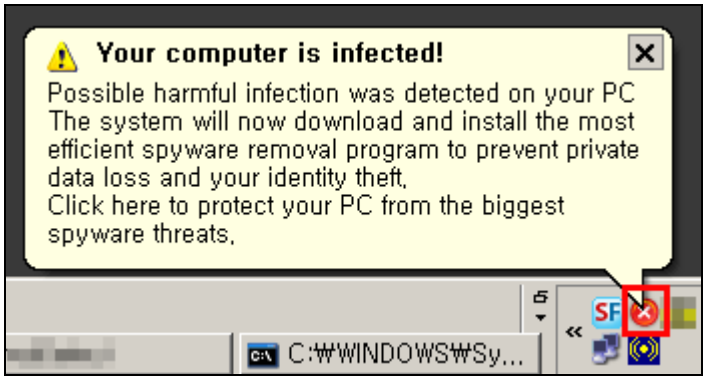
그렇다면 특정 스파이웨어가 기능 설정 상태를 변경하는 게 나오지 않을까 라는 예상이 가능하나, 이 부분은 안심을 해도 좋을 것 같다. 해당 기능을 사용하기 위해서는 구글 계정(Google Account) 정보를 입력해야 가능하기 때문이다.



[그림3] Search Across Computers 옵션

허위(Rogue) 안티 스파이웨어 스파이팔콘(SpyFalcon)

지속적으로 발견되고 있는 허위 안티 스파이웨어 류 중에 최근 가장 많은 샘플이 접수되고, 재감염 문의가 많은 것이 바로 스파이팔콘 스파이웨어 이다. 특징은 트레이아이콘 어플리케이션으로 동작하는 다운로더에 의해 설치되고 사용을 유도하며, 주기적으로 경고 툴 팁을 출력시켜 사용자로 하여금 클릭을 유도한다.



[그림4] 경고메시지 툴팁

트레이아이콘을 클릭하게 되면 설치된 스파이팔콘 스파이웨어를 실행하게 되며, 설치되어 있지 않을 경우 설치 페이지로 이동하여 설치를 유도하므로, 사용자의 주의가 필요하다.

[그림5] 스파이팔콘 스파이웨어 설치 페이지

III. 2월 시큐리티 동향

작성자: 이정형 주임연구원(jungh@ahnlab.com)

2월에 발표된 보안 취약점 동향

2월에는 마이크로소프트사(이하 MS)의 2월 정기 보안 패치가 윈도우 미디어 플레이어 취약점을 포함하여 총 7개 발표되었다. 이중 긴급 보안 공지(MS06-004, MS06-005)가 2건, 중요 보안 공지(MS06-006, MS06-007, MS06-008, MS06-009, MS06-010)가 5건이며 이 정보 중 4건은 OS인 윈도우에 관한 것이고, 1건은 윈도우와 오피스 양쪽에 관련된 것이다. 또한 나머지 2건은 각각 오피스와 윈도우 미디어 플레이어에 대한 보안 패치이다. 2월 보안 패치 중에서 윈도우 미디어 플레이어에 대한 취약점을 간략히 알아보기로 하자.

MS06-005는 윈도우 미디어 플레이어에서 BMP 파일 처리시 오류로 인하여 힙 오버플러우(Heap Overflow)가 발생할 수 있어, 조작된 이미지 파일을 이용하여 원격에서 특정코드를 실행할 수 있게 된다. MS06-006은 윈도우 미디어 플레이어 플러그인을 사용하는 IE를 제외한 파이어폭스(Firefox)나 오페라(Opera) 브라우저 등에서 EMBED 태그의 SRC 속성에 긴 문자열이 포함되면 버퍼 오버플러우(Buffer Overflow)가 발생되며, 역시 원격에서 특정코드의 실행이 가능하다.
요즈음은 취약점이 포함된 악성 웹페이지를 통해 악성코드 유포가 많이 이용되고 있는데, 윈도우 미디어 플레이어에 대한 취약점 역시 악용될 소지가 크다. 더구나 이 취약점에 대한 익스플로잇이 이미 공개되어 있어 이를 이용한 악성코드 출현가능성이 높으므로, 사용자들의 즉각적인 패치가 필요하다.

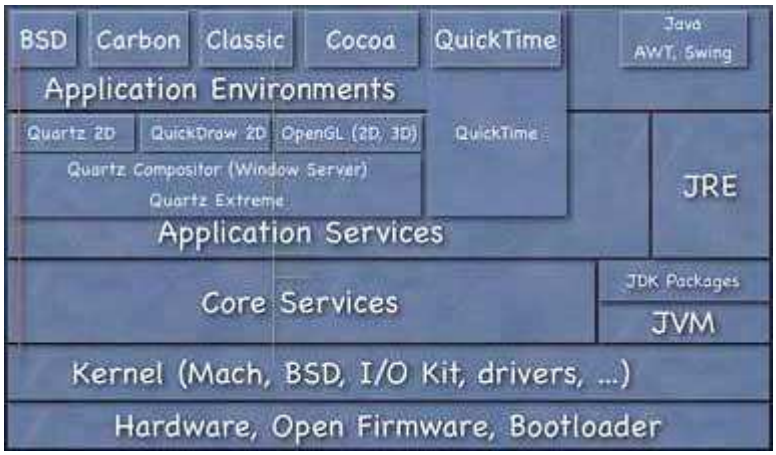
마이크로소프트사의 2월 주요 보안 패치 현황

위험등급	취약점	공격코드 유/무
HIGH	Windows Media Player의 취약점으로 인한 원격 코드 실행 문제점(MS06-005)	유
HIGH	TCP/IP의 취약점(IGMP)으로 인한 서비스 거부 문제점(MS06-007)	무
HIGH	웹 클라이언트 서비스의 취약점으로 인한 원격 코드 실행 문제점(MS06-008)	무 / (계정필요)
MIDDLE	한국어 IME의 취약점으로 인한 권한 상승 문제점(MS06-009)	공격코드 필요없음 (계정필요)

Mac OS X에 대한 보안 위협(악성코드 유포)

애플(Apple) 컴퓨터 사는 PowerPC칩에서 동작하는 자사의 운영체제인 Mac OS 9를 가지고 있었다. 그러나 2001년도에 유닉스에 기반한 새로운 운영체제를 발표하게 되었는데, 이것이

Mac OS X이다. 현재에는 플랫폼을 확장하여, Intel x86 칩에서도 동작을 할 수 있으며, 클라이언트 버전과 서버 버전의 두 종류를 가지고 있다. 깔끔한 디자인과 사용하기 쉬운 인터페이스로 인해, 앞으로 사용자 수가 많이 증가할 것으로 예상된다.
Mac OS X는 기본적으로 PowerPC 칩(G3, G4, G5등) 및 Intel 칩(x86)에서 동작하며, Mach 커널과 BSD 커널기반의 유닉스 호환 운영체제로써, 상위계층에 GUI와 관련된 레이어(Layer)들이 작동하고 있다. Mac OS X의 구조는 아래와 같다.



[그림1] Mac OS X 구조(출처: www.kernelthread.com)

2월에는 Mac OS X에서 동작하는 메신저 프로그램인 iChat으로 유포되는 첫 트로이목마가 발견되었다는 소식과 함께, 사파리(Safari) 웹 브라우저의 Zip관련 취약점이 공개된 일이 있었다.

Mac OS X는 대부분의 유닉스 프로그램과 명령어들을 사용할 수 있기 때문에 악성 프로그램 제작이 비교적 쉽다. 일례로 쉘 스크립트를 이용하여 특정사이트의 특정파일을 받는 트로이목마나 파일삭제가 가능한 프로그램을 만들 수도 있어 앞으로 다양한 종류의 악성코드가 출현할 것으로 예상된다. 이런 악성코드 감염의 문제는 취약점이나 특정 파일을 다운로드 하게 되어 권한을 빼앗기게 된다. 이에 대한 해결책은 주기적으로 애플사의 홈페이지에 접속하여 최신 보안 패치를 받아 적용하는 것이다. 2월에 나온 취약점에 대한 패치는 아래 사이트에서 받을 수 있다.

http://docs.info.apple.com/article.html?artnum=303382

게임사이트 명의도용 사건

2월에는 국내 유명 게임인 리니지의 사용자 계정에 대한 개인 명의도용 사건이 발생하여 사회적으로 큰 문제가 되고 있다. 현재 명의도용 신고가 15만 건이 넘고 있고, 명의도용을 당한 개인들로부터 집단 손해배상 움직임마저 일고 있다. 이 문제는 주민등록번호 등의 개인정보를 획득한 악의적인 사람들이 돈과 관련된 게임의 아이템 획득에 사용이 되는 것으로

보이며, 다른 사이트 역시 명의도용 건이 많이 있을 것으로 추정된다.
이에 대한 해결책은 해당 사이트 가입 시에, 인증을 주민등록번호로 하지 않고 핸드폰 인증 또는 공인인증서 등을 이용하는 것이다. 또한 개인정보를 필요로 하는 사이트에서는 주민등록번호 등의 개인정보를 데이터베이스에 저장 시 암호화 해서 저장을 해야 하며 개인정보가 들어가 있는 문서(이력서, 업무문서 등)의 관리에 신중을 기하는 것이 필요하다.

연이은 국내 웹사이트 해킹피해와 게임사이트 대규모 명의도용은 리니지핵 트로이목마(Win-Trojan/LineageHack)을 제작하는 중국 해커와 관련이 있을 것으로 보인다.

Ⅳ. 2월 세계 악성코드 동향

2006년 2월 전 세계적으로 가장 많이 확산된 악성코드는 넷스카이 웜이고 이러한 현상은 이전과 크게 차이가 없다. 이와 함께 나이젬 웜과 베이글 웜 또한 지속적으로 확산되고 있는 것으로 보인다.

매스메일러의 확산 이외에 특이할 점은 트로이목마나 애드웨어 등 직, 간접적으로 금전적인 이익을 노리는 악성코드가 점점 증가하는 추세에 있다는 것이다. 중국의 경우 확산 통계의 상위권을 차지하고 있는 대부분의 악성코드가 다운로더나 에이전트와 같은 개인 정보 유출 기능을 가지고 있는 경우가 많으며, 해외에서도 뱅커(Win-Trojan/Banker)와 같은 계정 정보 획득을 위한 악성코드들의 감염 피해가 증가하고 있는 것으로 보고되고 있다. 이러한 현상은 국내에서도 크게 다르지 않은데 최근 발생하고 있는 게임 계정을 노린 악성코드의 등장은 이러한 현상의 대표적인 예이다.

국가별로 악성코드 제작자들이 사용자들에게서 획득하고자 하는 정보의 차이는 있으나, 특정 사이트의 계정과 패스워드 정보 같이 공격 대상이 명확해지고 있는 점이나 정보를 획득하기 위한 기법이 점점 다양해지고 있는 점은 공통적으로 나타나고 있는 현상이다. 이는 지금까지의 일반적인 트로이목마와는 큰 차이가 있기 때문에 이들의 변화를 주의 깊게 관찰 할 필요가 있다.

(1) 일본의 악성코드 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

최근 일본에서는 P2P 파일 공유 프로그램인 위니(Winny)를 이용한 악성코드인 안티니 웜(Win32/Antinny.worm)으로 인한 정보 유출이 수 차례 발생하여 언론에 기사화 되었다. 유출된 정보 중에는 수 천명에 달하는 고객 정보나 일본 자위대의 기밀 사항이 기록된 서류도 포함되어 있는 것으로 알려졌다.

기업은 물론 개인의 작업 환경에 대한 컴퓨터의 의존도가 점점 높아지고 있고 PC에 저장된 데이터들의 중요도 또한 높아질 수 밖에 없는 현재의 상황에서 데이터의 유출로 인한 피해는 조직과 사용자를 심각한 위기 상황에 처하게 만들 수 있다. 최근 일본에서 발생한 P2P 웜으로 인한 정보 유출 사건들은 이러한 위기 상황에 대한 단적인 예라고 할 수 있다.

위니나 카자(Kazza) 등 P2P 프로그램을 악용하는 웜들은 PC에 저장된 파일들을 타인에게 유출시키는 기능을 가지고 있는 경우가 대부분이기 때문에 바이러스 감염으로 인한 데이터의 훼손보다 훨씬 더 심각한 피해를 유발함에도 불구하고 대부분의 사용자들은 이러한 상황에 대한 주의가 부족하다.

P2P 웜에 의한 피해 예방을 위해 기업의 경우 해당 프로그램의 설치나 외부로의 통신을 막는 것이 바람직할 것이다. 개인 사용자는 알 수 없는 파일에 대한 다운로드나 실행을 하지 않도록 하는 것이 필요하다. 백신 소프트웨어나 방화벽 프로그램을 설치하는 것도 정보 유출을 방지하기 위한 방법이 될 수 있다.

일본 악성코드 동향

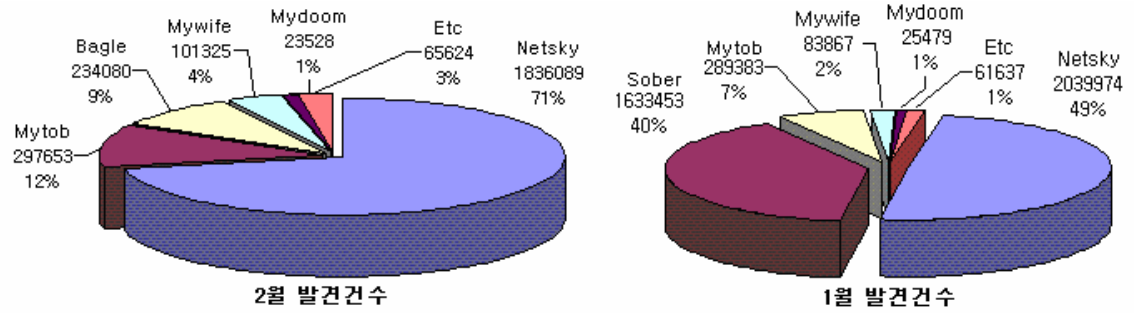
2006년 2월 한 달 동안 일본에서 가장 많이 유행한 악성코드는 넷스카이 웜(Win32/Netsky.worm)으로 이는 전월과 동일하다.

[표1]은 일본의 IPA에서 발표한 자료 중 악성코드 종류 별 감염 신고 현황에 대한 통계이다. 넷스카이 웜의 피해 신고 사례는 1,004건으로 전월과 비교해서 크게 차이가 없다.

Window/Dos Virus	금월피해 전월피해	Macro Virus	금월피해 전월피해	Script Virus	금월피해 전월피해
Win32/Netsky	1,004	Xm/Laroux	11	VBS/Redlof	42
	1,040		13		42
Win32/Mytob	526	W97M/X97M/P97 M/Tristate	7	VBS/Soraci	27
	630		2		2
Win32/Bagle	372	WM/Cap	3	VBS/Loveletter	6
	313		3		1
Win32/Mywife	310	W97M/Lexar	2	Wscript/ Fortnight	5
	162				7
Win32/Mydoom	251	W97M/Marker	2	VBS/Kakworm	5
	242				3
Win32/Lovgate	219	X97M/Divi	4	VBS/Internal	2
	212		1		2

[표1] 악성코드 피해 신고 현황

특이할 점은 소버 웜(Win32/Sober.worm)의 피해 건수가 전월에 이어 이번 달에도 현저하게 줄어들고 있는 것이다. [그림1]은 악성코드 발견 횟수에 대한 통계를 나타낸 것이다. 1월에 비해 소버 웜의 확산도가 현저하게 떨어진 것을 볼 수 있다.



[그림1] 악성코드 발견 통계(출처: 일본 IPA)

베이글 웜(Win32/Bagle.worm)과 나이젬 웜(Win32/Nyzem.worm, Win32/Mywife.worm)의 피해가 증가한 것도 주목할 사항이다. 베이글 웜의 경우 최근 새로운 변형들이 여러 가지 형태로 발견되고 있으나, 나이젬 웜은 최근 새로운 변형이 발견되지 않고 있는 상황에서 감염

피해 건수가 증가하고 있는 점이 이례적이다.

악성코드의 감염 경로 별 통계

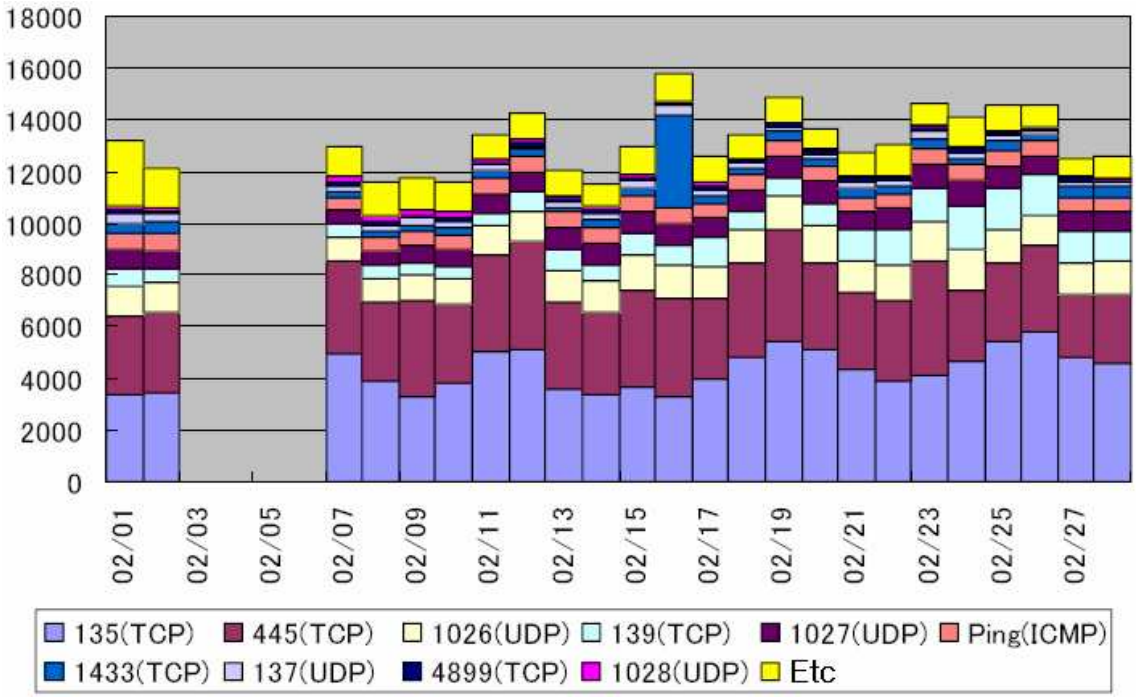
[표2]는 악성코드의 감염 경로 별 통계를 나타낸 것이다. 전월과 마찬가지로 메일을 이용해서 전파되는 악성코드가 가장 많은 양을 차지하고 있는 것을 알 수 있다. 네트워크를 이용한 악성코드에 감염 피해를 당하는 사례 또한 이전에 비해 증가하고 있는 것을 볼 수 있는데 작년의 수치와 비교하여 보았을 때 현재의 감염 피해 건수는 매우 많은 증가율을 기록하고 있으며 이러한 증가 수치는 당분간 지속될 것으로 생각된다.

감염경로	피해 건수					
	2006년 1월		2006년 1월		2005년 2월	
메일	4,207	97.9%	4,385	97.9%	4,111	99.1%
외부의 모체	0	0.0%	0	0.1%	0	0.0%
다운로드	3	0.1%	4	0.1%	0	0.0%
네트워크	112	2.6%	109	2.0%	39	0.9%
기타	2	0.0%	1	0.0%	0	0.0%
합계	4,999	4,999	4,999		4,880	

[표2] 악성코드 감염 경로 통계(출처: 일본 IPA)

일본 네트워크 트래픽 현황

[그림2]는 일본의 네트워크 트래픽 현황을 그래프로 나타낸 것이다. 그래프에서 보는 것처럼 TCP 135 포트와 TCP 445 포트의 트래픽이 매우 많은 것을 알 수 있다. 해당 포트들은 윈도우 OS에서 사용되는 포트들이지만 아이알씨봇(IRCBot)과 같은 악성코드들에서도 보안 취약점을 공격하기 위해 악용되므로 주의가 필요하다.



[그림2] 일본의 네트워크 트래픽 현황(출처: 일본 IPA)

[그림2]에서 특이한 사항은 2월 16일 TCP 1433 포트의 트래픽이 급격하게 증가한 것이다. 해당 포트는 MS사의 SQL 서버에서 사용하는 포트이다. IPA에서는 이러한 트래픽 증가의 원인으로 중국을 발신지로 하는 IP에서의 SQL 서버로의 공격이 발생한 것이라고 파악하고 있으며 IPA의 보고서에서도 실제로 해당일에 중국에서의 트래픽이 급격하게 증가한 것을 확인할 수 있었다.

(2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

2006년 2월 중국 악성코드는 지난 동향과 유사하게 트로이목마 류가 악성코드 순위의 대부분을 차지하고 있으며 악성코드의 형태도 세분화되고 있는 것으로 분석된다. 특히 기존의 단독 실행형태에서 다른 정상 프로세스에 자신의 코드 또는 DLL을 주입시키는 방식이 특히 많이 발견되고 있으며 이외에도 네트워크를 통해 다른 악성코드 또는 애드웨어를 다운로드하는 다운로더 형태의 악성코드도 다량 발견된 것으로 보고 되었다. 광고 팝업창을 생성하는 애드웨어도 다시 순위권에 진입한 것으로 미루어 중국 내에서 다시 광고성 프로그램이 증가하고 있는 것으로 추정된다. 이러한 특징들이 이번 2월 중국 악성코드 동향의 새로운 흐름으로 분석된다.

중국의 악성코드 TOP 5

순위 변화	순위	라이징(Rising)
New	1	Trojan.DL.Agent
↑ 2	2	Trojan.DL.Small
-	3	Backdoor.Gpigeon
↓ 2	4	Trojan.PSW.LMir
New	5	AdWare.Hbang

[표1] 2006년 2월 라이징(Rising) 악성코드 TOP 5

'-' - 순위변동 없음, 'New' - 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

[표1]은 중국 로컬 백신 업체인 라이징(Rising)의 2006년 2월 악성코드 TOP 5 순위이다. 이번 2월 라이징의 순위에는 Backdoor.Agent(V3 진단명 Win-Trojan/Agent)이 순위권 밖으로 밀려나고 그 대신 Trojan.DL.Agent(V3 진단명 Win-Trojan/Agent)이 새롭게 1위를 차지하였다. 라이징의 보고에 따르면 Trojan.DL.Agent는 현재까지 20개의 변형들이 발견되었으며 해당 악성코드는 단독으로 실행 가능한 파일이 아니라 DLL 형태로 자신의 코드를 다른 정상 프로세스에 주입하는 코드 인젝션(Injection)형태이다.

2위에는 두계단 상승한 Trojan.DL.Small(V3 진단명 Win-Trojan/Xema)이며 3위에는 1월과 동일한 순위를 유지하고 있는 Backdoor.Gpigeon(V3 진단명 Win-Trojan/GrayBird 또는 Win-Trojan/Hupigon)이 차지하고 있다. 4위에는 두계단 하락한 Trojan.PSW.LMir(V3 진단명 Win-Trojan/LmirHack)이 차지하고 있다. 새롭게 5위로 악성코드 TOP 5에 진입한 AdWare.Hbang은 광고성 팝업창을 생성하기 위해서 제작된 애드웨어이다. 이 애드웨어 역시 DLL 형태로 자신을 정상 인터넷 익스플로러 프로세스에 스레드로 인젝션시킨 후 주기적으로 광고성 팝업창을 생성시킨다.

순위 변화	순위	강민(JiangMin)
New	1	TrojanDownloader.Delf.sn
New	2	TrojanSpy.Agent.jp
New	3	TrojanDownloader.Delf.sy
↓ 3	4	TrojanDownloader.QQHelper.f
New	5	TrojanSpy.Agent.jr

[표2] 2006년 2월 강민(JiangMin) 악성코드 TOP 5

'-' - 순위변동 없음, 'New' - 순위에 새로 진입, '↑'- 순위 상승, '↓' - 순위 하락

[표2]는 강민(JiangMin)의 2006년 2월 악성코드 TOP 5 순위이다. 강민의 악성코드 TOP 5 역시 모두 트로이목마 형태의 악성코드들이 차지하고 있으며, 특히 다른 악성코드 또는 애드웨어를 다운로드하는 다운로더 형태의 트로이목마가 많이 발견된 것으로 보고되었다. 그리고 순위에 포함된 대부분의 악성코드가 이번 2월에 새롭게 발견된 악성코드들로 이루어져 있다. 이번 2월 악성코드 TOP 5의 1위에는 TrojanDownloader.Delf.sn(V3 진단명 Win-Trojan/Downloader)가 차지하고 있으며 2위에는 TrojanSpy.Agent.jp(V3 진단명 Win-Trojan/ Agent)가 그 뒤를 잇고 있다. 3위 역시 이번 2월 새로 순위권에 포함된 다운로더 형태의 트로이목마인 TrojanDownloader.Delf.sy(V3 진단명 Win-Trojan/Downloader)가 차지하고 있으며 4위에는 지난 달 1위에서 세 계단 하락한 TrojanDownloader.QQHelper.f(V3 진단명 Win-Trojan/QQHelper)가 차지하고 있다. 마지막으로 5위에는 TrojanSpy.Agent.jr(V3 진단명 Win-Trojan/ Agent)가 차지하고 있다

주간 악성코드 순위

순위	1주	2주	3주
1	Trojan.DL.Agent	Trojan.DL.Agent	Trojan.DL.Agent
2	Trojan.DL.Small	Trojan.DL.Small	Trojan.DL.Small
3	Backdoor.Gpigeon	Backdoor.Gpigeon	Backdoor.Gpigeon
4	Trojan.PSW.LMir	Trojan.PSW.LMir	Trojan.PSW.LMir
5	Dropper.Agent	AdWare.Hbang	AdWare.Hbang

[표3] 2006년 2월 라이징(Rising) 주간 악성코드 순위

라이징의 주간 악성코드 순위에는 큰 변동 없이 1주차부터 3주차까지 유지되고 있으나 2주차에서 애드웨어인 AdWare.Hbang가 5위로 순위권에 진입하고 드롭퍼 형태인 Dropper.Agent(V3 진단명 Dropper/Agent)가 순위권 밖으로 밀려난 것으로 보고되었다.

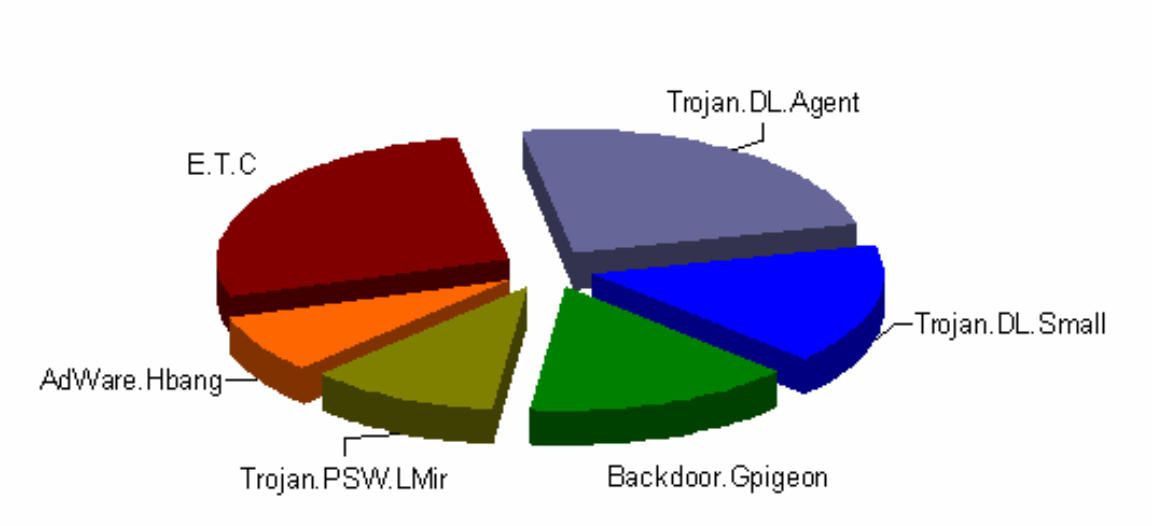
순위	1주	2주	3주

1	TrojanDownloader.Delf.sn	TrojanDownloader.Delf.sn	TrojanDownloader.Delf.sn
2	TrojanDownloader.Delf.sy	TrojanDownloader.QQHelper.f	TrojanSpy.Agent.jp
3	TrojanDownloader.QQHelper.f	TrojanDownloader.Delf.sy	TrojanSpy.Agent.jr
4	TrojanSpy.Agent.ex	TrojanDownloader.QQHelper.x	Adware/Downloader.QQHelper.f
5	TrojanDownloader.Agent.wu	TrojanSpy.Agent.ex	TrojanSpy.Agent.ex

[표 4] 2006년 2월 강민(JiangMin) 주간 악성코드 순위

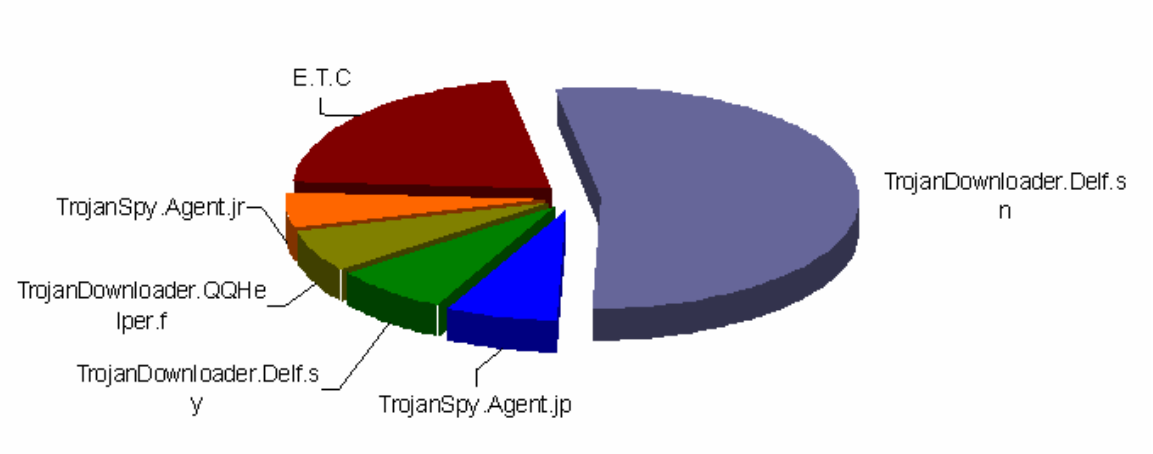
강민의 주간 악성코드 순위는 라이징의 순위와 달리 악성코드간의 순위 변화가 큰 것으로 보고 되었다. 1위를 차지한 TrojanDownloader.Delf.sn를 제외한 나머지 순위는 주간 순위 변화가 다양하였다. 특히 TrojanDownloader.QQHelper.f는 2주차에서 새로운 변형인 TrojanDownloader.QQHelper.x(V3 진단명 Win-Trojan/QQHelper)까지 4위로 순위권에 진입하였으나 3주차에서는 이 두 악성코드 모두 하락세를 보여주었다. 3주차에서는 전체 악성코드 TOP 5에서 2위를 차지한 TrojanSpy.Agent.jp가 2위를 차지하며 비교적 많은 확산을 보였던 것으로 분석된다.

악성코드 분포



[그림1] 2006년 02월 라이징(Rising)의 악성코드 분포

[그림1]을 살펴보면 TOP 5에 포함된 악성코드 간의 분포율은 큰 차이를 보이지 않고 있다. Backdoor.Gpigeon는 악성코드 TOP 5에서는 순위 변동이 없었지만 분포면에서는 2월에 14%를 차지하며 1월보다 1% 증가하였다. 그리고 두단계 하락한 Trojan.PSW.LMir은 14%에서 10%로 감소하였다. 그 외에 순위에 새로 진입한 AdWare.Hbang은 7%를 차지하고 있다. TOP5에 포함된 악성코드 이외에도 전체 분포에서 악성코드 TOP 5에 포함되지 않은 기타 악성코드가 전체 분포의 30%를 차지하고 있어 여러 악성코드들이 활발하게 활동하고 있음을 알 수 있다.



[그림2] 2006년 02월 강민(JiangMin)의 악성코드 분포

2월 강민의 악성코드 분포에서는 1위를 차지한 TrojanDownloader.Delf.sn가 전체의 절반을 조금 넘는 53%를 차지하고 있어 라이징과는 상반된 악성코드 분포를 보여주고 있다. 그리고 1월 악성코드 분포에서는 49%를 차지하던 기타 악성코드들은 이번 2월에서는 22%를 차지하며 27%의 큰 감소를 보여주었다.

(3) 세계의 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

2006년 2월도 전통적인 매스메일러 웜들이 피해 집계의 대부분을 차지하고 있다. 다만 유럽 지역에서 애드웨어 성 트로이목마가 대량의 메일로 배포되어 순위권에 든 점이 흥미롭다.

영국 소포스사의 통계[1]에 따르면 1위는 넷스카이 웜 변형이며 2위는 나이젬 웜 변형이다. 나머지 악성코드도 순위가 조금 차이가 있을 뿐 큰 변화는 없다. 하지만, Troj/Clagger-G라는 트로이목마가 8위로 처음 순위권에 진입했다. 자체 전파력이 없는 트로이목마 특성상 트로이목마가 순위권에 들어오는 것은 흔하지 않은 일이다. 해당 트로이목마는 메일로 전파되었으며 유럽 지역에서 매우 다량의 메일이 발송된 것으로 추정된다. 하지만, 이런 트로이목마는 자기 전파 능력이 없으므로 제작자가 메일 형태로 배포하지 않으면 다음 달에는 순위에서 빠질 가능성이 높다.

캐스퍼스키 연구소의 2월 통계[2]에 따르면 마이톱 웜 변형과 러브게이트 웜 변형이 1, 2위를 차지하고 있다. 러브게이트 웜의 피해 집계는 유독 캐스퍼스키 연구소에만 두드러지는데, 제작국의 인접국인 러시아에서 보고가 많은 것이 통계에 영향을 미친 것이 아닐까 하는 추정을 해본다. 2월에 등장한 베이글 웜 변형(Email-Worm.Win32.Bagle.fi)이 6위로 순위권에 진입했다. 피해 신고나 메일에 따른 집계가 아닌 사용자들이 온라인 스캐너를 통해 검사한 결과에 따른 순위[3]에 따르면 1위는 베이글 웜 변형이며 다른 통계에서는 전혀 집계되지 않은 뱅커와 반코스 변형들이 2, 3, 4위를 차지하고 있다. 이들 트로이목마는 브라질의 특정 은행 계정과 비밀번호를 탈취하기 위해 제작되었다. 그 외에 실제 감염 통계에서는 웜보다 트로이목마가 많았다.

피해 통계 방법에 따라 악성코드 피해 동향은 사용자의 체감과는 달라 질 수 있다. 물론 온라인 스캐너의 결과도 특정 지역이나 국가에서 온라인 스캐너 서비스 이용 비율이 높다면 특정 지역에서 활동하는 악성코드의 감염 비율이 더 높게 나타날 수 있다.

[1] http://www.sophos.com/pressoffice/news/articles/2006/03/toptenfeb06.html
[2] http://www.viruslist.com/en/analysis?pubid=181064361
[3] http://www.viruslist.com/en/analysis?pubid=181202144

V. 이달의 ASEC 컬럼 - 중국 언더그라운드 해커의 변화

작성자: 장영준 연구원(zhang95@ahnlab.com)

얼마 전 한국의 대표적인 온라인 게임인 리니지를 즐기는 사용자들의 개인 정보가 대규모로 도용되는 사건이 발생하였다. 이러한 대규모의 개인 정보 도용 사건은 악의적인 중국인 해커들에 의해 발생한 사건으로 알려져 그 충격을 더하고 있다. 게다가 개인 정보 도용은 리니지 게임 사용자들뿐 아니라 피망, 한게임 그리고 마비노기 등 한국에서 제작되어 널리 알려진 대부분의 온라인 게임으로 번져 나가고 있어 온라인 게임을 즐기는 유저들의 우려를 더해 가고 있는 실정이다.

이러한 중국발 해킹으로 국내에서도 서서히 중국 언더그라운드 해커들에 대한 관심이 증가하고 있다. 중국 언더그라운드 해커[1]들은 미국 또는 유럽과 달리 1990년대 중반부터 중국 특유의 정치적인 사상과 컴퓨터 시스템 그리고 컴퓨터 네트워킹에 대한 연구가 합쳐져 다른 나라에서 볼 수 없는 독특한 언더그라운드 해커 문화들을 형성하게 되었다. 이러한 고유한 문화를 가진 중국의 언더그라운드 해커들은 어떠한 변화를 겪으며 현재까지 흘러 왔는지 살펴보도록 하자.

컴퓨터 네트워크의 등장

1994년에서 1996년은 중국 컴퓨터 네트워크 산업의 토대가 이루어지기 시작한 시기이다. 그러나 컴퓨터 네트워크라는 개념자체가 전문적인 연구기관이나 연구인력에 의해서 만들어진 연구자료 등에서만 등장하고 있는 실정이었고 컴퓨터 네트워크를 사용하는 계층도 대부분 연구기관의 연구인력에 의해서였다. 이 시기에는 해커라는 단어 자체가 존재하지 않았으며 컴퓨터를 오락용 게임기로 생각하는 사람들이 대부분이었다. 그리고 소수의 컴퓨터 사용자들 역시 도스(DOS)에서 실행되는 프로그램이나 개인 컴퓨터(PC)용 게임 프로그램을 복제하여 보관하는 정도였다. 이 시기에는 해커라기 보다는 일반 프로그램의 복제판을 제작하는 사람들이 많았으며 더 많은 프로그램을 복제하여 용량이 얼마 되지 않는 하드디스크(HDD)에 보관하는 것이 큰 유행이었다. 그 중에서도 최신 유행하는 외국 프로그램을 복사하는 것이 가장 큰 인기를 끌었었다. 이 시기에 활발한 활동을 한 대부분의 사람들이 후일 중국 소프트웨어와 네트워크 개발 산업에 많은 도움을 준 인물들로 성장하게 되었다. 이러한 면에서 본다면 이들이 곧 초기 중국 언더그라운드 해커들의 기원이라고 볼 수 있다.

언더그라운드 해커의 등장과 해커 조직의 결성

1997년에서 1999년까지가 중국 언더그라운드 해커들에 있어서 많은 변화와 발전을 이룬 해라고 볼 수 있다. 그리고 현재 알려진 중국 언더그라운드의 고급 기술을 가지고 있는 해커들

[1] 중국어로 해커는 흑객(黑客)로 표기하며 Hacker의 영어 발음에서 유래 되었다.

대부분이 이 시기에 가장 많이 등장하였다. 이 시기의 중국 언더그라운드 해커들 사이에서 가장 발달된 기술은 특정 웹 사이트나 전자 메일 주소로 다량의 메일을 전송하는 메일폭탄(Mail Bomb)이 알려져 있었다. 그러나 이 시기 대부분의 해킹 기술은 스스로 개발한 프로그램이 아니라 외국에서 개발된 프로그램을 이용하는 수준이었다. 그리고 아직까지는 중국 언더그라운드 해커들이 스스로 개발한 해킹 프로그램은 찾아 볼 수 없었으며 미국에서와 같은 독특한 언더그라운드 해커 조직이나 고유한 해커 문화도 존재하지 않았다. 1998년에 이르러서야 중국 언더그라운드 해커들에 의해 개발된 최초의 트로이목마인 넷스파이(Win-Trojan/NetSpy)가 제작된다. 그리고 이와 함께 PP, 천행과 사조령 등 고급 해킹 기술을 가진 고급 해커들이 등장하기 시작하였으며 서서히 해커들 스스로 개발한 트로이목마나 해킹 프로그램들이 발견되기 시작하였다. 이러한 악성코드의 빠른 발전에 비해서 아직 중국 내에서는 안티 바이러스(Anti-Virus)에 대한 기술 발전은 미약한 상태였으며 자체적인 백신 개발 기술이 없는 실정이었다.

1997년을 즈음하여 지금은 해체된 중국 최초의 언더그라운드 해커 조직인 녹색병단(綠色兵單)이 굿웰(Goodwell)에 의해서 조직된다. 굿웰은 네트워크 해킹을 중심으로 최초의 해커 조직인 녹색병단(綠色兵單)을 조직하고 중국 언더그라운드에서 개인으로 활동하던 고급해커들을 흡수하는데 큰 기여를 하게 된다.

1998년 7월에서 8월, 인도네시아에서 발생한 대규모의 폭동으로 인해 인도네시아에 진출해 있는 중국 화교들이 커다란 피해를 입는 사건이 발생하게 된다. 이러한 인도네시아 화교들의 피해가 중국 내부에 알려지자 아이알씨(IRC) 채팅방에는 대규모 중국 언더그라운드 해커 모임이 열리게 된다. 이 모임에서 중국 언더그라운드 해커들은 인도네시아 정부 웹 사이트에 대한 대규모 해킹 공격을 결정하게 되고 이 공격은 이후 점점 더 많은 해커들이 참가하게 되었다. 이 해커 모임으로 인해 고급 해킹 기술을 갖춘 몇몇 고급 해커들을 중심으로 '중국해커긴급회의중심'이라는 조직을 결성하여 인도네시아 정부에 대한 기술적이며 체계적인 공격을 지휘하게 된다. 이 모임은 중국 언더그라운드 해커들 사이에서는 고유한 해커 문화를 만들어 나갈 수 있는 조직을 결성하는 계기가 되었으며 이 후 이 조직은 최대의 중국 언더그라운드 해커 조직이라고 알려진 홍커(红客)를 조직하게 되는 밑바탕이 된다.

1999년 5월에 이르러 중국 최대의 언더그라운드 해커 조직과 웹 사이트가 등장하게 된다. 이들은 스스로를 '중국홍커(红客)조국단결전선' 이라고 부르며 다분히 정치적인 사상을 가지고 있는 모습을 보이게 된다. 그리고 두달 후인 7월, 이들은 자신들의 정식명칭을 '중국홍커(红客)조국통일전선'으로 바꾸며 해킹 기술의 연구라는 기반 위에 애국주의적인 사상을 주된 이념으로 삼는 고유한 문화를 이루게 된다. 홍커(红客)의 웹 사이트에는 애국주의적인 글과 모택동이 젊은 시절 남긴 사회주의 사상의 글들이 주를 이루고 있다. 홍커(红客)는 이 후 대만에서 중국과 대만은 별개의 나라라는 양국화론이 대두 되자 대만에서 제작된 소프트웨어에 트로이목마를 설치해 배포하고 대만 정부 웹 사이트에 대한 해킹 공격을 하는 등 그들이

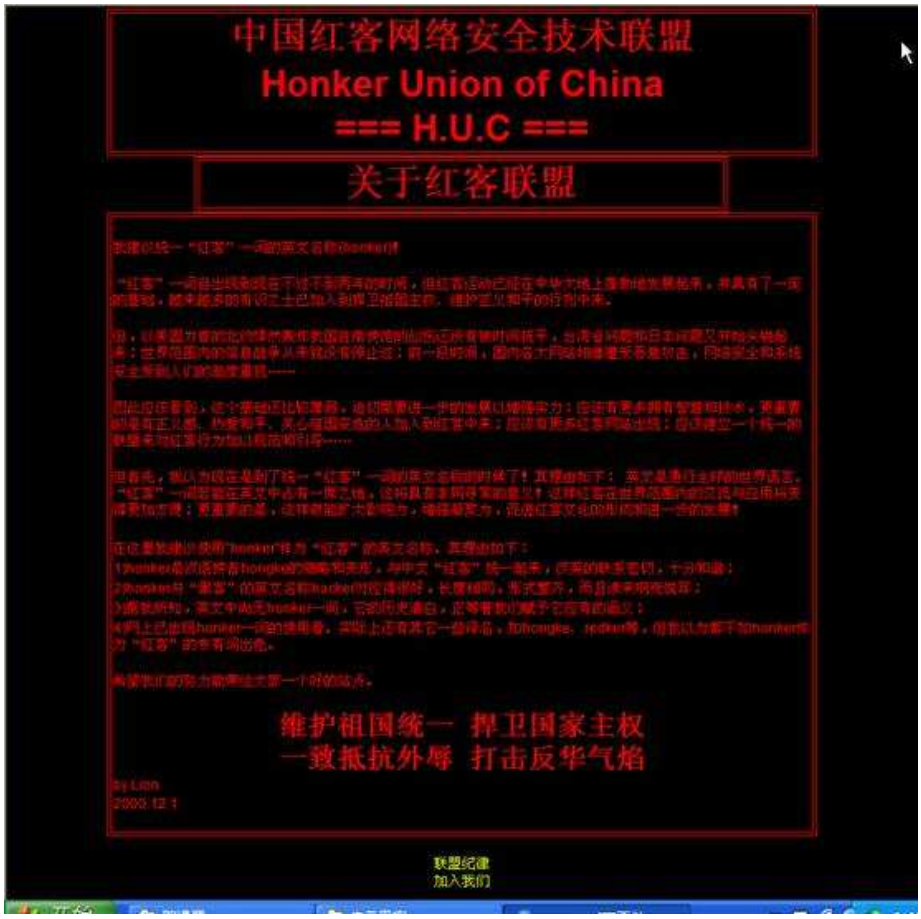
가진 고급 해킹 기술들을 정치와 사상적인 목적으로 이용하게 된다.

언더그라운드 해커 조직의 다양화

2000년에 이르러 중국 내 개혁과 개방 정책에 따라서 다양한 서구 문화가 중국으로 유입되며 정치적으로는 사회주의 노선을 표방하지만 경제면에서는 자본주의 시장 경제를 따라가는 변화를 맞이하게 된다. 이러한 중국 내 사회적인 변화와 함께 중국 언더그라운드 해커 조직에서도 새로운 문화를 가진 언더그라운드 해커 조직이 등장하기 시작한다.

이 시기의 해커 조직은 크게 세 가지 부류로 나누어지고 있다. 첫 번째가 홍커(红客)로 대표되며 이들은 강한 정치적인 색채와 애국주의적인 사상을 가진 단체들이며 그들이 가지고 있는 고급 해킹 기술들을 사상적인 목적에 활용하는 부류이다. 두 번째로는 난커(蓝客)로 대표되며 홍커(红客)와 반대로 순수하게 해킹 기술 습득을 주목적으로 하고 있다. 난커(蓝客)는 정치와 사상에는 전혀 관심을 가지지 않으며 오로지 해킹 기술 습득과 발전에만 전념하고 있다. 마지막으로는 근본적인 해커의 정신에 대해서만 다루며 정치와 컴퓨터 시스템에 대한 집착을 보이지 않는 해커 조직들이다. 그리고 이러한 전문적인 해커 조직 외에도 “중국 소년”이라고 불리는 저급한 크래커들이 등장하게 된다. 이들은 홍커(红客)와 난커(蓝客) 같이 조직적인 체계를 갖춘 집단이 아니라 혼자서 활동을 하며 해킹에 대한 전문적인 지식이 현저하게 떨어져 언더그라운드 해커 조직에서 개발한 해킹 프로그램들을 주로 이용하였다.

2003년에 이르러 중국 언더그라운드의 대표적인 해커 조직인 홍커(红客)는 일대 변화를 맞이하게 된다. 홍커(红客)의 리더인 Lion이 해킹 기술 습득과 함께 해킹에 대한 흥미를 잃어버리고 홍커(红客) 조직을 해체하게 된다. 이로 인해 홍커(红客)는 웹사이트 폐쇄와 함께 잠정적으로 모든 활동을 중단하게 된다. 그리고 이시기를 즈음하여 중국 언더그라운드 해커 조직에서도 서서히 해킹자체에 대한 기술 연구보다는 컴퓨터 보안에 대한 연구를 추구하는 조직들이 등장하기 시작하여 중국 언더그라운드 해커 조직의 다양화를 형성하기 시작하였다.



[그림1] 해체되기 전 홍커(红客)의 웹사이트]

현재 중국 언더그라운드 해커조직은 홍커(红客)의 해체 이후 중국 최초의 언더그라운드 해커 조직인 녹색병단(綠色兵單)과 비슷한 시기인 1997년에 조직된 중국응파(中國應派)가 리더인 Chinaeagle Union이 가장 큰 해커 조직으로 알려져 있으며 현재까지도 왕성한 활동을 하고 있는 것으로 알려져 있다. 그러나 예전과 같이 시스템 해킹과 같은 악의적인 활동 보다는 컴퓨터 보안에 대한 많은 연구 활동을 하고 있는 것으로 알려져 있다. 그리고 비교적 최근에 알려진 언더그라운드 해커와 해커 조직으로는 고독검객(孤獨劍客)과 그가 소속되어 있는 HackerBase Union이다. 고독검객(孤獨劍客)은 중국 차세대 해커로 꼽힐 정도로 고급 해킹 기술을 구사하고 있는 것으로 알려져 있다. 그리고 난커(蓝客)로 알려진 Lanke Union의 리더인 빙하(氷河)가 있다. 빙하(氷河)는 Lanke Union을 조직하고 그가 가지고 있는 고급 해킹 기술들을 문서화하여 조직의 해킹 기술을 끌어 올리는데 많은 기여를 한 것으로 알려져 있다. 그리고 마지막으로 EvilOctal Security Team의 리더인 빙설봉정(氷雪封情)이 고급 해커로 알려져 있다.