ASEC Report 3월

® ASEC Report

2006. 4

안철수연구소의 시큐리티대응센터(AhnLab Security Emergency 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. 3월 AhnLab 악성코드 동향

(1) 악성코드 피해동향

작성자: 박태환 주임연구원(juun5@ahnlab.com)

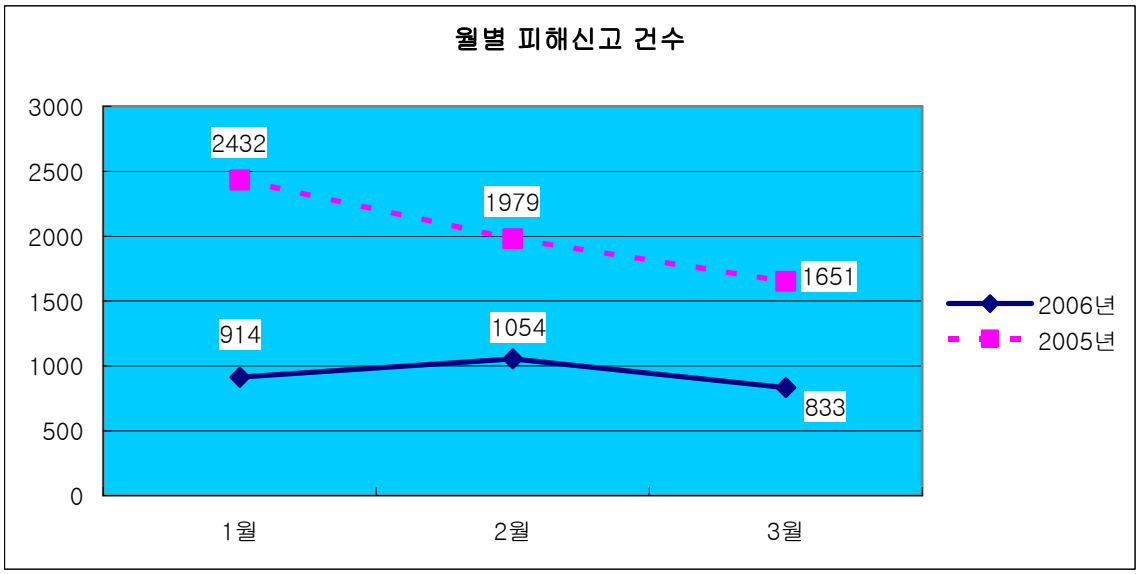
순위		악성코드명	건수	%
1	↑1	Win32/Netsky.worm.Gen	164	19.69%
2	New	Win-Trojan/Xema.183808.B	43	5.16%
3	New	Win-Trojan/Downloader.38925	35	4.20%
4	↓1	Win32/Bagle.worm.19666	20	2.40%
5	New	Win32/Bagle.worm.27136	17	2.04%
6	New	Win32/Tenga.3666	14	1.68%
7	↑2	Win32/IRCBot.worm.Unknown	10	1.20%
8	↓4	Win32/Parite	9	1.08%
9	↓4	Win32/Mytob.worm.Gen	8	0.96%
10	New	Win-Trojan/KorGameHack.11264	7	0.84%
		기타	506	60.75%
합계			**833**	100.00%

[표1] 2006년 3월 악성코드 피해 Top 10

3월 악성코드 피해 동향

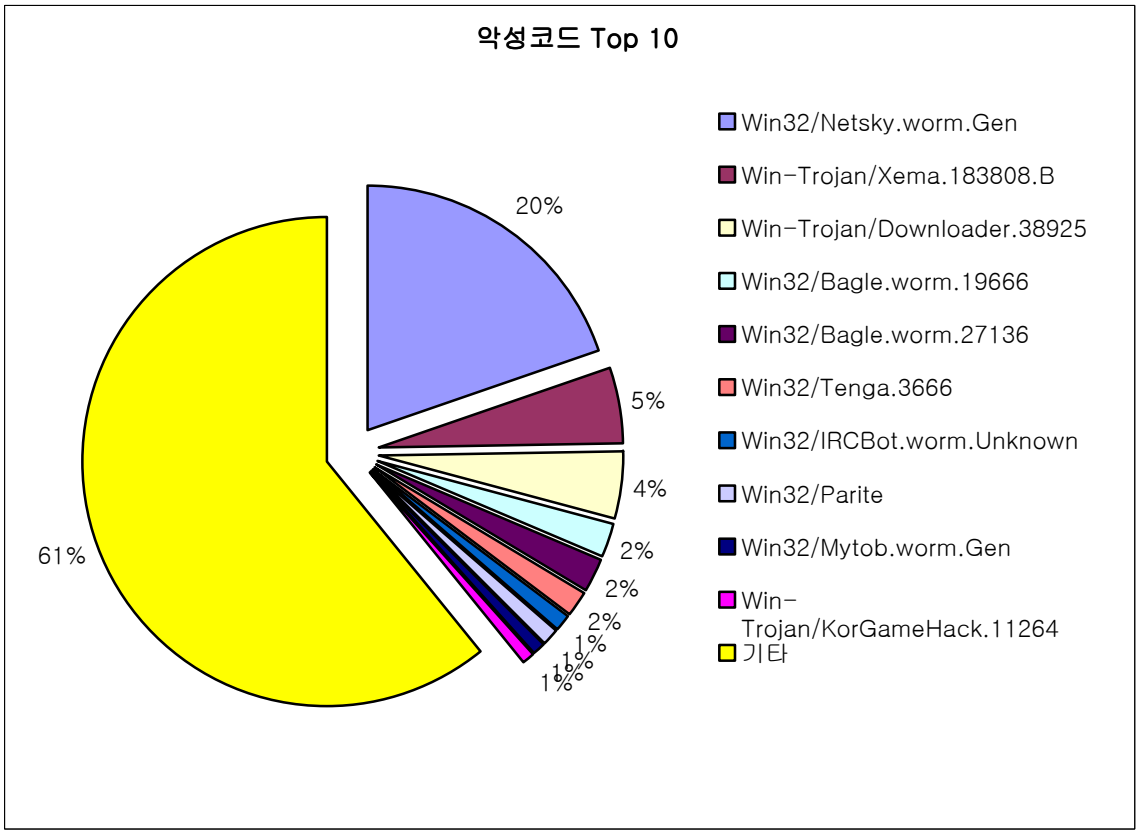
2006년 3월에는 제마.183808.B 트로이목마(Win-Trojan/Xema.183808.B), 다운로더.38925 트로이목마(Win-Trojan/Downloader.38925), 코어게임핵.11264 트로이목마(Win-Trojan/KorGameHack.11264)와 같은 트로이목마 프로그램이 악성코드 피해 Top 10에 랭크 되었다. 이는 아이알씨봇(IRCBot)류나 메스메일러 등의 웜이 주류를 이루던 종전과는 사뭇 다른 양상이다.

넷스카이 웜(Win32/Netsky.worm.Gen)과 아이알씨봇 웜(Win32/IRCBot.worm.Unknown)은 전월 순위에서 각각 1, 2단계 상승하였으나, 베이글 웜(Win32/Bagle.worm.19666), 패리테 바이러스(Win32/Parite), 마이탑 웜(Win32/Mytob.worm.Gen)등은 순위가 하락하였다. 피해건수가 20건 미만인 악성코드의 수가 전체 피해통계의 69%에 해당하는 571건이며, 전체 피해건수는 전년도 동월 1,651건의 50.45%에 해당하는 833건으로 집계되었다.



[그림1] 2006년 월별 피해신고 건수

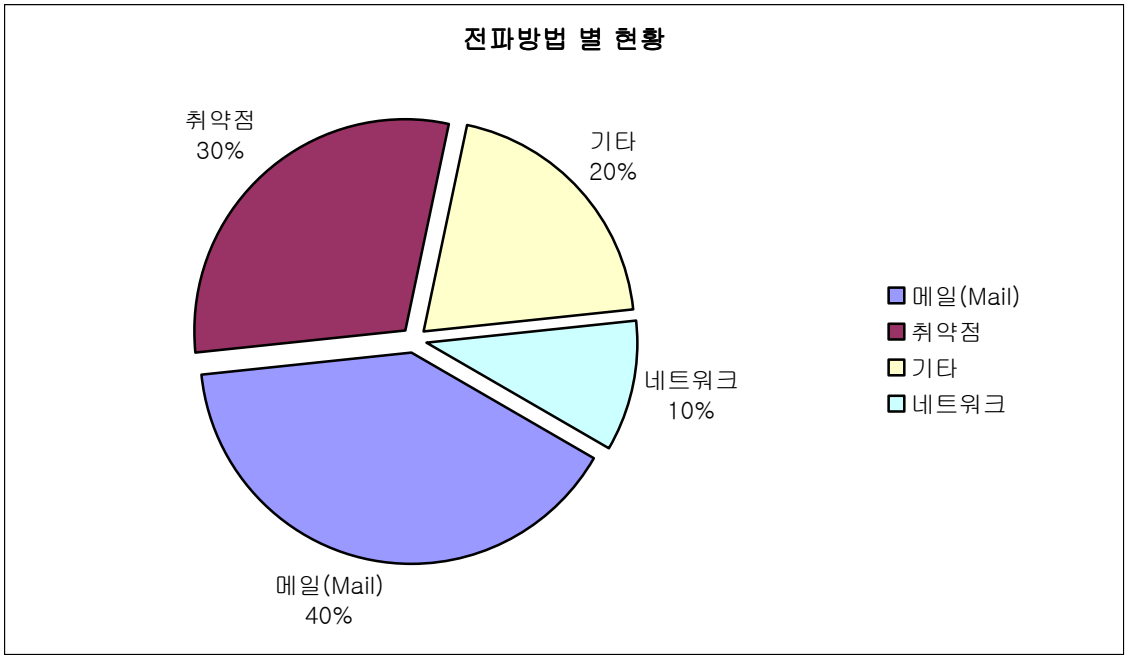
3월의 악성코드 피해 Top 10을 도표로 나타내면 [그림2]과 같다.



[그림2] 2006년 3월 악성코드 피해 Top 10

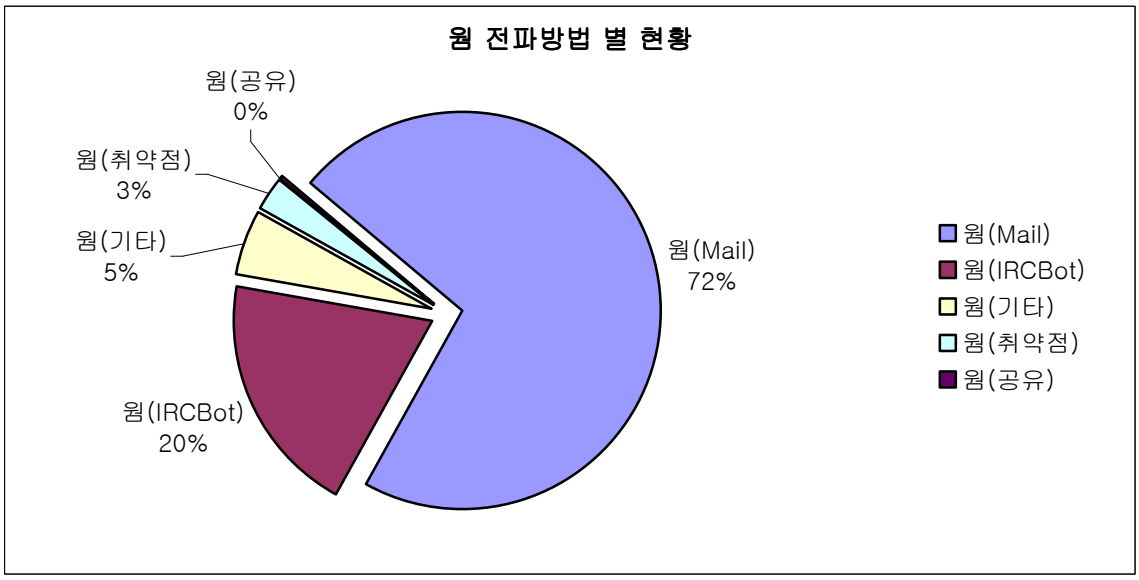
3월 악성코드 Top 10 전파방법 별 현황

[표1]의 Top 10 악성코드들은 주로 어떠한 감염 경로를 가지고 있는지 [그림3]에서 확인할 수 있다.



[그림3] 2006년 3월 악성코드 Top 10의 전파방법 별 현황

메일로 전파되는 특징이 있는 매스메일러는 40%, 취약점, 네트워크의 특징을 이용하여 전파되는 악성코드가 각각 30%와 10%를 차지했다. 매스메일러의 경우 2006년 1월 60%에서 2월에는 50%로 10% 감소하였는데, 3월에는 40%를 차지해 또 다시 10%가 줄어드는 현상을 보였다. 반면 취약점을 이용하는 악성코드의 수는 전월 10%에서 20%로 증가한 것을 볼 수 있다.

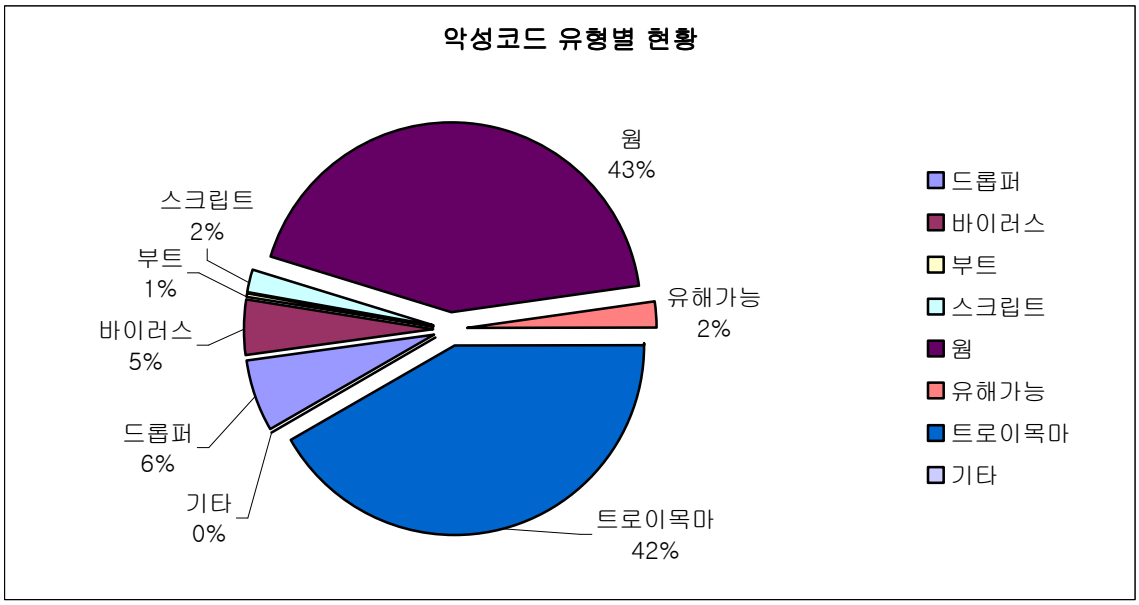


[그림4] 2006년 3월 웜의 전파방법 별 현황

매스메일러는 전월 78%에서 6% 하락한 72%를, 아이알씨봇 웜은 전월 10%에서 10% 상승한 20%를 차지하였다. 매스메일러와 아이알씨봇 웜이 전체 92%를 차지하고 있음을 알 수 있다.

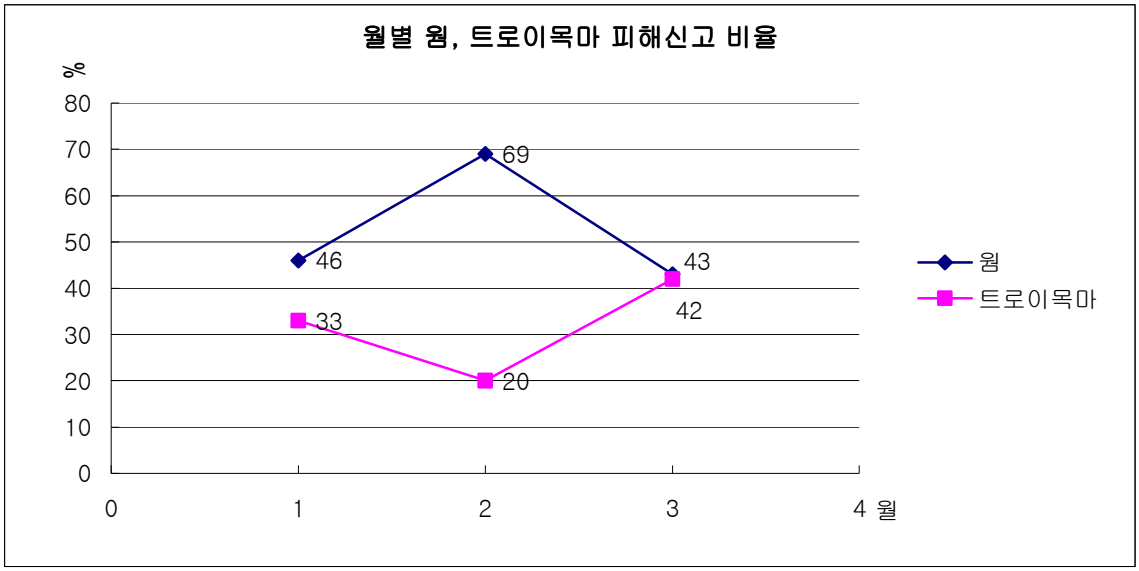
피해신고 된 악성코드 유형 현황

악성코드 유형별 현황은 [그림5]와 같다.



[그림5] 2006년 3월 피해 신고된 악성코드 유형별 현황

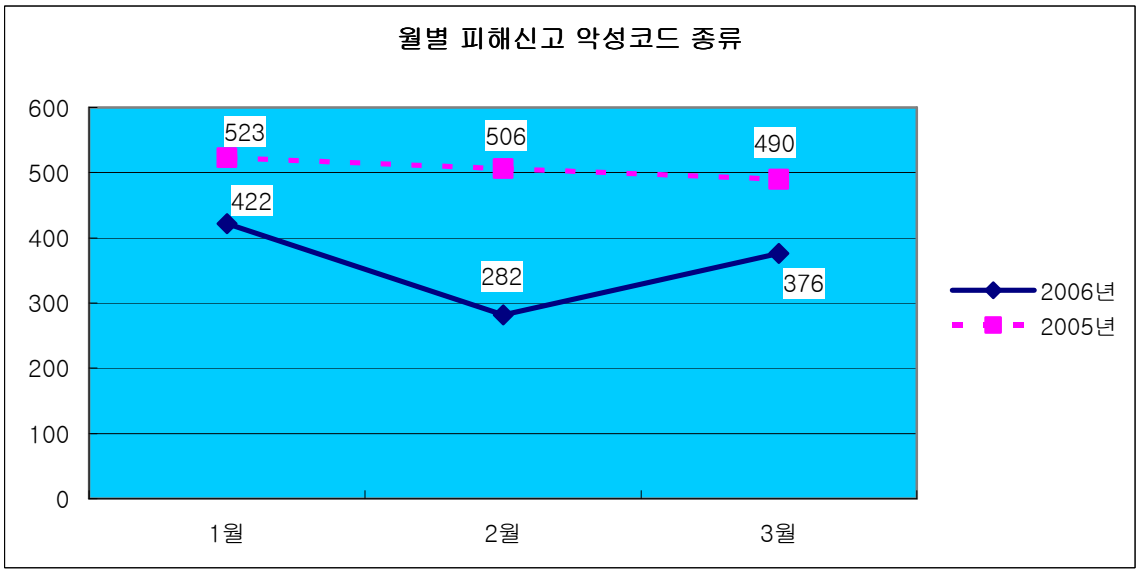
악성코드 유형에서는 웜이 43%, 트로이목마가 42%를 차지하는 가운데 드롭퍼와 바이러스가 각각 6%와 5%를 차지하였다. 웜과 트로이목마의 비율이 거의 비슷한 것이 다소 이례적이다.



[그림6] 2006년 월별 웜, 트로이목마 피해신고 비율

월별 피해신고 된 악성코드 종류 현황

3월에 피해 신고된 악성코드 갯수는 모두 376개로, 이는 전년도 동월에 비해 100건 정도 감소한 수치로 약 76.7%에 해당하는 수치이다.



[그림7] 2006년 월별 피해신고 악성코드 종류

특정 게임사이트의 정보유출을 노리거나, 특정 사이트에 접속한 후 악성코드를 다운로드 하는 트로이목마가 출현과 동시에 악성코드 피해 Top 10까지 진입한 3월이다. 따라서, 사용자는 악성코드의 동향에 주목함과 동시에 보안취약점에 대한 인식을 더욱 강화하고, 확인되지 않은 프로그램 사용에 주의를 기울이는 것이 필요하겠다. 무엇보다 좀 더 다양해진 개인정보

의 유출위협에 대한 경각심을 가지고 주기적인 암호변경이나 개인방화벽 프로그램 사용 등의 조치를 취하여 좀 더 안전한 PC사용환경을 구축하는데 관심을 가져야 할 것이다.

(2) 신종(변형) 악성코드 발견 동향

작성자: 정진성 주임연구원 (jsjung@ahnlab.com)

3월 한달 동안 접수된 신종(변형) 악성코드의 건수는 [표1], [그림2]와 같다.

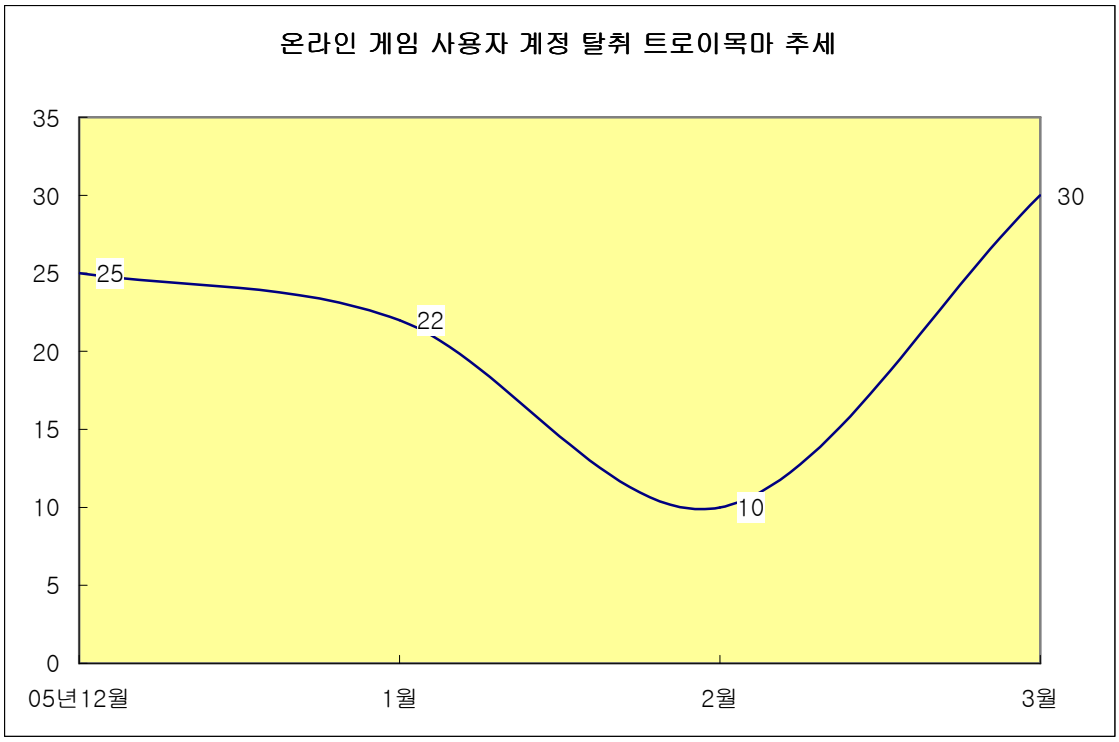
웜	트로이	드롭퍼	스크립트	파일	매크로	부트	부트/파일	유해가능	비윈도우	합계
61	131	28	2	6	0	0	0	13	0	241

[표1] 2006년 3월 유형별 신종(변형) 악성코드 발견현황

3월은 지난 2월과 달리, 신종(변형) 악성코드의 발견이 다시 증가하여 1월과 비슷한 정도의 수준을 보이고 있다. 2월에는 악성 아이알씨봇(IRCBot) 웜이나 온라인 게임의 사용자 계정을 탈취하는 트로이목마의 발견 보고가 현저히 낮았기 때문에 그 수가 적었으나, 3월에는 트로이목마와 웜의 발견 보고가 다시 증가하면서 전체적인 신종(변형) 악성코드 수가 지난달에 비해 증가하였다.

올해 3월과 작년 동기의 신종(변형) 악성코드 발견 경향을 비교해 보면, 2005년은 악성 아이알씨봇 웜 유형이 가장 많은 수를 차지했던 반면, 2006년은 트로이목마가 가장 많은 수를 차지하고 있다. 이는 작년 말부터 악성코드의 전체적인 흐름이 악성 아이알씨봇 웜에서 트로이목마 유형으로 그 흐름이 이동하고 있음을 보여주고 있다.

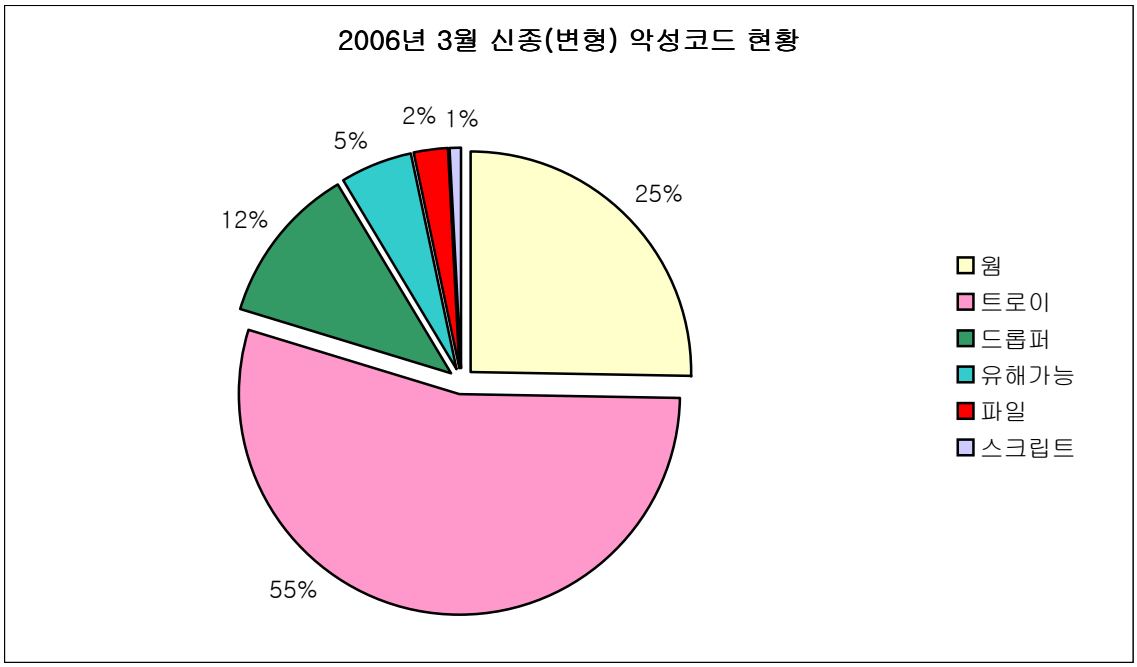
다음은 국내에 많은 피해를 주고 있는 온라인 게임의 사용자 계정을 탈취하는 악성코드 발견 건수에 대한 그래프이다.



[그림1] 온라인 게임 사용자 계정 탈취 트로이목마 현황

작년까지만 해도 온라인 게임 사용자 계정을 탈취하는 트로이목마들은 몇 종류의 유명한 게임들만을 대상으로 사용자 계정을 탈취하는 형태였다. 그러나 올해 들어 인기게임이 나오고, 중국이나 일본 등으로 수출되는 게임이 늘어나자 계정을 탈취하려는 게임의 종류가 증가하고 있다. 이 트로이목마들은 대부분 유사한 형태이고 모두 툴에 의해서 자동으로 생성되므로 대상이 되는 게임의 프로세스 등을 설정하기만 하면 간단히 만들 수 있도록 되어 있다. 따라서 향후에도 인기 온라인 게임이 출시된다면 이들도 이 트로이목마의 표적이 되는 건 불을 보듯 뻔 하다.

[그림2]는 3월 신종(변형)악성코드의 비율을 나타낸 것이다.

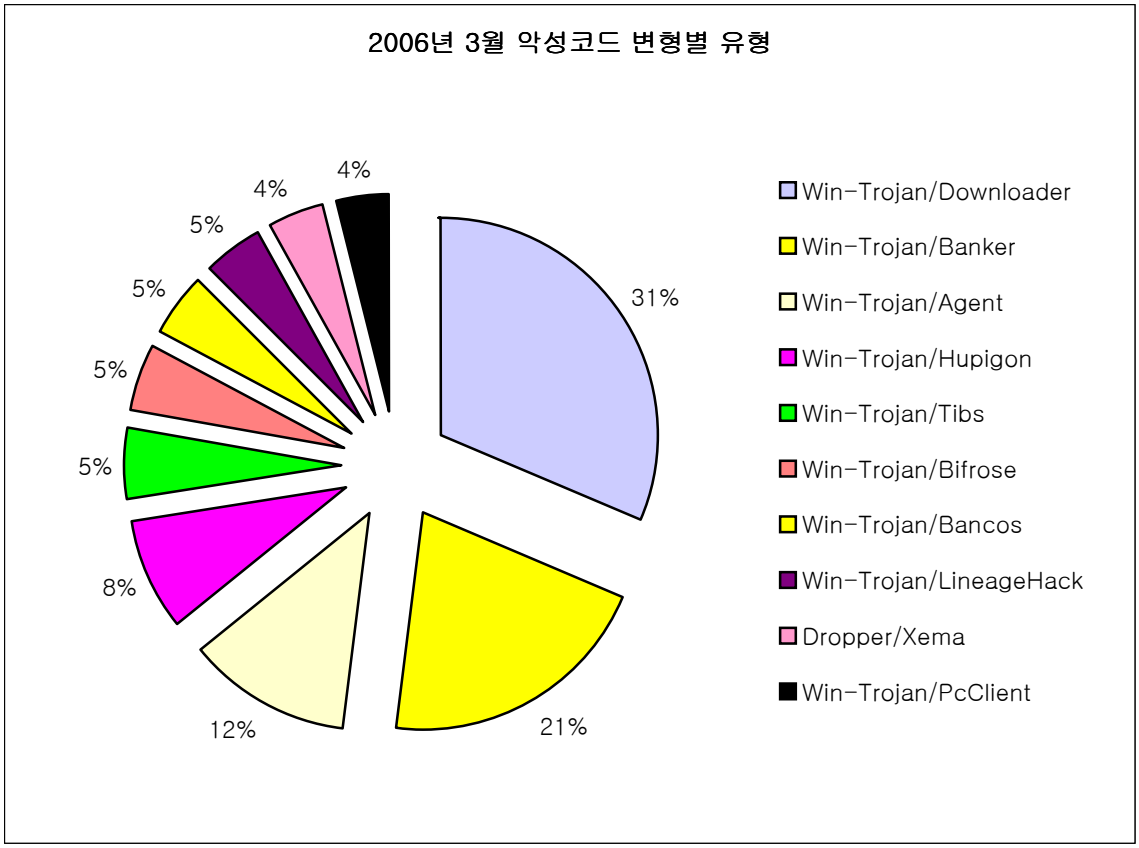


[그림2]2006년 3월 신종(변형) 악성코드 비율

2005년 말부터 바이러스가 종종 보고 되고 있다. 특히 이번 달은 무려 6종의 바이러스가 보고 되어, 2006년 들어 총 9종의 바이러스가 발견, 보고 되었다. 이는 작년 한 해 총 9종의 바이러스가 발견된 것과 동일한 수치이다. 이번 달 에 발견된 바이러스 절반이 중국에서 제작된 것으로 보고 되었다. 발견된 바이러스는 1종을 제외하고 모두 평범한 형태의 감염기법 -주로 DOS 바이러스들이 사용하는 방법으로 EntryPoint를 변경하지 않고 바이러스의 시작 주소로 JMP 또는 CALL 명령문을 사용하는 형태의 후위형 바이러스-을 사용하였다.

남은 1종의 바이러스는 3월말에 발견된 뎃냇 바이러스(Win32/Detnat)이다. 중국에서 제작된 것으로 추정되며 온라인 게임의 사용자 계정을 탈취하는 트로이목마를 다운로드 받아 설치한다. 이는 중국 발 해킹이 트로이목마 유포를 넘어서 이제는 실행파일을 감염시키는 바이러스 유형을 만들어 유포하는 형태로 변화되고 있음을 알 수 있다. 특히 이 바이러스는 감염

대상 파일을 압축하여 바이러스 자신이 이를 가지고 있어 원본 파일은 삭제한 후 감염된 파일을 실행 할 때마다 원본 파일을 생성한 후 실행한다. 또한 은폐기능을 하는 드라이버를 가지고 있어 감염된 파일 중 첫 번째로 실행되는 형태가 감염 컴포넌트가 된다. 감염 컴포넌트는 은폐 된 채로 실행되며 이후 다른 파일을 감염시킨다. 사용된 은폐기법은 커널 서비스 디스크립터 테이블(Service Descriptor Table)에서 특정 함수를 후킹하는 방식이다. 근래 들어 은폐기법 자체를 사용한 악성코드뿐 아니라 하나의 증상으로 은폐기법을 사용하는 악성코드의 수도 증가하는 추세이다.



[그림3] 악성코드 변형 별 유형 및 분포율

2월은 중국에서 제작된 것으로 추정되는 악성코드의 수와 종류가 전체적으로 적었다. 그러나 3월은 1월과 마찬가지로 중국에서 제작된 악성코드로 익숙한 후피곤 트로이목마(Win-Trojan/Hupigon), 리니지핵 트로이목마(Win-Trojan/LineageHack), 피씨클라이언트 트로이목마(Win-Trojan/PcClient)가 다시 Top 10 순위로 진입하였다. 이는 다시 해당 악성코드 변형이 제작 되고 있다는 것을 보여주고 있는 것이다.

다른 악성코드로는 여전히 스파이웨어와 악성코드 등을 다운로드하는 다운로더(Win-Trojan/Downloader)가 부동의 1위를 지키고 있다. 그리고 중남미와 유럽지역에서 은행계정 탈취목적으로 만들어진 뱅커 트로이목마(Win-Trojan/Banker)도 꾸준히 발견, 보고 되고 있

다.

3월 주요 신종(변형) 악성코드 정리

이번 달은 악성코드에 의한 피해 이슈 보다는 새로운 악성코드의 소식과 관련된 내용이 많았다.

► 은폐기법 소스 및 지식의 판매 중지

핵데프 트로이목마(Win-Trojan/HackDef)의 제작자로 유명하고, 은폐기법에 대한 소스와 툴을 판매하고 있는 것을 알려진 제작자가 더 이상 은폐기법과 관련된 지식을 판매하지 않겠다고 선언했다. 어떤 이유인지는 밝혀지지 않았지만 현재 알려진 은폐기법들은 모두 해제가 가능하기 때문에 더 이상 해당 기술을 판매하기 어려워졌기 때문인 것으로 추정된다.

► 개념증명형태의 악성코드 보고

개념증명형태의 악성코드 3종이 보고 되었다.

첫 번째로 MS Infopath 제품에 대한 악성코드이다. 실행가능한 형태의 확장자를 갖는 이 악성코드는 Infopath가 설치되어 있다면 해당 제품이 사용하는 *.XML을 찾아 감염 시키는 형태이다. 두 번째는 RFID 태그를 감염시키는 또는 전파되는 악성코드이다. 네덜란드에 거주하는 학생들로부터 보고된 RFID 악성코드의 개념증명이론은 매우 현실적이라 할 수 있다. 또한 RFID를 관리하는 미들웨어나 데이터베이스도 공격대상이 될 수도 있다고 한다. RFID 태그에는 몇 백 바이트 이내의 작은 공간이 존재한다. 여기에 악성코드를 충분히 저장할 수 있다고 설명한 그들 때문에 RFID 태크가 부착된 모든 사물에는 별도의 안티 바이러스 제품이 나와야 할지도 모른다는 조크성 얘기도 있었다. 세번째로는 가상머신 기반의 루트킷(Rootkit) 이다. 루트킷은 일반적으로 은폐형 악성코드를 말한다. 여기서 말하는 루트킷은 가상머신 기반의 루트킷 이다. 즉, 정상적인 OS에 가상머신을 동작시키고 그 환경 또는 악성코드가 자체적으로 구현한 OS 환경에서 동작하는 루트킷을 말한다. 이와 비슷한 악성코드가 이미 도스시절에도 있었다. PMBS라고 불리는 이 부트 바이러스는 실행되면 보호모드를 V86의 가상모드로 변환하며 동작하는 모든 응용 프로그램 역시 V86에서 실행 되도록 해둔다.

이러한 개념증명형태의 악성코드는 일반 사용자들에게 피해를 줄 목적으로 제작 하기 보다는 단지 제작이 가능하다는 개념을 증명해 보이기 위한 것에 불과하다. 물론 몇몇의 개념증명형태의 악성코드들은 후에 일반 사용자들도 감염되는 사례가 있거나 또는 제작기술이 여러 악성코드에 이용된 적도 있다. 하지만 이러한 개념증명형태의 악성코드가 새롭기 때문에 진단 하거나 치료하기 어려운 경우는 없었으며 단지 새롭다는데 그 초점이 맞춰졌다 하겠다.

► 일본에서 사용되는 P2P 프로그램과 이를 이용한 악성코드의 사회적 이슈화

일본에서는 P2P 프로그램과 이를 이용하여 사용자 정보를 유출하는 악성코드가 사회적인 이슈를 불러 일으켰다. 일본 내에서 위니(Winny)와 셰어(Share)라고 불리는 P2P 프로그램을

이용하여 자신을 전파하거나 오피스 문서 류의 사용자 정보를 유출하는 악성코드의 피해가 연이어 터져 사회적으로 큰 문제가 되었다.

► 마이둠.28160 웜(Win32/MyDoom.worm.28160)

이 웜은 이전에 발견되었던 마이둠 웜 변형들과 매우 유사하다. 그러나 이전에 발견되었던 것과는 달리 은폐증상을 가지고 있는 것이 특징이다. 그리고 그 은폐기법 또한 특이하다. 일반적인 커널 은폐기법은 별도의 드라이버를 통하거나 유저 모드에서 physical memory의 커널 영역을 수정하는 기법을 사용한다. 이 웜 역시 별도의 드라이버 없이 커널 은폐기법을 사용하는데 유저모드에서 call gate를 통해 직접 GDT (Global Descriptor Table) 영역을 수정하여 타켓을 은폐한다.

► 베이글.22272 트로이목마(Win-Trojan/Bagle.22272)

베이글 트로이목마는 지금까지 수 많은 변형이 나왔지만 은폐증상을 갖는 형태는 이번이 처음이다. M_hook.sys 란 파일명을 갖는 별도의 커널 드라이버를 이용한다. 후킹방식은 커널 서비스 디스크립터 테이블에서 6개 정도의 커널 함수를 후킹한 후 트로이목마 자신과 레지스트리, 파일을 숨긴다. 그러나 은폐방식은 매우 일반적인 형태를 사용하고 있다.

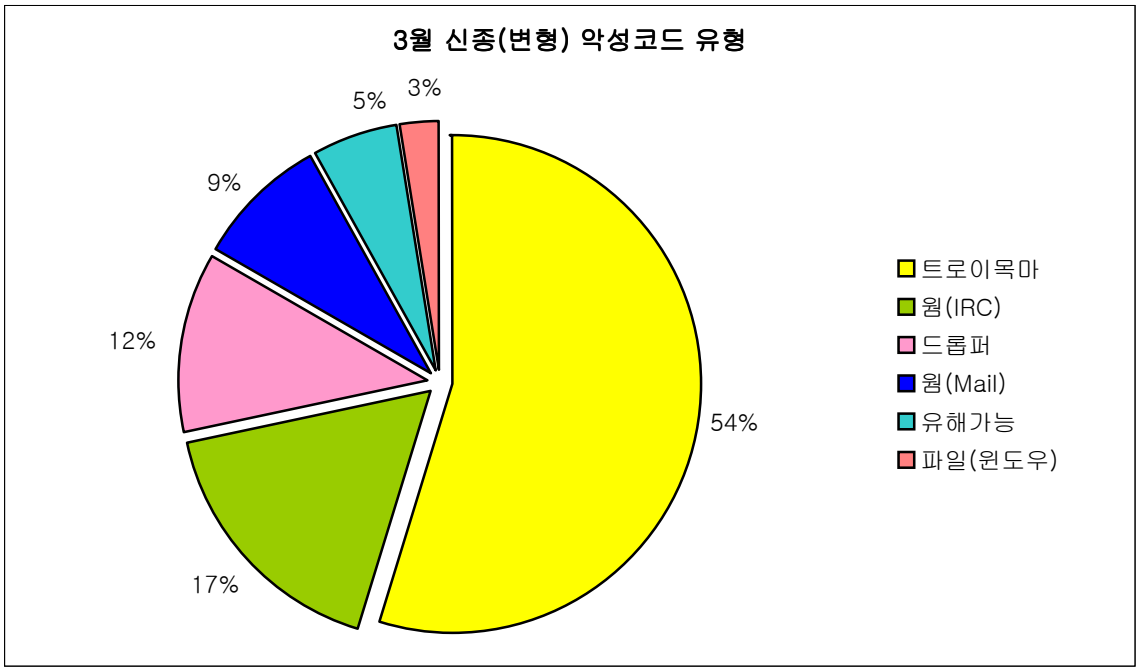
► 뎃냇 바이러스(Win32/Detnat)

중국 발 웹 해킹으로 해킹된 웹사이트에서 이 바이러스의 드롭퍼가 발견된 점으로 미루어 중국에서 제작된 것으로 추정된다. 이 바이러스는 국내 특정 호스트에서 온라인 게임의 사용자 계정을 탈취하는 트로이목마를 다운로드하고 실행파일을 감염시키는 증상을 가지고 있다. 또한 감염 컴포넌트는 은폐된 채로 실행된다.

► 인터넷 익스플로러의 'createTextRange' 취약점

이 취약점은 인터넷 익스플로러가 "createTextRange()" 메서드를 호출하는 과정에서 발생하는 메모리 Corruption Error가 원인이 된다. 공격자는 createTextRange() 메서드를 포함하여 잘 조작된 웹 페이지를 통해서 원격으로 인터넷 익스플로러 크래쉬(crash)시키거나 임의의 코드를 실행할 수 있다. 이 취약점이 공개된 이후 이를 이용한 악성코드가 보고 되었지만 그 수가 이전의 WMF 취약점과 비교하면 매우 적다

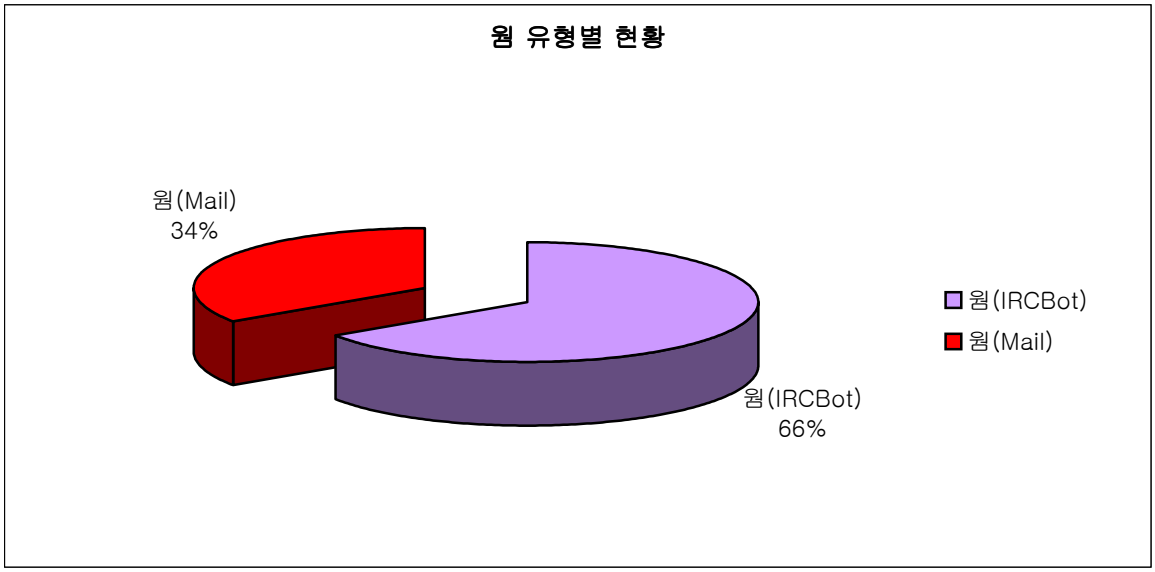
다음은 이번 달에 발견된 신종(변형) 악성코드에 대한 유형별 분포이다.



[그림4] 3월 신종(변형) 악성코드 유형별 현황

3월 신종(변형) 악성코드 현황을 살펴보면 트로이목마 유형이 과반수 이상을 차지하고 있으며, 파일 바이러스가 전체의 3%를 차지하고 있는 것이 특징이다.

다음은 가장 확산력이 큰 웜 유형만 전파 형식에 따라 분류해 보았다. 근래 들어 메신저 웜 그리고 P2P 웜의 보고가 적어지고 있다. 이들 웜은 이메일 웜과 악성 아이알씨봇 웜과 달리 유행처럼 나타났다가 사라지는 경향을 보인다. 즉, 누군가가 메신저 웜을 만들어 유포하면 이후 비슷한 변형이 우후죽순 나오다가 사라진다. 이는 P2P 웜도 마찬가지로, P2P를 통한 불법 자료를 공유하는 사용자층이 많아지거나 새로운 P2P 가 나오면 금새 이를 이용해서 전파되는 악성코드가 출현했다가 사라지는 일이 비일비재 하다.



[그림5] 3월 신종 및 변형 웜 유형별 현황

2006년 1분기 악성코드 동향

작년과 올해 1분기의 악성코드 흐름은 완전히 다르다. 이는 가장 많은 피해건수나 또는 변형 건수를 차지하는 악성코드 유형이 악성 아이알씨봇 웜에서 트로이목마 유형으로 이동한 것이다. 이렇게 변화된 이유는 금전적인 이득을 취하려는 제작자들의 욕구로 인한 것이다. 또한 사용자들의 보안의식 향상, 윈도우 XP SP2의 보급과 정부기관들의 적극적인 보안활동의 결과로 악성 아이알씨봇 웜의 감염 및 피해보고가 감소하고 있는 추세이다.

또한 악성코드 피해유형은 과거와 달리 국지적인 양상을 보이고 있다. 더 이상 광범위하게 퍼지는 악성코드가 많아지기 보다는 어떠한 이익을 목적으로 특정 국가나 특정 IP 대역에서 피해가 발생하곤 한다. 국내는 해외의 여느 국가와 달리 - 주로 해외는 이메일 웜 또는 은행 계정을 탈취하는 트로이목마가 기승을 부린다 - 온라인 게임 계정을 탈취하려는 트로이목마 목마의 수가 높다. 또한 중국 발 해킹의 후폭풍으로 발생하는 여러 중국산 트로이목마들의 피해 및 발견보고가 한 몫을 하고 있다.

트로이목마라고 하더라도 올해와 작년 동기에 비해서 차이를 보이고 있는데 2005년에는 주로 원격제어를 할 수 있는 '에이전트', 홈페이지를 변조하는 '스타트페이지' 그리고 '프록시 서버류'가 주류를 이루었다. 다음과 같다.

- 에이전트 트로이목마(Win-Trojan/Agent)
- 다운로더 트로이목마(Win-Trojan/Downloader)
- 스타트페이지 트로이목마(Win-Trojan/StartPage)
- 스몰 트로이목마(Win-Trojan/Small)

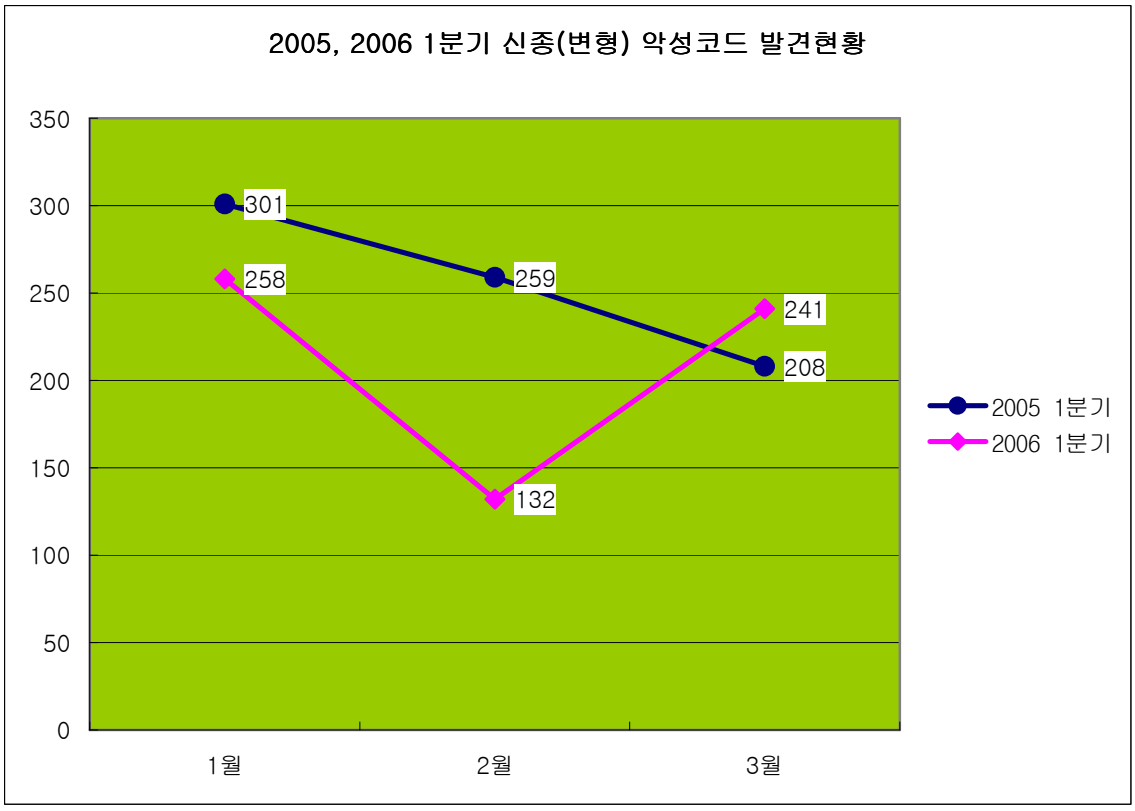
- 프록시에이전트 트로이목마(Win-Trojan/ProxyAgent)

2006년은 국내 온라인 게임의 사용자 계정을 탈취하는 트로이목마와 중국산 트로이목마 그리고 다른 악성코드를 다운로드하는 다운로더류가 증가 하였다.

- 리니지핵 트로이목마(Win-Trojan/LineageHack)
- 행핵 트로이목마(Win-Trojan/HangHack)
- 코어게임핵 트로이목마(Win-Trojan/KorGameHack)
- 그레이버드 트로이목마(Win-Trojan/GrayBird)
- 후피곤 트로이목마(Win-Trojan/Hupigon)

2005년 동기의 트로이목마들은 주로 감염 대상의 시스템을 원격제어 혹은 프록시 서버로 사용하는 모습이었다면 2006년 동기의 트로이목마들은 주로 감염 대상의 시스템에서 사용자 정보를 훔쳐내는 형태로 그 목적이 변화된 것을 알 수 있다.

다음은 올해 1분기와 작년 동기의 신종 및 변형 악성코드의 수를 비교 한 것이다.



[그림6] 2005, 2006 1분기 신종(변형) 악성코드 발견현황

작년 동기의 경우 악성 아이알씨봇 웜의 비율이 점차 감소하여 전체적으로 1분기 악성코드

의 수가 감소하였다. 반면 올해는 2월의 이상적인 감소를 제외하고는 대체적으로 비슷한 악성코드의 수를 보여주고 있다. 또한 작년 이 맘 때부터 시작된 중국 발 웹 해킹의 영향으로 트로이목마의 비중이 증가하기 시작했다. 2월의 이상적인 감소의 원인도 중국 최대 명절휴일로 인해 악성코드 제작 및 유포가 뜸했던 걸로 추정 되고 있을 정도로 중국산 악성코드가 이제는 국내의 악성코드 동향에 빠질 수 없는 소재로 자리 잡았다.

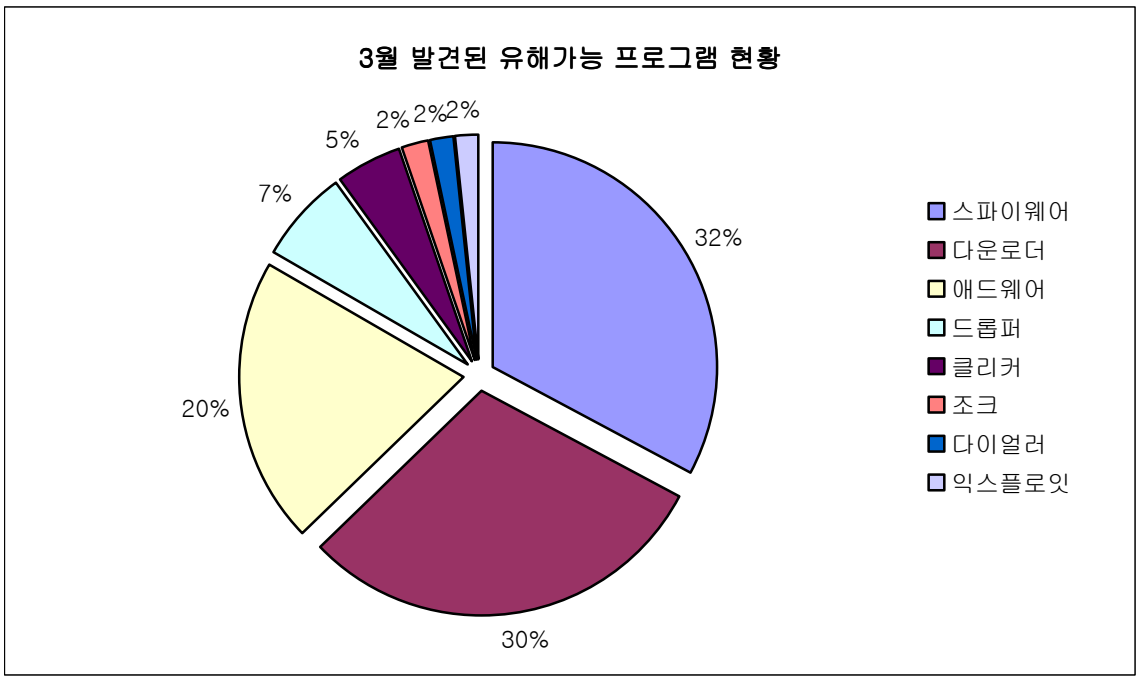
II. 3월 AhnLab 스파이웨어 동향

작성자: 김정석 주임연구원(js_kim@ahnlab.com)

3월 한 달 동안 접수된 신종(변형) 유해가능 프로그램 건수는 [표1], [그림1]과 같다.

스파이웨어	다운로더	애드웨어	드롭퍼	클리커	조크	다이얼러	익스플로잇	합계
82	75	51	17	12	5	4	4	250

[표1] 2006년 3월 유형별 스파이웨어 발견 현황



[그림1] 2006년 3월 유형별 유해가능 프로그램 발견 비율

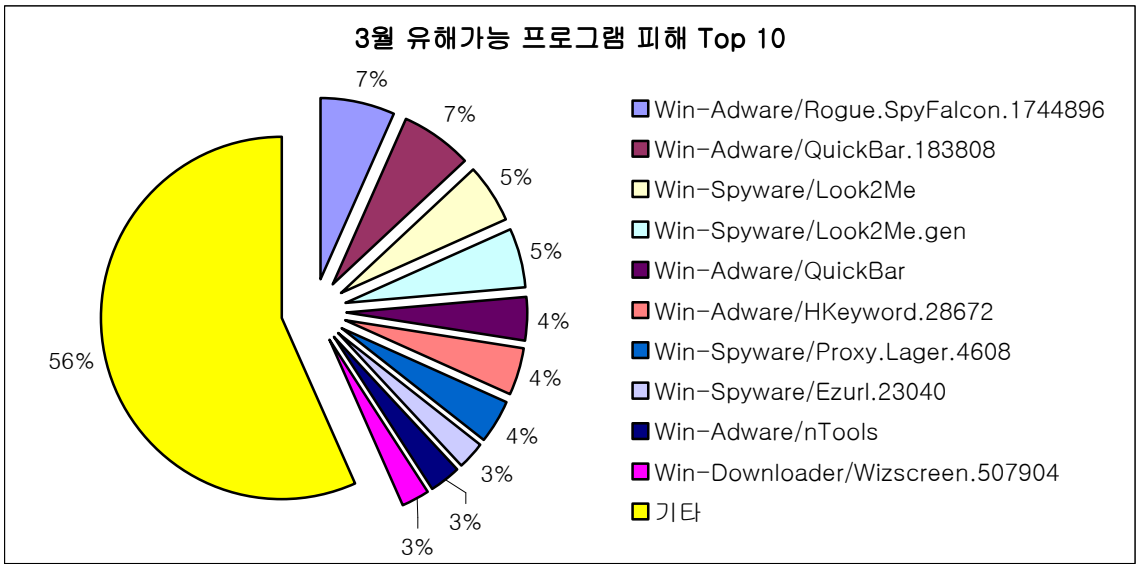
3월에는 지난 1, 2월과 달리 애드웨어보다 스파이웨어, 다운로더가 많이 발견되었다. 이는 여러 가지 유해가능 프로그램을 설치하는 애드로드 다운로더(Win-Downloader/Adload)의 새로운 변형이 발견되었기 때문인 것으로 풀이된다. 애드로드는 아이알씨봇(IRCBot) 웜에 의해 설치되며, 룩투미 스파이웨어(Win-Spyware/Look2Me), 크립터 스파이웨어(Win-Spyware/Crypter) 등 다수의 스파이웨어를 설치하고 실행하며 컴퓨터의 성능을 크게 저하시킨다. 윈도우 취약점을 이용하여 전파하는 아이알씨봇 웜에 의해 다운로드되고 실행되기 때문에 그 피해는 광범위할 것으로 예상된다.

3월 피해 신고된 스파이웨어 Top 10을 살펴보면 [표2], [그림2]와 같다.

순위		유해가능 프로그램명	건수	비율
1	↑1	Win-Adware/Rogue.SpyFalcon.1744896	5	7%

2	New	Win-Adware/QuickBar.183808	5	7%
3	↓2	Win-Spyware/Look2Me	4	5%
4	New	Win-Spyware/Look2Me.gen	4	5%
5	New	Win-Adware/QuickBar	3	4%
6	New	Win-Adware/HKeyword.28672	3	4%
7	New	Win-Spyware/Proxy.Lager.4608	3	4%
8	↓4	Win-Spyware/Ezurl.23040	2	3%
9	New	Win-Adware/nTools	2	3%
10	New	Win-Downloader/Wizscreen.507904	2	3%
		기타	43	56%
합계				

[표2] 2006년 3월 유해가능 프로그램 Top10



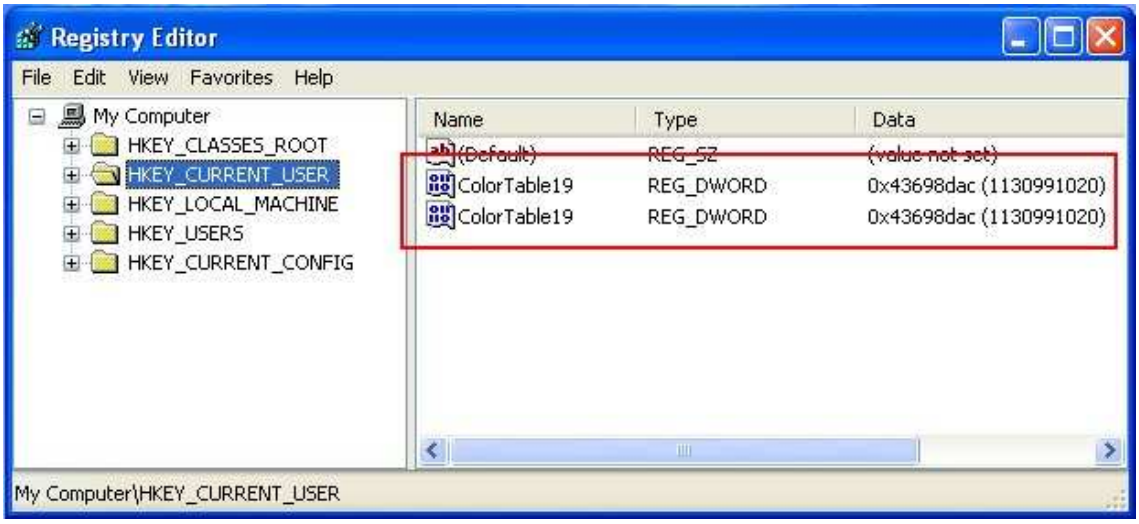
[그림2] 3월 유해가능 프로그램 피해 Top 10

3월 피해 동향을 살펴보면 지난 달 2위를 차지했던 스파이팔콘(Win-Adware/SpyFalcon.1744896)이 피해 접수 1위를 차지한 것을 볼 수 있다. 스파이팔콘은 훼이크얼럿 클리커(Win-Clicker/FakeAlert)에 의하여 사용자 동의 없이 설치되는 허위 안티스파이웨어 프로그램(Rogue/Suspected Anti Spyware)이다. 스파이팔콘은 주로 재감염 피해가 많이 접수되었으며, 이는 스파이팔콘을 설치하는 훼이크얼럿의 변형이 매우 많기 때문으로 보인다.

2월과 마찬가지로 애드로드 다운로더에 의해 설치되는 룩투미(Win-Spyware/Look2Me)가 피해 신고의 상위를 차지하고 있다. 룩투미는 Winlogon Notify에 등록되어 안전모드에서도 동작하며 프로세스 중지가 어렵고 수동제거가 까다롭기 때문인 것으로 풀이된다.

3월 달에 새로 Top 10에 진입한 라거 스파이웨어(Win-Spyware/Proxy.Lager.4608)는 광고

성 스팸메일을 발송하는 은폐형 스파이웨어이다. API 후킹(Hooking)을 이용하여 라거 스파이웨어가 생성하는 taskdir.exe, taskdir.dll 파일과 레지스트리 정보를 은폐하고 조작하는 특징으로 많은 피해 신고가 접수되었으며, 자체 업데이트 기능이 있기 때문에 앞으로도 많은 변형이 발견될 것으로 예상된다.



[그림3] 라거 스파이웨어가 생성하는 레지스트리 값 이름(Value Name)[1]

2006년 1분기 유해가능 프로그램 동향

2006년 1분기를 돌아보면 허위 안티스파이웨어 프로그램에 의한 피해와 웜에 의해 배포되는 유해가능 프로그램 피해가 증가했던 것을 알 수 있다.

허위 안티스파이웨어 프로그램 피해 지속

2006년 2월 발견된 비패스트(Win-Adware/Rogue.Befast)는 국내에서 제작된 허위 안티스파이웨어 프로그램이다. 2005년 12월부터 포털 사이트의 게시판이나 블로그를 통하여 ActiveX 형태로 배포되었으며 약 25만 대의 시스템에 설치된 것으로 추정된다.
일반적인 허위 안티스파이웨어 프로그램이 임시파일, 사용하지 않는 레지스트리를 진단하거나 정상 파일 또는 레지스트리를 진단하여 검사결과를 과장하는 반면, 비패스트는 설치 시에 스파이웨어가 사용하는 레지스트리 키를 스스로 생성하고 이를 진단하여 검사 결과에 표시하며 치료 시 유료사용을 요구한다. 이 방법을 이용하여 약 1억 8천만원의 부당 이익을 취한 비패스트 제작자는 2006년 4월에 허위 안티스파이웨어 프로그램 제작자로는 국내 최초로 경찰에 구속되었다.

3월 유해가능 프로그램 피해동향의 1위를 차지한 허위 안티스파이웨어 프로그램인 스파이팔

[1] 레지스트리 키 아래에 동일한 이름의 값이 생성될 수 없으나, 라거에 의해 동일한 값이 두 개 생성된 것처럼 보인다. 이들 중 한 개의 실제 이름은 “ColorName20” 이다.

콘(Win-Adware/SpyFalcon.1744896)은 동구권에서 제작되었으며, 훼이크얼럿(Win-Clicker/FakeAlert)에 의해 사용자 동의 없이 설치 되는 방법으로 최근까지 지속적인 피해를 입히고 있다. 2005년 안티바이러스골드(Win-Adware/Rogue.AntiVirusGold)를 시작으로 가장 최근의 스파이웨어퀘이크(Win-Adware/Rogue.SpyQuake)까지 동일한 프로그램을 UI와 이름만 바꾼 형태로 지속적으로 배포하고 있으며, 2006년에는 한 달에 한 번 꼴로 새로운 프로그램을 배포하고 있다. 이들 허위 안티스파이웨어 프로그램의 계보를 정리해 보면 [표3]과 같다.

이름	최초 배포	진단명
안티바이러스골드(AntiVirusGold)	2005년 6월	Win-Adware/Rogue.AntiVirusGold
스파이액스(SpyAxe)	2005년 11월	Win-Adware/Rogue.SpyAxe
스파이웨어스트라이크(SpywareStrike)	2006년 1월	Win-Adware/Rogue.SpyStrike
스파이팔콘(SpyFalcon)	2006년 2월	Win-Adware/Rogue.SpyFalcon
스파이웨어퀘이크(SpywareQuake)	2006년 3월	Win-Adware/Rogue.SpyQuake

[표3] 허위 안티스파이웨어 프로그램의 계보

웜이 배포하는 유해가능 프로그램의 피해 증가

3월 피해동향에서도 언급한 애드로드 다운로더는 아이알씨봇 웜이 감염된 시스템에 다운로드 되고 실행된다. 웜에 의해 설치되기 때문에 주로 보안에 취약한 가정용 컴퓨터에서 많이 발견되고 있으며 2005년 12월부터 최근까지 꾸준한 피해를 입히고 있다.

봇마스터(BotMaster)가 웜에 감염된 시스템을 이용하여 애드웨어를 설치하고 성인, 도박 사이트 등에 방문을 유도하여 트래픽을 발생시켜 웹 사이트로부터 그 대가를 받는 방법으로 이익을 취한다. 웜 제작자가 금전적인 이익을 목적으로 애드웨어나 스파이웨어를 이용한다는 이야기가 최근에 나온 것은 아니지만, 최근에서야 주체, 방법 등의 웜과 애드웨어의 관계가 구체적으로 밝혀지고 있다. 2006년 2월에는 워싱턴포스트지에 "0x80"으로 자처하는 미국의 한 청년이 자신이 제작한 웜에 감염된 시스템을 이용하여 애드웨어를 설치하고 한 달에 약 6,800 달러를 벌고 있다는 흥미로운 인터뷰 기사가 게재되기도 하였다[1]. 앞으로도 웜에 의한 유해가능 프로그램 설치 피해가 증가할 것으로 예상된다.

[1] http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html

III. 3월 시큐리티 동향

작성자: 최동균 연구원(cdk@ahnlab.com)

3월에 발표된 보안 취약점 동향

마이크로소프트사(이하 MS)의 3월 정기 보안 패치는 총 2건으로, MS 윈도우 서비스와 관련된 중요보안 공지 1건(MS06-011)과, MS 오피스 취약점과 관련된 긴급 보안 공지 1건(MS06-012)의 보안 패치가 발표되었다. 3월 정기 보안패치가 발표된 후 인터넷 익스플로러 특정함수 처리와 관련된 취약점(917077)이 3월 22일 추가로 공개 되었으며, MS사는 취약점 해결을 위한 패치를 4월 11일 정기 보안패치 일정에 맞추어 배포할 예정이다. 현재 해당 취약점을 이용하는 악성코드 및 공격코드가 공개되어 제약조건에 해당하는 일부 시스템의 피해가 예상되므로 사용자는 보안패치가 제공되기 까지의 공백기간 동안 MS사의 가이드를 준수하는 등 보다 세심한 주의가 필요하다.

마이크로소프트사의 3월 주요 취약점 현황[1]

위험등급	취약점	공격코드 유/무
HIGH	HTML 개체의 예상치 못한 메서드 호출 처리 방식에 존재하는 취약점으로 인한 원격 코드 실행 (917077)[2]	유
HIGH	Microsoft Office의 취약점으로 인한 원격 코드 실행 문제점 (MS06-012)[3]	무
MID	필요 이상의 사용 권한을 허용하는 Windows 서비스 DACL로 인한 권한 상승 문제점 (MS06-011)[4]	무 계정필요

► HTML 개체의 예상치 못한 메서드 호출 처리 방식에 존재하는 취약점으로 인한 원격코드 실행 (917077)

이 취약점은 MS 인터넷 익스플로러의 create TextRange() DHTML 메서드를 호출하는 과

[1] 취약점 현황은 ASEC 의 보안전문가들에 의해 공격코드 유/무, 악성코드 활용가능성, 취약점의 위험도등 다양한 관점에서 판단하여 선별된 것으로, 사용자들의 주의가 필요한 것임을 나타낸다. 공격코드의 존재유무는 이 리포트를 작성하는 시점에서 인터넷 상에서 접할 수 있는 기준으로 작성되었다.

[2] MS 보안권고(917077), http://www.microsoft.com/korea/technet/security/advisory/917077.mspx

[3] MS06-012, http://www.microsoft.com/korea/technet/security/bulletin/MS06-012.mspx

[4] MS06-011, http://www.microsoft.com/korea/technet/security/bulletin/MS06-011.mspx

정에서 메모리 Corruption Error가 발생하는 것이 원인으로, 현재 공개된 공격코드는 Heap 메모리 영역에 대량의 데이터(NOP+ShellCode)를 채우고 이는 최초 설계된 범위(3c04074c2 지점)를 넘겨 데이터를 덮어쓰게 된다.

```
75BB1E1D   8BCF          MOV ECX,EDI
75BB1E1F   8B78 08       MOV EDI,DWORD PTR DS:[EAX+8]
75BB1E22   8BD1          MOV EDX,ECX
75BB1E24   C1E9 02       SHR ECX,2
75BB1E27   F3:A5         REP MOVS DWORD PTR ES:[EDI],DWORD PTR DS:[ESI]     *** 데이터 복사
```

그 결과 시스템의 EIP 레지스터 값이 존재하지 않거나 임의의 특정 메모리 값으로 덮어쓰기 되어 Heap 메모리 영역의 ShellCode(공격자가 의도한 코드)가 실행될 수 있다. 현재 MS사는 취약점을 제거할 수 있는 보안패치를 4월 정기 보안 패치에 포함하여 배포할 예정이며, 패치를 제공받지 못하는 공백기간 동안 인터넷 익스플로러에서 Active 스크립팅의 자동실행을 사용하지 않거나 수동으로 변경하는 것을 권장하고 있다.

► 센드메일(Sendmail) 원격 시그널 핸들링 취약점[1]

이메일 서비스를 위한 대표적 오픈 소스인 센드메일(Sendmail)에서 원격 시그널 처리 취약점이 발견되었다. 외부 클라이언트의 데이터를 수신하고 시그널 핸들링의 타임아웃 처리에 관여하는 setjmp 및 longjmp 함수를 호출하는 과정에서 Heap 메모리 영역을 덮어쓰게 되어 시스템이 예상하지 못한(공격자가 의도한) 메모리에 접근하여 권한 획득이 가능한 취약점이 발생한다. Sendmail 8.13.5를 포함한 하위 버전이 이 취약점을 가지고 있으며 센드메일 컨소시엄(Sendmail Consortium)은 이 취약점에 안전한 Sendmail 8.13.6 버전을 공개하였으며, 즉시 업그레이드 할 것을 권고하고 있다.

► 신용정보 유출사고 사례들

국내 모 금융기관이 고객 3만 여명의 개인정보를 메일로 유출시킨 사고가 있었다. 인터넷 뱅킹으로 복권을 구입한 후 3개월간 활동이 없었던 고객에게 발송하기 위한 마케팅 메일에 직원의 실수로 고객파일이 첨부되어 발송된 사고이며 첨부된 파일에는 3만 여명의 이름, 주민등록번호, 이메일 주소 등이 포함된 것으로 알려졌다. 잘못 발송되었음을 바로 인지하여 이를 중단하고 발송된 3000여건의 메일을 회수하는 등의 사태 수습에 나섰으나, 200여건의 메일은 이미 고객이 수신한 것으로 파악되고 있다. 관계자는 '전산을 입력하는 도중 실수로 발생한 사고였다. 재발 방지를 위해 최선을 다하겠다'고 해명하였으나, 고객파일에 포함되었던 피해자들이 손해배상에 대한 민사소송을 제기할 예정이어서 법정 분쟁으로 비화될 전망이다.

외국에서는 미국의 한 보안 소프트웨어 업체가 자사 직원 수 천명의 정보를 분실하는 사고

[1] CVE-2006-0058, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0058

가 있었다. 외부 감사업체의 직원이 해당 업체의 정보가 담긴 백업 CD를 항공기 좌석에서 분실한 사고인데, 분실한 CD에는 직원의 이름, 주소, 생년월일, 사회보장번호 등이 포함되었으며 데이터는 암호화되지 않았던 것으로 밝혀졌다.
그 밖에 한 다국적 IT 기업은 자사 직원 20만 명의 정보를 분실하는 사고도 있었다. 해당 기업에 서비스를 제공하는 투자신탁 회사의 직원이 사용하는 노트북을 사외에서 사용 중 분실한 사고인데 분실한 노트북에는 직원의 이름, 사원정보, 사회보장번호 등이 포함되었다. 그러나 앞선 보안 소프트웨어 업체의 경우와는 이 정보를 이용하기 위해서는 고유한 어플리케이션이 필요하며 분실 즉시 보고되어 관련 어플리케이션에 대해 비활성화 처리를 하여, 해당 데이터가 악용될 소지는 희박하다고 밝혔다.

앞의 사례에서 다루었던 신용정보 유출사고는 외부 침입에 의한 사고가 아닌 내부자의 실수로 인한 유출 사고였다. 외부 침입에 의한 정보보안은 대다수의 기업이 중요성을 인식하고 보안정책에 있어 지속적인 투자를 하지만 내부정보 보안의 경우 그 중요성은 공감하고 있으나 보안체계는 상대적으로 미흡한 것이 현실이다. 기업의 중요한 정보자산을 다루는 클라이언트 중 수많은 변수를 가지며 솔루션으로 통제가 어려운 것은 바로 사람이다. 휴먼에러의 가능성을 예측하고 피해가 발생할 수 있는 정보자산에 대해 위험을 제거하는 것이 내부보안의 1차적 방법이며 최종적으로 내부 직원의 지속적인 교육을 통해 보안 의식을 높이는 것이 궁극적인 해법이 될 수 있겠다.

국내에서 발생한 고객정보 유출사고의 경우 금융기관에서만 국한되어 발생할 수 있는 것이 아닌 신용정보를 관리하는 모든 기업에게 간과할 수 없는 사안이라 할 수 있다. 재난이 우리에게 주는 교훈은 앞으로 일어날 수 있는 더 큰 재난에 대한 예방을 배우는 기회를 주는 것이다. 이번 신용정보 유출사고를 반면교사(反面教師)로 삼아 보호될 정보 자산의 위험 관리(Risk Management)에 대해 다시 한번 살펴보는 기회로 삼아야 하겠다.

Ⅳ. 3월 세계 악성코드 동향

최근 몇 달 동안 전세계 컴퓨터 보안의 동향은 개인 정보 유출에 초점이 맞추어지는 듯 하다. 한국에서는 온라인 게임 아이템 탈취를 목적으로 제작된 트로이목마가 2005년 여름부터 확산되기 시작하였으며 일본 역시 2005년 겨울부터 이러한 형태의 트로이목마가 발견되기 시작하였다. 그리고 2006년에는 유럽 지역 역시 사용자 개인 정보 유출을 위한 목적으로 제작된 트로이목마가 외신에 자주 등장하고 있으며 각종 보안 컨퍼런스에서도 개인 정보 유출과 관련한 논문들이 등장하고 있다.
이러한 전세계 컴퓨터 보안의 큰 흐름 속에서 일본의 악성코드 동향은 전반적인 악성코드의 수치 감소에도 불구하고 P2P 프로그램을 이용하여 확산되는 웜에 의해 감염된 시스템의 개인 정보가 유출되는 큰 사고가 발생하여 개인 정보 보호를 중요시하는 일본 사회에 큰 충격을 주었다. 그리고 중국은 트로이목마의 강세 속에서도 애드웨어의 급격한 증가를 이루고 있어 큰 우려를 낳고 있다. 이러한 아시아권의 흐름과는 달리 유럽 지역의 악성코드 동향에서는 메일로 전파되는 메스메일러(Mass Mailer)가 여전히 강세를 보이고 있다.

(1) 일본의 악성코드 동향

작성자: 김소헌 주임연구원(sohkim@ahnlab.com)

개인정보 불법 취득을 위한 공격으로 인해 입게 되는 금전적 피해의 위험성이 대두되고 있는 것은 세계적인 현상으로 보여진다. 한국에서는 리니지핵 트로이목마[1] 등 온라인 게임의 계정을 불법적으로 취득하기 위한 트로이목마 형태의 악성코드가 확산되고 있듯이 일본도 P2P프로그램의 취약점을 악용하는 안티니 웜[2]에 의한 피해가 심각한 상황이다. 게다가 최근 일본에서는 일본어로 만들어진 피싱 사이트가 발견되어 사용자의 경각심을 필요로 하고 있다. 일본의 경우 과거부터 사용자를 속여서 요금을 청구하는 형태의 사기로 인한 피해가 종종 발생하고 있었으나 최근 발생하는 피싱은 그 대상이 카드회사나 증권관련 회사 등 금융 관련 기관으로 확대되고 피싱 서버까지 운영되고 있는 실정이다. [그림1]은 마치 원래 홈페이지인 것처럼 위장하여 피싱 서버로 운영되고 있는 웹사이트이다. 해당 사이트의 원래 URL은 www.kabu.com 이지만 [그림1]과 같이 wwwkabu.com으로 되어 있어 사용자로 하여금 착각하도록 유도하고 있는 것을 볼 수 있다.

[1] V3 진단명, Win-Trojan/LineageHack
[2] V3 진단명, Win32/Anntiny.worm

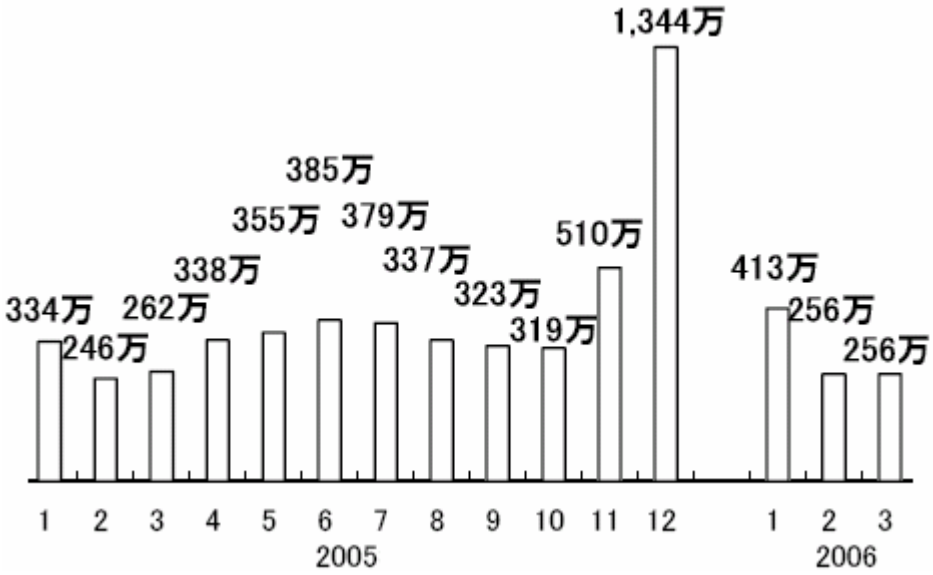
[그림1] 일본에서 발견된 피싱사이트(출처: www.rbl.jp)

이외에도 최근에는 일본의 카드회사 홈페이지인 것처럼 위장한 메일이 사용자들에게 배포된 사례도 보고되고 있다. 금융기관의 특성 상 개인의 정보가 유출될 경우 매우 심각한 상황에 빠질 가능성이 매우 높으므로 이에 대한 경각심을 가져야 할 것이다.

많은 보안관련 기관에서는 피싱에 의한 피해가 점점 늘어날 것이라고 예상하고 있고 피싱의 기법이 점점 다양해지는 현재 상황으로 미루어보아 일본에서도 피싱에 의한 피해가 발생할 가능성은 점점 높아질 것으로 생각된다.

일본의 악성코드 동향

일본의 악성코드 동향과 관련한 가장 큰 이슈는 전월에 이어 악성코드 발견 건수가 점차적으로 줄어들고 있는 것이다. [그림2]는 일본 IPA에서 집계한 월별 악성코드 발견 통계이다. 1월의 경우 소버 웜의 영향으로 수치가 증가했으나, 이 웜의 확산이 줄어든 시점인 2월부터는 전년도에 비해서 악성코드 발견 수치가 크게 줄어든 것을 알 수 있다.



[그림2] 일본의 월별 악성코드 발견 추이

이러한 현상이 발생한 원인은 최근 발견되는 악성코드 유형이 매스메일러와 같은 웜 보다는 트로이목마나 애드웨어류가 많기 때문이다. 일반적으로 트로이목마는 자체 전파력을 가지고 있지 않지만 최근에는 취약점이 존재하는 웹사이트에 자신을 배포할 수 있도록 스크립트를 삽입하는 등 다른 매체들을 적극적으로 이용하고 있다. 그러나 이러한 전파 방식의 특성 상 웹 사이트에서 배포하는 스크립트나 악성코드 파일이 제거되면 더 이상 확산되지 못하고 소멸되는 한계가 있기 때문에 웜에 비해 전파력은 미비한 수준이다.

2006년 3월 일본에서 가장 많은 확산을 보였던 악성코드는 넷스카이 웜[1]이었다.

[1] V3 진단명, Win32/Netsky.worm

Window/Dos Virus	금월피해 전월피해	Macro Virus	금월피해 전월피해	Script Virus	금월피해 전월피해
Win32/Netsky	988 1,004	Xm/Laroux	11 11	VBS/Redlof	46 42
Win32/Mytob	531 526	XF/Sic	7	VBS/Loveletter	8 6
Win32/Bagle	449 372	W97M/X97M/P97 M/Tristate	5 7	VBS/Kakworm	3 5
Win32/Mydoom	298 251	W97M/Ethan	1	Wscript/Fortnight	2 7
Win32/Mywife	288 310	W97M/Marker	2	VBS/Soraci	1 27
Win32/Klez	195 183	W97M/Melissa	1		

[표1] 악성코드 피해 신고 현황(출처: 일본 IPA)

[표1]은 일본의 IPA(www.ipa.go.jp)에서 발표한 자료 중 악성코드 종류 별 감염 신고 현황에 대한 통계이다. 넷스카이 웜의 피해 신고는 988건으로 전월에 비해 약간 감소하였다. 넷스카이 웜을 제외한 다른 악성코드들의 경우 전월과 비슷한 수준을 보이고 이와 관련해서 특이할 만한 사항은 없는 것으로 보여진다.

악성코드의 감염 경로 별 통계

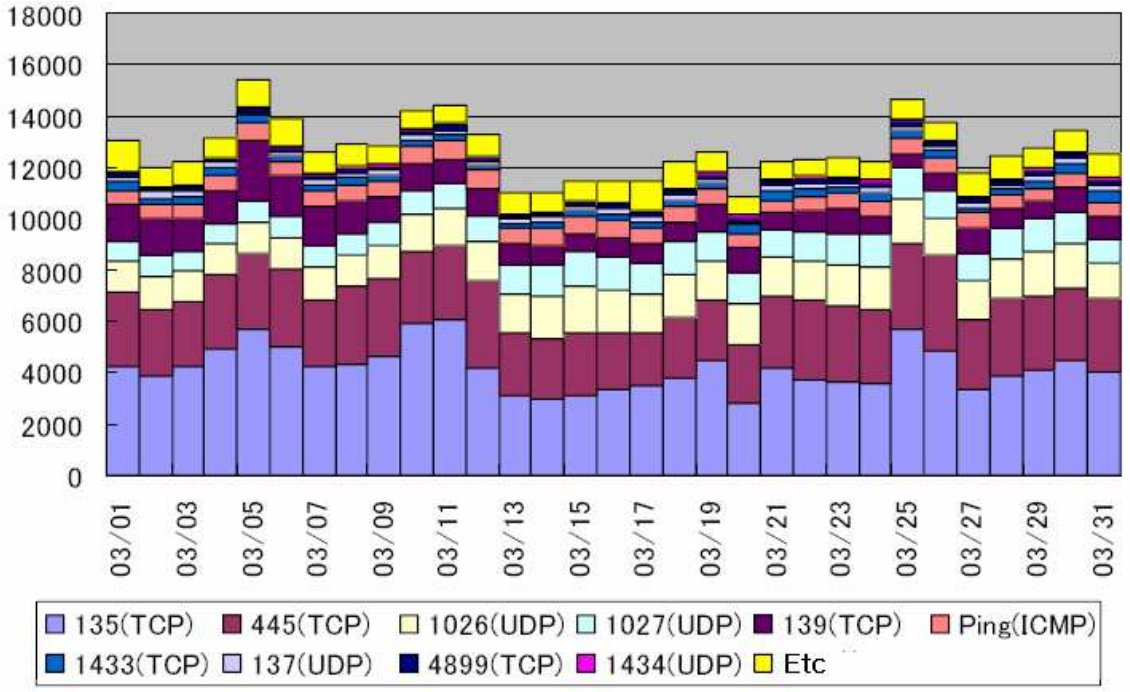
[표2]는 악성코드의 감염 경로 별 통계를 나타낸 것이다. 전월과 동일하게 메일을 이용해 확산되는 매스메일러 류가 가장 많은 양을 차지하고 있는 것을 알 수 있다. 메일 이외에는 주로 네트워크가 악성코드의 확산 경로로 사용되고 있는 것을 볼 수 있다. 네트워크를 이용한 악성코드의 확산은 작년의 수치와 비교하여 많은 증가율을 기록하고 있는 것으로 보여지며 이러한 증가 수치는 당분간 지속될 것으로 예측된다.

감염경로	피해 건수					
	2006년 3월		2006년 2월		2005년 3월	
메일	4,140	96.9%	4,207	97.9%	4,780	99.1%
외부의 모체	1	0.0%	0	0.0%	2	0.0%
다운로드	4	0.1%	3	0.1%	3	0.0%
네트워크	122	2.9%	112	2.6%	54	1.1%
기타	3	0.1%	2	0.0%	8	0.2%
합계	4,270		4,324		4,846	

[표2] 악성코드 감염 경로 통계(출처: 일본IPA)

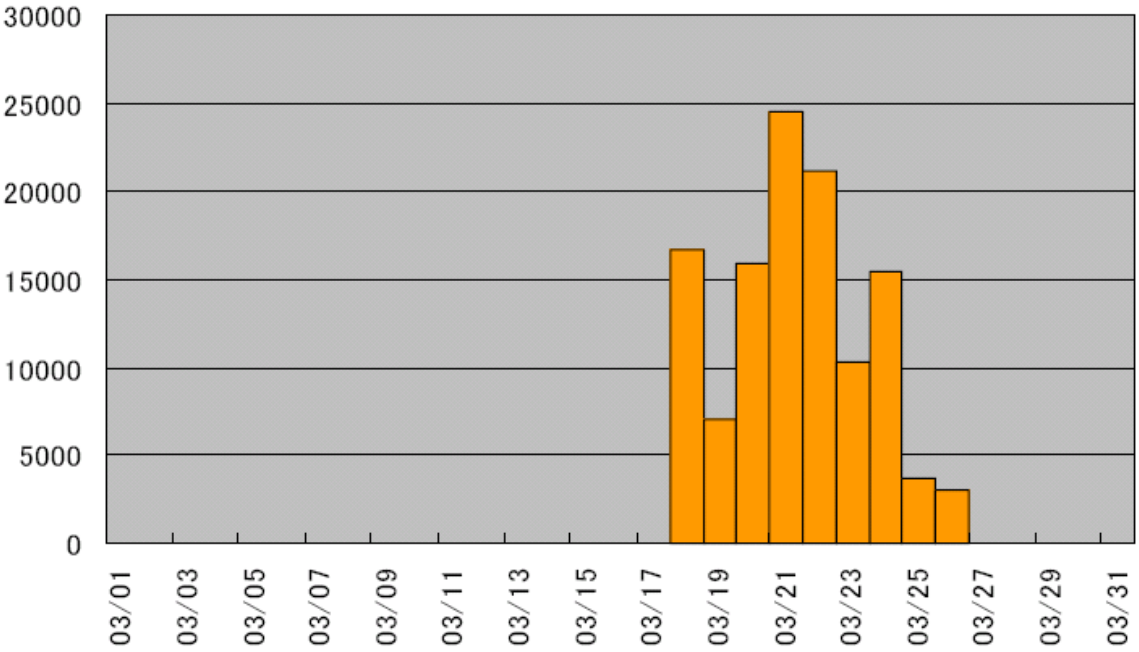
일본 네트워크 트래픽 현황

[그림3]은 3월 한 달 동안 일본의 네트워크 트래픽 현황에 대한 통계를 그래프로 나타낸 것이다. TCP 135번 포트와 TCP 445번 포트의 트래픽이 매우 많은데 이 두 포트들은 윈도우 시스템에서 사용되는 포트들이지만, 악성 봇 등이 윈도우 시스템의 취약점을 이용하여 전파될 때 사용되기도 하므로 주의가 필요하다.



[그림3] 일본의 네트워크 트래픽 현황(출처: 일본IPA)

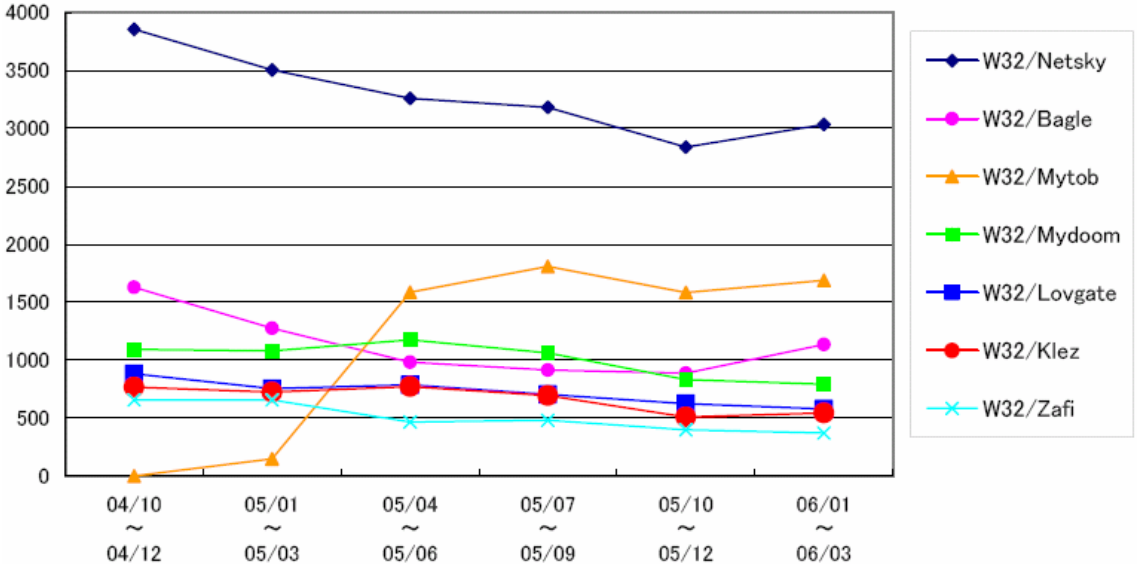
3월의 일본 네트워크 트래픽 현황과 관련하여 특이할 사항은 중국으로부터의 서비스 거부 공격이 발생한 것이다. [그림4]는 공격이 발생한 시점에서 트래픽 발생량에 대한 집계인데 3월 18일부터 급격하게 트래픽이 증가한 것을 볼 수 있다. 그러나 일본에서 이로 인한 실제 피해가 발생하지는 않았다.



[그림4] 일본의 3월 네트워크 트래픽 현황(출처: 일본IPA)

2006년 1분기 일본 동향

2006년 1분기 일본의 악성코드 동향의 특징은 넷스카이 웜과 마이톱 웜, 베이글 웜의 확산이 여전히 계속되고 있다는 것이다. [그림5]는 분기별 악성코드 피해 현황을 그래프로 나타낸 것이다.



[그림5] 분기별 악성코드 피해 현황

넷스카이 웜의 피해가 여전히 가장 많은 수치를 기록하고 있는 것을 볼 수 있다. 최근에도 여러 변형이 발견되고 있는 마이톱 웜, 베이글 웜과 달리 오랜 기간 동안 변형이 발견되지 않고 있음에도 불구하고 넷스카이 웜이 여전히 많은 확산도를 유지하고 있는 현상은 PC 사

용자나 기업 보안 의식 강화의 필요성 등 여러 면에서 시사하는 바가 크다.

(2) 중국의 악성코드 동향

작성자: 장영준 연구원(zhang95@ahnlab.com)

2006년 3월 중국 악성코드 동향은 2월에 이어서 트로이목마와 백도어 유형이 여전히 강세를 보이고 있다. 라이징(Rising)과 강민(JiangMin)의 악성코드 동향들을 살펴보더라도 트로이목마 유형이 강세라는 것을 잘 알 수 있으나, 강민의 경우에는 애드웨어 형태가 악성코드 동향의 주된 키워드로 작용하는 것으로 미루어 애드웨어와 스파이웨어 형태가 중국 내에서도 심각한 우려를 낳을 정도로 확산되어 있는 것을 짐작할 수 있다. 이러한 사항들을 바탕으로 2006년 3월 중국 악성코드 동향을 살펴보도록 하자.

악성코드 TOP 5

순위		Rising
1	-	Trojan.DL.Agent[1]
2	↑ 1	Backdoor.Gpigeon[2]
3	↓ 1	Trojan.DL.Small[3]
4	-	Trojan.PSW.LMir[4]
5	New	Dropper.Agent[5]

[표1] 2006년 3월 라이징(Rising) 악성코드 TOP 5

2006년 3월 라이징의 악성코드 TOP 5를 살펴보면 5위를 차지하고 있는 Dropper.Agent가 새롭게 순위권에 진입한 것을 제외하고는 전체적인 순위 상으로는 큰 변화가 없다.

순위		JiangMin
1	New	Adware/Downloader.QQHelper.cb
2	-	TrojanSpy.Agent.jp[6]
3	↓ 2	TrojanDownloader.Delf.sn[7]
4	New	Adware/Downloader.QQHelper.gen
5	New	TrojanSpy.Agent.ex[8]

[1] V3 진단명, Win-Trojan/Agent
[2] V3 진단명, Win-Trojan/GrayBird 또는 Win-Trojan/Hupigon
[3] V3 진단명, Win-Trojan/Xema
[4] V3 진단명, Win-Trojan/LmirHack
[5] V3 진단명, Dropper/Agent
[6] V3 진단명, Win-Trojan/Agent
[7] V3 진단명, Win-Trojan/Downloader
[8] V3 진단명, Win-Trojan/Agent

[표2] 2006년 3월 강민(JiangMin) 악성코드 TOP 5

강민의 악성코드 TOP 5에는 라이징의 순위와는 달리 많은 변동들이 있었다. 먼저 지난 2월 1위를 차지한 TrojanDownloader.Delf.sn은 2계단이나 하락하여 3위를 차지하였으며 그 자리를 대신해서 Adware/Downloader.QQHelper.cb라는 애드웨어가 자치하고 있다. 2006년 들어서 강민의 중국 악성코드 동향에서 애드웨어가 1위를 차지한 것은 이번이 처음이며 해당 애드웨어와 유사한 변형들인 Adware/Downloader.QQHelper.gen도 4위를 차지하며 순위권에 새로 진입한 것으로 미루어 해당 애드웨어 변형들이 중국 내 상당히 많이 퍼져 있는 것으로 보인다. 2위에는 TrojanSpy.Agent.jp이 순위 변동없이 그 자리를 지키고 있으며 5위 역시 이번 3월에 새롭게 순위에 진입한 TrojanSpy.Agent.ex이 차지하고 있다

주간 악성코드 TOP 5

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

[표3] 2006년 3월 라이징(Rising) 주간 악성코드 순위

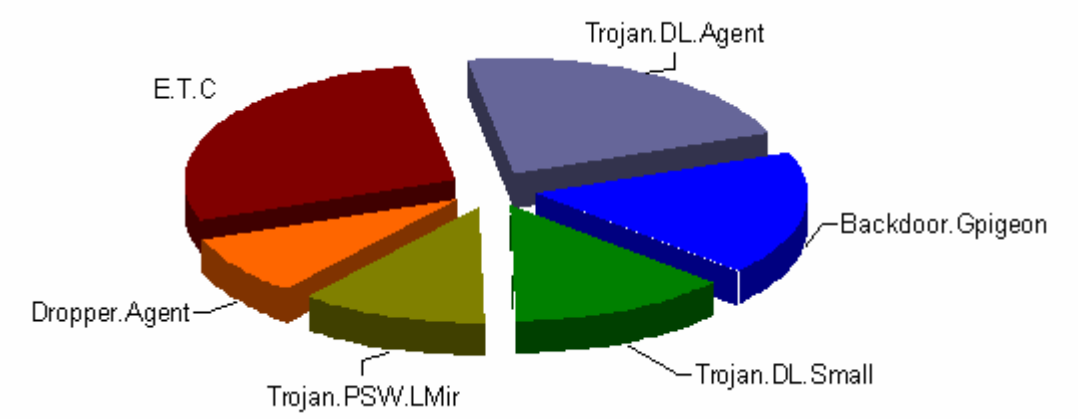
2006년 3월 주간 악성코드 동향을 살펴보면 라이징의 경우에는 커다란 변화 없이 악성코드 TOP 5에서와 유사한 순위 흐름을 보여주고 있다. 그러나 1주차에서는 5위에 AdWare.Hbang라는 애드웨어가 잠시 순위권에 진입하였으나 2주차에 이르러서는 Dropper.Agent가 순위에 진입하면서 AdWare.Hbang이 순위권에서 밀려나게 되었다.

순위	1주	2주	3주	4주
1	TrojanSpy.Agent.jp	TrojanSpy.Agent.jp	Adware/Downloader.QQHelper.cb	Adware/Downloader.QQHelper.gen
2	TrojanDownloader.Delf.sn	Adware/Downloader.QQHelper.cb	TrojanDownloader.Delf.sn	Adware/Downloader.QQHelper.cb
3	Adware/Downloader.QQHelper.f	Adware/Downloader.QQHelper.bb	Adware/Downloader.QQHelper.f	Adware/Downloader.QQHres.gen
4	TrojanSpy.Agent.ex	TrojanDownloader.Delf.sn	TrojanSpy.Agent.ex	Adware/Downloader.QQHjit.gen
5	Adware/Downloader.QQHelper.aq	TrojanDownloader.Agent.yi	Trojan/PSW.MimaThief.20.k	TrojanSpy.Agent.ex

[표4] 2006년 3월 강민(JiangMin) 주간 악성코드 순위

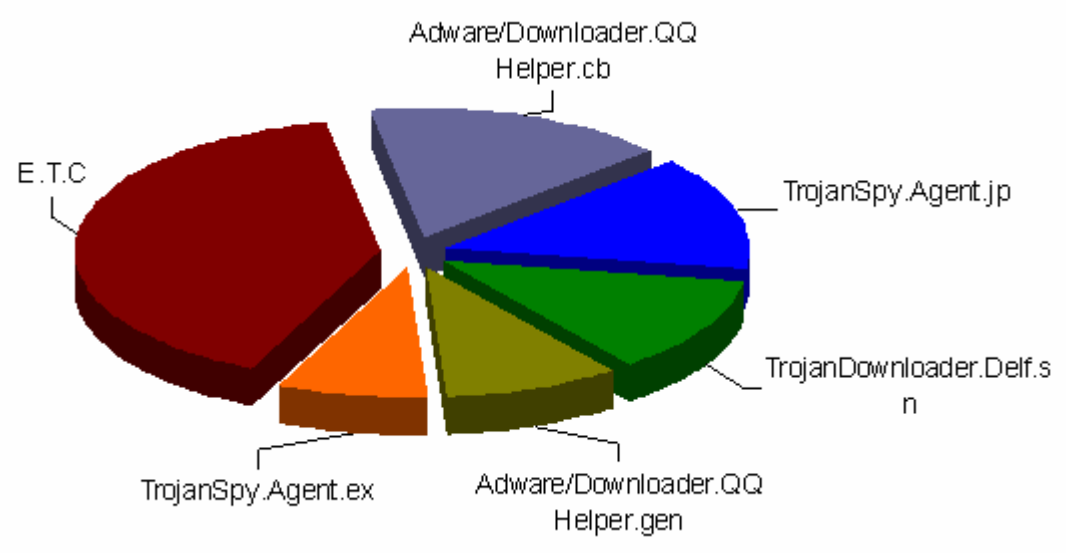
라이징의 정적인 흐름과 반대로 강민의 주간 악성코드 동향에서는 1주차에서부터 Adware/Downloader.QQHelper 애드웨어들이 순위권으로 진입하기 시작하며 1주차에서만 2개의 변형들이 순위권으로 진입하였다. 해당 애드웨어들은 2주차에서는 1주차에서보다 순위가 상승하며 점차적으로 감염 신고가 많아졌었던 것으로 분석된다. 그리고 3월 20일 이후인 4주차에 이르러서는 1위에서 4위까지 모두 해당 애드웨어들이 차지하고 있어 3월 중순부터 중국 내에서는 해당 애드웨어들이 급격하게 증가하기 시작한 것으로 분석되며 이에 따른 피해사례도 급격하게 증가했으리라 예상된다. 해당 애드웨어가 4월에 이르러서는 어떠한 동향을 보이게 될지 상당히 주목된다. 그리고 중국 내에서도 다른 국가에서와 같이 별도의 전문적인 애드웨어 및 스파이웨어 치료 소프트웨어가 주목을 받고 해당 시장이 열리게 될 가능성도 클 것으로 보여진다.

악성코드 분포



[그림1] 2006년 3월 라이징(Rising)의 악성코드 분포

라이징의 악성코드 분포에서는 지난 2월과 거의 유사한 분포를 보이며 대부분의 악성코드가 현재 상태를 유지하고 있다. 1위를 차지한 Trojan.DL.Agent는 지난달 보다 3% 가량 감소한 21%를 차지하고 있다. 그리고 Backdoor.Gpigeon은 17%를 차지하며 지난달에 비해 4% 증가하며 유일하게 3월 악성코드 분포에서 증가치를 보여주고 있다. Trojan.DL.Small은 13%를 차지하고 있으며 Trojan.PSW.LMir은 지난 달과 동일한 10%를 유지하며 커다란 변화를 보여주지 않고 있다. 기타에 포함된 악성코드들은 30%를 보여주었던 지난 달에 비하여 3% 가량 감소한 27%를 보여주고 있다.



[그림2] 2006년 3월 강민(JiangMin)의 악성코드 분포

악성코드 TOP 5에서 큰 변화를 보여 주었던 강민의 동향에서는 Adware/Downloader.QQHelper 변형들이 전체 악성코드 분포에서 25%를 차지하고 있다. 그러나 기타에 포함된 악성코드들이 전체의 40%를 차지하고 있어 순위권에 포함되지 않은 다양한 악성코드들이 많이 통계에 포함되어 있는 것으로 보여진다. TrojanSpy.Agent.jp가 14%, TrojanDownloader.Delf.sn가 11%를 차지하며 겨우 2자리의 수치를 확보하고 있으며 나머지 악성코드들의 분포는 10% 미만대를 이루고 있다. 이로 미루어 강민의 통계에서는 널리 확산되지 않은 군소 악성코드들이 많은 것으로 추정되며 다음 달 악성코드 동향에 얼마나 많은 영향을 미치게 될지 주목된다.

2006년 1분기 악성코드 동향

2006년 1분기는 전반적으로 웜과 트로이목마라는 이 두 악성코드 형태의 흐름을 이야기 해 볼 수 있다. 2005년 1분기와 비교하여 2006년 1분기는 어떠한 변화가 중국 악성코드 동향에서 나타났는지 한번 되돌아 보도록 하자.

2006년 1월 순위		Rising	2006년 1월 순위		Rising
1	↑1	TrojanDroper.Worm.Bagz	1	↑1	Backdoor.Agent
2	↑3	Backdoor.Rbot	2	↑1	Trojan.PSW.LMir
3	New	Worm.Agobot	3	↓2	Backdoor.Gpigeon
4	↓3	Worm.Netsky	4	New	Trojan.DL.Small
5	↓2	Worm.Lovgate	5	↓2	TrojanDownloader.Small

[표5] 2005년 1월과 2006년 1월 라이징의 악성코드 TOP 5

[표5]는 2005년 1월과 2006년 1월 라이징의 악성코드 TOP 5를 같이 나타낸 것이다. 순위 내용만으로 놓고 본다면 작년와 올해 동기간의 중국 악성코드 동향 자체가 판이하게 다른 악성코드들로 이루어져 있다는 것을 알 수 있다. 2005년 1월 동향에서는 네트워크 또는 메일로 전파되는 웜들이 절대 강세를 이루고 있으며 그 순위도 계속 상승하였으나, 2006년 1월 동향에서는 트로이목마와 백도어 유형들이 지속적으로 순위가 상승하며 동향의 전반을 이루고 있는 것을 잘 알 수 있다.

2005년 2월 순위		CNCVERC	2006년 2월 순위		Rising
1	New	Worm_Bropia.F	1	New	Trojan.DL.Agent
2	↓1	Worm_Netsky.D	2	↑2	Trojan.DL.Small
3	-	Worm_Bbeagle.J	3	-	Backdoor.Gpigeon
4	-	Worm_AgoBot	4	↓2	Trojan.PSW.LMir
-	-	-	5	New	AdWare.Hbang

[표6] 2005년 2월과 2006년 2월 CNCVERC와 라이징의 악성코드 TOP 5

[표6]은 2005년 2월과 2006년 2월 중국 국가 컴퓨터 바이러스 대응중심과 라이징의 악성코드 TOP 5를 비교한 것이다. 이 도표에서도 [표5]에서와 같이 웜과 트로이목마가 절대적인 강세를 이어가고 있는 것을 알 수 있다. 2005년 2월에는 메일로 전파되는 웜이 전반적인 강세를 이루고 있었다면 2006년 2월에는 트로이목마와 애드웨어가 주된 강세를 이루고 있다.

2005년 3월 순위		Rising	2006년 3월 순위		Rising
1	-	TrojanDroper.Worm.Bagz[1]	1	-	Trojan.DL.Agent
2	-	Backdoor.Rbot	2	↑1	Backdoor.Gpigeon
3	New	Worm.MSN.Bropia[2]	3	↓1	Trojan.DL.Small
4	↓1	Worm.Agobot	4	-	Trojan.PSW.LMir
5	New	Trojan.Win32.StartPage[3]	5	New	Dropper.Agent

[표7] 2005년 3월과 2006년 3월 라이징의 악성코드 TOP 5

[표7]은 2005년 3월과 2006년 3월 라이징의 악성코드 TOP 5를 같이 나타낸 것이다. 2005

[1] V3 진단명, Win32/Bagz.worm
[2] V3 진단명, Win32/Bropia.worm
[3] V3 진단명, Win-Trojan/StartPage

년 3월에는 중국내에서는 메일로 전파되는 TrojanDroper.Worm.Bagz과 MSN 메신저로 전파되는 Worm.MSN.Bropia가 많은 확산을 보였던 것에 반해 2006년은 개인정보 유출 증상을 가진 트로이목마로 인한 피해가 증가한 것을 알 수 있다.

앞서 살펴본 바와 같이 2006년 1분기는 2005년 동기에 비해 웜에 의한 피해는 감소한 반면, 개인정보 유출을 목적으로 하는 트로이목마로 인한 피해는 대폭 증가하였다. 이러한 추세는 2006년 한 해 동안 당분간 지속될 것으로 전망된다.

(3) 세계의 악성코드 동향

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

2006년 3월도 전통적인 매스메일러 웜들이 피해 집계의 대부분을 차지하고 있다. 다만 2월에 이어 3월에도 유럽 지역에서 애드웨어 성 트로이목마가 스팸 메일 형태로 배포되어 순위권을 차지하고 있다.

영국 소포스사의 통계[1]에 따르면 1위는 자피 변형(V3 진단명 Win32/Zafi.worm)으로 지난 2월에는 4위를 차지하였으나 다시 1위를 차지하여 유럽 지역에서 여전히 피해가 큰 것을 알 수 있다. 자피 웜 변형으로 인해 지난 달 1, 2 위였던 넷스카이 웜 변형과 나이젬 변형(V3 진단명 Win32/Nyxem.worm)은 2위, 3위로 순위에서 밀려났다. 지난 달에도 트로이목마인 Troj/Clagger-G가 8위를 차지했는데 또 다른 변형인 Troj/Clagger-I가 다시 6위로 새롭게 진입했다. 자체 전파력이 없는 트로이목마 특성상 트로이목마가 순위권에 들어오는 것은 흔하지 않은 일이므로 동일 제작자가 3월에도 스팸 메일을 통해 트로이목마를 대량으로 배포한 것으로 추정된다.

캐스퍼스키 연구소의 3월 통계[2]에 따르면 마이톱 웜 변형(V3 진단명 Win32/Mytob.worm)과 넷스카이 웜 변형이 1, 2위를 차지하고 있으며 지난 달 2위였던 러브게이트 웜(V3 진단명 Win32/Lovgate.worm)은 3위가 되었다. 그러나 피해 신고나 메일에 따른 집계가 아닌 사용자들이 온라인 스캐너를 통해 검사한 결과에 따른 순위[3]에 따르면 1위는 사용자 정보를 훔쳐가는 LdPinch 변형이 차지했으며 특정 은행의 인터넷 뱅킹 계정과 비밀번호를 훔쳐가기 위해 제작된 뱅커(V3 진단명 Win-Trojan/Banker)와 반코스 변형(V3 진단명 Win-Trojan/Bancos)들이 3, 6, 7위를 차지하고 있어 여전히 이들 트로이목마가 많이 제작되고 퍼졌음을 알 수 있다.

온라인 검색의 경우 백신을 사용하지 않거나 다른 백신을 사용하다가 검색되지 않을 때 이용하는 경우가 많으므로 온라인 검색 결과 역시 100% 정확하게 어떤 악성코드가 많이 퍼졌는가를 통계내기는 어렵지만 백신사의 신고와 메일 검사 결과에 의존한 통계와 달리 실제 사용자 시스템에서 검사된 결과이므로 해당 순위는 동향 파악을 위한 참고 자료 정도로 사용될 수 있다.

[1] http://www.sophos.com/pressoffice/news/articles/2006/03/toptenmar06.html
[2] http://www.viruslist.com/en/analysis?pubid=183159280
[3] http://www.viruslist.com/en/analysis?pubid=183170874

V. 이달의 ASEC 컬럼 - 일본의 위니 사건을 통해 본 P2P와 보안

작성자: 차민석 주임연구원(jackycha@ahnlab.com)

위니란?

위니(Winny)는 2002년 도쿄대 조교수인 카네코 이사무씨에 의해 개발된 일본의 대표적인 P2P(Peer-to-Peer) 프로그램으로 한국의 소리바다와 유사한 프로그램이라 할 수 있다. 하지만, 소리바다는 MP3 파일만 공유하는데 반해 위니는 모든 파일을 공유할 수 있다. 위니 프로그램이 인기를 끌면서 한국의 소리바다처럼 저작권 침해 문제가 불거지고 결국 위니 제작자는 저작권법 위반방조 혐의로 2004년 5월 10일 오전 7시 52분 경찰에 체포되어 현재 재판 중이다. 위니 제작자는 2006년 3월 11일 NPO 법인 소프트웨어 기술자 연맹(LSE) 오사카 세미나에서 "위니는 기술 검증을 위해서 개발한 것으로 바이러스에 의한 정보 누설은 예상 외의 사건"이라고 밝혔다. 그는 "바이러스에 의한 정보 누설은 유감이고 예상 외의 사건이다. 문제는 위니가 아니고 바이러스를 만드는 사람, 네트워크 상에 전파 시키는 사람 그리고 감염되는 사람"이라고 밝혔다. 카네코 씨는 경찰에 더 이상 위니를 업데이트하지 않겠다고 밝혔다.

위니를 악용한 악성코드들

위니가 일본에서 유행하면서 일본의 악성코드 제작자들은 위니를 이용한 악성코드를 제작하기 시작한다. 안티니 웜(Win32/Antinny.worm)이 대표적이며 이 웜은 2003년 8월에 최초 보고되었다.[1] 이 웜은 위니의 공유 폴더에 자신을 복사해 전파될 기회를 삼는다. 이후 안티니 웜과 위니를 악용하는 악성코드가 등장했는데 최근에 등장한 악성코드는 시스템에 존재하는 문서 파일 등을 찾아 압축 후 공유 폴더에 복사하기도 한다. 이에 개인의 사생활 자료와 기밀자료 유출 문제가 생겼고 2006년 3월 기업과 자위대 등의 기밀자료 유출이 언론으로 알려졌다.

사건, 사고들

일본에서도 P2P 프로그램을 이용한 저작권 침해 문제로 2001년 WinMX 이용자가 사용 소프트웨어를 공개해서 2001년 체포되었고 2003년 9월에 위니 이용자 2명이 저작권법 위반 혐의로 체포된 적이 있다.

안티니 웜으로 인한 피해는 2003년부터 존재했지만 본격적으로 일본에서 크게 알려진 것은 2006년 2월 하순 해상자위대 자위함의 암구어와 전투훈련 내용 등 기밀정보가 안티니 웜에 감염된 위니를 통해 인터넷에 유출되고 항공 자위대와 JAL 항공에서도 유사한 사건이 일어나는 등 그 파장이 일본 사회 각계로 확산되었고, 이후 다른 기업에서도 유사 문제가 발생한 것이 알려 지면서이다.[2] 2006년 3월 8일 NTT 서일본은 사원의 자택에 있는 개인용 컴퓨터

[1] http://info.ahnlab.com/smart2u/virus_detail_1212.html
[2] http://www.ddaily.co.kr/news/?fn=view&article_num=8727

가 웜에 감염되어 컴퓨터에 보관되어 있던 고객 정보를 포함한 업무 관련 파일이 위니를 통해 유출되었다고 발표했다. 모 보안업체 직원 역시 2005년 3월에 회사 자료를 집에 가져갔다가 영업 자료가 유출되었다고 한다.

이에 안철수 연구소는 2006년 3월 13일 위니를 이용한 악성코드를 진단/치료하는 전용백신과 위니 프로그램 자체도 찾아 지워주는 전용백신을 제공하기도 했다.[1]

이번 사건의 교훈

악성코드 감염으로 인한 자료 유출은 어제 오늘의 일은 아니며 P2P 프로그램이 처음 등장했을 때도 개인정보나 기밀자료의 유출을 우려했었다. P2P 프로그램을 통해 발생할 수 있는 보안 위험은 크게 사용자 미숙으로 인한 자료 유출과 악성코드로 인한 자료 유출로 나눌 수 있다. 과거 발생한 개인자료나 기밀자료의 누출은 보통 사용자가 P2P 프로그램을 제대로 이해하지 못해 기밀자료가 포함된 폴더까지 공유해 버리는 실수에서 발생했다. 이에 악성코드 제작자들은 P2P 프로그램 설정을 변경해 시스템 전체를 공유 폴더로 만들거나 시스템에 존재하는 문서 파일이나 그림 파일을 공유 폴더로 몰래 복사시키는 형태로 악용했다.

이번 사건에서 간과해서는 안될 문제가 회사 주요 문서를 집에 가져가는 직원에 대한 통제이다. 회사에서는 비교적 보안을 철저히 하지만 개인이 회사 자료를 집에 가져갈 경우 회사 자료가 유출될 가능성이 높아진다. 특히 모 보안업체의 직원 역시 회사 자료를 집에 가져가서 유출되었는데 집에 있는 컴퓨터에는 보안 프로그램을 설치하지 않고 사용했다고 한다. 회사는 직원들에 대해 회사 기밀 자료를 집에 가져가서 작업하지 말 것과 보안에 대한 교육을 철저히 해야 할 것이다.

현재 위니는 제작자가 체포되어 재판 중이고 제작자도 더 이상의 프로그램 개선은 없을 것이라고 발표했다. 위니의 사용자가 줄어든다면 위니를 통해 전파되는 악성코드로 인한 피해는 줄어 들겠지만, 최근에는 셰어(Share)라는 P2P 프로그램이 일본에서 사용자가 증가하고 있어 셰어 프로그램 사용자를 목표로 하는 악성코드가 증가할 것으로 예상된다.

[1] http://info.ahnlab.com/ahnlab/report_view.jsp?num=512